Sven Venzke-Caprarese

Blockchain-Shops im Web3

Datenschutzrechtliche Betrachtung am Beispiel des OnChain-Shops der Österreichischen Post

Die Österreichische Post hat am 11. Juni 2019 die erste Blockchain Briefmarke der Welt herausgegeben. Bei dieser sogenannten „Crypto stamp" handelt es sich um eine normale Briefmarke, die jedoch zusätzlich durch einen für jede Marke einzigartigen, digitalen Token in der Ethereum-Blockchain repräsentiert wird. Die tokenisierte Briefmarke wird in einer Auflage von 150.000 Stück verkauft. Neben dem Verkauf der Briefmarke auf klassischem Weg, bietet die Österreichische Post auch eine limitierte Stückzahl von 500 Marken über einen neuartigen „OnChain-Shop" zum Kauf an. Der nachfolgende Beitrag stellt am Beispiel der Österreichischen Post näher dar, was unter einem OnChain-Shop zu verstehen ist und bewertet den Kauf von Crypto stamps im OnChain-Shop unter datenschutzrechtlichen Gesichtspunkten.

1 OnChain-Shop in der Blockchain

Was ist eigentlich ein OnChain-Shop und wie wird der Kauf von Crypto stamps im OnChain-Shop unter datenschutzrechtlichen Gesichtspunkten bewertet, diesen Fragen soll im Rahmen dieses Beitrages näher nachgegangen werden. Aufgrund der Komplexität können nicht alle Fragen abschließend behandelt werden, vielmehr soll mit dieser datenschutzrechtlichen Behandlung des Themas Blockchain anhand praktischer Beispiele die Diskussion hierzu vorangetrieben und die Möglichkeit aufgezeigt werden, nicht nur die Risiken dieser Technologie, sondern auch deren datenschutzrechtliche Chancen zu sehen.

1.1 Kauf im OnChain-Shop

Der Webauftritt des OnChain-Shops der Österreichischen Post ist unter *https://crypto.post.at/onchainshop* zu erreichen. Alternativ kann der OnChain-Shop auch über seine eigene Ethereum-Adresse erreicht werden.[1]

Um eine Crypto stamp über den Webauftritt des OnChain-Shops kaufen zu können, muss dieser mit einem Browser besucht werden, der über Web3-Funktionen verfügt – sich also mit dem Netzwerk der Ethereum-Blockchain verbinden kann. Dies ist zum Beispiel mit den Browsern Chrome und Firefox sowie der Erweiterung Metamask möglich. Zudem muss der Käufer bereits über eine eigene Ethereum-Adresse verfügen. Bezahlt wird in der Kryptowährung Ether. Der Kauf der Crypto stamps an sich erfolgt direkt über einen Smart Contract. Dieser beinhaltet, vereinfacht dargestellt, das folgende Regelwerk: Wenn von einer Ethereum-Adresse der geforderte Kaufpreis in Ether an die Adresse des Smart Contracts des OnChain-Shops transferiert wird, wird im Gegenzug ein einzigartiger Token an die Ethereum-Adresse des Käufers übertragen.

Genau genommen ist zum Kauf der Crypto Stamps noch nicht einmal der Besuch des Webauftritts der Österreichischen Post erforderlich. Es würde ausreichen, die Überweisung manuell direkt über die Blockchain auszulösen.

Die Eingabe unmittelbar personenbezogener Daten ist somit zum Kauf im OnChain-Shop nicht notwendig. Der Käufer muss lediglich seine Ethereum-Adresse offenbaren. Am Ende des Kaufs findet der Käufer dort einen digitalen Token mit der Bezeichnung „Crypto stamp Edition 1" und einer einzigartigen Token ID. Der Transfer des einzigartigen Tokens vom OnChain-Shop an die Et-

Sven Venzke-Caprarese

Prokurist | Justiziar
datenschutz nord GmbH

E-Mail: svenzke@datenschutz-nord.de

1 Der Smart Contract ist unter der Adresse 0xC5BA58b8362a25b1dd-B59E2106910B6c324A5668 abrufbar und kann über https://etherscan.io/address/0xc5ba58b8362a25b1ddb59e2106910b6c324a5668#contracts eingesehen werden, letzter Abruf am 30.6.2019.

