Datensouveränität und Vertrauen: Der »Amazon-Fall«

Dr. jur. Christian Szidzek, Prof. Dr. Harald J. Bolsinger

Abstract: In der gesamten EU gilt erstmals die EU-Datenschutzgrundverordnung (DSGVO) als unmittelbar anzuwendendes Recht und betrifft damit sämtliche Unternehmen, die ihre Produkte auf dem europäischen Markt anbieten möchten. Szidzek und Bolsinger analysieren ordnungsethisch, juristisch und wirtschaftspolitisch die Chancen aus der neuen Norm für Unternehmen, Vertrauen zu Kunden und Gesellschaft aufzubauen, um ihre »license to operate« zu sichern. Anhand eines exemplarischen Praxisbeispiels mit Amazon werden im Artikel wesentliche Grundlagen für Vertrauensaufbau und -sicherung vor dem Hintergrund der neuen Datenschutzanforderungen aufgezeigt, die vor allem in vertrauensbasierten Märkten höchste Relevanz besitzen. Die Abstrahlwirkung einer proaktiv verfolgten und öffentlich wahrnehmbaren Verantwortungsübernahme für den Umgang mit personenbezogenen Daten durch Unternehmen wird dabei als marktförderliche Kernfunktion der DSGVO im Rahmen funktionierenden Wettbewerbs im Kontext der Digitalisierung sichtbar.

Schlüsselwörter: EU-Datenschutzgrundverordnung (DSGVO), Datenschutz, Datenethik, Informationssicherheit, Digitalisierung, Reputationsmanagement, Ordnungspolitik, trust-driven markets, Vertrauen

1 DIE EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG

Am 25. Mai 2018 läuft die Frist zur nationalen Umsetzung der am 25. Mai 2016 in der gesamten EU in Kraft getretenen EU-Datenschutzgrundverordnung (DSGVO) ab [Regulation (EU) 2016/679 of the European Parliament and of the Council]. Das neue Marktortprinzip [Art. 3 Abs. 2 lit. a DSGVO] unterwirft als unmittelbar anzuwendendes Recht nicht nur sämtliche Unternehmen mit Sitz oder Zweigstellen in der Europäischen Union (EU) den Vorgaben der neuen DSGVO, sondern im Gegensatz zum bisher in der EU gültigen Territorialprinzip auch sämtliche Unternehmen, die ihre Produkte auf dem europäischen Markt anbieten. Während die zuvor gültige allgemeine Datenschutzrichtlinie 95/46/EG [Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995] die Mitgliedstaaten lediglich verpflichtete, die darin niedergelegten Grundsätze und Anforderungen an die Verarbeitung personenbezogener Daten durch eigene Gesetzgebungsakte umzusetzen, ist die neue DSGVO unmittelbar anzuwendendes Recht. Ein Umsetzungsakt durch die Mitgliedstaaten ist nicht erforderlich. Die DSGVO gestattet lediglich einen Spielraum für Konkretisierungen durch die Mitgliedstaaten innerhalb der vorhandenen Öffnungsklauseln, im Übrigen ist sie von allen staatlichen Behörden und Unternehmen direkt anzuwendendes Recht. Sollten die nationalen

Kontaktdaten der Autoren: : Christian Szidzek[1], Harald J. Bolsinger[2]
[1]Dr. jur. Christian Szidzek: Rechtsanwalt, Projektmanager, Datenschutzbeauftragter und -auditor, Place-de-Caen 11, 97084 Würzburg, Mail: christian.szidzek@kanzlei-szidzek.de
[2]Prof. Dr. Harald J. Bolsinger: Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt, Fakultät Wirtschaftswissenschaften, Münzstraße 12, 97070 Würzburg, https://fwiwi.fhws.de

Datenschutzgesetze bei der Ausfüllung der Öffnungsklauseln gegen die Grundprinzipien der DSGVO verstoßen, kann dies durch ein Vertragsverletzungsverfahren gerügt werden. Das Vertragsverletzungsverfahren ist in den Art. 258 bis 260 AEUV vorgesehen und ermöglicht es, sowohl der EU-Kommission (sog. Aufsichtsklage, Art. 258) als auch den Mitgliedstaaten (sog. Staatenklage, Art. 259) Verstöße eines Mitgliedstaates gegen das EU-Recht geltend zu machen. Von der Möglichkeit, ein ergänzendes konkretisierendes Gesetz zu erlassen, hat die Bundesrepublik Deutschland als erster Mitgliedstaat der EU Gebrauch gemacht. Das neue Bundesdatenschutzgesetz tritt in Deutschland ebenfalls zum 25. Mai 2018 in Kraft.

Freiheitlich-demokratischen Verfassungen eigen ist der Grundsatz, dass Rechtssubjekte tun und lassen dürfen, was sie für richtig erachten, soweit dabei nicht Rechte anderer verletzt oder gegen verfassungskonforme Gesetze verstoßen wird. Im Datenschutzrecht gilt dieser Grundsatz nicht. Hier gilt ein Verbot der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt. Demnach ist die Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn, es findet sich eine gesetzliche Erlaubnis dafür. Maßgebend hierfür sind die DSGVO selbst (Art. 6 ff. DSGVO) und gegebenenfalls ergänzende nationale Regelungen. Ausgenommen vom Anwendungsbereich ist lediglich die Verarbeitung zu rein persönlichen oder familiären Zwecken ohne kommerzielle Absichten (sog. »Haushaltsausnahme«, Art. 2 Abs. 2 lit. c DSGVO).

Zulässig ist die Verarbeitung personenbezogener Daten, wenn sie zur Anbahnung oder Durchführung von Vertragsverhältnissen erforderlich ist, Gefahren für Leib und Leben abgewendet werden sollen, bestimmte hoheitliche Aufgaben dies erfordern, der Verarbeitende gegenüber dem Betroffenen ein überwiegendes berechtigtes Interesse geltend machen kann oder wenn die betroffene Person in die Verarbeitung eingewilligt hat.

Unter personenbezogenen Daten versteht Art. 4 DSGVO:
»(…) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (…) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.«

Bei Verletzungen der Vorgaben der DSGVO drohen Unternehmen nach Art. 83 Abs. 5,6 DSGVO drastische Sanktionen von Bußgeldern bis zu 20 Millionen Euro im Einzelfall und bei internationalen Konzernen bis zu 4 % des weltweiten Jahresumsatzes. Die Umsetzung der Anforderungen der DSGVO stellt für die betroffenen Unternehmen indes eine beträchtliche Herausforderung dar. Allein die geforderte Bestandsaufnahme aller digitalen und analogen Verarbeitungsvorgänge personenbezogener Daten in ein übersichtliches Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DSGVO setzt eine Analyse sämtlicher Geschäftsprozesse voraus. Nach deren Erfassung sind die Vorgänge auf Zulässigkeit der Verarbeitung nach der DSGVO zu prüfen, gegebenenfalls anzupassen oder abzuschaffen. Dabei sind insbesondere die zum Schutz personenbezogener Daten ergriffenen technischen und organisatorischen Maßnahmen dahingehend zu überprüfen, ob diese den neuen Anforderungen der Art. 5 und 32 DSGVO standhalten. Zu erwähnen sind insbesondere auch die neuen Erfordernisse des sog. »privacy by design« und »privacy by default« [Laue, Nink, und Kremer (2016), S. 212 f.]. Daneben ist eine Implementierung von Neuprozessen zur Sicherstellung neuer und deutlich weitgehenderer Betroffenenrechte als bisher erforderlich. Auskunftsansprüchen und Meldepflichten ist unver-

züglich nachzukommen. Die DSGVO konstatiert in Art. 33 DSGVO zudem eine – dem deutschen Strafrecht fremde – Pflicht zur Selbstanzeige innerhalb von 72 Stunden für Unternehmen bei allen Datenschutzverstößen, es sei denn die Datenpanne führt »voraussichtlich nicht zu einem Risiko« für die Betroffenen.

