Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

7/8
K&R

Editorial: Weckruf für deutsche Großunternehmen? – Der neue Entwurf des IT-Sicherheitsgesetz 2.0 · *Dr. Alexander Golland*

469 Der neue Medienstaatsvertrag – Was gilt für Medienplattformen, Benutzeroberflächen und Medienintermediäre? *Dr. Christoph Enaux* und *Dr. Lucas Wüsthof*

476 Datenschutz im Homeoffice – Ein Überblick *Dr. Jan Verheyen* und *Daniel Elgert*

479 Datengestützte Wahlwerbung wie Microtargeting aus datenschutzrechtlicher Perspektive · *Tristan Radtke*

486 Beweislastverteilung und Haftungsgrundsätze beim Filesharing *Christian Galetzka* und *Erik Stamer*

493 Die Entwicklung des Urheberrechts seit Mitte 2019 *Dr. Alexander R. Klett* und *Dr. Natascha M. Leyendecker*

500 Aktuelle Herausforderungen für Telekommunikationsüberwachungsmaßnahmen durch die Nachrichtendienste *Prof. Dr. Franziska Schneider*

506 Länderreport Österreich · *Prof. Dr. Clemens Thiele*

509 EuGH: Verfügbare Telefonnummer im Impressum muss in Widerrufsbelehrung genannt werden

511 BVerfG: Recht auf Chancengleichheit der Parteien durch Veröffentlichung auf Ministeriums-Webseite verletzt

533 BGH: Metall auf Metall IV: Keine Verletzung des Vervielfältigungsrechts durch Übernahme von Audiofragmenten

537 BGH: Rückabwicklung eines Amazon-Marketplace-Kaufvertrags

547 OLG Köln: SmartLaw: Generator für Rechtsdokumente stellt keine erlaubnispflichtige Rechtsdienstleistung dar

553 LG Köln: Unerlaubte TV-Werbung für Online-Glücksspiel mit Kommentar von *Carsten Bringmann*

564 Glosse: Onlinezensur via Haftung · *Clemens Kochinke*

23. Jahrgang **Juli/August 2020** Seiten 469 – 564

dfv Mediengruppe · Frankfurt am Main

V. Fazit und Ausblick

Der MStV zeigt einmal mehr, wie schwierig es ist, konventionelle Regulierungsinstrumente der Medienregulierung auf neuartige digitale Medienformen anzuwenden und allgemeingültige Lösungen für vielfältige neue Angebotsformen auf sich rasant entwickelnden Märkten zu finden. Die unscharfen und zum Teil überlappenden Definitionen von Medienplattformen, Benutzeroberflächen und Medienintermediären und die dargestellten offenen Fragen auf Rechtsfolgenebene verdeutlichen, welchen Schwierigkeiten Gesetzgeber und Regulierer gegenüberstehen, wenn sie den Versuch unternehmen hybride Medienformen für den Rechtsanwender greifbar zu machen – und auch, welche Unsicherheiten damit für alle Marktteilnehmer verbunden sind. Es erscheint insofern zweifelhaft, ob die Länder mit dem MStV ein rechtssicheres und praxistaugliches Gesetz auch für neue Angebotsformen geschaffen haben.

Umso mehr sind nun die Landesmedienanstalten aufgefordert durch klare Satzungsvorgaben und Auslegungshilfen eine praxistaugliche und verhältnismäßige Anwendung des MStV für alle Regulierungsadressaten sicherzustellen.

RA Dr. Jan Verheyen, Düsseldorf und RA Daniel Elgert, Bielefeld*

Datenschutz im Homeoffice – Ein Überblick

Das Thema Homeoffice hat aufgrund der Corona-Krise einen immensen Bedeutungszuwachs erfahren. Laut einer aktuellen Studie der Universität Mannheim vom 16. 4. 2020[1] arbeitete im Zeitraum vom 20. 3. 2020 bis zum 15. 4. 2020 jeder vierte von zu Hause aus. Die Dynamik der Ereignisse mag vielfach dazu geführt haben, dass nicht ausreichend Zeit vorhanden war für eine sorgfältige datenschutzrechtliche Ausgestaltung der Telearbeit. Unternehmen waren vorranging damit beschäftigt, die Arbeit der Mitarbeiter im Homeoffice faktisch zu organisieren. Die rechtlichen Rahmenbedingen werden vielfach im Sinne der Gewährleistung des weiteren Betriebsablaufes in den Hintergrund gestellt worden sein. Der vorliegende Beitrag knüpft an diese besondere Lage an und wirft ein Schlaglicht auf wesentliche Aspekte des Homeoffice aus der Perspektive des Datenschutzes.