Abb. 1 | Dieser Auszug des Smart Contracts des OnChain-Shops enthält die wichtigsten Regeln für den Verkauf des digitalen Tokens.

```
449     // For buying a single asset, just send enough ether to this contract.
450     function()
451     external payable
452     requireOpen
453     {
454         //get from eurocents to wei
455         uint256 curPriceWei = priceWei();
456         //update the price according to the strategy for the following buyer.
457         uint256 remaining = cryptostamp.balanceOf(address(this));
458         priceEurCent = pricingStrategy.adjustPrice(priceEurCent, remaining);
459
460         require(msg.value >= curPriceWei, "You need to send enough currency to
    actually pay the item.");
461         // Transfer the actual price to the beneficiary
462         beneficiary.transfer(curPriceWei);
463         // Find the next stamp and transfer it.
464         uint256 tokenId = cryptostamp.tokenOfOwnerByIndex(address(this), 0);
465         cryptostamp.safeTransferFrom(address(this), msg.sender, tokenId);
466         emit AssetSold(msg.sender, tokenId, curPriceWei);
467         deliveryStatus[tokenId] = Status.Sold;
468
469         /*send back change money. last */
470         if (msg.value > curPriceWei) {
471             msg.sender.transfer(msg.value.sub(curPriceWei));
472         }
473     }
```

Abb. 3 | Dieser Eintrag findet sich unter dem Transaktionshash 0x8cce083157c5ffcfbbfcd5ef18602a5c264bb02dba66e5f5a4cec0b24f01f17c innerhalb der Ethereum-Blockchain

```
Function: shipToMe(string _deliveryInfo, uint256 _tokenId)

MethodID: 0x1fbe480e
[0]:  0000000000000000000000000000000000000000000000000000000000000040
[1]:  000000000000000000000000000000000000000000000000000000000000747fc
[2]:  0000000000000000000000000000000000000000000000000000000000001f8
[3]:  7b226976223a22353562656538383966393433663437353964343930363335363
[4]:  333565643130622222c22657068656d5075626c69634b6579223a223034353162
[5]:  666566643631356161663766333734326535666386464356238313366638835623
[6]:  396638353564383165623262653462393736361316539366638326337313764
[7]:  316532333236613634653532323162666234373766306562663163663539303838
[8]:  356362303364666431303234356566613338623462363939364363430312222c22
[9]:  636970686572746578742223a22336230643736303437343966316231653964322
[10]: 653064303732393939363434653836353634636666336366137343433611316238
[11]: 323962643863333383539653930306430393030613116632303562346237383136
[12]: 373265366135663130636338393038316635653835396535323063934323036
[13]: 616132323663538323266356630303362366265623363333130316333936643
[14]: 663661356432316262346134633965623730643766306439396238343464633322
[15]: 646235386536333764353839356265323465636363633636363663839386166
[16]: 626239356639343635313364652222c226d6163223a223938333534326531313232
[17]: 333830316237613533623330163376564363432636538626439653230326461
[18]: 626565316531316630613563326336336132316134382277d0000000000000000
```

Er stellt die Bekanntgabe der Versandadresse zu einem bestimmten Token durch den Käufer gegenüber der Österreichischen Post innerhalb der Blockchain dar, die diese Nachricht mit Hilfe ihres privaten Schlüssels entschlüsseln kann.

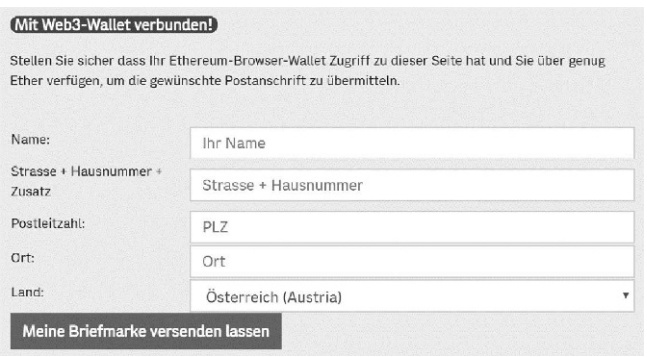
hereum-Adresse des Käufers wird dabei in der Ethereum Blockchain öffentlich einsehbar protokoliert.

1.2 Übermittlung der Versandadresse

Jedem einzigartigen Token, der im OnChain-Shop verkauft wird, ist eine einzigartige physische Briefmarke zugeordnet. Dies ist dadurch sichergestellt, dass die physische Briefmarke mit der entsprechenden Token ID bedruckt wurde.