Organisationen, die sich diesem Thema bislang nicht gewidmet haben, sind gut beraten, sich schnellstmöglich um die Umsetzung der neuen Vorgaben der DSGVO zu kümmern. Ein Projekt zur Umsetzung der DSGVO-Vorgaben kann Monate in Anspruch nehmen und bindet Ressourcen aus nahezu allen betrieblichen Fachbereichen. Es ist angesichts dieser erstmaligen umfassenden Regulierung des Datenschutzes in Europa und unter Berücksichtigung der empfindlichen Strafen in einem zunehmend regulierten Compliance-Umfeld auf den ersten Blick verständlich, wenn das neue Datenschutzrecht der EU von Unternehmen zunächst als Hindernis freier geschäftlicher Entfaltung verstanden wird. Auf einem globalen Markt, auf dem zunehmend Produkte austauschbar werden, nahezu alle Hersteller in der Lage sind, ein identisches technisches Qualitätsniveau bei entsprechendem Preis-Leistungsverhältnis herzustellen, bedarf es neuer Kriterien zur Erzeugung von Alleinstellungsmerkmalen in einem internationalen Umfeld.

Um zu illustrieren, welches Datenschutzniveau in der EU bis zum Inkrafttreten der DSGVO als Praxis sichtbar wird, ist die Betrachtung eines Präzedenzfalles hilfreich. Trotz gesteigerter Wahrnehmung des Datenschutzes in der Bevölkerung stellen selbst Weltkonzerne ihre eigene Reputation in Frage, indem sie das Bedürfnis ihrer Kunden nach angemessenem Umgang mit personenbezogenen Daten aus deren Sicht vernachlässigen. Der sorgsam dokumentierte Fall um eine kundendatenbezogene Löschungsbitte gegenüber Amazon [Bolsinger (2015)] steht stellvertretend für die Erfahrungen von Millionen von Kunden mit entsprechenden Internetkonzernen aus den USA.

2 THE AMAZON-CASE – WIE UNTERNEHMEN IM BIG-DATA-ZEITALTER KUNDENVERTRAUEN ZERSTÖREN KÖNNEN

Wir befinden uns im Jahr 1999. Harald Bolsinger (im weiteren Verlauf als Amazonkunde bezeichnet) bestellt bei Amazon sein erstes Buch unter Angabe seines Namens sowie seiner Adressdaten. Es handelt sich um ein Werk zu Studienzwecken. Die Bezahlung erfolgt per Kreditkarte, deren Daten ebenfalls an Amazon übertragen werden. Weitere Bestellungen erfolgen alsbald bis hinein in das Jahr 2013 und inzwischen längst nicht mehr nur durch den Autor selbst. Auch dessen Familie hatte längst erkannt, wie bequem es scheint, über Amazon Produkte zu bestellen.

Es sammelten sich bei Amazon im Laufe der Zeit sämtliche Kreditkartendaten, Girokonto-Informationen, jede Adresse, unter welcher der Amazonkunde jemals erreichbar war, sowie die Adressen von Verwandten im Rahmen von Geschenkbestellungen. Je mehr der Amazonkunde bestellte, desto größer wurde das Potenzial, aus der Bestellhistorie über den Kunden ein Profil zu erstellen, das weit über dessen Konsuminteressen hinausgeht: Es ließen sich zunehmend Aussagen über die weltanschaulich-religiöse Prägung treffen, politische Interessen einschätzen, wissenschaftliches Know-how beurteilen, Meinungen über Rezensionen ableiten und weitere Präferenzen über die getätigten Käufe und Zahlungsdaten erahnen. Selbst Rückschlüsse auf die Einkommensentwicklung ließen sich über die Jahre ziehen, aus dem jeweils neuen Wohnumfeld und anhand des zunehmenden Wertes von Geschenkbestellungen. Freundschaftliche Beziehungen wurden zunehmend transparent.

Da der Amazonkunde den Überblick über die bei Amazon über ihn verfügbaren Informationen bekommen wollte, beschloss er, Amazon um Auskunft zu bitten. Am 23. August 2013 wandte er sich per Fax an Amazon mit der Bitte um Auskunft nach § 34 des deutschen Bundesdatenschutzgesetzes (BDSG). Diese Vorschrift normiert einen kostenfreien Auskunftsanspruch des Betroffenen gegen datenverarbeitende Stellen. Die Vorschrift stellt zwingendes Recht dar, dessen Verletzung bußgeldrechtlich sanktioniert ist und verpflichtet Unternehmen und Behörden bei Geltendmachung des Anspruches dazu, auf Anfrage unverzüglich mitzuteilen, welche konkreten Daten die jeweilige Stelle über den Betroffenen erhoben und gespeichert hat, woher diese Daten stammen, wie diese verwendet werden, an wen diese weitergegeben werden und wann diese gelöscht werden.

Nachdem die Auskunft mehr als zwei Wochen auf sich warten ließ, erinnerte der Autor Amazon am 10. September 2013 erneut per Fax an sein Anliegen. Am 13. Oktober 2013, also 61 Tage nach Einreichen des Auskunftsersuchens reagierte Amazon mit einem über 30-seitigen Schreiben, das zum einen die gewünschte Auskunft über die gespeicherten Daten beinhaltete und dessen Aussage unter anderem darin bestand mitzuteilen, dass die deutsche Amazon.de GmbH (im Folgenden: »Amazon») nicht zuständig sei, sondern die EU S.A.R.L in Luxemburg. Die gespeicherten Daten erfassten alles, was der Amazonkunde seit 1999 im Rahmen der Geschäftsbeziehung übermittelt hatte, unabhängig davon, ob diese noch aktuell waren oder nicht wie z. B. längst gelöscht geglaubte Wohnadressen, Telefonnummern, Kreditkartendaten, eingelöste Gutscheine im Detail, Rücksendungen und vieles mehr. Der Kunde entschloss sich daher, Amazon am 22. November 2013 unter der Kontaktadresse von Amazon (amazon.de/kontakt) aufzufordern, die nicht mehr aktuellen oder längst überholten Daten der Kundenhistorie zu löschen.

Amazon erklärte daraufhin, dass es nicht möglich sei, einzelne Bestellungen oder Daten zu löschen. Nachdem der Autor sein Verlangen jedoch aufrechterhielt, teilte Amazon mit, dass die Löschung der Daten nach Ablauf der Aufbewahrungspflicht erfolgen werde. Konkrete Aufbewahrungspflichten oder -fristen wurden jedoch nicht benannt. Dem Amazonkunden selbst waren zu diesem Zeitpunkt selbst keine solchen Aufbewahrungspflichten bekannt, die Unternehmen verpflichten würden, Datensätze, die bis ins Jahr 1999 zurückreichten, noch immer, also über einen Zeitraum von nunmehr knapp 14 Jahren aufzubewahren. Dieser Umstand weckte bei dem Amazonkunden die Befürchtung, dass es möglicherweise ganz andere Gründe seitens Amazon geben könnte, Kundendaten zu sammeln und aufzubewahren, als die bloße Erfüllung von Aufbewahrungspflichten. Der Amazonkunde hielt daher sein Begehren auf Löschung der überholten und seiner Meinung nach nicht mehr aufbewahrungspflichtigen Daten aufrecht.