I. Nutzung privater Geräte

Für die Arbeit im Homeoffice gilt: Grundsätzlich ist der Arbeitgeber verpflichtet, seinem Arbeitnehmer alle notwendigen Arbeitsmittel zur Verfügung zu stellen, folglich auch die entsprechende Hard- und Software.[2] Daneben besteht die Möglichkeit, die Nutzung von privaten Geräten zu gestatten. Diese zweite Alternative, auch unter dem Schlagwort „Bring Your Own Device (kurz: BYOD)“[3] thematisiert, birgt jedoch eine Vielzahl an Gefahren.

Auf einem privaten Gerät befinden sich denklogisch auch private Daten, die mit betrieblichen Daten in Berührung kommen können. Dadurch steigt die Wahrscheinlichkeit, dass es zu einer Vermischung von privaten und betrieblichen Daten kommt. Die Konsequenz kann sein, dass es beispielsweise zur Löschung von privaten Daten durch den Arbeitgeber kommt mit der Folge, dass sich dieser einem Schadensersatzanspruch ausgesetzt sieht.[4] Auch eine (versehentliche) Löschung betrieblicher Daten durch den Mitarbeiter ist denkbar. Daher sollte stets auf eine strikte Datentrennung geachtet werden mittels des Einsatzes entsprechender Programme.[5]

Des Weiteren besteht ein erhöhtes Sicherheitsrisiko, da es in der Eigenverantwortung des Telearbeiters liegt, für ein ausreichendes Schutzniveau seines Systems zu sorgen. Lebensnah betrachtet dürfte dabei davon auszugehen sein, dass nicht jeder Arbeitnehmer über das notwendige Wissen hierzu verfügt. Daher sollte der Mitarbeiter für das Thema entsprechend sensibilisiert werden, um einer Gefährdung von Betriebs- und Geschäftsgeheimnissen wirksam zu begegnen.[6] Bereits die vorgenannten Aspekte zeigen, dass die Gestattung der Nutzung von privaten Geräten wohl bedacht sein will. Auch wenn das Bedürfnis seitens des Angestellten nach mehr Flexibilität und das Interesse von Unternehmen nach Kostenreduzierung verständlich sind, ist doch im Zweifel von BYOD abzuraten.[7]

II. Remote-Zugriff

Die räumliche Trennung zwischen dem privaten Arbeitsplatz und dem betrieblichen Büro führt zu einer Einschränkung der ansonsten verfügbaren betrieblichen Ressourcen. Um ein effektives Arbeiten im Homeoffice zu eröffnen, sollte ein Zugriff aus der Ferne auf das Firmennetzwerk ermöglicht werden. Hierfür bietet sich die Einrichtung eines Virtuellen Privaten Netzwerks (VPN)[8]

---

* Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 20. 6. 2020.

1 Abrufbar unter: https://www.uni-mannheim.de/media/Einrichtungen/gip/Corona_Studie/2020-04-16_Schwerpunktbericht_Erwerbstaetigkeit.pdf.

2 *Müller*, Homeoffice in der arbeitsrechtlichen Praxis, 2019, Rn. 155.

3 Zum Begriff s. Wissenschaftliche Dienste des Deutschen Bundestags – Arbeitsrechtliche Aspekte der dienstlichen Nutzung privater Endgeräte, Punkt 4, abrufbar unter: https://www.bundestag.de/resource/blob/648356/20739233cb4f10a7512aa9d66436fe0a/WD-6-056-19-pdf-data.pdf; differenzierend nach Erscheinungsformen des BYOD *Helfrich*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V. Kapitel 2 Rn. 2 ff.

4 *Müller* (Fn. 2), Rn. 176.

5 So auch *Bartz/Grothenrath*, CCZ 2019, 184, 185; *Imping/Pohle*, K&R 2012, 470, 471.

6 Bundesamt für Sicherheit in der Informationstechnik (BSI) – Tipps für sicheres mobiles Arbeiten, Nr. 4, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf?__blob=publicationFile&v=4.

