Rechtliche Studie zum Cypher Social Contracts Konzept „Fides“

erstellt im Auftrag des

Projektkonsortiums Landleuchten

von

Prof. Dr. iur. Indra Spiecker gen. Döhmann, LL.M.

Professorin für Öffentliches Recht, Informationsrecht, Umweltrecht und Verwaltungswissenschaften sowie

Direktorin der Forschungsstelle Datenschutz

- Goethe Universität Frankfurt am Main -

sowie

Dr. iur. Sebastian Bretthauer und Dipl.-Jur. Dirk Müllmann

- Goethe Universität Frankfurt am Main -

- vorläufige Endfassung -

Stand: Januar 2023

Inhaltsübersicht

A. Studienfragen

Gegenstand der vorliegenden Studie ist die Untersuchung rechtlicher Fragen im Zusammenhang mit der Verwendung der Software Fides, die auf dem Konzept der „Cypher Social Contracts“ beruht. Die Betrachtung gliedert sich in zwei Arbeitspakete, wobei das erste Arbeitspaket zivilrechtliche Fragestellungen (C.) und das zweite Arbeitspaket (D.) datenschutzrechtliche Fragestellungen adressiert.

Im Rahmen des ersten Arbeitspakets wird aus zivilrechtlicher Sicht analysiert, ob mit der Software Fides erstellte Verträge rechtlich bindend sind bzw. seien können. Zur Beantwortung dieser Frage erfolgt zunächst eine allgemeine Bewertung der Rechtssicherheit des Konzepts sowie seiner Übertragbarkeit auf andere Systeme, wobei eine zivilrechtliche Betrachtung der aktuellen Software vorgenommen wird.

Darüber hinaus wird das System in den Stand der Forschung und der dortigen rechtlichen Lage eingeordnet. Dabei wird ein Vergleich des Abschlusses von Smart Contracts über Fides mit der Eingehung eines Vertrages mittels blockchainbasierter Systeme, wie z.B. Ethereum, vorgenommen.

Abschließend erfolgt zudem eine zivilrechtliche Bewertung des Einsatzes der Middleware LoRaWAN, die als zentraler Dienst beim Einsatz von Fides verwendet wird, sofern die Software nicht direkt ausgeführt werden kann. Der Fokus der Betrachtung liegt dabei darauf, ob sich die zuvor getroffenen zivilrechtlichen Bewertungen durch den Einsatz der Middleware ändern, sofern die Verträge im Namen der Clients (durch die Middleware) geschlossen werden.

Das zweite Arbeitspaket zielt auf die Beantwortung datenschutzrechtlicher Fragen. Im Rahmen der Untersuchung erfolgt eine Bewertung des Systems Fides in Bezug auf die allgemeinen Anforderungen der DSGVO unter besonderer Berücksichtigung von Fragen der Verschlüsselung, der Art der Kommunikation und der Datensparsamkeit.

Auch im Rahmen des zweiten Arbeitspakets erfolgt darüber hinaus eine datenschutzrechtliche Bewertung des Einsatzes eines zentralen Dienstes als Middleware,

den Fides im Namen von Geräten verwendet, die das Programm nicht direkt ausführen können.

B. Grundsätzliche Funktionsweise von Fides

Die vorliegende Studie beruht auf folgenden Angaben zur Funktionsweise von Fides und LoRaWAN:

I. Struktur und grundsätzliche Funktionsweise

Bei Fides handelt es sich um ein offenes, dezentrales Netzwerk, innerhalb dessen Nutzer Verträge schließen und abwickeln können. In dem Netzwerk werden zwei verschiedene Arten von Nutzerkategorien miteinander verknüpft: Full Nodes und Clients.

Full Nodes bilden das Rückgrat von Fides. Ihre Betreiber unterhalten Server mit in der Regel statischer IP-Adresse, auf denen die Transaktionsdaten verschlüsselt gespeichert sind. Diese Daten können zwar allgemein abgerufen, aufgrund der Verschlüsselung aber nur von den beteiligten Parteien entschlüsselt und eingesehen werden. Gespeichert werden einerseits die Templates und andererseits Informationen zum aktuellen Zustand eines existierenden Contracts, d.h. Angaben dazu in welchem Abwicklungsschritt sich ein Contract gerade befindet. Diese Informationen werden in Form des Template Index und des Contract Index vorgehalten. Ein Contract stellt dabei keinen Vertrag im Rechtssinn dar, sondern lediglich eine Verpflichtung zur Kommunikation zwischen zwei Clients, sodass in der Folge beide Begriffe in bewusster Abgrenzung zueinander verwendet werden.

Die im Full Node gespeicherten Informationen werden durch die Clients ständig aktualisiert und im Fall, dass ein Contract oder ein Template nicht im Netzwerk durch den Full Node gefunden wird, von den Parteien auch republiziert. Das Funktionieren von Fides erfordert lediglich die Existenz eines Full Nodes. Sofern jedoch mehrere existieren, sind sie in einer Ringstruktur miteinander unter einem gemeinsam gewählten Netzwerknamen verbunden. In diesem Fall kennt jeder Full Node, für den Fall des Verlassens oder Hinzutretens eines neuen Full Nodes in die Ringstruktur, lediglich die Routing Tabelle, seinen Vorgänger und eine Liste einiger Nachfolger und somit den Weg der Einwahl.

Mehrere Full Nodes teilen sich die zu speichernden Informationen untereinander auf, sodass jeder für andere Contracts und Templates zuständig ist. Die Zuständigkeit eines Full Nodes wird dabei anhand des Kriteriums der Nähe bestimmt. Dieses definiert sich

über die Nähe der Hashwerte einer Full Node ID zum Hashwert des zu speichernden Contracts und Templates. Erreicht einen Full Node die Anfrage eines Clients, für die er nicht zuständig ist, leitet er sie an den zuständigen Full Node weiter. Zur Weiterleitung an die zuständige Instanz nutzt jeder Full Node die Routing Tabelle. Im Fall der Unzuständigkeit für eine Anfrage ergibt sich aus der Routing Table jedoch immer nur der Weg zum nächsten weiterleitenden Full Node. Dadurch wird die Anfrage eines Clients mit jeder Weiterleitung näher an die für sie zuständigen Instanz herangeführt und kommt letztendlich immer beim zuständigen Full Node an, obwohl sich jede Anfrage zunächst an einen anderen Full Node richten kann.

Die Integrität der in den Full Nodes gespeicherten Inhalte kann zusätzlich über Zertifikate abgesichert werden, wobei so private Netzwerke entstehen. Die Integrität der Daten ist im Allgemeinen durch die digitale Signatur sichergestellt. Durch die zusätzliche Verwendung von Zertifikaten können aber Außenstehende zwar weiterhin auf die verschlüsselt gespeicherten Inhalte zugreifen, es ist ihnen aber nicht möglich, eigene Inhalte einzuschleusen. Ein solches Unterbinden des Schreibzugriffs schützt das Netzwerk gegen Attacken in Form von Spam. Die Einschränkung des Lesezugriffs durch Außenstehende wird hingegen bereits durch die Verschlüsselung der gespeicherten Inhalte erreicht, die nur von den Parteien eines Contracts entschlüsselt werden können. Doch auch ohne eine Absicherung des Zugangs durch Zertifikate wird der Zugriff von außen durch unberechtigte Clients als auch andere, unzuständige Full Nodes auf die Ringstruktur und die gespeicherten Informationen zurückgewiesen und so eine Bearbeitung durch unzuständige Instanzen verhindert.

Fides ist ein dezentrales System, dessen Funktionieren, anders als bei einer Blockchain, keine Etablierung von zeitlichen Beziehungen zwischen den jeweiligen Transaktionen für die Datenspeicherung voraussetzt. Dies äußert sich sowohl in Bezug auf die Full Nodes als auch die Clients. So können verschiedene, voneinander unabhängige Full Node Ringstrukturen betrieben werden, wobei die Betreiber Fides jeweils zu den von Ihnen avisierten Zwecken nutzen können. Die einzelnen Ringstrukturen stehen dann nicht in Kontakt miteinander und tauschen keine Daten aus. Vor diesem Hintergrund ist es jedoch erforderlich, dass die Clients ihre Anfragen an die richtige Ringstruktur richten. Ferner äußert sich die Dezentralität dadurch, dass auch Clients ihre Daten lokal und damit dezentral speichern.

Clients sind im Gegensatz zu Full Nodes einfache Nutzer von Fides. Sie verfügen über einen Account, der aus einem Public- und einem Private Key besteht und keine anderen Daten über ihre Person enthält. Der Account wird auf dem Endgerät der Nutzer, in der sog. Fides Instanz, gespeichert. Hier wird auch der Zugang zu mindestens einem Full Node hinterlegt, damit dem Client zumindest ein Zugangspunkt zur Ringstruktur bekannt ist. Der Kontakt zum Full Node erfolgt über den sog. Publisher als Intermediär auf dem Endgerät des Nutzers.

Die Informationen zum Template und zum Contract werden auf den Endgeräten der beteiligten Clients und im zuständigen Full Node gespeichert. Die Informationen zum Template sind dabei im Full Node für jeden lesbar, dem der Hash bekannt ist. Aktuelle bearbeitete Contracts werden dort hingegen verschlüsselt gespeichert. Die Endgeräte sind dabei die einzigen Akteure, die in der Lage sind, die Informationen zu entschlüsseln. Die Full Nodes sind zugleich nicht beliebig durchsuchbar, sodass Transaktionen nur aufgefunden werden können, sofern man über den Hash oder weitere Informationen zur Transaktion verfügt. Vor diesem Hintergrund können nur die Parteien des Contracts selbst auf die lokal gespeicherten Accountdaten zugreifen und haben somit die volle Kontrolle über die Weitergabe ihrer personenbezogenen Daten. Für das Funktionieren von Fides ist eine Weitergabe von Accountdaten zudem bereits an sich nicht erforderlich und wird in der Regel auch nicht vorgenommen. Lediglich dem Full Node am Eintrittspunkt eines Clients in eine Ringstruktur muss die IP-Adresse für den Datenaustausch bekannt sein. An dieser Stelle könnte die IP daher, jedenfalls theoretisch, von diesem Full Node getrackt und somit verarbeitet werden. Zugleich stehen die Clients nicht in direktem Kontakt miteinander. Sie tauschen sich nur über die Full Nodes als Mittlerinstanz aus.

II. Anbahnung, Abschluss und Abwicklung von Verträgen

Vor dem Hintergrund dieser grundsätzlichen Funktionsweise erfolgt die Nutzung von Fides durch Clients zur Anbahnung, dem Abschluss und der Durchführung von Verträgen wie folgt:

Einerseits kann das System, sofern ein Client den Public Key einer anderen Vertragspartei kennt, autonom zur Vertragsabwicklung zwischen beiden Seiten verwendet werden. Dies wird jedoch den Ausnahmefall darstellen. Regelmäßig wird Fides vielmehr in ein

Verifikationssystem, wie z.B. einen Onlinemarktplatz oder eine andere Art von Onlineplattform, eingebunden sein. Auf diesem Weg wird ein Client auf von anderen Clients angebotene Leistungen aufmerksam gemacht und kann deren Public Key in Erfahrung bringen. Möglich wäre aber auch eine Kommunikation beider Seiten und ein Austausch der Templatehashes oder der Public Keys per Mail.

Die Vertragsabwicklung selbst basiert sodann auf Templates. Hierbei handelt es sich um individualisierte, feststehende Vorlagen, in denen die Informationen über einen zukünftigen Vertrag enthalten sind. Sie können von einem Client für ein konkretes Geschäft erstellt werden und alle für einen Vertrag erforderlichen Informationen enthalten. Es ist jedoch auch möglich, bereits existierende Templates für andere Geschäfte erneut oder bei gleichartigen (Massen-)Geschäften immer wieder zu verwenden. Der im Full Node gespeicherte Template Index kann für das Auffinden eines passenden Templates jedoch nicht durchsucht und genutzt werden.

Ein Template wird regelmäßig von dem Client, der eine Leistung anbietet, zusammen mit seinem Public Key, z.B. auf einer Onlineplattform, in der Fides eingebunden ist, bereitgestellt werden und alle für den Vertrag erforderlichen Angaben enthalten. Es kann dort von einem anderen Client bezogen und zur Vertragsanbahnung genutzt werden. Es ist jedoch auch möglich, dass der Client, der eine Leistung erwerben will, statt des vorhandenen ein eigenes Template erstellt oder ein selbst angefertigtes nutzt.

Auf der Grundlage eines Templates erstellt ein Client lokal auf seinem Endgerät einen Contract. Hierbei handelt es sich nicht um einen Vertrag im Rechtssinne, sodass der Begriff hier, wie schon zuvor angeführt, in bewusster Abgrenzung zum Terminus Vertrag verwendet wird. Vielmehr stellt ein Contract zunächst nur die Verpflichtung zu einer Art der Kommunikation zwischen zwei Clients dar. Die Erstellung eines Contracts aus einem Template erfolgt durch die Verbindung des Templates mit dem Public Key der anderen Partei. Der Public Key, der mit dem Private Key signiert werden muss, ist somit Teil der Transaktion. Für jeden Contract wird zusätzlich ein neuer temporärer Key erstellt, wobei sich die Keys aber nicht zueinander in Beziehung setzen lassen. Die Keys werden in den Schritten „offer“ und „accept“ des jeweiligen Contracts ausgetauscht und dienen der Verschlüsselung der Daten des Contracts. Die Transaktionen, in denen die verschlüsselten

Daten enthalten sind, werden weiter von den eigentlichen privaten Schlüsseln zu den zuvor erwähnten public keys signiert.

Der Client veröffentlicht den Contract in der Folge über einen Full Node. Auf diesen neuen Contract wird der so angesprochene Client durch die Prüfung des Template Index aufmerksam gemacht. Er kann den Contract, als Aufforderung zur Kommunikation, annehmen oder ablehnen.

Die auf eine Annahme des Contracts folgenden Schritte hängen von der Gestaltung des Templates und der konkreten Situation der Vertragsanbahnung ab. Zunächst ist denkbar, dass der Client, dem der Contract offeriert wurde, einen Vertrag mit den im Template vorgesehenen Angaben eingehen möchte. Dies wird regelmäßig der Fall sein, wenn der anfragende Client, insbesondere im Fall gleichartiger Massengeschäfte, das Template des Anbieters verwendet hat oder beide Seiten zuvor außerhalb von Fides, z.B. auf einer Onlineplattform, in die Fides eingebunden ist, oder aber in der realen Welt, Vertragsverhandlungen geführt haben und sich über die Vertragsinhalte einig sind. In diesem Fall wird der Client im Contract eine entsprechende Task bestätigen, wobei er die Bestätigung an den Full Node sendet. Dort wird der geänderte Status des Contracts durch Überschreiben des alten Status aktualisiert und die neue Transaktion zu den vorhergehenden gespeichert. Möglich wäre es – als Abwandlung dieser Fallgestaltung - jedoch auch, dass das Contract offer bereits alle für den Vertragsschluss erforderlichen Informationen enthält und ein Vertrag angenommen werden soll. In beiden Fällen würden die Clients in der Folge alle für die Vertragserfüllung notwendigen Schritte vornehmen, die als Tasks im Template des Contracts aufgeführt sind, und deren Erledigung in Form der Änderung des Contract Status im Full Node sowie auf den eigenen Endgeräten aktualisieren und speichern lassen.

Will der Client einen Vertrag mit einem entsprechenden Inhalt nicht eingehen, lehnt er das Contract offer entweder ab oder er sendet die Ablehnung als erfüllte Task an den Full Node. Es steht dem Client, dem der Contract zugesandt wurde, dann frei, dem anfragenden Client selbst einen neuen Contract zu übermitteln, der auf einem anderen Template der jeweils anderen Partei beruht und andere Vertragsinhalte enthält, z.B. einen höheren Preis oder niedrigere Mengenangaben, wodurch der zuvor beschriebene Prozess der Vertragseingehung neu beginnt. Es ist auch möglich, dass der den Contract

anfragende Client dem anderen auf der Basis eines neuen Templates einen geändertes Template zukommen lässt, damit dieser ihm einen Contract mit entsprechend geändertem Inhalt anträgt. Auf diese Weise besteht die Möglichkeit Fides selbst zur Durchführung von Vertragsverhandlungen zu nutzen. Auch hierbei würde der Prozess der Vertragseingehung von vorne beginnen.

Grundsätzlich lässt sich festhalten, dass die Kommunikation zwischen den einen Contract betreffenden Client über die Bestätigung von Tasks, die in dem Template vorgesehen sind, abläuft und die mit der Bestätigung verbundene Änderung des Contracts verschlüsselt im Full Node und lokal bei den betroffenen Clients gespeichert wird. Die Bestätigung einer Task stellt dabei zunächst lediglich ein Behaupten der bestätigenden Seite dar, für das eine tatsächliche Erfüllung nicht nachgewiesen werden muss.

Unabhängig vom Ablauf der Abwicklung eines Contracts sind die Contractdaten zwar im Full Node und bei den Clients gespeichert, jedoch nur auf den Endgeräten der Clients zu entschlüsseln. Die zu den Accounts der Clients gehörenden personenbezogenen Daten, insbesondere in Form des Private Key, sind hingegen nur auf deren Endgerät gespeichert. Der Full Node kann außerdem keinen Einfluss auf die Verarbeitung der auf den Endgeräten gespeicherten Daten oder des im Full Node gespeicherten Zustands des Contracts nehmen.

Die Status von Contracts bleiben im Full Node gespeichert bis die involvierten Parteien den Zustand selbst nicht mehr aktualisieren und werden dann gelöscht.

III. Die Nutzung von Fides mithilfe von LoRaWAN in Regionen ohne Netzinfrastruktur

In Regionen mit keiner, schlechter oder unzuverlässiger Onlineverbindung kann die Nutzung von Fides mit einer Nutzung von LoRaWAN kombiniert werden. In diesen Fällen ändert sich einerseits der Transportweg der Daten, aufgrund von Limitierungen der Datenmengen aber auch deren Art und Menge.

Bei einer Einbindung von LoRaWAN sendet eine LoRaWAN-fähige Hardware, z.B. ein Raspberry Pi, die für die Nutzung von Fides erforderlichen Informationen per Funk an ein LoRaWAN-Gateway. Dieses ist mit dem Internet verbunden und kann Daten sowohl senden als auch empfangen. Über diese Internetverbindung werden die Daten an ein sog.

„The Things Network“ weitergesendet, das in der Regel von einem Kollektiv einer Vielzahl von Nutzern betrieben wird und in dem der LoRaWAN-Nutzer über einen Account verfügt. Von dort gelangen die Daten über eine gesicherte Internetverbindung an eine Middleware, die von jedermann, insbesondere auch von Full Node Betreibern, bereitgestellt werden kann. Sie „übersetzt“ die übermittelten Daten, die in Umfang und Art im Vergleich zur regulären Fidesnutzung anders sind, in ein Format, das für Fides nutzbar ist, und übermittelt diese Daten im Namen des Nutzers mit dessen Private Key digital signiert sodann ins Fidesnetzwerk.

Aus dem Netzwerk kommende Informationen werden, auf dem umgekehrten Weg, zunächst von der Middleware in ein von LoRaWAN handhabbares Format übersetzt und sodann über eine sichere Internetverbindung in das „The Things Netzwerk“ und von dort per Internet zum LoRaWAN Gateway transportiert. Dieses überträgt die Informationen sodann per Funk an das LoRaWAN-fähige Endgerät.

Die Daten, die über LoRaWAN gesendet und empfangen werden können, sind im Vergleich zu normalen Internetverbindungen deutlich reduziert. Es können lediglich 10 Downlinknachrichten und in Abhängigkeit von deren Größe ebenso nur wenige Uplinknachrichten pro Tag übermittelt werden. Eine Uplink-Nachricht sollte dabei einen Umfang von 12 Byte nicht überschreiten. Vor diesem Hintergrund ist es im Fall der Nutzung von Fides über LoRaWAN nicht möglich, eigene Templates zu erstellen und zu übertragen. Vielmehr muss auf bereits vorhandene Templates zurückgegriffen werden. Wird ein Contract erstellt, wird dieser zudem nicht vollständig über LoRaWAN übertragen. Vielmehr werden nur die für den konkreten Contract relevanten Daten hierüber versendet. Die Middleware setzt die übermittelten Informationen sodann, vergleichbar mit dem Ausfüllen eines vereinheitlichten Lückentextes, an den richtigen Stellen in den Contract ein, und lässt auf diese Weise wieder ein fidesfähigen Contract entstehen, der in der Folge regulär verarbeitet werden kann.

Der Contract kann lokal jederzeit, z.B. auch durch sog. Blind Operations, aktualisiert werden. Dies ist sinnvoll, da der Nutzer von LoRaWAN nur eine geringe Anzahl von Downlinknachrichten zur Verfügung hat. Angesichts deren Limitierung findet eine Aktualisierung daher nur auf Anforderung des Nutzers statt. Sofern es dabei jedoch zu einem Konflikt zwischen den im Full Node und lokal gespeicherten Zuständen eines

Vertrages kommt, wird der lokale Zustand durch den im Full Node gespeicherten Zustand überschrieben.

C. Zivilrechtliche Betrachtung

Im Rahmen der zivilrechtlichen Bewertung wird eine allgemeine Analyse der Rechtssicherheit des Konzepts von Fides vorgenommen und anschließend die Übertragbarkeit der Ergebnisse auf andere Systeme thematisiert. Hierfür werden zunächst die rechtlich relevanten Grundlagen eines Vertragsschlusses dargestellt, die sodann auf den vorliegenden Fall angewendet werden. Gegenstand der Betrachtung ist dabei die voranstehende Schilderung der Funktionsweise der aktuellen Software. In der Folge wird das System in den Stand der Forschung und der dortigen rechtlichen Lage eingeordnet. Dabei wird ein Vergleich des Abschlusses von Smart Contracts über Fides mit der Eingehung eines Vertrages mittels des Systems Etherum vorgenommen. Abschließend erfolgt zudem eine zivilrechtliche Bewertung des Einsatzes der Middleware LoRaWAN, die als zentraler Dienst beim Einsatz von Fides verwendet wird, sofern die Software nicht direkt ausgeführt werden kann. Der primäre Fokus der Betrachtung liegt dabei darauf, ob sich die zuvor getroffenen zivilrechtlichen Bewertungen durch den Einsatz der Middleware ändern, sofern die Verträge im Namen der Clients (durch die Middleware) geschlossen werden.

I. Möglichkeit des Vertragsschlusses unter Einsatz von Fides

Die Möglichkeit unter Einsatz von Fides einen rechtswirksamen Vertrag zu schließen, hängt davon ab, ob mittels der Software die an einen Vertragsschluss zu stellenden rechtlichen Anforderungen erfüllt werden können. In der Folge werden die Voraussetzungen dargestellt und anschließend auf den konkreten Anwendungsfall Fides übertragen. Auch wenn sich die vorliegende Studienfrage ausschließlich darauf bezieht, ob mittels Fides rechtswirksame Verträge geschlossen werden können, sind durchsetzbare Ansprüche aus einem Vertrag lediglich dann herzuleiten, wenn ihm keine rechtshindernden Einwendungen, rechtshemmenden Einreden oder Treu und Glauben (§ 242 BGB) entgegenstehen. Da in einigen Fällen rechtliche Ursachen für solche Einwendungen oder Einreden beim Vertragsschluss gelegt werden, wird in der Folge über Fragen des Vertragsschlusses hinaus auf solche Aspekte eingegangen werden, die im Zusammenhang mit dem Vertragsschluss Auswirkungen auf das spätere Bestehen von Einreden oder Einwendungen haben können. Hierbei werden insbesondere nur solche Fragen angesprochen, für die gerade der Einsatz von Fides und somit das Medium des Vertragsschlusses rechtlich relevant ist, nicht aber allgemeine und jeden Vertrag betreffende Überlegungen.

1. Anforderungen an einen rechtswirksamen Vertrag

Die Prüfung, ob ein Vertrag wirksamen geschlossen wurde, lässt sich in verschiedene Prüfungsschritte aufteilen.

a) Voraussetzungen eines wirksamen Vertragsschlusses

Ein Vertrag ist ein Rechtsgeschäft, das aus inhaltlich übereinstimmenden und mit Bezug auf einander abgegebenen Willenserklärungen von mindestens zwei Personen besteht, wobei die zeitlich erste als Angebot oder Antrag bezeichnet wird (§145 BGB[1]) und die spätere als Annahme (§146 BGB).[2] Ein Angebot stellt dabei eine empfangsbedürftige Willenserklärung dar, die alle vertragswesentlichen Bestandteile (essentialia negotii) enthalten muss.[3] Sie muss so konkret gefasst sein, dass ein Empfänger sie ohne Weiteres annehmen kann.[4] Was die wesentlichen Vertragsbestandteile sind, die ein Angebot als essentialia negotii zwingend enthalten muss, unterscheidet sich zwar je nach angestrebten Vertragstypus, umfasst jedoch grundsätzlich den Vertragsgegenstand, die Vertragsparteien und die vertraglichen Leistungen.[5]

Eine Willenserklärung ist eine private Willensäußerung, die auf die Erzielung einer Rechtsfolge gerichtet ist.[6] Der auf die Erzielung einer Rechtsfolge gerichtete Wille einer erklärenden Person besteht dabei aus zwei Elementen: dem inneren Willen und seiner Äußerung.[7]

Der innere Wille setzt sich dabei aus dem Handlungswillen, dem Erklärungswillen bzw. -bewusstsein und dem Geschäftswillen zusammen.[8] Der Handlungswille ist das Bewusstsein zu handeln, sodass sich eine Willenserklärung als bewusster Willensakt darstellt, der auf die Vornahme eines äußeren Verhaltens gerichtet ist.[9] Der Erklärungswille hingegen ist das Bewusstsein einer Person, dass ihr Verhalten als

---

[1] Bürgerliches Gesetzbuch - in der Folge BGB.
[2] BGH, NJW 2107, 468, Tz. 21; *Eckert* in: BeckOK BGB, § 145 Rn. 2; Brox/Walker, BGB AT Rn. 77 f.; *Ellenberger* in: Grüneberg, Einf v § 145 Rn. 1.
[3] BGH, NJW 2006, 1972; BAG, NJW 2008, 937; *Mansel* in: Jauernig, § 145 Rn. 2; Busche, in: MK-BGB, § 145 Rn. 6; *Dörner* in: Schulze, § 145 Rn. 3.
[4] OLG Düsseldorf, NJW-RR 2016, 1073, Rn. 23; *Busche* in: MK-BGB, § 145 Rn. 6; *Mansel* in: Jauernig, § 145 Rn. 2.
[5] *Busche* in: MK-BGB, § 145 Rn. 6; *Dörner* in: Schulze, § 145 Rn. 3; *Eckert* in: BeckOK BGB, § 145 Rn. 3.
[6] BGH, NJW 2001, 289, 289f.; Brox/Walker, BGB AT Rn. 82; *Mansel* in: Jauernig, Vor §§ 116 Rn. 2 f.; *Ellenberger* in: Grüneberg, Überbl v § 104 Rn. 2; Einf v § 116 Rn. 1.
[7] Brox/Walker, BGB AT Rn. 83; *Ellenberger* in: Grüneberg, Einf v § 116 Rn. 1.
[8] *Mansel* in: Jauernig, Vor §§ 116 Rn. 4 ff.; Brox/Walker, BGB AT Rn. 84.
[9] *Mansel* in: Jauernig, Vor §§ 116 Rn. 4; Brox/Walker, BGB AT Rn. 84.

rechtserhebliche Erklärung aufgefasst werden kann.[10] Es ist umstritten, ob er bzw. sein potentielles Vorhandensein als notwendiger konstituierender Bestandteil einer Willenserklärung anzusehen ist.[11] Das letzte Element des subjektiven Willens stellt der Geschäftswille dar, der als Wille definiert ist, mit einer Erklärung eine bestimmte Rechtsfolge herbeizuführen.[12]

Als objektives Element einer Willenserklärung stellt sich deren Äußerung bzw. Kundgabe dar. Sie ist ein äußerlich erkennbares Verhalten, das den Willen zum Ausdruck bringt, eine bestimmte Rechtsfolge herbeizuführen. Sie ist gegeben, sofern ein objektiver Dritter von dem erkennbaren Verhalten auf einen dadurch ausgedrückten Willen zum Handeln schließen kann.[13] Die Äußerung kann dabei sowohl explizit als auch konkludent und in Ausnahmefällen (vgl. § 362 Abs. 1 HGB) sogar durch Schweigen erfolgen.[14]

Sofern eine Willenserklärung, wie das Angebot, empfangsbedürftig ist, muss sie von der erklärenden Person abgegeben werden und dem Erklärungsempfänger zugehen. Eine empfangsbedürftige Willenserklärung ist abgegeben, wenn die erklärende Person sich ihrer willentlich in Richtung einer empfangenden Person entäußert hat, sodass unter normalen Umständen mit einem Zugang zu rechnen ist.[15]

Eine empfangsbedürftige Willenserklärung muss einem Empfänger zudem auch zugehen. In Bezug auf die Frage, wann eine Willenserklärung einem anderen Teil zugegangen ist, wird zwischen Anwesenden und Abwesenden unterschieden. Hierbei ist von einem Zugang einer Willenserklärung unter Anwesenden gemäß der (abgeschwächten) Vernehmungstheorie auszugehen, wenn der Empfänger die Nachricht richtig verstanden hat bzw. der Erklärende nach den für ihn erkennbaren Umständen davon ausgehen darf, dass der andere Teil die Erklärung versteht, wodurch beim Empfänger liegende Vernehmungshindernisse einen Zugang nicht stören, wenn die erklärende Person diese

---

[10] BGH, NJW 1984, 2279; *Mansel* in: Jauernig, Vor §§ 116 Rn. 5; Brox/Walker, BGB AT Rn. 85.
[11] BGHZ 91, 324; 109, 177; Medicus/Petersen, Bürgerliches Recht Rn. 130; Thiele, JZ 1969, 405, 407; Wieacker, JZ 1967, 385, 389.
[12] OLG Düsseldorf, OLGZ 1982, 241, 241 ff.; *Mansel* in: Jauernig, Vor §§ 116 Rn. 6; Brox/Walker, BGB AT Rn. 86.
[13] *Mansel* in: Jauernig, Vor §§ 116 Rn. 7 ff.; Brox, BGB AT Rn. 88.
[14] BGH, NJW 2018, 296; Fabricius, JuS 1966, 1 ff.; Petersen, Jura 2003, 687 ff.; *Busche* in: MK-BGB, § 133 Rn. 70; Brox/Walker, BGB AT Rn. 89 ff.
[15] *Einsele* in: MK-BGB, § 130 Rn. 13; Medicus/Petersen, Bürgerliches Recht, Rn. 263 f.

nicht erkennen kann. [16] Unter Abwesenden gilt eine Willenserklärung nach der Möglichkeitstheorie als zugegangen, sofern die Willenserklärung derart in den Machtbereich eines Empfängers gelangt ist, dass dieser unter normalen Umständen die Möglichkeit der Kenntnisnahme hat.[17]

Von einem Angebot abzugrenzen ist eine „invitatio ad offerendum". Hierbei handelt es sich um eine Aufforderung zur Offerte. Sie stellt somit selbst kein Angebot dar, sondern ist vielmehr eine Aufforderung an andere, dass diese ein Angebot abgeben sollen, wobei die so aufgeforderten Personen wiederum frei darin sind, die invitatio ad offerendum anzunehmen oder abzulehnen.[18] Die Abgrenzung erfolgt zwar anhand der Umstände des Einzelfalls,[19] es lassen sich jedoch allgemeine Fallgruppen herausarbeiten. Dabei kommt es nicht auf den inneren Willen des Antragenden, sondern vielmehr auf den objektiven Erklärungswert seines Verhaltens an.[20] So stellen Verlautbarungen an die Allgemeinheit oder auch Anzeigen in Zeitungen, Plakate, Kataloge, Preislisten, Speisekarten oder Ankündigungen von Ereignissen keine Angebote dar.[21] Aus derartigen Äußerung lässt sich nicht auf den Willen schließen, sich endgültig binden zu wollen, da es der äußernden Person an entsprechenden Lagerbeständen fehlen könnte, um mit allen, die die Äußerung erreicht, Verträge einzugehen. Ferner könnten möglicherweise auch Bedenken gegenüber bestimmten Kunden bestehen, sodass kein Wille vorliegt, mit ihnen einen Vertrag einzugehen.[22]

b) Besonderheiten des Vertragsschlusses im Fall der Verwendung von Allgemeinen Geschäftsbedingungen

Allgemeine Geschäftsbedingungen[23] sind für eine Vielzahl von Verträgen vorformulierte Vertragsbedingungen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrages stellt (§ 305 Abs. 1 S. 1 BGB). Vertragsbedingungen sind Bestimmungen, die Inhalt eines Vertrages werden sollen.[24] Sie werden für eine Vielzahl

---

[16] Vgl. nur *Einsele* in: MK-BGB, § 130 Rn. 16; 27; 30.
[17] RGZ 142, 402, 407; BGH, NJW 2003, 3270; BGH, NJW 2014, 2020 Rn. 8; BAG, NJW 2019, 3666 Rn. 12; *Einsele* in: MK-BGB, §130 Rn. 17, 19.
[18] AG Butzbach, NJW-RR 2003, 54; *Busche* in: MK-BGB, § 145 Rn. 10; Brox/Walker, BGB AT Rn. 167; Schewe/Muscheler, Jura 2000, 565.
[19] Brox/Walker, BGB AT Rn. 167; *Busche* in: MK-BGB, § 145 Rn. 10.
[20] *Ellenberger* in: Grüneberg, § 145 Rn. 2; *Busche* in: MK-BGB, § 145 Rn. 10.
[21] *Ellenberger* in: Grüneberg, § 145 Rn. 2; Brox/Walker, BGB AT Rn. 167.
[22] *Ellenberger* in: Grüneberg, § 145 Rn. 2; *Busche* in: MK-BGB, § 145 Rn. 10; Brox/Walker, BGB AT Rn. 167.
[23] In der Folge AGB.
[24] BGHZ 101, 271, 274; BGHZ 148, 74, 76; *Becker* in: BeckOK BGB, § 305 Rn. 12; Brox, BGB AT, Rn. 222.

von Fällen verwendet, sofern mindestens drei Verwendungen geplant sind.[25] Irrelevant ist insoweit, ob ein Verwender die Bedingungen selbst oder aber ein Dritter sie aufgesetzt hat.[26] Bedingungen gelten als vom Verwender gestellt, wenn sie von ihm einseitig auferlegt, das heißt, die Bedingungen nicht einzeln zwischen den Parteien ausgehandelt werden (§ 305 Abs. 3 BGB). Damit Bedingungen als ausgehandelt angesehen werden, verlangt die Rechtsprechung, dass der Verwender die Bedingungen ernsthaft zur Disposition stellt und dem Partner Gestaltungsfreiheit zur Wahrung eigener Interessen mit der realen Möglichkeit eingeräumt wird, die inhaltliche Ausgestaltung von Vertragsbedingungen zu beeinflussen.[27] Die AGB müssen zudem durch Einbeziehung Bestandteil des Vertrages werden, was gemäß § 305 Abs. 2 BGB der Fall ist, wenn der Verwender bei Vertragsschluss ausdrücklich auf sie hinweist, oder, sofern ausnahmsweise ein ausdrücklicher Hinweis unverhältnismäßige Schwierigkeiten bereitet, ein deutlich sichtbarer Aushang am Ort des Vertragsschlusses vorhanden ist (§ 305 Abs. 2 Nr. 1 BGB). Zudem muss der andere Vertragsteil in zumutbarer Weise von dem Inhalt der AGB Kenntnis nehmen können (§ 305 Abs. 2 Nr. 2 BGB) und sich mit deren Geltung ausdrücklich oder konkludent einverstanden erklären (§ 305 Abs. 2 a.E. BGB). Ist eine Bestimmung nach den Umständen so ungewöhnlich, dass der Vertragspartner nicht mit ihr rechnen muss, wird sie nicht Vertragsbestandteil (§ 305c BGB).

