FELIX SUWELACK

Datenschutzrechtliche Vorgaben für Homeoffice und Remote Work

Nachhaltige und rechtssichere Umstellung – New Work. New Normal. New Problems?

Mobile Office
Bring Your Own Device
Konferenzsoftware
Homeoffice-Vereinbarung
Arbeitnehmerkontrolle

■ Die Corona-Pandemie hat viele Unternehmen zur Umstellung auf Homeoffice gezwungen, auch wenn die technischen und organisatorischen Voraussetzungen hierfür noch nicht gegeben waren. Dieser Beitrag zeigt, welche arbeits- und datenschutzrechtlichen Herausforderungen sich stellen, wenn Tätigkeiten der Arbeitnehmer ins Homeoffice verlagert werden sollen. Er gibt den Arbeitgebern zudem einen Leitfaden an die Hand, um diese Umstellung nachhaltig und rechtssicher zu gestalten oder künftig in Krisenfällen auch kurzfristig entsprechende Maßnahmen treffen zu können.

■ The Corona pandemic has forced many companies to switch to home office, even if the technical and organizational requirements for this were not yet established. This article will show which labor and data protection law challenges are present when the employee's work shall be shifted to home office. Furthermore, it will provide the employers with a manual for implementing a transition which is sustainable and legally certain or for implementing such respective measures in events of crises on short notice.
Lesedauer: 24 Minuten

I. Einleitung

Bei der plötzlichen pandemiebedingten Umstellung auf Homeoffice mussten arbeits- und datenschutzrechtliche Überlegungen häufig hintanstehen. Und auch wenn die DS-GVO keine Ausnahmen für derartige Situationen vorsieht, haben die Datenschutzbehörden zunächst versprochen, eine gewisse Nachsicht bei pandemiebedingten Datenschutzverstößen walten zu lassen.[1]

Nachdem die Unternehmen nun mehrere Monate Zeit hatten, sich auf die „neue Normalität" im Umgang mit dem Corona-Virus einzustellen, dürfte kein Anlass mehr für diese Nachsicht bestehen.[2] Dieser Beitrag gewährt einen Überblick darüber, welche Maßnahmen notwendig sind, um eine nachhaltige und rechtssichere Umstellung von Arbeitstätigkeiten auf Homeoffice zu gewährleisten. Er skizziert, welche arbeitsrechtlichen Rahmenbedingungen hierbei gelten (II.), und stellt die einschlägigen datenschutzrechtlichen Vorgaben dar (III.).

Hiervon ausgehend wird gezeigt, welche Maßnahmen erforderlich sind, um eine datenschutzkonforme Gestaltung der Homeoffice-Tätigkeit zu gewährleisten (IV.). Abschließend werden die zu treffenden Maßnahmen in einer kurzen Checkliste zusammengefasst, anhand derer etwaiger Handlungsbedarf überprüft und erkannt werden kann (V.).

II. Arbeitsrechtliche Rahmenbedingungen

1. Einführung von Homeoffice

Ohne wirksame Rechtsgrundlage besteht weder ein Recht noch eine Pflicht des Arbeitnehmers, dienstliche Tätigkeiten im Homeoffice zu verrichten.[3] Da viele Arbeitnehmer ein großes Interesse an Tätigkeiten im Homeoffice haben,[4] dürfte insoweit meist der Abschluss einvernehmlicher Regelungen gelingen, die zudem ad hoc oder konkludent möglich sind.[5] Darüber hinaus kommt jedoch auch der Abschluss einer Betriebsvereinbarung oder eine einseitige Anordnung des Arbeitgebers in Betracht.

a) Betriebsvereinbarung

Wirksame Betriebsvereinbarungen gelten unmittelbar und zwingend, ohne Bestandteil des jeweiligen Arbeitsvertrags zu werden. Allerdings müssen sich die jeweiligen Vereinbarungen in den Grenzen der Gesetzes- und Tarifsperren nach §§ 77 Abs. 3, 87 Abs. 1 BetrVG bewegen und gem. § 75 BetrVG den Grundsätzen von Recht und Billigkeit entsprechen. Sie müssen insbesondere die Persönlichkeitsrechte der Arbeitnehmer wahren und verhältnismäßig sein.[6]

1 *LfDI Rheinland-Pfalz*, Gesundheitsnot kennt Datenschutzgebot, abrufbar unter: https://verfassungsblog.de/gesundheitsnot-kennt-datenschutzgebot/; *Wünschelbaum*, NZA 2020, 612.
2 *Wünschelbaum*, NZA 2020, 612.
3 *Günther/Böglmüller*, ArbRAktuell 2020, 186; *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (474 ff.); *Benkert*, NJW-Spezial 2019, 306; *Günther/Böglmüller*, ArbRAktuell 2020, 186.
4 *Hofmann/Piele/Piele*, Arbeiten in der Corona Pandemie – Auf dem Weg zum New Normal, abrufbar unter: http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-5934454.pdf.
5 *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (474).
6 *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (477); *Wulff*, in: Helm/Bundschuh/Wulff, Arbeitsrechtliche Beratungspraxis in Krisenzeiten, 2020, § 8 Rn. 20.

Vereinbarungen, welche die Arbeitnehmer ohne deren Zustimmung verpflichten, ihre Arbeit nunmehr im Homeoffice zu verrichten, berühren jedenfalls mittelbar ihre private Lebensführung und bedingen einen Eingriff in Art. 13 Abs. 1 GG.[7] Ohne besondere Veranlassung und ohne zeitliche Beschränkung dürften sie daher unwirksam sein.[8] Umgekehrtes gilt jedoch wohl für eine partielle oder temporäre Versetzung der Arbeitnehmer ins Homeoffice zum Infektionsschutz in Krisenzeiten.[9] Hierzu müssen die Betriebsparteien jedoch eine Regelung finden, die die Voraussetzungen und Wirkungen so konkret wie möglich fasst und Raum zur Berücksichtigung von Interessen einzelner Arbeitnehmer lässt.[10]

Ein Recht der Arbeitnehmer auf Homeoffice kann dagegen ohne weiteres durch eine Betriebsvereinbarung statuiert werden.