7 Eindringlich dahingehend appellierend Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) – Broschüre „Datenschutz: Plötzlich im Homeoffice – und nun?“, abrufbar unter: https://www.datenschutzzentrum.de/artikel/1322-Ploetzlich-im-Homeoffice-und-der-Datenschutz-Die-Landesbeauftragte-fuer-Datenschutz-Schleswig-Holstein-informiert.html.

8 Umfassend zum VPN insgesamt s. BSI, IT-Grundschutz-Kompendium, NET.3.3: VPN, 1 ff., abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html.

an.[9] Rechtlicher Anknüpfungspunkt sind die technischen und organisatorischen Maßnahmen (kurz: TOM) gem. Art. 32 Abs. 1 DSGVO. Danach ist die sichere Weitergabe von personenbezogenen Daten zu gewährleisten.[10] Dabei empfiehlt es sich, eine entspreche Regelung intern schriftlich zu fixieren, um jederzeit nachvollziehen zu können, wann und an welchen Stellen die Übergabe von schutzbedürftigen Daten stattgefunden hat.[11]

III. Technische Sicherheitsmaßnahmen

Der Verantwortliche muss jederzeit damit rechnen, dass er gegenüber der zuständigen Aufsichtsbehörde die Einhaltung der datenschutzrechtlichen Bestimmungen nachzuweisen hat. Dazu zählt auch, dass technische[12] Sicherheitsmaßnahmen zur Erfüllung der Verpflichtungen aus Art. 32 DSGVO ergriffen wurden. Bezugspunkt der Verpflichtungen sind sowohl die Hard- als auch die Software.[13] Die Vorschrift eröffnet einen relativ weiten Gestaltungsspielraum aufgrund der in ihr enthaltenen unbestimmten Rechtsgriffe.[14] Um für die Ausgestaltung eine Orientierung zu bieten, haben die Datenschutzbehörden der Länder ein „Standard-Datenschutzmodel (SDM)"[15] geschaffen.[16] Diese „Methode (…) soll sicherstellen, dass eine einheitliche Datenschutz-Beratungs- und Prüfpraxis in Bezug insbesondere zu den technisch-organisatorischen Maßnahmen der DSGVO erreicht werden kann.".[17]

In Bezug auf die IT-Systeme sollte darauf geachtet werden, dass sie angemessen konfiguriert und gehärtet[18] sind. Zudem sollten notwendige Patches eingespielt,[19] eine Antivirus-Software verwendet[20] und eine Firewall installiert werden.[21] Mobile Geräte und Datenträger sind nach Möglichkeit zu verschlüsseln.[22] Eine Datensicherung am heimischen Arbeitsplatz sollte vermieden werden.[23]

IV. Verhaltensregeln

Es liegt auf der Hand, dass nicht jeder private Arbeitsplatz dem anderen gleicht, sondern die Umstände, unter denen im Homeoffice gearbeitet wird, ganz unterschiedlich sind. Die Umsetzung eines betrieblichen Raumkonzepts zur Schaffung vergleichbarer, sicherer Umgebungen ist nicht möglich. Unternehmen sollten daher darauf achten, dieses strukturelle Defizit durch ausgleichende Verhaltensregeln zu kompensieren. Die rechtliche Verpflichtung hierzu folgt aus Art. 32 DSGVO. Danach sind technische und organisatorische Maßnahmen zu ergreifen, um insbesondere auch „die Vertraulichkeit (…) der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen" (Abs. 1 lit. b). Der Begriff „Vertraulichkeit" meint den „Schutz vor unbefugter Preisgabe von Informationen und dass vertrauliche Daten und Informationen ausschließlich Befugten in der zulässigen Weise zugänglich sind".[24] Die Vorschrift adressiert in Bezug auf den „persönlichen" Anwendungsbereich lediglich „Systeme und Dienste". Es fallen darunter aber auch natürliche Personen, die mit den Systemen und Diensten arbeiten.[25]