Für die Verwendung und Einbeziehung von AGB im Verhältnis zwischen Unternehmen und Verbrauchern sind einige Besonderheiten gemäß § 310 Abs. 3 BGB zu beachten. Unternehmer sind gemäß § 14 Abs. 1 BGB natürliche oder juristische Personen oder rechtsfähige Personengesellschaften, die bei Abschluss eines Rechtsgeschäfts in Ausübung ihrer gewerblichen oder selbständigen beruflichen Tätigkeit handeln. Ein Verbraucher ist dem gegenüber gemäß § 13 BGB jede natürliche Person, die ein Rechtsgeschäft zu Zwecken abschließt, die überwiegend weder ihrer gewerblichen noch ihrer selbständigen beruflichen Tätigkeit zugerechnet werden können. Bei Verträgen zwischen einem Unternehmer und einem Verbraucher (Verbraucherverträge) gelten AGB als vom Unternehmer gestellt, es sei denn, sie sind vom Verbraucher in den Vertrag

[25] BGH, NJW 2004, 1454; NJW 2002, 138; NJW 2019, 2997; *Fornasier* in: MK-BGB, § 305 Rn. 18; *Becker* in: BeckOK BGB, § 305, Rn. 24; *Grüneberg* in: Grüneberg, § 305 Rn. 9.
[26] BGHZ 144, 242; BGHZ 184, 259; *Becker* in: BeckOK BGB, § 305 Rn. 25; *Fornasier* in: MK-BGB, § 305 Rn. 19; Brox/Walker, BGB AT Rn. 222.
[27] BGH, NJW 1992, 2760 m.w.N.; *Stadler* in: Jauernig, § 305 Rn. 8 f.; *Fornasier* in: MK-BGB, § 305 Rn. 21; *Becker* in: BeckOK BGB, § 305 Rn. 26 f.

eingeführt worden (§ 310 Abs. 3 Nr. 1 BGB). Zudem findet eine Kontrolle von AGB in diesem Verhältnis auch dann statt, wenn die vorformulierten Bedingungen nur zu einer einmaligen Verwendung bestimmt sind und soweit der Verbraucher wegen der Vorformulierung keinen Einfluss auf den Inhalt nehmen konnte (§ 310 Abs. 3 Nr. 2 BGB).

Im Verhältnis zwischen Unternehmern finden die Anforderungen des § 305 Abs. 2 BGB gemäß § 310 Abs. 1 BGB keine Anwendung, sodass eine Einbeziehung von AGB auch konkludent erfolgen kann.[28]

Sind AGB wirksam in einen Vertrag einbezogen worden, unterliegen sie einer gesonderten Inhaltskontrolle gemäß §§ 309, 308 und 307 BGB. In § 309 BGB genannte Klauseln sind stets (Klauselverbote ohne Wertungsmöglichkeit) und die in § 308 BGB aufgeführten Klauseln immer dann unwirksam, wenn sie im Einzelfall eine unangemessene Benachteiligung der Vertragspartei darstellen (Klauselverbote mit Wertungsmöglichkeit).[29] Gemäß § 307 Abs. 1, 2 BGB als Auffangtatbestand sind zudem Klauseln unwirksam, die eine Vertragspartei entgegen Treu und Glauben unangemessen benachteiligen. Eine Inhaltskontrolle in Verträgen zwischen Unternehmern findet demgegenüber allein anhand der §§ 307, 308 Abs. 1 Nr. 1a und 1b BGB Anwendung.[30]

Die Folge der Verwendung unwirksamer Klauseln ist gemäß § 306 Abs. 1 BGB nicht die Nichtigkeit des gesamten Vertrages, sondern dessen Aufrechterhaltung mit Ausnahme der unwirksamen Klausel (salvatorische Klausel). Durch die Unwirksamkeit entstehende Regelungslücken werden gemäß § 306 Abs. 2 BGB durch gesetzliche Vorschriften oder, sofern das nicht möglich ist, durch ergänzende Vertragsauslegung [31] geschlossen. Unwirksame Klauseln werden zudem auch nicht insoweit aufrechterhalten als sie noch gesetzlich zulässig wären (keine geltungserhaltende Reduktion), da die Nutzung unwirksamer Klauseln für den Verwender andernfalls risikolos möglich wäre und

---

[28] *Becker* in: BeckOK BGB, § 305 Rn. 81; § 310 Rn. 2; *Grüneberg* in: Grüneberg, § 310, Rn. 4; *Stadler* in: Jauernig, §310 Rn. 2.
[29] *Schulte-Nölke* in: Schulze, Vorbem §§ 305-310 Rn. 10; *Wurmnest* in: MK-BGB, Vor § 307 Rn. 6 ff.; Brox/Walker, BGB AT Rn. 235.
[30] *Fornasier* in: MK-BGB, § 310 Rn. 11 ff.; *Grüneberg* in: Grüneberg, § 310 Rn. 5; *Stadler* in: Jauernig, § 310 Rn. 2; *Becker* in: BeckOK BGB, § 310 Rn. 2.
[31] BGHZ 90, 69, 73 ff.; 117, 98; *Fornasier* in: MK-BGB, § 306 Rn. 33; *Stadler* in: Jauernig, § 310 Rn. 5.

Unklarheiten in Bezug auf die rechtlichen Verhältnisse zu befürchten wären.[32] Eine Ausnahme von diesem Grundsatz findet sich jedoch in § 306 Abs. 3 BGB.

c) Fehlen rechtshindernder Einwendungen

Die Entstehung eines Anspruchs aus einem geschlossenen Vertrag setzt voraus, dass der Vertrag wirksam ist und ihm keine rechtshindernden Einwendungen entgegenstehen. Rechtshindernde Einwendungen stehen der Entstehung des Anspruchs entgegen. Die Rechtsfolge des Entgegenstehens einer rechtshindernden Einwendung ist die Nichtigkeit des Vertrages. Wie oben bereits ausgeführt sollen vorliegend nur solche Einwendungen angesprochen werden, in deren Zusammenhang sich die Art des Vertragsschlusses über Fides auszuwirken vermag. Dies gilt zum Beispiel nicht für die Nichtigkeit eines Vertrages gemäß § 105 Abs. 1 BGB aufgrund der Geschäftsunfähigkeit einer Vertragspartei nach § 104 BGB, da eine solche sich aufgrund von Eigenschaften ergibt, die in den Parteien liegen und bei jedem Vertragsschluss, unabhängig von dem hierfür gewählten Medium auftreten können. Dasselbe gilt für eine Nichtigkeit des Vertrages aufgrund von anderen Mängeln in der Geschäftsfähigkeit (§ 105 Abs. 2 BGB), wegen schwerwiegender Fehler in der abgegebenen Willenserklärung (§§ 116 – 118 BGB), wegen inhaltlicher Mängel des Vertrages (§§ 134, 138 BGB), wegen Teilnichtigkeit nach § 139 Abs. 1 BGB oder eines Dissenses (§§ 154 f., 139 BGB) oder der Umgehung von Vergütungsregeln gemäß § 656c Abs. 2 S. 1 BGB.

Im vorliegenden Kontext relevant, da mit dem Medium des Vertragsschlusses verknüpft, ist hingegen die rechtshindernde Einwendung der Nichtigkeit aufgrund der Nichteinhaltung einer gesetzlich (§ 125 S. 1 BGB) oder vertraglich (§ 125 S. 2 BGB) vorgesehenen Form. Auch, wenn Verträge grundsätzlich formlos wirksam geschlossen werden können, sodass die Erklärenden frei in der Wahl des Erklärungsmittels ihrer Willenserklärung sind, existieren auch formbedürftige Rechtsgeschäfte, für deren Wirksamkeit das Gesetz oder auch eine Vereinbarung zwischen den beteiligten Parteien die Einhaltung einer bestimmten Form vorsehen.[33] Hierbei ist zwischen verschiedenen Arten der Formen zu unterscheiden:

---

[32] BGHZ 84, 109, 114 ff.; 92, 312, 315; 124, 380; BGH, NJW 2000, 1113; *Stadler* in: Jauernig, § 310 Rn. 5; Brox/Walker, BGB AT Rn. 238.
[33] *Ellenberger* in: Grüneberg, § 125, Rn. 1; *Dörner* in: Schulze, § 125 Rn. 1; *Einsele* in: MK-BGB, § 125 Rn. 1; Brox/Walker, BGB AT Rn. 298 f.; *Mansel* in: Jauernig, § 125 Rn. 1 ff.

Bei der Textform muss gemäß § 126b S. 1 BGB eine lesbare Erklärung, in der die Person des Erklärenden genannt ist, auf einem dauerhaften Datenträger abgegeben werden. Was ein dauerhafter Datenträger ist, wird in § 126b S. 2 BGB definiert. Zur Einhaltung der in § 126 BGB geregelten Schriftform muss eine Urkunde erstellt und von dem Aussteller eigenhändig durch Namensunterschrift oder durch notariell beglaubigtes Handzeichen unterzeichnet werden (§ 126 Abs. 1 BGB). Sofern es sich bei der Urkunde um einen Vertrag handelt, muss die Unterzeichnung der Parteien auf derselben Urkunde erfolgen (§ 126 Abs. 2 S. 1 BGB), es sei denn, dass mehrere gleichlautende Urkunden aufgenommen werden, wobei dann jede Partei auf der für die andere Partei bestimmten Urkunde unterzeichnen kann (§ 126 Abs. 2 S. 2 BGB). Die elektronische Form nach § 126a Abs. 1 BGB, mit der die Schriftform ersetzt werden kann (§ 126 Abs. 3 BGB), ist hingegen gewahrt, wenn der Aussteller einer Erklärung seinen Namen zu dieser Erklärung hinzufügt und das elektronische Dokument mit einer qualifizierten Signatur versieht. Bei einem Vertrag müssen die Parteien gemäß § 126a Abs. 2 BGB ein gleichlautendes Dokument in der zuvor genannten Weise elektronisch signieren. Ferner existiert die Form der öffentlichen Beglaubigung. Damit sie gewahrt ist, muss gemäß § 129 Abs. 1 BGB die Erklärung schriftlich abgefasst und die Unterschrift des Erklärenden von einem Notar beglaubigt werden. Die Form der notariellen Beurkundung gemäß § 128 BGB ist gewahrt, wenn die Anforderungen des Beurkundungsverfahrens eingehalten werden, die im Beurkundungsgesetz geregelt sind. In wenigen Ausnahmefällen ist zudem die Form der Abgabe einer Erklärung vor einer Behörde vorgesehen, wie zum Beispiel im Fall der Eheschließung, bei der die Willenserklärungen persönlich bei gleichzeitiger Anwesenheit vor einem Standesbeamten erklärt werden müssen (vgl. §§ 1310 ff. BGB).

Ein Vertrag, der nicht in der gesetzlich vorgesehenen Form geschlossen worden ist, ist gemäß § 125 S. 1 BGB nichtig. Dasselbe gilt im Zweifel auch für die Nichteinhaltung einer zwischen Parteien vorgesehenen Form (§ 125 S. 2 BGB).

d) Fehlen rechtsvernichtender Einwendungen

Wie zuvor im Zusammenhang mit den rechtshindernden Einwendungen dargelegt, gilt auch in Bezug auf das Vorliegen rechtsvernichtender Einwendungen, dass sie nur insoweit thematisiert werden, als das Medium des Vertragsschlusses Auswirkungen auf ihr Bestehen hat. Rechtsvernichtende Einwendungen lassen einen entstandenen

Anspruch untergehen. Der Anspruch ist somit im Fall des Vorliegens rechtsvernichtender Einwendungen erloschen.

Vor dem Hintergrund der Relevanz des Mediums für das Bestehen einer rechtsvernichtenden Einwendung wird vorliegend nicht auf Fragen der Erfüllung (§ 362 BGB) oder von Erfüllungssurrogaten (§§ 364 Abs. 1, 378 BGB) eingegangen, da diese unabhängig von der Art des Vertragsschlusses begründet werden. Ebenso verhält es sich mit rechtsvernichtenden Einwendungen in Form von Verträgen, wie einem Erlass- (§ 397 BGB) oder Aufhebungsvertrag (§ 311 BGB), einer Schuldübernahme (§ 414f. BGB) oder einer Abtretung (§ 398 BGB). Ebenso nicht vom Medium des Vertragsschlusses abhängig sind rechtsvernichtende Einwendungen, die auf tatsächlichen Ereignissen beruhen, wie zum Beispiel Tatbestände der Unmöglichkeit (§ 275 BGB), der Fixhandelskauf (§ 376 Abs. 1 2 HGB), der Eintritt einer auflösenden Bedingung (§ 158 Abs. 2 BGB), Tatbestände eines Forderungsübergangs (§§ 398, 426 Abs. 2 BGB) oder der Eintritt von Konfusion. Auch der Eintritt der Störung der Geschäftsgrundlage (§ 313 BGB) ist nicht mit dem Medium des Vertragsschlusses assoziiert.

Die Verwendung von Fides kann sich hingegen im Rahmen der Ausübung von Gestaltungsrechten auswirken. Ein Gestaltungsrecht ist ein relatives subjektives Recht, das dem Inhaber einseitig die Möglichkeit einräumt, ohne Mitwirkung eines Dritten durch einen Gestaltungsakt, wie zum Beispiel eine Erklärung, auf die bestehende Rechtslage einzuwirken und sie zu verändern. Auch aus der Gruppe der Gestaltungsrechte sind jedoch nicht alle im vorliegenden Kontext gesondert zu betrachten. Sowohl bei einer Anfechtung (§ 142 BGB) als auch einem vertraglich vereinbarten oder gesetzlich vorgesehenen Rücktrittsrecht (§§ 346, 323, 326 BGB) ergeben sich aufgrund des Einsatzes von Fides keine explizit zu betrachtenden Besonderheiten. Dies gilt auch für Aufrechnungen (§ 389 BGB).

Besonderheiten können sich insoweit ergeben als das Gesetz für bestimmte Verbraucherverträge[34] besondere Rechte für Verbraucher und spezielle Pflichten für Unternehmer vorsieht. Relevant ist vorliegend insoweit einerseits die Kategorie der Fernabsatzverträge gemäß § 312c Abs. 1 BGB. Hierbei handelt es sich um Verträge, bei

[34] Siehe hierzu C. I. 1. b).

denen der Unternehmer oder eine in seinem Namen oder Auftrag handelnde Person und der Verbraucher für die Vertragsverhandlungen und den Vertragsschluss ausschließlich Fernkommunikationsmittel verwenden, es sei denn, dass der Vertragsschluss nicht im Rahmen eines für den Fernabsatz organisierten Vertriebs- oder Dienstleistungssystems erfolgt. Fernkommunikationsmittel werden nach § 312c Abs. 2 BGB definiert als alle Kommunikationsmittel, die zur Anbahnung oder zum Abschluss eines Vertrages eingesetzt werden können, ohne dass die Vertragsparteien gleichzeitig körperlich anwesend sind, wie Briefe, Kataloge, Telefonanrufe, Telekopien, E-Mails, SMS sowie Rundfunk und Telemedien. Von diesem Anwendungsbereich ausgenommene Verträge finden sich in § 312 Abs. 2 BGB. Unternehmer sind im Rahmen von Fernabsatzverträgen verpflichtet, Verbraucher nach Maßgabe des Art. 246a EGBGB[35] zu informieren. Diese vom Unternehmer gemachten Angaben werden nach § 312d Abs. 1 S. 2 BGB Vertragsbestandteil.[36] Der Unternehmer muss dem Verbraucher ferner eine Bestätigung des Vertrages, die den in § 312f Abs. 2 BGB niedergelegten Anforderungen gerecht wird, zur Verfügung stellen. Dem Verbraucher steht bei einem Fernabsatzvertrag gemäß § 312g Abs. 1 BGB ein Widerrufsrecht nach § 355 BGB zu, sofern nicht eine Ausnahme nach § 312g Abs. 2 BGB vorliegt. Ein Ausschluss oder ein vorzeitiges Erlöschen des Widerrufsrechts ist in den Fällen des § 356 Abs. 4 und 5 BGB gegeben.

Bei Verletzung der Informationspflicht in Bezug auf Fracht-, Liefer- und Versandkosten kann der Unternehmer diese gemäß § 312e BGB nicht vom Verbraucher verlangen. Weiterhin beginnt die Frist, in der ein Verbraucher den Widerruf des Vertrages wirksam erklären kann, gemäß § 356 Abs. 3 S. 1 BGB nicht, bevor eine ordnungsgemäße Unterrichtung des Verbrauchers erfolgt ist. Zudem kann der Unternehmer in diesen Fällen nicht die Kosten der Rücksendung der Ware sowie keinen Wertersatz für den Wertverlust der Ware verlangen.[37] Verstöße gegen die Informationspflichten können zudem eine Nebenpflichtverletzung des Unternehmers darstellen, aus der Schadenersatzansprüche hergeleitet werden können. [38] Verstöße gegen die Informationspflicht können zudem wettbewerbsrechtliche Folgen nach sich ziehen.[39]

---

[35] Einführungsgesetz zum Bürgerlichen Gesetzbuch – in der Folge EGBGB.
[36] Vgl. hierzu ausführlich: *Martens* in: BeckOK BGB, § 312d Rn. 7 ff.
[37] *Martens* in: BeckOK BGB, § 312d Rn. 14.
[38] *Wendehorst* in: MK-BGB, § 312d Rn. 157; *Singbartl/Zintl*, NJW 2016, 1848, 1848 ff.; *Martens* in: BeckOK BGB, § 312d Rn. 14.
[39] KG, ZGS 2008, 154; *Martens* in: BeckOK BGB, § 312d Rn. 15.

Sofern es sich bei dem Vertrag aufgrund der Verwendung von Fides um einen Vertrag im elektronischen Geschäftsverkehr nach § 312i Abs. 1 BGB handelt, gelten zudem weitere Anforderungen nach §§ 312j – 312l BGB. Ein solcher Vertrag liegt vor, wenn sich ein Unternehmer zum Zweck des Abschlusses eines Vertrages über die Lieferung von Waren oder über die Erbringung von Dienstleistungen Telemedien bedient (§ 312i Abs. 1 S. 1 BGB). In Abgrenzung zum Fernabsatzvertrag fallen unter Verträge nach § 312i BGB nur solche, die unter Einsatz von elektronischen Kommunikationsmitteln geschlossen wurden. Wird ein Fernabsatzvertrag mittels elektronsicher Kommunikationsmittel geschlossen, so gelten sowohl §§ 312 ff. BGB als auch §§ 312i ff. BGB.[40] Im Fall des Abschlusses ohne Einsatz von elektronischen Kommunikationsmitteln gelten allein §§ 312 ff. BGB.[41] Anders als ein Fernabsatzvertrag, bei dem es sich um einen Verbrauchervertrag handelt, kann ein Vertrag im elektronischen Geschäftsverkehr jedoch auch zwischen zwei Unternehmern geschlossen werden, sodass bei, Vertragsschluss zwischen zwei Unternehmern lediglich §§ 312i ff. BGB, nicht aber §§ 312 ff. BGB anwendbar sind.[42] Besondere Pflichten für Verträge im elektronischen Geschäftsverkehr sieht § 312i Abs. 1 S. 1 BGB vor. So muss es dem Kunden möglich sein, Eingabefehler zu berichtigen (Nr. 1), der Unternehmer muss die in Art. 246c EGBGB vorgesehenen Informationen rechtzeitig vor Abgabe der Bestellung klar und verständlich mitteilen (Nr. 2), den Zugang einer Bestellung unverzüglich elektronisch bestätigen (Nr. 3) und eine Möglichkeit zum Abruf und zur Speicherung der Vertragsbestimmungen schaffen (Nr. 4).

Ein Verstoß gegen diese Pflichten berührt die Wirksamkeit des Vertrages nicht und hat auch keinen Einfluss auf den Beginn der Widerrufsfrist.[43] Es ist jedoch möglich, dass aufgrund der Pflichtverletzung der Anbieter keinen Anspruch auf Ersatz des Vertrauensschadens im Fall einer Anfechtung durch den Kunden hat.[44] Zugleich kann eine Schadenersatzpflicht gegenüber dem Kunden begründet werden und die Möglichkeit von

[40] *Grüneberg* in: Grüneberg, § 312i Rn. 4.
[41] *Grüneberg* in: Grüneberg, § 312i Rn. 4.
[42] *Maume* in: BeckOK BGB, § 312i Rn. 2; *Grüneberg* in: Grüneberg, § 312i Rn. 4.
[43] *Maume* in: BeckOK BGB, § 312i Rn. 35; *Grüneberg* in: Grüneberg, § 312i Rn. 11.
[44] *Maume* in: BeckOK BGB, § 312i Rn. 36.

Unterlassungsklagen nach § 3 UKlaG[45] oder nach wettbewerbsrechtlichen Grundsätzen gemäß UWG[46] in Betracht kommen.[47]

Sofern ein Vertrag im elektronischen Geschäftsverkehr mit einem Verbraucher geschlossen wird, treten besondere Pflichten nach § 312j BGB hinzu. Neben erweiterten Informationspflichten (Abs. 1) und Anforderungen an deren Bereitstellung (Abs. 2), muss mit der Bestellung ausdrücklich die Zahlungspflicht des Verbrauchers ausdrücklich bestätigt werden (Abs. 3). Ausnahmen gelten, nach §312j Abs. 5 BGB, sofern ein Vertrag ausschließlich durch individuelle Kommunikation geschlossen wird.

Eine Verletzung der Informationspflichten aus § 312j Abs. 1, 2 BGB führt, wie bei den anderen zuvor dargestellten Verträgen auch, zu einem möglichen Schadensersatzanspruch wegen Verletzung vorvertraglicher Pflichten sowie Ansprüchen aus UKlaG und UWG.[48] Eine Verletzung der Pflicht nach § 312j Abs. 3 BGB, also den expliziten Hinweis des Verbrauchers auf die Zahlungspflicht und ihre Bestätigung durch ihn, stellt jedoch eine Voraussetzung für das Zustandekommen des Vertrages und damit seine Wirksamkeit dar.[49] [50]

Sofern es sich bei dem Vertrag um ein Dauerschuldverhältnis handelt, in dem ein Unternehmer von einem Verbraucher zu einer wiederkehrenden entgeltlichen Leistung verpflichtet wird, treffen den Unternehmer zudem die Pflichten nach § 312k BGB. Ein Dauerschuldverhältnis ist ein Schuldverhältnis, das auf wiederkehrende, sich über einen längeren Zeitraum wiederholende Leistungen und Gegenleistungen gerichtet ist.[51] Die Pflichten nach § 312k BGB betreffen dabei die Kündigung des Dauerschuldverhältnisses. Gemäß § 312l BGB treffen weitere Informationspflichten in Form des Art. 246d EGBGB Betreiber eines Online-Marktplatzes (§ 312l Abs. 1 BGB). Bei einem Online-Markplatz

---

[45] Unterlassungsklagegesetz – in der Folge UKlaG.
[46] Gesetz gegen den unlauteren Wettbewerb – in der Folge UWG.
[47] *Maume* in: BeckOK BGB, § 312i Rn. 37 ff.
[48] *Maume* in: BeckOK BGB, § 312i Rn. 38; LG Arnsberg, BeckRS 2016, 05962.
[49] *Maume* in: BeckOK BGB, § 312i Rn. 39; *Alexander*, NJW 2012, 1985, 1986; *Kirschbaum*, MMR 2012, 8.
[50] Vor dem Hintergrund dieser dogmatischen Einordnung, die vielfach kritisiert wird, da sie dem System des BGB fremd ist (vgl. *Maume*, in: BeckOK BGB, § 312i Rn. 40, hätte eine Darstellung dieses Aspekts des § 312j Abs. 3, 5 BGB bereits oben im Kapitel C.I.1. erfolgen müssen. Aus Gründen der Verständlichkeit und der gemeinsamen Behandlung des Themenkomplexes besonderer Vertragstypen, die sich in erster Linie im Bereich der rechtsvernichtenden Einwendungen auswirken, ist hiervon abgewichen worden.
[51] *Gaier* in: MK-BGB, § 314 Rn. 9 f.; *Stadler* in: Jauernig, § 311 Rn. 14.

handelt es sich gemäß § 312l Abs. 3 BGB um einen Dienst, der es Verbrauchern ermöglicht, durch die Verwendung von Software, die vom Unternehmer oder im Namen des Unternehmers betrieben wird, einschließlich einer Webseite, eines Teils einer Webseite oder einer Anwendung, Fernabsatzverträge mit anderen Unternehmern oder Verbrauchern abzuschließen. Betreiber des Online-Marktplatzes ist der Unternehmer, der ihn für Verbraucher zur Verfügung stellt (§ 312l Abs. 4 BGB).

Nicht aufgrund des Mediums des Vertragsschlusses, sondern wegen dessen Gegenstandes können sich zudem weitere besondere Informationspflichten und Widerrufsrechte ergeben, für die sich im Rahmen des Vertragsschlusses über Fides besondere Anforderungen ergeben können. Dies gilt zum Beispiel für Verbraucherdarlehensverträge (§§ 491 ff. BGB), Verbraucherbauverträge (§§ 650i ff. BGB), Teilzeit-Wohnrechteverträgen (§§ 481 ff. BGB) und andere. Da sich diese Besonderheiten jedoch nicht aus dem Vertragsschluss über Fides, sondern aus dem Vertragsgegenstand ergeben und somit immer zu beachten sind, werden sie vorliegend nicht weiter thematisiert.

e) Fehlen rechtshemmender Einreden und kein Entgegenstehen von § 242 BGB

Dem Anspruch aus einem Vertrag können ferner rechtshemmende Einreden entgegenstehen. Rechtshemmende Einreden bewirken, dass ein Anspruch nicht durchsetzbar ist, obwohl er wirksam entstanden und nicht untergegangen ist. In der Gruppe der Einreden sind keine ersichtlich, die bei einem Vertragsschluss über Fides besondere Auswirkungen haben könnte. Weder im Rahmen der Verjährung (§ 214 BGB), von Zurückbehaltungsrechten (§§ 273, 1000 BGB, §369 HGB[52]), der Einrede des nicht erfüllten Vertrages (§ 320 BGB), der Stundung (§§ 311, 241 BGB), noch bei der Arglisteinrede (§§ 821, 853 BGB) oder den Bürgschaftseinreden (§§ 768, 770, 771 BGB) wirkt sich insoweit das Medium des Vertragsschlusses aus. Dasselbe gilt für die Fallgruppen des Einwands des Rechtsmissbrauchs nach § 242 BGB. Auch hier ist nicht zu erkennen, dass sich ein Vertragsschluss über Fides im Rahmen des dolo-agit-Einwandes, noch der Einrede des widersprüchlichen Verhaltens noch im Zusammenhang mit der Fallgruppe rechtsmissbräuchlichen Verhaltens bzw. der Verwirkung beim Vertragsschluss über Fides auswirken könnte.

[52] Handelsgesetzbuch – in der Folge HGB.

f) Besonderheiten eines Vertragsschlusses gemäß Handelsgesetzbuch (HGB)

Im HGB werden einige Vorschriften des BGB für den Wirtschaftsverkehr zwischen Kaufleuten modifiziert. Hierzu gehören auch Regeln zum Vertragsschluss. Grundsätzlich kommt auch im Handelsrecht ein Vertrag nur durch Angebot und Annahme zustande, jedoch wird nach § 362 Abs. 1 S. 1 HGB die Annahmeerklärung eines Kaufmannes fingiert, wenn er auf das Angebot eines Geschäftsbesorgungsvertrages gemäß § 675 BGB schweigt.[53] Ein weiterer Anwendungsfall des Vertragsschlusses durch Schweigen liegt in den Fällen des gewohnheitsrechtlich anerkannten Kaufmännischen Bestätigungsschreibens unter Rückgriff auf § 346 HGB vor.[54]

Da in beiden Fällen bereits fraglich erscheint, ob eine entsprechende Situation des Vertragsschlusses sich unter dem Einsatz von Fides überhaupt ergeben kann und sich in diesen Fällen keine Besonderheiten aus der Verwendung von Fides als Medium des Vertragsschlusses ergeben würden, soll in der Folge auf eine Behandlung der Frage verzichtet werden.

g) Zwischenergebnis

Damit aus einem Vertrag wirksam ein Anspruch hergeleitet werden kann, muss der Vertrag wirksam geschlossen worden sein. Dies setzt ein wirksames Angebot und dessen Annahme sowie deren Abgabe und Zugang voraus. Die Einbeziehung von allgemeinen Geschäftsbedingungen in einen Vertrag macht die Beachtung besonderer Anforderungen erforderlich. Es ist zudem notwendig, dass dem Vertrag keine rechtshindernden und keine rechtsvernichtenden Einwendungen, keine rechthemmenden Einreden sowie kein Einwand eines Rechtsmissbrauchs nach § 242 BGB entgegenstehen.

2. Möglichkeit eines wirksamen Vertragsschlusses mittels Fides

Nachdem die allgemeinen rechtlichen Anforderungen an einen Vertragsschluss dargestellt worden sind, ist nunmehr zu untersuchen, ob ein wirksamer Vertrag unter Einsatz von Fides geschlossen werden kann.

---

[53] Vgl. ausführlich *Hopt* in: Baumbach/Hopt, § 362 Rn. 3 ff.; Kindler, § 7 Rn. 13.
[54] Kindler, § 7 Rn. 16 ff.; *Fest* in: Ebenrotz/Boujong/Joost/Strohn, § 346 Rn. 243 ff.

a) Möglichkeit der Erfüllung der Voraussetzungen eines wirksamen Vertragsschlusses

Die Frage, ob und, falls ja, wie mittels Fides ein rechtswirksamer Vertrag geschlossen werden kann, muss angesichts der zuvor[55] dargestellten verschiedenen Möglichkeiten der Clients zur Kontaktaufnahme, Verwendung von Templates sowie Eingehung von Contracts individuell für die verschiedenen Fallgestaltungen analysiert werden.

Hierbei ist zwischen der grundsätzlichen Möglichkeit eines Vertragsschlusses und dem tatsächlichen Vertragsschluss im Einzelfall zu differenzieren. Denn selbst wenn grundsätzlich die Möglichkeit eines Vertragsschlusses besteht, kann es im Einzelfall, z.B. aufgrund von Willensmängeln am Vorliegen der für eine wirksame Willenserklärung erforderlichen Voraussetzungen fehlen. Gegenstand der folgenden Betrachtung ist gemäß der Studienfrage die Untersuchung der generellen Möglichkeit eines Vertragsschlusses. Denn auch, wenn das Auftreten bestimmter Willensmängel, zum Beispiel aufgrund technischer Unkenntnis, in besonderem Maß mit dem Medium Fides assoziiert sein kann, können Willensmängel bei jeder Form des Vertragsschlusses auftreten und stellen insoweit keine Besonderheit des Mediums Fides dar. Willensmängel im Einzelfall bleiben in der folgenden Betrachtung somit unbeachtet.

aa) Public Key des Vertragspartners ist ohne vorhergehenden Kontakt bekannt

In der ersten Fallgestaltung will ein Client, ohne dass es zuvor zu einem Kontakt zwischen den Parteien gekommen ist, einen Vertrag auf der Basis eines von ihm erstellten Templates eingehen.

Gemäß den zuvor dargestellten Grundsätzen käme ein Vertrag hier zustande, sofern zwischen beiden Seiten inhaltlich übereinstimmende und mit Bezug aufeinander abgegebene Willenserklärungen in Form eines Angebots und dessen Annahme ausgetauscht werden.

Im vorliegenden Fall kann das Template an sich noch kein Angebot darstellen. Unabhängig davon, ob es die inhaltlichen Anforderungen an eine Willenserklärung erfüllt und die essentialia negotii beinhaltet, entäußert sich der Client in diesem Fall nicht des

[55] Vgl. Kap. B. II.

Templates und es geht dem anderen Client auch nicht zu. Dies wäre für den Charakter als Angebot und daher empfangsbedürftige Willenserklärung aber zwingend erforderlich.

Ein Angebot kann vielmehr in dem Contract zu sehen sein, der durch die Verbindung eines Templates mit dem Public Key des anderen Clients entsteht. Erstellt ein Client einen Contract, erzeugt er eine Willensäußerung, die auf das Erreichen einer Rechtsfolge, nämlich die Eingehung eines Vertrages mit einem anderen Client, gerichtet ist. Der erstellende Client handelt bewusst, da er die Eingehung eines Vertrages mit dem anderen Teil beabsichtigt. Der Contract wird somit zielgerichtet kreiert und stellt sich daher als bezweckter Willensakt dar, der auf die Vornahme eines äußeren Verhaltens gerichtet ist.[56] Angesichts des Ziels der Erstellung eines Contracts, nämlich einen Vertrag mit dem anderen Client einzugehen, handelt der Ersteller des Contracts auch in dem Bewusstsein, dass sein Verhalten als rechtserhebliche Erklärung aufgefasst werden kann. Es ist sogar sein Ziel, dass sein an den anderen Client gerichteter Contract als solcher aufgefasst wird, beabsichtigt er doch die Eingehung eines Vertrages. Ebenso kann über den Contract der Willen zur Herbeiführung einer bestimmten Rechtsfolge, d.h. eines Vertrages bestimmten Inhalts, zum Ausdruck gebracht werden, sofern der Contract die relevanten Parameter des Vertrages enthält. Vor diesem Hintergrund bietet Fides die Möglichkeit, sowohl den eigenen Handlungs-, Erklärungs- und auch Geschäftswillen zum Ausdruck zu bringen und insoweit eine wirksame Willenserklärung abzugeben. Ob, und inwieweit es sich dabei um eine automatisierte Willenserklärung, Computererklärung, eine computergestützte Willenserklärung oder lediglich eine elektronische übermittelte Willenserklärung handelt, kann dahinstehen, da die Einordnung ohne Bedeutung für die Klassifizierung als wirksame Willenserklärung ist, da diese jedenfalls immer auf einen menschlichen Willen zurückzuführen ist.[57] Computergestützt ist insoweit, wenn überhaupt, der objektive Tatbestand der Willenserklärung, während der subjektive immer von einem Menschen erfüllt wird.[58]

---

[56] Vgl. hierzu für blockchainbasierte Smart Contracts auch *Heckelmann*, NJW 2018, 504, 505, der richtigerweise darauf hinweist, dass eine Willenserklärung als Ausdruck eines rechtlichen Willens sogar in einem Bierdeckel oder einer Tätowierung bestehen könne.

[57] BGH, NJW 2005, 53, 54; BGHZ 195, 126; *Paulus*, JuS 2019, 960, 961 f.; *Köhler*, AcP 1982, 117; *Paulus/Matzke*, ZfPW 2018, 431, 441.

[58] BGH, NJW 2013, 598, 599; *Paulus*, JuS 2019, 960, 963; *Köhler*, AcP 1982, 117, 132 ff.; *Paulus/Matzke*, ZfPW 2018, 431, 441.

Da es sich bei dem Angebot um eine empfangsbedürftige Willenserklärung handelt, muss der Client sich des Contracts zudem willentlich so entäußern können, dass er unter normalen Umständen so in den Empfangsbereich des anderen Teils gelangt, sodass dieser ebenfalls unter normalen Umständen die Möglichkeit zur Kenntnisnahme hat. Da beide Parteien sich nicht an derselben Örtlichkeit aufhalten, kommt es bei Fides insoweit auf den Zugang zwischen Abwesenden an. Durch das Veröffentlichen des Contracts im Full Node, über den der andere Client Zugang zum Contract bekommt, bringt der den Contract erstellende Client seine Willenserklärung in Richtung des anderen Teils auf den Weg. Dies geschieht zudem nicht automatisch, sondern willentlich in Form des Hochladens in den Full Node mittels eines entsprechenden Klicks oder einer Tasteneingabe als nach außen tretenden Willensakt. Im Full Node kann der andere Client wiederum auf den Contract zugreifen und wird durch das Prüfen des Template Index auf den neuen Vertrag auch aufmerksam gemacht. Mit dem Hochladen in den Full Node erhält der andere Client daher eine Zugriffsmöglichkeit auf den Contract, wobei unter normalen Umständen auch mit der Kenntnisnahme durch ihn zu rechnen ist.

Ein über Fides im Full Node veröffentlichter Contract stellt somit eine Willenserklärung dar, die abgegeben worden ist und mit deren Zugang beim Empfänger unter normalen Umständen zu rechnen ist. Ob es sich bei dieser Willenserklärung aber auch um ein Angebot handelt, hängt wesentlich von ihrem Inhalt ab. Erforderlich ist insoweit, dass alle vertragswesentlichen Bestandteile (essentialia negotii) bereits enthalten sind. Angesichts der hohen Variabilität des Einsatzes von Fides und der Gestaltung von Templates sowie darauf basierenden Contracts kann dies nur im Einzelfall bestimmt werden. Grundsätzlich ist es aber möglich, dass ein publizierter Contract die essentialia negotii enthält, sodass er auch die inhaltlichen Anforderungen an ein Angebot erfüllen kann, das so konkret gefasst sein ist, dass es mit einer einfachen Bestätigung angenommen werden kann.