b) Einseitige Durchsetzung

Darüber hinaus wird diskutiert, ob der Arbeitgeber durch Ausübung seines Direktionsrechts nach § 106 GewO berechtigt ist, einseitig eine Arbeit im Homeoffice anzuweisen. Zwar ging die Rechtsprechung bislang davon aus, dass eine Versetzung ins Homeoffice nicht von diesem Direktionsrecht gedeckt sei.[11] Allerdings wird in der rechtswissenschaftlichen Literatur inzwischen überwiegend die Auffassung vertreten, dass sich die bisher getroffenen Wertungen nicht auf pandemiebedingte Krisensituationen übertragen ließen und jedenfalls eine vorübergehende Versetzung zur Abwehr von Infektionsgefahren in Krisenzeiten grundsätzlich zulässig sei.[12]

Ein Recht des Arbeitnehmers auf Homeoffice ohne Zustimmung des Arbeitgebers besteht nicht.[13] Allenfalls in absoluten Ausnahmesituationen kann der Arbeitgeber auf Grund seiner Rücksichtnahmepflicht gehalten sein, einer Tätigkeit im Homeoffice zuzustimmen. Denkbar wäre dies etwa, wenn der Arbeitnehmer zu einer sog. Risikogruppe gehört, der Arbeitgeber gängige Hygienestandards in einer akuten pandemiebedingten Krisensituation nicht einhalten kann und die Verrichtung der geschuldeten Tätigkeit im Homeoffice möglich ist.[14]

2. Arbeitsschutzrechtliche Pflichten bei Umstellung auf Homeoffice

Da die Möglichkeiten zur Durchsetzung von Arbeitsschutzmaßnahmen im Homeoffice beschränkt sind, beschränken sich die Arbeitsschutzpflichten des Arbeitgebers im Wesentlichen auf Organisations- und Hinweispflichten.[15] Besondere Beachtung erfordern insoweit die Gefährdungsbeurteilung nach § 5 ArbSchG und die Unterweisungspflichten nach § 12 ArbSchG. Insoweit wird insbesondere empfohlen, den Arbeitnehmer über Bewegungsmangel, Ergonomie sowie psychische Belastungen im Zusammenhang mit der Entgrenzung von Arbeits- und Freizeit aufzuklären und auf die Vorgaben des Arbeitszeitrechts hinzuweisen.[16]

III. Datenschutzrechtliche Rahmenbedingungen für Arbeitstätigkeiten im Homeoffice

1. Datenschutz/Datensicherheit beim Datenumgang durch den Arbeitnehmer

Tätigkeiten im Homeoffice unterliegen im Ausgangspunkt keinen datenschutzrechtlichen Besonderheiten. Der Arbeitnehmer handelt beim betrieblichen Umgang mit personenbezogenen Daten weiterhin auf Weisung des Arbeitgebers gem. Art. 29 DS-GVO. Der Arbeitgeber bleibt datenschutzrechtlicher Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO.[17] Für die materiell-rechtliche Betrachtung der Datenverarbeitung spielt es keine Rolle, wo sie erfolgt. Durch eine Umstellung auf eine Tätigkeit im Homeoffice ändert sich daher weder die Rechtsgrundlage noch der erlaubte Umfang der Datenverarbeitung.[18]

Da die Arbeitnehmer beim Umgang mit den personenbezogenen Daten im Homeoffice dem räumlichen Kontroll- und Einflussbereich des Arbeitgebers entzogen sind, verdienen allerdings die erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO besonderes Augenmerk.[19] Der Arbeitgeber muss bei der Umstellung auf Homeoffice seinen datenschutzrechtlichen Organisationspflichten in besonderer Weise gerecht werden, um keine Haftung zu riskieren.[20] Er muss gewährleisten, dass die Grundsätze der Informationssicherheit eingehalten werden, und daher insbesondere die Vertraulichkeit, die Integrität und die Verfügbarkeit der jeweiligen Daten sicherstellen.[21]

Eine Gewährleistung der Vertraulichkeit setzt voraus, dass die betroffenen Daten ausschließlich den zur Datenverarbeitung Befugten in der jeweils zulässigen Weise und dem jeweils zulässigen Umfang zugänglich und vor unbefugter Kenntnisnahme geschützt sind. Auch wenn die DS-GVO hierzu keine konkreten Vorgaben macht und stets eine Risikobetrachtung im Einzelfall notwendig ist, lassen sich bestimmte Standards umreißen, die auch bei einer Tätigkeit der Arbeitnehmer im Homeoffice eingehalten werden sollten:[22]

- Durch eine Zugangskontrolle ist sicherzustellen, dass lediglich Befugte Zugang zu Datenverarbeitungssystemen und Datenträgern sowie physischen Unterlagen haben, um eine unbefugte Einwirkung oder Kenntnisnahme zu verhindern („Ob" der Zugangsberechtigung).
- Es ist eine Zugriffskontrolle erforderlich, die den Zugriff der berechtigten Personen auf diejenigen Daten beschränkt, die von ihrer Berechtigung umfasst sind („Wie" der Zugangsberechtigung und Prinzip der geringstmöglichen Rechtevergabe).
- Durch eine Weitergabekontrolle ist zu gewährleisten, dass personenbezogene Daten nicht an unbefugte Dritte übermittelt, auf unsichere Speicherorte übertragen oder in sonstiger Weise der Kontrolle des Verantwortlichen entzogen werden.
- Durch eine Verschlüsselung von Daten auf Datenträgern oder bei Datentransfers ist sicherzustellen, dass keine unbefugten Zugriffsmöglichkeiten von außen bestehen.