Auch wenn – wie zuvor beschrieben – ein jeder privater Arbeitsplatz seine Besonderheiten aufweist, so lassen sich dennoch bestimmte Maßnahmen identifizieren, die der Sicherheit allgemein zuträglich sind.[26] So sollte für die Arbeit ein eigener Raum genutzt werden. Falls eine solche Möglichkeit nicht vorhanden ist, sollte der Rechner zumindest derart platziert werden, dass der Bildschirm nicht ohne Weiteres von Dritten eingesehen werden kann oder es sind Sichtschutzfolien[27] zu verwenden. Beim Verlassen des Raums ist anzuraten, die Bildschirmsperre zu aktivieren und die Tür zu verschließen.[28] Beim Führen von dienstlichen Telefonaten ist darauf zu achten, dass die Fester geschlossen sind und zusätzlich darauf Wert gelegt wird, dass Haushaltsmitglieder keine Kenntnis vom Inhalt des Gesprächs erlangen.[29] Physische Unterlagen sind nach der Verwendung in abschließbaren Behältnissen aufzubewahren.[30] Eine Entsorgung von betrieblichen Unterlagen in Papierform hat nicht im privaten Hausmüll zu erfolgen, sondern fachgerecht am regulären Arbeitsplatz. Zur Vermeidung der Ansammlung von gedruckten Dokumenten empfiehlt es sich, nach Möglichkeit keine Dienstpapiere mit nach Hause zu nehmen.[31]

---

9 In Abgrenzung zur VPN-Lösung kommt das Cloud-Computing in Betracht, welches aber mit erheblichen Risiken verbunden ist, vgl. dazu *Spies*, in: v. d. Bussche/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 7. Cloud-Computing, Rn. 1 ff.

10 Für einzelne Sicherungsmaßnahmen s. *Schmieder*, in: Forgó/Helfrich/Schneider (Fn. 3), Teil XII. Kapitel 2 Rn. 69 ff.

11 *Müller*, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, E. II. 2., Nr. 24.

12 Zur Abgrenzung der technischen von den organisatorischen Maßnahmen *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, E. II. 2. b) Rn. 825.

13 *Jandt*, in: Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, B. Art. 32 Rn. 22 im Zusammenhang mit Art. 32 Abs. 1 lit. b DSGVO.

14 Dies zeigt sich beispielsweise daran, dass nach dem Wortlaut des Art. 32 DSGVO die Maßnahmen „geeignet" sein müssen (Abs. 1, 1. Hs.) oder aber dass die Maßnahmen „unter anderem" bestimmte Aspekte einschließen (Abs. 1, Einleitung 2. Hs.). Aufgrund der letztgenannten Formulierung wird hier auch von einem „unvollständigen Maßnahmenkatalog" gesprochen, vgl. *Jandt*, in: Kühling/Buchner (Fn. 13), B. Art. 32 Rn. 14.

15 Die aktuelle Version 2.0b wurde von der 99. Konferenz der Datenschutzbehörden des Bundes und der Länder am 17. 4. 2020 beschlossen und ist abrufbar unter: https://www.datenschutzzentrum.de/sdm/.

16 *Schultze-Melling*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, EU-Datenschutzgrundverordnung, Art. 32 Rn. 20.

17 Vgl. die Einleitung unter https://www.datenschutzzentrum.de/sdm/.

18 Zum Begriff der „Härtung" s. die Definition des Instituts für Kooperative Systeme an der FernUniversität Hagen unter https://its.iks-hagen.de/index.php/leistungen/systemhaertung.

19 Ausführlich hierzu BSI, IT-Grundschutz-Kompendium (Fn. 8), OPS. 1.1.3: Patch- und Änderungsmanagement, 1 ff.

20 BSI, IT-Grundschutz-Kompendium (Fn. 8), OPS. 1.1.4: Schutz vor Schadprogrammen, 3 ff.

21 Benutzt der Anwender bei seiner Arbeit ein privates Gerät ist aus Sicht des Verantwortlichen zu bedenken, dass die Umsetzung der technischen Sicherheitsmaßnahmen an diesen delegiert werden und sich damit der eigenen Einflusssphäre entziehen; zu diesem Risikofaktor *Dury/Leibold*, ZD-Aktuell 2020, 04405, Nr. 4. BYOD (Bring your own device). Wird dagegen ein dienstlicher Rechner benutzt, sollte „keine private Hardware angeschlossen werden, um die Wahrscheinlichkeit des Einschleusens von Schadsoftware zu verringern", ULD – Broschüre „Datenschutz: Plötzlich im Homeoffice – und nun?" (Fn. 7), 3.

