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

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur siebten Ausgabe des BayWiDI-Newsletters. Ein insbesondere aus IT-sicherheitsrechtlicher Perspektive spannendes Jahr neigt sich dem Ende zu. Allen voran die jüngst bekannt gewordenen Datendiebstähle, allgemeine Sicherheitslücken im Bereich des e-Commerce sowie Erpresser-Software im Einsatz gegen Bürger, Industrie, Infrastruktur und Staat prägten maßgeblich die deutsche Medienlandschaft. Korrespondierend zu der gesellschaftlichen Sensibilisierung lässt sich aber auch feststellen, dass die entsprechende legislative Regulierung im Jahr 2017 an Fahrt aufgenommen hat. Beispielhaft sei hier auf die Änderung der Verordnung zur Bestimmung kritischer Infrastrukturen[1] vom 21. Juni 2017 hingewiesen, auf deren Grundlage nunmehr sämtliche Betreiber aus den sieben Sektoren des § 2 Abs. 10 Nr. 1 BSIG in der Lage sind, ihre Infrastrukturen auf eine mögliche Kritikalität zu prüfen. Aber auch digitale Dienstleistungen, mithin Online-Marktplätze, Suchmaschinen respektive Cloud-Computing-Dienste waren 2017 im Fokus der gesetzgeberischen Tätigkeit. Von zentraler Bedeutung ist dabei das deutsche Umsetzungsgesetz zur NIS-Richtlinie[2], welches in § 8c BSIG erhöhte Anforderungen an die Anbieter entsprechender Dienstleistungen stellt. Insbesondere sind ab dem 10. Mai 2018 geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme zu reduzieren. Zudem bringt der Mai 2018 weitere signifikante Novellen im Bereich der Datensicherheit mit sich: Sowohl die Datenschutz-Grundverordnung (DS-GVO) als auch das neugefasste Bundesdatenschutzgesetz (BDSG) erlangen zeitgleich ab dem 25. Mai 2018 Geltung. Aus IT-sicherheitsrechtlicher Perspektive sind dabei allen voran die Grundsätze Privacy by Design sowie Privacy by Default von besonderem Interesse. Die wesentlichen Grundlagen dieser schillernden Begriffe des Datenschutzes können Sie dem Beitrag auf Seite 2 entnehmen.

Mit Blick auf die technischen Innovationen wurde das Jahr 2017 insbesondere durch die zunehmende Verbreitung digitaler Sprachassistenten geprägt. Siri, Cortana, Bixby, Google Assistant oder auch Alexa bilden das Rückgrat des „Internet of Voice“ und zugleich den Brennpunkt IT-sicherheitsrechtlicher Bedenken – nicht nur wenn Letztgenannte die Abwesenheit des Hausherrn dazu nützt, ausgiebig zu feiern[3]. Eine Einschätzung der (rechtlichen) Chancen und Risiken liefert der Beitrag auf Seite 5.

Mit diesen einleitenden Worten wünsche ich Ihnen eine unterhaltsame Lektüre bei unserem Newsletter, ein frohes Weihnachtsfest sowie einen guten Rutsch in das neue Jahr.

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

Inhalt

1 Erste Verordnung zur Änderung der BSI-Kritisverordnung vom 21. Juni 2017, BGBl. I 2017, S. 1903.

2 Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23. Juni 2017, BGBl. I 2017, S. 1885.

3 Vgl. dazu: *Klasen*, Alexa feiert alleine eine Party – bis die Polizei kommt, Süddeutsche Zeitung v. 10. November 2017. Online abrufbar unter: http://www.sueddeutsche.de/panorama/sprachassistent-alexa-feiert-alleine-party-bis-die-polizei-kommt-1.3737128, zuletzt abgerufen am 7. Dezember 2017.

Datensicherheit im Kontext der DS-GVO: Privacy by Design – Privacy by Default

Die Datensicherheit gestaltet sich als wesentlicher Teil des IT-Sicherheitsrechts. Wenngleich bereits die Datenschutzrichtlinie in Art. 17 als auch das bisherige Bundesdatenschutzgesetz (BDSG) in § 9 Bestimmungen zur Datensicherheit normierten, werden diese in Zukunft durch die abschließenden Regelungen der Datenschutz-Grundverordnung verdrängt.[1] Mit den nunmehr unter anderen in Art. 25 Datenschutzgrundverordnung (DS-GVO) kodifizierten Vorgaben werden die Bestimmungen zur Datensicherheit erweitert, wobei insbesondere als „Novum“[2] datenschutzfreundliche Voreinstellungen verlangt werden. Der folgende Beitrag liefert eine prägnante Übersicht über die ab dem 25. Mai 2018 zu beachtenden Regulierungen im Bereich der Datensicherheit.