Käufer des digitalen Tokens können sich grundsätzlich frei entscheiden, ob und wann Sie eine physische Versandadresse angeben und den Versand der physischen Briefmarke auslösen wollen. Eine Anmeldung mit unmittelbar personenbezogenen Daten am OnChain-Shop ist hierzu nicht erforderlich, denn der OnChain-Shop prüft zur Authentisierung lediglich, ob der Ethereum-Adresse des Besuchers der digitale Token zugeordnet ist, der die physische Briefmarke repräsentiert. Erst wenn sich ein Käufer entscheidet, den Versand der physischen Briefmarke auszulösen, müssen das erste Mal unmittelbar personenbezogene Daten in Form der Versandadresse bereitgestellt werden.

Abb. 2 | Auslösen der Versandanforderung durch Eingabe der Versandadresse im On-Chain-Shop.



Das Formular zur Eingabe der Versanddaten im OnChain-Shop sieht auf den ersten Blick aus, wie ein normales Webformular. Tatsächlich werden die eingegebenen Daten aber nicht an einen Server der Österreichischen Post übermittelt, sondern mit einem öffentlichen Schlüssel der Post verschlüsselt und anschließend direkt in die Blockchain geschrieben.

1.3 An- und Weiterverkauf des Tokens ohne Übermittlung der Versandadresse

Käufer des digitalen Tokens können sich entscheiden, den Versand der physischen Briefmarke nicht sofort auszulösen. Stattdessen besteht die Möglichkeit des Käufers seinen Token innerhalb der Ethereum-Blockchain an die Ethereum-Adresse einer anderen Person zu übertragen – etwa, weil der Token außerhalb des OnChain-Shops auf dem Zweitmarkt weiterverkauft wurde.

Kommt es dem Käufer eines solchen Tokens dabei darauf an, die physische Briefmarke zu erhalten, muss er vor dem Kauf prüfen, ob der Versand der zugeordneten physischen Marke bereits ausgelöst wurde oder nicht. Eine solche Überprüfung ist über die Blockchain ebenfalls möglich, da die Anforderung des Versands des Tokens dort als Bekanntgabe der physischen Versandadresse protokolliert wäre. Sofern der Versand vom Erstkäufer nicht angefordert wurde, wüsste ein etwaiger Zweitkäufer, dass er mit der Übermittlung des Tokens die einzige Möglichkeit erhält, die Versandadresse der physischen Briefmarke zu bestimmen. Hintergrund ist, dass der Token immer nur dem aktuellen Inhaber als Authentisierungsmerkmal gegenüber der Österreichischen Post dient, die die physische Briefmarke nur einmalig an die vom aktuellen Token-Inhaber angegebene physische Versandadresse sendet.

Es ist also nicht unwahrscheinlich, dass die Österreichische Post von vielen Erstkäufern lediglich die Angabe der Ethereum-Adresse erhält und zu keinem Zeitpunkt unmittelbar personenbezogene Daten von diesen erhebt. Trotzdem ist es möglich, dass die Erstkäufer den digitalen Token verkaufen bzw. übertragen und damit gleichzeitig die Rechte an der physischen Briefmarke weitergeben.[2]

2 Der Verkauf von tokenisierten physischen Gegenständen ist in der Literatur und Rechtsprechung noch unbehandelt. Hier eröffnet sich ein spannendes juris-

2 Datenschutzrechtliche Bewertung

Nachfolgend soll der Vorgang des Ankaufes im OnChain-Shop der Österreichischen Post datenschutzrechtlich näher betrachtet werden.

2.1 Personenbezug

Die Anwendung des Datenschutzrechts setzt nach Art. 2 Abs. 1 DS-GVO zunächst einmal voraus, dass personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden.

2.1.1 Personenbezug der Versandadresse

Vorliegend kann schnell festgestellt werden, dass zumindest im Hinblick auf die Bereitstellung der Versandadresse personenbezogene Daten verarbeitet werden, indem die Post Zugriff auf die innerhalb der Blockchain verschlüsselt gespeicherten Adressinformationen des Käufers erhält und über die Mittel verfügt, diese Daten zu entschlüsseln. Ein Personenbezug und damit die grundsätzliche Anwendbarkeit des Datenschutzrechts kann demnach zumindest bei Kaufvorgängen angenommen werden, in denen die Versandadresse bereitgestellt wird.