Am 23. November 2013 teilte Amazon sodann unvermittelt mit, dass sein Anliegen nun verstanden worden sei. Man könne das gesamte Konto des Kunden schließen. Dies war jedoch nicht das Ziel des Amazonkunden. Er wandte sich daraufhin an die Geschäftsführung von Amazon Deutschland und teilte mit, dass er lediglich sein Recht auf Datenlöschung nach dem deutschen BDSG geltend gemacht habe, ohne aber sein Kundenkonto einhergehend mit dem Verlust digitaler Einkäufe löschen zu wollen. Am 12. Dezember 2013 ließ Amazon sodann verlautbaren, dass aus bilanz- und steuerrechtlichen Gründen sämtliche personenbezogene Daten auch dann weiterhin gespeichert würden, wenn eine Kontolöschung verlangt würde, was die Skepsis des Amazonkunden gegenüber der Datenverarbeitungspraxis von Amazon weiter nährte.

Er leitete daraufhin die Korrespondenz mit Amazon nebst einer Zusammenfassung der Geschehnisse weiter an die Bundesbeauftragte für Datenschutz und Informationsfreiheit der Bundesrepublik Deutschland sowie an das Bayerische Landesamt für Datenschutzaufsicht, verbunden mit der Aufforderung, die Amazon Deutschland zur datenschutzkonformen Löschung seiner personenbezogenen Daten anzuhalten, soweit keine bilanz- oder steuerrechtlichen Aufbewahrungspflichten mehr bestünden. Die Behörden reagierten prompt: Sowohl die Bundesbeauftragte für den Datenschutz und die Informationssicherheit sowie das Bayerische Landesamt für Datenschutzaufsicht erklärten sich für unzuständig mit dem Hinweis, der Amazonkunde möge sich an die luxemburgische Datenschutzaufsicht wenden, da dort das Unternehmen seinen Sitz habe.

Am 06. Februar 2014 verlangte der Amazonkunde von Amazon Deutschland erneut Auskunft über die zu ihm gespeicherten personenbezogenen Daten. Am 28. Februar 2014 wurde die Auskunft durch Übersendung einer CD-ROM erteilt. Der Umfang der gespeicherten Daten entsprach noch immer demjenigen von Oktober 2013. Der Bitte nach Löschung überholter und nicht mehr aufbewahrungspflichtiger Daten war nicht entsprochen worden.

Da sich die deutsche Datenschutzaufsicht für unzuständig erklärt hatte, beschwerte sich der Amazonkunde am 31. März 2014 bei der nationalen Kommission für den Datenschutz in Luxemburg (CNPD) – mit Abdruck an die deutsche Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und an das Bayerische Landesamt für Datenschutzaufsicht – unter Darlegung des Sachverhalts und verbunden mit der erneuten Aufforderung, Amazon zur Löschung der nicht rechtmäßig gespeicherten Daten anzuhalten. Es erfolgte wieder eine Reaktion, dieses Mal seitens der deutschen Bundesbeauftragten für Datenschutz und Informationssicherheit. Diese ließ verlautbaren, dass die luxemburgischen Behörden zuständig seien, nicht aber die deutschen.

Nach Verstreichen eines Monats und zusätzlicher Erinnerung an die Beschwerde reagierte endlich auch die CNPD und teilte mit, dass die Rechtmäßigkeit der Datenspeicherung geprüft werde, es jedoch in Luxemburg kein »Recht auf informationelle Selbstbestimmung« gebe, da dies ein Recht sei, das lediglich auf deutsche Rechtsprechung zurückzuführen sei. Nach drei weiteren Aufforderungen an die CNPD im Mai, Juni und Juli 2014, konkret Stellung zu beziehen und nach Inaussichtstellen einer Beschwerde bei dem Justizministerium, erreichte den Amazonkunden am 29. Juli 2014 die offizielle Antwort der CNPD: Das Verhalten von Amazon sei durch die »gegenwärtigen und künftig geplanten Zweckbestimmungen« gerechtfertigt. Zudem habe Amazon Aufbewahrungspflichten nach dem luxemburgischen Handelsgesetzbuch (Code du Commerce) nachzukommen, die eine Datenlöschung vor dem Ablauf von zehn Jahren untersagten. Zudem wurde erneut darauf hingewiesen, dass es in Luxemburg kein Recht auf informationelle Selbstbestimmung wie etwa in Deutschland gebe.

»Gegenwärtige und künftig geplante Zweckbestimmungen«? Waren die Daten nicht seitens des Amazonkunden mit einer ganz konkreten Zweckbestimmung an Amazon übermittelt worden? Wo sollte hier Raum für künftige Zweckbestimmungen sein? Welche Aufbewahrungspflichten nach dem Code du Commerce erforderten eine Aufbewahrung von Daten über 14 Jahre hinweg? Was meint die CNPD, wenn sie mitteilt, es gebe in Luxemburg kein »Recht auf informationelle Selbstbestimmung«?

Am 06. August 2014 bat der Amazonkunde erneut bei Amazon um Löschung konkreter Daten und Auskunft über die Löschung verhindernden Rechtsvorschriften. Er wandte sich direkt an den »Associate General Counsel and EU Legal Director for Privacy, Competition and Litiga-

tion«. Am 19. September 2014 erwiderte nunmehr die Rechtsabteilung von Amazon, dass sämtliche Kundendaten über einen Zeitraum von zehn Jahren über den Zeitpunkt hinaus gespeichert würden bis zu dem das Kundenkonto bestehe.

Die Sache wurde nun immer kurioser: Zunächst war eine Löschung einzelner Daten nicht möglich, sondern allenfalls des gesamten Kundenkontos. Dann stellte sich heraus, dass auch bei Löschung des Kundenkontos, keine Datenlöschung erfolgte, da einer solchen angeblich gesetzliche Aufbewahrungspflichten entgegenstünden. Daten müssten demnach über zehn Jahre hinweg aufbewahrt werden. Und jetzt das: Die vermeintliche Zehnjahresfrist bis zur Löschung der Daten begann für Amazon nicht etwa mit dem Zeitpunkt der Erhebung der Daten zu laufen, sondern erst mit dem Zeitpunkt der Löschung des Kundenkontos, mit der Folge, dass Daten aus dem Jahr 1999 bei Schließung des Kundenkontos im Jahr 2014 erst im Jahr 2024 gelöscht würden, d. h. 25 Jahre nach deren Erhebung.