22 Ausführlich hierzu *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, Teil A. § 2 III. 5.

23 BSI – Tipps für sicheres mobiles Arbeiten (Fn. 6), Nr. 8.

24 BSI, IT-Grundschutz-Kompendium (Fn. 8), Glossar, 12; s. hierzu auch den Datenschutzgrundsatz in Art. 5 Abs. 1 lit. f DSGVO.

25 *Hansen*, in: Simitis/Hornung/Spieker gen. Döhmann, Datenschutzrecht, 2019, VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung), Kapitel IV Abschnitt 2 Art. 32 Rn. 37.

26 Ein gesetzlicher Katalog der abschließend festlegt, welche Maßnahmen die Sicherheit gewährleisten, existiert nicht. Es liegt in der Verantwortung der zuständigen Person, Regelungen zu treffen, die für ein ausreichendes Schutzniveau sorgen. Die DSGVO eröffnet insoweit einen Ermessensspielraum, indem sie in Art. 5 Abs. 1 lit. f von „angemessener" Sicherheit und in Art. 32 Abs. 1 lit. b von „Fähigkeit" spricht; vgl. dazu auch *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung), Art. 32 Rn. 14.

27 *Gilga*, ZD-Aktuell 2020, 07113.

28 BSI – Tipps für sicheres mobiles Arbeiten (Fn. 6), Nr. 3.

29 *Granetzny/Markworth*, in: Hohenstatt/Sittard, Arbeitsrecht in Zeiten von Corona, 2020, IX. 34.

30 BSI – Tipps für sicheres mobiles Arbeiten (Fn. 6), Nr. 3.

31 *Granetzny/Markworth*, in: Hohenstatt/Sittard (Fn. 29), IX. 34.

V. Homeoffice-Richtlinie

Arbeiten Mitarbeiter im Homeoffice, so bleibt der Arbeitgeber verantwortlich i. S. d. Art. 24 DSGVO für die Datenverarbeitung und deren Sicherheit mit der Folge, die Sicherheit der Datenverarbeitung nach Art. 32 DSGVO gewährleisten zu müssen. Der Arbeitgeber hat jedoch bei Homeoffice-Tätigkeiten keine oder nur bedingte Kontroll- und Zugriffsmöglichkeiten im Hinblick auf die Datenverarbeitung. Zudem ist die Einflussnahme- und Missbrauchsgefahr durch Dritte erhöht.[32] Als organisatorische Maßnahme i. S. d. Art. 32 DSGVO sollte die Arbeit im Homeoffice daher zwingend durch eine geeignete Richtlinie geregelt werden, um im Zweifel belegen zu können, entsprechende Maßnahmen getroffen zu haben.

Vor der Erstellung einer Homeoffice-Richtlinie ist zu prüfen, ob die zu leistende Arbeit überhaupt geeignet ist für die Auslagerung ins private Büro. Entscheidungskriterien sind dabei bezüglich des Arbeitnehmers in persönlicher Hinsicht die Vertrauenswürdigkeit, seine Fähigkeiten an sich und die Frage nach seiner Kompetenz in Sachen Datenschutz.[33] Objektiv ist von Relevanz, ob eine Präsenz im Betrieb entbehrlich ist. Daneben ist danach zu differenzieren, ob überhaupt personenbezogene Daten verarbeitet werden. In Abhängigkeit vom Einzelfall sind anschließend die Inhalte der Richtlinie auszuarbeiten. Typische Themen sind beispielsweise die Nutzung privater Geräte[34] oder Verhaltensregeln.[35] Aber auch Fragen nach dem Recht zur Betretung von privaten Wohnungen für Kontrollmaßnahmen oder Pflichten bei der Beendigung des Homeoffice werden häufig geregelt.[36]

VI. Meldepflichten bei Datenschutzverletzungen

Trotz aller Vorsichtsmaßnahmen kann niemals ganz ausgeschlossen werden, dass es zu einer (unbeabsichtigten) Datenschutzverletzung[37] kommt. Tritt eine solche Situation ein, hat der Verantwortliche gegebenenfalls bestimmte Meldepflichten zu erfüllen. In Abhängigkeit von der wahrscheinlichen Auswirkung der Datenschutzverletzung ist danach zu differenzieren, ob lediglich die Aufsichtsbehörde oder darüber hinaus auch der Betroffene zu informieren ist.