Die Gewährleistung von Datenintegrität erfordert Maßnahmen zur Bewahrung der Vollständigkeit, Richtigkeit und Authentizität der erfassten Daten.[23] Es ist sicherzustellen, dass die entspre-

7 *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (477).
8 *Wulff* (o. Fußn. 6), Rn. 20.
9 *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (477); *Fuhlrott/Fischer*, NZA 2020, 345 (349).
10 *Hülsemann*, ArbRAktuell 2017, 483; *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (477).
11 *LAG Berlin-Brandenburg* U. v. 14.11.2018 – 17 Sa 562/18.
12 *Sagan/Brockfeld*, NJW 2020, 1112 (1114); *Günther/Böglmüller*, ArbRAktuell 2020, 186; *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (477); *Fuhlrott/Fischer*, NZA 2020, 345 (349).
13 *Günther/Böglmüller*, ArbRAktuell 2020, 186 (187); *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (478).
14 *Sagan/Brockfeld*, NJW 2020, 1112 (1114); *Günther/Böglmüller*, ArbRAktuell 2020, 186 (187); *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (478).
15 *Günther/Böglmüller*, ArbRAktuell 2020, 186 (187); *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (479 f.).
16 *Krieger/Rudnik/Povedano Peramato*, NZA 2020, 473 (479 f.), mwN.
17 *Hoppe*, in: Kramer, IT-Arbeitsrecht, 2. Aufl. 2019, Teil B. Rn. 642; *Dury/Leibold*, ZD-Aktuell 2020, 04405.
18 *Wünschelbaum*, NZA 2020, 612 (614).
19 *Hoppe* (o. Fußn. 17), Rn. 644; *Müller*, in: Müller, Homeoffice in der arbeitsrechtlichen Praxis, 1. Aufl. 2019, § 3 Rn. 192.
20 *Dury/Leibold*, ZD-Aktuell 2020, 04405; *Hoppe* (o. Fußn. 17), Rn. 642.
21 Vgl. *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, DSGVO, Art. 32 Rn. 38; *Hoppe* (o. Fußn. 17), Rn. 689.
22 Vgl. hierzu *Laue*, in: Spindler/Schuster, Recht der Elektronischen Medien, 4. Aufl. 2019, DS-GVO, Art. 32 Rn. 14; *Hansen* (o. Fußn. 21), Rn. 39; *Hofmann*, in: Nägele/Apel, Beck'sche Online-Formulare IT- und Datenrecht, 3. Ed. 2020, Form. 2.19 Rn. 18.
23 *Martini*, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, Art. 32 Rn. 36; *Laue* (o. Fußn. 22), Rn. 14; *Hansen* (o. Fußn. 21), Rn. 40

chenden Daten nicht durch Fehlfunktionen im System oder durch äußere Zugriffe beschädigt werden bzw. im Falle einer Beschädigung wieder vollständig hergestellt werden können und dass keine unerlaubte manuelle Veränderung der Daten vorgenommen wird. Dies kann insbesondere durch eine Eingabekontrolle (Protokollierung vorgenommener Veränderungen) sowie durch regelmäßige Backups und Synchronisationen mit den Unternehmensservern gewährleistet werden.[24]

Eine hinreichende Datenverfügbarkeit setzt voraus, dass die Daten von den Berechtigten stets wie vorgesehen genutzt werden können.[25] Der Verantwortliche muss jederzeit auf die Daten zugreifen und seinen Löschpflichten nachkommen können, wenn die Voraussetzungen einer weiteren Verarbeitung nicht mehr vorliegen.[26] Im Einzelfall richtet sich der erforderliche Umfang der Schutzmaßnahmen danach, welche Gefahren für die Rechte und Freiheiten der betroffenen Personen im Falle einer Vernichtung, eines Verlusts, einer Veränderung oder einer unbefugten Offenlegung personenbezogener Daten drohen, Art. 32 Abs. 1, 2 DS-GVO.

2. Datenschutzrechtliche Vorgaben zum Schutz des Arbeitnehmers

Der Arbeitgeber ist auch verpflichtet, geeignete Maßnahmen zum Schutz der Daten seiner Arbeitnehmer zu ergreifen, § 26 Abs. 5 BDSG. Denn es besteht das Risiko einer Vermischung privater und betrieblicher Sphären, wenn die private Telefonnummer des Arbeitnehmers intern zu Kommunikationszwecken zirkuliert wird oder i.R.v. Videokonferenzen ggf. die Wohnungseinrichtung des Arbeitnehmers oder dessen Familienangehörige zu sehen sind. Soweit die Verarbeitung von derart persönlichen Daten betrieblich nicht erforderlich ist, fehlt es insoweit an einem datenschutzrechtlichen Erlaubnistatbestand. Die Arbeit im Homeoffice darf nicht dazu führen, dass die Persönlichkeit des Arbeitnehmers in höherem Umfang als bei einer Arbeit an dessen betrieblichem Arbeitsplatz offenbart wird.[27]

Darüber hinaus könnte der Arbeitgeber versucht sein, gewisse Kontroll- oder Überwachungsmaßnahmen zu treffen, um zu verhindern, dass der Arbeitnehmer sich seinen dienstlichen Pflichten im Homeoffice entzieht oder diesen nicht mehr ausreichend nachkommt. Auch insoweit bedarf es jedoch der Einhaltung datenschutzrechtlicher Vorgaben.

IV. Datenschutzrechtssichere Gestaltung des Homeoffice

1. Identifizierung datenschutzrechtlicher Risiken

Im Homeoffice droht ein Verlust faktischer und technischer Kontrollmöglichkeiten des Arbeitgebers. Technische Geräte befinden sich außerhalb seiner physischen Zugriffsmöglichkeit und er kann nicht mehr überwachen, wer Zugang und Zugriff auf technische Geräte oder sonstige Datenträger und Dokumente hat. Endgeräte könnten außerhalb des Firmennetzwerks eingesetzt werden und nicht mehr von dem Arbeitgeber kontrollierbaren Sicherheitsrisiken ausgesetzt sein.[28]

Besondere Risiken bestehen beim Einsatz privater Endgeräte (Bring Your Own Device – BYOD), da die verarbeiteten Daten hier ohne besondere technische Maßnahmen dem Einfluss und der Kontrolle des Arbeitgebers vollständig entzogen wären.[29] Hinzu kommt, dass die Kommunikation zwischen Mitarbeitern, die zuvor im Büro stattfand, nunmehr über andere Kanäle stattfindet. Mitarbeiter könnten auf ihre privaten Kommunikationswege zurückgreifen und hierbei vertrauliche Daten über kritische Anwendungen übermitteln und sie auf privaten Endgeräten speichern. Ebenso könnten Inhalte von Telefongesprächen von Familienangehörigen, Mitbewohnern oder Besuchern zur Kenntnis genommen werden.