2.1.2 Personenbezug der Ethereum-Adresse

Allerdings wurde unter Ziffer 1.3 bereits dargestellt, dass eine Bereitstellung der Versandadresse nicht in jedem Fall zwingend erforderlich ist und die tokenisierte Briefmarke vom Käufer sogar weiterverkauft werden kann, ohne dass die Post Name und Anschrift des Erstkäufers erhält. Die einzige Information, die zum Kauf einer Crypto Stamp im OnChain-Shop erforderlich ist, ist die Ethereum-Adresse des Käufers, welche genutzt wird, um Ether an den Smart Contract der Post zu transferieren und den digitalen Token in Empfang zu nehmen. Fraglich ist also, ob die Ethereum-Adresse des Käufers ein personenbeziehbares Datum darstellt. An dieser Stelle kommt es darauf an, genauer zu verstehen, was eine Ethereum-Adresse überhaupt ist.

Eine Ethereum-Adresse ist eine 42-stellige Zeichenfolge, die mit dem Präfix „0x" beginnt und grundsätzlich durch den Nutzer selbst erstellt werden kann. Ausgangspunkt ist die Erzeugung einer zufälligen Zahlenfolge, mit einer Länge von 256 bit, die als privater Schlüssel dient. Mit Hilfe dieser Zahlenfolge lässt sich dann sowohl ein öffentlicher Schlüssel als auch eine Ethereum-Adresse berechnen. Eine Ethereum-Adresse ist somit nur das Ergebnis einer mathematischen Berechnung, die eine Zufallszahl mit einer Länge von 256 bit verändert.[3] Da eine solche Berechnung auch vollkommen offline durchgeführt werden kann und keine Anmeldung oder Registrierung der Ethereum-Adresse erforderlich ist, sondern diese aus sich heraus im Zusammenspiel zwischen privatem Schlüssel, öffentlichem Schlüssel und Ethereum-Adresse innerhalb der Blockchain funktioniert, muss festgestellt werden, dass Ethereum-Adressen anonym erstellt werden können und im Grundsatz keinen Personenbezug aufweisen.

tisches Betätigungsfeld.

3 Vgl. auch *Wood*, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER EIP-150 REVISION, Rn. 213: "For a given private key, *pr*, the Ethereum address A(*pr*) (a 160-bit value) to which it corresponds is defined as the right most 160-bits of the Keccak hash of the corresponding ECDSA public key: $A(pr) = B_{96..255}$ KEC ECDSAPUBKEY(*pr*)"

Eine Personenbeziehbarkeit kann aber durch die Nutzung der Ethereum-Adresse entstehen. Denn bei der Ethereum-Blockchain handelt es sich um eine öffentliche Blockchain, die jede eingehende und ausgehende Transaktion zu der Ethereum-Adresse öffentlich einsehbar protokolliert. Je nach Nutzung der Ethereum-Adresse kann dies schnell zu einer Personenbeziehbarkeit führen. Hier einige Beispiele:

- Ein Nutzer veröffentlicht unter seinem Klarnamen im Internet ein Bild seiner Crypto Katze[4], die ebenfalls als digitaler Token seiner Ethereum-Adresse zugeordnet ist. Damit wäre öffentlich einsehbar, wem die Ethereum-Adresse zu diesem Zeitpunkt zugeordnet ist. Ein Personenbezug wäre gegeben.
- Ein Nutzer tauscht Echtgeld gegen Ether bei einer Krypto Börse, nachdem er sich dort mit seinen personenbezogenen Daten angemeldet hat. Die Krypto Börse transferiert die gekaufte Kryptowährung anschließend an die vom Nutzer angegebene Ethereum-Adresse. Zumindest für den Betreiber der Krypto Börse ist die Ethereum-Adresse somit personenbeziehbar.

2.1.3 Anonymer Einkauf möglich

Als Zwischenergebnis kann festgestellt werden, dass ein anonymer Kauf im OnChain-Shop der Österreichischen Post durchaus möglich ist. Dies setzt jedoch voraus, dass der Käufer in der Vergangenheit mit seiner Ethereum-Adresse vorsichtig umgegangen ist und die Information, dass er diese Adresse nutzt, nicht Dritten bekannt geworden ist. Zudem setzt es voraus, dass sich der Käufer auf den „Besitz" des digitalen Tokens beschränkt, der allerdings auch das Recht am Erhalt der physischen Briefmarke repräsentiert. Die Möglichkeit eines anonymen Kaufs wird dadurch unterstrichen, dass noch nicht einmal der Webauftritt der Post hierfür genutzt werden muss, sondern der Kauf auch ausschließlich über die dezentralisierte Ethereum Blockchain-Infrastruktur abgewickelt werden kann.

