Landesbeauftragte
für Datenschutz
und Akteneinsicht

Technische und organisatorische Maßnahmen zur Umsetzung des Datenschutzes bei Heimarbeit

Stand: August 2025

Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Telefax: 033203 356-49
E-Mail: Poststelle@LDA.Brandenburg.de

www.LDA.Brandenburg.de

Inhaltsverzeichnis

1 Einführung

Dieses Dokument enthält Anforderungen, Empfehlungen und Hinweise zur Umsetzung von Datenschutz und Informationssicherheit bei der Heimarbeit. Es richtet sich sowohl an öffentliche als auch an nicht öffentliche Stellen.

Unter Heimarbeit verstehen wir das Arbeiten in einer privaten, häuslichen Umgebung des Beschäftigten (Homeoffice). Hierbei kann die Arbeit dauerhaft, zeitweise oder alternierend mit der Tätigkeit in der Behörde bzw. dem Unternehmen erfolgen. In jeder dieser drei Formen müssen die folgenden Anforderungen, Empfehlungen und Hinweise zugrunde gelegt werden. Das Arbeiten außerhalb der privaten, häuslichen Umgebung, wie z. B. im Café oder in der Bahn, wird hier explizit nicht betrachtet. Gleichwohl bestehen hinsichtlich der umzusetzenden Maßnahmen Gemeinsamkeiten.

Die Verarbeitung personenbezogener Daten im Homeoffice ist im Vergleich zur Verarbeitung innerhalb der Räumlichkeiten einer Behörde oder eines Unternehmens zusätzlichen Risiken für die Rechte und Freiheiten der betroffenen Personen ausgesetzt, welche durch geeignete Maßnahmen kompensiert werden müssen. Wichtig ist hierbei, dass der Arbeitsplatz im Homeoffice als Teil der Behörde bzw. des Unternehmens gilt und daher bereits vorhandene datenschutzrechtliche und informationssicherheitstechnische Anforderungen, welche sich maßgeblich aus Art. 5, 24, 25 und 32 Datenschutz-Grundverordnung (DS-GVO) ergeben, dort ebenfalls umzusetzen sind. Die weiteren Anforderungen resultieren z. B. aus den konkreten Verarbeitungstätigkeiten, der Art und dem Umfang der im häuslichen Bereich verarbeiteten personenbezogenen Daten, den lokalen Gegebenheiten, den zusätzlichen Risiken, dem Stand der Technik und dem erforderlichen Sicherheitsniveau. In jedem Fall bleibt die Behörde bzw. das Unternehmen Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO und kann diese Verantwortung nicht auf die Beschäftigten in Heimarbeit abwälzen.

Dieses Dokument enthält keine vollständige Liste an Anforderungen und Maßnahmen, sondern ist als Mindeststandard zu verstehen. Es wird eine Differenzierung zwischen normalem und hohem Risiko bei der Verarbeitung personenbezogener Daten sowie hinsichtlich „MUSS-“, „SOLLTE-“ und „KANN-“ Anforderungen vorgenommen. MUSS-Anforderungen sind immer umzusetzen. SOLLTE-Anforderungen können im Einzelfall durch eine Alternative ersetzt werden, die ein vergleichbares Schutzniveau garantiert. Die Entscheidung ist zu begründen und zu dokumentieren. Die Umsetzung einer KANN-Anforderung ist optional.

2 Konzeptionelle Vorarbeiten

2.1 Allgemeine Maßnahmen

Grundsätzlich MUSS der Verantwortliche (Behörde, Unternehmen) zunächst evaluieren, ob und unter welchen datenschutzrechtlichen Anforderungen sich eine Verarbeitung personenbezogener Daten überhaupt für das Homeoffice eignet. Vor dem Hintergrund, dass sich Papierunterlagen in der Regel schwerer schützen lassen als mittels Rechentechnik verarbeitete Daten, SOLLTE auf Erstere im Rahmen des Homeoffice weitestgehend verzichtet werden. Der Verantwortliche MUSS einschränkende Festlegungen treffen, welche Papierunterlagen im Homeoffice zulässig und welche unzulässig sind. Speziell bei Ver-

arbeitungen von personenbezogenen Daten, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen haben, MÜSSEN gesonderte Maßnahmen zur Herstellung eines adäquaten Schutzniveaus getroffen werden.