Adressat der Vorgaben zur Datensicherheit

Adressat der Vorgaben des Art. 25 DS-GVO ist nur der Verantwortliche im Sinne des Datenschutzrechts, nicht schon der Hersteller von datenschutzrechtlich relevanten Produkten. Die Verantwortlichkeit richtet sich dabei grundsätzlich nach Art. 4 Nr. 7 DS-GVO. Mithin ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle als verantwortlich im Sinne des Datenschutzes anzusehen, welche allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Verantwortliche Stelle ist dementsprechend jedenfalls wer die „Kontrolle über die Verarbeitung [innehat], also über die Vorgänge an sich entscheiden“[3] kann und auch tatsächlich entscheidet[4]. Aus Erwägungsgrund 78 DS-GVO ergibt sich allerdings, dass „in Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten [...] die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden [sollten], das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen“.[5] Dieser bloßen Appellfunktion kann unter Umständen auch eine wirtschaftliche Notwendigkeit[6] zukommen.

Art. 25 Abs. 1 DS-GVO - Datenschutz durch Technik: »Privacy by Design«

Unter „Privacy by Design“[7] beziehungsweise „data protection by design“[8] wird „Datensicherheit durch Technikgestaltung“ verstanden.

Art. 25 Abs. 1 DS-GVO verpflichtet in diesem Sinne den Verantwortlichen dazu, geeignete technische und organisatorische Maßnahmen (TOMs)[9] zu treffen. Dies bezweckt zweierlei: Zunächst sollen die allgemeinen Verarbeitungsgrundsätze[10], neben dem beispielhaft genannten Grundsatz der Datenminimierung also auch die Grundsätze der Transparenz, der Zweckbindung, der Richtigkeit, der Speicherbegrenzung sowie der Integrität

1 *Baumgartner/Gausling*, ZD 2017, 308, 309.

2 *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl 2017, Art. 25 Rn. 22.

3 *Schreiber*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 4 DSGVO Rn. 26; so auch *Klabunde*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 4 Rn. 25.

4 *Raschauer*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 4 Rn. 123.

5 Vgl.: Erwägungsgrund 78 DS-GVO.

6 *Brüggemann*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Aufl. 2017, Art. 25 DSGVO Rn. 5.

7 So *Nolte/Werkmeister*, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 25 Rn. 1; *Brüggemann*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Aufl. 2017, Art. 25 DSGVO Rn. 1; *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl 2017, Art. 25 Rn. 25.

8 Vgl.: Erwägungsgrund 78 DS-GVO; ebenso: *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 25 DSGVO Rn. 1. *Schulz*, CR 2012, 204, 206, merkt diesbezüglich kritisch an, dass es dem Begriff an einer hinreichend klaren Definition des Schutzgutes fehlt.

9 Vgl. etwa *Brüggemann,* in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Aufl. 2017, Art. 25 DSGVO Rn. 8; »Was bedeutet Privacy by Design / Privacy by Default wirklich?«. Online abrufbar unter: https://www.datenschutzbeauftragter-info.de/was-bedeutet-privacy-by-design-privacy-by-default-wirklich/, zuletzt abgerufen am 7. Dezember 2017.

10 Der Begriff ist als Verweis auf Art. 5 Abs. 1 DS-GVO zu verstehen, vgl. nur *Nolte/Werkmeister*, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 25 Rn. 11; *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 25 DSGVO Rn. 6.

und der Vertraulichkeit,[11] wirksam umgesetzt werden. Darüber hinaus sollen aber auch die notwendigen Garantien beziehungsweise „safe guards“[12] in die Verarbeitung aufgenommen werden, um den Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen zu schützen. Insbesondere gelten diese Anforderungen für die Programmierung, Erstellung und Konzeptionierung der entsprechenden Anwendungen.[13] Nach *Wolff* werden „dem Verantwortlichen [...] in gewisser Form die Obliegenheiten der betroffenen Person, durch eigenes Verhalten die Umsetzung des Grundsatzes der Datenminimierung zu erreichen, übertragen“.[14]

Im Unterschied zu Art. 24 DS-GVO wird dem Konzept des Datenschutzes durch Technik in Art. 25 DS-GVO inhaltliche Kontur verliehen,[15] sodass Art. 25 DS-GVO eigenständige Bedeutung zukommt.