2.2 Datenschutzrechtliche Verantwortung

Sofern ein Personenbezug bejaht wird, stellt sich die Frage, ob und ggf. an welcher Stelle die Österreichische Post als Verantwortliche i. S. d. Art. 4 Nr. 7 DS-GVO angesehen werden muss. Demnach ist Verantwortlicher, wer „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Vorliegend müssen zur Bestimmung der Verantwortlichkeit die verschiedenen Verarbeitungsschritte näher betrachtet werden.

2.2.1 Transfer von Ether an den Smart Contract der Post

Um den digitalen Token zu erhalten, der die physische Briefmarke repräsentiert, ist es erforderlich, Ether an den Smart Contract der Post zu transferieren. Der Transfer an sich geht vom Nutzer aus. Übersendet der Käufer Ether direkt innerhalb der Blockchain an den Smart Contract der Post und nutzt hierzu nicht die Website der Post, ist bei der Bestimmung der Verantwortlichkeit folgendes zu beachten:

- Die Post hat den Versand des Ethers nicht vorgenommen. Sie hat lediglich eine eigene Ethereum-Adresse erstellt, die in der Lage ist, Ether zu empfangen. Sie hat zudem erklärt, dass sie bei Empfang von Ether an diese Adresse im Gegenzug einen digitalen Token übermittelt.
- Die Post hat nicht die Mittel, darüber zu entscheiden, ob der entsprechende Versand des Ethers in der Blockchain protokolliert wird oder nicht. Die Protokollierung ist zwingende Voraussetzung der verwendeten Technologie.

Es spricht vieles dagegen, dass die Post für den reinen Transfer des Ethers durch den Käufer Verantwortliche i. S. d. Art. 4 Nr. 7 DS-GVO ist. Sie kann über die Mittel der Verarbeitung nicht mehr entscheiden. Sie könnte noch nicht einmal ihre Ethereum-Adresse schließen, um die Protokollierung des Empfangs von Ether zu unterbinden.

Sofern der Käufer Ether unter Zuhilfenahme der Website des OnChain-Shops unter https://crypto.post.at/onchainshop transferiert, könnte sich eine andere Bewertung ergeben. Zwar wird auch hier im Ergebnis nur Ether von der Adresse des Käufers an die Adresse des Smart Contracts gesendet. Die Website bereitet diesen Transfer für den Nutzer aber so weit vor, dass er nur noch einen Knopf zu drücken braucht. Die Abgrenzung ist an dieser Stelle vage.

Insgesamt spricht aber vieles dafür, an dieser Stelle nicht von einer Verantwortlichkeit der Post auszugehen

2.2.2. Übertragung des Tokens an die Ethereum-Adresse des Käufers

Nachdem ein Käufer Ether in ausreichender Höhe an die Adresse des Smart Contracts transferiert hat, überträgt der Smart Contract einen digitalen Token an die Ethereum-Adresse des Käufers. Um zu bestimmen, ob die Post hierfür eine datenschutzrechtliche Verantwortung trägt, kommt es darauf an, zu wissen, welche Mittel der Post im Hinblick auf den Smart Contract noch zur Verfügung stehen. Dabei kann vom Vorhandensein des Smart Contracts nicht automatisch auf eine Verantwortlichkeit der programmierenden Stelle geschlossen werden. Denn dezentralisierte Applikationen können innerhalb der Blockchain auch ohne jede weitere Steuerungsmöglichkeit betrieben werden. Dann stellt sich hingegen die Frage, ob dem ursprünglichen Initiator überhaupt noch eine datenschutzrechtliche Verantwortung zukommen kann.

Wird der Source Code des Smart Contracts des OnChain-Shops der Österreichischen Post aber genauer betrachtet, ist zu sehen, dass sich die Post die Möglichkeit vorbehalten hat, den Shop jederzeit wieder zu schließen.[5] Die Datenverarbeitung durch den Shop und somit der Versand des Tokens an die Ethereum-Adresse des Käufers bleibt also im Einflussbereich der Post und liegt daher in ihrer datenschutzrechtlichen Verantwortung.

