Datenschutz im Home-Office

TELEARBEIT *Auch im Home-Office gilt das Datenschutzrecht. Dabei müssen einige Besonderheiten beachtet werden.*

VON **BRUNO SCHIERBAUM**

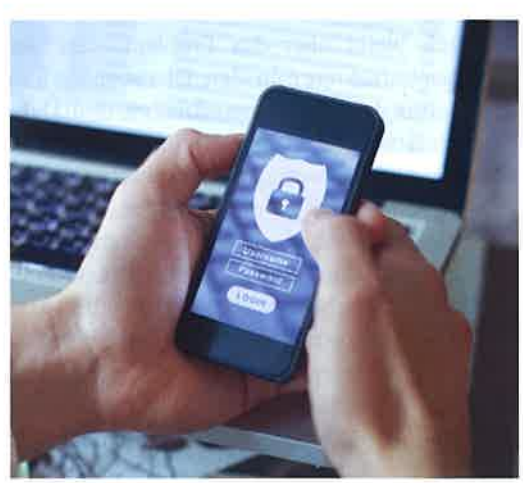
DARUM GEHT ES

1. Bei der Arbeit im Home-Office werden regelmäßig auch personenbezogene Daten verarbeitet.

2. Mit einer Vorabkontrolle bzw. Datenschutz-Folgenabschätzung lassen sich mögliche Datenschutzrisiken feststellen.

3. Mit technischen und organisatorischen Maßnahmen ist der Datenschutz auch im Home-Office zu gewährleisten.

Das Datenschutzrecht ist zwingend zu beachten, wenn personenbezogene Daten verarbeitet werden. Dabei ist es unerheblich, an welchem Ort Beschäftigte ihre Arbeit verrichten, ob in der Dienststelle oder an anderen Orten. Auch für Arbeiten im Home-Office – häufig auch als Tele-(heim)arbeit bezeichnet – und auch bei mobiler Arbeit ist das Bundesdatenschutzgesetz (BDSG) zwingend einzuhalten. Das Gleiche gilt für das jeweilige Landesdatenschutzgesetz, auch wenn die Gesetze vorrangig auf die klassischen Datenverarbeitungsstrukturen abzielen, wie sie etwa in Rechenzentren gegeben sind[1], und weniger die mobile Datenverarbeitung berücksichtigen. Grundsätzlich gelten für Arbeiten im Home-Office oder für mobile Arbeit datenschutzrechtlich die gleichen Bestimmungen wie in den Dienststellen. Allerdings sind bei der außerbetrieblichen Arbeit die Kontroll- und Einflussmöglichkeiten der Dienststellenleitung erschwert und die Missbrauchsmöglichkeiten personenbezogener Daten und mögliche Zugriffe unbefugter Dritter sind deutlich höher als in der Dienststelle. So können zum Beispiel beim Transport von Dokumenten, Akten oder Datenträgern Daten oder Unterlagen verloren gehen, entwendet und von Unbefugten eingesehen werden.[2]



Durch Verschlüsselung lassen sich Daten schützen.

Anzuwendendes Datenschutzrecht

Aktuell sind das BDSG bzw. die Landesdatenschutzgesetze zu beachten. Das BDSG gilt für öffentliche Stellen des Bundes (§ 1 Abs. 2 BDSG). Die Landesdatenschutzgesetze sind für die Behörden und öffentlichen Stellen der jeweiligen Länder anzuwenden.

Unternehmen, Behörden und sonstige öffentliche Stellen müssen sich ab dem 25.5.2018 nach der Datenschutz-Grundverordnung (DS-GVO)[3] richten. Zusätzlich sind die ergänzenden Vorgaben des BDSG-neu[4] bzw. der Landesdatenschutzgesetze-neu[5] anzuwenden, in denen unter anderem Regelungen zum Beschäftigten-Datenschutz enthalten sind.

Verarbeitung personenbezogener Daten

Werden bei der Arbeit im Home-Office keine personenbezogenen Daten verarbeitet oder genutzt, ist das Arbeiten von zu Hause daten-

1 Vgl. Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl., § 9 Rn. 30.
2 Vgl. Deutscher Bundestag/Wissenschaftliche Dienste, Telearbeit und Mobiles Arbeiten – Voraussetzungen, Merkmale und rechtliche Rahmenbedingungen, WD 6 – 3000 – 149/16, S. 11; Zilkens, Datenschutz in der Kommunalverwaltung, S. 409.
3 Verordnung (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 Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Näher hierzu Schierbaum, PersR 7-8/2017, 44 ff.
4 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz – DSAnpUG-EU), BGBl. 2017, S. 2097 ff. Näher hierzu Schierbaum, PersR 7-8/2017, 44 ff.
5 Auf Landesebene gibt es beispielsweise Gesetzgebungsaktivitäten in Sachsen (LT-Drs. 6/10918), Brandenburg (LT-Drs. 6/7365) und in Sachsen-Anhalt (LT-Drs. 7/1736); hierzu Horstmann, Stand der Anpassung des Datenschutzrechts an die DS-GVO in den Ländern, ZD Fokus, S. XIII f., in: Zeitschrift für Datenschutz-Aktuell 18/17.