2. Maßnahmen zur Wahrung datenschutzrechtlicher Grundsätze

a) Allgemeine Anforderungen an die Tätigkeit und die Einrichtung des Arbeitsplatzes

Im Homeoffice geht der Arbeitnehmer seiner Tätigkeit in einer völlig anderen Umgebung nach. Es findet eine automatische Annäherung privater und betrieblicher Sphären statt und es fehlt jegliche (soziale) Kontrolle durch Kollegen oder Vorgesetzte. Vor diesem Hintergrund sollten den Arbeitnehmern noch einmal die allgemeinen datenschutzrechtlichen Grundsätze und Richtlinien des Betriebs verdeutlicht werden. Insbesondere sollten die Arbeitnehmer für die zusätzlichen datenschutzrechtlichen Risiken im Homeoffice sensibilisiert werden.[30]

Auf die Mitnahme von Unterlagen oder physischen Datenträgern mit personenbezogenen Daten sollte verzichtet werden. Die Verwendung und der Verbleib derartiger Unterlagen und Datenträger ist für den Arbeitgeber nicht zu kontrollieren und begründet stets ein gewisses Verlustrisiko. Aus diesem Grunde sollte der Arbeitnehmer auch angewiesen werden, keine physischen Kopien und Ausdrucke von vertraulichen Daten im Homeoffice anzufertigen.[31]

Durch die äußere Gestaltung des Arbeitsplatzes muss sichergestellt werden, dass keine unbefugten Personen Kenntnis von personenbezogenen Daten erlangen können. Es bedarf einer Zugangskontrolle zu betrieblichen Unterlagen und den verwendeten technischen Geräten. Am besten eignet sich hierzu ein eigens abschließbares Arbeitszimmer, mindestens muss eine sichere Verwahrung der Unterlagen und Geräte in einem verschlossenen Schrank gewährleistet werden.[32] Unter Umständen sind Sichtschutzfolien einzusetzen, wenn anders nicht verhindert werden kann, dass vertrauliche Daten bereits durch flüchtige Blicke von Haushaltsangehörigen erfasst und zur Kenntnis genommen werden können.[33] Bei der Verwendung technischer Geräte muss der Zugang zu vertraulichen Informationen durch einen Kennwortschutz des Betriebssystems und durch die Aktivierung der Bildschirmsperre selbst beim kurzzeitigen Verlassen des Arbeitsplatzes beschränkt werden. Anmeldeinformationen wie Benutzernamen oder Passwörter dürften keinesfalls für Dritte zugänglich notiert und verwahrt werden.[34] Vertrauliche Telefonate müssen ohne unbefugte Mithörer geführt werden. Sie sollten keinesfalls im Garten oder bei offenen Türen oder Fenstern oder in Anwesenheit unberechtigter Dritter geführt werden.[35]

b) Technische Maßnahmen

Hiervon abgesehen ist vor allem durch die Einrichtung eines geeigneten IT-Sicherheitssystems die Einhaltung datenschutzrechtlicher Standards im Homeoffice sicherzustellen.[36]

---

24 *Martini* (o. Fußn. 23), Rn. 37; *Hoppe* (o. Fußn. 17), Rn. 689; *Hansen* (o. Fußn. 21), Rn. 40.
25 *Laue* (o. Fußn. 22), Rn. 14; *Hansen* (o. Fußn. 21), Rn. 41
26 *Hansen* (o. Fußn. 21), Rn. 41; vgl. auch *Paal*, in: Paal/Pauly (o. Fußn. 23), Art. 17 Rn. 6 ff.
27 *Wünschelbaum*, NZA 2020, 612 (614); *Kort*, RdA 2018, 24 (25 ff.).
28 Vgl. zu den datenschutzrechtlichen Risiken im Homeoffice auch *Gilga*, ZD-Aktuell 2020, 07113; *Müller* (o. Fußn. 19), Rn. 192; *Dury/Leibold*, ZD-Aktuell 2020, 04405.
29 *Dury/Leibold*, ZD-Aktuell 2020, 04405; *Hoppe* (o. Fußn. 17), Rn. 688 ff.
30 *Wünschelbaum*, NZA 2020, 612 (614); *Dury/Leibold*, ZD-Aktuell 2020, 04405; *Gilga*, ZD-Aktuell 2020, 07113.
31 *Dury/Leibold*, ZD-Aktuell 2020, 04405; *Gilga*, ZD-Aktuell 2020, 07113.
32 *Müller* (o. Fußn. 19), Rn. 193, 196; *Dury/Leibold*, ZD-Aktuell 2020, 04405.
33 *Gilga*, ZD-Aktuell 2020, 07113; *ULD Schleswig-Holstein*, Datenschutz: Plötzlich Homeoffice – und nun?, abrufbar unter: https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf.
34 *Hoppe* (o. Fußn. 17), Rn. 648; *Sächsischer DSB*, Hinweise zum Datenschutz bei der (Tele-)Heimarbeit/im Home-Office, abrufbar unter: https://www.saechsdsb.de/147-pandemie/607-datenschutz-bei-der-heimarbeit-bzw-im-home-office.
35 *ULD Schleswig-Holstein* (o. Fußn. 33).
36 *Gilga*, ZD-Aktuell 2020, 07113.

Idealerweise stellt der Arbeitgeber dem Arbeitnehmer für dessen Tätigkeit im Homeoffice die notwendigen technischen Geräte zur Verfügung, um ein jederzeitiges Zugriffsrecht auf den Client zu haben und die eingesetzte Hard- und Software vollständig kontrollieren zu können.[37] Die notwendige Zugangskontrolle kann über einen starken Passwortschutz und ggf. eine Zwei-Faktor-Authentifizierung erreicht werden. Zudem kann sichergestellt werden, dass die Geräte sich im Hinblick auf Verschlüsselungstechnologien und Anti-Viren-Software jederzeit auf dem neusten Stand befinden und entsprechende Updates vorgenommen werden.

Bestenfalls erfolgen Datenverarbeitungsvorgänge rein serverbasiert innerhalb des Unternehmensnetzwerks und lassen keine lokale Speicherung von vertraulichen Daten zu.[38] Bei firmeneigenen Geräten können derartige Einstellungen durch entsprechende Software ohne größere Schwierigkeiten herbeigeführt werden. Sie dienen der Zugriffs- und Weitergabekontrolle sowie Eingabekontrolle zur Sicherstellung von Datenvertraulichkeit und Datenintegrität. Gleichzeitig wird sichergestellt, dass der Arbeitgeber jederzeit die Möglichkeit des Fernzugriffs auf die verarbeiteten Daten behält, sodass ihre Verfügbarkeit sichergestellt wird und stets die Möglichkeit einer Datenlöschung besteht.