Ein Vertrag zwischen den Parteien kann nur zustande kommen, wenn ein in Form des Contracts unterbreitetes Angebot vom anderen Teil auch angenommen wird. Die auf die Veröffentlichung des Contracts im Full Node folgende Annahme des Contracts statuiert noch keine Annahme des Angebots und lässt noch keinen Vertrag im Rechtssinne zwischen den Parteien entstehen. Dies liegt darin begründet, dass mit der initialen Annahme des Contracts zunächst lediglich die mit ihm ausgedrückte Aufforderung zur

Aufnahme einer Kommunikation akzeptiert wird. Ähnlich wie beim Öffnen eines Briefes, der ein zugesandtes Angebot enthält oder beim Annehmen eines Telefonats, in dessen Rahmen über ein unterbreitetes Angebot gesprochen wird, hat der empfangende Teil zu diesem Zeitpunkt noch keine Kenntnis vom Inhalt des Angebotes und kann daher noch nicht wissen, ob er einen Vertrag mit dem unterbreiteten Inhalt wirklich eingehen will. Diesen muss er zunächst wahrnehmen können, was aber die Annahme des Contracts erforderlich macht.

In Ausnahmefällen kann die Annahme eines „Contract Offers" jedoch auch als Annahme eines Angebots zum Vertragsschluss zu werten sein. Diese in der Praxis voraussichtlich seltene Möglichkeit ergibt sich, sofern im bereitgestellten Template alle für den Vertragsschluss erforderlichen Informationen bereits unveränderlich enthalten sind und die Person des Kotrahierenden dem Client, z.B. aufgrund einer vorherigen Registrierung, bekannt ist. In diesem Fall müssten also der genaue Vertragsgegenstand, sein Preis und die Menge im Template aufgeführt sein und der Client müsste im Rahmen der Registrierung seinen Public Key angegeben haben. Der das Template bereitstellende Client wäre sich dann im Moment der Entscheidung über die Annahme des „Contract Offers" aller für einen Vertrag relevanten Angaben bewusst, sodass keine Unsicherheit über den Vertragsinhalt bestehen würde. Angesichts der exakten Nennung insbesondere auch der Menge und Kenntnis des Vertragspartners wäre er in der Lage bereits zu diesem Zeitpunkt abzuschätzen, ob er einen Vertrag dieses Inhalts mit diesem Client eingehen will und, ob er über ausreichende Lagerbestände zur Erfüllung des Vertrages verfügt. Dies wird in der Praxis insofern eine Ausnahme darstellen, als es dann erforderlich wäre, für jedes angebotene Produkt ein eigenes Template bereitzuhalten und bei der Bestellung größerer Mengen eines Produkts gegebenenfalls mehrere Contracts entsprechend der gewünschten Stückzahl erzeugt werden müssten.

Wann der andere Teil ein in einem Contract enthaltenes Angebot annimmt, hängt vielmehr wiederum von den Umständen des Einzelfalls und insbesondere der Gestaltung des Templates ab. Dort kann einerseits eine eigenständige Task „Annahme" enthalten sein, durch dessen Bestätigen und die darauf folgende Publikation im Full Node das Angebot angenommen wird. Zu beachten ist insoweit, dass es sich auch bei der Annahme

um eine empfangsbedürftige Willenserklärung handelt[59], wobei deren Zugang nur in den Ausnahmefällen des § 151 BGB entbehrlich ist. Damit erfolgt die Annahme nicht durch das Bestätigen der Task, sondern die Publikation im Full Node, mit der sich der annehmende Client der Erklärung entäußert und für den anbietenden Client, wie oben in Bezug auf das Angebot ausführlich dargestellt, die Möglichkeit der Kenntnisnahme über den aktualisierten Full Node besteht.

Möglich ist ferner eine konkludente Annahme des Angebots durch eine bestätigende Handlung. Eine solche kann, erneut je nach Gestaltung des Templates, auch darin zu sehen sein, dass der annehmende Teil eine mit der Ausführung des Vertrages verbundene Task bestätigt und an den Full Node sendet. Auch in diesen Fällen ist jedoch eine nach außen tretende bestätigende Handlung erforderlich. Verengt man die Betrachtung einer solchen Bestätigung im Rahmen von Fides auf die rein virtuellen Möglichkeiten und blendet somit Fälle aus, in denen ohne vorhergehende Handlung bei Fides ein Vertrag in der realen Welt vom annehmenden Teil einfach ausgeführt wird, ist zur Annahme des Vertrages somit das Bestätigen eines Tasks und die Veröffentlichung im Full Node erforderlich.

Die Ablehnung eines Angebots, das in einem Contract enthalten ist, kann entsprechend der vorstehenden Subsumtion somit durch das explizite Erfüllen einer Task „Angebot ablehnen“ erfolgen. Möglich ist aber auch die Ablehnung durch Nichtreagieren im Anschluss an die Aufnahme der Kommunikation, die mittels der Annahme des Contracts erfolgt. Denn durch ein Schweigen wird, außer in den zuvor[60] genannten Ausnahmefällen, keine Annahme ausgedrückt.

An die Ablehnung eines Angebots oder auch in Fällen von Contracts, die nicht bereits die essentialia negotii enthalten, können sich Vertragsverhandlungen anschließen, die, wie oben dargestellt, über Fides geführt werden können. Für einen sich hieraus ergebenden Vertragsschluss gelten die zuvor ausgeführten Anforderungen entsprechend.

bb) Templates und Public Key werden öffentlich bereitgestellt

Den häufigsten Fall stellt die Einbindung von Fides in ein Verifikationssystem, wie zum Beispiel einen Onlinemarktplatz oder eine andere Onlineplattform dar, über die ein Client

[59] *Mansel* in: Jauernig, § 147 Rn. 1; *Ellenberger* in: Grüneberg, § 147 Rn. 1; *Busche* in: MK-BGB, § 147 Rn. 2.
[60] B. II. 1.

seine vertraglichen Leistungen anbietet und über die er seinen Public Key sowie unter Umständen ein eigenes Template für einen Contract bei Fides bereitstellt.

Nutzt der Client, der die vertragliche Leistung der auf der Plattform vertretenen Partei in Anspruch nehmen möchte, ein eigenes Template für die Eingehung eines Vertrages und publiziert es, ergeben sich in Bezug auf den Vertragsschluss keine Unterschiede zu der im vorhergehenden Unterkapitel geschilderten Situation. Das Anbieten einer Ware oder Leistung auf einer Onlineplattform stellt noch kein Angebot dar, wenn nicht die AGB des Seitenbetreibers etwas Abweichendes vorsehen. [61] Wie auch bei physischen Warenauslagen in Schaufenstern von Geschäftsräumen stellt das Darstellen der Ware auf einer Plattform kein Angebot, sondern vielmehr eine invitatio ad offerendum dar.[62] Für die Gründe sei auf die Ausführungen oben[63] verwiesen. Im Übrigen ist die Möglichkeit eines Vertragsschlusses wie in der zuvor[64] geschilderten Fallkonstellation zu bewerten.

Eine andere rechtliche Bewertung könnte sich ergeben, sofern der eine Ware oder Dienstleistung anbietende Client zugleich auch ein Template für die Erstellung eines Contracts bei Fides öffentlich zur Verfügung stellt. Hier könnte bereits das öffentlich bereitgestellte Template als Angebot verstanden, das dann mittels des von der anderen Seite daraus erzeugten und im Full Node publizierten Contract angenommen wird. Gegen dieses Verständnis sprechen jedoch verschiedene Argumente. Zunächst enthält das Template nicht die andere Partei, mit der ein Vertrag geschlossen werden soll, sodass ein wesentlicher Vertragsbestandteil fehlt. Dies wäre nur in Fällen einer „Offerte ad incertas personas“ nicht erforderlich, in denen es dem Vertragspartner egal ist, mit wem er einen Vertrag schließt.[65] Hierbei handelt es sich jedoch um Fälle, in denen die gegenseitigen Leistungen umgehend bewirkt werden und erkennbar ist, ob eine Leistung verfügbar ist und somit tatsächlich noch ein Angebot vorliegt, wie zum Beispiel bei Warenautomaten.[66] Eine solche Beschränkung des Angebots ist im Rahmen von Fides schon nicht möglich. Daher ergäbe sich das oben[67] bereits angeführte Problem, dass mit dem Anbieter eine

[61] BGH, NJW 2002, 363; NJW 2013, 598 Tz. 14; *Ellenberger* in: Grüneberg, § 145 Rn. 2.
[62] BGH, NJW 1980, 1388; Brox, BGB AT, Rn. 167; *Ellenberger* in: Grüneberg, § 145 Rn. 2.
[63] B. II. 1. a).
[64] B. II. 2. a) bb).
[65] Brox/Walker, BGB AT Rn. 166; *Ellenberger* in: Grüneberg, § 145, Rn. 7.
[66] Padeck, VersR 1989, 541, 542; Brox/Walker, BGB AT Rn. 166; *Ellenberger* in: Grüneberg, § 145 Rn. 7.
[67] B. II. 1. a).

unbegrenzte Anzahl von Verträgen geschlossen werden könnte, wenn man bereits das Template als Angebot verstünde. Zu deren Erfüllung wäre der Anbieter jedoch nicht in der Lage, sodass er sich schadenersatzpflichtig machen könnte.[68] Zudem wird es dem Client, über dessen Waren oder Dienstleistungen der Vertrag geschlossen werden soll, regelmäßig schon wegen der Bezahlung auf die Person des Vertragspartners ankommen. Diese Gründe sprechen dafür, das Bereitstellen des Templates nicht als Angebot, sondern als „invitatio ad offerendum" zu bewerten. Vor diesem Hintergrund ist die Situation des Vertragsschlusses hier mit der zuvor[69] betrachteten Fallkonstellation identisch. Ein Angebot wird auch hier durch das Publizieren des Contracts abgegeben.

Auch die Annahme erfolgt wie in der vorhergehenden Konstellation geschildert, d.h. also nicht bereits durch die Annahme des Contracts nach dessen Veröffentlichung im Full Node. Es kann argumentiert werden, dass bei der Verwendung des von der anderen Seite bereitgestellten Templates bereits mit der Annahme der Kommunikation über den Contract zum Ausdruck gebracht wird, dass die andere Seite einen Vertrag schließen will. Auch die für eine invitatio ad offerendum sprechenden Argumente würden dabei nicht unterlaufen, da der Client einen Contract einfach ablehnen kann, sofern er, zum Beispiel aufgrund fehlender Vorräte, nicht zu einem Vertragsschluss bereit wäre. Hiergegen spricht jedoch, dass für den Vertragspartner, der den Contract empfängt, dessen Inhalt in der Regel nicht zu erkennen ist, wenn nicht zuvor die Kommunikation durch Annehmen des Contracts zugelassen wird. Eine Ausnahme stellt insoweit lediglich die zuvor beschriebene Gestaltung eines sehr eng gefassten Templates dar.[70] Auch wenn der Client somit ein Template zur Erstellung eines Contracts zur Verfügung gestellt hat, kann er erst nach Annehmen des Contracts und der Bereitstellung der nötigen Informationen überprüfen, ob es sich um einen von ihm gewollten Vertragsinhalt handelt. Aus diesen Gründen entsteht hierdurch noch kein Vertrag im Rechtssinn.

cc) Vorhergehen von Kommunikation zwischen den Clients

Zuletzt besteht die Möglichkeit, dass im Rahmen einer vorhergehenden Kommunikation beider Seiten ein Austausch von Templatehashes oder der Public Keys erfolgt ist und sogar Vertragsverhandlungen stattgefunden haben. Eine geänderte rechtliche Bewertung

---

[68] *Busche* in: MK-BGB, § 145 Rn. 10; Brox/Walker, BGB AT, Rn. 167.
[69] B. II. 2. a) aa).
[70] Vgl. Kap. C. I. 2. a) aa).

des Vertragsschlusses ergibt sich hieraus jedoch nur, sofern die Parteien im Rahmen dieser Verhandlungen bereits außerhalb von Fides Willenserklärungen ausgetauscht habe, die als Angebot und dessen Annahme zu werten sind. Im Übrigen kann auch hier aus den zur vorhergehenden Fallkonstellation besprochenen Gründen eine Annahme des Vertrages noch nicht in der Annahme des Contracts zu sehen sein, da diese erforderlich ist, um den Inhalt des Contracts wahrnehmen zu können. Auch im Fall vorhergehenden Kontakts muss es der Partei, der ein Vertrag angetragen wird, möglich sein, dessen Inhalt zu prüfen. Dies ist in der Regel nur durch Zulassen der Kommunikation und damit das Akzeptieren des Contracts möglich, sodass erst im Anschluss hieran durch eine bestätigende Handlung, z.B. in Form der Annahme einer Task und der Publikation im Full Node, die Annahme erklärt werden kann.

dd) Zwischenergebnis

Aufgrund der vorstehend durchgeführten Untersuchung kann festgestellt werden, dass grundsätzlich die Möglichkeit besteht, Verträge mithilfe von Fides zu schließen. Angesichts der hohen Variabilität des Einsatzes von Fides ist die konkrete Wirksamkeit des Vertragsschlusses von einer Einzelfallbetrachtung, insbesondere dem Inhalt des Contracts und seiner konkreten Gestaltung sowie dem konkret beabsichtigten Vertrag abhängig. Hierbei handelt es sich jedoch um keine mit Fides assoziierte Besonderheit. Vielmehr stellt die Einzelfallabhängigkeit eine rechtliche Problematik dar, die bei allen zum Abschluss eines Vertrages eingesetzten Mitteln – selbst mündlich oder per Brief – auftritt.

b) Mögliche Auswirkungen auf den Vertragsschluss durch die Verwendung von AGB

Fragen in Bezug auf die Verwendung von AGB können sich im Zusammenhang mit Fides in zwei verschiedenen Kontexten stellen. Einerseits kann es erforderlich sein, existierende AGB in einen über Fides zu schließenden Vertrag zu integrieren. Anderseits kann es sich bei den Bestimmungen des über Fides geschlossenen Vertrages selbst um AGB handeln.

Für die Einbeziehung existierender AGB in einen über Fides zu schließenden Vertrag sind die Anforderungen des § 305 Abs. 2 BGB von Bedeutung. Auf die einzubeziehenden AGB muss daher beim Vertragsschluss hingewiesen werden und es muss dem anderen Teil in zumutbarer Weise möglich sein, von deren Inhalt Kenntnis zu nehmen. Hierfür gibt es bei der Verwendung von Fides für einen Vertragsschluss verschiedene geeignete

Möglichkeiten. Ein Weg könnte darin besteht, die Einbeziehung der AGB zum Bestandteil der Task „Annahme des Vertrages“ zu machen und die Möglichkeit der Kenntnisnahme, zum Beispiel über einen Link, zu eröffnen. Die Einbeziehung von existierenden AGB ist bei der Verwendung von Fides somit grundsätzlich möglich.

Angesichts der mehrfachen Verwendungsmöglichkeit von Templates aber auch der Regelung des § 310 Abs. 3 BGB bei einmaliger Verwendung durch einen Unternehmer gegenüber einem Verbraucher kann auch die in einem Template selbst enthaltene Regelung selbst eine AGB im Sinne des § 305 Abs. 1 S. 1 BGB darstellen. In diesen Fällen unterliegt sie einer gesonderten Inhaltskontrolle gemäß den §§ 307 ff. BGB.

Sofern die gesetzlichen Anforderungen beachtet werden, stellt somit weder die Einbeziehung existierender AGB, noch die Möglichkeit, dass eine Bestimmung eines über Fides geschlossenen Vertrages selbst als AGB zu werten ist, ein rechtliches Problem für die Verwendung von Fides dar, das sich gerade aus dem Einsatz der Software als Medium des Vertragsschlusses selbst ergibt.

c) Auswirkungen rechtshindernder Einwendungen

Relevanz kann ein Vertragsschluss über Fides dann entfalten, sofern ein formbedürftiges Rechtsgeschäft geschlossen werden soll. Insoweit ist zu betrachten, welchen Formanforderungen ein Vertragsschluss unter Verwendung von Fides gerecht werden kann.

Für die Einhaltung der Textform ist es insoweit erforderlich, dass die Erklärung in einer zur dauerhaften Wiedergabe in Schriftzeichen geeigneten Weise abgegeben wird. Dies ist bei der Verwendung eines dauerhaften Datenträgers der Fall. Er wird gemäß § 126b S. 2 BGB definiert als Medium, das es dem Empfänger ermöglicht, eine auf dem Datenträger befindliche, an ihn persönlich gerichtete Erklärung so aufzubewahren oder zu speichern, dass sie ihm während eines für ihren Zweck angemessenen Zeitraums zugänglich ist, und geeignet ist, die Erklärung unverändert wiederzugeben. Bei elektronischen Erklärungen, wie sie für Fides relevant sind, wird unterschieden, ob die Erklärung der Person übermittelt wird oder nicht. Im Fall der Übermittlung genügt es für die Dauerhaftigkeit der Wiedergabe, dass der Empfänger die Erklärung speichern und ausdrucken kann,

während ein tatsächlicher Ausdruck nicht erforderlich ist.[71] Bei nicht übermittelten Texten, die lediglich online abrufbar sind, muss für die Wahrung der Textform ein Download, also mindestens ein Abspeichern, vorgenommen werden.[72] Soweit es darauf ankommt, ob eine über Fides abgegebene Erklärung die Textform erfüllt, muss auf den Contract abgestellt werden. Dieser wird sowohl in verschlüsselter Form im Full Node als auch auf den Endgeräten der beteiligten Clients gespeichert. Ähnlich wie bei einer Email kann daher davon ausgegangen werden, dass die Erklärung den Beteiligten übermittelt worden ist, sodass nach den zuvor dargestellten Grundsätzen auf die reine Möglichkeit zur Speicherung des Contracts abgestellt werden kann und Fides damit die Anforderungen an einen dauerhaften Datenträger erfüllt. Dies gilt umso mehr als der Status von geschlossenen Contracts bei ausbleibenden Aktualisierungen im Full Node zwar gelöscht wird, der Contract auf den Endgeräten jedoch abrufbar bleibt. Somit ergibt sich auch in Bezug auf die Verfügungsgewalt über die Dauerhaftigkeit der Erklärung in Form des Contracts kein materieller Unterschied zur Übersendung der Erklärung per Mail, da sie nicht ohne Zutun des Clients von dessen Handy und damit dem Datenträger gelöscht werden kann. Selbst wenn man von nur von einer Abrufbarkeit des Contracts als Erklärung im Full Node ausgehen wollte, wäre das Erfordernis des Downloads mit der Speicherung der Contractdaten auf dem Endgerät des Clients erfüllt.

Die Erklärung muss die Person des Erklärenden nennen. Hierfür genügt eine mechanische Angabe als Unterschrift, im Kopf der Erklärung oder in deren Text.[73] Dabei ist es nicht erforderlich, dass der bürgerliche Name genannt wird, sondern, sofern es für den Empfänger verständlich ist, genügt vielmehr auch ein Wahl- oder Spitzname.[74] Vorliegend besteht angesichts der unterschiedlichen Gestaltungsmöglichkeiten eines Templates und daraus abgeleiteter Contracts nicht die Möglichkeit eine pauschale Aussage darüber zu treffen, ob dort eine Name aufgeführt ist. Da jedoch das Aufführen eines Wahl- oder Spitznamens zur Nennung der erklärenden Person genügt, muss es vorliegend zur Erfüllung der Anforderung auch ausreichend sein, wenn der Public Key eines Clients genannt wird, da hierüber vom Erklärungsempfänger eine Identifikation des Erklärenden

[71] *Einsele* in: MK-BGB, § 126b Rn. 3; *Ellenberger* in: Grüneberg, § 126b Rn. 3.
[72] EuGH, EuZW 2012, 638; BGH, NJW 2010, 3566, Tz. 19.
[73] *Einsele* in: MK-BGB, § 126b Rn. 5; *Ellenberger* in: Grüneberg, § 126b Rn. 4.
[74] *Arnold* in: Erman, § 126b Rn. 4; *Ellenberger* in: Grüneberg, § 126b Rn. 4.

erfolgen kann und die so vorgenommene Bezeichnung ein eindeutiges Identifikationsmittel für den Empfänger darstellt.

Zuletzt muss eine Erklärung auch abgeschlossen, d.h. beendet, sein, wobei es jedoch keiner Unterschrift bedarf.[75] Vielmehr genügt hierfür eine Datierung, eine Grußformel oder auch eine sonstige Weise des Abschlusses einer Erklärung.[76] Da sich das Ende einer Erklärung und damit ihr Umfang somit auch aus rein inhaltlichen Gesichtspunkten ergeben kann, erscheint es möglich, sowohl einen Contract als Ganzes als auch eine darin enthaltene Task als in sich abgeschlossene Erklärungen zu verstehen, deren Umfang sich aus inhaltlichen Gesichtspunkten ergibt.

Mittels Fides kann vor dem Hintergrund der vorstehenden Ausführungen somit die Textform gemäß § 126b BGB gewahrt werden.[77] Die Einhaltung anderer Formen ist jedoch nicht möglich. Eine zur Einhaltung der Schriftform nach § 126 BGB notwendige eigenhändige Namensunterschrift oder notariell beglaubigtes Handzeichen kann im Rahmen von Fides nicht verwendet werden. Die elektronische Schriftform nach § 126a BGB wiederum erfordert eine qualifizierte elektronische Signatur im Sinne des Art. 3 Nr. 10 eIDAS-VO, die im Zusammenhang mit Fides ebenfalls nicht vorgenommen werden kann. Auch erfüllt Fides nicht die Anforderungen einer öffentlichen Beglaubigung oder einer notariellen Beurkundung, da die Regeln des Beurkundungsverfahrens nicht eingehalten werden und auch keine Beglaubigung der Erklärung stattfindet. Verträge, die eine Einhaltung dieser Formvorschriften erfordern und über Fides abgeschlossen würden, wären gemäß § 125 S. 1 BGB nichtig.

d) Auswirkungen rechtsvernichtender Einwendungen

Wie zuvor[78] ausgeführt kann der Vertragsschluss über Fides dazu führen, dass aufgrund der daraus resultierenden Typisierung mit dem Vertrag besondere Rechte und Pflichten für die Parteien verbunden sind.

---

[75] BGH, NJW 2011, 295, Tz. 13; *Ellenberger* in: Grüneberg, § 126b Rn. 5.
[76] BGH, NJW 2011, 295, Tz. 13; BGH, NJOZ 2012, 926, Tz. 20; *Ellenberger* in: Grüneberg, § 126b Rn. 5.
[77] Anders, jedoch für nicht in natürlicher Sprache abgefasste, blockchainbasierte Smart Contracts *Bertram*, MDR 1416, 1419. Auch für blockchainbasierte Smart Contracts bejahend *Heckelmann*, NJW 2018, 504, 507.
[78] B. I. 1. d).

aa) Klassifizierung als Fernabsatz-, Verbraucher- oder außerhalb von Geschäftsräumen geschlossener Vertrag

Für Fides ist insbesondere die mögliche Kategorisierung als Fernabsatzvertrag relevant. Gemäß § 312c Abs. 1 BGB muss ein Vertrag unter der ausschließlichen Verwendung von Fernkommunikationsmitteln abgeschlossen werden. Ein Fernkommunikationsmittel ist nach § 312c Abs. 2 BGB jedes Kommunikationsmittel, das zur Anbahnung oder zum Abschluss eines Vertrages eingesetzt werden kann, ohne dass die Vertragsparteien gleichzeitig körperlich anwesend sind, wie Briefe, Kataloge, Telefonanrufe, Telekopien, Emails, SMS sowie Rundfunk oder Telemedien. Da es sich bei den im Gesetz aufgeführten Fernkommunikationsmitteln um keine abschließende Aufzählung handelt, kann hier dahinstehen, ob Fides unter eine der genannten Kategorien fällt. Wie der Sachverhalt ausführt und auch die vorhergehenden Ausführungen gezeigt haben, besteht die Möglichkeit, mittels Fides einen Vertrag zu schließen, ohne dass die daran beteiligten Parteien hierfür gleichzeitig physisch anwesend sein müssen. Angesichts der vielseitigen Einsatzmöglichkeiten von Fides und der sich daraus ergebenden unterschiedlichen Arten des Vertragsschlusses stellen über Fides geschlossene Verträge jedoch auch nicht zwangsläufig Fernabsatzverträge dar, da auch Fallkonstellationen denkbar sind, in denen neben der Verwendung von Fides und anderen Fernkommunikationsmitteln auch ein persönlicher Kontakt erfolgt ist. Fernabsatzverträge müssen jedoch unter ausschließlicher Verwendung von Fernkommunikationsmitteln zustande gekommen sein, sodass ein persönlicher Kontakt in der Phase der Vertragsanbahnung die Charakterisierung als Fernabsatzvertrag ausschließt. [79] Ein Fernabsatzvertrag liegt zudem nur vor, wenn sich ein Unternehmer (§ 14 BGB) und ein Verbraucher (§ 13 BGB) als Vertragsparteien gegenüberstehen, was ebenfalls eine Frage des konkreten Einzelfalls in Bezug auf einen mittels Fides geschlossenen Vertrages darstellt. Bei Fides handelt es sich zudem um ein für den Fernabsatz organisiertes Vertriebs- oder Dienstleistungssystem. Hierfür genügt es, dass ein Unternehmer planmäßig mit dem Angebot der Bestellung per Fernabsatzvertrag und Lieferung der Ware wirbt und seinen Betrieb so organisiert, dass Verträge regelmäßige im Fernabsatz abgeschlossen und abgewickelt werden können. [80] Durch diesen Ausnahmetatbestand sollen

[79] BGH, NJW 2018, 1387; OLG Hamburg, WM 2014, 1538; OLG Saarbrücken, NJW-RR 2014, 1521; *Grüneberg* in: Grüneberg, § 312c Rn. 4.
[80] BGH, NJW 2004, 3699, 3700 f; *Wendehorst* in: MK-BGB, § 312c Rn. 22; *Grüneberg* in: Grüneberg, § 312c Rn. 6.

Fallgestaltungen ausgeschlossen werden, in denen es auch zufällig zu Vertragsschlüssen per Fernkommunikationsmitteln kommt oder lediglich Kontaktdaten auf einer Homepage angegeben werden.[81]

Es muss sich bei dem Vertrag zudem um einen entgeltlichen Vertrag handeln und es darf keine Bereichsausnahme gemäß § 312 Abs. 2 BGB einschlägig sein. Sofern nach den dargestellten Anforderungen ein Fernabsatzvertrag vorliegt, sind die oben[82] angeführten Rechte und Pflichten sowie Ausnahmen von diesen zu beachten. Insbesondere erscheint hierbei aber auch die Erfüllung der gemäß § 312d BGB bestehenden Informationspflichten nach Art. 246a EGBGB unproblematisch möglich.

Aus der Verwendung von Fides ergeben sich keine Besonderheiten nach § 312a BGB, wobei insbesondere § 312a Abs. 1 und 2 BGB nicht anwendbar sind, da sie Informationspflichten bei Telefonaten und im stationären Handel betreffen.[83] Lediglich theoretisch ist die Möglichkeit, dass es sich bei einem über Fides geschlossenen Vertrag um einen außerhalb von Geschäftsräumen geschlossenen Vertrag im Sinne des § 312b BGB handelt. Hierfür ist erforderlich, dass ein Vertrag zwischen einem Verbraucher und einem Unternehmer bei gleichzeitiger körperlicher Anwesenheit an einem Ort geschlossen wird, der kein Geschäftsraum des Unternehmers ist (§ 312b Abs. 1 S. 1 Nr. 1 BGB). Zwar ist es denkbar, dass sich die Vertragsparteien eines über Fides geschlossenen Vertrages außerhalb des Geschäftsraumes treffen und dort über Fides einen Vertrag abschließen. Dieser umständliche Weg eines Vertragsschlusses stellt jedoch ein eher theoretisches Einsatzfeld für Fides dar, denn in diesen Fällen könnte ein Vertrag einfacher ohne den Einsatz von Fides direkt mündlich geschlossen werden. Damit verbundene besondere Rechte und Pflichten der Parteien wären zudem nicht auf den Einsatz von Fides, sondern den Vertragsschluss außerhalb des Geschäftsraumes eines Unternehmers zurückzuführen und sollen daher vorliegend nicht thematisiert werden.

bb) Klassifizierung als Vertrag im elektronischen Geschäftsverkehr

Verträge, die über Fides geschlossen werden, können zudem als Verträge im elektronischen Geschäftsverkehr nach § 312i BGB klassifiziert werden, was der Fall ist,

---

[81] LG Memmingen, MMR 2004, 769, 770; *Wendehorst* in: MK-BGB, § 312c Rn. 22; *Grüneberg* in: Grüneberg, § 312c Rn. 6.
[82] B. I. 1. d).
[83] *Schulte-Nölke* in: Schulze, § 312a Rn. 2 f.; *Grüneberg* in: Grüneberg, § 312a Rn. 2 f.

wenn sich ein Unternehmer zum Abschluss eines Vertrages über die Lieferung von Waren oder die Erbringung von Dienstleistungen Telemedien bedient. Die Norm ist für Fides daher jedenfalls nur dann von Bedeutung, sofern der Anbieter ein Unternehmer im Sinne des § 14 BGB ist.

Zudem müsst es sich bei Fides dann auch um ein Telemedium handeln. Telemedien sind gemäß der Legaldefinition in § 1 Abs. 1 TMG[84] alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienst nach § 3 Nr. 61 des TKG[85], telekommunikationsgestützte Dienste nach § 3 Nr. 63 TKG oder Rundfunk nach § 2 RStV[86] sind.

Ein Informations- und Kommunikationsdienst stellt einen Oberbegriff für alle multimedialen Angebote dar, bei denen die Dienstleistung selbst elektronisch erbracht werden muss und im Fall von Telemedien Bereitstellung von Inhalten elektronisch erfolgt.[87] Dies ist bei Fides der Fall. Die Erbringung der Dienstleistung in Form der Möglichkeit eines Vertragsschlusses unter Einsatz von Fides ist rein elektronisch, sodass es sich um einen Informations- und Kommunikationsdienst handelt.

Telekommunikationsdienste nach § 3 Nr. 61 TKG sind in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetzte und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen: Internetzugangsdienste, interpersonelle Telekommunikationsdienste und Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste die für Maschine-Maschine-Kommunikation und den Rundfunk genutzt werden. Für die Abgrenzung zu einem Inhaltsdienst dient dabei in der Praxis die Frage, ob der Anbieter dem Kunden eine bestimmte Telekommunikationsleistung schuldet oder die Leistung lediglich auf einer Datenverbindung aufbaut.[88] Fides ist kein Access Provider und stellt damit keinen Internetzugangsdienst dar. Auch dient es nicht ganz oder überwiegend der

[84] Telemediengesetz – in der Folge TMG.
[85] Telekommunikationsgesetz – in der Folge TKG.
[86] Rundfunkstaatsvertrag – in der Folge RStV.
[87] *Ricke* in: Spindler/Schuster, § 1 Rn. 4; *Spindler* in: Spindler/Schmitz, TMG, § 1 Rn. 10; *Martini* in: BeckOK Informations- und Medienrecht, TMG, § 1 Rn. 8.
[88] *Assion* in: Assion, TTDSG, § 3 Rn. 71.

Signalübertragung. Es lässt jedoch Elemente eines interpersonellen Telekommunikationsdienstes erkennen. Hierbei handelt es sich um einen gewöhnlich gegen Entgelt erbrachten Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Telekommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen. Es besteht die Möglichkeit für Clients über Fides in Kontakt zueinander zu treten und Vertragsverhandlungen durchzuführen, wobei anders als bei anderen Systemen die Verwendung von natürlicher Sprache und somit echte Kommunikation möglich ist. Dies ändert jedoch nichts daran, dass die Funktion von Fides darin besteht, Verträge schließen zu können. Auch wenn das System die Verwendung natürlicher Sprache ermöglicht, ist der Zweck des Einsatzes von Fides doch gerade nicht wie bei einem Messanger- oder Maildienst der sprachliche Austausch zwischen den Clients, sondern vielmehr der Abschluss und die Verwaltung von Verträgen. Die Kommunikationsfunktion stellt sich somit als untergeordnete Nebenfunktion des Dienstes dar, was dazu führt, dass Fides nicht als interpersoneller Telekommunikationsdienst und damit auch nicht als Telekommunikationsdienst im Sinne von § 3 Nr. 61 TKG zu klassifizieren ist.

Ein telekommunikationsgestützter Dienst im Sinne des § 3 Nr. 63 TKG ist ein Dienst, der keinen räumlich oder zeitlich trennbaren Leistungsfluss auslöst, sondern bei dem die Inhaltsleistung noch während der Telekommunikationsverbindung erbracht wird. Bei diesen Diensten wird somit über die telekommunikationsseitige Vermittlungsfunktion die inhaltliche Leistung eines Dienstleisters erbracht.[89] Eine solche Inhaltsleistung, wie sie bei Mehrwertdiensten erbracht wird, existiert im Rahmen von Fides nicht, da hier lediglich eine Plattform für den Vertragsschluss und dessen Anbahnung, und somit für fremde Inhalte angeboten wird. Es handelt sich somit nicht um einen telekommunikationsgestützten Dienst.

[89] *Ditscheid/Rudloff* in: Geppert/Schütz, Vorbem §§ 66 – 67 Rn. 8; *Ricke* in: Spindler/Schuster, § 3 Rn. 51; *Arndt/Fetzer* in: Fetzer/Scherer/Graulich, TMG, § 3 Rn. 105.

Rundfunk ist gemäß § 2 Abs. 1 RStV ein linearer Informations- und Kommunikationsdienst; er ist die für die Allgemeinheit und zum zeitgleichen Empfang bestimmte Veranstaltung und Verbreitung von Angeboten in Bewegtbild oder Ton entlang eines Sendeplans unter Benutzung elektromagnetischer Schwingungen. Der Begriff schließt Angebote ein, die verschlüsselt verbreitet werden oder gegen besonderes Entgelt empfangbar sind. Vor diesem Hintergrund handelt es sich bei Fides somit auch nicht um Rundfunk, da Fides weder linear funktioniert noch für den zeitgleichen Empfang in Bild oder Ton ausgelegt ist.

Da Fides somit ein Informations- und Kommunikationsdienst ist, der weder Telekommunikationsdienste nach § 3 Nr. 61 TKG, telekommunikationsgestützter Dienst im Sine des § 3 Nr. 63 TKG noch Rundfunk gemäß § 2 Abs. 1 RStV ist, handelt es sich bei Fides um ein Telemedium im Sinne des § 1 Abs. 1 TMG.[90]

Für die Klassifizierung als Vertrag im elektronischen Geschäftsverkehr müsste sich der Unternehmer als Client des Telemediums Fides bedienen. Das ist der Fall, wenn er es zurechenbar und aktiv in funktionellem Zusammenhang mit der von ihm ausgeübten wirtschaftlichen Tätigkeit einsetzt, wobei er potenziell die Möglichkeit haben muss, den Einsatz und die Ausgestaltung des Dienstes zu kontrollieren.[91] Dabei wird sowohl der Einsatz eigener wie auch fremder Dienste erfasst.[92] Besonderheiten in Bezug auf die Anwendbarkeit können sich im Zusammenhang mit Unternehmern als Plattformbetreibern ergeben, auf denen Verbraucher miteinander Verträge schließen.[93] Diese Konstellation ist im Fall von Fides jedoch nicht einschlägig, da dessen Einsatz den konkreten Vertragsschluss betrifft und nicht eine Vermittlungsleistung auf einer Plattform darstellt.

Das Bedienen müsste ferner zum Zweck des Abschlusses eines Vertrages erfolgen, was der Fall ist, wenn der Dienst zur Übermittlung der zum Vertragsschluss führenden

---

[90] Vgl. für die Kategorisierung der Blockchain als Telemedium *Kloth*, VuR 2022, 214, 216; Braegelmann/Kaulartz, Rechtshandbuch Smart Contracts, 138.
[91] *Wendehorst* in: MK-BGB, § 312i Rn. 29.
[92] *Wendehorst* in: MK-BGB, § 312i Rn. 29.
[93] *Wendehorst* in: MK-BGB, § 312i Rn. 36 ff.

Willenserklärungen genutzt wird.[94] Die Erbringung der Dienstleistung selbst über das Telemedium ist hingegen nicht erforderlich.[95]

Die für im elektronischen Geschäftsverkehr geschlossenen Verträge geltenden Pflichten nach §§ 312i Abs. 1 S. 1 Nr. 1 -3, 312j Abs. 1 – 4 BGB sind nach §§ 312i Abs. 2 S. 1, 312j Abs. 5 S. 1 BGB nicht anwendbar, wenn der Vertrag ausschließlich durch individuelle Kommunikation zustande kommt. Die Pflichten nach § 312 Abs. 1 S. 1 Nr. 4 BGB sowie ggf. nach § 312j Abs. 1 BGB bleiben hingegen anwendbar. In den Fällen individueller Kommunikation fehlt es an den spezifischen Besonderheiten des Onlineeinkaufs.[96] Als individuelle Kommunikation wird der Kontakt per Mail oder SMS verstanden, d.h. Situationen bei dem der Kunde und der Unternehmer den Vertrag in bilateraler und spezifisch subjektiver Weise miteinander schließen und nicht in einer an eine Vielzahl nicht individualisierter Personen gerichteter Weise, sodass kaum Unterschiede zu einem Vertragsschluss per Brief existieren.[97] Eine solche individuelle Kommunikation ist im Rahmen von Fides denkbar, sodass die genannten Pflichten hier entfallen können. Das setzt jedoch die Ausschließlichkeit individueller Kommunikation voraus, sodass der individuelle Kommunikationsweg auch nicht verlassen werden und zum Beispiel für vertragsrelevante Informationen auf eine Homepage verlinkt werden darf.[98] Dies wird jedoch regelmäßig, z.B. in Bezug auf in den Vertrag einzubeziehende AGB, der Fall sein.