Der Amazonkunde nahm dies im Dezember 2014 zum Anlass, erneut sein Bestellkonto durchzusehen und stellte fest, dass noch immer längst ungültige Lieferadressen, Kreditkartendaten und Bestelldetails aus dem Jahr 1999 angezeigt wurden. Lediglich einzelne Bestelldokumente aus dem Jahr 2000 waren offenbar entfernt worden, die Bestellhistorie erfasste diese Käufe jedoch noch immer. Löschungen von sonstigen Daten, die älter als zehn Jahre waren, hatten nicht stattgefunden. Bei dem Amazonkunden machten sich nun zunehmend Ärger über die Behandlung seiner Anfragen bemerkbar sowie die Sorge, dass Amazon offenbar überhaupt nicht gewillt sein könnte, die von ihm erhobenen Daten überhaupt irgendwann einmal zu löschen. Der Amazonkunde richtete daher am 22. Dezember 2014 eine Beschwerde an das luxemburgische Justizministerium, da er zusätzliche Zweifel am Vorgehen der CNPD bekam. Er informierte darüber hinaus auch das Datenschutzreferat der EU-Kommission.

Am 20. April 2015 erreichte den Amazonkunden ein Antwortschreiben des Leiters des Datenschutzreferates in der Generaldirektion Justiz der EU-Kommission. Dieser teilte darin sowie in einem persönlichen Gespräch mit, dass der Kommission in dieser Sache die Hände gebunden seien und verwies auf die Möglichkeit einer Klage vor luxemburgischen Gerichten.

Da seitens des Justiz- und Premierministeriums aus Luxemburg eine Antwort ausblieb, erinnerte der Amazonkunde den luxemburgischen Premierminister im Mai 2015 noch einmal an seine Eingabe vom März 2015 und forderte Amazon gleichzeitig erneut auf zur Löschung aller Nummern abgelaufener Kreditkarten, aller vergangenen Wohnorte und aller Handynummern, die im Zuge von über zehn Jahre zurückliegenden Käufen übermittelt wurden sowie zur Löschung konkreter Bestellungen aus den Jahren 1999 und 2001.

Am 28. Mai 2015 erhielt der Amazonkunde eine Antwort des luxemburgischen Justizministers, in der er eine eingeholte Stellungnahme der Präsidentin der CNPD vom 09. April 2015 weiterleitete. Diese stellte in ihrem Schreiben fest, dass die durch Amazon vorgenommene Datenverarbeitung auf Basis der luxemburgischen Datenschutzrechtslage von 2002 richtig, zulässig und rechtmäßig sei. Ebenso wies sie darauf hin, dass Amazon sich erst im Jahr 2004 in Luxemburg niedergelassen habe und luxemburgisches Recht daher erst ab diesem Zeitpunkt zur Anwendung komme. Es stehe dem Autor frei, vor einem luxemburgischen Gericht Klage zu erheben. Der Amazonkunde beschwerte sich ein weiteres Mal am 09. Juli 2015 bei der nationalen Kommission für den Datenschutz in Luxemburg (CNPD) und nun auch zusätzlich darüber, dass Amazon entgegen der gesetzlichen Lage in Luxemburg weder seinen Löschverpflichtungen nachkomme noch die Rechtsgrundlage für die weitere Speicherung über zehn Jahre hinaus benenne. Er führte aus, dass Amazon die Datenlöschung offenbar erst zehn Jahre

nach der erfolgten Kundenkontoschließung vornehme und eine Weiterverwendung des Kundenkontos, ohne dieses zu schließen, dazu führe, dass überhaupt keine Daten gelöscht würden. Ferner nahm er Bezug auf das Schreiben der Präsidentin der CNPD vom April 2015, das ihm vom luxemburgischen Justizminister weitergeleitet worden war, indem die DNPD sich für die Datenlöschung nicht zuständig sah, da sich Amazon erst im Jahr 2004 in Luxemburg niedergelassen habe, obgleich Amazon bereits auf den Rechnungen aus dem Jahr 1999 als Amazon EU S.A.R.L. firmiert hatte. Er äußerte, dass der subjektive Eindruck entstehe, dass alle zuständigen Behörden sowie das betroffene Unternehmen dessen einfache Forderung nach Löschung konkreter nicht mehr rechtmäßig gespeicherter Daten mit allen zur Verfügung stehenden Mitteln abwehren wollten. Er verwies zudem auf den Umstand, dass nicht lediglich die eigenen personenbezogenen Daten von der unzulässigen Löschpraxis von Amazon betroffen seien, sondern die von vielen Millionen Nutzern und die Behörden aufgrund ihrer Untätigkeit gegenüber Amazon für die erwiesene Unrechtmäßigkeit der Speicherpraxis des Unternehmens mitverantwortlich seien. Zeitgleich reichte der Amazonkunde erneut Beschwerde bei der Bayerischen Landesdatenschutzaufsicht ein unter Verweis auf den Umstand, dass Amazon im Jahr 1999 Daten unter der Firmierung Amazon.de GmbH mit Sitz in Regensburg erhoben hätte, seinerzeit auf den datenschutzkonformen Umgang mit personenbezogenen Daten hingewiesen habe und somit für diesen Zeitraum bis ins Jahr 2004, also bevor Amazon sich in Luxemburg registrieren ließ, deutsches Recht Anwendung finde und die Zuständigkeit der Bayerischen Landesdatenschutzaufsicht folglich gegeben sein müsse. Er verwies auch hier auf den vermuteten massenhaften Verstoß gegen deutsches Datenschutzrecht. Am 29. Juli 2015 erklärte die Bayerische Landesdatenschutzaufsicht erneut ihre Unzuständigkeit, woraufhin der Amazonkunde im August 2015 um Mitteilung bat, wer denn nun für die Löschung seiner in den Jahren 1999 bis 2004 erhobenen Daten zuständig sei. Die Bayerische Landesdatenschutzaufsicht erklärte daraufhin im September 2015, dass es für den Zeitpunkt der Zuständigkeit für die Datenlöschung durch Unternehmen auf den Zeitpunkt der Geltendmachung des Löschanspruches durch den Kunden bzw. den Betroffenen ankomme und nicht den Zeitpunkt der Erhebung. Sie selbst bleibe daher unzuständig. Wie nun das? Nach der Logik der Aufsichtsbehörde könnten sich demnach Unternehmen allein durch einen Sitzwechsel in einen Staat mit nicht vorhandenem Datenschutzrecht der Verpflichtung entziehen, personenbezogene Daten zu löschen, die sie unter Versicherung der Einhaltung nationaler Datenschutzbestimmungen in EU-Staaten erhoben haben. Denn für die Datenlöschung gelte das Recht des Staates, in welchem das Unternehmen zum Zeitpunkt der Geltendmachung des Löschanspruches seinen Firmensitz habe, nicht zum Zeitpunkt der Erhebung.

Am 24. August beantragte der sich von Behörden und Amazon alleine gelassen fühlende Amazonkunde, der zwischenzeitlich jegliches Vertrauen in das Unternehmen und die Behörden in Luxemburg verloren hatte, die Löschung seines Kundenkontos, um zu erreichen, dass nun wenigstens die von Amazon selbst angegebene Zehnjahresfrist für die Löschung nach Kontoschließung zu laufen beginne. Amazon teilte mit, dass das Kundenkonto zum 07.10.2015 geschlossen werde, die Daten des Autors jedoch gespeichert blieben. Im Ergebnis waren daher die jahrelangen Bemühungen des Amazonkunden um Löschung einiger weniger veralteter, überholter, nicht mehr aufbewahrungspflichtiger Daten bis zum heutigen Tag vergeblich. Die nächste Datenschutzauskunft wird der Amazonkunde am 07. 10. 2025 von Amazon einholen.

