Grußwort des Forschungsprojektleiters »BayWiDI« Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur achten Ausgabe des BayWiDI-Newsletters. Ich freue mich sehr Ihnen mitteilen zu können, dass mein Lehrstuhl zusammen mit Prof. Dr. Thomas Riehm, Anne Paschke und Ninja Marnau vom CISPA – Helmholz Zentrum i.G. in Saarbrücken den Zuschlag für das BSI Forschungsprojekt 356 im Rahmen einer europaweiten Ausschreibung erhalten hat. Ziel dieses Projektes ist die Erarbeitung von Eckpunkten für die Regulierung der IT-Sicherheit für die nächsten Jahre. Der folgende Beitrag wird das Vorhaben näher beleuchten.

Durch die Geltungserlangung der Datenschutzgrundverordnung (DS-GVO) am 25. Mai 2018 ergeben sich einige Änderungen im Hinblick auf die Vorgaben zum Datensicherheits- und auch IT-Sicherheitsrecht. Die DS-GVO bringt teilweise umfassende Neuerungen mit sich, deren Auswirkungen und Umsetzungserfordernisse noch nicht vollständig absehbar sind. In diesem Newsletter befindet sich daher eine Übersicht über die datensicherheitsrechtlichen Neuerungen der DS-GVO im Vergleich zum derzeit noch geltenden Bundesdatenschutzgesetz.

Auch auf der Ebene des „Internet of Things" trifft die Europäische Union neue Regelungen. So besteht ab dem 31. März 2018 für Autohersteller die Pflicht, neue Fahrzeuge mit einem „auf dem 112-Notruf basierenden bordeigenen eCall-System" auszustatten.[1] Dieses System wird bei einem Unfall entweder manuell oder mittels Sensoren automatisch aktiviert und stellt über das Mobilfunknetz eine Tonverbindung zwischen den Fahrzeuginsassen und einer eCall-Notrufabfragestelle her. Das Europäische Parlament geht davon aus, dass hierdurch jedes Jahr 2.500 Menschenleben gerettet werden können.

Aber nicht nur die Vernetzung der Welt, sondern auch die Schaffung beweissicherer digitaler Transaktionen verändert unseren Alltag. Die Blockchain-Technologie wird derzeit medial als die Lösung für viele technische Probleme und IT-Unsicherheiten präsentiert. Aus diesem Grund soll ein kurzer Überblick über die Relevanz dieser Technologie für den Bereich der IT-Sicherheit präsentiert werden.

Zudem möchte ich Sie herzlich zu unserem am 11. und 12. April 2018 stattfindenden 13. Internationalen For..Net Symposium mit dem Titel „Wertschöpfung durch Digitalisierung: Innovation. Ethik. Sicherheit." einladen. Neben der Forschungsstelle für Rechtsfragen der Digitalisierung (FREDI) ist erstmals auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) unser Kooperationspartner. Genaueres zum Inhalt dieses Symposiums können Sie ebenfalls diesem Newsletter entnehmen.

Ich wünsche Ihnen nun viel Spaß bei der Lektüre des Newsletters!

Ihr Prof. Dr. Dirk Heckmann,
Leiter des Forschungsprojekts »BayWiDI«

1 Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG.

Inhalt

- »IT-Sicherheit ist Lebenssicherheit« BSI Forschungsprojekt 356 / 2
- 13. Internationales For..Net Symposium »Wertschöpfung durch Digitalisierung – Innovation. Ethik. Sicherheit.« am 11. und 12. April 2018 in Passau / 3
- Alles neu macht der Mai? – Ein Vergleich der Regelungen zur Datensicherheit in DS-GVO und BDSG a.F. / 4
- Die Bedeutung der Blockchain-Technologie für die Schaffung von IT-Sicherheit / 8
- Impressum / 11

„IT-Sicherheit ist Lebenssicherheit“

BSI Forschungsprojekt 356

Ob digitale Assistenzsysteme, E-Government, Gesundheits-Apps oder autonomes Fahren: Die vielfältigen Vorteile, die die Digitalisierung unseres Alltags und unserer Arbeitswelt mit sich bringt, bergen auch Risiken. Durch unsichere Hard- und Software können schlimmstenfalls Kunden- oder Unternehmensdaten gestohlen, Gesundheitsdaten manipuliert oder smarte Fahrzeuge gehackt und ferngesteuert werden. Ohne eine zuverlässige IT-Sicherheit, die die Verfügbarkeit, Integrität und Vertraulichkeit von Daten und IT-Systemen gewährleistet, kann unser digitales Leben nicht gelingen. Mit immer weiter fortschreitender Digitalisierung nimmt so auch das Bedürfnis nach funktionierenden IT-Sicherheitskonzepten weiter zu. Dabei ist dies nicht nur eine Frage der Technik, sondern auch eine juristische Herausforderung. Wie können Unternehmen dazu bewegt werden, IT-Sicherheit wirksam umzusetzen? Kann dies besser durch Gebote und Strafen oder durch Zertifizierungen und Gütesiegel erreicht werden? Wer soll im Falle eines Schadens in welchem Umfang haften? Welche Pflichten können dem Verbraucher in diesem Bereich auferlegt werden? Wie ist ein angemessenes IT-Sicherheitsniveau überhaupt zu qualifizieren?

„IT-Sicherheit ist Lebenssicherheit“, so Projektleiter Prof. Dr. Dirk Heckmann. Deshalb soll in den Jahren 2018 und 2019 im Rahmen des Forschungsprojekts 356, welches durch das BSI mit 400.000 Euro gefördert wird, nach Regulierungsmöglichkeiten in diesem Bereich geforscht werden. Ziel ist es, Richtlinien für die Gewährleistung von IT-Sicherheit aufzustellen. Hierfür soll unter anderem eine Rechtsdogmatik der IT-Sicherheit herausgearbeitet sowie der konkrete Regulierungsbedarf ermittelt werden. Zudem werden betroffene Verbände, Institutionen und Unternehmen in die Entwicklung und Forschung miteinbezogen, um praxisnahe und zukunftsorientierte Regulierungsvorschläge zu erarbeiten.

