SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz

Hinweise zum Homeoffice in Behörden und Betrieben

„Homeoffice“, „Telearbeit“, „mobiles Arbeiten“, zunehmend verlagert sich die Verarbeitung von personenbezogenen Daten aus den Büros und Dienststellen in den häuslichen Bereich. Der häusliche Arbeitsplatz wird mittels Informations- und Kommunikationstechnologie (IKT) mit dem Büro/der Dienststelle verbunden. Gelegentlich erfolgt auch ortsunabhängiges mobiles Arbeiten unter Einsatz von IKT.

Die Landesregierung hat mit dem Bericht zur Telearbeit in der Landesverwaltung Sachsen-Anhalt (LT-Drs. 7/5474) bereits im Dezember 2019 dargestellt, dass in einer Vielzahl von Landesbehörden die Möglichkeiten der Telearbeit genutzt werden. Zudem ist zur Förderung der Telearbeit eine Rahmenrichtlinie über flexibles Arbeiten in Telearbeit in der Landesverwaltung als Anlage zu diesem Bericht entwickelt worden. Der Bericht (Nr. 5.3) und die Rahmenrichtlinie (Nr. 4 und Nr. 8) haben bereits einige datenschutzrelevante Hinweise aufgenommen.

Infolge der Corona-Pandemie und der notwendigen Kontaktreduzierungen hat die Anzahl der Beschäftigten im Homeoffice/in Telearbeit nochmals erheblich zugenommen. In vielen Fällen ist die Telearbeit mit der Verarbeitung personenbezogener Daten verbunden, sodass auch im Hinblick auf den Datenschutz besondere Anforderungen zu bedenken sind. Die technischen und organisatorischen Anforderungen an den Telearbeitsplatz richten sich nach dem Schutzbedarf der zu verarbeitenden Daten. Je höher der Schutzbedarf, desto mehr Maßnahmen müssen ergriffen werden, um den gebotenen Schutz zu gewährleisten. Durch die Auslagerung der Verarbeitung in den häuslichen Bereich stehen dabei zunächst nicht mehr die Schutzmaßnahmen und Sicherheitsvorkehrungen zur Verfügung wie im betrieblichen/dienstlichen Bereich, sodass eine noch höhere abstrakte Gefährdung gegeben ist. Der Arbeitgeber/die Dienststelle bleibt aber der für die Verarbeitung der personenbezogenen Daten Verantwortliche nach Art. 4 Nr. 7 DS-GVO (s. auch Nr. 5.3 des Berichts und Nr. 11.1 der Rahmenrichtlinie). Die verbindlichen datenschutzrechtlichen Anforderungen gelten auch für diese Bereiche (s. Nr. 5.3 des Berichts). Es sind daher ergänzende technische und organisatorische Maßnahmen (Art. 32 DS-GVO) zu treffen, um durch Vorgaben und Einrichtungen zum Datenschutz und zur Datensicherheit das gebotene gleiche Datenschutzniveau zu erreichen (s. auch Nr. 11.2 der Rahmenrichtlinie). Auch besondere Situationen, wie in der Corona-Pandemie, suspendieren nicht von den gesetzlichen Vorgaben, deren Einhaltung gerade in der Krise Stabilität gewährleistet. Daher muss sich der Arbeitgeber/Dienstherr vor der Auslagerung von Datenverarbeitungen

mit einer Reihe von Fragen befassen, um den datenschutzrechtlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) hinreichend Rechnung zu tragen. Soweit dargestellt wird, dass Maßnahmen getroffen werden „sollten“, ist zu berücksichtigen, dass diese zumeist nicht freistehen, sondern vielfach aufgrund der Verarbeitungssituation, insbesondere im öffentlichen Bereich, als unumgänglich anzusehen sind.

I. Allgemeines

1. Werden Beschäftigte in (auch teilweiser bzw. sporadischer) Telearbeit mit der Verarbeitung personenbezogener Daten befasst und wenn ja, in welchem Umfang?

Bei der Auslagerung von Verarbeitungsvorgängen ist stets zu berücksichtigen, ob und inwieweit **personenbezogene** Daten erfasst sind. Art. 1 Abs. 1 DS-GVO gebietet den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Infolge des Schutzgebotes und insbesondere der notwendigen Prüfung der jeweils zu treffenden angemessenen Maßnahmen des Datenschutzes ist vor der Auslagerung der Datenverarbeitung eine entsprechende Betrachtung der vorgesehenen Prozesse durchzuführen. Je umfänglicher und sensibler die zu verarbeitenden Datenbestände werden, desto größer wird auch die Grundrechtsbetroffenheit. Auch aus der Sache heraus können sich im Einzelfall gesteigerte Schutzanforderungen ergeben (z. B. bei banalen Meldedaten, wenn der Betroffene mit Sprengstoff handelt).

2. Ist vor der Einrichtung von Telearbeit für eine konkrete Aufgabe jeweils geprüft worden, ob die Verarbeitung von personenbezogenen Daten im häuslichen Bereich erforderlich ist bzw. ob Alternativen gegeben sind?

Im Hinblick auf das Schutzgebot aus Art. 1 Abs. 1 DS-GVO und das Gebot der Datenminimierung aus Art. 5 Abs. 1 lit. c) DS-GVO ist vor der Einrichtung von Homeoffice/Telearbeit zu prüfen, ob die Arbeitsabläufe organisatorisch so geregelt werden können, dass sich für die auszulagernde Arbeit die Möglichkeit ergibt, auf personenbezogene Daten zu verzichten bzw. möglichst wenig Daten mit Personenbezug zu verarbeiten. Weiter ist in angemessenem Rahmen zu prüfen, ob es möglich ist, den zu verarbeitenden Datenbestand zu anonymisieren oder zumindest zu pseudonymisieren.

3. Sind für die jeweilige Aufgabe und die Art bzw. Kategorie der anfallenden Daten gesondert die Sensibilität der Daten, das Risiko durch die Art der vorgesehenen Verarbeitung und die gebotenen Schutzmaßnahmen geprüft worden? Ist diese Prüfung für die jeweilige Aufgabe dokumentiert worden?