Amazon nahm es in Kauf, dass ein zuvor treuer Kunde sich genötigt fühlte, seine Kundenverbindung vollständig aufzugeben, nur um zu erreichen, dass wenigstens zehn Jahre danach seine personenbezogenen Daten gelöscht werden würden. Man verzichtete auf weiteren Umsatz mit dem Kunden, anstelle das Kundenbegehren zum Anlass zu nehmen, die eigene Löschpraxis zu hinterfragen. Sicher handelte es sich bei dem Amazonkunden in den Augen von

Amazon um einen Einzelfall, für den man nicht sogleich bereit war, ein gesamtes Konzernkonzept ad hoc zu ändern. War man seitens Amazon einfach technisch nicht in der Lage, die gewünschten Daten fristgerecht zu löschen? Möglicherweise beabsichtigt Amazon auch, mit all den gesammelten Kundendaten zukünftig etwas viel Größeres anzufangen? Vielleicht war es Amazon aber einfach auch nur egal, dass angesichts der marktbeherrschenden Rolle, die der Konzern spielt, ein Kunde es tatsächlich wagt, die gebräuchliche selbst definierte Praxis im Umgang mit personenbezogenen Daten in Frage zu stellen. Egal was Amazon bewegte: Es sind Begriffe wie Hochmut, mangelnde Kundenempathie, etwaige technische Unfähigkeit, Datensammlungswut mit grenzenlosen Auswertungs- und Vermarktungsmöglichkeiten in naher Zukunft oder schlicht arrogante Gleichgültigkeit gegenüber den eigenen, zuvor treuen und zahlenden Kunden, mit denen Amazon nunmehr in Verbindung gebracht werden kann. Was immer Amazon diesbezüglich auch vorhat: Wir können es nicht vorhersagen. Das Ergebnis ist eine Empfindung der negativen Art, die beim Kunden hervorgerufen wird. Weitab von jener subjektiven Überzeugung, die noch zuvor als Basis für die Geschäftsbeziehung zwischen Amazon und seinem Kunden galt: dem gegenseitigen Vertrauen zweier Geschäftspartner und dem Respekt vor der informationellen Selbstbestimmung des Kunden.

3 PRIVATHEIT IM KONTEXT VON UNTERNEHMEN UND STAAT

Im Zusammenhang mit dem dargestellten Amazon-Case lässt sich argumentieren, dass derjenige, der nichts zu verbergen hätte, auch nichts zu verheimlichen hätte und demnach die informationelle Selbstbestimmung im vorliegenden Fall eher nachrangig sei. Was sollte gegen eine unbefristete Speicherung personenbezogener Daten sprechen? Kann es nicht gleichgültig sein, was mit diesen Daten geschieht, ob diese kommerziell verwendet, weitergegeben, ausgewertet werden, wenn der Betroffene redlich ist und daher nichts zu befürchten hat? Doch das würde den Kern der Fragestellung verfehlen. Privatheit bedeutet nicht, dass der Betroffene etwas zu verheimlichen hätte. Es gibt Informationen, die aufgrund der persönlichen Einschätzung des Individuums nicht für die Öffentlichkeit oder Dritte bestimmt sind. Bereits Hannah Arendt hat festgestellt, dass unter dem Privaten all das zu verstehen sei, was nur im Verborgenen gedeihen kann [Arendt (2007)]. Das Bewusstsein vom Wert der eigenen Privatheit nimmt zu. Menschen wollen nicht überwacht und analysiert werden. Sie sind keine Objekte des Marktes, sondern Individuen mit persönlicher unabdingbarer Würde jenseits gewinnorientierter Geschäftsmodelle, die den Menschen auf informationsbasierte Ertragspotenziale reduzieren. Seit den sogenannten Snowden-Enthüllungen werden Menschen, die ihre Webcam bei der Internetnutzung abklemmen, deutlich weniger belächelt. Immer mehr Menschen beschäftigen sich mit Ende-zu-Ende-Verschlüsselung. Generell nimmt die Verschlüsselung des Datenverkehrs zu. In Europa hat sich der verschlüsselte Verkehr binnen eines Jahres seit den Snowden-Enthüllungen vervierfacht, berichtet der Netzwerkanbieter Sandvine [Böhm (o. J.)]. Statt 1,5% beträgt sein Anteil jetzt 6,1%. Eine Umfrage des deutschen Branchenverbands Bitkom ergab Ende 2014, dass 5 Millionen Deutsche eine E-Mail-Verschlüsselungssoftware verwenden. Im Juli 2013 waren es erst 3,3 Millionen [Ebd.].

Wenngleich die NSA-Affäre die heimliche staatliche Überwachung betrifft, die Datenweitergabe an Unternehmen aber aus freien Stücken erfolgt, bleibt die Ursache für die Sorge der Menschen, was den Umgang mit ihren Daten angeht, jedoch in beiden Fällen identisch. Es darf über Daten verfügt werden, wenn der Zweck legitim und festgelegt ist und die Daten nicht anderweitig als vereinbart verwendet werden. Geht es um die Verhinderung von Terroranschlägen besteht allgemeiner Konsens, dass in diesem Zusammenhang auch die Daten vieler Unschuldiger ausgewertet werden müssen und dass dies ebenso zulässig wie zur Abwehr

geboten erscheint. Dass die Datenerhebung in diesem Zusammenhang heimlich erfolgt, ist dabei akzeptabel, da andernfalls jeglicher Ermittlungserfolg von vorneherein gefährdet wäre [Kahl (2017), S. 137 ff.]. Die Vorratsspeicherung von Daten jedoch, die zu irgendeinem Zeitpunkt einmal verwendet werden könnten, wird jedoch zu Recht als Gefahr empfunden.

Ebenso überlässt in der freien Wirtschaft auch der Bankkunde seinem Kreditinstitut freiwillig Informationen über Zahlungseingänge und -ausgänge sowie die überweisenden Personen zur Durchführung des bargeldlosen Zahlungsverkehrs. Er wünscht jedoch nicht, dass in diesen Daten ohne seine ausdrückliche Einwilligung Analysen getätigt werden, um geschäftliche Potenziale zu erkennen oder Profile über ihn anzufertigen. Ebenso gibt der Kunde sein Fahrtziel in das Navigationssystem ein, um sich sicher lotsen zu lassen. Er will jedoch nicht, dass andere ohne seine Erlaubnis Bewegungs- und Sozialprofile zu seiner Person erstellen. Es ist allgemein anerkannt, dass ohne die Verarbeitung personenbezogener Daten weder ein Staat noch wirtschaftliche Aktivitäten möglich sind. Personen wollen jedoch zumindest im Rahmen von Geschäftsbeziehungen Herrschaft über ihre Daten ausüben können. Die Weiterverwendung von Daten, die für bestimmte geschäftliche Zwecke übermittelt wurden zu darüberhinausgehenden kommerziellen Zwecken des Empfängers dieser Daten, die eigene Bereicherung des Empfängers durch Verwendung, Auswertung und den Verkauf unserer Daten, wird jedoch als Unrecht empfunden.