Zur Übertragungs- und Transportkontrolle sollte ein Datentransfer lediglich unter Verwendung von Remote-Verbindungen zum Firmennetzwerk, also insbesondere unter Verwendung von VPN-Tunneln, erfolgen.[39] So kann die Sicherheit des Datentransfers gewährleistet und gleichzeitig weitgehend nachvollzogen werden, an welche Stelle personenbezogene Daten übermittelt oder zur Verfügung gestellt werden. Sofern der Arbeitnehmer durch eine entsprechende Anbindung an das Firmennetzwerk und die Verwendung von Firmenendgeräten die gleiche IT-Infrastruktur und Software benutzt, die er auch bei einer Beschäftigung im Betrieb nutzt und damit auch den bereits zuvor getroffenen technischen und organisatorischen Schutzmaßnahmen unterliegt, sind dagegen in technischer Hinsicht in der Regel keine zusätzlichen Maßnahmen erforderlich.

c) Besonderheiten beim Einsatz von Fremdgeräten

Sollen bei der Arbeit im Homeoffice Endgeräte des Arbeitnehmers eingesetzt werden (BYOD), ist dies mit zusätzlichen Risiken verbunden, da hier keine vollständige Kontrolle des Arbeitgebers über das Gerät, das eingesetzte Betriebssystem und die installierte Software besteht.[40] Ohne besondere technische Vorkehrungen besteht die Gefahr einer mangelnden Trennung von Privat- und Betriebsdaten sowie die Möglichkeit einer unkontrollierten Speicherung oder Vervielfältigung vertraulicher Daten. Der hiermit verbundene Kontrollverlust wäre datenschutzrechtlich grob pflichtwidrig.[41]

Allerdings sind auch die mit dem Einsatz von Fremdgeräten einhergehenden Risiken durch den Einsatz spezieller IT-Systeme beherrschbar.[42] Durch sog. Container-Apps können zwei komplett voneinander getrennte Nutzeroberflächen geschaffen werden. Die betriebliche Oberfläche kann so gestaltet werden, dass eine Verbindung zum Firmennetzwerk lediglich über VPN-Tunnel erfolgt und betriebliche Daten lediglich mittels Terminalserver oder Citrix-Umgebung verarbeitet werden. So kommt es zu einer technisch vermittelten physischen Trennung von privaten und dienstlichen Daten. Die betriebliche Oberfläche kann vollständig durch die IT des Arbeitgebers administriert werden, sodass i.E. beinahe die gleiche Kontrolle über die betroffenen Daten ausgeübt werden kann wie bei einem arbeitgebereigenen Gerät.[43] Es kann also ein in sich abgeschlossenes IT-System eingerichtet werden, in dem die betriebliche Kommunikation sowie die Speicherung von Arbeitsergebnissen stattfindet.

Trotz dieser technischen Möglichkeiten stehen die zuständigen Behörden einer Nutzung von privaten Endgeräten ausgesprochen skeptisch gegenüber.[44] So geht der *Sächsische Datenschutzbeauftragte* davon aus, dass der Arbeitgeber die datenschutzrechtlich erforderlichen Schutzmaßnahmen beim Einsatz privater Endgeräte „in der Regel nicht effektiv gewährleisten" könne,[45] auch wenn diese Auffassung bei Einhaltung der oben empfohlenen technischen Vorkehrungen schwer haltbar sein dürfte. Es sollte jedoch in jedem Fall sichergestellt werden, dass die o.g. Sicherungsmaßnahmen eingehalten werden, um das Risiko behördlicher Verfahren weitgehend zu minimieren. Die Einführung und Ausgestaltung von BYOD unterliegt zudem grundsätzlich der Mitbestimmung durch den Betriebsrat.[46]

d) Einsatz von Konferenzsoftware

Die datenschutzrechtlichen Risiken hängen zunächst von der Art und den Funktionen einer Konferenzsoftware ab. So sind neben klassischen Videokonferenzlösungen auch Dienste verfügbar, die das Teilen von Bildschirminhalten, eine Integration von Kalenderinhalten oder bestimmten Anwendungen oder den gemeinsamen Zugriff der Anwender auf bestimmte Dokumente erlauben. Der Einsatz von Konferenzsoftware kann ein eigenständiges Sicherheitsrisiko darstellen, da neben den jeweiligen Teilnehmerdaten auch die sonstigen übertragenen Daten auf Servern der jeweiligen Diensteanbieter verarbeitet werden.[47]

Datenschutzrechtlich stellt sich die Einbindung eines Konferenzdienstes als Fall der Auftragsverarbeitung i.S.v. Art. 28 DS-GVO dar.[48] Der Verantwortliche muss nicht nur einen Vertrag mit den entsprechenden Mindestinhalten mit dem Diensteanbieter schließen, er muss bei der Auswahl des Anbieters auch sicherstellen, dass die Verarbeitung personenbezogener Daten durch den Anbieter im Einklang mit den Anforderungen der DS-GVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist, Art. 28 Abs. 1 DS-GVO.[49] Diese Voraussetzungen sind von dem Verantwortlichen grundsätzlich zu prüfen und zu kontrollieren, wobei eine ordnungsgemäße Beauftragung in der Regel ausgeschlossen sein dürfte, wenn tatsächliche Hinweise auf eine datenschutzrechtswidrige Datenverarbeitung vorliegen.[50]

Vor diesem Hintergrund stellt sich die datenschutzrechtskonforme Auswahl eines Konferenzanbieters derzeit als schwierig dar. Bei einem Test der *Berliner Beauftragten für Datenschutz und Informationssicherheit* sind insbesondere populäre Dienste wie Zoom, Skype for Business oder Microsoft Teams durchgefallen.[51] Auch wenn die Einschätzung der *Berliner Aufsichts-*