Es ist stets vor der Auslagerung eine sorgfältige Prüfung der vorgesehenen Datenverarbeitungen durchzuführen, insbesondere in Bezug auf mögliche Auswirkungen im Fall eines Missbrauchs bzw. einer Verletzung der Sicherheit der Datenverarbeitung. Nach Art. 24 Abs. 1 DS-

GVO setzt der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Gemäß Art. 32 Abs. 1 DS-GVO hat er dabei ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Jeweils im Einzelfall sind für die zu verarbeitenden Daten der Schutzbedarf und das Risiko zu prüfen, um die erforderlichen Maßnahmen festzulegen, die das Risiko auf ein angemessenes Maß reduzieren (vgl. dazu Kurzpapier Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen“ der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder – Datenschutzkonferenz). Weiter ist zu berücksichtigen, dass der Verantwortliche die grundverordnungskonforme Verarbeitung auch nachzuweisen hat (Art. 5 Abs. 2 DS-GVO), sodass eine Dokumentation der Prüfung sinnvoll ist.

4. Welche Arten von personenbezogenen Daten werden in Telearbeit verarbeitet?

Es sollte vorab festgelegt sein, was für Daten (Gesundheitsdaten, Einkommensdaten, Kontaktdaten, Verhaltensweisen, Steuerdaten etc.) auf welchen Datenträgern in welcher Weise verarbeitet werden dürfen. Nach dem risikobasierten Ansatz der DS-GVO kommt es für die gebotene Sicherheit der Verarbeitung darauf an, ob für die jeweilige Datenart die risikobegrenzenden technischen und organisatorischen Maßnahmen zu den Rechten der Betroffenen in angemessenem Verhältnis stehen. Für die Bewertung des Risikos ist insbesondere auch der Schutzbedarf zu berücksichtigen (vgl. dazu Standard-Datenschutzmodell der Datenschutzkonferenz, Seite 42). Ein besonderer Schutzbedarf kann sich ergeben, wenn besondere Kategorien personenbezogener Daten (siehe Art. 9 Abs. 1 DS-GVO, u. a. Gesundheitsdaten, rassische und ethnische Herkunft, biometrische Daten) verarbeitet werden. Ein erhöhter Schutzbedarf kann sich auch aus einer gesetzlich bzw. berufsständisch gebotenen Verschwiegenheits- bzw. Schutzpflicht ergeben, wie beispielsweise in Bezug auf Personalaktendaten (Personalaktengeheimnis) oder Sozialdaten (Sozialdatengeheimnis).

5. Ist vor der Einrichtung der Telearbeit der betriebliche bzw. behördliche Datenschutzbeauftragte beteiligt worden?

Dem betrieblichen bzw. behördlichen Datenschutzbeauftragten obliegt nach Art. 39 Abs. 1 lit. a) DS-GVO die Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten hinsichtlich ihrer Pflichten nach dieser Verordnung. Eine Einbindung erscheint daher im Hinblick auf besondere Kompetenz und die Möglichkeit, durch persönliches Wirken des Datenschutzbeauftragten für die vielfältigen Risiken bei Homeoffice/Telearbeit zu sensibilisieren, sinnvoll. Der Datenschutzbeauftragte hat damit die Gelegenheit, die konkreten Arbeitsabläufe festzu-

stellen, die verschiedenen Risiken in Bezug auf den Datenbestand und die eingesetzten Verfahren zu bewerten und konkretisierte Empfehlungen zu geben. In Bezug auf den Datenschutzbeauftragten ist auch zu berücksichtigen, dass ihm die Möglichkeit der Kontrolle zur Erfüllung der Überwachungsaufgabe (Art. 39 Abs. 1 lit. b) DS-GVO) gegeben sein muss.

6. Gibt es eine Betriebsvereinbarung/Dienstvereinbarung zu Homeoffice/Telearbeit, die datenschutzrelevante Vorgaben enthält?

Die intensive Beteiligung der Interessenvertretung erscheint, soweit nicht ohne hin rechtlich geboten, sinnvoll. In einer Vereinbarung können die wesentlichen datenschutzrechtlichen Anforderungen und Verfahrensweisen festgelegt werden. Vorgaben werden transparent und für den einzelnen Beschäftigten nachvollziehbar. Seine Interessen können im Zusammenhang mit Sicherungsmaßnahmen, wie z. B. Protokollierungen für Kontrollzwecke, gewahrt werden.

7. Sind Beschäftigte, die Telearbeit verrichten, zuvor bezüglich der erhöhten Risiken und gebotenen Schutzmaßnahmen sensibilisiert worden, z. B. durch Belehrung oder schriftliche Verpflichtung?

Über die regelmäßige Schulung bzw. Fortbildung zu datenschutzrechtlichen Aspekten der jeweiligen Aufgaben der Beschäftigten hinaus ist es notwendig, für die hinreichende Sensibilität der in Homeoffice/Telearbeit Tätigen Sorge zu tragen. Dafür bleibt der Verantwortliche auch bei Verarbeitung außer Haus in der Verantwortung. In der Arbeit jenseits von Büro und Dienststelle sind vielfältige besondere Risiken enthalten, derer sich die Beschäftigten bewusst sein müssen, um Datenpannen zu verhindern. So sind z. B. Hinweise zur Sicherung (gegen Kenntnisnahme, (Einbruchs-)Diebstahl etc.) notwendig. Dies betrifft die Einrichtung des häuslichen Arbeitsplatzes, den Sichtschutz zur Vermeidung der Einsicht Unbefugter, Sperren des Gerätes und/oder Schließen der Fenster oder Terrassentüren beim Verlassen des häuslichen Arbeitsplatzes.