Art. 33 Abs. 1 DSGVO statuiert einleitend eine generelle Meldepflicht gegenüber der Aufsichtsbehörde. Ausnahmsweise muss der offiziellen Stelle jedoch keine Mitteilung gemacht werden für den Fall, „dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt". Nach dem Wortlaut ist dabei also eine Prognoseentscheidung zu treffen.[38] Eine solche verlangt ebenfalls Art. 34 Abs. 1 DSGVO, wenn es um eine etwaige Benachrichtigung von Betroffenen geht. Der Unterschied zu Art. 33 liegt darin begründet, dass hier ein gesteigertes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zu erwarten sein muss („hohes Risiko").

Neben der Information der Adressaten verpflichtet Art. 33 DSGVO den Verantwortlichen zusätzlich zur Dokumentation des Vorfalls (Abs. 5).[39] Auch wenn der Wortlaut von Art. 34 DSGVO keine Pflicht zur Dokumentation vorschreibt, sollte dennoch ein Festhalten des Sachverhalts erfolgen, da sich zumindest aus der allgemeinen Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO eine Nachweispflicht ergibt. Sämtliche Verpflichtungen sind zudem bewehrt und können empfindlich sanktioniert werden.[40]

VII. Auswirkungen auf das Verarbeitungsverzeichnis

Tätigkeiten im Homeoffice können gegebenenfalls auf die Inhalte des Verarbeitungsverzeichnisses[41] ausstrahlen. Gemäß Art. 30 Abs. 1 S. 2 lit. g DSGVO hat der Verantwortliche eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO vorzunehmen.[42] Sofern entsprechende Arbeitsplätze dort noch nicht berücksichtigt sein sollten, ist anzuraten, dies nachzuholen. Auch der – zwar nicht zu empfehlende[43] – Umstand, dass ein privater PC genutzt wird, sollte entsprechend in das Verarbeitungsverzeichnis[44] aufgenommen werden.

VIII. Auswirkungen auf Kontrollbefugnisse

Die Arbeit im Homeoffice wirkt sich auch auf die Kontrollbefugnisse aus, so im Hinblick auf solche der Aufsichtsbehörden nach Art. 58 DSGVO. Art. 58 Abs. 1 lit. f DSGVO begründet zwar ein Betretungsrecht der Aufsichtsbehörde von Grundstücken und Geschäftsräumen zu Kontrollzwecken.[45] Diese Befugnis erfährt aber bei Arbeit im Homeoffice insbesondere durch die Unverletzlichkeit der Wohnung nach Art. 13 GG sowie des Rechts des Arbeitnehmers auf Privatsphäre Einschränkungen oder kann ggf. sogar gänzlich ausgeschlossen sein.[46]

Gleiches gilt für die Zugriffs- und Kontrollrechte des Datenschutzbeauftragten. Dieser wird seine Befugnisse nicht ohne das Einverständnis des Mitarbeiters, dem das Hausrecht zusteht, ausüben können. Auch dem Arbeitgeber fehlt in der Wohnung des Arbeitnehmers mangels Zutrittsrechten die Verfügungsgewalt.[47] Daher sollte ein aus Sicht des Arbeitgebers notwendiges Zutrittsrecht vertraglich vereinbart werden, wobei auch das Einverständnis