Die Einordnung als Vertrag im elektronischen Geschäftsverkehr hängt somit erneut vom Einzelfall des Einsatzes von Fides ab. Für die aus der Typisierung erwachsenden Rechtsfolgen wird auf die Ausführungen oben [99] verwiesen. Auch hier stehen der Möglichkeit zur Erfüllung der Informations- und Hinweispflichten nach §§ 312i ff. BGB im Rahmen des Vertragsschlusses mittels Fides jedoch keine Bedenken entgegen.

---

[94] *Wendehorst* in: MK-BGB, § 312i, Rn. 32; *Schulte-Nölke* in: Schulze, § 312i Rn. 4; *Maume* in: BeckOK BGB, § 312i Rn. 16.
[95] *Schulte-Nölke* in: Schulze, § 312i Rn. 4; *Maume* in: BeckOK BGB, § 312i Rn. 18.
[96] *Grüneberg* in: Grüneberg, § 312i Rn. 9; *Maume* in: BeckOK BGB, § 312i Rn. 20; Raue, MMR 2012, 438, 440.
[97] *Schulte-Nölke* in: Schulze, § 312i Rn. 5; *Maume* in: BeckOK BGB, § 312i Rn. 20; *Raue*, MMR 2012, 438, 440. Enger zieht den Anwendungsbereich *Wendehorst* in: MK-BGB, § 312i Rn. 52, der nicht nur technisch-formal, vorgehen, sondern in einer zweistufigen Prüfung durch eine inhaltlich-materielle Prüfung vergleichbare Gefährdungslagen durch vom Unternehmer standardisierte und damit gelenkte Kommunikation ausschließen will.
[98] BT-Drs. 17/7745, S.12; *Grüneberg* in: Grüneberg, § 312i Rn. 9.
[99] B. I. 1. d).

cc) Pflichten als Betreiber eines Onlinemarktplatzes

Keine Auswirkungen auf die Verwendung von Fides haben hingegen die Regelungen des § 312l BGB, der für Betreiber von Online-Marktplätzen besondere Informationspflichten vorsieht. Ein Online-Marktplatz ist gemäß § 312l Abs. 3 BGB ein Dienst, der es Verbrauchern ermöglicht, durch die Verwendung von Software, die vom Unternehmer oder im Namen des Unternehmers betrieben wird, einschließlich einer Webseite, eines Teils einer Webseite oder einer Anwendung, Fernabsatzverträge mit anderen Unternehmern oder Verbrauchern abzuschließen. Entscheidend ist insoweit die Verwendung von Software und das Auftreten als Intermediär in Form der Ermöglichung eines Vertragsschlusses mit anderen Personen.[100]

Auch wenn einer der Hauptanwendungsfälle von Fides die Einbindung in andere Plattformen darstellt, um dort den Abschluss und die Abwicklung von Verträgen zu ermöglichen, sind die Clients von Fides selbst keine Intermediäre. Die Verwendung von Fides erfolgt, um selbst als Parteien auf diese Weise Verträge zu schließen und abzuwickeln, nicht aber um eine Vermittlung von Verträgen zwischen Dritten zu ermöglichen. Fides ist dabei das Medium des Vertragsschlusses und vermittelt ihn nicht im Sinne einer Angebots- und Begegnungsplattform.

e) Auswirkungen rechtshemmender Einreden sowie von § 242 BGB und des HGB

Wie bereits oben[101] ausgeführt, sind keine rechtshemmenden Einreden oder Fallgruppen des § 242 BGB zu erkennen, bei denen der Einsatz von Fides Auswirkungen auf die Möglichkeit der Herleitung von Ansprüchen aus einem Vertrag haben könnte. Auch Besonderheiten des Handelsrechts lassen keine mit der Verwendung von Fides im Zusammenhang stehenden Besonderheiten erkennen, da die handelsrechtlichen Besonderheiten beim Vertragsschluss sich nicht spezifisch beim Einsatz von Fides auswirken.

f) Zwischenergebnis

Vor dem Hintergrund der durchgeführten Analyse können über Fides auf den Abschluss eines Vertrages gerichtete Willenserklärungen wirksam ausgetauscht werden. Dabei stellt das Publizieren eines Contracts regelmäßig die Abgabe eines Angebots dar, das in

---

[100] *Wendehorst* in: MK-BGB, § 312l Rn. 5; *Schulte-Nölke* in: Schulze, § 312l Rn. 1.
[101] B. I. 1. e).

der Folge von dem anderen Client angenommen werden kann. Die Einbeziehung von AGB in einen über Fides geschlossenen Vertrag ist dabei möglich. Mittels Fides geschlossene Verträge können die Textform nach § 126b BGB erfüllen und als Fernabsatzverträge und Verträge im elektronischen Geschäftsverkehr zu klassifiziere sein. Die Verwendung von Fides allein führt hingegen nicht zur Anwendbarkeit der Regeln über Online-Marktplätze.

3. Ergebnis

Die durchgeführte Untersuchung hat gezeigt, dass ein wirksamer Vertragsschluss unter Einsatz von Fides erfolgen kann. Die Antwort auf die erste Studienfrage des ersten Arbeitspakts lautet daher, dass unter Beachtung der Umstände des jeweiligen Einzelfalls die Möglichkeit besteht mithilfe von Fides wirksame Verträge schließen zu können.

II. Einordnung in den Stand der Forschung

Im Rahmen der zweiten Studienfrage des Arbeitspakets erfolgt eine Einordnung des Systems Fides in den Stand der Forschung und der dort zivilrechtlich vertretenen Ansichten zum Vertragsschluss. Dabei wird ein Vergleich des Abschlusses von Smart Contracts über Fides mit der Eingehung eines Vertrages mittels blockchainbasierter Systeme, wie z.B. Ethereum, vorgenommen.

1. Stand der Forschung

Zum Themenbereich Smart Contracts ist inzwischen äußerst umfangreiche Fachliteratur in Form von Fachbeiträgen in Zeitschriften und Sammelbänden erschienen. Das Thema ist auch Gegenstand der Kommentarliteratur und von Monografien[102]. In der Folge wird ein Überblick über ausgewählte, zu dem Thema erschienene Beiträge und deren groben Inhalte gegeben. Hierbei erfolgt ein Schwerpunkt auf Beiträge, die das Thema aus zivilrechtlicher Sicht betrachten.

In seinem Beitrag nimmt Heckelmann[103] eine allgemeine Einführung zur Nutzbarkeit mit Schwerpunkt auf Treuhandkonstellationen für Smart Contracts vor, deren Funktionsweise auf einer Blockchainarchitektur basiert. Hierbei führt er zivilrechtliche Erwägungen zum Vertragsschluss durch und betrachtet, welche Folgen technische Besonderheiten im Blockchainkontext für einen Vertrag zum Beispiel im Zusammenhang

[102] Vgl. nur Timmermann, Legal Tech-Anwendungen; Fries/Paal, Smart Contracts; Wilkens/Falk, Smart Contracts; Hartung/Bues/Halbleib, Legal Tech; Braegelmann/Kaulartz, Rechtshandbuch Smart Contracts.
[103] *Heckelmann*, NJW 2018, 504.

mit dem Vertragsschluss, der Vertragssprache, der Form, Unwirksamkeitsgründen, AGB-Kontrolle, Vertragstyp, Vertragsabwicklung, Leistungsstörung dem anwendbaren Recht und Smart Judges haben können.

Auch Kipker et al.[104] nehmen zunächst eine allgemeine Einführung zur Nutzbarkeit von Smart Contracts, die auf einer Blockchainarchitektur basieren, und deren Funktionsweise vor und ordnen sie in die Vertragssystematik des BGB ein. In der Folge betrachten sie Anwendungsbeispiele. Dabei werden Schwierigkeiten durch nicht darstellbare Sachverhaltsparameter aufgezeigt. Sie beschäftigen sich in der Folge mit dem Vertragsschluss, der AGB-Kontrolle und dem Problem der Leistungsstörung.

Kaulartz und Heckmann[105] kommen in ihrem Beitrag hingegen nach einer allgemeinen Einführung und Überlegungen zur Definition von Smart Contracts zu dem Ergebnis, dass es sich bei Smart Contracts nicht um Verträge im Rechtssinn handelt.[106] Sie nehmen eine technische Einführung mit Codebeispiele vor und betrachten anschließend für Smart Contracts auf der Basis von Blockchain charakteristische zivilrechtliche Fragen wie Rechtssicherheit, Transparenz, technische Limitierung auf digitale Leistungen, Vertragssprache, Problematiken bei AGB-Nutzung, Anfechtbarkeit wegen Unkenntnis der Programmiersprache, Lücke zwischen dem Programmcode des Smart Contracts und dem Rechtsgeschäft, Umgang mit Programmierfehlern, mangelnde Durchsetzbarkeit rechtlicher Mittel und fehlende Standardisierung.

Kloth [107] befasst sich mit Einsatzmöglichkeiten von Smart Contracts aus verbraucherrechtlicher Sicht. Neben allgemeinen Ausführungen zur technischen Funktionsweise von Blockchain und Smart Contracts, stellt er die Frage, ob ein Smart Contract einen Vertrag nach allgemeinen Regeln darstellt oder nur eine Art „Warenautomat“ verkörpert. Dies wird anhand unterschiedlicher Vertragstypen diskutiert. Im Weiteren untersucht er, wie ein Widerruf, und eine Umsetzung der „Button-Lösung“ (§ 312j Abs. 3 BGB) bei ausschließlicher Nutzung von Blockchain basierten Smart Contracts, möglich ist.

---

[104] *Kipker/Birreck/Niewöhner/Schnorr*, MMR 2020, 509.
[105] *Heckmann*, CR 2016, 618.
[106] So auch: *Paulus/Matzke*, ZfPW 2018, 431; *Timmermann*, BRJ 2021, 7.
[107] *Kloth*, VuR 2022, 214.

Legner[108] befasst sich mit der automatisierten Abwicklung von Verbraucherverträgen. Im Rahmen der Auseinandersetzung mit dem Begriff des Smart Consumer Contracts erfolgt dabei eine Auseinandersetzung mit den technischen Grundlagen und der Frage des Verhältnisses von Smart Contracts zu Verträgen im Rechtssinn. Zudem wird die Verbraucherstellung im Rahmen der Smart Consumer Contracts thematisiert. Hierfür wird der Schutzzweck des Verbraucherrechts aufgezeigt und untersucht, wie die Verwendung von Smart Consumer Contracts das Verhältnis zwischen Unternehmer und Verbraucher modifiziert. Gegenstand der Betrachtung sind Risiken durch einen Verstoß gegen die Klauselverbote aus § 309 Nr. 2, 8a und 12 BGB, sowie aufgrund inhaltlicher Widersprüche zwischen dem Programmcode des Smart Contract und der Rechtslage. Darüber hinaus kommt die Autorin auf die technischen Hindernisse bei der Ausübung von Verbraucherrechten zu sprechen und betrachtet insbesondere die Umwandlung des Schuldverhältnisses in ein Rückgewährschuldverhältnis. Daran anknüpfend werden aber auch Chancen für Verbraucher dargestellt, die sich insbesondere durch eine vereinfachte Rechtsdurchsetzung, Kostenersparnisse aufgrund automatisierter Rechtsdurchsetzung sowie eine partielle Rechtssicherheit ergäben. Auch etwaige Einsatzmöglichkeiten für Smart Consumer Contracts werden thematisiert.

Bertram[109] geht in ihrem Beitrag auf das Verständnis von Smart Contracts sowie die Möglichkeiten einer verknüpften Blockchainnutzung sowie Einsatzmöglichkeiten ein. Zudem behandelt sie vertragsrechtliche Probleme im Kontext von Smart Contracts mit Schwerpunkten bei Fragen zu Formerfordernissen, der Abgabe und dem Zugang von Willenserklärungen, Willensmängeln, Leistungsstörungen, Rückabwicklung und dem Umgang mit Einreden sowie der Auslegung einzelner Klauseln.

In seinen Beiträgen beschäftigt sich Wilhelm[110] damit, wie die Digitalisierung in den Bereichen Legal Tech und Fin-Tech den Einsatz von Smart Contracts befördert hat. Er widmet sich verschiedenen juristischen Fragen, den technischen Hintergründen und zeigt die aktuellen Einsatzgebiete von Smart Contracts auf. Der Autor thematisiert die Verschiebung der Prozesslast durch den Einsatz von Smart Contracts aufgrund der

[108] *Legner*, VuR 2021, 10.
[109] *Bertram*, MDR 2018, 1416.
[110] *Wilhelm*, WM 2020, 1807; *ders.*, WM 2020, 1849.

Durchsetzung von Ansprüchen und stellt Überlegungen zur Notwendigkeit einer ex-ante-Kontrolle von Smart Contracts vor. Er untersucht den konkreten Vertragsschluss sowie die AGB-rechtliche Bewertung solcher Verträge. Hierbei überträgt er die allgemeinen Regelungen zur Rechtsgeschäftslehre auf die Smart Contracts und diskutiert unter anderem Zurechnungsfragen im Kontext von Willenserklärungen. Überdies fließen Einzelaspekte zur Anwendung des AGB-Rechts in die Überlegungen ebenso ein, wie eine Erörterung von Sonderproblemen hinsichtlich des Insolvenz- und Gesellschaftsrechts.

Jacobs und Lange-Hausstein[111] betrachten die technischen Hintergründe der Blockchain-Technologie sowie der damit verbundenen Idee von Smart Contracts. In diesem Zusammenhang erörtern sie verschiedene Blockchainmodelle und die allen Modellen immanente Registerfunktion der Blockchain-Technologie. Sie betrachten typische Anwendungsfälle von Smart Contracts, wobei sie für den Abschluss von Smart-Contract-Geschäften neben einer wertungsfreien Definition von Leistungsgegenstand und Leistungsmodalitäten auch die Möglichkeit zur digitalen Überprüfung der Voraussetzungen und zur digitalen Setzung der Rechtsfolgen für erforderlich halten. Sie weisen ferner auf die aufsichtsrechtlichen Bedingungen hin, die beim Einsatz der Blockchain-Technologie zu berücksichtigen seien.

Aufderheide definiert in ihren Beiträgen[112] wesentliche Begrifflichkeiten und erläutert technische Grundlagen, unter anderem auch in Bezug auf die Funktion einer Blockchain. Anschließend untersucht sie Anwendungsfälle sowie die wirtschaftliche Dimension der Thematik. Sie geht auf die Frage ein, ob ein Smart Contract einen Vertrag darstellen kann, was in der Literatur teilweise abgelehnt wird, da Smart Contracts in einem Programmiercode verfasst würden, welcher nicht für jeden verständlich sei. Sie thematisiert die Grundsätze der Irrtumsanfechtung und weist hinsichtlich einer AGB-Kontrolle darauf hin, dass in der Regel nicht derselbe Code von demselben Verwender mehrfach verwendet werde. Zugleich könne das Verwenden einer Programmiersprache aber als überraschend im Sinne des § 305c BGB, betrachtet werden. Sie befasst sich zudem mit den Problemen anonymer Vertragsparteien und der Verknüpfung von Smart

[111] *Jacobs/Lange-Hausstein*, ITRB 2017, 10.
[112] *Aufderheide*, WM 2021, 2273; *dies.*, WM 2021, 2313.

Contracts mit „KI“. Ferner thematisiert sie Alternativen zur gerichtlichen Durchsetzung sowie Fragen des Besitzschutzes.

Über die hier vorgestellten Beiträge hinaus existieren weitere Artikel, die sich mit allgemeinen zivilrechtlichen oder grundsätzlichen rechtsdogmatischen Fragen im Zusammenhang mit Smart Contracts auseinandersetzen.[113] Zudem widmen sich viele Beiträge besonderen Rechtsfragen oder Einsatzfeldern im Zusammenhang mit Smart Contracts und betrachten deren Auswirkungen auf spezielle Rechtsgebiete [114], insbesondere auch dem Datenschutzrecht[115].

2. Vertragsschluss bei blockchainbasierten Smart Contracts

In der Literatur ist bereits umstritten, ob ein blockchainbasierter Smart Contract überhaupt einen Vertrag im Rechtssinn darstellen kann. Die Vertreter der ablehnenden Ansicht führen aus, dass eine Transaktion, die in das Blockchain-Netzwerk geschickt werde, eine konkludente Willenserklärung darstellen könne, der Programmcode an sich jedoch ungeeignet sei, Willenserklärungen inhaltlich auszudrücken.[116] Der Programmcode sei für die meisten Nutzer eine unverständliche Blackbox[117], der ihnen nicht ohne weiteres verständlich sei oder sein könne, sodass im Code nicht ohne Weiteres eine Willensäußerung des Rechtssubjekts auf die Herbeiführung einer Rechtsfolge zu sehen sei, sodass es am Erklärungswillen des Nutzers fehle.[118] Der Smart Contract führe vielmehr wie ein Warenautomaten aus, was aus den Umständen und nicht aus der Mechanik heraus vereinbart worden sei.[119] Anders könne dies zu bewerten sein, wenn die Programmiersprache als Vertragssprache zwischen den Parteien vereinbart sei.[120]

Eine vermittelnde Ansicht geht hingegen davon aus, dass Smart Contracts Verträge im Rechtssinn sein können.[121] Mit dieser Aussage stellen sie jedoch weniger auf die generelle

---

[113] Vgl. nur: *Söbbing*, ITRB 2018, 43; *Bernzen*, ZKM 2021, 219; *Linardatos*, K&R 2018, 85; *Fries*, REL 2018, 46; *Blocher*, AnwBl 2016, 612; *Börding/Jülicher/Röttgen/v. Schönfeld*, CR 2017, 134.
[114] Vgl. nur: *Eschenbruch/Gerstberger*, NZBau 2018, 3; *Schnell/Schwaab*, BB 2021, 1091; *Rupa*, MMR 2021, 371; *Tavakoli*, ZRP 2020, 46; *Schnurr*, ZVglWiss 2019, 257; *Treiber*, REL 2018, 10; *Linardatos*, ZIP 2022, 153; *Lehmann/Krysa*, BRJ 2019, 90; *Fries*, AnwBl 2018, 86; *Aufderheide*, WM 2022, 264.
[115] Vgl. nur: *Lupu*, CR 2019, 631; *Potel/Hessel,* jM 2020, 354; *Schawe*, MMR 2019, 218; *Klar/Wegmann/Galandi*, BB 2022, 2691.
[116] *Kaulartz/Heckmann*, CR 2016, 618, 623; *Legner*, VuR 2021, 10, 12.
[117] *Kaulartz/Heckmann*, CR 2016, 618, 623.
[118] *Legner*, VuR 2021, 10, 12; *Paulus/Matzke*, ZfPW 2018, 431, 459.
[119] *Kaulartz/Heckmann*, CR 2016, 618, 623.
[120] *Legner*, VuR 2021, 10, 12; *Kaulartz/Heckmann*, CR 2016, 618, 621.
[121] *Schrey/Thalhofer*, NJW 2017, 1431; *Hoffmann/Skwarek*, InfSpek 2019, 197.

rechtliche Möglichkeit eines Austauschs von Willenserklärungen zwischen Vertragsparteien ab, sondern heben eher die begrifflichen Unterschiede zwischen einem Vertrag im Rechtssinn und einem Smart Contract hervor, der ein Stück Software zur Kontrolle rechtlich relevanter Aktivitäten darstellt und nicht immer ein rechtlicher Vertrag sein muss.[122] Dies verdeutlicht ein generelles Problem in der Debatte um den Rechtscharakter von Smart Contracts. Deren widerstreitende Bewertung in der Literatur sind das Ergebnis aus einer uneinheitlichen Definition des Begriffs und daraus resultierenden unterschiedlichen Vorstellungen darüber, was als Smart Contract zu verstehen ist[123].[124]

Nach einer dritten Ansicht können Smart Contracts Verträge im Rechtssinne darstellen,[125] sodass einerseits Smart Contracts existieren, die einen in der realen Welt geschlossen Vertrag lediglich wiedergeben und dessen Ausführung vornehmen, andererseits Smart Contracts aber auch ein Mittel zum Vertragsschluss sein können.[126] Als Hauptargument wird hier angeführt, dass es keinen Grund gebe, warum ein Smart Contract keine Willenserklärung ausdrücken könne, sogar mit einem Bierdeckel oder einer Tätowierung ein rechtlicher Wille kundgetan werden könne.[127] Die hierfür erforderliche automatisiert erzeugte und übermittelte Willenserklärung eines automatisierten Systems müsse dafür auf konditional und vorhersehbaren zu einem früheren Zeitpunkt gegebenen Anweisungen beruhen.[128] Dies sei gerade ein Charakteristikum von Smart Contracts.[129] Mit einem gestreckten, arbeitsteiligen Erklärprozess speise der Kunde die von ihm gewünschten Parameter als für die Willenserklärung erforderliche Grundentscheidungen in das System ein, auf deren Grundlage die Erklärung selbst dann algorithmisch erzeugt werde.[130] Während die Abgabe der Willenserklärung durch das Signieren der eigenen Erklärung mit dem privaten Schlüssel erfolgt,[131] kann für den Zugang der Erklärung auf

---

[122] *Schrey/Thalhofer*, NJW 2017, 1431.
[123] Vgl. nur Froitzheim, K&R 2020, 122, 125; *Riehm* in: Fries/Paal, Smart Contracts, 99.
[124] *Aufderheide*, WM 2021, 2313, 2318.
[125] Vgl. *Bertram*, MDR 2018, 1416, 1417; *Heckelmann*, NJW 2018, 504, 505; *Kloth*, VuR 2022, 214; *Potel/Hessel*, jM2020, 354, 356; *Linardatos*, K&R 2018, 85, 88f.; *Möslein*, ZHR 2019, 254, 270 ff.
[126] *Kloth*, VuR 2022, 214, 215.
[127] *Heckelmann*, NJW 2018, 504, 505.
[128] *Kloth*, VuR 2022, 214, 215; *Kumkar*, K&R 2020, 801, 803.
[129] *Kloth*, VuR 2022, 214, 215; *Paulus*, JuS 2020, 107; *Möslein*, ZHR 2019, 254, 271.
[130] *Möslein*, ZHR 2019, 254, 271; *Linardatos*, K&R 2018, 85, 89; *Paulus/Matzke*, ZfPW 2018, 431, 441, 446; *Paulus*, JuS 2019, 960, 961, 963; *Wilhelm*, WM 2020, 1849.
[131] *Heckelmann*, NJW 2018, 504, 505 f.; *Bertram*, MDR 2018, 1416, 1419 unter Verwerfung der Idee des Einstellens im Mempool als relevanten Zeitpunkt wie von *Kaulartz/Heckmann*, CR 2016, 618, 621 vertreten wird.

das Anhängen des die Erklärung enthaltenen Blocks, die Bildung von mindestens sechs Nachfolgeblöcken oder eine schwebende Unwirksamkeit der Erklärung bis zur Klarheit über das Bestehen eines Forks abgestellt werden.[132] Da das Abwarten bis zur Klarheit über das Bestehen eines Fork rechtlich keine Vorteile gegenüber dem Abstellen auf das Anhängen bietet und zeitkritische Anwendungsszenarien erschwert, erscheint das Abstellen auf das Anhängen des neuen Blocks an die Blockchain für den Zugang als sinnvoll.[133]

Die Frage, ob es sich bei einer Willenserklärung um ein Angebot, eine invitatio ad offerendum oder eine Annahme handelt, bestimmt sich auch in diesem Zusammenhang nach den oben dargestellten[134] allgemeinen Regeln der Rechtsgeschäftslehre.[135]

3. Vergleichende Einordnung von Fides

Die Funktionsweise von Fides unterscheidet sich wesentlich von blockchainbasierten Smart Contract Systemen. Das hat rechtliche Auswirkungen und führt zu unterschiedlichen Bewertungen, insbesondere in Bezug auf die Möglichkeit und die Art, Verträge zu schließen. Unter Zugrundlegung der vorangestellten Literaturanalyse wirkt sich hierbei zunächst aus, dass im Rahmen von Fides natürliche und keine Programmiersprache verwendet wird. Die von der oben dargestellten[136], in der Literatur geäußerten Zweifel, ob ein Rechtssubjekt mit Erklärungswillen handelt und somit eine Willenserklärung abgibt, wenn es sich eines blockchainbasierten Smart Contracts bedient, sind auf Fides somit nicht übertragbar. Ferner weist die vorliegend untersuchte Funktionsweise keine Automation bei der Erstellung und der Publikation eines Contracts und somit der Abgabe einer Willenserklärung auf. Auch die diesbezüglich auftretenden Fragen im Kontext blockchainbasierter Smart Contracts stellen sich im Zusammenhang mit Fides daher nicht. Eine Einbindung von Fides in automatisierte Systeme erscheint jedoch nicht ausgeschlossen, da auch hier eine menschliche Auswahlentscheidung getroffen wird, die in einem gestreckten, arbeitsteiligen Erklärprozess durch eine Software umgesetzt werden könnte. Insoweit erscheinen die von der oben dargestellten,

---

[132] *Heckelmann*, NJW 2018, 504, 505 f.; *Wilhelm*, WM 2020, 1849; *Bertram*, MDR 2018, 1416, 1419; *Schnurr*, ZVglWiss 2019, 157, 167f.
[133] *Heckelmann*, NJW 2018, 504, 506.
[134] B. I. 1. a).
[135] *Wilhelm*, WM 2020, 1849, 1850; *Möslein*, ZHR 2019, 254, 274 ff.; *Paulus*, JuS 2019, 960, 963.
[136] B. II. 2.

befürwortenden Ansicht[137], vorgebrachten Argumente auf Fides übertragbar. Eine rechtssichere Bewertung hängt jedoch auch hier von den Umständen des Einzelfalls ab. Vorliegend wird zudem keine Aussage über den Einsatz von Künstlicher Intelligenz oder deren Verbindung mit Fides getroffen. Die sich hierbei stellenden rechtlichen Probleme sind thematisch so breit gefächert und inhaltlich divers,[138] dass selbst grundlegende rechtliche Aussagen nur anhand eines konkreten Szenarios getroffen werden können.

In Bezug auf die Einbindung von oder die Charakterisierung eines Smart Contracts als AGB ergeben sich keine Unterschiede zwischen Fides und blockchainbasierten Smart Contracts. So besteht grundsätzlich Einigkeit über die Anwendbarkeit der §§ 305 ff. BGB auf Smart Contracts und die Möglichkeit, dass diese einer Inhaltskontrolle unterworfen sein können.[139]

Die vertretene Ansicht, dass selbst im Fall von Massengeschäften Smart Contracts nur selten als AGB zu qualifizieren sein werden, da das Haupteinsatzgebiet im Peer-to-Peer Bereich und einer einmaligen Verwendung liege,[140] erscheint nicht zwangsläufig und zeigt, dass eine Bewertung des konkreten Einzelfalls zu erfolgen hat, zumal gemäß § 310 Abs. 3 Nr. 2 BGB auch Fälle einmaliger Verwendung von AGB zur Anwendung der §§ 305 ff. BGB führen können. Die teilweise postulierte Unanwendbarkeit von § 305 Abs. 2 BGB[141] kann zudem nicht nachvollzogen werden und wird auch in dem in Bezug genommenen Urteil des BGH[142] so nicht vertreten, sondern stellt vielmehr eine Besonderheit des dort entschiedenen Einzelfalls dar.[143]
Der in der Literatur ebenfalls geführt Streit darüber, ob Smart Contracts der Textform nach § 126b BGB genügen können,[144] stellt sich für Fides so nicht. Anders als bei blockchainbasierten Smart Contracts wird bei Fides natürliche Sprache verwendet,

---

[137] Vgl. B. II. 2., insbesondere Fn. 133.
[138] Vgl. nur *Wilhelm*, WM 2020, 1849, 1851 f.; *Timmermann*, BRJ 2021, 7; *Aufderheide*, WM 2021, 2273.
[139] *Heckelmann*, NJW 2018, 504, 507; *Aufderheide*, WM 2313, 2314 f.; *Legner*, VuR 2021, 10, 13; *Kaulartz/Heckmann*, CR 2016, 618, 622.
[140] *Heckelmann*, NJW 2018, 504, 507.
[141] *Kaulartz/Heckmann*, CR 2016, 618, 622.
[142] BGH, NJW 1995, 190.
[143] Vgl. BGH, NJW 1995, dort 190, II 1. a).
[144] Grundsätzlich bejahend *Wilhelm*, WM 2020, 1849, 1851, *Heckelmann*, NJW 2018, 504, 507; zweifelnd bis ablehnend *Aufderheide*, MW 2021, 2313, 2317; *Bertram*, MDR 2018, 1416, 1418 f.

sodass es sich in jedem Fall um eine lesbare Erklärung handelt, an der es im Zusammenhang mit programmiersprachenbasierten Contracts fehlen soll.[145]

In Bezug auf die Klassifizierung als Fernabsatzvertrag und Vertrag im elektronischen Geschäftsverkehr sowie den daraus resultierenden Rechtsfolgen in Form von Informationspflichten, Widerrufsrechten oder auch der Anwendung der „Button-Lösung" nach §312j Abs. 3 BGB ergeben sich keine Unterschiede zu blockchainbasierten Smart Contracts.[146]

4. Ergebnis

Aufgrund der grundlegend unterschiedlichen Funktionsweise von Fides im Vergleich zum Einsatz blockchainbasierter Smart Contracts ergeben sich beim Einsatz des Systems aus rechtlicher Sicht an einigen Stellen Unterschiede. Aufgrund der Unterschiede werden jedoch in der Literatur bestehende Zweifels- und Streitfragen eher ausgeräumt, was die Einsatzfähigkeit von Fides rechtssicherer gestaltet. So können aufgrund der Verwendung natürlicher Sprache und dem fehlenden Einsatz von Automation bestehende Bedenken in Bezug auf das tatsächliche Vorliegen von Willenserklärungen gegen den Einsatz von Fides nicht vorgebracht werden. Dasselbe gilt in Bezug auf die Erfüllung der Anforderungen an die Textform gemäß § 126b BGB. Keine Unterschiede ergeben sich hingegen in den Themenkomplexen des AGB- sowie des Verbraucherschutzrechts.

III. Einsatz von LoRaWAN

Gegenstand der dritten Studienfrage des ersten Arbeitspakets ist die zivilrechtliche Bewertung des Einsatzes der Middleware LoRaWAN, die als zentraler Dienst beim Einsatz von Fides verwendet wird, sofern die Software nicht direkt ausgeführt werden kann. Hierbei wird betrachtet, ob sich die zuvor getroffenen zivilrechtlichen Bewertungen durch den Einsatz der Middleware ändern, sofern die Verträge im Namen der Clients (durch die Middleware) geschlossen werden.

1. Praktische Unterschiede durch die Verwendung von LoRaWAN

Zur Beantwortung der Frage, ob sich eine geänderte rechtliche Bewertung der Möglichkeit oder Art des Vertragsschlusses mittels Fides beim Einsatz der Middleware

[145] *Aufderheide*, MW 2021, 2313, 2317; *Bertram*, MDR 2018, 1416, 1418.
[146] Vgl. *Kloth*, VuR 2022, 214, 216 ff.

LoRaWAN ergibt, muss zunächst untersucht werden, welche relevanten Änderungen sich durch den Einsatz ergeben. Hierbei sind verschiedene Punkte von Bedeutung.

Zunächst ist die Hardware, auf der ein Contract erstellt wird, nicht mehr selbst mit dem Internet verbunden und nimmt somit auch keine direkte Übermittlung an den Full Node vor. Das Endgerät ist vielmehr LoRaWAN-fähig und übermittelt die Daten per Funk an ein Netzwerk, über das sie an eine Middleware gesendet werden. Hier werden die Daten in ein Fides-lesbares Format umgewandelt und ins Fidesnetzwerk übermittelt.

Ferner sind der Umfang der Daten und die Häufigkeit ihres Sendens und Empfangens deutlich reduziert. Es können somit keine eigenen Templates erstellt und übertragen werden, sodass auf bereits existierende Templates zurückgegriffen werden muss. Contracts werden zudem nicht vollständig, sondern es werden nur die für einen Contract relevanten Daten versendet. Die Middleware übernimmt dabei das Platzieren der Informationen an der erforderlichen Stelle im vereinheitlichten Contract.

Zuletzt kann der Contract zwar lokal jederzeit aktualisiert werden, die Anzahl der Verbindungen zur Publikation oder zum Empfang von Aktualisierungen ist jedoch deutlich begrenzt, was zu einem zeitlichen Auseinanderfallen der Aktualisierungen eines Contracts auf beiden Ebenen und damit der jeweiligen Zustände des Contracts dort führen kann, wobei im Falle eines Konflikts der lokale dem im Full Node gespeicherten Zustand vorgeht.

2. Rechtliche Bewertung des Einsatzes von LoRaWAN

Die dargestellten Unterschiede zwischen einer Nutzung von Fides ohne sowie unter Verwendung der Middleware LoRaWAN wirken nicht sich auf die grundsätzliche Möglichkeit aus, mittels Fides Verträge schließen zu können. Dennoch sind einige zivilrechtliche Überlegungen zu beachten.

Die initiale Übertragung der Daten vom Endgerät in das Netzwerk per Funk beim Einsatz von LoRaWAN betrifft lediglich die Art des Übertragungsweges. Dies hat grundsätzlich keine Auswirkungen auf die zivilrechtliche Bewertung des Vertragsschlusses. Relevant ist lediglich, dass die Willenserklärung auf dem gewählten Weg abgegeben werden und dem Empfänger verlässlich zugehen kann. Dies zeigt sich auch an der Vielzahl der denkbaren

Möglichkeit eine Willenserklärung zu übermitteln, wie z.B. im persönlichen Gespräch, per Telefon, Brief, Email, Webformular oder Applikation. Beachtlich ist der Einsatz einer Funkverbindung anstelle der direkten Übertragung in das Fides-Netzwerk nur, sofern es bei der Übertragung zu Fehlern und zur Notwendigkeit der Klärung der Frage von Zurechnungen käme.

Der Einsatz der Middleware selbst erscheint aus zivilrechtlicher Perspektive ebenfalls möglich. Die grundsätzliche Funktionsweise von Fides auf der Bedienebene beim Client wird durch den Einsatz von LoRaWAN nicht berührt. Es handelt sich somit um eine Willenserklärung, bei der jedenfalls mindestens die subjektive Seite von einem Menschen herrührt. [147] Vor diesem Hintergrund bleiben die hierzu getroffenen rechtlichen Feststellungen zur Möglichkeit eines Vertragsschlusses und dessen Voraussetzungen weiter anwendbar. [148] Die Middleware nimmt im betrachteten Anwendungsbeispiel vielmehr drei Funktionen wahr: Zunächst ist sie das Medium der Übermittlung. Über das der Middleware zuzurechnende Netzwerk werden die Daten transportiert, die zwischen den Clients ausgetauscht werden sollen. In diesem Zusammenhang wandelt LoRaWAN die transportierten Daten zudem in ein Format um, das Fides-lesbar ist und platziert abschließend die Informationen an der richtigen Stelle im Contract. Aus rechtlicher Sicht stellt sich die Frage, wem die transportierten, umgewandelten und platzierten Daten bzw. die damit verbundene Willenserklärung [149] zuzurechnen sind. Hierbei kommen zwei mögliche Fallgestaltungen in Frage. Entweder stammen die Daten vom Client selbst und stellen seine Willenserklärung dar, die von der Middleware lediglich transportiert wird, oder es handelt sich bei den Daten um eine eigene Willenserklärung der Middleware, die sie im Namen des Clients abgibt. Abwegig ist hingegen die dritte Möglichkeit, dass die Middleware selbst mit den Daten eine eigene Willenserklärung für sich abzugeben beabsichtigt, da dies nicht in den technischen Prozessen angelegt und auch nicht im Interesse des Betreibers der Middleware ist.