Besonderer Aufmerksamkeit bedarf das Öffnen von Links und Dokumenten, die ungewohnt erscheinen, da die Telearbeit u. U. nicht von den Schutzmaßnahmen zentraler Systeme profitiert. Mit Phishing Mails (Vortäuschen der Herkunft von seriösen Versendern wie z. B. Banken oder Onlinehändlern) ist zu rechnen, die Daten ausspähen und dazu inzwischen täuschend echt und in perfekter Sprache auftreten. Im Zweifel sollte eine Rückfrage beim vermeintlichen Absender erfolgen. Eine besondere Sensibilisierung ist daher geboten. Die Beschäftigten sollten spezifische Gefahren kennen, wie z. B. bezüglich unsicherer Transporte oder unzureichender Vernichtung. Sie sollten hinsichtlich der Vorgaben und der einzuhaltenden Verfahren instruiert werden. Einzuhaltende Sicherheitsmaßnahmen sollten genau beschrieben werden. Dies sollte im Rahmen einer schriftlichen Anweisung erfolgen (ggf. Aushändigung von Merk-

blättern). Durch entsprechende Vorgaben wird die weisungsgemäße Verarbeitung personenbezogener Daten (Art. 29 DS-GVO) umgesetzt und gleichzeitig dem Schutz von Betriebs- oder Dienstgeheimnissen Rechnung getragen. Ergänzend dient dies dem gebotenen Nachweis organisatorischer Maßgaben (Art. 5 Abs. 2 DS-GVO).

8. Gibt es allgemeine Vorgaben zur Einrichtung des häuslichen Arbeitsplatzes?

Auch der häusliche Arbeitsplatz muss angemessene Sicherheiten bieten. Zur Gewährleistung korrekten Handelns kann es sinnvoll sein, allgemeine Vorgaben zu machen zu Verfahrensfragen, zu einzuhaltenden Grundsätzen und zu einzelnen allgemeinen Verhaltensaspekten (z. B. Handlungsleitfaden). Dazu kann beispielsweise vorgegeben werden, unbefugte Einsichtnahmen, z. B. durch Mitbewohner oder Besucher, zu vermeiden, Unterlagen nach Arbeitsende vom Schreibtisch zu entfernen und sicher zu verschließen, das Mithören unbefugter Personen zu vermeiden oder dienstliche/betriebliche Datenbestände von privaten Daten zu trennen.

9. Gibt es ein den Gegebenheiten angepasstes Sicherheitskonzept für die Telearbeit?

Im Hinblick auf die vielfältigen Risiken durch den Prozess der Verlagerung der Verarbeitung erscheint es geboten, ein den besonderen Arbeitsbedingungen angepasstes Sicherheitskonzept zu erstellen. Darin können allgemeine und spezifische Maßnahmen und Vorgaben zur Datensicherheit zusammengefasst werden. Spezielle Risiken aus dem konkreten Verfahren und dem konkreten Geräteeinsatz können herausgearbeitet (Schutzbedarf) und Sicherheitsziele formuliert werden. Diese können mit den entsprechenden technischen und organisatorischen Maßnahmen verbunden werden (zu den verschiedenen Sicherheitsaspekten siehe die folgenden Fragen). Insbesondere in technischer Hinsicht können darin Festlegungen enthalten sein, wie z. B. zu Hard- und Softwarekomponenten. Auch die Verschlüsselung der Kommunikation (Ende-zu-Ende-Verschlüsselung, VPN), aktuelle Protokolle (z. B. mindesten TLS 1.2) oder Sicherheitskopien könnten benannt sein. Die Festlegungen können Empfehlungen aus den technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik aufnehmen. Im öffentlichen Bereich wären vorgegebene Mindeststandards einzubeziehen, wie z. B. Informationssicherheitsrichtlinien des Landes.

10. Ist eine Regelung zur Versendung dienstlicher E-Mails an private E-Mail-Postfächer erfolgt?

Eine Weiterleitung von betrieblichen/dienstlichen E-Mails an private Postfächer erscheint problematisch und sollte entfallen. Die für ggf. sehr sensible Daten gebotene umfassende Sicherung des digitalen Transports, die Sicherung der Verfügbarkeit und des Schutzes vor Zugriffen Fremder auf das private Postfach, wie z. B. sichere Verschlüsselungen, sind nur bedingt, durch den Arbeitgeber/Dienstherrn direkt gar nicht zu gewährleisten.

11. Wird für die Telearbeit ausschließlich von der Dienststelle/vom Betrieb kontrollierte und gewartete Technik (z. B. Laptop) eingesetzt oder ist auch die Nutzung privater (End)geräte vorgesehen bzw. gestattet?

Professionell administrierte Technik gewährleistet in hohem Maße Datensicherheit (z. B. in Bezug auf Firewall, Virenschutz, Malwareschutz, sichere Verbindungen, Verschlüsselungen). Für private Geräte dürfte wohl nur in Ausnahmefällen gewährleistet sein, dass die Konfiguration den betrieblichen/dienstlichen Sicherheitsanforderungen hinreichend Rechnung trägt. Dem Verantwortlichen ist in der Regel nicht die Möglichkeit gegeben, die Installation und Konfiguration der genutzten privaten Geräte sowie notwendige Aktualisierungen von (Sicherheits)Software zu steuern und zu prüfen. Private Geräte sind oft mit Anwendungen versehen, die sich bei der Installation umfassende Zugriffsrechte haben gewähren lassen. Mit der Nutzung von privaten Geräten im privaten Umfeld (Familie) erhöht sich auch die Gefahr, dass diese mit Schadsoftware infiziert werden. Weiter würde die notwendige Einrichtung von sicheren Arbeitsbereichen (u. a. Speicher) auf privaten Geräten entsprechende Fachkompetenz erfordern. Auf die Nutzung privater Endgeräte sollte daher, auch im Interesse der Vermeidung von Haftungsproblemen, verzichtet werden.

12. Wie, wie oft, in welchem Umfang und durch wen erfolgen Kontrollen hinsichtlich der Einhaltung der technischen und organisatorischen Vorgaben?

In Bezug auf technische und organisatorische Maßnahmen ist zu berücksichtigen, dass sich die Anforderungen im Laufe der Zeit beispielsweise infolge von technischen Entwicklungen ändern. Die Sicherung der Einhaltung organisatorischer Vorgaben kann ggf. die Überprüfung erfordern. Gemäß Art. 24 Abs. 1 Satz 2 DS-GVO sind getroffene Maßnahmen daher erforderlichenfalls zu überprüfen und zu aktualisieren.