Zu unterscheiden ist zwischen zwei Zeitpunkten: Zum einen dem, zu dem die Mittel für die Verarbeitung festgelegt werden,[16] zum anderen dem, zu dem die eigentliche Verarbeitung stattfindet. Besonders hervorzuheben ist also, dass die Datenschutzgrundsätze schon bevor es zu irgendeiner Art der Datenverarbeitung kommt, umzusetzen sind. In zeitlicher Hinsicht wird damit der gesamte Lebenszyklus[17] einer Anwendung erfasst. Allerdings ist der sachliche Anwendungsbereich der DS-GVO gem. Art. 2 Abs. 1 erst dann eröffnet, wenn tatsächlich personenbezogene Daten

verarbeitet werden, sodass ein Pflichtverstoß wohl auch erst zu diesem Zeitpunkt vorliegt.[18]

Art. 25 Abs. 1 DS-GVO nennt vier Kriterien, an denen die Eignung der TOMs im Einzelfall[19] zu messen ist:

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zweck der Verarbeitung
- Unterschiedliche Eintrittswahrscheinlichkeiten und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten des Betroffenen

Zur Bestimmung der erforderlichen TOMs können die Vorgaben des IT-Grundschutzkatalogs als Orientierungshilfe herangezogen werden.[20]

Insgesamt kann festgehalten werden, dass dem Verantwortlichen ein Auswahl- und Gestaltungsermessen hinsichtlich der TOMs zugesprochen wird.[21]

Explizit wird allein die Pseudonymisierung als in Frage kommende TOM benannt, aus der Formulierung der Norm („wie z.B.“) ergibt sich jedoch, dass weitere geeignete Maßnahmen heranzuziehen sind. Wenn schon die Pseudonymisierung tauglich ist, muss dies erst recht für die Anonymisierung von Daten gelten.[22]

Art. 32 Abs. 1 lit. a DS-GVO, der die Verschlüsselung grundsätzlich als probates Mittel der Datensicherung benennt, lässt den Rückschluss zu, dass die Verschlüsselung auch im Kontext des Datenschutzes durch Technikgestaltung zum Einsatz gebracht werden kann.

Ferner kommen Zugangs- und Zutrittskontrollen in Betracht.[23] Jedenfalls als Anhaltspunkt für weitere geeignete Maßnahmen bietet es sich zudem an, die bisherige Anlage zu § 9 Satz 1 BDSG heranzuziehen.[24] Auch eine Zertifizierung, etwa nach dem Standard ISO 27001, stellt grundsätzlich eine taugliche TOM dar.[25] Weitere Möglichkeiten können schließlich dem korrespondierenden Erwägungsgrund entnommen werden. So stellt Erwägungsgrund 78 Satz 3 DS-GVO klar, dass beispielsweise die Schaffung einer Überwachungsmöglichkeit der Datenverarbeitung durch die betroffene Person eine Maßnahme im Sinne des Art. 25 Abs. 1 DS-GVO sein kann.[26] Dies gilt entsprechend für die Schaffung eines automatisierten Verfahrens, mit dem der Betroffene von seinem Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO Gebrauch machen kann.[27]

Verallgemeinernd lässt sich festhalten, dass es jedenfalls eines wie auch immer gearteten Datenschutzkonzepts bedarf.[28] Hierfür kann insbesondere der Bericht der Europäischen Agentur für Netz- und Informationssicherheit herangezogen werden.[29]

11 Vgl. auch: Erwägungsgrund 78 DS-GVO.

12 *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 25 DSGVO Rn. 6.

13 *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 25 DSGVO Rn. 6.

14 *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl 2017, E. Technisch-Organisatorische Pflichten Rn. 832.

15 *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl 2017, Art. 25 Rn. 9.

16 Der Ansatz steht damit im deutlichen Kontrast zu bisherigen Konzepten, welche oftmals Fragen zur Datensicherheit erst im Anschluss an die eigentliche Planung der Verarbeitung einbeziehen, vgl.: *Steinebach/Krempel/Jung/Hoffmann*, DuD 2016, 440, 441.

17 *Brüggemann*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Aufl. 2017, Art. 25 DSGVO Rn. 7.

18 So jedenfalls *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 25 DSGVO, Rn. 4.

19 *Brüggemann*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Aufl. 2017, Art. 25 DSGVO Rn. 8.

20 So jedenfalls *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 25 Rn. 40.

21 *Nolte/Werkmeister*, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 25 Rn. 20.

22 So i. E. wohl auch *Steinebach/Krempel/Jung/Hoffmann*, DuD 2016, 440, 443.

23 *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 25 DSGVO, Rn. 4.

24 *Brüggemann*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Aufl. 2017, Art. 25 DSGVO Rn. 10.

25 *Brüggemann*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Aufl. 2017, Art. 25 DSGVO Rn. 10.

26 Vgl.: Erwägungsgrund 78 Satz 3 DS-GVO.

27 *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl 2017, Art. 25 Rn. 32.