schutzrechtlich als unproblematisch anzusehen. Werden jedoch personenbezogene Daten verarbeitet – was die Regel sein wird – sollte unter Berücksichtigung der Art der zu verarbeitenden Daten, insbesondere im Hinblick auf die Sensibilität der Daten geprüft werden, ob Teleheimarbeit vertretbar ist oder im Einzelfall davon abzuraten ist.[6] Besonders in den Blick zu nehmen sind dabei besondere Datenkategorien (siehe Überblick auf Seite 27).

Die Zulässigkeit bzw. Rechtmäßigkeit[7] der Verarbeitung dieser oder anderer weniger sensibler personenbezogener Daten wird bereits im Vorfeld der Arbeit von Beschäftigten im Rahmen des Home-Offices geprüft worden sein. Denn mit der Weitergabe der Daten an den Beschäftigten im Home-Office liegt datenschutzrechtlich keine Übermittlung von Daten vor und bedarf daher keiner zusätzlichen Zulässigkeitsprüfung nach § 4 BDSG. Beim Arbeiten im Home-Office geht es vielmehr darum, den Datenschutz in der besonderen Verarbeitungssituation bei den Beschäftigten zu Hause zu gewährleisten. Es sollte gerade hinsichtlich der besonderen Daten (siehe nebenstehende Randspalte) das Risiko eines Missbrauchs im Vorfeld abgeschätzt und eine Bewertung vorgenommen werden, ob und unter welchen Umständen die Verarbeitung dieser Daten im Home-Office in Betracht kommt.[8] Dies sollte im Rahmen einer Vorabkontrolle und künftig im Rahmen einer Datenschutz-Folgenabschätzung geschehen (Art. 35 DS-GVO).

PRAXISTIPP

Sicherheitskonzept für das Home-Office

Da eine Vorabkontrolle und eine Datenschutz-Folgenabschätzung dokumentiert werden müssen, sollte als Ergebnis ein Sicherheitskonzept[9] für das Arbeiten im Home-Office erstellt werden.[10] Dabei ist insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nach § 9 BDSG aufzunehmen.

Datenschutz-Folgenabschätzung

Da die Verarbeitung personenbezogener Daten im Home-Office »besondere Risiken für die Rechte und Freiheiten der Betroffenen« aufweisen können, ist eine Vorabkontrolle nach § 4d Abs. 5 und 6 BDSG[11] durchzuführen. Eine Vorabkontrolle sollte folgende Aspekte umfassen:[12]

1. Erstellung einer Systembeschreibung
2. Prüfung der Rechtsgrundlagen der Verarbeitung
3. Gefahrenanalyse
4. Risikoanalyse
5. Erstellung eines Datenschutz- und Datensicherungskonzeptes
6. Beschreibung der Gefahren-Beherrschung[13].

Die Vorabkontrolle ist durch den internen Datenschutzbeauftragten durchzuführen und das Ergebnis ist schriftlich zu dokumentieren.[14]

Ab 25.5.2018 wird an Stelle der Vorabkontrolle eine Datenschutz-Folgenabschätzung durchgeführt werden müssen. Eine Datenschutz-Folgenabschätzung ist dann vorgeschrieben, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 35 Abs. 1 DS-GVO). Das ist insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Fall. Für das Arbeiten im Home-Office kommt eine vorherige Datenschutz-Folgenabschätzung deshalb in Betracht, weil hier durchaus »neue Technologien« angewandt werden. Insbesondere wird aufgrund der »besonderen Umstände« der Arbeit von zu Hause und des damit verbunden Risikos eine Datenschutz-Folgenabschätzung erforderlich sein. Der interne Datenschutzbeauftragte hat hier im Gegensatz zur Vorabkontrolle lediglich eine beratende Funktion. Der Mindestumfang für Prüfungsmaßnahmen, die im Rahmen einer Datenschutz-Folgenabschätzung durchzuführen sind, ist in der Randspalte auf Seite 26 aufgelistet.