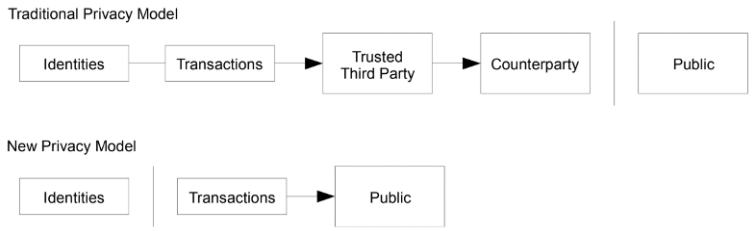
2.2.3 Anforderung der Versandadresse durch den Token Inhaber

Die Anforderung der Versandadresse durch den Inhaber des Tokens kann über die Website des Österreichischen Post veranlasst werden. Die in ein Webformular eingegebene Daten werden zwar nicht an einen von der Post betriebenen Server oder eine von der

4 Nähere Informationen unter https://www.cryptokitties.co/ (letzter Abruf 30.6.2019) sowie im Artikel des Autors: Es miaut in der Blockchain, c`t 1/2019, S. 160 ff.

5 Im Smart Contract des OnChain-Shops, der unter der Adresse https://etherscan.io/address/0xC5BA58b8362a25b1ddB59E2106910B6c324A5668#contracts eingesehen werden kann, ist ab Zeile 422 erkennbar, dass der Shop auch wieder geschlossen werden kann (letzter Abruf 30.6.2019).

Abb. 4 | Auszug aus dem Bitcoin Whitepaper (https://bitcoin.org/bitcoin.pdf), welches an dieser Stelle aber auch für die Ethereum-Blockchain passen würde. Hier wird dem traditionellen Datenschutzmodell ein neues Datenschutzmodell gegenübergestellt.



Post betriebene Infrastruktur gesendet. Allerdings löst die Eingabe in das Formular auf https://crypto.post.at/onchainshop die verschlüsselte Speicherung innerhalb der Ethereum-Blockchain aus. Aufgrund der Bereitstellung des Formulars spricht an dieser Stelle viel für die Verantwortlichkeit der Post, wenngleich die Abgrenzung vage ist.

2.2.4 Entschlüsseln der Versandadresse und Versand durch die Post

Im Hinblick auf die Entschlüsselung der gespeicherten Versanddaten ist die Post eindeutig datenschutzrechtlich verantwortlich. Das gleiche gilt auch für die anschließende Verwendung der Versandadresse.

2.3 Rechtsgrundlage

Die Datenverarbeitung an sich erfolgt grundsätzlich auf der Grundlage von Art. 6 Abs. 1 lit. b DS-GVO – sie ist zur Vertragserfüllung erforderlich. Es spricht insoweit vieles dafür, dass die Nutzung der Blockchain-Technologie keine gesonderte Rechtsgrundlage benötigt, sondern ebenfalls von Art. 6 Abs. 1 lit. b DSGVO gedeckt ist, denn ohne die öffentlich einsehbare Speicherung der Token-ID wäre eine Authentisierung des Inhabers des Übertragungsrechts an der Briefmarke nicht möglich.

2.4 Privacy by Design

Fraglich ist allerdings, ob die Nutzung der Ethereum-Blockchain an sich einen Verstoß gegen den Grundsatz Privacy by Design darstellt. Nach Art. 25 Abs. 1 DS-GVO muss der Verantwortliche bereits bei Festlegung der Mittel für die Verarbeitung geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen. Es darf sich daher die Frage gestellt werden, ob unter diesem Gesichtspunkt bereits die Auswahl der Ethereum-Blockchain einen Verstoß gegen den Privacy by Design Grundsatz darstellt. Schließlich wurde bereits unter Ziffer 2.1.2 dieses Beitrages festgestellt, dass die Personenbeziehbarkeit der Ethereum-Adresse zwar nicht in jedem Fall, aber durchaus schnell gegeben sein kann. Zudem wird die Post als datenschutzrechtlich Verantwortliche in der Regel nicht wissen, welche Ethereum-Adresse aufgrund ihrer Historie für einzelne Dritte bzw. für die Allgemeinheit einem konkreten Inhaber zugeordnet werden kann. Womit fragwürdig ist, inwieweit die Auswahl der Ethereum-Blockchain dann überhaupt datenschutzrechtlich noch vertretbar ist. Vielmehr kann es auch bedeuten, dass die Österreichische Post jede Ethereum-Adresse so behandeln muss, als sei dieses Datum personenbeziehbar.