Sollten Sie Teil diese Projekts werden wollen und Ihr Wissen in die zukünftige Regulierung der IT-Sicherheit miteinfließen lassen, wenden Sie sich bitte an: *heckmann@uni-passau.de*

Projektteam

Prof. Dr.
Dirk Heckmann

Prof. Dr.
Thomas Riehm

Ninja Marnau

Anne Paschke

13. Internationales For..Net Symposium »Wertschöpfung durch Digitalisierung – Innovation. Ethik. Sicherheit.« am 11. und 12. April 2018 in Passau

Die gesamtwirtschaftliche digitale Wertschöpfung betrug 2016 in Deutschland rund 330 Milliarden Euro. So resümiert die Studie „Neue Wertschöpfung durch Digitalisierung", die die Vereinigung der Bayerischen Wirtschaft (vbw) im letzten Jahr veröffentlicht hat. Es gibt keinen Lebens- oder Wirtschaftsbereich, den Digitalisierung nicht erfasst oder gar umwälzt. Wo bleiben dabei Werte wie Persönlichkeitsschutz und Autonomie? Wo bleibt der Mensch? Der Einsatz künstlicher Intelligenz, die Entwicklung innovativer Apps, Vernetzung und Automatisierung im Gesundheitswesen und im Straßenverkehr sind nur einige der Themenfelder, die unter rechtlichem und ethischem Blickwinkel im Rahmen dieses Symposiums betrachtet werden. Außerdem wird der Entwurf eines Gesetzes zur Verbesserung des Persönlichkeitsrechtsschutzes vorgestellt, den der Leiter der Forschungsstelle Prof. Dr. Dirk Heckmann und die Geschäftsführerin der Forschungsstelle Anne Paschke auf Initiative der ARAG Rechtsschutzversicherung verfasst haben.

Während es am ersten Veranstaltungstag um grundsätzliche Herausforderungen technischer Innovationen aus rechtlicher und (unternehmens-)ethischer Perspektive geht, widmet sich der zweite Tag konkreten Fragen, die insbesondere die am 25. Mai 2018 in Kraft tretende Datenschutzgrundverordnung aufwirft. Das genaue Veranstaltungsprogramm ist unserem Flyer zu entnehmen. Dieser ist unter folgendem Link abrufbar:

https://www.for-net.info/wp-content/uploads/2018/03/Symposium2018-Flyer.pdf

Das Symposium sieht sich als Plattform und Impulsgeber für eine werteorientierte und sichere Internetnutzung. Es richtet sich an Interessierte aus Wissenschaft und Wirtschaft, Recht und Gesellschaft. Kooperationspartner ist neben der Forschungsstelle für Rechtsfragen der Digitalisierung (FREDI) erstmals auch das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Im Mittelpunkt des Symposiums steht deshalb auch das Forschungsprojekt zur IT-Sicherheitsregulierung, das die Universität Passau unter der Leitung von Prof. Dr. Dirk Heckmann für das BSI in den Jahren 2018 und 2019 durchführen wird. Zwei der beteiligten Wissenschaftler berichten über die aktuellen Projekterkenntnisse und stellen sich der Frage: Welchen Beitrag kann das Recht zu einer Verbesserung des IT-Sicherheitsniveaus leisten?

Die zweitägige Fachveranstaltung in den Passauer Redoutensälen hat ein besonderes kulturelles Rahmenprogramm. Während des traditionellen Galaabends auf der Veste Oberhaus wird bereits zum 5. Mal der For..Net-Award, ein Preis für Innovationen zu Datenschutz und IT-Sicherheit, verliehen.

Wir hoffen, dass wir Ihr Interesse wecken konnten und freuen uns über Ihre Anmeldung. Ein Tagungsbeitrag wird nicht erhoben, eine Anmeldung ist jedoch erforderlich. Um diese wird unter folgendem Link gebeten:

https://www.for-net.info/symposien/13-internationales-for-net-symposium/anmeldung/

Sie sind herzlich eingeladen uns auch unter @ForNet_Passau auf Twitter zu folgen. Dort werden Sie mit aktuellen Nachrichten vor und während der Veranstaltung versorgt. Darüber hinaus können Sie unter #fornet18 aktiv an Diskussionen teilhaben.

for..net
Forschungsstelle für IT-Recht und Netzpolitik

Alles neu macht der Mai?

Ein Vergleich der Regelungen zur Datensicherheit in DS-GVO und BDSG a.F.

Am 25. Mai 2018 erlangt die europäische Datenschutzgrundverordnung Geltung. Gleichzeitig wird damit das derzeit noch geltende BDSG a.F. obsolet. Dieses wird durch ein neues BDSG ersetzt, welches einerseits eine Spezifizierung der DS-GVO vornimmt und andererseits die EU-Richtlinie für den Datenschutz bei Polizei und Justiz (JI-Richtlinie) in nationales Recht umsetzt.[1] Grund genug um sich einen Überblick darüber zu verschaffen, welche Neuerungen die DS-GVO auf dem Gebiet der IT-Sicherheit mit sich bringt.

§ 9 BDSG a.F. und Art. 32 DS-GVO

Die bisherigen Vorgaben zur Datensicherheit wurden bisher zentral in § 9 BDSG a.F. sowie der dazugehörigen Anlage geregelt.[2] Diese Regelungen werden nunmehr durch Art. 32 DS-GVO umfassend ersetzt.

1. Zielsetzung und Adressaten

Ziel von § 9 BDSG a.F. war die Umsetzung des Datenschutzrechts auf technischer Ebene: Den Schutz des Einzelnen vor einer Beeinträchtigung in seinem Persönlichkeitsrecht durch den Umgang mit personenbezogenen Daten, § 1 Abs. 1 BDSG a.F.[3] Dies sollte dadurch erreicht werden, dass die verantwortlichen Stellen und Auftragsverarbeiter dazu verpflichtet wurden, die organisatorischen und technischen Maßnahmen zu ergreifen die notwendig waren, um Gefahren für die Daten der Betroffenen zu minimieren.[4] Der Anforderungskatalog der Anlage zu § 9 BDSG a.F. beschränkte sich auf die automatisierte Datenverarbeitung.

Art. 32 DS-GVO zielt ebenfalls auf „Daten- und Systemsicherheit“[5] ab und will einen Ausgleich zwischen dem Schutzbedürfnis des Betroffenen und seiner Daten sowie den wirtschaftlichen Interessen der verarbeitenden Stellen schaffen.[6] Die Vorschrift richtet sich gleichermaßen an Verantwortliche und Auftragsverarbeiter, also den Kreis der Personen, der die Verarbeitung selbst durchführt oder im rechtlichen Sinne dafür verantwortlich ist.[7] Es werden dabei sowohl automatisierte als auch nicht automatisierte Datenverarbeitungen erfasst.[8]

Art. 32 DS-GVO
Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit

1 BGBl. I 2017, 2132.

2 *Ernestus*, in: Simitis, BDSG, 8. Aufl. 2014, § 9 Rn. 1.