Es MUSS ein Datenschutz- und Sicherheitskonzept erarbeitet werden, welches auf lokale Gegebenheiten angepasst, regelmäßig aktualisiert und mit dem bereits bestehenden Konzept harmonisiert wird. Hierbei MÜSSEN insbesondere die in diesem Dokument aufgelisteten Anforderungen für die Heimarbeit berücksichtigt und gegebenenfalls ergänzt werden.

Wenn sich im Verlauf der Arbeiten herausstellt, dass durch die Datenschutz- und Sicherheitsmaßnahmen das im Rahmen der Heimarbeit entstehende Risiko für die Rechte und Freiheiten betroffener Personen nicht hinreichend eingedämmt werden kann, MUSS auf die Heimarbeit verzichtet werden.

Es MÜSSEN organisatorische Regelungen für das Homeoffice getroffen werden. Diese MÜSSEN insbesondere Vorgaben zur Erreichbarkeit von IT-Betreuung, Datenschutzbeauftragtem und Verantwortlichem, zur Kommunikation zwischen in Heimarbeit tätigen Beschäftigten, zum Austausch von Daten zwischen Behörde bzw. Unternehmen und Homeoffice, zur Aufbewahrung der Daten sowie zum Verhalten bei Datenschutzverletzungen, insbesondere bei Verlust von Unterlagen und Geräten, enthalten.

Der Verantwortliche (Behörde, Unternehmen) MUSS die Möglichkeit einer Kontrolle des Heimarbeitsplatzes haben, gleiches gilt für die zuständige Datenschutzaufsichtsbehörde. Soll eine Vor-Ort-Kontrolle des Heimarbeitsplatzes stattfinden, ist wegen des Grundrechts auf Unverletzlichkeit der Wohnung ein Einverständnis der betroffenen Personen erforderlich.

Es MUSS ein Nachweis der Einhaltung der Regelungen im Homeoffice gewährleistet werden. Hierzu SOLLTE die Behörde bzw. das Unternehmen als Arbeitgeber eine Checkliste für die Beschäftigten im Homeoffice ausarbeiten und sich die Einhaltung der Anforderungen durch sie per Unterschrift bestätigen lassen.

Schulung und Sensibilisierung:

- Die Beschäftigten MÜSSEN die entsprechenden Regelungen und Sicherheitsmaßnahmen kennen, hinsichtlich ihrer Umsetzung geschult und für die Gefahren des Homeoffice sensibilisiert werden.
- Schulungen und Sensibilisierungen MÜSSEN regelmäßig wiederholt werden. Die Durchführung MUSS dokumentiert werden.
- Alle relevanten Regelungen und Maßnahmen für die Heimarbeit SOLLTEN in Textform bereitgestellt werden.

2.2 Zusätzliche Maßnahmen bei hohem Risiko

Hat die Verarbeitung von personenbezogenen Daten im Homeoffice voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge, MÜSSEN die entsprechenden Gefahren explizit bei der Bestimmung und Umsetzung von Datenschutz- und Sicherheitsmaßnahmen berücksichtigt werden.

Der Verantwortliche MUSS in diesem Fall immer evaluieren, ob er nach den Maßgaben des Art. 35 DS-GVO eine Datenschutz-Folgenabschätzung durchzuführen hat.

3 Einrichtung des häuslichen Arbeitsplatzes

3.1 Allgemeine Maßnahmen

Es MUSS gewährleistet werden, dass zu keinem Zeitpunkt eine Kenntnisnahme, Veränderung oder Vernichtung der personenbezogenen Daten durch unbefugte Dritte erfolgt. Für die Vermeidung der Kenntnisnahme sind insbesondere die beiden nachfolgenden Aspekte zu berücksichtigen.