37 *Dury/Leibold*, ZD-Aktuell 2020, 04405; *Müller* (o. Fußn. 19), Rn. 177; *BfDI*, Telearbeit und Mobiles Arbeiten, S. 22.
38 *Hoppe* (o. Fußn. 17), Rn. 644; *Gilga*, ZD-Aktuell 2020, 07113.
39 *Dury/Leibol*d, ZD-Aktuell 2020, 04405; *Gilga*, ZD-Aktuell 2020, 07113.
40 *Dury/Leibold*, ZD-Aktuell 2020, 04405; *Hoppe* (o. Fußn. 17), Rn. 688 ff.; *Göpfert/Wilke*, NZA 2012, 765 (766 f.).
41 *Dury/Leibold*, ZD-Aktuell 2020, 04405; *Gilga*, ZD-Aktuell 2020, 07113.
42 *Hoppe* (o. Fußn. 17), Rn. 688 ff.; *Dury/Leibold*, ZD-Aktuell 2020, 04405.
43 *Conrad*, in: Auer-Reinsdorff/Conrad, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 37 Rn. 317; *Hoppe* (o. Fußn. 17), Rn. 691; *Jandt/Steidle*, CR 2013, 338 (344).
44 Vgl. *BfDI* (o. Fußn. 37), S. 16 ff.; vgl. auch *Dury/Leibold*, ZD-Aktuell 2020, 04405.
45 *Sächsischer DSB* (o. Fußn. 34).
46 *Müller* (o. Fußn. 19), Rn. 179; *Hoppe* (o. Fußn. 17), Rn. 639 ff.
47 *Wünschelbaum*, NZA 2020, 612 (614); *Stoklas*, ZD-Aktuell 2020, 07093.
48 *Stoklas*, ZD-Aktuell 2020, 07093.
49 Vgl. auch *Spoerr*, in: Wolff/Brink, BeckOK Datenschutzrecht, 32. Ed. 2020, DS-GVO, Art. 28 Rn. 33.
50 Vgl. *Martini* (o. Fußn. 23), Art. 28 Rn. 21; *Spoerr* (o. Fußn. 49), Rn. 35.
51 *Berliner BDI*, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten v. 3.7.2020, abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf.

behörde nicht rechtsverbindlich ist, ist insoweit Vorsicht geboten.[52]

Im Hinblick auf das bereits angesprochene Risiko für die Privatsphäre der Arbeitnehmer durch die Offenbarung seines Lebensmittelpunkts ist bei Konferenzen in Anwendung von § 26 Abs. 1 BDSG ggf. zu erwägen, ob die Kommunikation in gleich effektiver Weise durch herkömmliche Telefonkonferenzen durchgeführt werden kann.[53] Wenn eine Videokonferenz stattfinden soll, sollte der jeweilige Konferenzdienst ausreichend Optionen zum Schutz privater Umstände durch den jeweiligen Anwender aufweisen. So bieten bestimmte Dienste die Möglichkeit, das Umfeld des Teilnehmers verschwimmen zu lassen, sodass nur der Teilnehmer selbst zu sehen ist. Es kann dem Arbeitnehmer aber auch die Möglichkeit zugestanden werden, seine Kamera zu deaktivieren.

e) Korrektiv der Verhältnismäßigkeit?

Wenn das Homeoffice lediglich zur kurzen Überbrückung besonders akuter pandemischer Entwicklungen geplant ist und kaum personenbezogene Daten verarbeitet werden sollen, kann sich die Frage stellen, ob die Einhaltung aller oben beschriebenen Vorgaben in jedem Fall zwingend ist.

Die DS-GVO kennt zwar keinen Ausnahmezustand,[54] sie sieht jedoch in Art. 32 Abs. 1 DS-GVO im Hinblick auf die zu treffenden technisch organisatorischen Maßnehmen einen Verhältnismäßigkeitsgrundsatz vor.[55]

Hiernach sind insbesondere auch unter Berücksichtigung der Implementierungskosten, der Art und des Umfangs der Verarbeitung und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen diejenigen Maßnahmen zu treffen, die ein dem Risiko angemessenes Schutzniveau gewährleisten. Die DS-GVO verlangt von dem Verantwortlichen daher nicht den maximalen Schutz, sondern lediglich das wirtschaftlich Zumutbare.[56] Es ist daher durchaus denkbar, von den o.g. Standards abzuweichen, wenn ihre Einhaltung im Einzelfall wirtschaftlich nicht darstellbar wäre und von der Tätigkeit im Homeoffice kein nennenswertes Risiko für die betroffenen Personen ausgeht.[57]

Wenn der Verantwortliche jedoch im Hinblick auf die technisch-organisatorischen Maßnahmen von den allgemeinen Standards abweichen möchte, verlangt ihm dies eine besonders sorgfältige Risikoeinschätzung ab.[58] Er muss die entsprechenden Erwägungen dezidiert erläutern und dokumentieren. Zudem sollte erhöhter Wert auf eine Sensibilisierung der Arbeitnehmer gelegt werden, da diese letztendlich das Weniger an technischen Schutzmaßnahmen durch ein Mehr an Sorgfalt und Pflichtbewusstsein im Umgang mit personenbezogenen Daten ausgleichen müssen.

Wenn die Arbeitnehmer im Homeoffice mit umfangreichen Datensammlungen umgehen oder gar sensible Daten i.S.v. Art. 9 DS-GVO verarbeiten, dürften Abweichungen der o.g. technisch-organisatorischen Schutzmaßnahmen von vorneherein ausgeschlossen sein.

3. Zulässigkeit von Maßnahmen zur Arbeitnehmerkontrolle

Im Hinblick auf Homeoffice fällt es dem Arbeitgeber schwerer, Arbeitszeiten oder Arbeitsleistung zu kontrollieren.[59] Es scheint daher eine große Verlockung zur technischen Überwachung der Arbeitnehmer zu bestehen.[60] Dabei ist aber jegliche Überwachung an den Anforderungen des § 26 Abs. 1 BDSG zu messen.[61]

Wenn der Arbeitgeber die Tätigkeiten im Homeoffice über ein von ihm betriebenes IT-Netzwerk ausführen lässt, kann er anhand der entsprechenden Log-In-Daten nachvollziehen, wann sich seine Arbeitnehmer in das Netzwerk eingeloggt und wann wieder ausgeloggt haben. Eine solche Auswertung entspricht im Wesentlichen dem allgemeinen Einstempeln am Arbeitsplatz, sie ist grundsätzlich nach § 26 Abs. 1 S. 1 BDSG zur Durchführung des Beschäftigungsverhältnisses erforderlich und wird daher als zulässig angesehen.[62]