2.4.1 Neues Datenschutzmodell

Aus Sicht des Autors spricht vieles dafür, dass der vorliegende OnChain-Shop nicht per se gegen den Grundsatz Privacy by Design verstößt. Denn die allgemeine Annahme, dass eine Ethereum-Adresse immer personenbeziehbar ist, stellt eine starke Vereinfachung des individuellen Sachverhalts dar.

Im Gegenteil: Die Konzeption des OnChain-Shops ist in der Lage einen anonymen Kauf und späteren Verkauf des Tokens zu ermöglichen. Sofern die Identität der Ethereum-Adresse nicht veröffentlicht wurde, stellt der vorliegende OnChain-Shop sogar ein datenschutzfreundlicheres Design dar, als normale Online-Shops, in denen Käufer sich zum Kauf mit personenbezogenen Daten anmelden müssen, personenbezogene Zahlungsmittel verwenden und ggf. vom Betreiber des Online-Shops beim Besuch der Website getrackt und analysiert werden. Der OnChain-Shop verfolgt an dieser Stelle einen anderes Datenschutzmodell, mit anderen Chancen und anderen Risiken.

Dieses Datenschutzmodell ist demnach nicht per se dem aktuellen Ansatz von Online-Shops unterlegen und auch nicht per se mit den Datenschutzanforderungen inkompatibel. Allerdings müssen die weiteren Datenschutzgrundsätze umgesetzt werden können.

2.4.2 Datenlöschung

Im Zusammenhang mit Blockchain-Anwendungen wird immer wieder das Thema der Löschung von Daten problematisiert, was auch im Falle des OnChain-Shops nicht einfach zu sein scheint. Denn die Transaktionsdaten können nicht mehr gelöscht werden. Und auch die physische Versandadresse, die nach der Versandanforderung in der Ethereum-Blockchain gespeichert wird, kann grundsätzlich nie wieder gelöscht werden. Allerdings nutzt der OnChain-Shop die Ethereum-Blockchain vorliegend nicht, um die Versandadresse im Klartext zu speichern, sondern speichert diese Daten ausschließlich verschlüsselt. Eine Löschung der Daten könnte somit durch die Vernichtung des privaten Schlüssels erreicht werden. Es bliebe insofern allenfalls das Risiko, dass in der Zukunft eine Entschlüsselungsmöglichkeit existiert, die die verschlüsselt in der Blockchain gespeicherten Daten betrifft – etwa, weil die Rechenleistung stark ansteigt oder heute als sicher geltende Verschlüsselungsmethoden künftig gebrochen werden. Hinzu kommt, dass durch eine Vernichtung des privaten Schlüssels grundsätzlich alle Daten in ihrer Gesamtheit betroffen wären. Die Löschung einzelner Daten muss aber möglich bleiben, um zum Beispiel einzelnen Betroffenenanfragen nachkommen zu können oder einzelne Daten berichtigen zu können. Eine Lösung an dieser Stelle wäre, für jede verschlüsselte Speicherung von an sich unmittelbar personenbezogenen Daten einen eigenen privaten Schlüssel zu verwenden.

Im Hinblick auf die Transaktionsdaten, die mit der Ethereum-Adresse in Verbindung gebracht werden können, ist eine Löschung jedoch nicht möglich. Sofern diese im konkreten Fall durch äußere Umstände personenbeziehbar sind, ergibt sich datenschutzrechtlich eine kaum auflösbare Situation. Allerdings

träfe vermutlich auch den Käufer eine gewisse Mitverantwortung. Perspektivisch ist die Lösung dieses Problems ggf. in einer technologischen Weiterentwicklung von Blockchain Technologien zu sehen. Blockchains, wie z. B. Monero, verfügen schon heute über Ansätze, Transaktionshistorien zu verschleiern, z. B. über sog. Ringsignaturen oder Stealth Adressen.[6] Daneben gibt es weitere Ansätze, wie etwa Mixing oder Zero-Knowledge-Verfahren[7] und auch ganz neue Konzepte.[8]

2.4.3 Datenberichtigung

Komplizierter als die Löschung von Daten, könnte im vorliegenden Fall die Berichtigung der Daten werden. Zwar wäre es auch hier möglich, den bereits übermittelten Datensatz durch Vernichtung des privaten Schlüssels zu löschen. Ein erneutes Überschreiben der Versandadresse durch den Token Inhaber ist jedoch nicht vorgesehen. Hier wäre vermutlich eine Anpassung des Smart Contracts erforderlich gewesen, bzw. eine Offchain-Berichtigung, also eine Löschung der Daten innerhalb und eine Speicherung außerhalb der Blockchain.