- Schutz gegen unbefugtes Einsehen, z. B. Fenster und Türen geschlossen halten, Bearbeitung im Erdgeschoss mit Fenster zur Straße vermeiden, Bearbeitung mit Rücken zum Fenster vermeiden, Sichtschutzfolien anbringen,

- Schutz gegen unbefugtes Mithören, z. B. Fenster und Türen geschlossen halten, Sprachassistenten deaktivieren, hellhörige Räume vermeiden, Vermeiden der Nennung personenbezogener Daten am Telefon.

Das Verschließen von Fenstern und Türen oder das Verlagern der Heimarbeit in höhere Etagen (falls möglich) sind auch geeignete Maßnahmen zur Vermeidung von unbefugter Veränderung oder Vernichtung personenbezogener Daten.

Der private Bereich und der häusliche Arbeitsplatz SOLLTEN durch Raumaufteilung getrennt sein. Der häusliche Arbeitsplatz SOLLTE sich in einem Raum befinden, der während der Arbeitszeit nicht von Dritten betreten wird. In Abhängigkeit von der Wohnsituation bedeutet dies beispielsweise, dass ein separater Raum und kein Durchgangszimmer zu wählen ist.

Steht kein separater Raum als Arbeitszimmer zur Verfügung, so MUSS der Verantwortliche sicherstellen, dass trotz der lokalen Gegebenheiten ein dazu äquivalentes Schutzniveau erreicht wird. Diese Bewertung MUSS gesondert in der allgemeinen Dokumentation der Heimarbeit berücksichtigt werden.

Es MUSS eine strikte Trennung von privaten und dienstlichen Tätigkeiten erfolgen.

- Private und dienstliche Dokumente bzw. Daten MÜSSEN stets getrennt sein.

- Werden dienstliche Tätigkeiten durch private Aktivitäten unterbrochen (z. B. Erledigung im Haushalt, Annahme eines Paketes), MUSS eine unbefugte Kenntnisnahme, Änderung oder Vernichtung der personenbezogenen Daten weiterhin ausgeschlossen werden.

3.2 Zusätzliche Maßnahmen bei hohem Risiko

Der Arbeitsplatz SOLLTE durch den Verantwortlichen (Behörde, Unternehmen) auf Tauglichkeit überprüft und das Ergebnis dokumentiert werden. Dabei ist insbesondere zu berücksichtigen, wie eine Trennung vom privaten Umfeld umgesetzt ist.

4 Aufbewahrung und Transport

4.1 Allgemeine Maßnahmen

Personenbezogene Daten MÜSSEN unabhängig vom Medium so verwahrt und transportiert werden, dass diese insbesondere vor Verlust und unbefugter Offenlegung sowie Veränderung geschützt sind. Dies gilt auch für Pausen u. a. Arbeitsunterbrechungen.

Dokumente und Geräte MÜSSEN sicher in einem verschlossenen (Transport-)Behältnis, welches gegen ungehinderte Entnahme und Einsichtnahme geschützt ist, transportiert werden. Das (Transport-)Behältnis SOLLTE durch den Verantwortlichen, KANN aber auch auf freiwilliger Basis durch den Beschäftigten bereitgestellt werden. Der Transport SOLLTE auf möglichst direktem Weg (z. B. kein Besuch in einem Café oder Ähnliches) erfolgen. Bei der Nutzung öffentlicher Verkehrsmittel MUSS besondere Sorgfalt gelten, insbesondere MUSS das (Transport-)Behältnis im öffentlichen Raum immer im Blick behalten werden.

Allgemein MUSS bei der Wahl des Aufbewahrungsortes von Dokumenten und Geräten, die Zugangsmöglichkeit sowie die Einsehbarkeit, insbesondere von außen (z. B. Fenster/Balkontüren), berücksichtigt werden.