3 *Karg*, in: Wolff/Brink, BeckOK, Datenschutzrecht, 22. Edition 2017, § 9 BDSG Rn. 37.

4 BT-Drs. 17/8999, S. 29; OVG Hamburg v. 7. 7. 2005 - 1 Bf 172/03 - NJW 2006, 310, 313.

5 *Jandt*, in: Kühling/Buchner, Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 32 Rn. 1.

6 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 26.

7 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 27.

8 *Schaffland/Holthaus*, in: Schaffland/Wiltfang, DS-GVO, Art. 32 Rn. 1.

der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

2. Einzelne Maßnahmen, Art. 32 Abs. 1 Satz 1 Hs. 2 DS-GVO

Bei einem ersten Vergleich zwischen den in Art. 32 Abs. 1 DS-GVO zu erreichenden Zielen und Maßnahmen und den in der Anlage zu § 9 BDSG a.F. aufgeführten Anforderungen, scheint die DS-GVO – allein schon aufgrund ihres Umfangs – grundsätzlich hinter der aktuellen deutschen Rechtslage zurückzubleiben, was den Grad der Detaillierung betrifft.[9]

In Art. 32 Abs. 1 Satz 1 Hs. 2 DS-GVO wird ein Maßnahmenkatalog aufgeführt, mit dessen Hilfe das jeweilige Schutzniveau erreicht werden soll. Dieser ist allerdings nicht abschließend formuliert. Es sind also unter Umständen weitere Vorkehrungen zu treffen.[10] Ebenso lieferte jedoch auch die Anlage zu § 9 BDSG a.F. keinen abschließenden Katalog, sondern lediglich allgemeine, gegebenenfalls zu ergänzende Anforderungen.[11]

Die in der Anlage zu § 9 BDSG a.F. viel kritisierte[12] fehlende Auflistung von allgemein anerkannten Schutzzielen des IT-Sicherheitsrechts – Vertraulichkeit, Integrität und Verfügbarkeit – wird nun vom Maßnahmenkatalog des Art. 32 Abs. 1 Satz 1 Hs. 2 DS-GVO vorgenommen. Die „acht Gebote der Datensicherheit“[13] der Anlage zu § 9 BDSG a.F. entsprechen in ihrem Inhalt teilweise diesen Anforderungen.[14]

Bisher nannten § 9 BDSG a.F. und die Anlage lediglich die Verschlüsselung als geeignete Maßnahme zur Datensicherung. Art. 32 Abs. 1 Satz 1 Hs. 2 lit. a DS-GVO übernimmt diese und ergänzt sie um die Pseudonymisierung.[15] Neu ist außerdem die ausdrückliche Erwähnung der Sicherstellung der Belastbarkeit der Systeme und Dienste.[16] Unklar ist allerdings bislang, wie der Begriff der „Belastbarkeit der Systeme“ in Art. 32 Abs. 1 Satz 1 Hs. 2 lit. b DS-GVO zu verstehen ist, da dieser dem deutschen Recht fremd ist.[17] So wird beispielsweise angenommen, dass die erforderliche Belastbarkeit dann vorliegt, wenn die Funktionsfähigkeit des Datenverarbeitungssystems auch starkem Zugriff standhält, wie er beispielsweise bei DoS- oder DDoS-Attacken[18] auftritt.[19]

Art. 32 Abs. 1 Satz 1 Hs. 2 lit. c DS-GVO greift noch einmal das Schutzziel „Verfügbarkeit“ auf und stellt klar, dass dies nicht nur präventiv zu verstehen ist, sondern auch eine „rasche Widerherstellung“ der Daten nach einem Zwischenfall gewährleistet sein muss.[20] Was genau mit dem Begriff „rasch“ gemeint ist, lässt sich dieser Vorschrift nicht entnehmen, die Übersetzung der englischen Fassung spricht von einem „angemessenen Zeitraum“.[21]

Zuletzt führt Art. 32 Abs. 1 Satz 1 Hs. 2 lit. d DS-GVO eine neue Pflicht zur regelmäßigen Überprüfung der technischen und organisatorischen Maßnahmen auf ihre Wirksamkeit ein. Dadurch soll sichergestellt werden, dass sich getroffene Maßnahmen dauerhaft auf dem Stand der Technik befinden und ggf. angepasst oder verändert werden.[22] Im

9 Kritisch hierzu: *Wybitul*, BB 2016, 1077, 1080; *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl. 2016, § 7 Rn. 21.

10 *Schreibauer/Spittka*, in: Wybitul, EU-Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 32 Rn. 30.

11 *Ernestus*, in: Simitis, BDSG, 8. Aufl. 2014, § 9 Rn. 47.

12 So unter anderem *Karg*, in: Wolff/Brink, BeckOK, Datenschutzrecht, 19. Edition 2017, § 9 BDSG Rn. 3.

13 *Jergl*, in: Veil, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 32 Rn. 9.

14 *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 32 Rn. 36.

15 *Schreibauer/Spittka*, in: Wybitul, EU-Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 32 Rn. 32.

16 *Schreibauer/Spittka*, in: Wybitul, EU-Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 32 Rn. 32.

17 Vgl. *Barlag*, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, § 3 Rn. 199.

18 „(Distributed) Denial of Service“, vgl. hierzu *Gerlach*, CR 2015, 581, 585.

19 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 39.

20 *Kramer/Meints*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Auflage 2017, Art 32 DS-GVO Rn. 29.

21 *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 1. Auflage 2017, Art. 32 Rn. 9.

22 *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, 1. Auflage 2017, Art. 32 Rn. 20.