28 In diesem Sinne auch *Nolte/Werkmeister*, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 25 Rn. 19.

29 Abrufbar unter https://www.enisa.europa.eu/publications/privacy-and-data-pro-

Relevant kann schließlich auch eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO werden; inwiefern diese selbst im Regelfall empfehlenswert ist, ist noch nicht abschließend geklärt.[30]

Art. 25 Abs. 2 DS-GVO - Datenschutz durch Voreinstellung: »Privacy by Default«

Der Grundsatz „Privacy by Default" beziehungsweise „data protection by default"[31] findet sich in Art. 25 Abs. 2 Satz 1 DS-GVO. Diesem zur Folge ist der Verantwortliche in der Pflicht, geeignete technische und organisatorische Maßnahmen zu treffen, welche sicherstellen, dass die Voreinstellungen der jeweiligen Anwendung nur die Verarbeitung der jeweils tatsächlich erforderlichen personenbezogenen Daten gestatten.

Die Vorschrift zielt dabei insbesondere auf digitale Dienste wie etwa soziale Netzwerke ab.[32] Diese erheben regelmäßig auf Grundlage der Voreinstellungen erheblich mehr personenbezogene Daten als tatsächlich für die Erbringung des Dienstes notwendig wäre.[33] Gerade in diesem Kontext wies der sog. *Düsseldorfer Kreis*[34] bereits mit Beschluss vom 8. Dezember 2011 darauf hin, dass die Voreinstellungen der entsprechenden Netzwerke das Recht auf informationelle Selbstbestimmung der Betroffenen hinreichend wahren müssen.[35] Der nunmehr formell im Datenschutzrecht normierte Grundsatz gestaltet sich letztlich als Konkretisierung der im bisherigen Datenschutzrecht bekannten Maßstäbe der Erforderlichkeit sowie der Zweckbindung.[36] Solange und soweit die Datenverarbeitung allerdings für die konkrete Anwendung erforderlich ist, wird diese nicht durch den Grundsatz der datenschutzfreundlichen Voreinstellungen begrenzt.[37]

Die Vorschrift beruht auf der Erkenntnis, dass die Betroffenen oftmals aus Bequemlichkeit keine Änderungen an den Voreinstellungen vornehmen.[38] Mithin reagiert die Norm auf das insbesondere in der Sozialwissenschaft diskutierte Phänomen des „Privacy Paradox", welchem zur Folge die Nutzer zwar grundsätzlich der Privatheit einen hohen Stellenwert beimessen, tatsächlich aber wenig Engagement für deren Erhalt in einer digitalisierten Umgebung an den Tag legen.[39] Um den Nutzer dennoch vor einer ungewollten und allen voran unbewussten Datenerhebung zu schützen, sind die Standardeinstellungen („by default") möglichst datensparsam zu setzen.[40] Ein Verstoß gegen Art. 25 Abs. 2 Satz 1 DS-GVO wäre beispielsweise dann gegeben, wenn die Voreinstellungen der Anwendung die Einwilligung zum Erhalt verschiedener Werbeangebote beinhalten würden.[41]

Freilich steht es dem Betroffenen dabei offen, entsprechend abweichende Einstellungen im Wege des „Opt-In" vorzunehmen.[42] Maßgeblich ist dabei allerdings, dass das „Maximum an Privatheit"[43] durch eine bewusste und aktive Entscheidung des Betroffenen minimiert wird[44]. Damit der Betroffene allerdings eine entsprechende Disposition vornehmen kann, obliegt es dem Verantwortlichen, den Nutzer vorab umfassend über die Tragweite seiner Entscheidung zu informieren, wobei gegebenenfalls die Einholung einer zusätzlichen Einwilligungserklärung erforderlich sein kann.[45]

Fazit

Die DS-GVO entwickelt die insbesondere im deutschen Datenschutzrecht bereits bekannten und bewährten Vorgaben zur Datensicherheit konsequent weiter, wobei auf einschneidende Veränderungen weitgehend verzichtet wurde. Auch nach den Vorgaben der Grundverordnung bestimmt sich das erforderliche Sicherheitsniveau dynamisch anhand offener Tatbestandsmerkmale wie beispielsweise dem Stand der Technik. So sinnvoll dieser Ansatz mit Blick auf den beständigen Wandel technischer Gegebenheiten ist, so sehr birgt er aber auch die Gefahr der Rechtsunsicherheit für die letztlich Verantwortlichen.

Scheurer/Brand

tection-by-design/at_download/fullReport. Zuletzt abgerufen am 7. Dezember 2017.