Unter Punkt 5 sind allgemeine Maßnahmen für Hardware und Software aufgeführt, welche die zusätzlichen Risiken bei der Verarbeitung personenbezogener Daten im Homeoffice effektiv reduzieren. Für den Transport und die Aufbewahrung von personenbezogenen Daten auf Speichermedien und Geräten sind bspw. Verschlüsselung, starke Authentisierung und Backups geeignete zusätzliche Maßnahmen, um vor Verlust, Offenlegung und Veränderung zu schützen. Um Laptops und Speichermedien gegen Diebstahl zu schützen, MÜSSEN sie außerhalb des Sichtfelds von draußen (z. B. Fenster/Balkontüren) aufbewahrt werden.

Papierunterlagen haben gegenüber elektronischen Speichermedien und Geräten den Nachteil, dass sich darin befindliche personenbezogene Daten bei der Aufbewahrung und dem Transport nur schwer schützen lassen. Daher MUSS durch den Verantwortlichen geregelt sein, welche Daten und Unterlagen nach Hause transportiert bzw. dort zeitweise aufbewahrt werden dürfen. Wann immer möglich, MÜSSEN Kopien mit geschwärzten personenbezogenen Daten anstelle von Originalen mit ins Homeoffice genommen werden. Bei der Aufbewahrung MUSS zusätzlich darauf geachtet werden, dass unbefugte Dritte (Mitbewohner, Kinder, Besuch, ggf. Passanten) die Unterlagen nicht einsehen und nicht darauf zugreifen können. So sind geeignete Aufbewahrungsorte beispielsweise ein abgeschlossenes Arbeitszimmer mit Sichtschutz oder ein abgeschlossener Schrank bzw. Schreibtisch. Sofern kein geeigneter Aufbewahrungsort existiert, SOLLTE der Verantwortliche ein geeignetes Aufbewahrungsbehältnis bereitstellen.

4.2 Zusätzliche Maßnahmen bei hohem Risiko

Elektronische Speichermedien und Geräte MÜSSEN so transportiert und aufbewahrt werden, dass ein Diebstahl erheblich erschwert wird. So MUSS beispielsweise auch das unberechtigte Öffnen des (Transport-)Behältnisses erheblich erschwert werden. Entsprechend SOLLTE der Verantwortliche ein geeignetes (Transport-)Behältnis bereitstellen.

Wird ein Hardwaretoken mit PIN als zweiter Faktor für den Zugang zu DV-Systemen eingesetzt SOLLTE dieses sicher und getrennt von dem Gerät, das den Zugang vermittelt, aufbewahrt werden.

Es MÜSSEN Kopien mit geschwärzten personenbezogenen Daten anstelle von Originalen mit ins Homeoffice genommen werden. Es MUSS sichergestellt sein, dass durch die Schwärzung eine Reidentifizierung für Dritte unmöglich ist. Hierbei gilt zu beachten, dass auch diejenigen Daten zu schwärzen sind, die zwar nicht direkt personenbezogen sind, durch deren Kombination jedoch ein Personenbezug hergestellt werden könnte.

5 Hardware- und Software-Management

5.1 Allgemeine Maßnahmen

Für die Arbeit im Homeoffice SOLLTEN grundsätzlich behörden- bzw. unternehmenseigene Geräte verwendet werden. Private Geräte KÖNNEN in eng begrenzten und begründeten Ausnahmefällen freiwillig durch die Beschäftigten zur Verfügung gestellt werden.

Werden ausnahmsweise private Geräte genutzt, SOLLTEN technische Lösungen zur Trennung von Daten aus dem privaten Kontext gegenüber Daten aus dem dienstlichen bzw. geschäftlichen Kontext eingesetzt werden (z. B. Verschlüsselungen, Container- oder Virtualisierungsprodukte, sicher gebootete Umgebungen ggf. mit beschränkten Netzverbindungen).

Die genannten technischen Lösungen für die Datentrennung bzw. die privaten Geräte selbst MÜSSEN durch den Verantwortlichen administriert und so konfiguriert werden, dass sie mindestens das gleiche Sicherheitsniveau wie ein behörden- bzw. unternehmenseigenes Gerät erreichen.