32 *Müller* (Fn. 2), Rn. 192.
33 *Bergt*, in: Koreng/Lachenmann (Fn. 11), D. III. 2. Nr. 1.
34 S. hierzu oben unter I.
35 S. zuvor unter IV.
36 Zum Vorgenannten insgesamt *Bergt*, in: Koreng/Lachenmann (Fn. 11), D. III. 2.
37 Zum Begriff s. die Legaldefinition in Art. 4 Nr. 12 DSGVO.
38 Für die Bewertung kann auf die von der Artikel-29-Datenschutzgruppe entwickelten Kriterien zurückgegriffen werden, s. *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 33 Rn. 11.
39 Eine bestimmte Form wird dabei nicht vorgeschrieben, vgl. *v. d. Bussche*, in: v. d. Bussche/Voigt (Fn. 9), Teil 2. Kapitel 7 Rn. 20.
40 Hinsichtlich der Art. 33 und Art. 34 DSGVO folgt dies aus Art. 83 Abs. 4 lit. a DSGVO und für Art. 5 Abs. 2 DSGVO ergibt sich die Sanktionsmöglichkeit aus Art. 83 Abs. 5 lit. a DSGVO.
41 Zum Begriff der „Verarbeitungstätigkeit" s. ausführlich *Spoerr*, in: Wolff/Brink, BeckOK Datenschutzrecht, Datenschutz-Grundverordnung, 31. Edition (Stand: 1. 2. 2020), Art. 30 Rn. 6.
42 Der Wortlaut von Art. 30 Abs. 1 S. 2 lit. g DSGVO lässt zwar vermuten, dass eine solche Verpflichtung nicht generell besteht wenn er davon spricht, dass die TOM „wenn möglich" aufzunehmen seien. Dagegen spricht jedoch, dass es sich bei Art. 32 Abs. 1 DSGVO um eine generelle Pflicht handelt und insofern eine Beschreibung stets möglich sein sollte. So auch *Bertermann*, in: Ehmann/Selmayr (Fn. 38), Art. 30 Rn. 15. Hinzukommt, dass der Sinn und Zweck von Art. 30 Abs. 1 S. 2 lit. g DSGVO darin besteht der Aufsichtsbehörde nachweisen zu können, dass bei der Verarbeitung von personenbezogenen Daten mittels bestimmter TOM für ein angemessenes Schutzniveau gesorgt wurde, *Schultze-Melling*, in: Taeger/Gabel (Fn. 16), Art. 30 Rn. 19. Auch vor diesem Hintergrund empfiehlt es sich, das Arbeiten aus dem Homeoffice heraus in das Verzeichnis aufzunehmen.
43 S. o. unter I.
44 Ein empfehlenswertes Muster eines Verarbeitungsverzeichnisses stellt die Datenschutzschutzkonferenz von Bund und Ländern zur Verfügung, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf; dazu *Spoerr*, in: Wolff/Brink (Fn. 41), Art. 30 Rn. 9.
45 *Weichert*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 58 Rn. 20.
46 *Ziebarth*, in: Sydow (Fn. 26), Art. 58 Rn. 33.
47 *Conrad/Treeger*, in: Auer-Reinsdorff/Conrad (Fn. 22), Teil F. § 34 Rn. 292.

der mit ihm in häuslicher Gemeinschaft zusammenlebenden Personen umfasst sein muss und der Datenschutzbeauftragte einzubeziehen ist.[48]

IX. Auftragsverarbeitung

Sofern jemand als Auftragsverarbeiter i. S. d. Art. 28 DSGVO wirkt, ist vor dem Einsatz von Mitarbeitern im Homeoffice zwingend zu prüfen, ob der mit dem Verantwortlichen geschlossene Auftragsverarbeitungsvertrag eine derartige Tätigkeit der eigenen Mitarbeiter und unter welchen Voraussetzungen gestattet.[49] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit empfiehlt dabei in seinem Muster zur Auftragsverarbeitung eine „vorherige ausdrückliche Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann".[50]

X. Fazit

Datenschutz endete auch schon vor dem Ausbruch der Corona-Krise nicht an der Haustür. Jedoch wird – bedingt durch die Krise – vielen Unternehmen und Unternehmern, die „Umzüge" ins Homeoffice bewerkstelligen mussten, nun erst aufgezeigt worden sein, dass hier nicht nur logistische Herausforderungen warteten und warten, sondern auch rechtliche. Neben dem geplanten Gesetz zur Etablierung eines Anspruchs auf Homeoffice[51] könnten Unternehmen im Übrigen auch weiterhin ein eigenes und gesteigertes Interesse daran haben, nach dem Abklingen der Krise die Möglichkeit für Mitarbeiter, (teilweise) im Homeoffice zu arbeiten, beizubehalten. Man mag es den Verantwortlichen nachsehen, wenn sie die rechtlichen Themen, die mit der Arbeit im Homeoffice verbunden sind, ggf. vernachlässigt haben, um zunächst den Betrieb am Laufen zu halten. (Bewusste) Versäumnisse sollten aber umgehend nachgeholt werden. Denn es ist ebenfalls zu vermuten, dass die Aufsichtsbehörden den verstärkten Wechsel ins Homeoffice aufarbeiten werden.[52] Verantwortliche sind daher gut beraten, sich dem Thema Datenschutz im Homeoffice eingehend zu widmen.

48 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit – „Telearbeit und Mobiles Arbeiten", S. 17, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html.