30 *Hartung*, in: Kühlung/Buchner, DS-GVO, 1. Aufl. 2017, Art. 25 Rn. 19, vertritt die These, dass die Schritte und Prüfungen nach Art. 25, 32, 35 DS-GVO möglicherweise zu verknüpfen sind, um zu sinnvollen Ergebnissen zu gelangen. *Brüggemann*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Aufl. 2017, Art. 25 DSGVO Rn. 10, scheint im Grundsatz nicht von einem gem. Art. 35 Abs. 1 geforderten hohen Risiko auszugehen. *Nolte/Werkmeister*, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 25 Rn. 24, sind der Ansicht, dass die Anforderungen an die Risikoanalyse in Art. 25 DS-GVO gerade geringer sein müssen, diese also im Regelfall im Rahmen von Art. 25 DS-GVO nicht vorzunehmen ist.

31 Vgl.: Erwägungsgrund 78 Satz 2 DS-GVO.

32 *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 25 Rn. 13.

33 *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil E. Rn. 838.

34 Bei dem Düsseldorfer Kreis handelt es sich um einen Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich. Dabei wird das Ziel verfolgt, grundlegende datenschutzrechtliche Fragen im Bundesgebiet einheitlich zu beantworten.

35 Düsseldorfer Kreis, Beschl. v. 08.12.2011 zu Datenschutz in sozialen Netzwerken. Online abrufbar unter: https://www.bfdi.bund.de/DE/Infothek/Entschliessungen/DuesseldorferKreis/functions/DKreis_table.html?nn=5217228. Zuletzt abgerufen am 7. Dezember 2017.

36 *Brüggemann*, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 5. Aufl. 2017, Art. 25 Rn. 294; *Paulus*, in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edit. Stand: 01.02.2017, Art. 25 DS-GVO Rn. 9.

37 *Barlag*, in: Roßnagel (Hrsg.), Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, § 3 Rn. 228.

38 *Baumgartner/Gausling*, ZD 2017, 308, 312.

39 *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 25 Rn. 12.

40 *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 25 Rn. 13.

41 Vgl.: *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 25 Rn. 14.

42 *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 25 DSGVO Rn. 9.

43 *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 25 DSGVO Rn. 9.

44 *Jandt*, DuD 2017, 562, 563; Baumgartner, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 25 Rn. 13.

45 *Brüggemann*, in: Eßer/Kramer/v. Lewinski, DSGVO BDSG, 5. Aufl. 2017, DS-GVO Art. 25 Rn. 15.

Sprachassistenten – alles unter Kontrolle?

Sprachassistenten haben in den letzten Jahren einen wahren Erfolg erfahren. Die kleinen Helfer eignen sich hauptsächlich dazu, verschiedene Geräte über ein einzelnes (fern) zu steuern. Alexa, Siri und andere sind dabei handlich in Form von Mikrofonen und kleinen Computern in Smartphones oder Lautsprecher eingebaut; aktiviert werden sie durch das Ansprechen mit dem eigenem Namen. Einmal aktiviert sind sie in der Lage, verschiedene Sätze und Befehle zu verarbeiten und auszuführen. Genannt seien beispielhaft das Ausführen einer Google-Suche, das Abspielen von Musik oder die Steuerung diverser Smart-Home Geräte von unterwegs.[1] Die Nutzung von Sprachassistenten bringt demnach zahlreiche Vorteile mit sich: Sowohl ihre Multi-Funktionalität als auch ihre Handlichkeit machen sie zu praktischen Alltagsbegleitern.

Aus rechtlicher Sicht haben sich durch die Nutzung von Sprachassistenten jedoch zahlreiche Fragen ergeben. Neben IT-sicherheits- und datenschutzrechtlichen Fragen sind verschiedene praktische Problematiken aufgetaucht, die aufgrund der Neuartigkeit der Geräte noch nicht geklärt sind.

Sprachassistenten in IT-sicherheitsrechtlicher und datenschutzrechtlicher Umgebung

Die Vernetzung von Geräten ist technisch bedingt hochkomplex. Sie zieht deswegen eine Reihe von Problemen mit sich, von denen hier lediglich einige ausgewählte exemplarisch dargestellt werden sollen.

IT-sicherheitsrechtlich bestehen nach derzeitigen Erkenntnissen zum Teil Sicherheitslücken im Bluetooth-System der Geräte.[2] Auch bei Behebung dieser Schwächen darf jedoch nicht vergessen werden, dass vernetzte Geräte bereits dem Grunde nach permanent der Gefahr des Zugriffs durch Dritte ausgesetzt sind. Dabei ist denkbar, dass vorhandene Sicherheitslücken ausgenutzt werden, um beispielsweise Steuerungselemente innerhalb der Wohnung zu manipulieren. Der Gedanke, dass Fremde unbemerkt die Heiztemperatur, die Position der Schlafzimmerrollläden oder die Aktivierung der Webcam kontrollieren können, erzeugt verständlicherweise erhebliches Unbehagen. Die Vorstellung, dass potenzielle Einbrecher die Abwesenheit der Bewohner bewusst durch das Ausspähen von Tagesabläufen ausnutzen können, vermag diese Bedenken sogar noch zu intensivieren.