Private Geräte MÜSSEN nach der Neukonfiguration wie ein unternehmenseigenes Gerät behandelt werden, wenn keine technischen Lösungen zur Trennung von privatem und dienstlichem bzw. geschäftlichem Kontext genutzt werden. So MÜSSEN z. B. auch bestehende Arbeitsanweisungen zur privaten Nutzung auf sie angewendet werden.

Nach der Nutzung eines privaten Gerätes MÜSSEN am Ende des Homeoffice-Zeitraumes die auf dem Gerät vorhandenen personenbezogenen Daten oder die dienstlich bzw. geschäftlich genutzte Umgebung unter Kontrolle der IT-Administration sicher gelöscht bzw. nach den Maßgaben der DIN 66399 vernichtet werden.

Alle IT-Geräte MÜSSEN mit technischen Maßnahmen so abgesichert sein, dass eine zweckwidrige Nutzung wesentlich erschwert wird. Dies SOLLTE vorrangig durch technische Maßnahmen umgesetzt werden (z. B. Gruppenrichtlinien, BIOS/UEFI-Einstellungen etc.).

Der Zugang zu im Homeoffice genutzten IT-Geräten wie PCs, Laptops oder Mobiltelefonen MUSS mit einem starken Passwort geschützt werden.

Es MUSS sichergestellt werden, dass nur befugte Personen Zugang zu den IT-Geräten und Zugriff auf die personenbezogenen Daten sowie die Gerätekonfiguration haben.

Die auf den Geräten eingesetzte Software MUSS durch den Verantwortlichen auf ihre datenschutzrechtliche Eignung geprüft, das Ergebnis begründet dokumentiert und die Nutzung freigegeben werden. Es MUSS eine vollständige und abgeschlossene Liste der im Homeoffice eingesetzten Software und IT-Geräte erstellt und aktuell gehalten werden.

Ist ein Zugriff aus dem Homeoffice auf Behörden- bzw. Unternehmensressourcen vorgesehen, MUSS dieser auf das für die Erfüllung der Arbeitsaufgaben im Homeoffice erforderliche Maß beschränkt werden (z. B. durch ein entsprechendes Berechtigungsmanagement).

Werden personenbezogene Daten im Homeoffice auf Datenträgern in IT-Geräten oder auf externen Medien gespeichert, MÜSSEN sie nach dem Stand der Technik verschlüsselt werden. So kann dem erhöhten Risiko durch Verlust oder Diebstahl von Geräten bzw. Datenträgern im häuslichen Kontext oder beim Transport begegnet werden.

Für alle Geräte mit Bildschirm SOLLTE eine Sichtschutzfolie verwendet werden.

Auf das Ausdrucken von Dokumenten im Homeoffice SOLLTE verzichtet werden. Ist es erforderlich, gelten für Drucker die oben getroffenen Aussagen zur Nutzung behörden- bzw. unternehmenseigener oder privater Geräte. Der Verbleib von personenbezogenen Daten im Druckerspeicher SOLLTE vermieden und der Drucker per Kabel direkt am PC, Laptop etc. angeschlossen werden.

5.2 Zusätzliche Maßnahmen bei hohem Risiko

Es MUSS immer behörden- bzw. unternehmenseigene Hardware eingesetzt werden.

Für die Authentifizierung des Nutzers MUSS eine 2-Faktor-Authentifizierung (2FA) zum Einsatz kommen (z. B. USB-Token mit PIN), spätestens wenn auf personenbezogene Daten zugegriffen werden kann (z. B. beim Start einer entsprechenden Anwendung).

6 Kommunikationsinfrastruktur

6.1 Allgemeine Maßnahmen

Die Verbindung zur Behörde bzw. zum Unternehmen MUSS nach dem Stand der Technik verschlüsselt erfolgen (z. B. ein sicherer VPN-Zugang, eine sichere Terminalservereinwahl, ein sicherer Webzugriff).