Die dargestellte Abgrenzungssituation entspricht rechtlich der Unterscheidung zwischen Stellvertretung und Botenschaft. Ein Stellvertreter gibt eine eigene Willenserklärung in

[147] Vgl. hierzu B. II. 1. a).
[148] Vgl. B. II. 1. a).
[149] Vgl. B. II. 1. a).

fremdem Namen ab, während ein Bote nur eine fremde Willenserklärung übermittelt.[150] Der Prozess der Eingabe der erforderlichen Informationen in den Contract zur Erzeugung einer Willenserklärung unterscheidet sich beim Einsatz von LoRaWAN nicht von der Verwendung von Fides im Übrigen. Die Willenserklärung geht somit allein auf den Willen und das Handeln des Clients zurück, der sich Fides zur Erzeugung seiner Willenserklärung bedient. LoRaWAN übernimmt insoweit lediglich den Transport dieser Willenserklärung des Clients zu einem anderen Client in einem Umfeld, in dem wegen einer fehlenden Internetverbindung Fides an seine technische Funktionsgrenzen stößt. Eine eigene Willenserklärung, die dem Client zuzurechnen wäre, entsteht nicht, da durch LoRaWAN kein eigener Willensbildungsprozess vorgenommen wird. Es leitet lediglich die vom Client selbst erstellte Willenserklärung weiter. Dies stellt einen typischen Fall der Botenschaft dar, in dem ein Erklärungsbote wie bei Post- und Telefondiensten[151] oder auch Internet-Providern[152] eine Willenserklärung lediglich übermittelt.[153]

Eine andere Sichtweise ergibt sich auch nicht durch die Umwandlung der übermittelten Daten durch LoRaWAN in ein Fides-lesbares Format. Hierbei handelt es sich um einen rein technischen Vorgang, mit dem keine Abgabe einer eigenen Willenserklärung oder Änderung der vorhandenen Willenserklärung einhergeht. Die abgegebene Willenserklärung wird vielmehr inhaltlich identisch überführt. Dies stellt eine reine Übersetzungs- bzw. Überführungsleistung oder auch Formatänderung ohne Änderung des entäußerten Inhalts dar. Soweit man hieraus angesichts der rein technischen Funktion des Arbeitsschrittes überhaupt eine rechtlich relevante Änderungsleistung ableiten möchte, bietet sich der Vergleich zum ebenfalls rechtlich als Boten qualifizierten Dolmetscher an.[154]

Zuletzt ergibt sich auch keine Änderung der rechtlichen Bewertung aufgrund der Platzierung der übermittelten Daten im vereinheitlichten Contract durch die Middleware.

---

[150] *Schubert* in: MK-BGB, § 164 Rn. 80; *Schäfer* in: BeckOK-BGB, § 164 Rn. 11; *Mansel* in: Jauernig, § 164 Rn. 14; Brox, BGB AT, Rn. 518.
[151] *Wendtland* in: BeckOK-BGB, § 120 Rn. 2.1; *Ellenberger* in: Grüneberg, § 120 Rn. 2; *Mansel* in: Jauernig, § 120 Rn. 2; *Dörner* in: Schulze, § 120 Rn. 2.
[152] OLG Frankfurt, OLGR Frankfurt 2003, 88; *Wendtland* in: BeckOK-BGB, § 120 Rn. 2.1; *Armbrüster* in: MK-BGB, § 120 Rn. 4; Heun, CR 1994, 595, 596; Ultsch, NJW 1997, 3007, 3009; *Ellenberger* in: Grüneberg, § 120 Rn. 2; *Dörner* in: Schulze, § 120 Rn. 2.
[153] *Wendtland* in: BeckOK-BGB, § 120 Rn. 2; *Armbrüster* in: MK-BGB, § 120 Rn. 3; *Ellenberger* in: Grüneberg, § 120 Rn. 2; *Dörner* in: Schulze, § 120 Rn. 1.
[154] BGH, BB 1963, 204; *Ellenberger* in: Grüneberg, § 120 Rn. 2.

Auch mit diesem Schritt ist von Seiten der Middleware keine eigenständige Erklärung verbunden. Sie stellt vielmehr nur die Umsetzung der vom menschlichen Client vorgegebenen Angaben dar, indem die vom Client an bestimmten Stellen eines vereinheitlichten Contracts gemachten Angaben nach einer Übertragung an eben diese Stellen gesetzt werden. Auch hierbei agiert LoRaWAN somit lediglich als Bote.

Es stellt sich ebenso unproblematisch dar, dass im Zuge des Einsatzes von LoRaWAN nicht der gesamte Contract, sondern lediglich die für einen Contract relevanten Daten übermittelt werden. Da das Template, das einem Contract zugrundliegt, vereinheitlicht und somit für beide Seiten identisch ist, hat es auf die Wirksamkeit des Vertrages keine Auswirkungen, dass insoweit nur sich ändernde Parameter des Contracts übermittelt werden. Vielmehr müssen die übermittelten Daten beim empfangenden Client ankommen und dort an den richtigen Stellen eingesetzt werden können, sodass die Inhalte des gesendeten dem empfangenen Contract tatsächlich entsprechen.

Es ist insoweit auch unproblematisch, dass im Rahmen von LoRaWAN keine eigenen, sondern lediglich existierende Templates zur Erstellung eines Contracts verwendet werden können. Damit diese für den Abschluss eines wirksamen Vertrages herangezogen werden können, müssen sie jedoch die oben[155] für einen wirksamen Vertragsschluss angeführten Anforderungen erfüllen und Inhalte aufweisen. Insbesondere muss trotz der Übermittlung von nur beschränkten Vertragsdaten die Einbindung von AGB und die Belehrung über Widerrufsrechte sowie die Wahrnehmung von Informationspflichten gewährleistet bleiben. Dies scheint bei einer Einbindung in die den beiden Clients vorliegenden Templates jedoch möglich. Zu beachten ist jedoch, dass im Fall der Einbindung von Informationen über Verweise im Template auf andernorts abrufbare Informationen auch die Möglichkeit zu deren Wahrnehmung bestehen muss. Dies kann jedoch gerade beim Einsatz von LoRaWAN problematisch sein, das für Situationen ohne Zugang zum Internet konzipiert ist, sodass diese Zugangsmöglichkeiten zu den in Bezug genommenen Informationen somit oftmals nicht existieren.

[155] B. I. 1. a).

Angesichts der Verwendung von existierenden Templates im Zusammenhang mit LoRaWAN ist die Klassifizierung von deren Bestimmungen als AGB zudem sehr wahrscheinlich.

Zuletzt ist zu beachten, dass sich das Auseinanderfallen der Aktualisierungen eines Contracts auf dem verwendeten Endgerät der Clients und dem Full Node rechtlich auswirken kann. Für den Zeitpunkt sowohl der Abgabe als auch des Zugangs einer Willenserklärung kann es daher relevant sein, wann sie im Full Node veröffentlicht wurde, sodass nicht der Zeitpunkt der Änderung im eigenen Endgerät, sondern auf den der Up- und Downlinknachrichten abzustellen wäre. Hier muss beachtet werden, inwieweit die Verwendung der Middleware durch einen Client und die sich daraus möglicherweise ergebenden Verzögerungen für den anderen Client ersichtlich sind. Dies gilt umso mehr, da nur einer der Clients Fides unter Einsatz der Middleware verwendet.

3. Ergebnis

Vor dem Hintergrund der durchgeführten Betrachtung lässt sich festhalten, dass der Einsatz der Middleware LoRaWAN keine Auswirkungen auf die grundsätzliche Möglichkeit hat, Verträge mittels Fides zu schließen. Der Einsatz von Funk zur Datenübermittlung stellt dabei eine bloße Funktionsfrage des Übermittlungsweges dar. Auch ändert der Einsatz nichts an dem Charakter der Erklärung als vom Client stammende Willenserklärung. LoRaWAN berührt insoweit nicht die grundsätzliche Funktionsweise und Abgabe der Willenserklärung über Fides, sodass sie sich weiter als vom Client stammend darstellt. LoRaWAN kommt vielmehr die rechtliche Rolle eines Boten zu, der die Willenserklärung des Clients transportiert, übersetzt und an der vom Client vorgegeben Stelle im Contract platziert. Ebenso unproblematisch ist die Übermittlung von lediglich variablen Informationen, die für den konkreten Contract relevant sind. Hierbei ist jedoch darauf zu achten, dass eine wirksame Kenntnisnahme von Informationen wie AGB, Widerrufsrechten oder Pflichtinformationen weiter möglich sein muss und es durch die Verwendung existierender Templates wahrscheinlich ist, dass die dort enthaltenen Bestimmungen rechtlich selbst als AGB eingeordnet werden. Die asynchrone Aktualisierung von Contracts im Full Node und auf den Endgeräten der Clients kann zudem im Zusammenhang mit dem Zeitpunkt der Abgabe und des Zugangs von Willenserklärungen relevant werden.

IV. Zusammenfassung der zivilrechtlichen Ergebnisse

1. Möglichkeit eines wirksamen Vertragsschlusses mittels Fides

Die durchgeführte Untersuchung hat gezeigt, dass grundsätzlich die Möglichkeit besteht, Verträge mithilfe von Fides zu schließen. Die auf den Abschluss eines Vertrages gerichtete Willenserklärungen wirksam ausgetauscht werden. Dabei stellt das Publizieren eines Contracts regelmäßig die Abgabe eines Angebots dar, das in der Folge von dem anderen Client angenommen werden kann. Angesichts der hohen Variabilität des Einsatzes von Fides ist die konkrete Wirksamkeit des Vertragsschlusses von einer Einzelfallbetrachtung, insbesondere dem Inhalt des Contracts und seiner konkreten Gestaltung sowie dem im Einzelfall beabsichtigten Vertrag abhängig. Sofern die gesetzlichen Anforderungen beachtet werden, stellt dabei weder die Einbeziehung existierender AGB, noch die Möglichkeit, dass eine Bestimmung eines über Fides geschlossenen Vertrages selbst als AGB zu werten ist, ein rechtliches Problem für die Verwendung von Fides dar. Es ist mittels Fides zudem möglich, die Textform gemäß § 126b BGB zu wahren. Die Einhaltung anderer Formen ist jedoch nicht möglich. Mittels Fides geschlossene Verträge können zudem als Fernabsatzverträge oder als Vertäge im elektronischen Geschäftsverkehr zu klassifizieren sein. Fides stellt jedoch keinen Online-Marktplatz dar.

2. Einordnung von Fides in den Stand der Forschung

Aufgrund der grundlegend unterschiedlichen Funktionsweise von Fides im Vergleich zum Einsatz blockchainbasierter Smart Contracts ergeben sich beim Einsatz des Systems aus rechtlicher Sicht an einigen Stellen Unterschiede. Aufgrund der Unterschiede werden jedoch in der Literatur bestehende Zweifels- und Streitfragen eher ausgeräumt, was die Einsatzfähigkeit von Fides rechtssicherer gestaltet. So können aufgrund der Verwendung natürlicher Sprache und dem fehlenden Einsatz von Automation bestehende Bedenken in Bezug auf das tatsächliche Vorliegen von Willenserklärungen gegen den Einsatz von Fides nicht vorgebracht werden. Dasselbe gilt in Bezug auf die Erfüllung der Anforderungen an die Textform gemäß § 126b BGB. Keine Unterschiede ergeben sich hingegen in den Themenkomplexen des AGB- sowie des Verbraucherschutzrechts.

3. Rechtliche Bewertung des Einsatzes von Fides unter Verwendung von LoRaWAN

Der Einsatz der Middleware LoRaWAN hat keine Auswirkungen auf die grundsätzliche Möglichkeit, Verträge mittels Fides zu schließen. Die Verwendung einer Funkverbindung

zur Datenübermittlung stellt dabei eine bloße Funktionsfrage des Übermittlungsweges dar. Auch ändert die Nutzung der Middleware nichts an dem Charakter der Erklärung als vom Client stammende Willenserklärung. LoRaWAN berührt insoweit nicht die grundsätzliche Funktionsweise und Abgabe der Willenserklärung über Fides, sodass sie sich weiter als vom Client stammend darstellt. LoRaWAN kommt vielmehr die rechtliche Rolle eines Boten zu, der die Willenserklärung des Clients transportiert, übersetzt und an der vom Client vorgegeben Stelle im Contract platziert. Ebenso unproblematisch ist die Übermittlung von lediglich variablen Informationen, die für den konkreten Contract relevant sind. Hierbei ist jedoch darauf zu achten, dass eine wirksame Kenntnisnahme von Informationen wie AGB, Widerrufsrechten oder Pflichtinformationen weiter möglich sein muss und es durch die Verwendung existierender Templates wahrscheinlich ist, dass die dort enthaltenen Bestimmungen rechtlich selbst als AGB eingeordnet werden. Die asynchrone Aktualisierung von Contracts im Full Node und auf den Endgeräten der Clients kann zudem im Zusammenhang mit dem Zeitpunkt der Abgabe und des Zugangs von Willenserklärungen relevant werden.

D. Datenschutzrechtliche Betrachtung

Nachdem im vorhergehenden Kapitel die zivilrechtlichen Grundlagen analysiert und vorgestellt wurden, wird in der Folge auf die mit dem Fidesnetzwerk verbundenen datenschutzrechtlichen Anforderungen – und soweit sich Besonderheiten bei der Nutzung von Fides mithilfe von LoRaWAN ergeben gesondert – eingegangen.[156] Dabei können nicht alle datenschutzrechtlichen Herausforderungen – schon allein aufgrund des beschränkten Umfangs der Studie – eingehend untersucht und dargestellt werden. Gleichwohl werden die gewichtigsten datenschutzrechtlichen Herausforderungen adressiert, die in Fides zu berücksichtigen sind und sich nach Maßgabe der Europäischen Datenschutzgrundverordnung (DSGVO)[157] stellen. Dabei handelt es sich insbesondere um den Anwendungsbereich datenschutzrechtlicher Vorschriften (I.), die Klärung datenschutzrechtlicher Verantwortlichkeiten (II.), die Einhaltung datenschutzrechtlicher Grundsätze (III.), die Rechtmäßigkeit der Datenverarbeitung (IV.) sowie ausgewählte Pflichten des Datenverarbeiters (V.) und ausgewählte Rechte der betroffenen Person (VI.). Eine Zusammenfassung der datenschutzrechtlichen Perspektive rundet das Kapitel ab (VII.).

I. Anwendungsbereich der DSGVO

Das Datenschutzrecht und insbesondere die DSGVO sind nur anwendbar, wenn personenbezogene Daten verarbeitet werden. Werden hingegen ausschließlich anonyme Daten verarbeitet, also Daten, die sich nicht einer bestimmten oder bestimmbaren natürlichen Person zuordnen lassen, so finden datenschutzrechtliche Regelungen keine Anwendung.[158] Pseudonyme Daten (vgl. zur Pseudonymisierung Art. 4 Nr. 5 DSGVO) hingegen unterfallen dem Datenschutzrecht.[159] Daher ist zunächst zwingend zu klären, ob in Fides personenbezogene Daten verarbeitet werden. Denn nur soweit dies der Fall ist, sind datenschutzrechtlichen Anforderungen zu berücksichtigen. Der Anwendungsbereich

---

[156] Vgl. allgemein zur Thematik Datenschutz und Smart Contracts bzw. Blockchain auch bei *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 66 ff.; *Pesch*, Blockchain, Smart Contracts und Datenschutz in: Fries/Paal, Smart Contracts, S. 13 ff.; *Quiel*, DuD 2018, 566 ff.; *Böhme/Pesch*, DuD 2017, 473 ff.; *Martini/Weinzierl*, NVwZ 2017, 1251 ff.; *Bechtolf/Vogt*, ZD 2018, 66 ff.; *Guggenberger*, ZD 2017, 49 f.

[157] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1 vom 4.5.2016.

[158] Vgl. EG 26 S. 5 und S. 6 DSGVO*; Karg* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 1 Rn. 20.

[159] Vgl. EG 26 S. 2 DSGVO*; Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 5 Rn. 15.

des Datenschutzrechts wird dabei durch die DSGVO auf sachlicher Ebene (vgl. Art. 2 DSGVO) sowie räumlicher Ebene (vgl. Art. 3 DSGVO) näher definiert.

1. Sachlicher Anwendungsbereich, Art. 2 DSGVO

Die DSGVO gilt grundsätzlich für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (vgl. Art. 2 Abs. 1 DSGVO). Auf die Art und Weise der Verarbeitung, automatisiert oder manuell, kommt es somit nicht an.[160] Eine nichtautomatisierte Verarbeitung personenbezogener Daten findet im Fidesnetzwerk nicht statt, da hierunter nur solche Verarbeitungen zu verstehen sind, die nicht rechnergestützt erfolgen.[161] Die Fides-Architektur basiert hingegen auf einem vollständigen rechnergestützten Daten- und Informationsaustausch.

a) Personenbezogene Daten im Fidesnetzwerk

Unter personenbezogenen Daten sind alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (vgl. Art. 4 Nr. 1 DSGVO). Eine Identifikation liegt vor, sofern eine Person durch oder mithilfe der betreffenden Information individualisiert oder erkennbar gemacht werden kann.[162] Eine namentliche Nennung oder die Kenntnis der bürgerlichen Identität ist hingegen nicht erforderlich.[163] Identifizierbar ist eine Person, wenn sie „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem mehreren besonderen Merkmalen, die Ausdruck der physischen oder physiologischen, genetischen, psychischen wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person, identifiziert werden kann“ (vgl. Art. 4 Nr. 1 HS. 2 DSGVO). Es ist somit ausreichend für eine Einordnung als personenbezogenes Datum, wenn zwischen der Information und der Person eine Beziehung hergestellt werden kann.[164]

---

[160] EG 15 DSGVO.
[161] *Zerdick* in: Ehmann/Selmayr, DS-GVO, Art. 2 Rn. 3.
[162] *Karg* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 1 Rn. 49; EuGH, Urt. v. 6.11.2003 – C-101/01, ECLI:EU:C:2003:596, EuZW 2004, 245 Rn. 27.
[163] *Karg* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 1 Rn. 48 f.
[164] *Karg* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 1 Rn. 57; *Art. 29-Datenschutzgruppe*, WP 136, S. 15 f.

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.[165] Dabei ist entscheidend, ob die datenverarbeitende Stelle einen Personenbezug herstellen kann, wobei der Begriff „Personenbezug" grundsätzlich weit auszulegen ist.[166] Ein Personenbezug liegt deshalb bereits dann vor, wenn die datenverarbeitende Stelle über Mittel verfügt, um durch Zusatzinformationen einen Personenbezug herstellen zu können.[167] Daher erfordert die Feststellung des Personenbezugs stets auch eine Risikoanalyse,[168] bei welcher der Informationsgehalt der in Rede stehenden Daten zu berücksichtigten ist.[169] Denn je geringer der Informationsgehalt der verarbeiteten Daten ist, desto geringer sind die Gefahren für eine Gefährdung der informationellen Selbstbestimmung der von der Datenverarbeitung Betroffenen.

Es ist daher zunächst zu klären, in welchem Umfang personenbezogene Daten in Fides verarbeitet werden.[170]

Im Fidesnetzwerk kommen Klarnamen nicht zum Einsatz, sodass jedenfalls Clients nicht unmittelbar identifiziert werden können. Da es sich um ein offenes und dezentrales Netzwerk handelt, lässt sich ein Personenbezug auch nicht insoweit herstellen, wie dies in einem zulassungsbeschränkten (Fides-)Netzwerk der Fall wäre, soweit dieses auf der Verifikation einer natürlichen Person basieren würde – im (Fides-)Netzwerk die Clients – und die kontrollierende zentrale Einheit – im (Fides-)Netzwerk die Full Nodes – die Möglichkeit hätte, Adressen oder Transaktionsdaten unmittelbar der Identität einer natürlichen Person zuzuordnen.[171]

---

[165] EG 26 S. 3 DSGVO.
[166] Vgl. zur Abgrenzung zwischen relativen Personenbezug und absoluten Personenbezug etwa *Herbst*, NVwZ 2016, 902, 903 ff.
[167] EuGH, Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779.
[168] *Klar/Kühling* in: Kühling/Buchner, DS-GVO BDSG, Art. 4 Nr. 1 Rn. 22.
[169] *Dix*, DuD 2020, 779, 781.
[170] Für Smart Contracts und Blockchains so schon *Pesch*, Blockchain, Smart Contracts und Datenschutz in: Fries/Paal, Smart Contracts, S. 13, 18 ff.
[171] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 73; *Janicki/Saive,* ZD 2019, 251, 252; *Martini/Weinzierl*, NVwZ 2017, 1251, 1253.

Die Clients verfügen jedoch grundsätzlich nur über einen Account, der aus einem Public- sowie einem Private Key besteht und keine weiteren Daten über ihre Person enthält. Diese Informationen werden ausschließlich auf dem Endgerät der Nutzer, in der sog. Fides Instanz, gespeichert. Im Rahmen der Anbahnung, des Abschlusses sowie der Abwicklung von Verträgen über Fides müssen diese Daten zwischen den beteiligten Clients ausgetauscht werden. Diese Informationen werden daher von einem Client zu einem anderen Client – mithilfe der Full Nodes – transferiert, wobei der Public Key jeweils das Äquivalent von Konto und Kontonummer darstellt.[172]

Im Fidesnetzwerk lassen sich die einzelnen Clients jedenfalls unter Hinzuziehung von Zusatzwissen in Form von Metadaten [173] oder Transaktionsfluss-Analysen – sofern hierauf ein Zugriff besteht – mit ausreichender Wahrscheinlichkeit identifizieren.[174] Denn durch derartige Zusatzinformationen – etwa wenn bestimmte Informationen über Merkmale anderer Daten oder bestimmte Transaktionen regelmäßig wiederkehren – besteht immer die Gefahr, dass die sich dahinter verbergenden Clients erkannt bzw. wiedererkannt werden. Daher besteht immer ein Restrisiko für eine Identifizierung der im Fidesnetzwerk agierenden Clients, das bei der rechtlichen Bewertung zu berücksichtigen ist.

Aber auch der Einsatz von Big-Data-Analysen – etwa entsprechende frei verfügbare Analysetools[175] – ermöglicht mit einem immer geringeren Aufwand die Identifizierung von Nutzern.[176] So ist es beispielsweise möglich, die IP-Adresse desjenigen Rechners zu ermitteln, den ein Client nutzt.[177] Denkbar ist schließlich auch, dass Anspruchsinhabern

---

[172] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 68; ähnlich *Pesch*, Blockchain, Smart Contracts und Datenschutz in: Fries/Paal, Smart Contracts, S. 13, 18.

[173] Metadaten bezeichnet strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten. Bei einer Computerdatei können dies etwa der Dateiname sein oder auch die gewährten Zugriffsrechte und das Datum der letzten Dateiänderung.

[174] So schon für die klassische Blockchain-Technologie *Böhme/Pesch*, DuD 2017, 473, 478; *Martini/Weinzierl*, NVwZ 2017, 1251, 1253; *Janicki/Saive*, ZD 2019, 251, 252; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 69.

[175] Siehe etwa https://www.chainalysis.com.

[176] Grundsätzlich dazu etwa *Brisch/Pieper*, CR 2015, 724 ff.; *Martini/Weinzierl*, NVwZ 2017, 1251, 1253.

[177] *Biryukov/Khovratovich/Pustogarov*, Deanonymisation of clients in Bitcoin P2P network, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM 2014, S. 15 ff.; ähnlich auch *Parino/Beiró/Gauvin*, Analysis of the Bitcoin blockchain: socio-economic factors behind the adoption, EPJ Data Science 7, 38 (2018).

oder dem Staat rechtliche Mittel zur Verfügung stehen, um eine Herausgabe von Zusatzinformationen zu erreichen, anhand derer eine Identifizierung sodann erfolgen kann.[178] Eine Identifizierung der Clients im Fidesnetzwerk kann daher grundsätzlich nicht ausgeschlossen werden, sodass bereits unter diesem Blickwinkel von einem Personenbezug und damit personenbezogenen Daten auszugehen ist.

Eine Identifizierung der Clients im Fidesnetzwerk kann allerdings auch schon allein anhand deren IP-Adresse erfolgen, da IP-Adressen personenbezogene Daten sind. Das gilt ohnehin für statische IP-Adressen, die in der Regel den Servern der Betreiber der Full Nodes zugewiesen sind.[179] Eine Identifikation der Betreiber der Full Nodes ist somit möglich. Daneben sind jedoch auch dynamische IP-Adressen, wie sie üblicherweise von den Clients genutzt werden, als personenbezogenes Datum anzusehen, wenn der Datenverarbeiter, der nicht der Internetzugangsanbieter selbst ist, über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand von Zusatzinformationen, über die ein Dritter verfügt, bestimmen zu lassen.[180] Daher kann jedenfalls nicht ausgeschlossen werden, dass der Betreiber einer Full Node einen Client identifizieren kann, da ihm wenigstens die IP-Adresse für den Datenaustausch bekannt sein muss. Die Clients stehen hingegen nicht im unmittelbaren Kontakt miteinander, da sie sich ausschließlich über die Full Node als Intermediär austauschen, sodass ein Client von einem anderen Client keine unmittelbare Kenntnis über dessen IP-Adresse hat.

Schließlich kann ein Personenbezug auch dann bejaht werden, wenn die Clients ihre Identität mittelbar oder unmittelbar selbst offenlegen.[181] Das kann beispielsweise durch die Registrierung der Clients auf einer Intermediärsplattform erfolgen oder schlicht bei der Angabe einer Zahlungsadresse gegenüber Käufern oder einer Lieferanschrift gegenüber Verkäufern.[182] Da über das Fidesnetzwerk insbesondere Verträge geschlossen und abgewickelt werden sollen, ist jedenfalls den Vertragsparteien – also den Clients – die gegenseitige Identität regelmäßig bekannt. Das gilt etwa dann, wenn über das

---

[178] *Martini/Weinzierl*, NVwZ 2017, 1251, 1253.
[179] Vgl. dazu schon *Härting*, CR 2008, 743, 745 f.; *Eckhardt*, CR 2011, 339 ff.; *Gerlach*, CR 2013, 478 ff.
[180] EuGH, Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779; *Eckhardt*, CR 2016, 786 ff.; *Moos*, K&R 2017, 566 ff.; *Kühling/Schildbach*, NJW 2020, 1545 ff.
[181] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 69; aA wohl *Schrey/Thalhofer*, NJW 2017, 1431, 1433.
[182] So auch schon *Quiel*, DuD 2018, 566, 568; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 69.

Fidesnetzwerk ein Kaufvertrag zwischen zwei (oder mehreren) Clients geschlossen werden soll. Denn ein derartiger Kaufvertrag muss zumindest Informationen über die Namen der Vertragsparteien, den Kaufgegenstand und den Kaufpreis enthalten.[183] Ein Client kann schließlich auch gegenüber dem Full Node seine Identität freiwillig preisgeben, was allerdings grundsätzlich nicht erforderlich ist. Gleichwohl wird dies bei der Anbahnung, dem Abschluss sowie der Abwicklung von Verträgen regelmäßig der Fall sein, wenn die Clients als Vertragsparteien die Möglichkeit der Durchsetzung von Sekundärrechten – wie etwa Schadensersatzansprüchen – auch faktisch bewahren wollen.[184]

Ein Personenbezug entfällt auch nicht deshalb, weil die Transaktionsdaten der beteiligten Clients auf einem Full Node verschlüsselt gespeichert werden. Eine Verschlüsselung eignet sich primär dazu, personenbezogene Daten für alle unbefugten Personen unzugänglich zu machen.[185] Demnach können befugte Personen auf rechtmäßige Weise sowie unbefugte Personen auf rechtswidrige Weise gleichwohl einen Personenbezug herstellen. Die Verschlüsselung von Daten und Informationen schließt die Herstellung eines Personenbezugs daher nicht aus, da es sich lediglich um eine technisch-organisatorische Maßnahme im Sinne von Art. 32 Abs. 1 lit. a DSGVO handelt.[186]

Schließlich vermögen auch mögliche und eingesetzte Anonymisierungstechniken im Fidesnetzwerk einen Personenbezug von Daten nicht ausschließen, da oftmals gängige Methoden zur Anonymisierung versagen und so auch zunächst vermeintlich anonyme Daten einen Personenbezug aufweisen können.[187]
Im Fidesnetzwerk werden grundsätzlich personenbezogenen Daten verarbeitet. Dabei ist gleichwohl für jeden Einzelfall zu prüfen, welche Daten einen Personenbezug aufweisen.

---

[183] *Westermann* in: Säcker/Rixecker/Oetker/Limperg, Münchener Kommentar zum Bürgerlichen Gesetzbuch Band 4, § 433 Rn. 7.
[184] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 74.
[185] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 Rn. 35.
[186] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 70.
[187] *Rocher/Hendrickx/de Montjoye*, Estimating the success of re-identifiactions in incomplete datasets using generative models, Nature Communications 10, 3069, https://doi.org/10.1038/s41467-019-10933-3; vgl. dazu etwa https://netzpolitik.org/2019/weitere-studie-belegt-luege-anonymer-daten sowie https://www.heise.de/newsticker/meldung/36C3-Wie-gaengige-Methoden-zur-Anonymisierung-von-Daten-versagen-4624450.html; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 71.

Unproblematisch sind insbesondere diejenigen Fälle, in denen zwei (oder mehrere) Clients hinsichtlich der Anbahnung, des Abschlusses und der Abwicklung eines Vertrages gegenüber dem jeweils anderen Vertragspartner ohnehin personenbezogene Daten offenbaren müssen. Andernfalls würde das Fidesnetzwerk seinen Zweck nicht erfüllen können. Wird Fides mithilfe von LoRaWAN genutzt, ergibt sich keine andere rechtliche Bewertung.

b) Automatisierte Verarbeitung personenbezogener Daten im Fidesnetzwerk

Unter Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung zu verstehen (vgl. Art. 4 Nr. 2 DSGVO).

Der Verarbeitungsbegriff ist – auch schon aufgrund der zahlreichen nicht enumerativ genannten Erscheinungsformen – weit zu interpretieren.[188] Außerdem muss der Verarbeitungsvorgang als solches dabei immer im Zusammenhang mit personenbezogenen Daten stehen.[189] Die Verarbeitung erfolgt automatisiert, wenn Datenverarbeitungsanlagen eingesetzt werden.[190] Erfasst werden somit alle Verfahren, bei denen zumindest ein Teil eines Datenverarbeitungsprozesses anhand eines vorgegebenen Programms ohne weiteres Eingreifen eines Menschen selbständig erfolgt.[191] Der Anwendungsbereich ist aus technischer Sicht bewusst so weit gewählt, um Technologieneutralität zu erreichen und Datenschutz auch bei zukünftigen technischen Entwicklungen gewährleisten zu können.[192]

Bei der Anbahnung, dem Abschluss sowie der Abwicklung von Verträgen zwischen am Fidesnetzwerk beteiligten Clients werden ganz unterschiedliche personenbezogene Daten – je nach Vertragsart, -kontext und -partner – erhoben, gespeichert, verändert,

---

[188] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 2 Rn. 10; EuGH, Urt. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317, NJW 2014, 2257, 2260 Rn. 53.
[189] *Roßnagel in:* Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 2 Rn. 12.
[190] *Kühling/Raab* in: Kühling/Buchner, DSGVO BDSG, Art. 2 Rn. 15.
[191] *Bäcker in:* Wolff/Brink, BeckOK Datenschutzrecht, Art. 2 Rn. 2.
[192] Vgl. EG 15 DSGVO; *Kühling/Raab* in: Kühling/Buchner, DSGVO BDSG, Art. 2 Rn. 15.

abgefragt, verknüpft oder gelöscht. Um über das Fidesnetzwerk einen zivilrechtlichen Vertrag rechtskonform abzuschließen, müssen etwa Daten über den Kaufgegenstand und -preis sowie die beteiligten Vertragsparteien erhoben und zwischen den Clients auch ausgetauscht werden. Wird eine Contract offer abgelehnt, müssen Informationen wiederum verändert, neu verknüpft und übermittelt werden. Auch die Löschung von Daten kommt hier in Betracht, wenn diese etwa aufgrund der Ablehnung einer Contract offer nicht mehr benötigt werden. Im Fidesnetzwerk werden somit unterschiedliche personenbezogene Daten verarbeitet. Bei einer zusätzlichen Integration von LoRaWAN ergibt sich keine andere rechtliche Bewertung.

c) Keine Bereichsausnahme nach Art. 2 Abs. 2 lit. c DSGVO

Bei Fides handelt es sich um ein offenes und dezentrales Netzwerk, sodass generell eine unbegrenzte Anzahl an Clients beitreten kann. Eine persönliche oder familiäre Zulassungsbeschränkung liegt nicht vor. Daher kommt eine entsprechender Ausschluss der datenschutzrechtlichen Vorschriften nicht in Betracht (vgl. Art. 2 Abs. 2 lit. c DSGVO), zumal die Bereichsausnahme ohnehin eng auszulegen ist.[193]

2. Räumlicher Anwendungsbereich, Art. 3 DSGVO

Die DSGVO findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet (vgl. Art. 3 Abs. 1 DSGVO). Daneben wird der räumliche Anwendungsbereich auf Fälle ausgedehnt, in denen personenbezogene Daten von betroffenen Personen, die sich in der Union befinden, verarbeitet werden und der Datenverarbeiter ein nicht in der Union niedergelassener Verantwortlicher oder Auftragsverarbeiter ist und die Datenverarbeitung im Zusammenhang damit steht betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten oder das Verhalten betroffener Personen in der Union zu beobachten (vgl. Art. 3 Abs. 2 DSGVO). Der räumliche Anwendungsbereich wird maßgeblich durch das Niederlassungsprinzip (Abs. 1) sowie durch das Marktortprinzip (Abs. 2) bestimmt.[194] Die dezentrale und offene Struktur des Fidesnetzwerks und die damit einhergehende grundsätzliche örtliche

[193] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 2 Rn. 23; EuGH, Urt. v. 11.12.2014 – C-212-13, ECLI:EU:C:2014:2428, Rn. 28 ff.
[194] *Hornung* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 3 Rn. 1.

Unabhängigkeit der Nutzer der Fidesstruktur spielen an dieser Stelle eine wesentliche Rolle.

a) Niederlassungsprinzip, Art. 3 Abs. 1 DSGVO

Soweit die Full Nodes des Fidesnetzwerks in der EU angesiedelt sind, fallen deren Betreiber aufgrund des Niederlassungsprinzips (Art. 3 Abs. 1 DSGVO) in den räumlichen Anwendungsbereich der Norm.[195] Denn eine Niederlassung ist eine feste Einrichtung, von der aus eine Tätigkeit effektiv und tatsächlich ausgeübt wird.[196] Hierfür genügt angesichts der extensiven Auslegung der Merkmale bereits das Zusammenwirken persönlicher und sachlicher Mittel mit einem gewissen Grad an Beständigkeit.[197] Auch an die effektive und tatsächliche Ausübung einer Tätigkeit sind keine hohen Anforderungen zu stellen.[198] Sie liegt jedenfalls dann vor, wenn die Niederlassung die Verarbeitung technisch vornimmt oder selbst maßgeblich steuert.[199] Auf den in der EU stehenden Full Nodes Servern werden zumindest die relevanten und maßgeblichen Datenverarbeitungen vorgenommen, die für die Anbahnung, den Abschluss sowie die Abwicklung von Verträgen zwischen den Clients notwendig sind. Auch ein zusätzlicher Einsatz von LoRaWAN führt zu keiner anderen rechtlichen Bewertung.

b) Marktortprinzip, Art. 3 Abs. 2 DSGVO

Aber selbst wenn die Full Nodes nicht in der EU lokalisiert sein sollten, ist der Anwendungsbereich für deren Betreiber auch aufgrund des Marktortprinzips (Art. 3 Abs. 2 DSGVO) eröffnet. Der Ort der technischen Datenverarbeitung ist hiernach unerheblich,[200] sodass es keine Rolle spielt, dass die Server der Full Node Betreiber nicht in der EU stehen. Es genügt für die Eröffnung des räumlichen Anwendungsbereichs, wenn ein Zusammenhang zwischen dem Angebot und der Datenverarbeitung besteht.[201] Da das Fidesnetzwerk als dezentrales und offenes System gestaltet ist und somit global für alle potentiellen Clients offensteht, richten sich die entsprechenden Dienste – hier

---

[195] Ebenso *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 75.
[196] Vgl. EG 22 DSGVO; *Hornung* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 3 Rn. 2; *Hanloser* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 3 Rn. 13 ff.; *Klar* in: Kühling/Buchner, DSGVO BDSG, Art. 3 Rn. 41.
[197] EuGH, Urt. v. 4.7.1985 – C-168/84, Rn. 18; EuGH, Urt. v. 1.10.2015 – C-230/14, ECLI:EU:C:2015:639, Rn. 29; EuGH, Urt. v. 28.07.2016 – C-191/15, ECLI:EU:C:2016:612, Rn. 77; EuGH, Urt. v. 25.7.1991 – C-221/89, Rn. 20; *Klar* in: Kühling/Buchner, DSGVO BDSG, Art. 3 Rn. 44.
[198] *Klar* in: Kühling/Buchner, DSGVO BDSG, Art. 3 Rn. 48.
[199] *Hornung* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 3 Rn. 26.
[200] *Hornung* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 3 Rn. 46.
[201] *Hanloser* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 3 Rn. 31.

insbesondere die Anbahnung, der Abschluss sowie die Abwicklung von Verträgen – auch an betroffene Personen in der EU. Daher dürfte regelmäßig bei derartigen Verträgen, wie sie im Rahmen von Fides angebahnt, abgeschlossen und abgewickelt werden, das Kriterium des Dienstleistungsangebots erfüllt sein. [202] Der Sinn und Zweck der Fidesnetzwerkstruktur besteht gerade darin, zwischen den beteiligten Clients vereinbarte Verträge, denen ein Angebot vorausgegangen sein muss, umzusetzen, sodass Dienstleistungen angeboten werden. Ein ergänzender Einsatz von LoRaWAN hat hierauf keine weitergehenden Auswirkungen.