Sofern Sprachassistenten im beruflichen Umfeld genutzt werden, ergeben sich zudem weitere Problemfelder. Von Bedeutung ist dabei beispielsweise die Gefährdung von Betriebsgeheimnissen im Rahmen von eigenen oder jedenfalls im Besitz befindlichen Arbeitsgeräten. Werden Sprachassistenten gezielt beruflich genutzt stellt sich außerdem die Frage, wie Schädigungen des Betriebsablaufs von außen vermieden werden können und wie diese in der Folge behandelt werden.

Regelmäßig verarbeiten Sprachassistenten personenbezogene Daten, so dass die entsprechenden datenschutzrechtlichen Regelungen der DS-GVO respektive des BDSG zur Anwendung gelangen.[3] Die Geräte lassen sich regelmäßig nur schwer mit den Grundprinzipien des Art. 5 DS-GVO vereinbaren.[4] Besonders problematisch ist dabei das Gebot der Zweckbindung gem. Art. 5 Abs. 1 lit. b DS-GVO. Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine eindeutige Festlegung der Zwecke der Datenverarbeitung im Kontext der Sprachassistenten

1 Bundesbeauftragte für Datenschutz und Informationssicherheit, Informationsblatt: Sprachassistenten, 2017, S. 1. Online abrufbar unter: https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSkompakt_Sprachassistenten.html, zuletzt abgerufen am: 7. Dezember 2017.

2 *Von Westernhagen*, BlueBorne: Bluetooth-Schwachstellen auch in Amazon Echo und Google Home (16.11.2017). Online abrufbar unter: https://www.heise.de/security/meldung/BlueBorne-Bluetooth-Schwachstellen-auch-in-Amazon-Echo-und-Google-Home-3891500.html, zuletzt abgerufen am 7. Dezember 2017.

3 Vgl.: *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 1 Rn. 20; *Ernst*, in: Paal/Pauly, DSGVO, 1. Aufl. 2017, Art. 1 Rn. 2.

4 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016 – Smart genug für die Zukunft?, Kassel 2016, S. 115.

wird aber vorab kaum darstellbar sein, da die Funktionsweise der Sprachassistenten darauf basiert, dass die Geräte jederzeit bereit sind zahlreiche (vorab unbestimmte) Befehle auszuführen. Wenn aber die konkreten Zwecke nicht benannt werden können ist bereits fraglich, ob in die Datenverarbeitung wirksam eingewilligt werden kann. Jedenfalls verlässt eine „Generaleinwilligung" zum Betrieb des Assistenten den Rechtsboden der Zweckbindung.[5] Weiter in Spannung stehen die Sprachassistenten zu datenschutzrechtlichen Auskunftsansprüchen.[6] Besucher von vernetzten Wohnungen sowie Personen, die unbewusst in Hörweite eines Sprachassistenten sprechen, sind sich der Erhebung ihrer Daten meist nicht bewusst.[7] Eine dahingehende, ausnahmslose Hinweispflicht des Gewahrsamsinhabers wäre praktisch nicht durchsetzbar. Dadurch wird die Schutzwirkung von § 34 BDSG außer Kraft gesetzt. In der Folge kann auch hier eine wirksame Einwilligung in die Datenerhebung nicht erfolgen.

Mit der Nutzung der Assistenten innerhalb der Wohnung ergeben sich weitere spezifische Probleme: Mit den von Alexa und anderen gespeicherten Daten lassen sich neben Verhaltensabläufen auch Gespräche aufzeichnen und abhören. Der in Art. 13 GG geschützte private Wohnraum wird in grundrechtlich bedenklicher Weise nach außen geöffnet. Problematisch ist zudem, dass die Vertraulichkeit und Integrität der Daten im Sinne des IT-Grundrechts, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, kaum gewährleistet werden kann, da es insbesondere an einem zuverlässigen Kontrollmechanismus seitens der Betroffenen mangelt. In der vernetzten Welt ist eine umfassende Übersicht über den Verbleib von Daten nur schwer zu erlangen,[8] wobei insbesondere das häufig fehlende technische Verständnis eine Rolle spielt. Denkbar ist darüber hinaus eine Verletzung des Rechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG.