Die Authentizität der Kommunikationspartner MUSS sichergestellt werden.

Bei der Nutzung des privaten Internetanschlusses SOLLTE grundsätzlich eine Kabelverbindung zum Router hergestellt werden.

Wird eine WLAN-Verbindung genutzt, MÜSSEN eine WLAN-Verschlüsselung nach dem Stand der Technik sowie ein sicheres, langes und komplexes Passwort eingesetzt werden. Voreingestellte Passwörter MÜSSEN vor der ersten Verwendung des WLAN geändert werden.

Der private Router MUSS dem Stand der Technik entsprechen und über eine aktuelle Firmware sowie einen eingeschalteten Paketfilter verfügen.

6.2 Zusätzliche Maßnahmen bei hohem Risiko

Die Internetverbindung der im Homeoffice genutzten Geräte (PC, Laptop, Mobiltelefon) SOLLTE grundsätzlich über einen von der Behörde bzw. dem Unternehmen administrierten Router (z. B. UMTS/LTE-Router) oder direkt vom Gerät selbst über eine sichere Mobilfunkverbindung aufgebaut werden. Im begründeten Ausnahmefall KANN auch ein privater Router zum Einsatz kommen, wenn die Risiken zuvor analysiert und geeignete Maßnahmen wirksam beherrscht werden.

Die Verbindung mit dem Router MUSS grundsätzlich mittels Netzwerkkabel hergestellt werden. Ist dies z. B. aus baulichen oder arbeitsschutzrechtlichen Gründen nicht möglich, kann eine nach dem Stand der Technik verschlüsselte WLAN-Verbindung zum Router genutzt werden, falls ein sicherer VPN-Tunnel zwischen Endgerät (Laptop, PC) und Institution aufgebaut wird.

Der gesamte Datenverkehr MUSS mittels VPN in das eigene Behörden- bzw. Unternehmensnetzwerk getunnelt werden. Hierbei MUSS die Umsetzung so ausgestaltet sein, dass die Geräte von behörden- bzw. unternehmensinternen Firewalls profitieren. Öffentliche VPN Lösungen erfüllen diese Anforderung nicht.

7 Kommunikation zwischen Beschäftigten und Unternehmen

Beschäftigte, die sich in Heimarbeit befinden, MÜSSEN über dienstliche Belange informiert werden und ihrerseits über alle relevanten arbeitsbezogenen Aspekte informieren. Der Verantwortliche MUSS Regelungen für sichere und datenschutzgerechte Kommunikationskanäle treffen.

Sämtliche Kommunikationsmittel MÜSSEN den datenschutzrechtlichen Anforderungen entsprechen. Soweit möglich, SOLLTE auf die Übermittlung von personenbezogenen Daten verzichtet oder diese pseudonymisiert werden.

Kommunikation per E-Mail über unsichere Netze

- E-Mails, welche personenbezogene Daten enthalten, MÜSSEN verschlüsselt übertragen werden. Hier ist eine Transportverschlüsselung nach dem Stand der Technik ausreichend.

- E-Mails, welche personenbezogene Daten enthalten, deren Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen hat (z. B. Daten besonderer Kategorien nach Art. 9 DS-GVO), MÜSSEN im Regelfall zusätzlich nach dem Stand der Technik Ende-zu-Ende verschlüsselt werden (z. B. S/MIME, PGP oder verschlüsselter Dateianhang).

Kommunikation per Telefon

- Der Verantwortliche (Behörde, Unternehmen) MUSS eine Regelung zur Nutzung von (Mobil-) Telefonen/Smartphones im Behörden- bzw. Unternehmenskontext schaffen.

- Mit Einwilligung des bzw. der in Heimarbeit tätigen Beschäftigten KANN auch das Privatgerät genutzt werden. Anderenfalls MUSS ein dienstliches Gerät gestellt werden. Wird ein privates Mobiltelefon genutzt, so MUSS dieses nach den Vorgaben unter Punkt 5, Hardware- und Software-Management, behandelt werden. Dies betrifft auch die Administration der Geräte und die Freigabe von Apps.