Falle eines besonders hohen anzunehmenden Risikos für besonders empfindliche personenbezogene Daten kann es damit erforderlich sein, sogenannte Penetrationstests[23] durchzuführen.[24]

3. Verhaltensregeln, Zertifizierung, Art. 32 Abs. 3 DS-GVO

Gemäß Art. 32 Abs. 3 DS-GVO kann der Nachweis, dass die in Art. 32 Abs. 1 geforderten Maßnahmen erbracht wurden, durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder durch ein genehmigtes Zertifizierungsverfahren gemäß Art. 42 DS-GVO erbracht werden. Daraus kann geschlossen werden, dass die Beweispflicht für die Einhaltung der Maßnahmen dem Verantwortlichen bzw. dem Auftragsverarbeiter obliegt.[25]

Somit wird erstmals in der DS-GVO auf das Instrument der „regulierten Selbstregulierung“[26] zurückgegriffen. Hierdurch wird die Überwachung der Normanwendung teilweise in die Hände von nichtstaatlichen Stellen gelegt, indem das Bereithalten von Zertifikaten oder die Erfüllung von gewissen Verhaltensregeln eine Indizwirkung für die Regelkonformität des Systems erfüllt.[27]

4. Interne Sicherheitsmaßnahmen, Art. 32 Abs. 4 DS-GVO

Art. 32 Abs. 4 DS-GVO richtet sich an den Verantwortlichen und an den Auftragsverarbeiter und verlangt von ihnen, dass die Verarbeitung personenbezogener Daten durch die ihnen unterstellten Personen nur auf Anweisung erfolgen soll und die Einhaltung der Weisung kontrolliert wird. Damit wird sowohl die Verpflichtung auf das Datengeheimnis aus § 5 Satz 2 BDSG a.F. umgesetzt,[28] als auch die Zugriffs-, Weitergabe- und Eingabekontrolle nach der Anlage zu § 9 BDSG a.F. eingehalten.[29] Hierzu sind geeignete Maßnahmen zur Sicherstellung zu treffen.

Wie diese konkret auszusehen haben, ist noch nicht vollständig geklärt und wird einzelfallabhängig zu entscheiden sein, es wird unter anderem über (Selbst-) Verpflichtungserklärungen, regelmäßige Schulungsmaßnahmen und die Durchführung von Sensibilisierungsmaßnahmen diskutiert.[30]

5. Verhältnismäßigkeitsgrundsatz, Art. 32 Abs. 1 DS-GVO

Müssten nun uneingeschränkt alle theoretisch möglichen IT-Sicherheits-Maßnahmen umgesetzt werden, so würde dies für die Verarbeiter eine erhebliche wirtschaftliche und zeitintensive Belastung darstellen. Dies würde in vielen Fällen zu ungerechtfertigten Eingriffen in die Eigentumsfreiheit (Art. 14 GG) und mittelbar auch in die Berufsfreiheit (Art. 12 GG) führen, da der Aufwand teilweise nicht im Verhältnis zur Schutzbedürftigkeit der konkret verarbeiteten Daten stehen würde. Deshalb wurde als Korrektiv der Grundsatz der Verhältnismäßigkeit in § 9 Satz 2 BDSG a.F. bzw. in Art. 32 Abs. 1 DS-GVO verankert. Dieser lässt eine Abwägung zwischen dem Aufwand und dem zu erreichenden Schutzzweck zu.[31] Es wird also kein absolutes Schutzniveau gefordert. Zur Ermittlung des konkreten Niveaus hat der Datenverarbeiter eine Risikoanalyse durchzuführen, basierend auf der theoretisch höchstmöglichen Gefahr für die zu verarbeitenden Daten.[32] Auf dieser Grundlage sind die entsprechenden Maßnahmen zu treffen. Der Einleitungssatz zur Anlage zu § 9 BDSG a.F. unterstreicht dieses Erfordernis für die automatisierte Verarbeitung, indem auf die Art der zu schützenden personenbezogenen Daten abgestellt wird.[33] Unter den Aufwand für den Verarbeiter sind dabei alle Kosten zu fassen, die aufgrund der jeweiligen Maßnahme anfallen, unter anderem Entwicklungskosten, Investitionskosten oder Betriebskosten.[34] Nicht erfasst werden die Kosten, die ohnehin durch die ordnungsgemäße Verarbeitung personenbezogener Daten fällig werden würden.[35] Strittig ist nach aktueller Rechtslage, ob der in der Anlage zu § 9 BDSG a.F. erwähnte „Stand der Technik“ nur auf eben diese Anwendung finden soll,[36] oder ob er als Maßstab für den gesamten § 9 BDSG a.F. heranzuziehen ist.[37]

Auch Art. 32 Abs. 1 DS-GVO spricht von einem „dem Risiko angemessenen Schutzniveau“ und fordert damit ebenfalls keine absolute Sicherheit, sondern lässt eine Abwägung zu. Damit wird Art. 52 Abs. 1 S.2 GRCh umgesetzt, der die Einschränkung von Grundrechten nur unter Wahrung der Verhältnismäßigkeit zulässt. Abwägungskriterien zur Bestimmung der Geeignetheit einer Maßnahme sind die Kosten, die Art und Weise der Verarbeitung, die Risiken für die Rechte und Freiheiten natürlicher Personen und der Stand der Technik. Durch letzteres ist der oben genannte Streit in Zukunft gegenstandslos. Jedoch herrscht hier Unklarheit darüber, ob die neuesten technischen Entwicklungen oder nur schon bekannte und erprobte, also verfügbare, Standards gemeint sind.[38] Zieht man hier Erwägungsgrund 83 Satz 4 heran, der vom „verfügbaren Stand der Technik“ in Bezug auf Verarbeitungsvorgänge

23 Zu deren Zulässigkeit: *Krischker*, ZD 2015, 464.

24 *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 32 Rn. 20.

25 *Schreibauer/Spittka*, in: Wybitul, EU-Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 32 Rn. 19.

26 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 62.

27 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 62.

28 *Kramer/Meints*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Auflage 2017, Art. 32 DS-GVO Rn. 52.

29 *Schreibauer/Spittka*, in: Wybitul, EU-Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 32 Rn. 22.

30 *Jergl*, in: Veil, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 32 Rn. 50.

31 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 73.

32 *Ernestus*, in: Simitis, BDSG, 8. Aufl. 2014, § 9 Rn. 39.

33 *Ernestus*, in: Simitis, BDSG, 8. Aufl. 2014, § 9 Rn. 58.

34 *Ernestus*, in: Simitis, BDSG, 8. Aufl. 2014, § 9 Rn. 34.

35 *Ernestus*, in: Simitis, BDSG, 8. Aufl. 2014, § 9 Rn. 36.

36 *Gitter/Meißner/Spauschus*, ZD 2105, 512, 516.

37 *Karg*, in: Wolff/Brink, BeckOK, Datenschutzrecht, 22. Edition 2017, § 9 BDSG Rn. 67.