Soweit die Arbeitnehmer dienstliche Geräte verwenden und der Arbeitgeber eine private Nutzung dieser Geräte von vorneherein untersagt und nicht faktisch duldet, darf er überprüfen, ob dieses Verbot eingehalten wird, indem er Stichproben der Verlaufsdaten oder der E-Mail-Kommunikation auswertet.[63] Die Rückschlüsse, die der Arbeitgeber hieraus auf das tatsächliche Arbeitsverhalten im Homeoffice ziehen kann, dürften allerdings begrenzt sein. Eine Überprüfung von Browser- oder E-Mail-Daten bei erlaubter oder geduldeter Privatnutzung dienstlicher Geräte ist von Anfang an unzulässig.[64]

In den meisten IT-Systemen besteht die Möglichkeit, die Speicheraktivität eines Nutzers nachzuvollziehen. Hierdurch ergibt sich häufig ein genauerer Eindruck der tatsächlichen Arbeitsaktivität des Arbeitnehmers. Allerdings dürfte eine anlasslose Auswertung insbesondere dann unzulässig sein, wenn hierdurch ein umfassendes Bild der Arbeitsleistung erzeugt wird. Sie kann lediglich bei konkreten Verdachtsmomenten rechtmäßig sein.[65]

Ein noch weitgehender Eingriff wäre z.B. die Protokollierung von Tastatureingaben oder die Erstellung regelmäßiger Screenshots. Die Installation derartiger Keylogger ist ein massiver Eingriff in das Recht auf informationelle Selbstbestimmung des Arbeitnehmers und allenfalls bei dem begründeten Verdacht schwerwiegender Pflichtverletzungen zulässig.[66]

Generell gilt es zu beachten, dass bei Überwachungsmaßnahmen aller Art ein Mitbestimmungsrecht des Betriebsrats gem. § 87 Abs. 1 Nr. 6 BetrVG besteht. Ist eine Anwendung bestimmter Maßnahmen in Verdachtsfällen grundsätzlich angedacht, sollte bereits im Vorfeld eine entsprechende Betriebsvereinbarung geschlossen werden, um im Falle entsprechender Verdachtsmomente schnell handeln zu können.[67] Ob der Einsatz von Überwachungsmaßnahmen stets offen erfolgen muss, ist von der Rechtsprechung nach Inkrafttreten der DS-GVO und nach der Novellierung des BDSG noch nicht endgültig geklärt. Ein Urteil des *VG Ansbach* deutet jedoch darauf hin.[68]

---

52 Vgl. auch *Stoklas*, ZD-Aktuell 2020, 07093.
53 *Wünschelbaum*, NZA 2020, 612 (614).
54 *Wünschelbaum*, NZA 2020, 612.
55 *Sydow*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, DSGVO Art. 32 Rn. 10; *Hansen* (o. Fußn. 21), Rn. 20 ff.; *Martini* (o. Fußn. 23), Art. 32 Rn. 60; *Müller* (o. Fußn. 19), Rn. 196.
56 *Martini* (o. Fußn. 23), Art. 32 Rn. 60.
57 Noch weitergehend *Martini* (o. Fußn. 23), Art. 32 Rn. 60: „im Einzelfall kann das Verhältnismäßigkeitsprinzip als Korrektiv auch gebieten, dass der Normadressat des Art. 32 Abs. 1 ausnahmsweise keine Maßnahme ergreifen muss."
58 *Hansen* (o. Fußn. 21), Rn. 20; f.; *Sydow* (o. Fußn. 55), Rn. 10.
59 *von Steinau-Steinrück*, NJW-Spezial 2018, 754.
60 *Moorstedt*, In der Krise boomt auch die Überwachung durch den Chef, SZ v. 6.4.2020, abrufbar unter: https://www.sueddeutsche.de/digital/home-office-ueberwachung-tracking-chef-zoom-1.4868739; *Lobe*, Wie Mitarbeiter im Homeoffice überwacht werden, Berliner Zeitung v. 26.4.2020, abrufbar unter: https://www.berliner-zeitung.de/lernen-arbeiten/wie-mitarbeiter-im-homeoffice-ueberwacht-werden-li.82174.
61 *Röller*, in: Kütter, Personalhandbuch, 27. Aufl. 2020, Homeoffice, Rn. 17.
62 *von Steinau-Steinrück*, NJW-Spezial 2018, 754 (755); *Ulber*, NZA 2019, 677 (678); *von Steinau-Steinrück*, NJW-Spezial 2018, 754.
63 *LAG Berlin-Brandenburg* ZD 2016, 336 (Ls.) m. Anm. *Tiedemann*; *LAG Köln* ZD 2020, 533 m. Anm. *Albrecht*.
64 *Seifert*, in: Simitis/Hornung/Spiecker (o. Fußn. 21), DSGVO Art. 88 Rn. 150; *Stück*, CCZ 2018, 88 (89).
65 *von Steinau-Steinrück*, NJW-Spezial 2018, 754 (755); *Stück*, CCZ 2018, 88 (89).
66 *Stück*, CCZ 2018, 88 (89); *von Steinau-Steinrück*, NJW-Spezial 2018, 754 (755).
67 *von Steinau-Steinrück*, NJW-Spezial 2018, 754 (755).
68 *VG Ansbach* ZD 2020, 607 – in diesem Heft.

V. Homeoffice-Richtlinie und Checkliste zur Umsetzung rechtlicher Vorgaben

Sollen bestimmte Tätigkeiten im Unternehmen künftig aus dem Homeoffice erbracht werden, bedarf es hierzu teils umfangreicher organisatorischer und technischer Vorbereitungen. Die wichtigsten Punkte sollen hier nunmehr noch einmal zusammengefasst und übersichtsartig dargestellt werden.

1. Richtlinie für die Arbeitnehmer zur Homeoffice-Nutzung

Der Arbeitgeber muss sicherstellen, dass seine Arbeitnehmer die datenschutzrechtlichen Vorgaben bei einem Umgang mit personenbezogenen Daten einhalten, vgl. Art. 32 Abs. 4 DS-GVO. Soweit seine Arbeitnehmer ihrer Tätigkeit im Homeoffice nachkommen, ist die Gestaltung des Arbeitsplatzes und das Verhalten seiner Arbeitnehmer seiner Kontrolle allerdings weitgehend entzogen.