- Werden auf den Telefonen Apps zu dienstlichen oder geschäftlichen Zwecken eingesetzt, so MUSS durch den Verantwortlichen deren datenschutzrechtliche Konformität überprüft und begründet dokumentiert sowie die Nutzung freigegeben werden.

Einsatz von Videokonferenzsystemen

- Werden Videokonferenzsysteme eingesetzt, MUSS die datenschutzrechtliche Konformität überprüft und begründet dokumentiert sowie die Nutzung freigegeben werden. Es sind die gängigen Sicherheitsmaßnahmen beim Einsatz von Videokonferenzsystemen zu beachten (z. B. passwortgeschützte virtuelle Konferenzräume, Verschlüsselung der Übertragung, datenschutzfreundliche Voreinstellungen). Bei der Übermittlung von Daten aus Videokonferenzen in Drittstaaten sind die rechtlichen Anforderungen der DS-GVO einzuhalten.

- Im Heimumfeld MUSS darauf geachtet werden, dass durch den Einsatz von Videokonferenzsystemen keine zusätzlichen datenschutzrechtlichen Risiken für Beschäftigte oder Dritte entstehen (z. B. durch Einblicke in die Privatsphäre oder das Erscheinen zufällig anwesender Personen im Bild).

8 Sonstiges

Datensicherung

- Personenbezogene Daten, welche in Heimarbeit verarbeitet werden, MÜSSEN in geeigneten und angemessenen Zeiträumen gesichert werden.
- Diese Sicherung MUSS entweder lokal oder auf einem zentralen Server erfolgen.
- Das gewählte Verfahren MUSS für die Art der Daten, die Umstände der Verarbeitung, die Art des Gerätes und die Risiken der Datenverarbeitung angemessen und geeignet sein.
- Die gewählten Verfahren MÜSSEN grundsätzlich automatisiert ausgeführt werden, um mögliche Fehlerquellen zu vermeiden.
- Bei einer lokalen Datensicherung SOLLTE ein Backup-Datenträger in der Behörde bzw. im Unternehmen hinterlegt werden.

Löschen und Vernichten

- Personenbezogene Daten, die im Homeoffice verarbeitet werden, MÜSSEN entsprechend den Richtlinien des Verantwortlichen sicher gelöscht werden – spätestens, wenn sie nicht mehr benötigt werden.
- Dokumente und Datenträger, welche personenbezogene Daten enthalten, MÜSSEN ebenfalls entsprechend den Richtlinien des Verantwortlichen und nach DIN 66399 sicher vernichtet oder sicher zur Behörde bzw. zum Unternehmen transportiert und dort vernichtet werden.
- Ist die Vernichtung im Homeoffice vorgesehen, MÜSSEN die nach DIN 66399 benötigten Geräte bereitgestellt werden. Sollen die Daten im Unternehmen vernichtet werden, so MUSS ein Transportbehältnis wie unter Punkt 3, Aufbewahrung und Transport, zur Verfügung gestellt werden.

Fernwartung

- Es SOLLTE ein spezielles Betreuungs- und Wartungskonzept für die im Homeoffice verwendete Informationstechnik entwickelt werden. Darin SOLLTEN insbesondere die Punkte Ansprechpartner für die Beschäftigten, (regelmäßige) Wartungstermine, Fernwartung, Verhalten bei Geräteausfällen und Transport wartungsbedürftiger IT-Geräte geregelt werden.
- Alle für die Fernwartung nicht relevanten Dokumente MÜSSEN vor deren Beginn geschlossen werden.
- Die Beschäftigten MÜSSEN bei der Fernwartung anwesend sein, um diese zu kontrollieren.

Private Nutzung dienstlicher Geräte im Homeoffice

- Im Homeoffice gelten zunächst die behörden- bzw. unternehmensspezifischen Vorgaben für die private Nutzung dienstlicher Geräte.