13. Sind Regelungen zur Kontrolle durch den behördlichen Datenschutzbeauftragten/den Landesbeauftragten für den Datenschutz im häuslichen Bereich getroffen, insbesondere im Hinblick auf die Rechte von Mitbewohnern?

Der Datenschutzbeauftragte muss Kontrollmöglichkeiten haben (Art. 39 Abs. 1 lit. b) DS-GVO, s. o.). Ihm muss daher notfalls auch ein Zugang zum häuslichen Bereich möglich sein. Nach § 24 Abs. 1 DSAG-LSA ist dem Landesbeauftragten für den Datenschutz durch Behörden oder sonstige öffentliche Stellen jederzeit Zugang zu den Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung seiner Aufgaben notwendig sind, zu gewährleisten.

Eine vergleichbare Zugangsregelung sieht § 40 Abs. 5 BDSG im nicht-öffentlichen Bereich vor. Ein Zutritt zu Privatwohnungen ist jedoch grundsätzlich ausgeschlossen. Eine Verlagerung in den privaten Bereich darf die Verarbeitung aber nicht der Kontrolle entziehen. Um die

von der DS-GVO geforderten Kontrollen zu ermöglichen, bedarf es daher der Zustimmung der zu Hause Beschäftigten. Dazu ist vorab die Zustimmung des Beschäftigten einzuholen. Weiter ist im Hinblick auf die Auswirkung des Schutzes des Wohnungsgrundrechts (Art. 13 Abs. 1 GG) zu beachten, dass auch eventuelle Mitbewohner einverstanden sein müssen. Bei Widerruf der Zustimmung bzw. einer Zutrittsverweigerung ist die Telearbeit daher einzustellen.

14. In welchem Verfahren erfolgen die Beantragung und Genehmigung von Homeoffice/Telearbeit?

Zu Zwecken der Dokumentation und des Nachweises nach Art. 5 Abs. 2 DS-GVO erscheint es nötig, die Auslagerung der personenbezogenen Datenverarbeitung zu erfassen. Dies betrifft insbesondere auch die Frage, welche Akten und Geräte und Datenspeicher mitgenommen werden dürfen. Mit einem formalisierten Beantragungs- und Genehmigungsverfahren kann der Verantwortliche sicherstellen, dass eine Prüfung der Einhaltung der Vorgaben zu rechtskonformer Telearbeit erfolgt. Mit einer Verfahrensfestlegung könnte z. B. auch die Einbeziehung des betrieblichen/behördlichen Datenschutzbeauftragten sichergestellt werden oder auf Betriebs-/Dienstvereinbarungen bzw. -anweisungen verwiesen werden.

15. Welche Verfahrensvorgaben bestehen für Datenpannen?

Nach Art. 33 Abs. 1 DS-GVO ist im Falle einer Verletzung des Schutzes personenbezogener Daten grundsätzlich eine Meldung an die Aufsichtsbehörde geboten. Verletzungen der Sicherheit der Verarbeitung als Voraussetzung der Verletzung des Schutzes personenbezogener Daten können aufgrund der mit der Arbeitsverlagerung verbundenen Prozeduren in organisatorischer und technischer Hinsicht häufiger verbunden sein. Demgemäß sollte insbesondere bei längerer Telearbeit berücksichtigt werden, dass im gegebenen Fall kurzfristig eine Reaktion notwendig werden kann. Ist z. B. das genutzte Gerät mit Schadsoftware infiziert, ist umgehend der Arbeitgeber/Dienstherr zu informieren. Die weiteren Schritte sind abzustimmen. Zumeist wird eine Meldung einer Datenschutzverletzung notwendig werden. Hierfür sollte den Beschäftigten das Verfahren vorgegeben/bekannt sein.

16. Führen der Betrieb/die Dienststelle Verarbeitungen für andere Stellen in Auftragsverarbeitungen durch, die durch Homeoffice/Telearbeit erledigt werden?

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt i. d. R. auf der Grundlage eines Vertrages, der den Auftragsverarbeiter in Bezug die Verarbeitung bindet (Art. 28 Abs. 3 Satz 1 DS-GVO). Auftragsverarbeiter müssen hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen getroffen werden (Art. 28 Abs. 1 DS-GVO). Dies kann durch die Wahrnehmung der Auftragsverarbeitungsaufgaben im Wege des Homeoffice/der Telearbeit in Frage gestellt sein. Die Durchführung sollte im Auftragsverarbeitungsvertrag zumindest gestattet sein.

17. Erfolgt eine Auswertung des Nutzungsverhaltens der Beschäftigten hinsichtlich der IT-Geräte und wenn ja, in welchem Umfang und durch wen?

Beim IKT-Einsatz kann es in Betracht kommen, dass zur Überwachung Protokollierungen stattfinden müssen. Dabei ist zu beachten, dass auf den häuslichen Arbeitsplatz bezogenen IKT-Nutzungen nicht derart beobachtet werden können, dass ein unverhältnismäßiger Überwachungsdruck entsteht. Die Daten aus der häuslichen Arbeit dürfen nicht ohne gesonderte Grundlage zu Zwecken einer Leistungs- bzw. Verhaltenskontrolle ausgewertet werden.

18. Werden zur Erreichbarkeit der Beschäftigten bei der Telearbeit/im Homeoffice die private Telefonnummer oder E-Mail-Adresse verwandt? Wenn ja, auf welcher Rechtsgrundlage?

Die Anforderung der privaten E-Mail-Adresse und Telefonnummer, insbesondere der Mobilfunknummer ist i. d. R. im Rahmen eines Beschäftigungsverhältnisses nicht erforderlich. Die ständige Erreichbarkeit ist zu vermeiden. Grundsätzlich genügt die postalische Erreichbarkeit. Ausnahmen können sich aus dem konkreten Beschäftigungsverhältnis heraus ergeben (z. B. zwecks Erreichbarkeit in Notfällen nach Rufliste). Soweit die häusliche Arbeit eine telefonische Erreichbarkeit erfordert, kann eine Rufumleitung erfolgen, wenn der Beschäftigte einwilligt. Dabei ist den strengen Vorgaben hinsichtlich der Freiwilligkeit Rechnung zu tragen, die im Beschäftigungsverhältnis stets sorgfältig zu hinterfragen ist (Art. 7, Erwägungsgründe 32, 42, 43 DS-GVO).