49 Bereits der Wortlaut von Art. 28 DSGVO gebietet eine entsprechende Vorgehensweise, da er schon zu Beginn festlegt, dass die Auftragsverarbeitung hinreichend Garantien dafür bieten muss, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

50 Abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html., dort § 3 Abs. 9.

51 https://www.handelsblatt.com/politik/deutschland/kein-rechtsanspruch-arbeitgeber-veraergert-ueber-geplantes-recht-auf-homeoffice/25774730.html?ticket=ST-1822245-udtEIBeVWmK4 YV3wpRZp-ap1; https://www.faz.net/aktuell/finanzen/corona-krise-hubertus-heil-will-home-office-per-gesetz-16742512.html.

52 Für eine mögliche Zunahme von Datenschutzgeldbußen im Allgemeinen *Behr/Tannen*, CCZ 2020, 120 ff.

Tristan Radtke, Freiburg i. Br.*

Datengestützte Wahlwerbung wie Microtargeting aus datenschutzrechtlicher Perspektive

Sei es im Bundestagswahlkampf 2017, im Europawahlkampf 2019 oder in den jüngsten Landtagswahlkämpfen: Die deutschen Parteien setzen vermehrt auf einen datengestützten Online- und Haustür-Wahlkampf und dabei auch auf die gezielte Wähleransprache (Microtargeting). Der Beitrag gibt einen Überblick über die Erscheinungsformen datengestützter Wahlwerbung und die datenschutzrechtlichen Implikationen.

I. Der Trend zum datengestützten Wahlkampf

Neben den noch immer nicht vollständig aufgeklärten,[1] zwischenzeitlich durch Netflix verfilmten Vorgängen rund um Cambridge Analytica[2] und den Erfolg von Persönlichkeitsanalysen im Wahlkampf auf Grundlage von Facebook-Profil-Daten, gibt es ihn tatsächlich in den USA: den datengestützten Wahlkampf. Über soziale Netzwerke, Online-Kampagnen, per Telefon und mittels datengestützten Haustürwahlkampfs werden Wähler für einen effizienteren[3] Wahlkampf möglichst zielgerichtet angesprochen[4] – das sog. (politische) Microtargeting.[5]

Auch hierzulande ist der datengestützte Wahlkampf mit seinen unterschiedlichen Facetten angekommen, wenngleich das europäische und deutsche Datenschutzrecht regelmäßig die Ansprache kleiner Gruppen statt einzelner Wähler notwendig werden lässt.

* Der Beitrag wurde anlässlich eines Vortrags des Verfassers im Rahmen der Veranstaltung „Von Brexit bis Bundestagswahl: Wie Microtargeting den Wahlkampf revolutioniert" am 30. 10. 2019 in Passau verfasst und basiert auch auf den dort geschilderten Ausführungen zum Wahlkampf. Internet-Verweise in diesem Beitrag wurden zuletzt abgerufen am 2. 6. 2020. Der Verfasser forscht zur Vornahme einer Systematisierung der Kriterien der gemeinsamen Verantwortlichkeit im Rahmen seines Dissertationsvorhabens. Mehr über den Autor erfahren Sie auf S. VIII.

1 Etwa *Confessore/Hakim*, https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html; *Reinbold/Schnack*, https://www.spiegel.de/netzwelt/netzpolitik/donald-trump-und-die-daten-ingenieure-endlich-eine-erklaerung-mit-der-alles-sinn-ergibt-a-1124439.html.

2 S. die aktualisierte Version des ursprünglichen Artikels *Grassegger/Krogerus*, https://www.tagesanzeiger.ch/ausland/europa/Ich-habe-nur-gezeigt-dass-es-die-Bombe-gibt/story/17474918. Zur rechtlichen Bewertung *Söbbing*, InTeR 2018, 182.

3 *Jungherr/Schoen*, Das Internet in Wahlkämpfen, 2013, S. 123.

4 Dazu ausführlich *Kolany-Raiser/Radtke*, Microtargeting – Gezielte Wähleransprache im Wahlkampf, in: Hoeren (Hrsg.), Phänomene des Big-Data-Zeitalters, 2019, S. 88 - 91.

5 *Barbu*, Advertising, Microtargeting and Social Media, Social and Behavorial Sciences 2014, S. 44, 45 und ursprünglich *Agan*, Silent Marketing: Microtargeting, 2007.