- Die private Nutzung durch Dritte (z. B. Kinder, Partner, Mitbewohner) MUSS ausgeschlossen werden. Darüber hinaus KÖNNEN Verantwortliche weitere Einschränkungen oder Verschärfungen vornehmen.

9 Literaturhinweise

Dokumente der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

- Standard-Datenschutzmodell Version 3.1
  https://www.datenschutzkonferenz-online.de => Infothek => Anwendungshinweise => 2024

- Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail
  https://www.datenschutzkonferenz-online.de => Infothek => Orientierungshilfen => 2021

- Orientierungshilfe Videokonferenzsysteme
  https://www.datenschutzkonferenz-online.de => Infothek => Orientierungshilfen => 2020

- Kurzpapier Nr. 5 zur Datenschutz-Folgenabschätzung
  https://www.datenschutzkonferenz-online.de => Infothek => Kurzpapiere => Kurzpapier 5

Dokumente des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

- BSI-Grundschutz: Baustein zur Telearbeit
  https://www.bsi.bund.de => Themen => IT-Grundschutz => IT-Grundschutzkompendium => OPS: Betrieb => OPS.1.2.4 Telearbeit

- BSI-Grundschutz: Baustein zur Einrichtung des häuslichen Arbeitsplatzes
  https://www.bsi.bund.de => Themen => IT-Grundschutz => IT-Grundschutzkompendium => INF: Infrastruktur => INF.8 Häuslicher Arbeitsplatz

- BSI-Grundschutz: Baustein zum Mobilen Arbeiten
  https://www.bsi.bund.de => Themen => IT-Grundschutz => IT-Grundschutzkompendium => INF: Infrastruktur => INF.9 Mobiler Arbeitsplatz

- BS-Grundschutz: Baustein zu VPN
  https://www.bsi.bund.de => Themen => IT-Grundschutz => IT-Grundschutzkompendium => NET: Netze und Kommunikation => NET.3.3 VPN

- BSI-Grundschutz: Baustein zur Fernwartung
  https://www.bsi.bund.de => Themen => IT-Grundschutz => IT-Grundschutzkompendium => OPS: Betrieb => OPS.1.2.5 Fernwartung

- BSI-Grundschutz: Umsetzungshinweise zum Baustein Identitäts- und Berechtigungsmanagement, u. a. mit Informationen zum Berechtigungsmanagement und zur Passwortlänge
  https://www.bsi.bund.de => Themen => IT-Grundschutz => IT-Grundschutzkompendium => Umsetzungshinweise => ORP.4: Identitäts- und Berechtigungsmanagement

- Technische Richtlinien zu kryptographischen Verfahren
  https://www.bsi.bund.de => Themen => Unternehmen und Organisationen => Standards und Zertifizierung => Technische Richtlinien => BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

- Maßnahmen zur Behandlung eines IT-Sicherheitsvorfalls
  https://www.bsi.bund.de => Themen => Unternehmen und Organisation => IT-Sicherheitsvorfall

- Maßnahmenkatalog zum Notfallmanagement und zur Überprüfung der eigenen Umsetzung
  https://www.bsi.bund.de => Themen => Unternehmen und Organisation => Cyber-Sicherheitsempfehlungen nach Angriffszielen => Unternehmen allgemein => IT-Notfallkarte => Maßnahmenkatalog zum Notfallmanagement

Dokumente weiterer Autoren

- Bundesverband IT-Sicherheit e.V. (TeleTrusT): Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen
  https://www.teletrust.de => Publikationen => Broschüren => Stand der Technik

- Material zur Sensibilisierung von Mitarbeitern für die Gefahren des Phishing
  https://www.verbraucherzentrale.de => Menü => Digitale Welt => Phishing-Radar => Phishing-Mails: Woran Sie sie erkennen und worauf Sie achten müssen

- Material der Allianz für Cybersicherheit
  https://www.allianz-fuer-cybersicherheit.de => Informationen und Empfehlungen

Der Zugriff auf die Links erfolgte zuletzt am 28. August 2025.