BESONDERE DATEN

Nach Art. 9 Abs. 1 DS-GVO sind die besonderen Kategorien personenbezogener Daten Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit hervorgehen sowie genetische Daten, biometrische Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

6 Vgl. hierzu Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), Telearbeit – Ein Datenschutz-Wegweiser, S. 6 ff.
7 Dieses ist in Art. 6 DS-GVO und in Bezug auf Beschäftigten-Daten zusätzlich in § 26 BDSG-neu geregelt und entspricht grundsätzlich den aktuell geltenden Vorgaben des § 4 BDSG.
8 Vgl. Zilkens, Datenschutz in der Kommunalverwaltung, S. 414 f.
9 Aktuell ist nach folgenden LDSG vorgeschrieben, Sicherheitskonzepte zu erstellen: § 5 Abs. 3 BlnDSG, § 9 Abs. 2 ThürDSG, § 10 Abs. 3 DSG NRW, § 22 Abs. 5 DSG MV, § 5 LDSG SH.
10 Vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge – M 2.117 Erstellung eines Sicherheitskonzeptes für Telearbeit.
11 Vorgaben zur Vorabkontrolle sind enthalten in: § 12 LDSG BW, Art. 26 Abs. 3 BayDSG, § 5 Abs. 3 BlnDSG, § 7 Abs. 3 BbgDSG, § 7 Abs. 2 BremDSG, § 8 Abs. 3 HmbDSG, § 7 Abs. 5 i.V.m. § 5 Abs. 2 Nr. 5 HDSG, § 19 DSG MV, § 7 Abs. 3 i.V. m. § 8a Abs. 3 NDSG, § 10 Abs. 3 LDSG NRW, § 9 Abs. 5 LDSG RP, § 11 Abs. 1 i.V.m. § 8 Abs. 2 Nr. 2 SDSG, § 10 Abs. 4 SächsDSG, § 14 Abs. 2 DSG LSA, § 9 i.V.m. § 10 Abs. 4 Nr. 5 LDSG SH, § 34 Abs. 2 ThürDSG.
12 So zum Beispiel § 4d Abs. 6 BDSG, § 10 a Abs. 1 BbgDSG, § 20 Abs. 3 Nr. 3 DSG MV, § 8 a Abs. 3 NDSG, § 9 Abs. 5 LDSG RP, § 11 Abs. 4 Nr. 4 SächsDSG.
13 Vgl. hierzu ausführlich Der Landesbeauftragte für den Datenschutz Niedersachen, Vorabkontrolle ... leichtgemacht.
14 Vgl. Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, a.a.O., § 4d Rn. 11.

MINDESTUMFANG

Mindestumfang einer Datenschutz-Folgenabschätzung nach Art. 35 Abs. 7 DS-GVO:
Die Datenschutz-Folgenabschätzung enthält zumindest
- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und den Zweck der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen,
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird und
- der Nachweis dafür, dass die DS-GVO eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Organisatorische Maßnahmen

Nach § 9 BDSG und der dazu gehörigen Anlage sind technische und organisatorische Maßnahmen zum Datenschutz vorgesehen, die es in ähnlicher Form auch in den Landesdatenschutzgesetzen gibt[15].

So ist unter anderem jedem Unbefugten der Zutritt zu den IT-Systemen zu verwehren (Zutrittskontrolle). Dazu gehören auch alle Personen im Haushalt des im Home-Office arbeitenden Beschäftigten. Zusätzlich müssen die Nutzung der Datenverarbeitungsanlage und der Zugriff auf personenbezogene Daten durch unbefugte Dritte verhindert werden, zum Beispiel durch die Nutzung eines Passworts. Werden Daten auf der Festplatte des Home-Office-Computers gespeichert, ist die Festplatte zu verschlüsseln (Zugangskontrolle). Über die Nutzung von VPN (Virtual Private Network)[16] kann gewährleistet werden, dass der im Home-Office arbeitende Beschäftigte seinen Arbeitsplatz und seine Daten auf den Computer zu Hause zur Verfügung gestellt bekommt und alle Daten und Programme zentral in der Dienststelle auf den Servern gespeichert werden.[18] Zudem wird im Rahmen der Eingabekontrolle eine Protokollierung erfolgen müssen, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind (siehe hierzu die Maßnahmen in der Tabelle). Die anfallenden personenbezogenen Daten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitung gespeichert und nur für diese Zwecke verwendet werden (§ 31 BDSG).