38 *Piltz*, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 32 Rn. 15.

mit hohem Risiko spricht, so ergibt sich im Umkehrschluss, dass dieser Standard auch alle anderen, weniger risikointensiven Vorgänge umfassen muss.[39] Art. 32 Abs. 1 DS-GVO stellt weiterhin nur noch auf die Implementierungskosten ab, also solche, die für die Integration der Maßnahme in das jeweilige Verarbeitungssystem anfallen, wobei Folgekosten nicht mehr zu berücksichtigen sind.[40]

Im Gegensatz zum § 9 BDSG a.F. nennt Art. 32 Abs. 1 DS-GVO nun explizit Kriterien zur Risikobestimmung und kann so Klarheit und ein höheres Maß an Rechtssicherheit schaffen.[41] Ergänzt wird dies durch Art. 32 Abs. 2 DS-GVO, der konkret zu beachtende Risiken nennt, nämlich die Vernichtung, den Verlust und die Veränderung personenbezogener Daten. Erwägungsgrund 84 Satz 2 ist außerdem zu entnehmen, dass die Ergebnisse einer etwaigen Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ebenfalls in diese Analyse miteinzubeziehen sind.[42]

6. Verschärfung der Bußgelder, Art. 83 DS-GVO

Bei Verstößen gegen Art. 32 DS-GVO können gemäß Art. 83 DS-GVO Bußgelder verhängt werden.[43] Art. 83 Abs. 4 lit. a DS-GVO sieht hierfür Geldbußen in Höhe von bis zu 10 Mio. EUR bzw. im Falle eines Unternehmens bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs vor. Werden die in Art. 32 DS-GVO geforderten Maßnahmen sowie die genehmigten Verhaltensregeln gemäß Art. 40 DS-GVO oder die genehmigten Zertifizierungsverfahren nach Art. 42 DS-GVO getroffen, führt dies gemäß Art. 83 Abs. 2 lit. d und lit. j DS-GVO im Falle eines Verstoßes zur Strafmilderung.

Bereichsspezifische datenschutzrechtliche Normen und Art. 32 DS-GVO

Durch die DS-GVO werden noch weitere Vorschriften zur Datensicherheit, z.B. § 78 SGB X (dieser regelt die Zweckbindung von Daten im Sozialverwaltungsverfahren und die Geheimhaltungspflicht eines Dritten, an den diese übermittelt werden), § 109 TKG, §§ 7, 13 Abs. 4 TMG, § 21e EnWG, § 8a BSI berührt. Soweit die DS-GVO diesbezüglich keine Bereichsausnahme regelt, werden diese Vorschriften durch den Anwendungsvorrang des Unionsrechts verdrängt.[44]

Ein besonderes Problem besteht im Falle des § 109 TKG, der auf Grundlage der ePrivacy-Richtlinie 2002/58/EG erlassen wurde. Art. 95 DS-GVO sieht ausdrücklich vor, dass keine über die ePrivacy-Richtlinie hinausgehenden Pflichten entstehen sollen. Auf dieser Basis wird davon ausgegangen, dass Vorschriften, die aufgrund dieser Richtlinie erlassen wurden, dann lex specialis darstellen, wenn sie dieselbe Zielrichtung verfolgen und Datenverarbeitungen im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste betreffen.[45] Gleiches ist wohl auch für Vorschriften des TMG anzunehmen, soweit sie auf dieser Richtlinie beruhen. Sobald jedoch die ePrivacy-Verordnung in Kraft tritt, ersetzt diese die ePrivacy-Richtlinie und gilt unmittelbar, so dass die entsprechenden nationalen Regelungen zurücktreten, sofern sie nicht zuvor aufgehoben worden sind.

Der technische Datenschutz soll auch im Bereich der Verarbeitung von personenbezogenen Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen umgesetzt werden. Die hierfür relevante Vorschrift findet sich in § 64 BDSG 2018, der auf der JI-Richtlinie (RL (EU) 2016/680 – JI-RL) beruht.

Fazit

Scheint Art. 32 DS-GVO auf den ersten Blick weniger ausführlich als § 9 BDSG a.F. und dessen Anlage, so wird bei genauerer Betrachtung deutlich, dass diese in weiten Teilen ähnlich sind. Durch das zielorientiertere Normkonzept ist es in Zukunft einfacher, individuelle Konzepte in diesem Bereich zu nutzen.[46] Das ausdrückliche Abstellen auf den Stand der Technik bietet Raum für Entwicklungen und kann Fortschritt ermöglichen, sorgt dabei jedoch für einen gewissen Grad an Unbestimmtheit. Wegen des dynamischen Wandels der Materie, dem Wissensgefälle zwischen Normgeber und Normanwender und der Notwendigkeit von technischen Standards ist es zu begrüßen, dass sich der Gesetzgeber explizit für das Instrument der regulierten Selbstregulierung entschieden hat und somit Offenheit für Innovation zum Ausdruck bringt. Aufgrund der neuen Sanktionsmöglichkeit der Nichtbeachtung von Datensicherheit ist davon auszugehen, dass diese nun stärkere Beachtung findet. Eine mögliche Hilfestellung hierzu gibt der Unionsgesetzgeber durch Zertifizierungsmaßnahmen und Verhaltensregeln, wobei abzuwarten bleibt, wie diese tatsächlich umgesetzt werden.

Paschke/Raab

39 *Piltz*, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 32 Rn. 18; *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 1. Auflage 2017, Art. 32 Rn. 5.

40 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 60.

41 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 74.

42 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 49.

43 *Karger/Gaycken*, in: Fargó/Helfrich/Schneider, Betrieblicher Datenschutz, 2. Aufl. 2017, Kapitel 5 Rn. 128.

44 *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DS-GVO Rn. 78.

45 *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 32 Rn. 34.

46 *Grages*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 32 DS-GVO Rn. 4.

Die Bedeutung der Blockchain-Technologie für die Schaffung von IT-Sicherheit

Was die Blockchain-Technologie verspricht, klingt wie der heilige Gral der IT-Sicherheit: Verfügbarkeit von Daten durch Dezentralität, Vertraulichkeit durch Anonymität und Integrität durch kryptografisch gesicherte und öffentlich-überwachte Unveränderlichkeit. Doch kann die Blockchain-Technologie diese Versprechen halten? Darüber wie sicher, praxisrelevant und rechtskonform diese Technologie wirklich ist, soll dieser Beitrag einen kurzen Überblick geben.[1]

Die Funktionsweise der Blockchain

Aus Gründen der Klarheit muss vorangestellt werden, dass hier die Blockchain in der Weise beleuchtet wird, wie sie der Kryptowährung Bitcoin zugrunde liegt. Dabei handelt es sich um eine sogenannte „Public Permissioned Blockchain“[2], also eine öffentliche Blockchain, die jeder einsehen und editieren darf.