19. Werden vom Dienstapparat Anrufumleitungen auf private Telefongeräte geschaltet?

Bei Rufumleitungen kommt es vor, dass dem Anrufer nicht die von ihm gewählte Nummer, sondern die des angewählten privaten Gerätes angezeigt wird. Die Verwendung der privaten Nummer mag für die Einrichtung einer häuslichen Erreichbarkeit nötig sein. Es erscheint aber nicht erforderlich, dem jeweiligen Anrufer die private Nummer des Beschäftigten zu übermitteln. Dies sollte daher vermieden werden. Im Telefon gespeicherte Kontakte in einer Anruferliste sollten kurzfristig gelöscht werden, da für eine längere Speicherung i. d. R. keine Rechtsgrundlage ersichtlich ist. Müssen für den Kontakt mit Dritten Kontaktdaten im Gerät gespeichert bleiben, ist der Zugriff von Dritten (z. B. auch durch auf dem Gerät installierte private Anwendungen) zu vermeiden (z. B. durch getrennte Speicherung).

II. Umgang mit Papierdokumenten

Für die Verarbeitung personenbezogener Daten in Papierform gelten für öffentliche Stellen in Sachsen-Anhalt die Regelungen der DS-GVO entsprechend (§ 3 Abs. 1 DSAG-LSA). Im nichtöffentlichen Bereich werden papiergebundene Verarbeitungen personenbezogener Daten grundsätzlich von der DS-GVO umfasst, wenn sie in einem Dateisystem verarbeitet werden

oder werden sollen (vgl. dazu Art. 2 Abs. 1, Art. 4 Nr. 6 DS-GVO) oder bei teilweiser automatisierter Verarbeitung (z. B. Hybrid-Akten). Im Rahmen von Vorgaben sollte auf die Datenminimierung und die Anforderungen der Integrität und Vertraulichkeit hingewiesen werden. Papierunterlagen sind sicher zu verwahren und vor dem unbefugten Zugriff bzw. der unbefugten Einsicht zu bewahren.

1. Wie werden Papierdokumente auf dem Transportweg in den häuslichen Bereich vor Verlust und Einsichtnahme geschützt?

Es sind konkrete Transportvorgaben notwendig, um die Verfügbarkeit und Vertraulichkeit der Daten zu gewährleisten. So sind Unterlagen stets in verschlossenen Behältern zu transportieren (Vermeidung des Einblicks des Sitznachbarn im öffentlichen Verkehrsmittel). Diese Behälter sind ständig zu bewachen. Es ist stets der direkte Weg zu nehmen (kein Liegenlassen im PKW auf dem Supermarktparkplatz).

2. Gibt es Vorgaben zur Aufbewahrung im häuslichen Bereich, insbesondere im Hinblick auf die Einsichtnahme Unbefugter oder Beschädigungen?

Es sind der Zugriff bzw. die Einsichtnahme von Unbefugten zu verhindern. Es ist wie sonst auch geboten, die Unterlagen grundsätzlich durch hinreichend sicheren Verschluss (Zugangstüren, Schrank, verschließbare Aktentasche) zu schützen. Auch beim kurzfristigen Verlassen des Arbeitsplatzes ist einem Zugriff vorzubeugen. Auch Beschädigungen von Unterlagen sind zu vermeiden (z. B. durch Bemalen durch Kinder).

3. Gibt es Vorgaben zur datenschutzkonformen Löschung bzw. Vernichtung von Unterlagen im häuslichen Bereich?

Soweit Papier mit personenbezogenen Daten vernichtet werden soll, ist der häusliche Papiermüll nicht der richtige Ort. Es sollte vorgegeben werden, die Vernichtung von Papier mit personenbezogenen Daten im Büro/in der Dienststelle vorzunehmen, um eine fachgerechte Löschung zu gewährleisten. Alternativ käme die Erlaubnis in Betracht, private Aktenvernichter zu nutzen, die die gebotene Sicherheitsstufe haben (mindestens Stufe 3 nach DIN 66399).

4. Gibt es Vorgaben zu Druckern?

Auf das Ausdrucken im Rahmen von Homeoffice/Telearbeit sollte weitestgehend verzichtet werden. Druckaufträge an private Drucker zu Hause könnten von diesen unnötig aufgezeichnet werden. Die Versendung von Druckaufträgen an Drucker beim Arbeitgeber/Dienstherren, die von mehreren Personen genutzt werden, kann dazu führen, dass Unbefugte Inhalte der Ausdrucke zur Kenntnis nehmen (Ausnahme: nur Befugte können den Ausdruck mittels PIN abrufen).

III. Nutzung dienstlicher Hardware

1. Welche Geräte werden für die Telearbeit genutzt (Notebook bzw. Laptop/Tablet bzw. Smartphone)?

Um die notwendigen Sicherheitsanforderungen zu erfüllen, sind die zu nutzenden Geräte entsprechend einzurichten. Es sollten daher einzelne Geräte festgelegt werden, die für diese Zwecke Verwendung finden sollen, um diese entsprechend vorzubereiten. Der Rückgriff auf nicht hinreichend administrierte Geräte sollte so vermieden werden. Im Hinblick auf Smartphones und vielfach auch Tablets ist zu berücksichtigen, dass diese Geräte oft mit vielfachen Anwendungen ausgestattet sind, die nur bedingt deaktiviert bzw. in ihrem Zugriff auf Daten eingeschränkt werden können.