In juristischen Kreisen besteht die Neigung, an dieser Stelle zu prüfen, ob der Betroffene, an dessen Daten sich der Empfänger wie auch immer bereichert, nicht gar einen Anspruch auf Herausgabe des somit erlangten Profits haben könnte unter dem Aspekt der römisch-rechtlichen Eingriffskondiktion, die im deutschen Bürgerlichen Gesetzbuch (BGB) in §812 Abs. 1 S. 1 Alt. 2 BGB geregelt ist. Die Eingriffskondiktion gründet auf dem Eingriff eines Fremden in den Zuweisungsgehalt eines Rechtsgutes – hier das Recht auf informationelle Selbstbestimmung [BVerfGE 65, 1 (42) (1983)], dessen wirtschaftliche Verwertung dem Bereicherungsgläubiger vorbehalten ist, also auf der Verletzung einer fremden, vermögensrechtlich nutzbaren Rechtsposition mit ausschließlichem Zuweisungsgehalt [Palandt und Sprau (201170), §812, Rn. 38]. Die Chancen, einen solchen Anspruch gerichtlich durchsetzen zu können, werden als nicht schlecht eingeschätzt.

4 TRUST DRIVEN MARKETS

Mayer, Davis und Schoorman definieren in ihrem relationalen Modell des Vertrauens eines Trustors gegenüber einem Trustee den Begriff des Vertrauens als die Bereitschaft des Trustors, eine riskante Handlung in einem Kontext vorzunehmen, den er selbst nicht vollständig kontrolliert in der Erwartung, dass der Trustee die Kontrolle übernimmt und den Trustor entsprechend schützt [Mayer, Davis and Schoorman (1995), S. 709-734]. Die von dem Trustor wahrgenommenen Eigenschaften auf Seiten des Trustees für die Vertrauensbildung sind dabei das Wohlwollen (benevolence), die Integrität (integrity) und die Fähigkeit (ability). Der Trustor quittiert dies seinerseits mit einer individuellen Vertrauensbereitschaft [Ebd]. Anhand dieser Kriterien wird das Verhalten von Amazon im geschilderten Fall vor dem Hintergrund der Vertrauenswürdigkeit aus Sicht des Kunden analysierbar:

Aus Sicht des Betroffenen, der seine Löschung längst nicht mehr benötigter Daten verlangte, ist seitens Amazon keinerlei Wohlwollen im Hinblick auf dessen Anliegen entgegengebracht worden. Amazon hätte durch Offenlegung der Rechtsgrundlage, auf der die angebliche fort-

dauernde Datenspeicherung beruht, Offenheit demonstrieren und durch ein Eingehen auf die Wünsche des Betroffenen ein Mindestmaß an Wohlwollen demonstrieren können. Indem dies nicht geschehen ist, fehlt es an grundlegenden Elementen des Wohlwollens gegenüber dem Kunden. Auch an Integrität im Sinne einer ethischen Forderung des philosophischen Humanismus nach möglichst weitgehender Übereinstimmung zwischen den kommunizierten Idealen und Werten einerseits und der tatsächlichen Lebenspraxis andererseits fehlte es, indem Amazon bei der Datenerhebung im Jahr 1999 zwar angab, das deutsche Datenschutzrecht zu beachten, offenbar jedoch rückwirkend keine ausreichende Bereitschaft zu einer dem entsprechenden, datenschutzkonformen Datenverarbeitung gezeigt hatte.

Schließlich steht auch die Fähigkeit, die Datenlöschung wie rechtlich gefordert durchzuführen in Frage. Denn über Jahre hinweg die berechtigte Forderung des Betroffenen nach Löschung der nicht mehr archivierungspflichtigen Daten abzulehnen, legt die Vermutung nahe, dass die vorhandenen IT-Systeme des Unternehmens nicht in der Lage sind, eine systematische Datenlöschung zum jeweils rechtmäßig festgelegten Zeitpunkt durchführen zu können. Dadurch hat Amazon es geschafft, anstatt Vertrauen seitens des Trustors größtmögliches individuelles Misstrauen auf Kundenseite zu erzeugen. Allein die Wahl des datenschutzrechtlich willfährigen Standortes Luxemburg mit entsprechend niedrigem Datenschutzniveau legt den Schluss nahe, dass es dem Unternehmen nicht um den Schutz der Daten seiner Kunden ging, sondern darum, diese Daten so wenig wie möglich schützen zu müssen. Wird Amazon als kommerzielle, technische Informationsverarbeitungsmaschine betrachtet, die nicht in der Lage ist, ethisch zu handeln, wäre eine Anwendung der Grundsätze des relationalen Modells für Vertrauen von Mayer, Davis, Schoormann auf den ersten Blick in Frage zu stellen. Die Anwendbarkeit ist aber gegeben, denn auch Amazon ist eine von Menschen gesteuerte Organisation, die voll verantwortungsfähig sind.

Grimm und Bräunlich haben sich mit der Frage der Anwendbarkeit des Referenzmodells auf technische Lösungen beschäftigt [Grimm und Bräunlich (2015), S. 289 ff. Nach deren Darstellung und unter Bezugnahme auf die ergonomische Untersuchung der Mensch-Maschine-Kommunikation von Lee und Moray sowie auf jüngere Arbeiten eines Informatikerteams der Universität Kassel über automatisierte Dienste im Internet sind auch bei automatisierten Diensten die Faktoren Fähigkeit (ability), Integrität (integrity) und Wohlwollen (benevolence) die vertrauensbildenden Faktoren [Ebd.].

Im beispielhaft geschilderten Fall hat Amazon durch sein Verhalten sämtliche Erwartungen des Trustors gegenüber dem Trustee enttäuscht und damit aus Sicht des Amazonkunden maximale Unglaubwürdigkeit erzeugt.

5 DATENSCHUTZ IN UNTERNEHMEN

Die Erfahrung zeigt, dass Unternehmen sich oftmals des Unterschieds zwischen Datenschutz und Datensicherheit nicht bewusst sind. Oftmals legen Unternehmen bei Anfragen von potenziellen Kunden oder Kooperationspartnern über die vorhandenen technischen und organisatorischen Maßnahmen zum Datenschutz ganz selbstverständlich das interne Datensicherheitskonzept vor und sind dann selbst überrascht, dass es sich hierbei nicht um das erwünschte Dokument, nämlich ein Datenschutzkonzept handelt. Datenschutz (Data Privacy) ist nicht gleichzusetzen mit Datensicherheit (Data Security). Datenschutz ohne ein funktionierendes internes IT-Sicherheitsmanagement [Borchert und Szidzek (2017⁴), S. 297 ff.] ist zwar nicht denk-

bar. Aber ein ausreichendes Maß an Datensicherheit gewährleistet noch lange keinen Datenschutz. IT-Sicherheit gewährleistet die Integrität, Vertraulichkeit und Verfügbarkeit von Daten. Datenschutz geht jedoch darüber hinaus.

Unter Datenschutz versteht man gemeinhin den Schutz vor missbräuchlicher Datenverarbeitung, Schutz des Rechts auf informationelle Selbstbestimmung, Schutz des Persönlichkeitsrechts bei der Datenverarbeitung und auch den Schutz der Privatsphäre. Die informationelle Selbstbestimmung umfasst die Befugnis des Einzelnen, grundsätzlich selbst darüber zu entscheiden, wenn und innerhalb welcher Grenzen persönliche Sachverhalte offenbart werden [BVerfGE 65, 1 (42) (1983)].