II. Datenschutzrechtliche Verantwortlichkeiten

Das Datenschutzrecht basiert auf der Zuschreibung von Verantwortlichkeiten von Datenverarbeitungsprozessen. Die Verantwortlichkeit für eine Datenverarbeitung ist daher ein wesentliches Grundprinzip.[203] Nur den datenschutzrechtlich verantwortlichen Akteur trifft der datenschutzrechtliche Pflichtenkanon. Daher werden zunächst die Grundlagen datenschutzrechtlicher Verantwortlichkeiten dargelegt, um diese sodann auf das Fidesnetzwerk zu übertragen.

1. Grundlagen datenschutzrechtlicher Verantwortlichkeiten

a) Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24 DSGVO

Art. 24 DSGVO ist die zentrale Vorschrift zur Pflichtenstellung des Verantwortlichen zur Einhaltung der Vorschriften der DSGVO. [204] Normadressat der Regelung ist der Verantwortliche. Verantwortlicher ist dabei jede 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 (vgl. Art. 4 Nr. 7 DSGVO). Der Begriff ist dabei weit auszulegen, um einen wirksamen und effektiven Schutz der betroffenen Personen zu gewährleisten. [205] Der Verantwortliche muss insbesondere geeignete technische und organisatorische Maßnahmen umsetzen, um sicherzustellen, dass die Datenverarbeitung gemäß der DSGVO erfolgt. Zur erstmaligen Feststellung der notwendigen Maßnahmen zur Anpassung an die DSGVO ist eine

---

[202] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 75.
[203] So schon *Bizer*, DuD 2007, 350, 350.
[204] *Petri* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 24 Rn. 1.
[205] *Petri* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 7 Rn. 21; EuGH, Urt. v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317, Rn. 34 – Google Spain.

umfassende Bestandsaufnahme der einzelnen Verarbeitungstätigkeiten sowie der bereits vorhandenen Maßnahmen geboten.[206]

b) Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO

Daneben regelt Art. 26 DSGVO eine gemeinsame Verantwortlichkeit von mehreren datenverarbeitenden Akteuren. Dieses Rechtsinstitut war zwar auch schon bisher in der EG-Datenschutzrichtlinie (vgl. dort Art. 2 lit. d DSGVO) angelegt, dort allerdings nicht detailliert ausgestaltet, und spielte deshalb bisher nur eine untergeordnete Rolle. Seit einer Entscheidung des EuGH zur Ausgestaltung der gemeinsamen Verantwortlichkeit[207] hat dieses Rechtsinstitut nun aber große Aufmerksamkeit erfahren, denn der Entscheidung lässt sich entnehmen, dass auch dann eine gemeinsame Verantwortlichkeit angenommen wird, wenn nur eine untergeordneten Einflussnahme eines Partners auf die Datenverarbeitung des anderen besteht, aber von dessen Datenverarbeitung jedenfalls in Teilen profitiert wird. Daher wird die ausdrückliche Regelung der gemeinsamen Verantwortlichkeit in der DSGVO nunmehr besonders für die Praxis erhebliche Auswirkungen haben.[208]

Art. 26 DSGVO reagiert auf die zunehmend vernetzte Verarbeitung personenbezogener Daten, wie sie für die Digitalisierung ganz generell und etwa das Internet charakteristisch ist. Verarbeiten mehrere oder gar viele Stellen arbeitsteilig personenbezogene Daten, kann diese Kooperation erhebliche datenschutzrechtliche Auswirkungen auf die betroffenen Personen haben, da die Dienstleistungen für die Betroffenen oftmals intransparent sind, weil Datenflüsse regelmäßig nicht nachvollzogen werden können.[209] Deshalb ist eine klare Zuteilung von Verantwortlichkeiten sowie der Haftung geboten.[210]

In dezentralen Strukturen wie dem Fidesnetzwerk bereitet die Zuschreibung von Verantwortlichkeiten und damit die Bestimmung eines Verantwortlichen oder mehrerer gemeinsamer Verantwortlicher erhebliche Schwierigkeiten. Derartige offene und

---

[206] *Petri* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 24 Rn. 11.
[207] Grundlegend dazu jeweils EuGH, Urt. v. 5.6.2018 – C-210/16, ECLI:EU:C:2018:388 – Facebook-Fanpages; EuGH, Urt. v. 29.7.2019 – C-40/17, ECLI:EU:C:2019:629 – Fashion ID; EuGH, Urt. v. 10.7.2018 – C-25/17, ECLI:EU:C:2018:551 – Zeugen Jehovas.
[208] *Datenschutzkonferenz*, Kurzpapier Nr. 16 – Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf, S. 1; zuletzt abgerufen am 3.1.2023.
[209] *Petri* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 26 Rn. 2.
[210] Vgl. EG 79 DSGVO.

dezentrale Strukturen entsprechen grundsätzlich weder dem Prototyp der DSGVO, einer zentralen Zuweisung von alleiniger Verantwortlichkeit (vgl. Art. 24 DSGVO) noch von gemeinsamer Verantwortlichkeit basierend auf einem gemeinsamen Entschluss (vgl. Art. 26 DSGVO).[211]

2. Datenschutzrechtliche Verantwortlichkeiten im Fidesnetzwerk

Da es sich bei Fides um ein offenes und dezentrales Netzwerk handelt sowie Clients und Full Nodes jederzeit der Netzwerkstruktur beitreten oder diese verlassen können, liegt eine besondere Schwierigkeit darin, eine datenschutzrechtliche Verantwortlichkeit (vgl. Art. 24 DSGVO) oder mehrere datenschutzrechtliche Verantwortlichkeiten (vgl. Art. 26 DSGVO) zu begründen. Denn ein wesentliches Merkmal des Fidesnetzwerks ist es, dass ein Einzelner – etwa ein Full Node oder ein Client – oder eine Gruppe von mehreren Akteuren keinen bestimmenden Einfluss auf das Gesamtnetzwerk als solches haben.[212]

Verantwortlicher im Fidesnetzwerk kann jedenfalls nur derjenige Akteur sein, der die Entscheidungshoheit über die Zwecke und Mittel der Datenverarbeitung hat (vgl. Art. 4 Nr. 7 DSGVO).[213] Die Entscheidungshoheit kann allein oder gemeinsam mit anderen ausgeübt werden.[214] Bei der Zuweisung von Verantwortlichkeiten ist auf die einzelnen Datenverarbeitungsschritte abzustellen.[215] Daher muss immer erkennbar sein – insbesondere für die betroffene Person, aber auch für die Aufsichtsbehörden –, wer für welche (Phase einer) Datenverarbeitung verantwortlich ist.[216] Im Fidesnetzwerk kommen insbesondere die Betreiber einer Full Node als datenschutzrechtlich Verantwortliche in Betracht, aber auch eine gemeinsame Verantwortlichkeit von Full Node Betreibern und Clients ist denkbar.

---

[211] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 91; *Böhme/Pesch*, DuD 2017, 473, 479.
[212] So auch schon *Schrey/Thalhofer*, NJW 2017, 1431, 1433; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 92; *Bechtolf/Vogt*, ZD 2018, 66, 69.
[213] *Petri* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 7 Rn. 20 ff.
[214] *Petri* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 7 Rn. 21.
[215] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 94; aA wohl *Schrey/Thalhofer*, NJW 2017, 1431, 1433; *Böhme/Pesch*, DuD 2017, 473, 479.
[216] *Piltz* in: Gola/Heckmann, DS-GVO – BDSG, DS-GVO Art. 26 Rn. 2.

a) Betreiber einer Full Node als alleiniger datenschutzrechtlich Verantwortlicher

Einzelne Datenverarbeitungsschritte werden im Fidesnetzwerk regelmäßig von einem bestimmten Full Node vorgenommen, wobei der Umfang der Datenverarbeitung mit der Funktion der Full Node variiert. So werden grundsätzlich sämtliche Transaktionsdaten im Full Node verschlüsselt gespeichert. Auf jedem Full Node sind darüber hinaus die Templates und Informationen zum aktuellen Zustand eines existierenden Contracts gespeichert, wobei jeder Full Node für andere Contracts zuständig ist und damit auch unterschiedliche Templates vorhalten. Auf dem Full Node werden ferner die Contracts der Clients veröffentlicht, sodass auch die relevanten Contractdaten im Full Node gespeichert sind. Ein Full Node verfolgt damit einerseits den eigenen Zweck der Teilnahme am Fidesnetzwerk und entscheidet andererseits über die Mittel der Datenverarbeitung, da er die relevanten personenbezogenen Daten der Clients erhebt, erfasst, ordnet und speichert. Daher lässt sich im Fidesnetzwerk zumindest jede Full Node, die an einer Vertragsanbahnung, einem Vertragsschluss sowie der Vertragsabwicklung beteiligt ist, als datenschutzrechtlich verantwortlicher Akteur ansehen. [217] Faktische Durchsetzungsschwierigkeiten – etwa im Hinblick auf die Durchsetzung von Betroffenenrechten (Auskunfts- oder Löschungsrecht) – stehen einer solchen Qualifizierung auch nicht entgegen.[218]

b) Gemeinsame Verantwortlichkeit von Full Node Betreibern und Clients

Denkbar ist aber auch, dass im Rahmen der Anbahnung, des Abschlusses und der Abwicklung von Verträgen über das Fidesnetzwerk alle an diesem Vorgang beteiligten Akteure – also der zuständige Full Node sowie die beteiligten Clients – als gemeinsam für die Verarbeitung Verantwortliche zu qualifizieren sind.[219]

Eine gemeinsame Verantwortlichkeit kann auch dann angenommen werden, wenn auch nur eine untergeordnete Einflussnahme eines Partners auf die Datenverarbeitung des anderen besteht, aber von dessen Datenverarbeitung jedenfalls in Teilen profitiert

---

[217] Für die Blockchain so schon *Martini/Weinzierl*, NVwZ 2017, 1251, 1253.
[218] Zutreffend so auch *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 94; aA *Böhme/Pesch*, DuD 2017, 473, 479.
[219] So auch schon *Quiel*, DuD 2018, 566, 569 f.; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 96.

wird.[220] Wesentlich sind die Umstände des Einzelfalls, wobei hier insbesondere auf das Kriterium der Entscheidungsbefugnis über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten abzustellen ist.[221] Eine gleichrangige Einflussnahme auf die Entscheidungsfindung ist nicht erforderlich.[222] Auch muss sich die Kontrolle der an der Datenverarbeitung gemeinsam beteiligten Akteure nicht über die gesamte Dauer der Datenverarbeitung erstrecken.[223]

Der Vertragsschluss sowie die Abwicklung von Verträgen zwischen den beteiligten Clients wären ohne eine Full Node nicht möglich. Die Betreiber einer Full Node verfolgen zwar eigene Zwecke und verfügen auch über eigene Mittel der Datenverarbeitung[224], gleichwohl profitieren hiervon die beteiligten Clients unmittelbar. So werden die Informationen zum Template und zum Contract nicht nur auf den Endgeräten der beteiligten Clients gespeichert, sondern eine Speicherung findet auch im zuständigen Full Node statt. Die Anbahnung, der Abschluss und die Abwicklung der Verträge können zwischen den Clients immer nur mithilfe einer Full Node erfolgen. So veröffentlicht der Client, der einen Vertrag anbahnen will, seinen Contract über die zuständige Full Node. Auf diesen neuen Contract wird der andere Client nunmehr aufmerksam gemacht. Er kann sodann den Contract – als Aufforderung zur Kommunikation – annehmen oder ablehnen. Generell erfolgt die Kommunikation zwischen den einen Contract betreffenden Clients über die Bestätigung von sog. Tasks, die in dem jeweiligen maßgeblichen Template vorgesehen sind. Dabei werden die relevanten Informationen einerseits im Full Node verschlüsselt und andererseits lokal bei den betroffenen Clients gespeichert. Unabhängig vom konkreten Ablauf der Abwicklung eines Contracts sind die Contractdaten zwar im Full Node und bei den Clients gespeichert, jedoch nur auf den Endgeräten der Clients zu entschlüsseln. Der Full Node kann keinen Einfluss auf die Verarbeitung der auf dem Endgerät gespeicherten Daten oder des im Full Node gespeicherten Zustands des Contracts nehmen. Gleichwohl basiert das Fidesnetzwerk auf einem gemeinsamen

[220] Siehe dazu etwa EuGH, Urt. v. 5.6.2018 – C-210/16, ECLI:EU:C:2018:388 – Facebook-Fanpages; EuGH, Urt. v. 29.7.2019 – C-40/17, ECLI:EU:C:2019:629 – Fashion ID; EuGH, Urt. v. 10.7.2018 – C-25/17, ECLI:EU:C:2018:551 – Zeugen Jehovas.
[221] *Spoerr* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 26 Rn. 19 mwN.
[222] *Spoerr* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 26 Rn. 20 mwN.
[223] *Spoerr* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 26 Rn. 31.
[224] Siehe hierzu bereits unter D. II. 2. a.

Zusammenwirken von Full Node und Clients, sodass eine gemeinsame Verantwortlichkeit möglich erscheint.

c) Gemeinsame Verantwortlichkeit von mehreren Full Node Betreibern

Prinzipiell können auch mehrere Full Nodes eine gemeinsame Verantwortlichkeit begründen, wenn sie die Zwecke und Mittel der Verarbeitung gemeinsam festlegen.[225] Da im Fidesnetzwerk aber jeder Full Node für andere Contracts und Templates zuständig ist, fehlt es regelmäßig an einer gemeinsamen Zielsetzung unterschiedlicher Full Nodes, sodass keine gemeinsame Verantwortlichkeit mehrerer Full Nodes vorliegt.

d) Zusammenfassung zur datenschutzrechtlichen Verantwortlichkeit im Fidesnetzwerk

Die Zuschreibung von evidenten Verantwortlichkeiten ist in offenen und dezentralen Netzwerkstrukturen nicht trivial. Das gilt auch für das vorliegende Fidesnetzwerk.

Vereinzelt wird daher eine singuläre datenschutzrechtliche Verantwortlichkeit – etwa eines bestimmten Full Node Betreibers oder eines einzelnen Clients – generell abgelehnt, [226] da die DSGVO insbesondere dezentrale Datenverarbeitungen weder würdigen noch fördern würde.[227] Andere wiederum qualifizieren einzelne Nutzer bzw. Initiatoren von (Trans-)Aktionen – im Fidesnetzwerk wären das die Clients – als alleinige Verantwortliche, da diese durch die Übermittlung der (Trans-)Aktionen an das Netzwerk die Kontrolle über den Datenverarbeitungsprozess wahrnehmen würden.[228]

Eine rechtliche Bewertung muss sich allerdings generell an den rechtlichen Maßstäben der DSGVO und damit insbesondere an Art. 24 DSGVO und Art. 26 DSGVO orientieren.

Im Fidesnetzwerk wird bei der Anbahnung, dem Abschluss sowie der Abwicklung von Verträgen eine gemeinsame Verantwortlichkeit der beteiligten Akteure begründet. Daher sind sowohl die Betreiber der zuständigen Full Node als auch die am Vertrag beteiligten Clients als datenschutzrechtlich gemeinsame Verantwortliche zu qualifizieren (vgl. Art. 26 DSGVO). Problematisch ist dabei allerdings, dass dadurch regelmäßig private Akteure – die Clients – zu Verantwortlichen werden und dieser Stellung oftmals nur schwer

---

[225] So auch *Martini/Weinzierl*, NVwZ 2017, 1251, 1254.
[226] In diese Richtung wohl *Schrey/Thalhofer*, NJW 2017, 1431, 1433 f.
[227] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 92.
[228] In diese Richtung etwa *Erbguth/Fasching*, ZD 2017, 560, 564.

gewachsen sind.[229] Bei der Ausgestaltung von Fides sind diese Überlegungen daher besonders zu berücksichtigen. Ob durch die Anknüpfung an einzelne Verarbeitungsschritte und die individuelle Zuschreibung von Verantwortlichkeiten klare Verhältnisse geschaffen werden und ob diese in dezentralen Netzwerken überhaupt möglich sind, muss sich in der Praxis erst noch zeigen.[230] Wird Fides mithilfe von LoRaWAN in Regionen ohne Netzinfrastruktur verwendet, ergibt sich keine andere datenschutzrechtliche Bewertung. Denn LoRaWAN ändert nur den Transportweg der Daten, aber nicht die Zuschreibung von Verantwortlichkeiten in der Netzwerkstruktur.

III. Grundsätze für die Verarbeitung personenbezogener Daten

Das Datenschutzrecht wird durch verschiedene Grundsätze geprägt, die in Art. 5 DSGVO niedergelegt sind. Im Kontext von offenen und dezentralen Netzwerkstruktur sind dabei insbesondere das Rechtmäßigkeits- und Transparenzprinzip (Art. 5 Abs. 1 lit. a DSGVO), das Datenminimierungsprinzip bzw. Datensparsamkeitsprinzip (Art. 5 Abs. 1 lit. c DSGVO), das Richtigkeitsprinzip (Art. 5 Abs. 1 lit. d DSGVO) sowie das Integritäts- und Vertraulichkeitsprinzip (Art. 5 Abs. 1 lit. f DSGVO) zu berücksichtigen.[231] Diese datenschutzrechtlichen Grundsätze sind daher auch bei der Ausgestaltung von Fides zu beachten.

1. Das Rechtmäßigkeitsprinzip in Fides, Art. 5 Abs. 1 lit. a Var. 1 DSGVO

Das Rechtmäßigkeitsprinzip als Teilausprägung der einfachgesetzlichen Ausgestaltung des Grundrechts auf Datenschutz (vgl. Art. 8 GRCh[232]) fordert für eine zulässige Datenverarbeitung entweder eine informierte Einwilligung in Kenntnis aller relevanten Umstände oder die Erfüllung eines Erlaubnistatbestandes, wie sie in Art. 6 DSGVO enthalten sind.[233] Der Grundsatz der Rechtmäßigkeit wird in der DSGVO durch Regelungen zur Zulässigkeit der Datenverarbeitung sowie der Art und Weise der

---

[229] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 97.
[230] *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 97.
[231] Das Zweckbindungs- (Art. 5 Abs. 1 lit. b DSGVO), das Speicherbegrenzungs- (Art. 5 Abs. 1 lit. e DSGVO) sowie das Rechenschaftspflichtprinzip (Art. 5 Abs. 2 DSGVO) stehen gleichwertig neben den anderen genannten Prinzipien. Auch wenn sie ebenfalls generell zu berücksichtigen sind, wird der Fokus in der vorliegenden Studie auf die besonders relevanten Grundsätze im Hinblick auf die Fidesnetzwerkstruktur gelegt.
[232] Vgl. dazu etwa ausführlich *Marsch*, Das europäische Datenschutzgrundrecht.
[233] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 31; EuGH, Urt. v. 1.10.2015 – C-201/14, ECLI:EU:C:2015:638, Rn. 30.

Datenverarbeitung näher ausgestaltet.[234] Das Rechtmäßigkeitsprinzip ist daher eng mit dem Prinzip des Verbots mit Erlaubnisvorbehalt verknüpft (vgl. Art. 6 DSGVO).

Im Fidesnetzwerk werden personenbezogene Daten verarbeitet, die dem Datenschutzrecht unterfallen, sodass auf sie daher die Regeln der DSGVO anwendbar sind.[235] Demnach muss die Datenverarbeitung entweder durch eine Einwilligung der an der Vertragsanbahnung, dem Vertragsabschluss oder der Vertragsabwicklung beteiligten Clients gedeckt sein oder aber ein gesetzlicher Erlaubnistatbestand die Datenverarbeitung legitimieren.[236] Das Prinzip ist auch zu berücksichtigen, wenn Fides mithilfe von LoRaWAN genutzt wird. Zu den Einzelheiten vgl. unter D. IV.

2. Das Transparenzprinzip in Fides, Art. 5 Abs. 1 lit. a Var. 3 DSGVO

Das Transparenzprinzip ist durch Art. 8 Abs. 2 S. 2 GRCh in der Weise primärrechtlich ausdrücklich abgesichert, als die Vorschrift jeder Person das Recht gewährleistet, Auskunft über die sie betreffenden erhobenen Daten zu erhalten.[237] Der Grundsatz beschränkt sich allerdings nicht nur auf das Auskunftsrecht der betroffenen Person, sondern umfasst alle Informationen und Informationsmaßnahmen, die erforderlich sind, damit die betroffene Person überhaupt überprüfen kann, ob die Datenverarbeitung rechtmäßig ist, und ihre Rechte wahrnehmen kann.[238] Das Transparenzprinzip wird durch eine Vielzahl von Vorschriften in der DSGVO ausgefüllt und dabei detailliert insbesondere in Art. 12 ff. DSGVO geregelt.

In Fides müssen bei der Datenverarbeitung ebenfalls die Anforderungen an das Transparenzprinzip eingehalten werden. Demnach müssen die Clients, deren personenbezogene Daten zum Vertragsschluss sowie zur Vertragsabwicklung verarbeitet werden, die ihnen nach der DSGVO niedergelegten Transparenzrechte auch wahrnehmen können.[239] Das Prinzip ist ebenfalls zu berücksichtigen, wenn Fides mithilfe von LoRaWAN genutzt wird. Zu den Einzelheiten vgl. unter B. VI.

---

[234] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 32.
[235] Siehe dazu ausführlich unter D. I. 1.
[236] Siehe hierzu im Detail unter D. IV.
[237] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 49.
[238] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 50.
[239] Siehe hierzu im Detail unter D. VI.

3. Das Datensparsamkeitsprinzip in Fides, Art. 5 Abs. 1 lit. c DSGVO

Der Grundsatz der Datensparsamkeit verlangt, dass die Daten für den Verarbeitungszweckweck erheblich, erforderlich und dem Zweck angemessen sein müssen.[240] Das Prinzip beschränkt die Datenverarbeitung und damit die Tiefe des Eingriffs in das Grundrecht auf Datenschutz der betroffenen Person.[241] Es geht dabei insbesondere darum, dass eine Reduzierung des Personenbezugs von Daten erfolgt. Der Personenbezug der zu verarbeitenden Daten muss im Rahmen der Zweckbindung qualitativ und quantitativ begrenzt werden.[242] Dies zu erreichen ist insbesondere eine Aufgabe der datenschutzrechtlichen Systemgestaltung nach Art. 25 DSGVO.[243] Für das Internet der Dinge, Big Data Analysen und lernende Systeme ist diese Zielsetzung eine große Herausforderung, da sie regelmäßig auf der Auswertung großer Mengen personenbezogener Daten beruhen. Soweit es im Rahmen der legitimen Zwecksetzung der Anwendungen möglich ist, müssen die Daten, die in die Analysen einbezogen werden, daher zuvor anonymisiert oder wenigstens pseudonymisiert werden.[244]

In Fides müssen bei der Datenverarbeitung die Anforderungen an das Datensparsamkeitsprinzip gewahrt werden. Auch hier enthält Fides bereits einige gute und brauchbare Ansätze, da Daten – soweit möglich im Rahmen der Anbahnung, des Abschlusses und der Abwicklung von Verträgen – nicht im Klartext verarbeitet werden, sondern die Verarbeitung pseudonym und verschlüsselt erfolgt. Damit wird ebenfalls einer datenschutzfreundlichen Technikgestaltung nach Maßgabe von Art. 25 DSGVO gedient.[245] Auch ansonsten wird bei der Gestaltung von Fides bereits jetzt der Datensparsamkeitsgrundsatz berücksichtigt, sofern bei der Anbahnung, dem Abschluss sowie der Abwicklung von Verträgen etwa nur die erforderlichen Daten und Informationen verarbeitet werden, die für den maßgeblichen Vertrag zwischen den beteiligten Clients notwendig sind. Eine Absicherung erfährt das Prinzip darüber hinaus auch über die Ermächtigungsgrundlage des Art. 6 Abs. 1 lit. b DSGVO.[246] .[247] Das Prinzip

---

[240] *Reimer* in: Sydow/Marsch, DSGVO, Art. 5 Rn. 29 ff.; *Schantz* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 5 Rn. 55 ff.; *Herbst* in: Kühling/Buchner, DSGVO BDSG, Art. 5 Rn. 57.
[241] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 116.
[242] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 126.
[243] Vgl. dazu unter D. V. 1.
[244] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 128; *Pötters* in: Gola/Heckmann, DS-GVO – BDSG, Art. 5 Rn. 24.
[245] Vgl. dazu im Detail unter D. V. 1.
[246] Vgl. dazu ausführlich unter D. IV. 2.
[247] Siehe hierzu im Detail unter B. VI.

ist auch zu berücksichtigen, wenn Fides mithilfe von LoRaWAN genutzt wird. Zu den Einzelheiten vgl. unter D. IV. 2. und D. V. 1.

4. Das Richtigkeitsprinzip in Fides, Art. 5 Abs. 1 lit. d DSGVO

Der Grundsatz der Richtigkeit der erhobenen und verarbeiteten Daten betrifft die Datenqualität.[248] Es ist erforderlich, dass die verarbeiteten Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind. Hierbei handelt es sich um ein objektives Kriterium, das fordert, dass die Daten über die Person mit der Realität übereinstimmen sollen[249] und falsche Daten umgehend zu berichtigen oder zu löschen sind, was durch den Anspruch der Betroffenen in Art. 16 f. DSGVO konkretisiert wird.[250]

In Fides müssen bei der Datenverarbeitung die Anforderungen an das Richtigkeitsprinzip gewahrt werden. Zu jedem Zeitpunkt müssen daher in der Fidesnetzwerkstruktur die verarbeiteten personenbezogenen Daten mit der Realität übereinstimmen. Von Bedeutung ist dieser Grundsatz insbesondere bei der Anbahnung, dem Abschluss sowie der Abwicklung von Verträgen über das Fidesnetzwerk, da eine Veränderung personenbezogener Daten in diesem Rahmen zu ungewollten und unbeabsichtigten Auswirkungen führen kann. Werden etwa – unabhängig von den Clients – Angaben über den Preis oder die Menge verändert, so müssen diese, wenn sie nicht dem Willen der Clients als Vertragsparteien entsprechend, korrigiert werden.[251] Das Prinzip ist auch zu berücksichtigen, wenn Fides mithilfe von LoRaWAN genutzt wird. Zu den Einzelheiten vgl. unter D. VI.

5. Das Integritäts- und Vertraulichkeitsprinzip in Fides, Art. 5 Abs. 1 lit. f DSGVO

Das Integritäts- und Vertraulichkeitsprinzip, das auch als Grundsatz des Systemdatenschutzes[252] bezeichnet wird, erfordert, dass bei der Datenverarbeitung eine angemessene Sicherheit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen gewährleistet wird. Diese Maßnahmen zielen insbesondere auf den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung sowie unbeabsichtigter

---

[248] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 136.
[249] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 139; *Herbst* in: Kühling/Buchner, DSGVO BDSG, Art. 5 Rn. 60.
[250] *Schantz* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 5 Rn. 28.
[251] Siehe hierzu im Detail unter B. VI.
[252] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 167.

Schädigung ab. Das Prinzip zielt damit insbesondere auf die technische und organisatorische Sicherung der anderen niedergelegten Grundsätze ab. [253] Eine Konkretisierung erfährt die Vorschrift einerseits durch Art. 32 DSGVO, der detailliert die Anforderungen an die Sicherheit der Datenverarbeitung normiert.[254] Andererseits wird die Regelung auch durch Art. 25 DSGVO konkretisiert, die Vorgaben zu einer datenschutzgerechten Systemgestaltung enthält.[255]

In Fides müssen bei der Datenverarbeitung das Integritäts- und Vertraulichkeitsprinzip gewahrt werden. Daher ist es erforderlich, dass im Fidesnetzwerk insbesondere (technische) Mechanismen implementiert werden, die zu einer datenschutzgerechten Systemgestaltung führen – etwa in Form von Pseudonymisierung – sowie die Sicherheit der Datenverarbeitung – etwa in Form von Pseudonymisierung oder Verschlüsselung von Daten – gewährleisten. [256] Das Prinzip ist ebenfalls zu berücksichtigen, wenn Fides mithilfe von LoRaWAN genutzt wird. Zu den Einzelheiten vgl. unter D. VI.

IV. Rechtmäßigkeit der Datenverarbeitung

Das Datenschutzrecht folgt dem Prinzip des Verbots mit Erlaubnisvorbehalt, wonach die Verarbeitung personenbezogener Daten verboten ist, wenn das Gesetz sie nicht ausdrücklich erlaubt.[257] Erlaubnisgründe für die Verarbeitung personenbezogener Daten finden sich sowohl in der DSGVO, hier insbesondere in Art. 6 DSGVO, als auch in europäischen oder nationalen Spezialgesetzen, soweit sie auf Öffnungsklauseln beruhen. Ergänzend kommen die allgemeinen nationalen Datenschutzgesetze wie das Bundesdatenschutzgesetz und die Datenschutzgesetze der Länder hinzu.

Für die vorliegende Studie werden die maßgeblichen potenziell einschlägigen Rechtsgrundlagen der DSGVO analysiert, die in Fides relevant sein können. Dabei handelt es sich insbesondere um die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), die Erfüllung eines Vertrages (Art. 6 Abs. 1 lit. b DSGVO) sowie die Datenverarbeitung zur Wahrung der

---

[253] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 168.
[254] *Herbst* in: Kühling/Buchner, DSGVO BDSG, Art. 5 Rn. 72 ff.
[255] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 171.
[256] Siehe hierzu im Detail unter B. VI.
[257] *Albrecht* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Rn. 1; *Bretthauer in:* Specht/Mantz, Handbuch Datenschutzrecht, Teil A Rn. 31; *Schneider/Härting*, ZD 2012, 199, 202; *Buchner*, DuD 2016, 155, 157; zur Kritik an der Begrifflichkeit: *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 35.

berechtigten Interessen des Verantwortlichen (Art. 6 Abs. 1 lit. f DSGVO).[258] Werden darüber hinaus im Rahmen der Anbahnung, des Abschlusses und der Abwicklung von Verträgen über das Fidesnetzwerk besondere Kategorien personenbezogener Daten verarbeitet – etwa weil Verträge Gesundheitsdaten (vgl. Art. 4 Nr. 15 DSGVO) zum Gegenstand haben – ist Art. 9 DSGVO zu berücksichtigen.

1. Einwilligung in die Datenverarbeitung, Art. 6 Abs. 1 lit. a DSGVO

a) Allgemeine Anforderungen

Die Einwilligung ist der „genuine Ausdruck der informationellen Selbstbestimmung".[259] Sofern ein Betroffener eine Einwilligung erteilt, ermöglicht sie dem Verantwortlichen die Verarbeitung personenbezogener Daten. Eine Einwilligung meint dabei jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (Art. 4 Nr. 11 DSGVO). Die betroffene Person hat außerdem das Recht, ihre Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3 DSGVO). Der verantwortliche Datenverarbeiter muss nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (Art. 7 Abs. 1 DSGVO).

b) Tauglichkeit der Einwilligung im Fidesnetzwerk

aa) Erteilung einer ausdrückliche Einwilligung durch die Clients

Zunächst könnte eine ausdrückliche Einwilligung durch die Clients in Betracht kommen, die das Fidesnetzwerk zur Anbahnung, dem Abschluss und der Abwicklung von Verträgen nutzen. Eine besondere Schwierigkeit besteht jedoch schon darin, dass in offenen und dezentralen Netzwerkstrukturen – wie auch im Fidesnetzwerk – die Identitäten der Datenverarbeiter[260] grundsätzlich (zunächst) unbekannt bleiben.[261] Damit konfligieren derartige Strukturen bereits mit dem Bestimmtheitsgrundsatz, der ein wesentliches

---

[258] Ebenso *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 77 ff.
[259] *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 3.
[260] Vgl. zu den datenschutzrechtlichen Verantwortlichkeiten bereits unter D. II.
[261] So für die Blockchain schon *Schrey/Thalhofer*, NJW 2017, 1431, 1434; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 79.

Element der Einwilligung darstellt[262]. Die Einwilligungserklärung muss aber gerade dem Bestimmtheitsgrundsatz genügen, damit der Betroffene auch Kenntnis vom datenschutzrechtlich verantwortlichen Akteur hat und diesem gegenüber seine Rechte wahrnehmen kann.[263] Die dezentrale Struktur macht das Einholen von ausdrücklichen Einwilligungen daher nahezu unmöglich, zumal die Nutzer einer solchen Netzwerkstruktur in der Regel auch keine ausdrückliche Einwilligung erteilen.[264] Das gilt insoweit auch für das Fidesnetzwerk und den betroffenen Clients.

bb) Erteilung einer Globaleinwilligung durch die Clients

Ebenso dürfte eine Globaleinwilligung der Clients von Fides – etwa in der Form: *„Ich willige ein, dass sämtliche personenbezogene Daten von mir für alle Arten von Datenverarbeitungen durch alle Akteure im Fidesnetzwerk künftig dauerhaft verwendet werden dürfen."* – nicht in Betracht kommen. Unter einer Globaleinwilligung versteht man solche Einwilligungen, bei denen eine Einwilligung für verschiedene Datenverarbeitungsvorgänge einheitlich abgegeben werden soll, obwohl eine entsprechende differenzierte Einwilligung möglich wäre.[265] In diesen Fällen fehlt es regelmäßig an der Freiwilligkeit der Einwilligung.[266]

cc) Konkludente Einwilligung durch die Clients

In Betracht könnte schließlich eine konkludente Einwilligung in die Datenverarbeitung im Fidesnetzwerk kommen. Bei hinreichender Eindeutigkeit des Betroffenenwillens sind derartige Einwilligungen grundsätzlich denkbar.[267] Im Internet kann die Einwilligung durch die „Auswahl technischer Einstellungen" erfolgen.[268] In Fides könnte eine solche konkludente Einwilligung in die Datenverarbeitung durch die Full Nodes sowie den anderen Client als Vertragspartner bejaht werden.[269] Diese Einwilligung kann dann aber höchstens die konkrete Anbahnung, den konkreten Abschluss sowie die konkrete Abwicklung eines bestimmten Vertrags umfassen und deckt insoweit auch nur die darauf

---

[262] *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO, Art. 7 Rn. 63; *Klement* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 7 Rn. 67 ff.
[263] *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO, Art. 7 Rn. 63.
[264] *Hofert*, ZD 2017, 161, 164; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 79.
[265] *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO, Art. 7 Rn. 64.
[266] *Schantz*, NJW 2016, 1841, 1845; *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO, Art. 7 Rn. 64.
[267] *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO, Art. 7 Rn. 37.
[268] EG 32 S. 2 DSGVO.
[269] So auch *Böhme/Pesch,* DuD 2017, 473, 479 für die Datenverarbeitung in der Blockchain durch die Knoten.

bezogenen personenbezogenen Daten der beteiligten Clients ab.[270] Eine weitergehende Verarbeitung dürfte jedenfalls nicht umfasst sein.[271]

dd) Zusammenfassung zur Tauglichkeit der Einwilligung

Eine Einwilligung eignet sich als Rechtsgrundlage für die Datenverarbeitung im Fidesnetzwerk nur bedingt. Ob sie als Legitimationsgrundlage in Betracht kommt, wird maßgeblich von der konkreten Ausgestaltung im Hinblick auf die Anbahnung, den Abschluss sowie die Abwicklung eines Vertrages zwischen den Clients abhängen. Jedenfalls wird die Effektivität der Einwilligung erheblich durch die Größe und Dezentralität des Fidesnetzwerks beschränkt.[272]

2. Erfüllung eines Vertrages, Art. 6 Abs. 1 lit. b DSGVO

a) Allgemeine Anforderungen

Einerseits kann sich eine Rechtfertigung für die Datenverarbeitung in Fides aus der Erfüllung eines Vertrags ergeben, dessen Vertragspartei die betroffene Person – ein Client im Fidesnetzwerk – ist (Art. 6 Abs. 1 lit. b Var. 1 DSGVO). Andererseits kann auch die Durchführung vorvertraglicher Maßnahmen die Datenverarbeitung rechtfertigen, die auf Anfrage der betroffenen Person – ein Client im Fidesnetzwerk – erfolgen (Art. 6 Abs. 1 lit. b Var. 2 DSGVO).