2. Welche grundlegenden Maßnahmen des Zugriffsschutzes sind gegeben?

Die Einrichtung dienstlicher/betrieblicher Geräte muss die grundlegenden Sicherungsanforderungen berücksichtigen (Art. 5 Abs. 1 lit. f), Art. 25, Art. 32 DS-GVO). Dem durch die Verlagerung der Arbeit entstehenden Risiko ist angemessen zu begegnen. Es ist daher der unbefugte Zugang auch zu Hause zu vermeiden. Der Systemzugriff muss insbesondere von einem sicheren Passwort abhängig sein, triviale Passworte sind durch Vorgaben bzw. Voreinstellungen zu vermeiden. Bei laufendem Betrieb muss ein Bildschirmschoner den Zugriff versperren, wenn die Nutzung unterbrochen wird.

3. Sind die Geräte vor digitalen Angriffen geschützt? Welche Sicherheitsmaßnahmen sind getroffen worden?

Der Schutz der Geräte vor digitalen Angriffen setzt ein regelmäßiges Einspielen von aktuellen Software-Patches sowie Updates der Virensignaturen voraus. Die Aktualisierung von Programmen zur Abwehr von Schadsoftware zählt zu den grundlegend notwendigen Maßnahmen. Weiter ist der Schutz durch eine Firewall geboten.

4. Werden die verarbeiteten Daten auf den mobilen dienstlichen Geräten gespeichert und wenn ja, nach dem Stand der Technik verschlüsselt?

Werden im Rahmen der Aufgabenerfüllung personenbezogene Daten verarbeitet, sind diese kurzfristig zu sichern, möglichst automatisch. Grundsätzlich ist die Speicherung der verarbeiteten Daten auf zentralen dienstlichen Netzwerken vorzugswürdig. Dies gilt insbesondere bezüglich der Verarbeitung von sensiblen Daten oder großen Datenbeständen. Dort nehmen sie an der regelmäßigen Datensicherung teil. Wenn eine Speicherung von personenbezogenen Daten auf dem Gerät notwendig erscheint, ist eine Verschlüsselung nach dem Stand der Technik geboten. Hierzu bieten sich einmal die Verschlüsselungen auf Betriebssystemebene bzw.

mit den verwendeten Programmen (Schreibprogramm) an. Weiter ist spezielle Verschlüsselungssoftware geeignet. Bei der Speicherung auf mobilen Geräten ist, wie in zentralen Systemen, für eine regelmäßige Datensicherung Sorge zu tragen (z. B. Backups).

5. Erfolgt eine Anbindung des Gerätes der Telearbeit an die dienstlichen Systeme über den Router im häuslichen Bereich oder werden dienstliche Surfsticks oder mobile Router genutzt? Ist die Einbindung durch ein sicheres Verfahren erfolgt?

Insgesamt sollte für Homeoffice/Telearbeit vorab – ggf. differenziert nach Datenarten und Verarbeitungsumfang – festgelegt werden, welche betrieblichen/dienstlichen Kommunikationswege zu nutzen sind (z. B. Telefon, verschlüsselte E-Mail, VPN, mobile Datenträger, Fax). Die Internetnutzung sollte geregelt sein. Die Nutzung dienstlich bzw. betrieblich administrierter Ausrüstung (Surfstick, mobile Router) ist grundsätzlich zu bevorzugen. Wenn eine Verbindung über den Router im häuslichen Bereich erfolgt, ist zunächst der Kabelanschluss die erste Wahl (LAN). Die kabellose Verbindung (W-LAN) ist zu verschlüsseln. Dies muss dem Stand der Technik entsprechen (WPA2-Standard, Passwort).

6. Ist die Nutzung der dienstlichen Geräte für private Zwecke erlaubt (wenn ja, unter welchen Bedingungen) oder ausdrücklich untersagt?

Grundsätzlich ist die Untersagung der Nutzung von dienstlichen Geräten für private Zwecke vorzugswürdig. Soweit private Nutzung zugelassen werden soll, ist die Gefährdung im Zusammenhang mit dem Schutzbedarf der gespeicherten Daten zu prüfen. Der Nutzungsumfang sollte dann festgelegt werden. Eingeschränkte Nutzungen (Schreibgerät) sind weniger bedenklich, die Installation von Programmen und die Änderung der Systemkonfiguration sind nicht akzeptabel. Vorsicht ist insbesondere bei der Öffnung von nicht-dienstlichen Mails geboten. Im Hinblick auf eine gestattete private Nutzung von Internetdiensten, insbesondere betrieblichen/dienstlichen Mailpostfächern, ist zu berücksichtigen, dass der Verantwortliche damit zum Internetdiensteanbieter werden dürfte und es ihm somit verwehrt ist, ohne Einverständnis des Beschäftigten auf das Mailpostfach zuzugreifen.

7. Ist die Verbindung dienstlicher Geräte mit privaten Geräten zugelassen oder untersagt?

Der Anschluss privater Geräte (Festplatte, USB-Sticks, etc.) ist mit Sicherheitsrisiken verbunden, da zumeist nicht fachgerecht geprüft werden kann, ob diese Geräte von Schadsoftware befallen sind. Der Anschluss muss daher untersagt werden.

8. Erfolgt die Verbindung mit dem Unternehmens- oder Behördennetz bzw. zur betrieblichen/dienstlichen Anwendung über eine besonders gesicherte Verbindung?

Die Anbindung an das Unternehmens- bzw. Behördennetz muss hinreichend gesichert werden. Dazu ist eine verschlüsselte Verbindung (VPN) notwendig. Der für den Zugriff erforderliche Identitätsnachweis sollte durch die Kombination zweier unterschiedlicher und insbesondere von einander unabhängiger Komponenten erfolgen („Zwei-Faktor-Authentisierung"). Weiter muss sichergestellt werden, dass die Zugangsdaten zum zentralen System nicht auf dem Gerät gespeichert sind.