Für sich genommen ist eine Blockchain eine dezentrale Datenbank, in die Informationen chronologisch in sogenannten „Blocks“ zusammengefasst und anschließend durch eine kryptografische Verschlüsselung miteinander verbunden werden.[3] Aus jeder in einen Block zu integrierenden Information wird eine Prüfsumme, ein sogenannter „Hashwert“ berechnet. Die jeweiligen Hashwerte ergeben wiederum den Hashwert des gesamten Blocks. Weiterhin enthält jeder Block den Hashwert der gesamten Kette. Eine Veränderung an einer dieser Stellen würde sich so also auf die gesamte Kette auswirken und wäre unmittelbar sichtbar. Der Vorgang wird durch die „Miner“ durchgeführt, die dem Netzwerk ihre Rechenleistung zur Verfügung stellen. Alle Miner beginnen gleichzeitig, alle aktuell stattfindenden Transaktionen zu erfassen und versuchen währenddessen, eine komplexe mathematische Aufgabe zu lösen. Derjenige, der diese zuerst löst, darf seinen errechneten Block an die Blockchain anhängen und erhält eine Belohnung in Form von einem festen Betrag an Bitcoins. Alle anderen Teilnehmer dieses Peer-to-Peer-Netzwerkes, die sogenannten Nodes, prüfen diesen Block, gleichen ihn mit ihrer Blockchain ab und hängen ihn anschließend an ihre Blockchain an. Die Blockchain wird dabei an keinem zentralen Ort gespeichert, sondern existiert bei jedem einzelnen Teilnehmer des Netzwerkes. Gültig ist immer die längste und somit aktuellste Blockchain.

Für eine Transaktion von Bitcoins sind sowohl ein öffentlicher Schlüssel, vergleichbar mit einer Kontonummer, als auch ein privater Schlüssel, vergleichbar mit einem Passwort, erforderlich. Jede Transaktion muss durch den geheimen Schlüssel signiert werden, der zugehörige öffentliche Schlüssel ist hierbei für jeden sichtbar. Aufgrund der asymmetrischen Verschlüsselung der Schlüsselpaare ist es nicht möglich, den privaten Schlüssel durch den öffentlichen zu errechnen.[4] Ist eine Transaktion erfolgreich, so wird in den jeweiligen Block die Quelle und der Adressat der Bitcoins sowie der Betrag und das genaue Datum gespeichert und ist dauerhaft einsehbar. Das Ergebnis ist eine dezentrale, öffentliche und unabänderliche Verkettung von Transaktionsnachweisen.

Praktische Relevanz

Während es zwar denkbar ist, dass Unternehmen sich ihre eigene, private Blockchain schaffen, für ihre Zwecke konfigurieren und anschließend nutzen,[5] soll hierauf nicht weiter eingegangen werden. Es ist nämlich möglich, die bereits bestehende Bitcoin-Infrastruktur

1 Ausführlich hierzu: https://bitcoin.org/bitcoin.pdf, dieser und alle folgenden Links wurden zuletzt abgerufen am 27.02.2018.

2 Andere Konfigurationsmöglichkeiten der Blockchain: https://dl.gi.de/bitstream/handle/20.500.12116/3865/B13-1.pdf?sequence=1&isAllowed=y

3 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

4 https://www.it-finanzmagazin.de/gar-kein-mysterium-blockchain-verstaendlich-erklaert-27960/

5 So die Firma mb Support beim ersetzenden Scannen, https://www.mbsupport.de/index.php/news-artikel/78-100-digital-blockchain-zum-schutz-gegen-manipulation

abseits der Kryptowährung zu nutzen. Eine dieser Lösungen nennt sich „Colored Coins“ und funktioniert wie folgt:[6] Die Programmiersprache von Bitcoin erlaubt es, einen kleinen zusätzlichen Datensatz in eine Transaktion einzubinden und auf der Blockchain zu speichern. Es wird nun ein sehr kleiner Betrag von Bitcoins (bestehend aus dem technisch vorgegebenen Mindestbetrag und der Mindestgebühr) gesendet, der als Transportmedium der Informationen fungiert. Es wird also ein Colored Coin über einen Bitcoin „gestülpt“. Die Daten werden über eine entsprechende Zugangssoftware („Wallet“) integriert und ausgelesen. Für Miner und Nodes unterscheidet sich der Vorgang grundsätzlich nicht von den übrigen und wird wie jede andere Transaktion behandelt. Die so „erzeugten“ Coins können mit beliebigen Werten verknüpft werden. Dabei kann es sich zum Beispiel um eine eigene Kryptowährung, Aktien,[7] Nutzungsrechte, Eigentum oder Immaterialgüterrechte handeln. Die denkbaren Anwendungsbereiche sind somit breit gefächert und reichen von Mikro-Transaktionen im Bereich des Urheberrechts bis hin zu „Smart-Contracts“ im Bereich des Auto-Leasings. Die Vorteile dieses Systems zeichnen sich vor allem durch die vollumfängliche Nutzbarkeit der Bitcoin-Infrastruktur aus, die durch die große Anzahl an Teilnehmern als grundsätzlich sehr sicher einzustufen ist. Weiterhin ist der Einrichtungsaufwand gering und die Transaktionskosten niedrig.

Sicherheit

Seit mittlerweile neun Jahren ist kein Fall bekannt, in dem die Bitcoin-Blockchain selbst in ihrem Inhalt manipuliert wurde.[8] Trotzdem wurden bereits Millionen von Euros durch zahlreiche Hacks

gestohlen.[9] Die Schwachstellen sind hierbei hauptsächlich die Wallets oder Handelsplattformen und damit die jeweiligen privaten Schlüssel. Werden die Speicherorte der Schlüssel nicht ausreichend sicher geschützt, können sich Unbefugte hierzu Zutritt verschaffen, den Schlüssel auslesen, und sich damit die Bitcoins zu ihren eigenen Adressen transferieren. Dies kann theoretisch auch auf oben beschriebene Anwendungsgebiete außerhalb der Kryptowährung übertragen werden. Das Problem stellen hier also die externen Schnittstellen dar, die den Zugang zur Blockchain bieten.[10]