Eine Datenverarbeitung zur Durchführung vorvertraglichen Maßnahmen setzt voraus, dass die Verarbeitung für den geplanten Abschluss eines Vertrags erforderlich sein muss. [273] Insofern wird ein besonderer Bezug zur Anbahnung des konkreten Vertragsschlusses hergestellt.[274] Die vorvertragliche Maßnahme muss auf Anfrage der betroffenen Person erfolgen. Typische Maßnahmen im Hinblick auf einen Vertragsschluss sind etwa die Erstellung eines Angebots für einen Kunden[275] oder die Reservierung eines Produkts für die betroffene Person.[276]

---

[270] So auch *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 79.
[271] Ebenso *Böhme/Pesch,* DuD 2017, 473, 479; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 79.
[272] So wohl auch generell *Schrey/Thalhofer*, NJW 2017, 1431, 1434.
[273] Vgl. EG 44 DSGVO.
[274] *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 40.
[275] *Heberlein* in: Ehmann/Selmayr, DS-GVO, Art. 6 Rn. 14.
[276] *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 40

Eine Datenverarbeitung zur Erfüllung eines Vertrags ist nur dann erforderlich, wenn sie für die Erfüllung der konkreten Vertragszwecke notwendig und nicht nur nützlich ist.[277] Das ist etwa der Fall bei der Mitteilung von Kreditkartendetails zur Abwicklung der Zahlung eines Online-Kaufs, der Anschrift des Kunden für die vertraglich bedingte Korrespondenz oder Lieferung oder der Angabe der Bankverbindung für die Geldüberweisung. [278] Erfüllung bezieht sich dabei sowohl auf sämtliche Hauptleistungspflichten als auch auf vertragliche Nebenpflichten, die mit der Hauptleistung zusammenhängen.[279]

In beiden Fällen sind die Datenverarbeitungen nur gerechtfertigt, soweit sie zum Erreichen dieser Ziele auch erforderlich sind. Dabei herrscht jedoch keine Einigkeit darüber, was als erforderlich angesehen werden muss. Während die Aufsichtsbehörden den Begriff eng auslegen und darunter nur Datenverarbeitungen verstehen, ohne die eine Erfüllung des Vertrages oder die Durchführung vorvertraglicher Maßnahmen nicht möglich ist, [280] sehen andere das Kriterium als erfüllt an, wenn nach es nach einer Interessenabwägung an einer zumutbaren Alternative fehlt[281] oder sie sogar nur objektiv sinnvoll im Sinne des Vertragskontexts ist[282]. Relevant ist vor diesem Hintergrund jedoch vielmehr die Frage, ob die Datenverarbeitung für den Betroffenen aufgrund des Vertrages erkennbar war und der Datenverarbeiter sich auf die Willensentschließung des Betroffenen aus dem Vertrag berufen kann, weil es seitens des Betroffenen treuwidrig wäre sich angesichts der vertraglichen Grundlage einer Datenverarbeitung zu verschließen. [283] Nicht erforderlich ist in diesem Zusammenhang jedenfalls eine Datenverarbeitung, die nicht unmittelbar der Vertragserfüllung dient, sondern vielmehr für das Funktionieren des vom Datenverarbeiter einseitig bestimmten Geschäftsmodells erforderlich ist.[284]

---

[277] *Heberlein* in: Ehmann/Selmayr, DS-GVO, Art. 6 Rn. 13.
[278] *Heberlein* in: Ehmann/Selmayr, DS-GVO, Art. 6 Rn. 13.
[279] *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 24.
[280] *Art. 29-Datenschutzgruppe*, WP 217, S. 23.
[281] *Buchner/Petri* in: Kühling/Buchner, DSGVO BDSG, Art. 6 Rn. 45.
[282] *Schulz* in: Gola/Heckmann, Datenschutz-Grundverordnung, Art. 6, Rn. 38.
[283] *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 32.
[284] *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 33.

b) Vorvertragliche Maßnahmen und Vertragserfüllung im Fidesnetzwerk

Da es sich bei Fides um ein Netzwerk handelt, das gerade auf die Anbahnung, den Abschluss und die Abwicklung von Verträgen angelegt ist, kann Art. 6 Abs. 1 lit. b DSGVO durchaus als Rechtsgrundlage herangezogen werden.[285] Für die Anwendbarkeit der Vorschrift kommt es nicht darauf an, dass der Vertragspartner – ein Client im Fidesnetzwerk – und der die Daten verarbeitende Verantwortliche – der Betreiber der Full Node als alleiniger Verantwortlicher oder aber als mit dem Client gemeinsam für die Verarbeitung Verantwortlicher[286] – personenidentisch sind.[287] Es reicht bereits aus, dass der Betroffene Vertragspartei ist und ein Dritter Daten in dem Umfang verarbeitet, in dem dies für die Erfüllung des Vertrags erforderlich ist.[288] Die Regelung legitimiert auch Datenverarbeitungen durch unbeteiligte Dritte, soweit diese für die Vertragsanbahnung oder Vertragserfüllung erforderlich sind.[289]

Ob Art. 6 Abs. 1 lit. b Var. 1 DSGVO (Erfüllung eines Vertrags) oder Art. 6 Abs. 1 lit. b Var. 2 DSGVO (Durchführung vorvertraglicher Maßnahmen) als taugliche Rechtsgrundlage für die Datenverarbeitung in Fides in Betracht kommt, wird maßgeblich vom Zeitpunkt und Status bestimmt, in dem sich der Vertrag zwischen den beteiligten Clients befindet.

Solange ein Contract von einer der beteiligten Vertragsparteien (noch) nicht angenommen wurde, lässt sich die Datenverarbeitung auf die Durchführung vorvertraglicher Maßnahmen stützen (Art. 6 Abs. 1 lit. b Var. 2 DSGVO). Daher lassen sich sämtliche Aktionen, die zwischen den beteiligten Clients stattfinden und vor einem Contract accept erfolgen hierunter subsumieren. Wird ein Contract offer daher von der anderen Vertragspartei abgelehnt und unterbreitet diese ein geändertes Contract offer,

---

[285] Für die klassische Blockchain so schon *Quiel*, DuD 2018, 566, 571 f.; *Schrey/Thalhofer*, NJW 2017, 1431, 1434; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 82.
[286] Siehe dazu ausführlich oben unter D. II.
[287] *Albers/Veit* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 6 Rn. 42; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 82.
[288] *Albers/Veit* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 6 Rn. 42; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 82
[289] *Albers/Veit* in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 6 Rn. 42.

findet sämtlicher Daten- und Informationsaustausch im Stadium der Durchführung vorvertraglicher Maßnahmen statt.

Erst wenn der Contract offer vom anderen Client angenommen wurde, kann in der Folge ein zivilrechtlicher Vertrag zwischen den Clients im Fidesnetzwerk zustande kommen[290] und die weitere Datenverarbeitung lässt sich auf die Erfüllung eines Vertrags stützen (Art. 6 Abs. 1 lit. b Var. 1 DSGVO).

Generell ist aber zu beachten, dass die verarbeiteten Daten auch erforderlich sein müssen. Das gilt sowohl bei der Durchführung vorvertraglicher Maßnahmen als auch bei der Erfüllung des Vertrags. Im Rahmen einer Vertragsanbahnung über das Fidesnetzwerk können dies etwa Daten sein, die für die Erstellung des Angebots eines Clients notwendig sind. Wurde ein Vertrag sodann über das Fidesnetzwerk zwischen den beteiligten Clients geschlossen, müssen etwa Information ausgetauscht werden, die für die Abwicklung einer Zahlung (z.B. Kreditkartendetails oder eine IBAN Nummer) oder aber auch für die Lieferung von Waren erforderlich sind (z.B. Lieferanschrift). Im Ergebnis kommt es hierbei auf die konkrete Ausgestaltung der über das Fidesnetzwerk angebahnten und geschlossenen Verträge an. Insofern muss für jeden einzelnen Vertrag separat geprüft werden, ob die verarbeiteten Daten erforderlich im Sinne von Art. 6 Abs. 1 lit. b DSGVO sind.

3. Wahrung berechtigter Interessen des Verantwortlichen, Art. 6 Abs. 1 lit. f DSGVO

a) Allgemeine Anforderungen

Eine Datenverarbeitung ist ebenfalls rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (Art. 6 Abs. 1 lit. f DSGVO). Der Begriff berechtigte Interessen ist dabei weit zu verstehen und umfasst in diesem Zusammenhang alle rechtlichen, wirtschaftlichen und ideellen Interessen.[291] Die Verarbeitung muss erforderlich für die Wahrung dieser Interessen sein,

[290] Zu den Einzelheiten vgl. unter C.I.
[291] EuGH, Urt. v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317, Rn. 81, 97 ff.; *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 98.

d.h. die Interessen dürfen nicht auf einem anderen, die Interessen und Rechte des Betroffenen weniger belastenden Weg erreicht werden.[292] Zentraler Inhalt der Norm ist die Vornahme einer Abwägung der Interessen des Datenverarbeiters oder eines Dritten sowie des Betroffenen.[293] Die Interessen und Rechte des Betroffenen dürfen dabei nicht überwiegen. In Abhängigkeit von der konkreten Art der verarbeiteten Daten und dem Zweck zu dem sie verarbeitet werden, ist daher Art. 6 Abs. 1 lit. f DSGVO als Rechtsgrundlage grundsätzlich denkbar.

b) Datenverarbeitung zur Wahrung berechtigter Interessen im Fidesnetzwerk

Im Fidesnetzwerk kommt ebenfalls eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO in Betracht.[294] Dabei ist ein Rückgriff auf die Norm insbesondere in solchen Fällen denkbar, in denen die Datenverarbeitung gemessen am objektiv-konkreten Maßstab nicht für die Vertragserfüllung im Sinne von Art. 6 Abs. 1 lit. b DSGVO [295] erforderlich ist.[296] Da das Fidesnetzwerk primär der Anbahnung, dem Abschluss sowie der Abwicklung von Verträgen dient, kommt eine Datenverarbeitung zur Wahrung berechtigter Interessen der Full Node Betreiber sowie der Clients vor allem dann in Betracht, wenn die Datenverarbeitung nicht im Zusammenhang mit der Vertragserfüllung steht. Das können etwa Situationen sein, in denen die personenbezogenen Daten Maßnahmen der IT-Sicherheit [297], der Rechtsverfolgung [298] oder ganz generell dem Internet der Dinge[299] zuzurechnen sind. Denkbar ist, dass die Full Node Betreiber die IP-Adressen der beteiligten Clients speichern, um etwa DoS-Angriffe abzuwehren[300] oder aber wenigstens die spätere Strafverfolgung von derartigen Angreifern zu erleichtern.[301] Der Datenverarbeitung zur Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen misst der Unionsgesetzgeber ohnehin einen sehr hohen Stellen wert

---

[292] *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 100.
[293] *Albers/Veit in:* Wolff/Brink, BeckOK Datenschutzrecht, Art. 6 Rn. 63; *Albrecht*, CR 2016, 88, 91.
[294] So schon allgemein für die Blockchain *Schrey/Thalhofer*, NJW 2017, 1431, 1434; *Quiel*, DuD 2018, 566, 572; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 84.
[295] Siehe hierzu oben unter D. IV. 2.
[296] *Quiel*, DuD 2018, 566, 572.
[297] Siehe dazu *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 119; EG 49 S. 1 DSGVO.
[298] Siehe dazu *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 123 ff.
[299] Siehe dazu *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 120 ff.
[300] Dazu *Krügel*, MMR 2017, 795, 796.
[301] Kritisch *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 119; einer generalpräventiven Wirkung wohl eher zuneigend BGH NJW 2017, 2416 Rn. 43.

bei.[302] Hier wird man daher innerhalb von Fides konkret zu analysieren haben, welche personenbezogenen Daten möglicherweise für die Rechtsverfolgung erforderlich sind. Ebenso lassen sich mit den im Fidesnetzwerk verarbeiteten personenbezogenen Daten umfangreiche Big-Data Analysen durchführen, um Wahrscheinlichkeiten, Korrelationen und Muster aufzuspüren.[303] Werden solche Datenverarbeitungen für derartige Zwecke innerhalb von Fides durchgeführt, ist detailliert zu prüfen, ob die Datenverarbeitungen erforderlich sind und die Interessen und Grundrechte der betroffenen Personen nicht überwiegen. Auch hier kommt es daher auf die konkrete Ausgestaltung im Einzelfall an.

4. Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 9 DSGVO

a) Allgemeine Anforderungen

Eine Datenverarbeitung besonderer Kategorien personenbezogener Daten ist nur unter den speziellen Voraussetzungen von Art. 9 DSGVO möglich. Dabei handelt es sich um personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung (Art. 9 Abs. 1 DSGVO). Die Verarbeitung dieser besonderen Kategorien von Daten ist nur unter den engen Voraussetzungen von Art. 9 Abs. 2 DSGVO zulässig, d.h. unter anderem wenn eine Einwilligung durch den Betroffenen erteilt wurde (Art. 9 Abs. 2 lit. a DSGVO), die Verarbeitung für Zwecke der Gesundheitsvorsorge (Art. 9 Abs. 2 lit. h DSGVO) oder die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Art. 9 Abs. 2 lit. i DSGVO) erforderlich ist. Der Grund liegt in den besonderen Diskriminierungsrisiken, die von diesen Daten für die Betroffenen ausgehen.[304]

b) Datenverarbeitung besonderer Kategorien personenbezogener Daten

Sofern bei der Anbahnung, dem Abschluss sowie der Abwicklung von Verträgen über das Fidesnetzwerk besondere Kategorien personenbezogener Daten betroffen sind, müssen sich derartige Datenverarbeitungen am Maßstab von Art. 9 Abs. 2 DSGVO messen lassen.

---

[302] *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 123; EuGH, Urt. v. 4.5.2017 – C-13/16, ECLI:EU:C:2017:336, Rn. 29.
[303] *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 Rn. 122.
[304] *Petri* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 9 Rn. 10; *Weichert* in: Kühling/Buchner, DSGVO BDSG, Art. 9 Rn. 15.

Denkbar wäre, dass über Fides Verträge zu medizinischen oder gesundheitlichen Dienstleistungen abgewickelt werden. In diesen Fällen müssten die am Vertrag beteiligten Clients eine Einwilligung erteilen (Art. 9 Abs. 2 lit. a DSGVO) oder aber die Datenverarbeitung lässt sich aufgrund einer Datenverarbeitung zur Gesundheitsvorsorge (Art. 9 Abs. 2 lit. h DSGVO) oder aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Art. 9 Abs. 2 lit. i DSGVO) legitimieren. Es kommt somit auf den Einzelfall sowie die konkrete inhaltliche Ausgestaltung des maßgeblichen Vertrags an, der über Fides geschlossen und abgewickelt werden soll.

5. Zusammenfassung zur Rechtmäßigkeit der Datenverarbeitung

Als maßgebliche Rechtsgrundlage für die Datenverarbeitung eignet sich im Fidesnetzwerk die Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO), da Fides für die Anbahnung, den Abschluss sowie die Abwicklung von Verträgen konzipiert ist.[305] Daneben kommt aber auch die Wahrung berechtigter Interessen in Betracht (Art. 6 Abs. 1 lit. f DSGVO), wobei dabei insbesondere solche Datenverarbeitungen adressiert werden, bei denen die personenbezogenen Daten nicht im unmittelbaren Zusammenhang mit der Vertragserfüllung stehen (z.B. Maßnahmen der IT-Sicherheit oder Rechtsverfolgung).[306] Die Einwilligung eignet sich im Fidesnetzwerk nur bedingt als taugliche Rechtsgrundlage.[307] Werden in Fides besondere Kategorien personenbezogener Daten verarbeitet sind schließlich auch die spezifischen Voraussetzungen von Art. 9 Abs. 2 DSGVO zu berücksichtigen.[308] Wird Fides mithilfe von LoRaWAN genutzt, ergibt sich hinsichtlich der Rechtmäßigkeit der Datenverarbeitung keine abweichende Bewertung.

V. Ausgewählte Pflichten des Datenverarbeiters

Die Verarbeitung personenbezogener Daten hat als weitere Konsequenz zur Folge, dass dem Datenverarbeiter umfangreiche Pflichten auferlegt werden. Die Rechte und Pflichten von Verantwortlichen und Auftragsverarbeitern werden umfassend in den Art. 24 – Art. 43 DSGVO geregelt. Im Folgenden werden ausgewählte und besonders relevante Regelungen für das Fidesnetzwerk dargestellt, um die spezifischen Anforderungen auf Fides zu übertragen. Dabei sind Art. 25 DSGVO (Datenschutz durch Technikgestaltung

[305] Siehe dazu im Detail unter D. IV. 2.
[306] Siehe dazu im Detail unter D. IV. 3.
[307] Siehe dazu im Detail unter D. IV. 1.
[308] Siehe dazu im Detail unter D. IV. 4.

und durch datenschutzfreundliche Voreinstellungen) sowie Art. 32 DSGVO (Sicherheit der Verarbeitung) von besonderer Relevanz.

1. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (privacy by design und privacy by default), Art. 25 DSGVO

a) Allgemeine Anforderungen

Art. 25 DSGVO normiert erstmalig und umfangreich das Grundprinzip „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen". [309] Der Verantwortliche [310] muss gemäß Art. 25 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen treffen, um die Datenschutzgrundsätze und die Anforderungen der DSGVO wirksam umzusetzen. Daneben muss er gewährleisten, dass durch Voreinstellung die personenbezogenen Daten nur im Rahmen ihrer Erforderlichkeit für den Verarbeitungszweck verarbeitet werden (Art. 25 Abs. 2 DSGVO). [311] Das Ziel der Vorschrift ist ein in die Verarbeitung personenbezogener Daten eingebauter Datenschutz, sodass datenschutzrechtliche Grundsätze proaktiv in Datenverarbeitungssystemen verankert werden.[312] Gleichwohl beschränkt sich die Regelung nicht nur ausschließlich auf den technischen Datenschutz, sondern nimmt vielmehr eine ganzheitliche Systemgestaltung in den Blick, die etwa auch organisatorische Prozesse, vertragliche Zusammenhänge und Geschäftsmodelle berücksichtigt.[313]

Art. 25 DSGVO konkretisiert die Anforderungen des Art. 24 DSGVO zur Verantwortung, um die Einhaltung der DSGVO sicherzustellen und den Nachweis dafür zu erbringen.[314] Adressat der Regelung ist ausschließlich der Verantwortliche.[315] Die Norm verfolgt dabei einen holistischen Ansatz und wird somit unter einer gestalterischen und operativen Perspektive zu einer der umfassendsten Normen der DSGVO. [316] Um das Ziel der

---

[309] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 1.
[310] Vgl. hierzu ausführlich unter D. II.
[311] Vgl. zum Verhältnis von Art. 25 Abs. 1 und Abs. 2 bei *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 24.
[312] *Mantz* in: Sydow/Marsch, DSGVO, Art. 25 Rn. 2; *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 1.
[313] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 7.
[314] Umfangreich *Hartung* in: Kühling/Buchner, DSGVO, Art. 25 Rn. 9 f.
[315] Ausführlich dazu *Mantz* in: Sydow/Marsch, DSGVO, Art. 25 Rn. 16 f. sowie *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 20 ff.
[316] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 15.

Datenverarbeitung mit eingebauten Datenschutz effektiv zu erreichen, erstreckt sich die in Art. 25 Abs. 1 DSGVO normierte Gestaltungsanforderung auf die gesamte Verarbeitung einschließlich der organisatorischen Prozesse sowie der rechtlichen Ausgestaltung für den konkreten Fall.[317] Die Anforderungen des „Datenschutz by Design"[318] erfordern, dass frühzeitig Einfluss auf die Gestaltung der Verarbeitung im Sinne der Datenschutzanforderungen genommen wird.[319] Bei der Eigenentwicklung eines Datenverarbeitungssystems, das personenbezogene Daten verarbeitet, müssen also bereits bei der Konzeption des informationstechnischen Systems sowie der Verfahrensabläufe die Anforderungen der DSGVO einfließen und bei der konkreten Umsetzung berücksichtigt werden.

b) Privacy by design und privacy by default im Fidesnetzwerk

Das Verhältnis von dezentralen und offenen Netzwerkstrukturen, wie sie für Fides exemplarisch ist, verhält sich zum Grundsatz des Datenschutzschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ambivalent.[320] Teilweise werden solche Strukturen, die sich durch Merkmale wie Verschlüsselung und Pseudonymisierung generell auszeichnen, schon aus sich heraus als die Verwirklichung von privacy by design und privacy by default angesehen.[321] Dies vermag jedoch nur begrenzt zu überzeugen,[322] da sich Art. 25 DSGVO auf den gesamten Datenverarbeitungsprozess bezieht und nicht nur einzelne Teilaspekte der Datenverarbeitung adressiert.[323] Ebenso ist es nicht einfach, die Frage zu beantworten, wer in einer derartigen dezentralen Netzwerkstruktur überhaupt in der Lage ist, den Grundsatz zu beachten.[324]

---

[317] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 16.
[318] Vgl. zur Abgrenzung von „Privacy by Design" und „Datenschutz by Design" *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 23 ff.
[319] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 18.
[320] So schon *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 90; *Quiel*, DuD 2018, 566, 570; *Böhme/Pesch*, DuD 2017, 473, 480; *Guggenberger*, ZD 2017, 49 f.
[321] Für die Blockchain-Technologie so etwa *Guggenberger*, ZD 2017, 49 f.; *Bechtolt/Vogt*, ZD 2018, 66, 71.
[322] Ebenso *Quiel*, DuD 2018, 566, 570.
[323] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 25 Rn. 16; in diese Richtung auch *Finck*, IDPL 2019, 78, 92.
[324] Nach *Quiel*, DuD 2018, 566, 570 kommt jedenfalls in klassischen Blockchain-Strukturen nur ein Intermediär in Betracht, der überhaupt in der Lage ist den Grundsatz „privacy by Design" zu beachten. Sofern auf zulassungsbeschränkten öffentlichen Blockchains Daten verarbeitet werden, sei davon auszugehen, dass die Verpflichtung (nach Art. 25 DSGVO) entweder mangels eines Verantwortlichen oder mangels Verhältnismäßigkeit solcher Verpflichtungen gegenüber Privaten nicht greifen.

Gleichwohl weist das Fidesnetzwerk erste gute Ansätze zur Realisierung von Datenschutz durch Technikgestaltung auf, da zahlreiche technische Mechanismen implementiert werden, welche die Datenschutzgrundsätze umsetzen und die notwendigen Garantien in die Verarbeitung aufnehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen. So werden die relevanten Daten und Informationen in Fides generell nur verschlüsselt gespeichert und übertragen. Das gilt sowohl für die Full Nodes, als auch die Clients. Die für die Anbahnung, den Abschluss sowie die Abwicklung von Verträgen notwendigen Daten werden dezentral bei den Clients gespeichert. Daneben teilen sich die Full Nodes die zu speichernden Informationen untereinander auf, sodass jede Full Node für andere Contracts und Templates zuständig ist. Somit gibt es keine einheitliche und zentrale Full Node, die über sämtliche Contracts und Templates verfügen kann. Die Verbindung der Full Nodes untereinander erfolgt über eine Ringstruktur, sodass jedem Full Node immer nur der „Vorgänger" und der „Nachfolger" bekannt sind. Die Integrität der in den Full Nodes gespeicherten Inhalte kann darüber hinaus zusätzlich durch Zertifikate abgesichert werden. Ebenso wird die Integrität der Daten durch eine digitale Signatur gewährleistet. Außenstehende haben nur einen eingeschränkten Lesezugriffe auf die vorhandenen Daten. Ein Schreibzugriff wird unterbunden. Daneben erfordert Fides auch keine Etablierung einer dauerhaften zeitlichen Beziehung zwischen den Clients, wie das für Blockchain-Systeme sonst üblich ist.[325] Die Clients speichern ihre Daten lokal und damit dezentral ab. Alle Informationen zum Template und Contract werden auf den Endgeräten der beteiligten Clients und im zuständigen Full Node ausschließlich verschlüsselt gespeichert. Eine Entschlüsselung ist nur auf den Endgeräten der Clients möglich. Ebenso ist es technisch ausgeschlossen, dass die Full Nodes beliebig durchsucht werden, sodass Transaktionen nur aufgefunden werden können, sofern man über den Hash oder weitere Informationen zur Transaktion verfügt. Ferner kennt auch nur der Full Node am Eintrittspunkt eines Clients in die Ringstruktur die IP-Adresse des Clients, da diese wenigstens für den Daten- und Informationsaustausch bekannt sein muss. Anderen Full Nodes oder Clients ist damit die IP-Adresse unbekannt. Die Full Nodes agieren als Mittlerinstanz zwischen den beteiligten Clients, sodass sie auch als Datentreuhänder angesehen werden können. Auf die Verarbeitung der auf dem Endgerät bei den Clients

[325] Vgl. zur dauerhaften Speicherung personenbezogener Daten bei der klassischen Blockchain-Technologie *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 90.

gespeicherten Daten haben die Full Nodes keinen Einfluss. Die zu den Accounts der Clients gehörenden personenbezogenen Daten werden ausschließlich auf dem Endgerät gespeichert. Die Trennung von verschiedenen Ringstrukturen, die für jeweils unterschiedliche Zwecke genutzt werden können, ermöglichen schließlich die Förderung des Zweckbindungsgrundsatzes.[326]

Im Fidesnetzwerk sind bereits jetzt zahlreiche technische Mechanismen implementiert, die dem Grundsatz des Datenschutzes durch Technikgestaltung sowie datenschutzfreundliche Voreinstellungen dienen. Inwiefern weitere Mechanismen integriert werden müssen, hängt aber auch von der inhaltlichen Qualität derjenigen Verträge ab, die über Fides angebahnt, geschlossen und abgewickelt werden. So ist etwa bei Verträgen denkbar, die besondere Kategorien personenbezogener Daten zum Gegenstand haben und über Fides abgeschlossen werden, dass weitergehende technische und organisatorische Maßnahmen integriert werden müssen. Auch hier kommt es auf die konkrete Ausgestaltung im Einzelfall an.[327] Wird Fides mithilfe von LoRaWAN genutzt, dann ist auch diesbezüglich auf Datenschutz durch Technik sowie datenschutzfreundliche Voreinstellungen zu achten sowie zu implementieren.

2. Sicherheit der (Daten-)Verarbeitung, Art. 32 DSGVO

a) Allgemeine Anforderungen

Art. 32 DSGVO regelt die Pflicht des Verantwortlichen und des Auftragsverarbeiters, bestimmte technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau im Hinblick auf die verarbeiteten personenbezogenen Daten zu gewährleisten.[328] Der Fokus der Norm ist die Sicherheit der Datenverarbeitung. Die Norm konkretisiert insbesondere den Datenschutzgrundsatz „Integrität und Vertraulichkeit“ aus Art. 5 Abs. 1 lit. f DSGVO – allerdings nicht ausschließlich[329] – und stellt insoweit auch kein neues Instrument dar, sondern folgt dem bisherigen Art. 17 Abs. 1 DSRL.[330]

---

[326] Vgl. zum Zweckbindungsgrundsatz *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rn. 63 ff.
[327] Ebenso im Kontext der Blockchain-Technologie *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 90.
[328] *Mantz* in: Sydow/Marsch, DSGVO, Art. 32 Rn. 1.
[329] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 Rn. 13.
[330] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 Rn. 1.

Art. 32 Abs. 1 DSGVO stellt die Kernaussage der Norm dar und verpflichtet insbesondere die Verantwortlichen zum Treffen von geeigneten technischen und organisatorischen Maßnahmen, die beispielhaft in Abs. 1 lit. a – d erläutert werden. Die Vorschrift regelt näher, wie das Ziel der Verarbeitungssicherheit erreicht werden kann. Um diesbezüglich festzulegen, welche Maßnahmen konkret geeignet sind, gibt Art. 32 Abs. 1 DSGVO – ähnlich wie bereits Art. 25 Abs. 1 DSGVO – zunächst vier für die Abwägung relevante Kriterien vor. Neben dem Risiko mit Eintrittswahrscheinlichkeit und Schwere sind der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung in die Abwägung einzubeziehen.[331] Bereits an dieser Stelle sind Verantwortliche aufgefordert zu dokumentieren, auf welcher Basis sie zu der Auswahl der Maßnahmen gekommen sind und wie sie die Abwägung der genannten Kriterien vorgenommen haben.[332] Es ist zu erwarten, dass der Europäische Datenschutzausschuss (EDSA) sowie die Datenschutzaufsichtsbehörden oder das BSI entsprechende Hilfestellungen herausgeben werden, an denen sich datenschutzrechtlich Verantwortliche orientieren können. Nachdem das relevante Schutzniveau festgestellt wurde, sind sodann die geeigneten technischen und organisatorischen Maßnahmen zu treffen. Diesbezüglich überlässt die DSGVO dem Verantwortlichen die konkrete Auswahl der Mittel. Als Hilfestellung dient jedoch die Aufzählung der in Abs. 1 genannten beispielhaften Maßnahmen. In Betracht kommen daher u.a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten sowie Maßnahmen, welche die Integrität der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

Die Pseudonymisierung wird in Art. 4 Nr. 5 DSGVO legal definiert. Demnach meint Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Es handelt sich insofern um eine technisch-organisatorische

[331] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 Rn. 19.
[332] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 Rn. 20.

Maßnahme, die risikoreduzierend wirkt und damit zur Sicherheit der Verarbeitung beitragen kann.[333] Für eine taugliche Pseudonymisierung kommen beispielsweise geeignete Hashwert- oder Verschlüsselungsverfahren, Referenztabellen oder Treuhänder in Betracht.[334]

Mit Verschlüsselung meint die DSGVO Maßnahmen, die geeignet sind, personenbezogene Daten für alle unbefugten Personen unzugänglich zu machen.[335] Es handelt sich also um einen Vorgang, dem eine klar lesbare Information mit Hilfe eines kryptographischen Verfahrens in eine „unleserliche" Zeichenfolge umgewandelt wird.[336] So sind ganz konkret die Verfahren der Kryptographie gemäß dem Stand der Technik ein wichtiger Mechanismus, um Informationssicherheit zu implementieren.[337] Es sind deshalb auch Daten auf „smarten" Geräten, die als Teil des Internet der Dinge personenbezogene Daten erheben und übermitteln, stets zu verschlüsseln, sofern Dritte physisch Zugriff auf diese Geräte haben können. Bei der Übermittlung von Daten sollte darum immer eine Ende-zu-Ende-Transportverschlüsselung verwendet werden, was auch für sämtliche IoT-Geräte gilt.[338]

Für die Integrität sind Daten insbesondere gegen unbeabsichtigte Zerstörung und unbeabsichtigte Schädigung zu schützen.[339] Hier kommen Maßnahmen wie Zutritts-, Zugangs-, Zugriffs-, Weitergabe- oder Eingabekontrolle sowie eine kontinuierliche Datensicherung in Betracht.[340]

b) Sicherheit der (Daten-)Verarbeitung im Fidesnetzwerk, insbesondere bei der Nutzung von Fides mithilfe von LoRaWAN

Im Fidesnetzwerk sind die Vorgaben über die Sicherheit der Datenverarbeitung und damit die Sicherheit personenbezogener Daten ebenfalls zu ermöglichen. Dabei sind bereits jetzt gute Ansätze erkennbar, die der Sicherheit der Datenverarbeitung besonders zuträglich sind. Dies bedingt bereits die grundlegende dezentrale Struktur von Fides,

---

[333] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 Rn. 34.
[334] *Art. 29-Datenschutzgruppe*, WP 216, S. 24 ff.
[335] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 Rn. 35.
[336] *Mantz in:* Sydow/Marsch, DSGVO, Art. 32 Rn. 11.
[337] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 Rn. 35.
[338] *Mantz in:* Sydow/Marsch, DSGVO, Art. 32 Rn. 11.
[339] *Mantz in:* Sydow/Marsch, DSGVO, Art. 32 Rn. 15.
[340] *Mantz in:* Sydow/Marsch, DSGVO, Art. 32 Rn. 15.

welche sich die Pseudonymisierung und die Verschlüsselung von Daten als zwei wesentlichen Kernelementen zunutze macht. [341] Pseudonymisierung und Verschlüsselung stellen dabei gerade technisch-organisatorische Maßnahmen im Sinne von Art. 32 Abs. 1 lit. a DSGVO dar.[342] Es ist jedoch gleichzeitig zu berücksichtigen, dass einige Ausprägungen einer derartigen dezentralen Struktur, die sich kryptographischen Verfahren zur Verschlüsselung bedient, in Konflikt mit den Betroffenenrechten geraten können.[343] Was auf der einen Seite aus technischer Sicht der Integritätssicherung dient, kann auf der anderen Seite dem Recht auf Berichtigung (Art. 16 DSGVO) oder dem Recht auf Löschung (Art. 17 DSGVO) entgegenstehen.[344] Daher sind weitergehende technische Mechanismen zu implementieren, welche die Einhaltung der weiteren datenschutzrechtlichen Anforderungen ermöglichen.[345]

Gleichwohl werden schon heute in Fides die maßgeblichen Transaktionsdaten verschlüsselt in der Full Node gespeichert, sodass nur die beteiligten Clients die Daten überhaupt entschlüsseln können. Die Integrität der in den Full Nodes gespeicherten Inhalte wird durch eine digitale Signatur gewährleistet und kann darüber hinaus zusätzlich durch Zertifikate abgesichert werden. Ebenso ist im Fidesnetzwerk für die beteiligten Clients nur ein eingeschränkter Schreib- und Lesezugriff auf die Daten möglich. Schließlich werden die aktuell bearbeiteten Contracts verschlüsselt in der Full Node gespeichert und ein direkter Kontakt zwischen den beteiligten Clients erfolgt nicht.

Wird Fides in Regionen ohne Netzinfrastruktur mithilfe von LoRaWAN betrieben, sind dessen technischer Besonderheiten bei der Bewertung der Sicherheit der Datenverarbeitung zu berücksichtigen. So müssen die hinzutretenden Komponenten (z.B. Raspberry Pi, LoRaWAN-Gateway, Funkübertragung) ihrerseits derart beschaffen sein, dass die Sicherheit der Datenverarbeitung gewährleistet wird. Dabei sind besondere Sicherheitsanforderungen an die Funkübertragung der Daten zu stellen, sodass diese nicht unbefugt abgegriffen werden können. Welche konkreten Maßnahmen hierbei im

---

[341] Ähnlich so für die Blockchain-Technologie *Ritter* in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 32 Rn. 57.
[342] Ebenso schon für die Blockchain-Technologie *Quiel*, DuD 2018, 566, 568.
[343] *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 Rn. 40.
[344] *Bechtolf/Vogt*, ZD 2018, 66, 69.
[345] Siehe dazu *Ritter* in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 32 Rn. 57 mwN.

Einzelfall zu treffen sind, hängt von einer umfassenden Analyse dieser besonderen Situation ab.