9. Sind Zugriffe auf betriebliche/dienstliche Server auf das für die Telearbeit Erforderliche begrenzt?

Der Fernzugriff auf betriebliche/behördliche Server sollte nicht das gesamte Netz des Arbeitgebers/der Dienststelle erfassen. Vielmehr sollte eine Anbindung lediglich an einen geschützten Teil der IT-Infrastruktur des Arbeitgebers/Dienstherren erfolgen. Der von außen zugängliche Teil sollte nur die Dienste zur Verfügung stellen, die für die Telearbeit genutzt werden sollen. Für den öffentlichen Bereich ist der verfassungsrechtliche Grundsatz der informationellen Gewaltenteilung zu beachten, wonach auch in der Telearbeit Beschäftigte nur Zugang zu den personenbezogenen Daten haben dürfen, die für ihre Aufgabenerfüllung unerlässlich sind. Im nicht-öffentlichen Bereich ist dieser Aspekt letztlich ebenso zu berücksichtigen, da die nicht notwendige Bekanntgabe von Daten an Beschäftigte, die diese nicht benötigen, eine unzulässige Verarbeitung darstellen dürfte.

10. Ist die Nutzung öffentlicher W-LAN-Hotspots gestattet und wenn ja, mit welchen zusätzlichen Sicherheitsvorgaben?

Mit der Nutzung von öffentlichen W-LAN-Hotspots sind infolge der Zahl der dort verbundenen Geräte mehr Gefahren verbunden, als mit der Verbindung über einen privaten Router. Auf die Nutzung sollte daher grundsätzlich verzichtet werden. Eine Nutzung wäre nur hinreichend sicher, wenn die Verbindung durchgängig VPN-verschlüsselt ist.

11. Erfolgt der Datenaustausch mit dem Gerät für die Telearbeit auch mittels USB-Sticks?

In allgemeinen Vorgaben bzw. Sicherheitskonzepten (s. o.) wäre auch festzulegen, ob und mit welchen Datenträgern ein Austausch stattfinden darf. Grundsätzlich ist der Datenaustausch über ein sicheres Netz zu bevorzugen. Auf die Verwendung verlustgefährdeter mobiler Datenträger wie USB-Sticks kann dann verzichtet werden. Wenn so verfahren wird, könnte die Nutzung von USB-Anschlüssen an dem genutzten Gerät nicht mehr notwendig sein. Dann empfiehlt sich, diese Anschlüsse für Speichermedien zu deaktivieren, zumindest aber, deren Nut-

zung ausdrücklich zu untersagen. Damit wird der (versehentliche) Anschluss von ggf. infizierten (privaten) Geräten ausgeschlossen. Ist die Nutzung von USB-Sticks nicht vermeidbar, sind die auf ihnen gespeicherten Daten nach dem Stand der Technik zu verschlüsseln. Weiter sind Vorgaben zum sicheren Transport erforderlich. Personenbezogene Daten sollten nur auf betriebliche/dienstliche Datenträger übertragen und zurückübertragen werden.

12. Gibt es in der Dienststelle einen kurzfristig erreichbaren Ansprechpartner für eventuelle technische Probleme?

Auch wenn die in Telearbeit Beschäftigten hinreichend sensibilisiert sind und klare Anweisungen haben, können - insbesondere technische - Probleme auftreten. Daher sollten für diese Probleme Ansprechpartner erreichbar sein, die helfen können.

13. Gibt es Vorkehrungen für den Verlustfall?

Die Nutzung mobiler Geräte birgt das Verlustrisiko. Zunächst müssten personenbezogene Daten, wenn sie auf dem Gerät gespeichert sind, verschlüsselt sein (s. o.). Um einem Verlust zu begegnen, ist der Weg zu sichern, d. h. die Geräte sollten verschlossenen transportiert werden. Es ist der direkte Weg zwischen Büro/Dienststelle und dem häuslichen Arbeitsplatz vorzugeben. Ein eventuelles Verlustrisiko sollte durch Sicherheitskopien aufgefangen werden. Für den Verlustfall sollte bei einer Verarbeitung von einer größeren Menge besonders sensibler Daten die Einrichtung einer Fernlöschungsmöglichkeit erwogen werden.

IV. Private Endgeräte

Ist die Nutzung von privaten Endgeräten für die Telearbeit gestattet? Sind konkrete Vorgaben für die Nutzung von privaten Geräten gegeben, insbesondere in Bezug auf Zugriffe, Sicherheit der Verarbeitung und die Anbindung an die betrieblichen/dienstlichen Systeme?

Aus Sicherheitsgründen sollte auf die Nutzung privater Geräte grundsätzlich verzichtet werden (s. o.). Ist die Nutzung privater Geräte unvermeidlich, sollten, wie bei betrieblichen/dienstlichen Geräten, umfassende Vorgaben hinsichtlich der Art und Umfang der Nutzung und der gebotenen Sicherheitsvorkehrungen gemacht werden. Ergänzend sind Hinweise und Maßnahmen in Bezug auf die besonderen Gefahren des privaten Gerätes geboten. Es sind für private Geräte die oben dargestellten Ausführungen zu den betrieblichen/dienstlichen Geräten entsprechend zu berücksichtigen.

Wie bei betrieblichen/dienstlichen Geräten ist insbesondere ein Zugriffsschutz geboten. Personenbezogene Daten sind vor dem Zugriff Unbefugter zu bewahren. Dies gilt vornehmlich

auch in Bezug auf die Gefahren, die sich aus zumeist auf privaten Geräten installierten privaten Anwendungen ergeben und Zugriffe auf bestimmte Datenbestände beinhalten. Entsprechende Installationen durch Arbeitgeber und Dienstherren auf privaten Geräten sind jedoch ohne Einwilligung des Betroffenen grundsätzlich nicht zulässig. Hinsichtlich der Einwilligung ist auf die strengen Anforderungen von Art. 7 DS-GVO (siehe auch Erwägungsgründe 32, 42 und 43 DS-GVO) zu verweisen.

Der Sicherung müssen Software- und Virenschutzaktualisierungen und eine Firewall dienen. Auf dem Gerät zu speichernde personenbezogenen Daten müssen verschlüsselt gespeichert sein. Die Anbindung an die IT-Struktur des Verantwortlichen setzt eine verschlüsselte Verbindung mit dem Router voraus. Die Kommunikation muss in einem verschlüsselten Netz ablaufen. Letztlich sind auch entsprechende Vorgaben für den Verlustfall zu machen.