Kann die Dienststellenleitung für außerhalb der Dienststelle liegende Home-Office-Arbeitsplätze keine ausreichenden Vorkehrungen zur Sicherstellung der in § 9 BDSG vorgeschriebenen Vorgaben treffen oder ist der technische oder finanzielle Aufwand zu hoch, muss auf die Verarbeitung personenbezogener Daten verzichtet werden. Die entsprechenden Arbeiten dürfen dann nicht im Rahmen des Home-Offices erledigt werden.[19]

Ähnliche Zielvorgaben zur Umsetzung von technischen und organisatorischen Maßnahmen sind in Art. 32 DS-GVO (Sicherheit der Verarbeitung) und in Art. 5 DS-GVO (Grundsätze der Verarbeitung) enthalten.

TABELLE

Technisch-organisatorische Maßnahmen

Technisch-organisatorische Maßnahmen zum Schutz von Daten sind beispielsweise[17]
- separates, abschließbares Arbeitszimmer
- Trennung zwischen beruflichem und privatem (Internet-)Anschluss
- Zugang zu (sensiblen) personenbezogenen Daten nur mit Benutzer-ID und PIN oder Karte
- Verbindung ausschließlich über ein Virtual Private Network (VPN)
- Zugangsmöglichkeit des Arbeitgebers, des Beauftragten für den Datenschutz, des Personalrats und der Datenschutzaufsichtsbehörde zum Telearbeitsplatz
- Sperrung von USB-Zugängen und anderen Anschlüssen
- keine private Nutzung der dienstlich zur Verfügung gestellten IT-Ausstattung
- Datenträger stets nur verschlüsselt und Papierunterlagen sorgsam zu verwahren

Zutrittsrecht zur Wohnung

Die Dienststellenleitung trägt die Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften. Diese Verantwortung kann sie nicht an die Beschäftigten delegieren. Sie bleibt stets die für den Datenschutz Verantwortliche. Aus diesem Grund muss die Dienststellenleitung die eigene gesetzlich verankerte Kontrollmöglichkeit auch bei Arbeiten im Home-Office vertraglich absichern. Dies muss auch für die externe Datenschutzaufsicht[20] und auch für den internen Datenschutzbeauftragten gelten. Der Personalrat hat die Einhaltung bestehender Dienstvereinbarungen und Datenschutzvorschriften zu überwachen und hat damit grundsätzlich auch Zutritt zum Home-Office, um seiner Überwachungsaufgabe nachkommen zu können. Dieser Kontrolle steht allerdings grundsätzlich die in Art. 13 GG

15 Einige Länder haben in ihren LDSG entsprechende Vorgaben wie in § 9 BDSG, so: § 10 HDSG, § 9 LDSG-BW, § 7 NDSG, § 9 LDSG-RP, Art. 7 BayDSG, § 11 SDSG, § 7 BremDSG, § 9 LDSG RP. Andere Länder knüpfen an den Vorgaben der klassischen IT-Sicherheit an, so: § 10 BbgDSG, § 10 DSG-LSA, § 21 DSG MV, § 10 Abs. 2 DSG NRW, § 8 HmbDSG, § 9 Abs. 2 SächsDSG, § 5 LDSG SH, § 9 Abs. 2 ThürDSG.

16 VPN bezeichnet ein virtuelles, privates und in sich geschlossenes Kommunikationsnetz. Mit einer entsprechenden VPN-Software kann der Beschäftigte im Home-Office sicher an das betriebliche/dienstliche Netzwerk angebunden werden.

17 Die Auflistung ist angelehnt an die Vorgabe des Bundesbeauftragten für den Datenschutz; vgl. Der Bundesbeauftragte für Datenschutz und Informationsfreiheit, Telearbeit – Ein Datenschutz-Wegweiser, S. 10 f.

18 Vgl. hierzu: Kramer, IT-Arbeitsrecht – Digitalisierte Unternehmen: Herausforderungen und Lösungen, S. 197.

19 Vgl. Fischer/Schierbaum, Telearbeit und Datenschutz – eine vernachlässigte Debatte, Computer und Recht, 6/98, S. 324.

20 Diese haben, wenn man § 22 Abs. 2 ArbSchG hinzuziehen will, nur in Ausnahmefällen ein Zutrittsrecht ohne Einwilligung des Beschäftigten bei Bestehen einer dringenden Gefahr für die öffentliche Sicherheit und Ordnung.