Folgeprobleme

Denkbar ist, dass gespeicherte Befehle oder Gespräche zu Beweiszwecken verwendet werden. Obwohl der erste solcher Fälle[9] aus den U.S.A. stammt, ist diese Konstellation nicht so weit hergeholt, wie es scheint: Es wird bereits darüber gestritten, ob durch sog. Dashcams[10] aufgenommene Videos, die nicht anlassbezogen entstanden sind, zu Beweiszwecken verwendet werden dürfen.[11] Die Verwendung von zufällig in der eigenen Wohnung aufgenommenen Worten dürfte im Lichte des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG rechtlich schwierig sein.

Problematisch ist auch, welche Haftungen eine fehlerhafte Befehlsausführung nach sich zieht. In zwei äußerst unerwarteten Situationen ist diese Frage bereits relevant geworden. Im ersten Fall hat ein Nachrichtensprecher durch die ungewollte Aktivierung des Sprachassistenten eine Massenonlinebestellung verursacht.[12] Es stellt sich die Frage, ob der Eigentümer oder der Zweckveranlasser für diese Bestellung haftet. Zudem ist – perspektivisch gedacht – daran zu denken, ob Alexa und andere möglicherweise sogar selbstständig Verträge abschließen könnten. Dies ist bislang freilich mangels Rechtspersönlichkeit von Robotern noch Zukunftsmusik. Ganz von der Hand zu weisen ist dieser Gedanke jedoch nicht, wie bereits aktuelle Diskussionen über die Rechtsfähigkeit von Robotern zeigen.[13]

In einem weiteren Fall wurde die Sprachassistentin Alexa ebenfalls auf bisher ungeklärte Ursache aktiviert und begann zur Nachtzeit laut Musik abzuspielen. Da der Eigentümer zu der Zeit nicht Zuhause war, riefen die Nachbarn die Polizei, die zur Beseitigung der Ruhestörung die Wohnungstür aufbrach.[14] Die Kosten für den Einsatz wurden im Anschluss von dem Eigentümer des Gerätes verlangt. Von besonderem Interesse ist dabei die Frage, ob der betroffene Eigentümer als Störer im Sinne des Polizeirechts herangezogen werden kann, wenn er tatsächlich zu diesem Zeitpunkt keine Möglichkeit der Einflussnahme auf das Gerät hatte. In Betracht kommt dabei die Haftung als sog. Zustandsstörer. Voraussetzung dafür ist allerdings, dass die herangezogene Person tatsächlich Inhaber der Sachherrschaft ist. Die Haftung als Zustandsstörer für die Gefahren, die von einem Gegenstand ausgehen, beruht auf dem Gedanken, dass der Inhaber der Sachherrschaft für die dem Gegenstand inhärenten Risiken einstehen muss. Die damit implizierte Sicherungspflicht setzt aber die rechtliche und tatsächliche Einwirkungsmöglichkeit voraus.[15] Daher ist zweifelhaft, ob solche Schäden, die völlig abseits vom üblichen Gebrauch und ohne die geringste Einwirkungsmöglichkeit des Gewahrsamsinhabers entstehen, auch darunter fallen können. Dieser Argumentation folgend könnte eine Inanspruchnahme auch unter dem Aspekt der Verhältnismäßigkeit problematisiert werden. Eine polizeiliche Inanspruchnahme stellt nämlich stets einen Grundrechtseingriff dar und muss daher im Rahmen der Verhältnismäßigkeit zur Gefahrenbeseitigung geeignet sein. Geeignet ist eine solche Maßnahme dann, wenn sie den mit ihr verfolgten Zweck

5 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016 – Smart genug für die Zukunft?, Kassel 2016, S. 116.

6 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016 – Smart genug für die Zukunft?, Kassel 2016, S. 113.

7 *Heidrich/Maekeler*, Alexa, darfst du das? Rechtliche Probleme durch Sprachssistenten, c´t 2017, S. 86 f.

8 *Heidrich/Maekeler*, Alexa, darfst du das? Rechtliche Probleme durch Sprachssistenten, c´t 2017, S. 86.

9 *Jurran*, Ermittler wollen Aufzeichnungen von Amazon Echo: Alexa als Zeugin einer Mordanklage? (28.12.2016). Online abrufbar unter: https://www.heise.de/newsticker/meldung/Ermittler-wollen-Aufzeichnungen-von-Amazon-Echo-Alexa-als-Zeugin-einer-Mordanklage-3582492.html, zuletzt abgerufen am 7. Dezember 2017.

10 Vgl. dazu ausführlich: *Starnecker*, Videoüberwachung zur Risikovorsorge, 2017.

11 Übersichtlich dazu *Mienert/Gipp*, ZD 2017, 514 ff.