Im Hinblick auf das erhöhte Risiko bei der Nutzung von privaten Geräten sind nicht vermeidbare Speicherungen getrennt von den privaten Daten vorzunehmen. Auf Computern ist dies durch die Einrichtung eines gesonderten, geschützten Kontos möglich. Neben anderen, gleich wirksamen Maßnahmen kommt auch ein Mobile Device Management in Betracht, um entsprechende Einstellungen sicherzustellen.

V. Mobiles Arbeiten

Ist mobiles Arbeiten gestattet? Wird den besonderen Gefährdungen durch Verarbeitungen an unterschiedlichen Orten Rechnung getragen?

Die Situation in Bezug auf die IT-Infrastruktur und die räumliche Sicherheit weicht bei mobilem Arbeiten (Hotelzimmer, Flughafen, Zug) noch stärker von der Lage im Betrieb/Büro ab als bei der Arbeit im häuslichen Bereich des Beschäftigten. Daher sind Vorgaben über die oben aufgeführten hinaus notwendig, die den gesteigerten Risiken angemessen begegnen. Es sollten daher die Örtlichkeiten beschrieben werden, an denen mobil bzw. auf keinen Fall mobil gearbeitet werden darf. Die Verarbeitung von Daten mit einem besonderen Schutzbedarf könnte eingeschränkt/untersagt werden. Die Nutzung bzw. das Ausschalten von Verbindungstechnologien des genutzten Gerätes muss festgelegt sein (Bluetooth, NFC, W-LAN im Hinblick auf öffentliche W-LAN-Hotspots). Weiter sind Aussagen notwendig, ob und inwieweit die Einbindung von genutzten Geräten in die Systeme Dritter zulässig sind. Dabei ist zu berücksichtigen, dass die Sicherheit von Systemen Dritter nicht zuverlässig beurteilt werden kann.

VI. Nutzung von Cloud-Diensten

1. Wenn Cloud-Dienste genutzt werden, wurde dann ein Vertrag nach Art. 28 DS-GVO geschlossen?

Im Rahmen von Homeoffice/Telearbeit kann es notwendig werden, Cloud-Dienste in Anspruch zu nehmen. Derartige Dienstleistungsverträge basieren zumeist auf Auftragsverarbeitungsverträgen (Art. 28 DS-GVO). Um rechtmäßig zu agieren, ist ein Vertrag des Verantwortlichen mit dem Auftragsverarbeiter nach Maßgabe des Art. 28 DS-GVO geboten. Insbesondere ist die Anforderung zu beachten, dass der Auftragsverarbeiter die hinreichende Garantie dafür bietet, dass geeignete technische und organisatorische Maßnahmen zur grundverordnungskonformen Verarbeitung getroffen sind. Weiter ist die Prüfung der Geeignetheit des Anbieters nach Art. 28 DS-GVO geboten, u. a. durch geeignete Dokumente bzw. Zertifizierungen. Die erfolgreiche Prüfung muss nachweisbar sein. Im Rahmen der Vereinbarungen sind auch wirksame Löschungsvorgaben vorzunehmen, um nicht erforderliche Datenverarbeitungen zu vermeiden (z. B. bei Beendigung des Vertrages).

2. Sind Zugriffssicherungen in Bezug auf die Cloud-Daten gegeben?

Der Zugriff auf die in der Cloud gespeicherten Daten bedarf eines starken Passwortschutzes. In Bezug auf administrative Konten sind Zwei-Faktor-Authentisierungen geboten. Weiter ist es sinnvoll, die Beschäftigten für die Risiken von Phishing-Attacken auch im Zusammenhang mit Cloud-Konten zu sensibilisieren.

3. Sind Transport- und Speicherverschlüsselung gegeben?

Für den Transport von personenbezogenen Daten auf den Server des Cloud-Dienste-Anbieters ist eine sichere Verschlüsselung nach dem Stand der Technik geboten (z. B. HTTPS). Auch für die Ruheverschlüsselung ist im Hinblick auf die Gebote der Datenminimierung und der Vertraulichkeit eine Verschlüsselung nach dem Stand der Technik notwendig. Weitere Hinweise finden sich in der Orientierungshilfe „Cloud-Computing“ der Datenschutzkonferenz.

4. Werden Anbieter aus sog. Drittstaaten (s. Art. 44 ff DS-GVO) eingebunden?

Bei der Einbindung von Diensteanbietern aus Drittstaaten ist das gleichwertige Datenschutzniveau zu gewährleisten. Dabei ist insbesondere zu berücksichtigen, dass ein Rückgriff auf die sog. Privacy-Shield-Zertifizierung von Anbietern aus den USA infolge des Urteils des Europäischen Gerichtshofs vom 16. Juli 2020 (AZ: C-311/18, „Schrems II“) nicht mehr möglich ist. Es muss daher durch Standarddatenschutzklauseln und weitere Maßnahmen im Zusammenwirken mit dem Anbieter die Einhaltung eines der DS-GVO vergleichbaren Datenschutzniveaus gesichert werden (weitere Hinweise hierzu auf meiner Homepage).

VI. Quellen und weitere Hinweise

Telearbeit und Mobiles Arbeiten, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Datenschutz: Plötzlich im Homeoffice – und nun?, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Datenschutzrechtliche Regelungen bei Homeoffice, Bayerisches Landesamt für Datenschutzaufsicht

Berliner Datenschutzbeauftragte zu Heimarbeit während der Kontaktbeschränkungen

Zu Videokonferenzen ist auf die Orientierungshilfe „Videokonferenzsysteme“ der Datenschutzkonferenz hinzuweisen.

Zur Nutzung privater Geräte (bring your own device) siehe den Beitrag Nr. 4.9 im XI. Tätigkeitsbericht auf meiner Homepage.

Einem Überblick und der Unterstützung für die Einrichtung von Homeoffice dient die „Checkliste Homeoffice“ auf meiner Homepage.

Impressum
Herausgeber:
Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Leiterstraße 9
39104 Magdeburg

Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt. de
https://datenschutz.sachsen-anhalt.de

Stand: Juli 2021