ÜBERBLICK

Besondere Datenkategorien

Bei folgenden Datenkategorien ist eine besondere Prüfung unerlässlich:

- Beschäftigten-Daten umfassen eine Fülle von personenbezogenen Daten, die gerade im öffentlichen Dienst ein umfassendes Bild des beruflichen Werdegangs wiedergeben. Diese Daten bedürfen eines besonderen Schutzes und unterliegen unter Umständen dem Personalaktenrecht nach den Beamtengesetzen bzw. dem Personalaktengeheimnis.
- Als besonders schutzwürdig gelten Sozialdaten nach § 67 SGB X. Diese Daten unterliegen dem Sozialgeheimnis, das die Verpflichtung umfasst, sicherzustellen, dass ausschließlich Befugte diese Daten nutzen dürfen. Oftmals unterliegt der zugriffsberechtigte Beschäftigtenkreis noch der besonderen Schweigepflicht nach § 203 StGB.
- Das BDSG und auch die DS-GVO deklarieren bestimmte Daten als »besondere Arten/Kategorien personenbezogener Daten«. Diese Daten werden als besonders sensibel und damit auch als besonders schützenswert eingestuft. Nach § 3 Abs. 9 BDSG handelt es sich um Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben einzelner Personen.

garantierte Unverletzlichkeit der Wohnung entgegen.[21] Deshalb bedarf es der Einwilligung des Beschäftigten und zusätzlich aller in der fraglichen Wohnung lebender, volljähriger Personen, damit Vertreter/innen der Dienststelle und des Personalrats den Home-Office-Arbeitsplatz in der Privatwohnung besichtigen dürfen. Das Zutrittsrecht sollte in zeitlicher wie auch in räumlicher Hinsicht auf das unbedingt Erforderliche beschränkt werden und mit einer vorherigen Anmeldung verbunden sein.[22] Es sollte in einer Dienstvereinbarung und auch einzelvertraglich geregelt werden.

Schulung der Beschäftigten

Die Beschäftigten, denen ein Telearbeitsplatz zu Hause eingeräumt wird, sollten in regelmäßigen Abständen für das Arbeiten im Home-Office geschult werden – vor allem hinsichtlich des Datenschutzes, der speziellen Besonderheiten von Arbeit im Home-Office und der einschlägigen innerbehördlichen Vorgaben, wie Regelungen in einer Dienstvereinbarung oder Vorgaben in Richtlinien (Merkblätter).[23] Solche Schulungsmaßnahmen gehören nach § 4g Abs. 1 Nr. 2 BDSG zu den Aufgaben des internen Datenschutzbeauftragten.[24] Mit der Anwendung der DS-GVO wird weiterhin die Schulung der Beschäftigten erforderlich sein, wobei dem internen Datenschutzbeauftragten lediglich ein Überwachungsrecht hinsichtlich »der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfung« zusteht (Art. 39 Abs. 1b DS-GVO).

Datenschutz-Pannen

Kommen personenbezogene Daten – auch bei der Arbeit im Home-Office – in unbefugte Hände, ist das eine so genannte »Datenschutz-Panne«. Die Dienststellenleitung wird dann diese Panne an die Datenschutz-Aufsicht melden müssen, und zwar unverzüglich und möglichst 72 Stunden nach dem Vorfall. Diese Vorgaben der Art. 33 und 34 DS-GVO gelten auch für öffentliche Stellen. Dienststellenleitung und auch die Beschäftigten sollten auf diese Situation vorbereitet sein und wissen, wie sie bei Datenverlust und/oder unbefugten Zugriff auf Daten zu reagieren haben.

Fazit

Der Personalrat sollte im Rahmen seiner Mitbestimmungsrechte[25] durch Abschluss einer Dienstvereinbarung[26] den Datenschutz der im Rahmen von Home-Office-Beschäftigten absichern. Vor dem Hintergrund der erforderlichen Umsetzung der DS-GVO bis zum 25.5.2018 sollten bestehende Dienstvereinbarungen überarbeitet werden. ◁

Bruno Schierbaum,
BTQ Niedersachsen GmbH,
Oldenburg.

»ACHT GEBOTE«

Nach der Anlage zu § 9 BDSG gelten »Acht Gebote« zum Datenschutz:

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Getrennte Verarbeitung

21 Vgl. hierzu Kramer (Hrsg.), IT-Arbeitsrecht, S. 198 f.
22 Vgl. Schwierung/Zurel, Das Homeoffice in der Arbeitswelt 2.0 – rechtliche Rahmenbedingungen für Telearbeit, Zeitschrift für Datenschutz 1/16, S. 19; vgl. hierzu auch BfDI, Telearbeit – ein Datenschutz-Wegweiser, S. 12 f.
23 Vgl. Brandl/Modlinger, Datenschutz-Praxis, 8/15, S. 9 f.
24 In vielen LDSG ist die Schulung der Beschäftigten nicht verankert.
25 Näher hierzu Witt, in diesem Heft ab S. 16.
26 Vgl. BfDI, Telearbeit – Ein Datenschutz-Wegweiser, S. 15.