Eine bisher noch nicht im Zusammenhang mit Bitcoin[11] erfolgte Angriffsmethode nennt sich „51% Attack“.[12] Der Name beschreibt hier die Art des Angriffs: Verfügt eine Partei über mehr als 50% der Rechenleistung des gesamten Netzwerks, so ist die Wahrscheinlichkeit, dass diese als erste den nächsten Block berechnen kann, gleich eins.[13] Hierdurch kann diese Partei den Prozess der Berechnung von neuen Blocks monopolisieren, da kein anderer Miner vor ihm die Rechenaufgabe lösen und somit seinen Block an die Kette anhängen kann. Die Folgen wären, dass alle Belohnungen für die Errechnung der Blocks dieser Partei zufallen würden, sie einzelne Transaktionen blocken könnte oder selbst Transaktionen ausführen, diese wieder rückgängig machen und noch einmal vornehmen könnte und es so möglich wäre, Bitcoins doppelt auszugeben. Eine rückwirkende Änderung an der Blockchain ist mit dieser Methode allerdings nicht möglich. Während die drei größten Mining-Pools (Unternehmen, die über technische Anlage zur Berechnung der Blöcke verfügen) zusammen zwar über mehr als 50% der Rechenleistung verfügen und eine solche Attacke somit nicht völlig ausgeschlossen wäre, ist es durch den hohen Kostenaufwand wohl zurzeit rentabler, weiter als Miner am Netzwerk teilzunehmen.[14] Auch ist im Falle eines solch tiefgreifenden und für jeden Teilnehmer öffentlich einsehbaren Angriffs davon auszugehen, dass die Stabilität des gesamten Systems in Frage gestellt, der Wert der Währung rapide absinken und eventuell erbeutete Bitcoins erheblich in ihrem Wert gemindert werden würden.[15] Es ist jedoch auch anzumerken,

6 Vgl. ausführlich: https://blockchain-nachrichten.com/blockchaintechnologien/colored-coins

7 Nasdaq nutzt die Blockchain als Grundlage für eine Handelsplattform, http://ir.nasdaq.com/releasedetail.cfm?releaseid=912196

8 http://www.zeit.de/digital/internet/2018-02/bitcoin-energieverbrauch-strom-nachhaltigkeit

9 Februar 2014: 450 Millionen Dollar, https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-and-frauds/; Januar 2015: 5 Million Dollar, https://arstechnica.com/information-technology/2015/01/bitcoin-exchange-bitstamp-claims-hack-siphoned-up-to-5-2-million/; August 2016: 77 Millionen Dollar, https://arstechnica.com/information-technology/2016/08/bitcoin-value-falls-off-cliff-after-58m-in-btc-stolen-in-hong-kong-exchange-hack/

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Eckpunktepapier.pdf?__blob=publicationFile&v=3

11 Ein solcher Angriff wurde bereits 2017 auf die Kryptowährung „Krypton“ erfolgreich durchgeführt, https://cryptohustle.com/krypton-recovers-from-a-new-type-of-51-network-attack

12 Ausführlich hierzu: https://www.investopedia.com/terms/1/51-attack.asp

13 https://www.btc-echo.de/tutorial/bitcoin-51-attacke/

14 https://www.krypto-magazin.de/was-ist-eine-51-attacke/

15 https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_artikel.html

dass es beispielsweise für Regierungen, die ein Interesse an der Änderung oder Unterdrückung der Bitcoin-Blockchain oder anderen Kryptowährungen haben, ohne erheblichen Aufwand möglich wäre, dies entweder durch die Beschlagnahme oder durch den Bau eigener technischer Anlagen zu erreichen.[16] Problematisch ist dies vor allem im Hinblick darauf, dass die größten Miner in China agieren, da dort die idealen Bedingungen hierfür – vor allem niedrige Strompreise – herrschen.

Ein weiteres, bisher noch relativ unbekanntes Problem, stellt die Anwendung von Big-Data-Systemen und Algorithmen auf die Blockchain dar. So hat es sich das Unternehmen „Bitfury" mit seinem Programm „Crystal" zum Ziel gesetzt, die Anonymität der Blockchain teilweise aufzuheben.[17] Erreicht werden soll dies durch die Analyse unter anderem von Börsen, Internetforen und dem Deepweb. Dabei wird beispielsweise untersucht, in welchem Zusammenhang Bitcoin-Adressen aufgetreten sind, was mit ihnen gekauft wurde und wer die Beteiligten dieser Transaktionen waren. Dabei wird ein „Risk Score" errechnet, der darauf basiert, ob an der Transaktion bereits bekannte und mit fragwürdigen Handlungen in Verbindung gebrachte Operatoren beteiligt waren. Dieses Vorgehen ist aufgrund der Struktur der Blockchain sehr erfolgversprechend, da aufgrund des lückenlosen Transaktionsnachweises durch die Identifizierung nur eines einzelnen Teilnehmers umfangreiche Erkenntnisse über eine Transaktionskette getroffen werden können. Anhand dieser Daten könnten Strafverfolgungsstellen entscheiden, welche Transaktionen es wert sind, einer eingehenden Prüfung unterzogen zu werden oder hinter welchen Adressen sich potentielle Straftäter verstecken könnten. Auch private Stellen könnten gegen entsprechende Bezahlung Informationen über ihren Vertragspartner erhalten. Eine Deanonymisierung kann zwar teilweise sinnvoll sein, allerdings kann eine gänzliche Aufhebung der Anonymität in datenschutzrechtlicher Hinsicht kritisch gesehen werden.

Rechtliches

Durch die Dezentralität des Systems und einer daraus folgenden hohen Ausfallsicherheit (kein „Single Point of Failure") sowie der Unabänderbarkeit der Daten und der vermeintlichen Anonymität scheint die Blockchain-Technologie grundsätzlich wie geschaffen für einen wirksamen Datenschutz zu sein.