Datenschutz wird häufig als Recht verstanden, dass jeder Mensch grundsätzlich selbst darüber befinden darf, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Der Wesenskern eines solchen Datenschutzrechts besteht dabei darin, dass die Machtungleichheit zwischen Organisationen und Einzelpersonen unter Bedingungen gestellt werden kann. Der Datenschutz soll damit der in der zunehmend digitalen und vernetzten Informationsgesellschaft bestehenden Tendenz zum sogenannten gläsernen Menschen, dem einer Ausuferungen staatlicher Überwachungsmaßnahmen (Überwachungsstaat) und der Entstehung von Datenmonopolen in privater Händen von Privatunternehmen entgegenwirken. Hier schließt sich der Kreis zum Amazon-Case. Das Problem war im Amazon-Case kein Fall der mangelnden Data-Security. Allein schon aus Performance-Aspekten kann davon ausgegangen werden, dass Amazon über ein hohes Maß an Datensicherheit verfügt. Das Unternehmen wird sich einen Datenverlust oder kompromittierte Daten nicht leisten können, besteht doch seine Kerntätigkeit in der Verarbeitung von Daten. Das Problem besteht vielmehr in einer mangelnden Bereitschaft, die erhaltenen personenbezogenen Daten nur so zu verwenden, wie dies unter dem Aspekt des Datenschutzes oder der individuellen Kundensicht auf Basis der informationellen Selbstbestimmung zulässig ist. Hierzu bedarf es aber vor allem des vorhandenen Willens, Datenschutz umzusetzen und entsprechende Strukturen zur Gewährleistung des Datenschutzes zusätzlich zu den Maßnahmen der Informationssicherheit zu implementieren.

6 FAZIT – DIE DSGVO ALS VERTRAUEN SCHAFFENDE NORM

Wie nachfolgend ausgeführt, war ein Grund für den Erlass der DSGVO sicher die Erkenntnis, dass nationale Datenschutzgesetze der Realität internationaler Unternehmen und Organisationen nicht gerecht werden und man zumindest für Europa eine einheitliche, verbindliche Grundlage schaffen wollte. Das Thema betrifft nicht nur Amazon. Es geht ebenso um Unternehmen wie Facebook, Google, Yahoo, Twitter, Microsoft, Apple und viele andere, die bereits heute über mehr Daten von Personen verfügen als viele Staaten, jedoch keinen verfassungsmäßigen Schranken unterworfen zu sein scheinen, was den Umgang mit diesen Daten betrifft.

Die DSGVO soll zum einen das Datenschutzrecht EU-weit vereinheitlichen [Albrecht und Jotzo (2017), S. 144]. Das Schutzniveau für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten soll in der gesamten EU gleichmäßig hoch und einheitlich sein [Wytibul (2017), S. 3]. Zugleich soll der Binnenmarkt in der Union gestärkt werden [Ebd.]. Die DSGVO verlangt daher den Aufbau umfassender Datenschutzstrukturen in Organisationen sowie die Implementierung von Datenschutzmaßnahmen bei der Entwicklung von Produkten und dem Design von Dienstleistungen, um die Einhaltung des Datenschutzes sicherzustellen. Daneben soll über die DSGVO europaweit ein möglichst einheitliches System der Datenschutzaufsicht geschaffen werden. Eines der im Gesetzgebungsverfah-

ren immer wieder betonten Ziele der DSGVO war die Etablierung des sog. »One-Stop-Shop«, so dass auch bei grenzüberschreitenden Sachverhalten zur Vereinfachung und Erleichterung der Kommunikation alle Abstimmungen eines Unternehmens mit einer einzigen Aufsichtsbehörde vorzunehmen wären [Laue, Nink und Kremer (2016), S. 288]. Ein Ping-Pong-Spiel von Behörden wie im Amazon-Case wäre dann nicht mehr möglich; widersprüchliche Zuständigkeiten wären beseitigt. Mit Art. 56 Abs. 6 DSGVO hat man dieses Ziel zwar nicht ganz erreicht, da der Grundsatz in Einzelfällen durchbrochen werden kann. Man hat aber zumindest sichergestellt, dass datenverarbeitende Unternehmen sich stets an eine federführende Aufsichtsbehörde zu wenden haben [Ebd., S. 289].

Die immanente Botschaft der DSGVO besteht darin, dass die Politik es im Gegensatz zu gro ßen Teilen der Privatwirtschaft bereits verstanden hat, dass Menschen in Big-Data-Zeiten zunehmend nur noch solchen Organisationen Vertrauen schenken werden, die einen datenschutzkonformen Umgang mit personenbezogenen Daten gewährleisten und bei denen ein Missbrauch zu anderen Zwecken als dem Zweck, zu dem diese Daten übermittelt wurden, ausgeschlossen ist. Um den Konsens der Menschen als Bürger und auch als Kunde hinsichtlich erforderlicher Datenverarbeitungen zu erreichen, bedarf es in allen Fällen eines Grundvertrauens in den Staat ebenso wie in Unternehmen, denen der Kunde seine Daten freiwillig übermittelt. Dies sicherzustellen, hat sich die DSGVO zur Aufgabe gemacht. Die DSGVO zielt damit auf etwas, über den Schutz des Rechtes auf informationelle Selbstbestimmung Hinausgehendes ab: Indem sie das erwartbare Schwinden des Vertrauens der Kunden in die datenverarbeitende Industrie – wenn auch unter dem Druck massiver Bußgeld- und Strafandrohungen – wiederherstellt und so zukunftsweisend alle Unternehmen, die ihrem Rechtsregime unterliegen, in einem aufgeklärten Informationszeitalter wettbewerbs- und konkurrenzfähig macht gegenüber all denen, die Datenschutz bestenfalls als lästigen Klotz am Bein empfinden. Betrachtet man die Grundprinzipien der DSGVO, so entsprechen diese dem Referenzmodell für Vertrauen in frappierender Weise:

Die DSGVO legt folgende Grundprinzipien für die rechtmäßige Verarbeitung personenbezogener Daten fest:

- Rechtmäßigkeit der Datenverarbeitung, Art. 5 Abs. 1 lit. a) DSGVO
- Verarbeitung nach Treu und Glauben, Transparenz, Art. 5 Abs. 1 lit. a) DSGVO
- Zweckbindung, Art. 5 Abs. 1 lit. b) DSGVO
- Datensparsamkeit und Speicherbegrenzung, Art. 5 Abs. 1 lit. c) DSGVO
- Richtigkeit und Aktualität, Art. 5 Abs. 1 lit. d) DSGVO
- Integrität und Vertraulichkeit, Art. 5 Abs. 1 lit. f) DSGVO
- Grundsatz der Verantwortlichkeit und Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO

Unter dem Faktor der Fähigkeit (ability) lassen sich die Grundprinzipien der Datensparsamkeit und Speicherbegrenzung, Art. 5 Abs. 1 lit. c) DSGVO sowie der Richtigkeit und Aktualität, Art. 5 Abs. 1 lit. d) DSGVO erfassen, d. h. die technische Fähigkeit mit Daten überhaupt datenschutzkonform umgehen zu können. Wo weder entsprechende technische und organisatorische Maßnahmen für einen datenschutzkonformen Umgang mit personenbezogenen Daten geschaffen ist, kann kein Datenschutz funktionieren. Wo jeder Mitarbeiter im Unternehmen auf sämtliche Daten zugreifen kann, ist eine unbefugte Kenntnisnahme vorprogrammiert.