12 Online abrufbar unter: https://www.stern.de/digital/homeentertainment/amazon-echo-bestellt-eigenmaechtig-massenhaft-puppenhaeuser-7272744.html, zuletzt abgerufen am 7. Dezember 2017.

13 *Häuser*, Roboter als Rechtsperson? Online abrufbar unter: https://www.it-business.de/roboter-als-rechtsperson-a-584846/, zuletzt abgerufen am 7. Dezember 2017.

14 Online abrufbar unter: https://www.berliner-zeitung.de/digital/wegen-ruhestoerung-amazons--alexa--verursacht-teuren-polizeieinsatz-28774978, zuletzt abgerufen am 7. Dezember 2017.

15 *Malmberg*, in: Drewes/Malmberg/Walter, 4. Aufl. 2010, § 18 BPolG Rn. 1 f.

fördert.[16] Eine Inanspruchnahme vermag den Zweck der Störungsbeseitigung jedoch dann nicht zu fördern, wenn der in Anspruch Genommene keine Macht über die Störung durch das Gerät hat.
Gegen den Verkäufer oder den Hersteller wiederum kommt – sofern ein Verschulden nicht nachweisbar ist – höchstens ein Regressanspruch in Betracht. Die verschuldensunabhängige Produzentenhaftung aus § 1 Abs. 1 Satz 1 ProdHG greift nur bei Schädigungen von Körper, Leben oder Sachen. Jedenfalls im Rahmen mittelbarer Verletzungen könnte man an eine entsprechende Anwendung der Vorschrift denken.

Aktuelle Rechtslage und Regelungsbedarf

Da, wie gezeigt, das Datenschutzrecht grundsätzlich auch bei Sprachassistenten zur Anwendung gelangt, sind die dort normierten Vorgaben zur Datensicherheit zu beachten. Damit ist eine Grundlage für die Datensicherheit im Ansatz vorhanden. Eine bereichsspezifische Regelung haben Sprachassistenten derzeit jedoch noch nicht erfahren.[17] Problematisch bleibt auch die Umsetzung eines ausreichenden Sicherheitsniveaus im Hinblick auf internationale Sachverhalte. Entscheidende Aspekte der IT- und Datensicherheit sind auch die Transparenz und die damit verbundene Kontrollmöglichkeit durch den Nutzer. Die Neuartigkeit der möglichen Fallkonstellationen begründet im Hinblick auf das Gebot des effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG auch einen Regelungsbedarf zu haftungsrechtlichen Folgefragen.
Erforderlich sind also Rahmenbedingungen, die von Experten gesetzt und kontrolliert werden. Dies muss vor dem Hintergrund der Globalisierung auch auf internationaler Ebene geschehen. Denkbar wäre konkret, die Vernetzung von Geräten – in Anlehnung an das Stichwort »Internet of Things« – zum Regelungsgegenstand eines besonderen Datenschutzrechts zu machen. IT-sicherheitsrechtlich ist das Festlegen von Sicherheitsstandards erforderlich, beispielweise durch Privacy by Design.[18] Zur Festsetzung und Einhaltung dieser Standards sind Verantwortliche zu bestimmen. Aus der Verantwortlichkeit müssen sich wiederum dynamische Plichten zur Instandhaltung ergeben, die unbefugten Datenzugriffen oder Steuerungsübernahmen vorbeugen. Trotz wachsenden technischen Verständnisses in der Gesellschaft muss die Verantwortlichkeit wegen der unüberschaubaren und sich stets wandelnden Risiken bei designierten Spezialisten angesiedelt werden. Insofern könnte darüber nachgedacht werden, ob (unter anderem) das sog. IT-Grundrecht eine staatliche Handlungspflicht auslöst.[19] Die Bedeutung von IT-Abteilungen in Unternehmen, die die Herstellung von Sprachassistenten und anderen vernetzten Geräten verantworten, könnte beispielsweise im Rahmen eines Aufgaben- und Standardkatalogs gesetzlich verankert werden. Die Bedeutung der betroffenen Grundrechte spricht jedenfalls für eine schnellstmögliche Schaffung von rechtlicher und technischer Sicherheit.

Nawrocki

16 *Grzeszick*, in: Maunz/Dürig, Kommentar zum GG, 80. EL Juni 2017, Art. 20 GG Rn. 112.

17 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016 – Smart genug für die Zukunft?, Kassel 2016, S. 64.

18 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016 – Smart genug für die Zukunft?, Kassel 2016, S. 143.

19 Vgl. hierzu: *Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleisung von IT-Sicherheit – Erste Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung", in: Rüßmann (Hrsg.), Festschrift für Gerhard Käfer, 2009, S. 129 ff.

Der nächste Newsletter erscheint im Frühjahr 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 einfach an 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.