Um seinen Organisationspflichten nachzukommen und seinen verbleibenden Einfluss bestmöglich geltend zu machen, sollte der Arbeitgeber seine Arbeitnehmer nicht nur hinreichend schulen, sondern sich die Einhaltung der o.g. Maßnahmen zum Schutz vertraulicher Daten bei der Tätigkeit im Homeoffice auch durch die Aufstellung einer verbindlichen Richtlinie zusichern lassen.[69] Eine solche Richtlinie kann z.B. als Zusatz zum Arbeitsvertrag oder als Betriebsvereinbarung abgeschlossen werden.[70]

In dieser Richtlinie sollten folgende Punkte geregelt werden:[71]

- Zulässigkeit und Voraussetzungen einer Tätigkeit im Homeoffice, insbesondere falls die Nutzung des Homeoffice den Mitarbeitern freigestellt wird;
- Bestimmung von Arbeitsort und Arbeitszeit, Festlegung von Dokumentationspflichten des Arbeitnehmers oder Kontrollmöglichkeiten des Arbeitgebers (Log-In-Kontrolle);
- Einrichtung des Homeoffice, insbesondere Regelung über Arbeitsmittel (Nutzung firmeneigener Geräte oder BYOD);
- Datenschutzrechtliche Verpflichtung des Arbeitnehmers, insbesondere
  - datenschutzrechtliche Anforderungen an den Arbeitsplatz zur Zugangs- und Zugriffskontrolle;
  - ordnungsgemäße IT-Einrichtung und -Nutzung, insbesondere im Falle von BYOD;
  - datenschutzrechtliche Verhaltenspflichten des Arbeitnehmers im Umgang mit Daten und Dokumenten (keine privaten Ausdrucke, keine private Speicherung, keine Weiterleitung an private E-Mail-Postfächer).

Insbesondere bei freiwilliger Nutzung des Homeoffice durch Arbeitnehmer erscheint es zudem denkbar, Zutrittsrechte sowie im Falle von BYOD Herausgabeansprüche oder Prüfungsrechte zu vereinbaren.[72] Ein Vorbehalt entsprechender Rechte bei einer einseitigen Anordnung des Homeoffice oder einer verpflichtenden Betriebsvereinbarung dürfte dagegen kaum zulässig sein.[73]

2. Checkliste

Vor der Umstellung auf Homeoffice sollte der Arbeitgeber überlegen, ob diese Umstellung für die einzelnen Arbeitnehmer freiwillig oder verpflichtend erfolgen soll. Hiervon hängt insbesondere ab, auf welcher arbeitsrechtlichen Grundlage die Umstellung zu erfolgen hat. Er sollte darüber hinaus prüfen, ob die zur Verrichtung der Arbeitstätigkeiten im Homeoffice erforderlichen Endgeräte für die Arbeitnehmer in ausreichender Zahl beschafft und zur Verfügung gestellt werden können oder ob (ergänzend) auf Endgeräte der Arbeitnehmer zurückgegriffen werden soll (BYOD). I.Ü. muss der Arbeitgeber insbesondere folgende Maßnahmen treffen, damit eine rechtssichere Umstellung auf Homeoffice gelingen kann:

- Schaffung der arbeitsrechtlichen Grundlagen für die Umstellung auf Homeoffice unter Berücksichtigung der arbeitsschutzrechtlichen Organisations- und Hinweispflichten;
- Überprüfung des bestehenden Datenschutzkonzepts, da sich aus etwaigen Schwächen und Lücken bei Tätigkeiten im Homeoffice besondere Risiken ergeben können;
- genaue Prüfung, welche Tätigkeiten ins Homeoffice verlagert werden sollen und welche Datenverarbeitungsvorgänge hierdurch betroffen sind, sowie Einschätzung daraus resultierender datenschutzrechtlicher Risiken;
- Schaffung der notwendigen technischen Infrastruktur zur Umsetzung der anerkannten technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten bzw. umfangreiche Abwägung und Dokumentation, wenn von den geltenden Sicherheitsstandards abgewichen werden soll;
- Entwurf und Implementierung einer Homeoffice-Vereinbarung bzw. einer Homeoffice-Richtlinie, ggf. weitergehende Schulung der Arbeitnehmer;
- Dokumentation der getroffenen Maßnahmen, um die Einhaltung datenschutzrechtlicher Grundsätze gem. Art. 5 Abs. 2 DS-GVO nachweisen zu können.

Schnell gelesen ...

- Sollen bestimmte Arbeitstätigkeiten im Homeoffice erbracht werden, stellen sich arbeits- und datenschutzrechtliche Herausforderungen.
- Die pandemiebedingte Umstellung auf Homeoffice erfolgte häufig ohne Berücksichtigung der einschlägigen arbeits- oder datenschutzrechtlichen Bestimmungen.
- Soweit die entsprechenden Vorgaben noch nicht umgesetzt sind, sollte dies nun schnellstmöglich geschehen, um eine rechtssichere Grundlage für Tätigkeiten im Homeoffice zu schaffen und auf etwaige Quarantäne-Maßnahmen oder künftige Lockdowns vorbereitet zu sein und durch aktuelle Homeoffice-Regelungen keinen Bußgeldrisiken ausgesetzt zu sein.

Dr. Felix Suwelack
ist Rechtsanwalt in der Kanzlei Baumeister Rechtsanwälte mbB in Münster.

69 *Gilga*, ZD-Aktuell, 2020, 07113; *Müller* (o. Fußn. 19), Rn. 199; *Dury/Leibold*, ZD-Aktuell 2020, 04405.
70 Ausf. und mit Formulierungsvorschlägen: *Hülsemann*, ArbRAktuell 2017, 483; *Dury/Leibold*, ZD-Aktuell 2020, 04405.
71 Muster und Gestaltungsvorschläge finden sich z.B. bei *Hoppe* (o. Fußn. 17), Rn. 676; *Hülsemann*, ArbRAktuell 2017, 483; *Müller* (o. Fußn. 19), Rn. 705 ff.; *Röller* (o. Fußn. 61), Rn. 7 ff.
72 Zur Zulässigkeit derartiger Vereinbarungen bei freiwilliger Nutzung des Homeoffice vgl. *Hoppe* (o. Fußn. 17), Rn. 650; *Benkert*, NJW-Spezial 2019, 306 (307); *Aligbe*, ArbRAktuell 2016, 132 (135).
73 *Hidalgo*, NZA 2019, 1449 (1452); *Richter*, ArbR-Aktuell 2019, 166 (168).