Integrität (integrity) kann als Metabegriff für die Prinzipien der Rechtmäßigkeit der Datenverarbeitung (Art. 5 Abs. 1 lit. a DSGVO), der Verarbeitung nach Treu und Glauben sowie Richtigkeit der vorgehaltenen Daten und Transparenz der Verarbeitung (Art. 5 Abs. 1 lit. a DSGVO),

verstanden werden. Wo Daten etwa vielfach redundant an verschiedenen Speicherplätzen in einem System abgelegt sind, wird eine Datenintegrität nicht zu gewährleisten sein. Dort ist auch die Transparenz der Verarbeitung ausgeschlossen, da eine Kontrolle über die Daten nicht gegeben ist.

Das geforderte Wohlwollen findet sich wieder im Grundsatz der Zweckbindung der Datenverarbeitung (Art. 5 Abs. 1 lit. b) DSGVO), sowie im Grundsatz der Verantwortlichkeit, Art. 5 Abs. 2 DSGVO. Wo sich ein Unternehmen über den Zweck, zu dem ihm Daten von Personen zur Verfügung gestellt werden, hinwegsetzt, kann nicht davon ausgegangen werden, dass dieses Unternehmen den Rechtspositionen seiner Kunden gegenüber wohlwollend eingestellt ist. Indem die DSGVO Vertrauen in die Einhaltung des Datenschutzes durch Staaten und Unternehmen wiederherzustellen versucht, trägt sie dazu bei, wieder Vertrauen der Kunden in die datenverarbeitenden Unternehmen selbst zu schaffen.

Man kann damit konstatieren, dass die DSGVO als Norm den Unternehmen nichts anderes als die Einhaltung des Referenzmodells für Vertrauen abverlangt, um auf einem trust-driven market auch in Zukunft Bestand haben zu können. Sollten sich künftig Unternehmen etablieren, welche vergleichbare Leistungen zu vergleichbaren Konditionen anbieten können wie z. B. Amazon, dabei aber Transparenz und rechtmäßigen Umgang mit Kundendaten gewährleisten, hätten diese Unternehmen gegenüber Amazon einen nicht zu unterschätzenden Wettbewerbsvorteil.

Die DSGVO unternimmt nun den Versuch – auch im Sinne einer volkswirtschaftlichen Notwendigkeit für die EU-Staaten – alle Unternehmen auf ein einheitliches und europäisches Datenschutzrecht zu verpflichten. So kann Vertrauen durch Rechtsetzung begünstigt und erzeugt werden, wo Unternehmen selbst nicht in der Lage oder willens sind, dieses Vertrauen in kluger Vorausschau selbst zu erzeugen [Bolsinger (2016), S. 385].
Im obigen Amazon-Case wurde die Frage, ob sich Amazon auf der Grundlage luxemburgischen oder deutschen Rechts rechtmäßig verhalten hat, bewusst nicht abschließend beantwortet, denn darum geht es nur vordergründig. Rechtskonformität allein schafft kein Vertrauen in ein Unternehmen.

Die Einhaltung des Datenschutzes wird künftig Voraussetzung für das Zustandekommen nahezu aller geschäftlichen Beziehungen innerhalb der EU oder mit Unternehmen der EU sein. Unternehmen werden sich künftig gemäß § 43 DSGVO von anerkannten Zertifizierungsstellen auf die Einhaltung des Datenschutzes zertifizieren lassen können. Wer europaweit aktiv ist, wird eine solche Zertifizierung nicht ausschließen können. Der wesentliche Mehrwert bei der Umsetzung der Vorgaben der DSGVO besteht für Unternehmen darin, dass durch Einhaltung dieser Vorgaben dem übergeordneten und zukunftsweisenden Referenzmodell Vertrauen Rechnung getragen wird. Hinzu kommt, dass nach dem Modell des emotionalen Framings nach Kahneman [Kahneman (2011), S. 447 ff.] die Abstrahlwirkung einer proaktiv verfolgten und öffentlich wahrnehmbaren Verantwortungsübernahme für den Schutz personenbezogener Daten auch ein generelles Vertrauen in das Unternehmen erzeugt: in die Produktqualität und -sicherheit, den Stand der Technik, die Verlässlichkeit. Allein weil der immer aufmerksamer wahrgenommene Referenzpunkt Datenschutz positiv besetzt wird.

REFERENZEN

Albrecht, J. P. und Jotzo, F. (2017): Das neue Datenschutzrecht der EU, Baden-Baden.

Arendt, H. (2007): Vita Activa. Vom tätigen Leben, München.

Böhm, M. (o. J.): Folgen der NSA-Affäre – Wie Snowden das Netz verändert hat, in: Spiegel-Online, http://www.spiegel.de/netzwelt/netzpolitik/nsa-skandal-wie-snowdens-enthuellungen-das-netz-veraendert-haben-a-973516.html, zuletzt aufgerufen am 09. 12. 2017.

Bolsinger, H. (2015): Amazon im Umgang mit Kundendaten – Ein Selbstversuch, www.datenschutz.wirtschaftsethik.biz, zuletzt aufgerufen am 09. 12. 2017.

Bolsinger, H. (2016): Wo bleibt die digitale Dividende für Europas Konsumenten?, in: DuD 40/2016, S. 382-385.

Borchert, M. und Szidzek, C. (2017[4]): Umsetzung, Prüfung und Beurteilung des internen IT-Sicherheitsmanagements, in: Weimer, L. (Hrsg.), Datenschutz, IT-Sicherheit & Cyber-Risiken, Heidelberg, S. 297-384.

Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. 01. 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 10 Absatz 2 des Gesetzes vom 31. 10. 2017.

Bundesverfassungsgericht (Urteil vom 15. 01. 1983), BVerfGE 65, 1 (42).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031-0050, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=DE, zuletzt aufgerufen am 12. 12. 2017.

Grimm, R., Bräunlich, K. (2015): Vertrauen und Privatheit – Anwendung des Referenzmodells für Vertrauen auf die Prinzipien des Datenschutzes, DuD 5/2015, S. 289-293.

Kahl, B. (2017): Aktuelle Herausforderungen für die äußere Sicherheit der Bundesrepublik Deutschland. Auswirkungen auf Arbeit und Aufgaben des Bundesnachrichtendienstes, in: Sensburg, P. E. (Hrsg.): Sicherheit in einer digitalen Welt, Baden-Baden.

Kahneman, D. (2011): Schnelles Denken, langsames Denken, München.

Laue, P., Nink, J. und Kremer, S. (2016): Das neue Datenschutzrecht in der betrieblichen Praxis, Köln.

Mayer, R.C., Davis, J.H. und Schoorman, F.D. (1995): An integrative model of organizational trust. Academy of Management Review, July 1, 1995, S. 709-734.

Palandt, O. und Sprau, H. (2011[70]): Bürgerliches Gesetzbuch, München.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation /GDPR), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?-uri=CELEX:32016R0679&from=DE, zuletzt aufgerufen am 12. 12. 2017.

Wytibul, T. (2017), in: Wytibul, T. (Hrsg.), EU-Datenschutz-Grundverordnung, Frankfurt a.M.