VI. Ausgewählte Betroffenenrechte

Die Verarbeitung personenbezogener Daten hat zur Folge, dass dem Betroffenen umfangreiche Rechte eingeräumt werden (sog. „Betroffenenrechte"). Dies ist so schon verfassungsrechtlich verankert und folgt einerseits auf europäischer Ebene unmittelbar aus Art. 8 Abs. 2 S. 2 GRCh und andererseits im nationalen Recht aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG (Recht auf informationelle Selbstbestimmung). [346] Grundlegende Voraussetzung für die Wahrnehmung der verfassungsrechtlich verbürgten Rechte ist es, dass der Betroffene weiß, wer wo welche Daten über ihn erhebt, verarbeitet, nutzt oder übermittelt. Erst diese positive Kenntnis versetzt die Betroffenen in die Lage zu entscheiden, ob sie eine Verarbeitung wollen oder nicht. Damit kann dem Schutzziel der Transparenz[347] besonders wirksam zur Geltung verholfen werden.[348] Ganz konkret stellt der Auskunftsanspruch etwa sicher, dass der Betroffene sich gegen eine rechtswidrige Datenverarbeitung zur Wehr setzen kann, denn nur derjenige, der überhaupt weiß, dass seine personenbezogenen Daten verarbeitet werden, kann sich dagegen entsprechend zur Wehr setzen. [349] Für das Auskunfts- und Berichtigungsrecht folgt dies bereits unmittelbar aus Art. 8 Abs. 2 S. 2 GRCh, sodass die Norm dem Betroffenen einen unmittelbaren grundrechtlichen Transparenzanspruch einräumt.[350]

Diese und weitere Betroffenenrechte werden einfachgesetzlich in der DSGVO umfassend ausgestaltet. Die einschlägigen Auskunfts-, Berichtigungs-, Löschungs-, Sperrungs-, Übertragbarkeits- und Widerspruchsrechte sollen es ermöglichen, über die Preisgabe, Verwertung und Verweigerung persönlicher Daten selbstbestimmt zu entscheiden, wenn es entsprechende normative Entscheidungsspielräume gibt. [351] Die Informations- und Benachrichtigungsrechte und -pflichten der DSGVO konkretisieren damit die

---

[346] Vgl. zum deutschen Recht grundlegend BVerfGE 65, 1, 46; vgl. zum europäischen Recht grundlegend EuGH, Urt. v. 12.11.1969 – 29/69, Rn. 7 sowie *Kingreen* in: Calliess/Ruffert, EUV/AEUV, GRCh Art. 8 Rn. 2 mwN.
[347] Vgl. oben unter D. III. 2.
[348] Vgl. zur Transparenz schon *Bizer*, DuD 2007, 350, 353 ff. sowie *Marsch*, Das europäische Datenschutzgrundrecht, S. 96 ff.
[349] *Jarass*, GRCh, Art. 8 Rn. 16; *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, GRCh Art. 8 Rn. 38.
[350] *Bretthauer* in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, S. 21.
[351] So auch schon *Roßnagel*, Handbuch Datenschutzrecht, S. 547.

primärrechtlichen Garantien aus Art. 8 GRCh sowie Art. 16 AEUV, sodass die DSGVO die Grundrechtsausübung durch umfangreiche einfachgesetzliche Regelungen absichert.[352]

Für die vorliegende Studie kann nicht auf alle Betroffenenrechte der DSGVO eingegangen werden, sodass die für das Fidesnetzwerk besonders gewichtigen Rechtsgrundlagen analysiert werden. Dabei handelt es sich insbesondere um das Recht auf Auskunft (Art. 15 DSGVO) sowie die Rechte auf Berichtigung (Art. 16 DSGVO) und Löschung (Art. 17 DSGVO). Gleichwohl wird deutlich werden, dass die Realisierung von Betroffenenrechten in dezentralen Netzwerkstrukturen wie dem Fidesnetzwerk mit erheblichen Herausforderungen behaftet ist.[353] Wird Fides mithilfe von LoRaWAN genutzt, ergibt sich keine andere rechtliche Bewertung, da LoRaWAN lediglich den Transportweg der Daten ändert. Das hat auf die Ausübung von Betroffenenrechten keine Auswirkung.

1. Allgemeine Anforderungen der Betroffenenrechte

a) Das Recht auf Auskunft, Art. 15 DSGVO

Das Auskunftsrecht nach Art. 15 DSGVO ist das zentrale Recht zur Schaffung von Transparenz. [354] Es ermöglicht den betroffenen Personen die Prüfung, ob der Verantwortliche Daten über sie verarbeitet und versetzt sie somit erst überhaupt in die Lage, die Verarbeitung dieser Daten durch Geltendmachung ihrer Rechte – insbesondere das Recht auf Berichtigung (Art. 16 DSGVO) und das Recht auf Löschung (Art. 17 DSGVO) – auszuüben.[355] Grundsätzlich ist das Auskunftsrecht nach Art. 15 Abs. 1 DSGVO ein abgestuftes Auskunftsrecht.[356] In einem ersten Schritt hat die betroffene Person generell das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten überhaupt verarbeitet werden. Ist das nicht der Fall, so ist gleichwohl eine Negativauskunft notwendig, d.h. das der Verantwortliche keine

---

[352] *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 12 Rn. 3.
[353] Bei der klassischen Blockchain-Technologie wird davon ausgegangen, dass die Betroffenenrechte generell ins Leere laufen. So etwa *Pesch*, Blockchain, Smart Contracts und Datenschutz in: Fries/Paal, Smart Contracts, S. 13, 19; *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 86; differenzierend hingegen *Bechtolf/Vogt*, ZD 2018, 66, 69 f.
[354] *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 15 Rn. 1; *Specht* in: Sydow/Marsch, DSGVO, Art. 15 Rn. 1; *Datenschutzkonferenz*, Kurzpapier Nr. 6 – Auskunftsrecht der betroffenen Person, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf, zuletzt abgerufen am 29.12.2022.
[355] *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 15 Rn. 1.
[356] *Datenschutzkonferenz*, Kurzpapier Nr. 6 – Auskunftsrecht der betroffenen Person, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf, zuletzt abgerufen am 29.12.2022.

Daten zu dieser Person verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert hat.[357] Sind personenbezogene Daten anonymisiert, empfiehlt sich zumindest eine Informierung über den Anonymisierungsprozess und das dahinterstehende Verfahren, da so gegenüber der betroffenen Person eine transparente Datenverarbeitung erfolgt.[358] Pseudonymisierte Daten (vgl. Art. 4 Nr. 5 DSGVO) sind dagegen stets personenbezogen und unterliegen deshalb auch inhaltlich dem Auskunftsrecht der betroffenen Person.[359] Das Auskunftsrecht umfasst alle Daten, die zum Zeitpunkt des Auskunftsverlangens, beim Verantwortlichen vorhanden sind.[360] Eine Ausnahme für bestimmte Datenkategorien sieht Art. 15 DSGVO nicht vor.[361]

b) Das Recht auf Berichtigung, Art. 16 DSGVO

Der Grundsatz der Richtigkeit der erhobenen und verarbeiteten Daten[362] (vgl. Art. 5 Abs. 1 lit. d DSGVO) wird durch das Recht auf Berichtigung nach Art. 16 DSGVO ausgefüllt, wobei dieses Recht zwei Bestandteile hat. Die betroffene Person kann sowohl Korrektur unrichtiger Daten (Art. 16 S. 1 DSGVO) als auch die Vervollständigung oder Ergänzung unvollständiger Daten (Art. 16 S. 2 DSGVO) verlangen.

Unrichtig sind Daten, die im Zeitpunkt der Geltendmachung des Berichtigungsanspruchs nicht mit der Tatsachenlage übereinstimmen, wobei zentraler Maßstab der Unrichtigkeit der objektive Aussagegehalt der Daten ist, unabhängig davon, was diese nach subjektiver Auffassung des Verantwortlichen aussagen.[363] Klassische Beispiele hierfür sind etwa falsche Namens- oder Adressangaben einer natürlichen Person. Demgegenüber sind Daten unvollständig, die zwar für sich genommen richtig sind, in der Gesamtheit aber eine objektiv falsche Aussage treffen oder in anderen Worten lückenhaft und dadurch objektiv

---

[357] *Datenschutzkonferenz*, Kurzpapier Nr. 6 – Auskunftsrecht der betroffenen Person, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf, zuletzt abgerufen am 29.12.2022; *Bäcker* in: Kühling/Buchner, DSGVO, Art. 15 Rn. 7.
[358] *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 15 Rn. 12.
[359] Problematisch ist die praktische Umsetzung des Auskunftsrechts bei Nutzung der Blockchain-Technologie, bei der der Verantwortliche aufgrund der besonderen Datenverarbeitung nicht weiß, ob personenbezogene Daten verarbeitet werden oder nicht. Vgl. dazu *Finck*, EDPL 2018, 17, 29 f.
[360] Ausführlich dazu *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 15 Rn. 13 ff.
[361] *Bäcker* in: Kühling/Buchner, DSGVO, Art. 15 Rn. 8; aA *Walter*, DSRITB 2016, 367, 381.
[362] Vgl. dazu oben unter D. III. 3.
[363] *Reif* in: Gola/Heckmann, DS-GVO – BDSG, DS-GVO Art. 16 Rn. 13 mwN.

missverständlich sind.[364] Ob Daten voll- bzw. unvollständig sind, lässt sich nur vor dem Hintergrund ihres konkreten Verwendungszusammenhangs klären.[365]

c) Das Recht auf Löschung, Art. 17 DSGVO

Art. 17 Abs. 1 DSGVO normiert das Recht auf Löschung und benennt diejenigen Fälle, in denen eine Löschung unverzüglich erfolgen muss.[366] Eine Verlängerungsmöglichkeit der Frist besteht nicht, sodass die erforderlichen Maßnahmen ohne schuldhaftes Zögern zu treffen sind. Gleichwohl ist dem Verantwortlichen eine angemessene Frist zur Prüfung einzuräumen.[367] Das mit dem Löschungsanspruch der betroffenen Person verbundene „Recht auf Vergessenwerden" wird erstmalig ausdrücklich in Art. 17 Abs. 2 DSGVO normiert. [368] Art. 17 Abs. 3 DSGVO statuiert schließlich Ausnahmen von der Löschungspflicht, soweit eine Verarbeitung personenbezogener Daten erforderlich ist. Das Recht auf Löschung nach Art. 17 DSGVO ermöglicht den Betroffenen somit steuernd auf die Verarbeitung ihrer Daten einzuwirken und deren Löschung zu erzwingen.[369]

Der Begriff der (datenschutzrechtlichen) Löschung wird in der DSGVO selbst nicht näher erläutert. [370] Allerdings können Daten beispielsweise durch eine ordnungsgemäße Vernichtung des betreffenden Datenträgers oder durch (mehrfaches) Überschreiben gelöscht werden (physikalische Löschung).[371] Da sich durch den technischen Fortschritt die Anforderungen an eine datenschutzkonforme Löschung ständig verändern, muss immer wieder neu geprüft werden, welche Maßnahmen effektiv in Betracht kommen. Die Möglichkeit der Wiederherstellung durch entsprechende Spezialprogramme darf dabei nicht außer Acht gelassen werden. [372] Der Einsatz spezieller Löschsoftware ist mit verhältnismäßigem Aufwand möglich und daher in aller Regel auch geboten.[373]

---

[364] *Kamann/Braun* in: Ehmann/Selmayr, DS-GVO, Art. 16 Rn. 36.
[365] *Reif* in: Gola/Heckmann, DS-GVO – BDSG, DS-GVO Art. 16 Rn. 16; *Kamann/Braun* in: Ehmann/Selmayr, DS-GVO, Art. 16 Rn. 36.
[366] Vgl. allgemein dazu *Hunzinger*, Das Löschen im Datenschutzrecht, Baden-Baden 2018.
[367] *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 17 Rn. 8.
[368] Vgl. zum „Recht auf Vergessenwerden" etwa *Becker*, Das Recht auf Vergessenwerden.
[369] *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 17 Rn. 1.
[370] Vgl. aber etwa § 3 Abs. 5 Nr. 5 BDSG aF, der vom „Unkenntlichmachen gespeicherter personenbezogener Daten" spricht.
[371] *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 17 Rn. 5.
[372] *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 17 Rn. 5; aA *Paal* in: Paal/Pauly, DSGVO BDSG, Art. 17 Rn. 30 mwN.
[373] Ausführlich dazu *Herbst* in: Kühling/Buchner, DSGVO, Art. 17 Rn. 38 mwN.

2. Betroffenenrechte im Fidesnetzwerk

Auch in Fides müssen die Betroffenenrechte wirksam und effektiv ausgeübt werden können. Sie können daher von der betroffenen Person als Anspruchsteller gegenüber dem Verantwortlichen (vgl. Art. 4 Nr. 7 DSGVO) als Anspruchsgegner wahrgenommen werden. In einer dezentralen und offenen Fidesnetzwerkstruktur ist die klare Zuschreibung von Verantwortlichkeiten komplex[374], sodass die Benennung eines Anspruchsgegners nicht offensichtlich ist. Im Fidesnetzwerk werden in der Regel die Clients die betroffene Person sein, da sie mithilfe der Full Nodes die Verträge anbahnen, abschließen und abwickeln. Daher werden vor allem personenbezogene Daten der Clients verarbeitet[375] , sodass diese als Anspruchsteller der Betroffenenrechte primär in Betracht kommen.

a) Full Node Betreiber als Anspruchsgegner bei Kenntnis

Sofern man die Full Node Betreiber als datenschutzrechtlich verantwortliche Akteure ansieht[376], können die Clients ihre Rechte ihnen gegenüber geltend machen. Maßgeblich und entscheidend ist daher, ob jeder Client den für ihn zuständigen Full Node identifizieren kann. Es kommt daher maßgeblich auf die konkrete Ausgestaltung im Fidesnetzwerk an und welche Teilnehmer von welchen anderen Teilnehmern im Netzwerk Kenntnis haben.

b) Full Node Betreiber als Anspruchsgegner bei Unkenntnis

Das Fidesnetzwerk besteht generell aus einer dezentralen und offenen Struktur, die das Hinzutreten und Hinweggehen von Clients sowie von Full Nodes jederzeit ermöglicht. Sofern die Betreiber der einzelnen Full Nodes den Clients daher nicht bekannt sind[377], bedingt die fehlende Transparenz, dass dem normativen Transparenzverständnis der DSGVO grundsätzlich nicht entsprochen werden kann.[378] Eine wirksame Wahrnehmung von Betroffenenrechten gegenüber den Full Nodes ist dann jedenfalls nicht möglich.

---

[374] Siehe dazu auch oben unter D. II.
[375] Siehe dazu auch oben unter D. I. 1.
[376] Siehe dazu auch oben unter D. II. 2.
[377] So jedenfalls für offene Blockchain-Architekturen *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 86.
[378] So auch für Blockchain-Netzwerke *Guggenberger*, Smart Contracts, ICOs und Datenschutz in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. EL März 2022, Teil 13.7 Rn. 86; *Pesch*, Blockchain, Smart Contracts und Datenschutz in: Fries/Paal, Smart Contracts, S. 13, 19; umfangreich zu Blockchain-Netzwerken und deren Vereinbarkeit mit datenschutzrechtlichen Grundsätzen *Marnau*, Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung in: Eibl/Gaedke, Informatik 2017, Lecture Notes in Informatics (LNI), S. 1015 ff.

c) Clients als Anspruchsgegner

Allerdings kommt eine Wahrnehmung der Betroffenenrechte gegenüber denjenigen Clients in Betracht, die selbst an der Anbahnung, dem Abschluss sowie der Abwicklung von Verträgen mitwirken. Sofern man diese ebenfalls als datenschutzrechtlich Verantwortliche qualifiziert[379], müssen sie ihren gesetzlichen Pflichten nachkommen. Daher können Auskunfts-, Berichtigungs- und Löschungsrechte auch ihnen gegenüber geltend gemacht werden.

d) Betroffenenrechte bei Verlassen der Fidesnetzwerkstruktur

Unklar ist allerdings auch, wie mit Betroffenenrechten umzugehen ist, wenn einzelne Clients oder Full Nodes die Ringstruktur verlassen, was grundsätzlich aufgrund der dezentralen Struktur jederzeit möglich ist. Denn in diesen Fällen können Verantwortlichkeiten entfallen, sodass eine Ausübung der Betroffenenrechte nicht mehr oder nur unter erheblichen Schwierigkeiten möglich ist. Hier ist darüber nachzudenken, inwiefern gespeicherte personenbezogene Daten für einen bestimmten Zeitraum dupliziert in der Netzwerkstruktur vorgehalten werden können, sodass auch bei einem Wegfall einzelner Full Nodes oder Clients die Ausübung von Betroffenenrechten ermöglicht wird, wenngleich mit einer solchen Gestaltung wiederum andere Datenschutzgrundsätze – wie etwa der Grundsatz der Datensparsamkeit (Art. 5 Abs. 1 lit. c DSGVO) und der Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) – tangiert werden.

VII. Zusammenfassung der datenschutzrechtlichen Ergebnisse

Das Fidesnetzwerk zeichnet sich durch eine dezentrale und offene Netzwerkstruktur aus, innerhalb derer Nutzer Verträge schließen und abwickeln können. Dabei gibt es einerseits die Kategorie der Clients sowie andererseits die Kategorie der Full Nodes. In datenschutzrechtlicher Hinsicht ergeben sich hieraus zahlreiche rechtliche Herausforderungen.

1. Anwendungsbereich der DSGVO

Der Anwendungsbereich der DSGVO ist in sachlicher und räumlicher Hinsicht eröffnet, da im Fidesnetzwerk – auch bei Nutzung von LoRaWAN – regelmäßig personenbezogene Daten verarbeitet werden und die Betreiber der Full Nodes entweder in der EU

[379] Siehe dazu auch oben unter D. II. 2.

niedergelassen sind oder jedenfalls über Fides Dienstleistungen an Clients in der EU anbieten (Art. 2 DSGVO, Art. 3 DSGVO).[380]

2. Datenschutzrechtliche Verantwortlichkeiten

Die Bestimmung von datenschutzrechtlichen Verantwortlichkeiten ist aufgrund des dezentralen Charakters sowie der Offenheit von Fides eine wesentliche Herausforderung. Entscheidend ist hierbei die konkrete Ausgestaltung der Fidesnetzwerkstruktur. In der Regel wird man jedoch davon ausgehen können, dass in Fides bei der Anbahnung, dem Abschluss sowie der Abwicklung von Verträgen eine gemeinsame Verantwortlichkeit der beteiligten Akteure begründet wird. Daher sind sowohl die Betreiber der zuständigen Full Node als auch die am Vertrag beteiligten Clients als datenschutzrechtlich gemeinsame Verantwortliche zu qualifizieren (vgl. Art. 26 DSGVO).[381] Der Einsatz von LoRaWAN hat hierauf keinen Einfluss.

3. Grundsätze für die Verarbeitung personenbezogener Daten

Im Fidesnetzwerk müssen die datenschutzrechtlichen Grundsätze (vgl. Art. 5 DSGVO) eingehalten werden.[382] Das gilt ebenfalls, sofern LoRaWAN genutzt wird. Dabei spielen insbesondere das Rechtmäßigkeitsprinzip (Art. 5 Abs. 1 lit. a Var. 1 DSGVO), das Transparenzprinzip (Art. 5 Abs. 1 lit. a Var. 3 DSGVO), das Datensparsamkeitsprinzip (Art. 5 Abs. 1 lit. c DSGVO), das Richtigkeitsprinzip (Art. 5 Abs. 1 lit. d DSGVO) sowie das Integritäts- und Vertraulichkeitsprinzip (Art. 5 Abs. 1 lit. f DSGVO) eine tragende Rolle. Die abstrakten Grundsätze werden durch zahlreiche Vorschriften in der DSGVO konkretisiert. Auf sie wird im Folgenden eingegangen.

4. Rechtmäßigkeit der Datenverarbeitung

Als Konkretisierung des Rechtmäßigkeitsprinzip (Art. 5 Abs. 1 lit. a Var. 1 DSGVO) ist eine Verarbeitung personenbezogener Daten nur rechtmäßig, wenn eine Einwilligung oder ein gesetzlicher Erlaubnistatbestand dies rechtfertigen (vgl. Art. 6 DSGVO). [383] Die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) sowie die Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) eignen sich in Fides nur bedingt als Legitimationsgrundlage. Als maßgebliche Rechtsgrundlage für die Datenverarbeitung eignet sich im Fidesnetzwerk allerdings die Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO), da Fides für die Anbahnung,

[380] Dazu ausführlich unter D. I.
[381] Dazu ausführlich unter D. II.
[382] Dazu ausführlich unter D. III.
[383] Dazu ausführlich unter D. IV.

den Abschluss sowie die Abwicklung von Verträgen konzipiert ist. Werden besondere Kategorien personenbezogener Daten verarbeitet sind die speziellen Anforderungen von Art. 9 DSGVO zu berücksichtigen. Beim Einsatz von LoRaWAN ergibt sich keine abweichende rechtliche Bewertung.

5. Ausgewählte Pflichten des Datenverarbeiters

Den datenschutzrechtlich Verantwortlichen treffen zahlreiche Pflichten. In Fides sind insbesondere die Regelungen zu Datenschutz durch Technikgestaltung und datenschutzrechtliche Voreinstellungen (Art. 25 DSGVO) sowie zur Sicherheit der Datenverarbeitung (Art. 32 DSGVO) relevant.[384] Dabei werden im Fidesnetzwerk nachvollziehbare Ansätze zur Realisierung der rechtlichen Anforderungen integriert. So werden etwa personenbezogene Daten in Gestalt pseudonymer Daten verarbeitet, Daten werden verschlüsselt übertragen und gespeichert und digitale Signaturen und Zertifikate verwendet. Gleichwohl ist auch hier die weitere technische Entwicklung, die sich jederzeit auf die rechtliche Bewertung auswirkt, zu berücksichtigen. Beim Einsatz von Fides mithilfe von LoRaWAN ist auch diesbezüglich die Sicherheit der Datenverarbeitung (Art. 32 DSGVO) besonders zu berücksichtigen und entsprechende Schutzmechanismen zu integrieren.

6. Ausgewählte Betroffenenrechte

Die Realisierung der Betroffenenrechte – insbesondere der Rechte auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO) sowie Löschung (Art. 17 DSGVO) – stellt eine weitere Herausforderung in Fides dar.[385] Zwar lassen sich diese Rechte grundsätzlich auch in Fides erfüllen, allerdings ist eine wesentliche Herausforderung dabei, einen tauglichen Anspruchsgegner zu identifizieren. Aufgrund der offenen und dezentralen Netzwerkstruktur lassen sich Verantwortlichkeiten nur schwer zuschreiben und damit auch Anspruchsgegner bestimmen. Daher kommt es entscheidend auf den Einzelfall an, wem welche Verantwortlichkeiten zugeschrieben werden können in der Fidesnetzwerkstruktur. Wird Fides mithilfe von LoRaWAN genutzt, ergeben sich hinsichtlich der Ausübung der Betroffenenrechte keine Besonderheiten.

---

[384] Dazu ausführlich unter D. V.
[385] Dazu ausführlich unter D. VI.

E. Literaturverzeichnis

Alexander, Neuregelungen zum Schutz vor Kostenfallen im Internet, NJW 2012, S. 1985 ff.

Albrecht, Das neue EU-Datenschutzrecht - von der Richtlinie zur Verordnung – Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog, CR 2016, S. 88 ff.

Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 01248/07/DE, WP 136

Artikel-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, 0829/14/DE, WP 216

Artikel-29-Datenschutzgruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 844/14/EN, WP 217

Assion, Telekommunikation-Telemedien-Datenschutz-Gesetz, München 2022

Aufderheide, Smart Contracts aus der Perspektive des Zivilrechts – Teil I, WM 2021, S. 2273 ff.

Aufderheide, Smart Contracts aus der Perspektive des Zivilrechts – Teil II, WM 2021, S. 2313 ff.

Aufderheide, Dezentrale Autonome Organisation (DAO) – Smart Contracts aus der Perspektive des Gesellschaftsrechts, WM 2022, S. 264 ff.

Baumbach/Hopt, Handelsgesetzbuch, 41. Auflage, München 2022

Bechtolf/Vogt, Datenschutz in der Blockchain - Eine Frage der Technik – Technologische Hürden und konzeptionelle Chancen, ZD 2018, S. 66 ff.

Becker, Das Recht auf Vergessenwerden, Tübingen 2019

Bernzen, Smart Contracts – Können „kluge Verträge“ zum Konfliktmanagement beitragen?, ZKM 2021, S. 219 ff.

Bertram, Smart Contracts – Praxisrelevante Fragen zu Vertragsschluss, Leistungsstörungen und Auslegung, MDR 2018, S. 1416 ff.

Biryukov/Khovratovich/Pustogarov, Deanonymisation of Clients in Bitcoin P2P Network, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, S. 15 ff.

Bizer, Sieben Goldene Regeln des Datenschutzes, DuD 2007, S. 350 ff.

Blocher, The next big thing – Blockchain – Bitcoin – Smart Contracts: Wie das disruptive Potential der Distributed Ledger Technology (nicht nur) das Recht fordern wird, AnwBl 2016, S. 612 ff.

Böhme/Pesch, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, DuD 2017, S. 473 ff.

Börderinger/Jülicher/Röttgen/v. Schönfeld, Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht in Praxis und Rechtsdogmatik, CR 2017, S. 134 ff.

Braegelmann/Kaulartz, Rechtshandbuch Smart Contracts, Wiesbaden 2019

Brisch/Pieper, Das Kriterium der "Bestimmbarkeit" bei Big Data-Analyseverfahren – Anonymisierung, Vernunft und rechtliche Absicherung bei Datenübermittlungen, CR 2015, S. 724 ff.

Brox/Walker, Allgemeiner Teil des BGB, 46. Auflage, München 2022

Buchner, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, S. 155 ff.

Calliess/Ruffert, EUV/AEUV – Das Verfassungsrecht der Europäischen Union mit der Europäischen Grundrechtecharta, 6. Auflage, München 2022

Datenschutzkonferenz, Kurzpapier Nr. 6 – Auskunftsrecht der betroffenen Person

Datenschutzkonferenz, Kurzpapier Nr. 16 – Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO

Dix, Die deutsche Corona Warn-App – ein gelungenes Beispiel für Privacy by Design?, DuD 2020, S. 779 ff.

Ebenroth/Boujong/Joost/Strohn, Handelsgesetzbuch, Band 2 §§ 343 – 475h – Transportrecht Bank- und Börsenrecht, 4. Auflage, München 2020

Eckhardt, IP-Adresse als personenbezogenes Datum - neues Öl ins Feuer – Personenbezug im Datenschutzrecht - Grenzen der Bestimmbarkeit am Beispiel der IP-Adresse, CR 2011, S. 339 ff.

Eckhardt, Anwendungsbereich des Datenschutzrechts - Geklärt durch den EuGH? – Der europarechtliche Grundsatz des Personenbezugs, CR 2016, S. 786 ff.

Erman, BGB – Handkommentar mit AGG, EGBGB, ErbbauRG, LPartG, ProdHaftG, VBVG, VersAusglG, WEG und ausgewählten Rechtsquellen des IPR, Band 1, 16. Auflage, München 2020

Ehmann/Selmayr, DS-GVO, 2. Auflage, München 2018

Eibl/Gaedke, Informatik 2017 – Lecture Notes in Informatics (LNI) – Proceedings, Bonn 2017

Erbguth/Fasching, Wer ist Verantwortlicher einer Bitcoin-Transaktion? – Anwendbarkeit der DS-GVO auf die Bitcoin-Blockchain, ZD 2017, S. 560 ff.

Eschenbruch/Gerstberger, Smart Contracts, NZBau 2018, S. 3 ff.

Fabricius, Stillschweigen als Willenserklärung, JuS 1966, S. 1 ff.

Fetzer/Scherer/Graulich, TKG – Telekommunikationsgesetz, 3. Auflage, Wiesbaden 2020

Finck, Smart contracts as a form of solely automated processing under the GDPR, IDPL 2019, S. 78 ff.

Finck, Blockchains and Data Protection in the European Union, EDPL 2018, S. 17 ff.

Fries, Smart Contracts – Pacta sunt servanda?, REL 2018, S. 46 ff.

Fries, Smart Contracts – Brauchen schlaue Verträge noch Anwälte?, AnwBl 2018, S. 86 ff.

Fries/Paal, Smart Contracts, Tübingen 2019

Froitzheim, Code is Law, isn't it? – Verkehrssitte und Software, K&R 2020, S. 122 ff.

Geppert/Schütz, Beck'scher TKG Kommentar, 4. Auflage, München 2013

Gerlach, Personenbezug von IP-Adressen, CR 2013, S. 478 ff.

Gersdorf/Paal, BeckOK Informations- und Medienrecht, 38. Edition, Stand 01.11.2022, München 2023

Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage, München 2022

Grüneberg, Bürgerliches Recht, 81. Auflage, 2022
Guggenberger, Datenschutz durch Blockchain – eine große Chance, ZD 2017, S. 49 f.

Hartung/Bues/Halbleib, Legal Tech – Die Digitalisierung des Rechtsmarktes, Tübingen 2018

Härting, Datenschutz im Internet – Wo bleibt der Personenbezug?, CR 2008, S. 743 ff.

Hau/Poseck, Beck'scher Online-Kommentar BGB, 62. Edition, Stand 01.08.2022

Heckelmann, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, S. 504 ff.

Herbst, Was sind personenbezogene Daten?, NVwZ 2016, S. 902 ff.

Heun, Die elektronische Willenserklärung – rechtliche Einordnung, Anfechtung, Zugang, CR 1994, S. 595 ff.

Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 58. Ergänzungslieferung, Stand März 2022, München 2022

Hoffmann/Swarek, Blockchain, Smart Contracts und Recht – Smart Contracts als Risiko für Informatiker, Informatik Spektrum 42 (2019), S. 197 ff.

Hofert, Blockchain-Profiling – Verarbeitung von Blockchain-Daten innerhalb und außerhalb der Netzwerke, ZD 2017, S. 161 ff.

Hunzinger, Das Löschen im Datenschutzrecht, Baden-Baden 2018

Jacobs/Lange-Hausstein, Funktionen, Anwendungsfälle, Perspektiven der Blockchain-Technologie, ITRB 2017, S. 10 ff.

Janicki/Saive, Privacy by Design in Blockchain-Netzwerken – Verantwortlichkeit und datenschutzkonforme Ausgestaltung von Blockchains, S. 251 ff.

Jarass, Charta der Grundrechte der Europäischen Union, 4. Auflage, München 2021

Jauernig/Stürner, Bürgerliches Gesetzbuch mit Rom-I-VO, Rom-II-VO, Rom-III-VO, EG-UnthVO/HUntProt und EuErbVO, 18. Auflage, München 2021

Kaulartz/Heckmann, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 2016, S. 618 ff.

Kindler, Grundkurs Handels- und Gesellschaftsrecht, 9. Auflage, München 2019

Kipker/Birreck/Niewöhner/Schnorr, Rechtliche Rahmenbedingungen der „Smart Contracts“ – Eine zivilrechtliche Betrachtung, S. MMR 2020, 509 ff.

Kirschbaum, Die gesetzliche Neuregelung der sog. „Internetfalle“, MMR 2012, S. 8 ff.

Klar/Wegmann/Galandi, Datenschutz im Metaverse, BB 2022, S. 2691 ff.

Kloth, Blockchain basierte Smart Contracts im Lichte des Verbraucherrechts, VuR 2021, S. 214 ff.

Köhler, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen, AcP (182) 1982, S. 128 ff.

Krügel, Der Einsatz von Angriffserkennungssystemen im Unternehmen – Geeignete Maßnahmen zur Erhöhung der Informationssicherheit, MMR 2017, S. 795 ff.

Kumkar, Rechtsgeschäfte unter Beteiligung automatisierter und autonomer Systeme, K&R 2020, S. 801 ff.

Kühling/Buchner, Datenschutz-Grundverordnung BDSG, 3. Auflage, München 2020

Kühling/Schildbach, Corona-Apps – Daten- und Grundrechtsschutz in Krisenzeiten, NJW 2020, S. 1545 ff.

Legner, Smart Consumer Contracts – Die automatisierte Abwicklung von Verbraucherverträgen, VuR 2021, S. 10 ff.
Lehmann/Krysa, Smart Contracts und Token aus der Sicht des (Internationalen) Privatrechts, BRJ 2019, S. 90 ff.

Linardatos, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, S. 85 ff.

Linardatos, Neue Technologien im Insolvenzrecht – Einsatzfelder von künstlicher Intelligenz, Blockchain und Smart Contracts, ZIP 2022, S. 153 ff.

Lupu, Ansätze zur Überwindung des Spannungsverhältnisses zwischen Smart Contracts und den zivil- und datenschutzrechtlichen Vorgaben, CR 2019, S. 631 ff.

Marsch, Nikolaus, Das europäische Datenschutzgrundrecht, Tübingen 2018

Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden – Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen, NVwZ 2017, S. 1251 ff.

Medicus/Petersen, Bürgerliches Recht, 22. Auflage, München 2009

Möslein, Smart Contracts im Zivil- und Handelsrecht, ZHR 183 (2019), S. 254 ff.

Moos, Flemming, Die Entwicklung des Datenschutzrechts im Jahr 2016, K&R 2017, S. 566 ff.

Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Auflage, München 2021

Padeck, Rechtsprobleme bei Schadensfällen in Autowaschanlagen, VersR 40 (1989), S. 541 ff.

Parino/Beiró/Gauvin, Analysis of the Bitcoin blockchain: socio-economic factors behind the adoption, EPJ Data Science 7, 38 (2018)

Paulus, Die automatisierte Willenserklärung, JuS 2019, S. 960 ff.
Paulus, Was ist eigentlich ... ein Smart Contract?, JuS 2020, S. 107 ff.

Paulus/Matzke, Smart Contracts und das BGB – Viel Lärm um nichts, ZfPW 2018, S. 431 ff.

Petersen, Schweigen im Rechtsverkehr, Jura 2003, S. 687 ff.

Potel/Hessel, Rechtsprobleme von Smart Contracts – automatisierte Abwicklung von verträgen, jM 2020, S. 354 ff.

Quiel, Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO – Ein Zwiespalt zwischen Innovation und unionalem Datenschutzrecht?, DuD 2018, S. 566 ff.

Raue, Kostenpflichtig bestellen – ohne Kostenfalle? – Die neuen Informations- und Formpflichten im Internethandel, MMR 2012, S. 438 ff.

Rocher/Hendrickx/de Montjoye, Estimating the success of re-identifications in incomplete datasets using generative models, Nat Commun 10, 3069 (2019)

Roßnagel, Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003

Rupa, Standardisierte Projektverträge als Smart Contracts, MMR 2021, S. 371 ff.

Säcker/Rixecker/Oetker/Limperg, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 9 Auflage, München 2021

Säcker/Rixecker/Oetker/Limperg, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2, 9. Auflage, München 2022

Säcker/Rixecker/Oetker/Limperg, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 3, 9. Auflage, München 2022

Säcker/Rixecker/Oetker/Limperg, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 4, 8. Auflage, München 2019

Schantz, Peter, Die Datenschutz-Grundverordnung - Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841 ff.

Schawe, Blockchain und Smart in der Kreativwirtschaft – mehr Probleme als Lösungen? – Einsatz von Blockchain-Anwendungen im Immaterialgüterrecht, MMR 2019, S. 218 ff.

Schewe/Muscheler, Die invitatio ad offerendum auf dem Prüfstand, Jura 2000, S. 565 ff.

Schneider/Härting, Wird der Datenschutz nun endlich internettauglich? – Warum der Entwurf einer Datenschutz-Grundverordnung enttäuscht, ZD 2012, S. 199 ff.

Schnell/Schwaab, Vertragsgestaltung beim Einsatz von Smart Contracts zur Automatisierung von Lieferbeziehungen, BB 2021, S. 1091 ff.

Schnurr, Anbahnung, Abschluss und Durchführung von Smart Contracts im Rechtsvergleich, ZVglWiss 2019, S. 257 ff.

Schrey/Thalhofer, Rechtliche Aspekte der Blockchain, NJW 2017, S. 1431 ff.

Schulze, Bürgerliches Gesetzbuch – Handkommentar, 11. Auflage, München 2022

Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 2. Auflage, Heidelberg 2020

Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht – DSGVO mit BDSG, Baden-Baden 2019

Sinbartl/Zintl, Schadensersatzhaftung des Verbrauchers bei nicht erfolgter oder fehlerhafter Widerspruchsbelehrung, NJW 2016, S. 1848 ff.

Söbbing, Smart Contracts und Blockchain-Technologie: Definition, Arbeitsweise, Rechtsfragen, ITRB 2018, S. 43 ff.
Specht/Mantz, Handbuch Datenschutzrecht, Baden-Baden 2019

Spindler/Schmitz, Telemediengesetz mit Netzwerkdurchsetzungsgesetz, 2. Auflage, München 2018

Spindler/Schuster, Recht der elektronischen Medien, 4. Auflage, München 2019

Sydow/Marsch, DS-GVO | BDSG, 3. Auflage, Baden-Baden 2022

Tavakoli, Automatische Fluggast-Entschädigung durch smart contracts, ZRP 2020, S. 46 ff.

Thiele, Zum Allgemeinen Teil des Deutschen Bürgerlichen Rechts, JZ 1969, S. 405 ff.

Timmermann, Eine Systematisierung – Legal Tech, IT-Recht, Smart Contracts und KI als Begriffe regulatorischer Herausforderungen, BRJ 2021, Sonderausgabe, 7

Timmermann, Legal Tech-Anwendungen – Rechtswissenschaftliche Analyse und Entwicklung des Begrifs der algorithmischen Rechtsdienstleistung, Tübingen 2022

Treiber, Schuldscheindarlehen als Smart Contracts, REL 2018, S. 10 ff.

Ultsch, Zugangsprobleme bei elektronischen Willenserklärungen – Dargestellt am Beispiel der Electronic Mail, NJW 1997, S. 3007 ff.

Walter, Die datenschutzrechtlichen Transparenzpflichten nach der Europäischen Datenschutz-Grundverordnung, DSRITB 2016, S. 367 ff.

Wieacker, Die Methode der Auslegung des Rechtsgeschäfts, JZ 1967, S. 385 ff.

Wilhelm, Smart Contracts im Zivilrecht – Teil I, WM 2020, S. 1807 ff.

Wilhelm, Smart Contracts im Zivilrecht – Teil II, WM 2020, S. 1849 ff.

Wilkens/Falk, Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden 2019

Wolff/Brink, BeckOK Datenschutzrecht, 42. Edition, Stand 01.11.2022, München 2023