Allerdings gibt es auch Kritik. Aufgrund der Komplexität der Materie wird im Folgenden aus datenschutzrechtlicher Perspektive hauptsächlich auf das Recht auf Vergessenwerden eingegangen.[18]

Zuerst ist zu klären, ob in den Daten ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 Hs. 1 Var. 2 DS-GVO vorliegt und der Betroffene „identifizierbar" ist. Dies ist weit auszulegen und auch schon dann anzunehmen, wenn es erst mit der Hilfe eines Dritten unter verhältnismäßigem Aufwand möglich ist, Daten zuzuordnen.[19] Von außen ist nur der öffentliche Schlüssel des Betroffenen sichtbar, der lediglich eine zufällig generierte Zahlenfolge darstellt. Registriert sich dieser jedoch mit seinem Schlüsselpaar beispielsweise auf einer Handelsplattform oder einer Zugangssoftware und gibt dort seinen Klarnamen preis, so können die Schlüssel der Person und den jeweiligen Transaktionen zugeordnet werden, woraus sich Auskünfte über persönliche Beziehungen und finanzielle Mittel ergeben können. Der niedrige Aufwand, der hierfür erforderlich ist, wird am Beispiel der größten deutschen Bitcoin-Handelsplattform sichtbar, die auf Nachfrage der Polizei entsprechende Daten herausgegeben hat.[20] Auch konnte schon gezeigt werden, dass die Möglichkeit besteht, die Bitcoin-Adressen des Absenders und des Empfängers den jeweiligen IP-Adressen der beteiligten Parteien zuzuordnen.[21] Es handelt sich somit um personenbezogene Daten.

Sollte also ein etwaiger Anspruch auf Löschung vorliegen, ist dieser technisch jedoch nicht durchsetzbar. Wie oben dargestellt ist einer der Hauptgründe für das hohe Sicherheitsniveau der Bitcoin-Blockchain, dass Blöcke nicht nachträglich editiert werden können.

Ungeklärt ist bisher die Frage, wer überhaupt für die Einhaltung datenschutzrechtlicher Vorgaben verantwortlich ist. Die DS-GVO verpflichtet nicht jeden, der mit den jeweiligen personenbezogenen Daten in Berührung kommt, sondern nur den Verantwortlichen (vgl. Art. 4 Nr. 7 DS-GVO), den Auftragsverarbeiter (vgl. Art. 4 Nr. 8 DS-GVO) und

16 https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/

17 http://bitfury.com/content/4-press/1_30_2018_bitfury_releases_crystal.pdf

18 Ausführlich hierzu: *Martini/Weinzierl*, NVwZ 2017, 1251; *Schrey/Thalhofer*, NJW 2017, 1431, 1432 ff.; *Bechtolf/Vog*, ZD 2018, 66; *Guggenberger*, ZD 2017, 49.

19 EuGH, Urt. v. 19.10.2016, Rs. C-582/14, BB 2016, 2830.

20 https://netzpolitik.org/2017/bitcoin-de-gibt-nutzerdaten-an-polizei-weiter-auch-ohne-richterlichen-beschluss/

21 https://arxiv.org/abs/1405.7418; vgl. auch https://arxiv.org/abs/1107.4524.

gegebenenfalls Dritte (vgl. Art. 4 Nr. 10 DS-GVO). Dabei geht der Gesetzgeber grundsätzlich davon aus, dass die Datenverarbeitung immer in einem hierarchisch aufgebauten Konstrukt erfolgt und im gesamten System Anweisungen befolgt werden.[22] Art. 26 DS-GVO geht zwar von mehreren Personen aus, die Daten für einen gemeinsamen Zweck kollektiv verarbeiten und bestimmt sie als gemeinsam für die Verarbeitung verantwortlich. Diese Regelung will jedoch die einzelnen Akteure eines komplexen und intransparenten in ein geordnetes und organisiertes System mit vorab geklärten Pflichten zwingen.[23] Dieses Ziel ist mit einer offenen Blockchain nicht zu vereinbaren und würde das Prinzip der „Trustlessness" konterkarieren.[24] Es wird deshalb unter anderem diskutiert, die Miner als Verantwortliche zu sehen,[25] wobei dies zum einen aufgrund der Anzahl und dem hohen Ermittlungsaufwand an der faktischen Durchsetzbarkeit scheitern würde und es zum anderen wenig Sinn ergeben würde, eine einzelne Stelle dazu zu verpflichten, gegenüber den anderen Teilnehmern die rechtlichen Vorgaben zu erfüllen, da ihr Einfluss hier verschwindend gering wäre.[26]

22 *Isler*, in: Jusletter, 2017, Rn. 31.

23 *Hartung*, in: Kühling/Buchner, DS-GVO, 1. Auflage 2017, Rn. 10.

24 *Isler*, in: Jusletter, 2017, Rn. 32.

25 https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/

26 *Böhme/Pesch*, DuD 2017, 473, 478 f.

Die Lösung, jeden Teilnehmer, der Daten empfängt, als Verantwortlichen zu qualifizieren,[27] würde noch weitaus mehr Personen erfassen und ist aus dem gleichen Grund wie die oben stehende Lösung abzulehnen.

Fazit

Die Blockchain-Technologie lässt sich trotz möglicher Angriffspunkte und vereinzelten Schwachstellen als sehr sicher einstufen und bietet viele Anwendungsmöglichkeiten sowie große Chancen für den Datenschutz. Allerdings steht ihr in ihrer derzeitigen Konfiguration aufgrund der fehlenden Bearbeitungsmöglichkeit und dem nicht erfüllbaren Erfordernis eines Verantwortlichen die europäische Datenschutzgrundverordnung entgegen. Lösungen könnten hier zum einen die Lockerung des Rechts auf Vergessenwerden für solche komplexen Systeme darstellen,[28] zum anderen ein neuer Regulierungsansatz im Hinblick auf die Verantwortlichkeit. Außerdem könnte auf technischer Ebene die Möglichkeit eingeführt werden, dass nur noch der Vermerk über das Vorhandensein von Daten für die jeweiligen Adressen auf der Blockchain gespeichert wird. Die Daten selbst werden jedoch an einem anderen Ort gespeichert und können innerhalb eines bestimmten Rahmens mithilfe eines privaten Schlüssels, den nur der Betroffene besitzt, durch Dritte geändert werden.[29]

Paschke/Raab

27 http://www.cms-lawnow.com/ealerts/2017/08/hungary-data-protection-aspects-of-blockchain

28 *Martini/Weinzierl*, NVwZ 2017, 1251, 1258.

29 Vgl. ausführlich dazu: *Wiefling/Iacono/Sandbrink*, DuD 2017, 482, 483.

Designed by Tobias Springer und Simon Raab

Der nächste Newsletter erscheint am 15. Juni 2018.

Sie finden den Newsletter und die Möglichkeit, sich an- bzw. abzumelden auch unter https://www.baywidi.de/

Hinweise, Anregungen, Lob und Kritik sind herzlich willkommen. Schreiben Sie uns einfach unter: baywidi@uni-passau.de

Impressum

Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Organisation
Gemäß Art. 11 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung:
Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.