2.4.4 Technische und organisatorische Maßnahmen

Im Hinblick auf die zu treffenden technischen und organisatorischen Maßnahmen kann ein OnChain-Shop durchaus Vorteile gegenüber einem klassischen Online-Shop aufweisen. Insgesamt dürfte ein OnChain-Shop auf Grund seiner Dezentralisierung nur eine überschaubare Infrastruktur auf Seiten des Shop Betreibers erfordern, denn es ist keine Registrierung mit personenbezogenen Daten erforderlich. Etwaige Anmelde- und Versanddaten müssen nicht auf Servern des Shop Betreibers gespeichert werden. Darüber hinaus kommt es vorliegend nicht auf die Sicherheit von klassischen Webapplikationen oder Webshop-Frameworks an, die immer wieder Angriffspunkte für Hacker bieten.

3 Fazit und Ausblick

Insgesamt fällt das datenschutzrechtliche Fazit im Hinblick auf die Bewertung des OnChain-Shops erstaunlich gut aus. Möglicherweise ist es an der Zeit, mit dem Vorurteil aufzuräumen, dass Blockchain-Anwendungen per se mit dem Datenschutz unvereinbar sind,[9] denn die Österreichische Post hat vorliegend etwas geschafft, was kaum ein Online-Shop leisten kann: Die Möglichkeit anonym einzukaufen.

Das konkrete Beispiel des OnChain-Shops der Österreichischen Post ist dabei nur eine mögliche Ausprägung eines OnChain-Shops. Möglicherweise gibt es künftig auch OnChain-Shops, die auf anderen Blockchain-Technologien basieren und deren datenschutzrechtliche Eigenschaften klug einsetzen. So gibt es bei einigen Blockchains bereits Ansätze, die Transaktionshistorien zu verschleiern. Zudem existieren verschiedene Ansätze der Datenspeicherung in Blockchain Umgebungen. Es ist z. B. denkbar, dass die Daten an sich gar nicht innerhalb der Blockchain gespeichert werden, sondern gewisse Teile der Datenspeicherung außerhalb der Blockchain vorgenommen werden.[10] Auch hier gibt es dann wieder zentrale und dezentralisierte Ansätze. In Zukunft wird es bei der Bewertung konkreter Projekte erforderlich sein, diese technischen Sachverhalte in der juristischen Bewertung angemessen zu berücksichtigen und der Technologie nicht von vornherein eine Absage zu erteilen.

6 Vgl. *Courtois, Mercer*: Stealth Address and Key Management Techniques in Blockchain Systems, abrufbar unter https://www.scitepress.org/Papers/2017/62700/62700.pdf (letzter Abruf 30.6.2019).

7 Vgl. *Bundesamt für Sicherheit in der Informationstechnik*, Blockchain sicher gestalten (abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf), Ziffer 5.4 (letzter Abruf 30.6.2019).

8 Z. B. das sog. „MimbleWimble-Protokoll, welches Transaktionen nicht öffentlich durchführt.

9 Vgl. hierzu z. B. den aktuellen 1. Tätigkeitsbericht der LfDI Bremen, Ziffer 5.3: *„Der große Trend Blockchain hat auch uns in Form allgemeiner Anfragen erreicht. Wir vertreten dabei grundsätzlich die Auffassung, dass insbesondere die Artikel 16 (Recht auf Berichtigung) und Artikel 17 (Recht auf Löschen) der Datenschutzgrundverordnung (DSGVO) nur schwer mit der Integrität und Vertraulichkeit der Blockchain in Einklang zu bringen sind."*

10 *Vgl. Bacon/ Michels/ Millard / Singh,* Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers, 25 Rich. J.L. & Tech., no. 1, 2018 (abrufbar unter https://jolt.richmond.edu/files/2018/11/Michelsetal-Final-1.pdf), Ziffer 6.2, Absatz 163 (letzter Abruf 30.6.2019).