Handreichung zum datenschutzkonformen „mobilen Arbeiten“

Stand: 21.12.2023

Inhaltsverzeichnis

Hinweise zum mobilen Arbeiten 3
Telearbeit, Home-Office und mobiles Arbeiten 3
Datenschutzrechtliche Grundlagen zum mobilen Arbeiten 3
Technische Maßnahmen, um im Zusammenhang mit dem mobilen Arbeiten ein dem Risiko angemessenes Schutzniveau zu gewährleisten 4
Organisatorische Maßnahmen, um im Zusammenhang mit dem mobilen Arbeiten ein dem Risiko angemessenes Schutzniveau zu gewährleisten: 6
Weitere Veröffentlichungen zu dem Thema 10

Das „mobile Arbeiten“ hat – nicht zuletzt während der Corona-Pandemie – eine zentrale Bedeutung in der Arbeitswelt erlangt.

Um ein datenschutzkonformes Arbeitsumfeld zu schaffen, ist der Arbeitgeber zum Ergreifen besonderer technischer und organisatorischer Schutzmaßnahmen und der Arbeitnehmer zur Einhaltung besonderer Verhaltensregeln angehalten. Die nachfolgenden Hinweise sollen eine erste Orientierung für ein datenschutzkonformes mobiles Arbeiten bieten.

Hinweise zum mobilen Arbeiten

Telearbeit, Home-Office und mobiles Arbeiten

Gesetzlich geregelt ist allein die **Telearbeit** in § 2 Abs. 7 Verordnung über Arbeitsstätten (ArbStättV). Hiernach sind Telearbeitsplätze vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten. Dabei übernehmen Arbeitgeber sowohl die Einrichtung des Arbeitsplatzes der Beschäftigten als auch die daraus entstehenden Kosten.

Home-Office ist hingegen umgangssprachlich geprägt und meint typischerweise die Ausübung der beruflichen Tätigkeit von zu Hause unter Einsatz von Telekommunikation.

Mobiles Arbeiten meint die Erbringung der geschuldeten Arbeitsleistung unter Verwendung von Informationstechnologie außerhalb der Betriebsstätte. Hierunter fällt die Arbeit im heimischen Büro und das Arbeiten unterwegs, zum Beispiel in der Bahn. Das mobile Arbeiten umfasst daher sowohl Aspekte der Telearbeit als auch des Home-Office.

Datenschutzrechtliche Grundlagen zum mobilen Arbeiten

Die Datenschutz-Grundverordnung (DS-GVO) und das Bundesdatenschutzgesetz (BDSG) kennen keine Ausnahmen oder Spezialregelungen für das mobile Arbeiten. Werden personenbezogene Daten gem. Art. 4 Nr. 1 DS-GVO verarbeitet, so sind die datenschutzrechtlichen Regelungen der DS-GVO und des BDSG zu beachten.

Arbeitgeber bleiben **Verantwortliche** für die Verarbeitung personenbezogener Daten i.S.d. Art. 4 Nr. 7 DS-GVO. Das bedeutet, dass sie nach Art. 5 Abs. 2 DS-GVO für die Einhaltung der Grundsätze der Verarbeitung des Art. 5 Abs. 1 DS-GVO verantwortlich sind und deren Einhaltung nachweisen müssen. Die Beschäftigten verarbeiten personenbezogene Daten nach Art. 29 DS-GVO auf Weisung der Arbeitgeber. Entsprechend müssen Arbeitgeber auch im Bereich der mobilen Arbeit für die Umsetzung und Einhaltung der datenschutzrechtlichen Anforderungen sorgen und haften in der Konsequenz für mögliche Verstöße.

Arbeitgeber, die selbst **Auftragsverarbeiter** nach Art. 4 Nr. 8 DS-GVO sind, müssen außerdem ihre vertraglich übernommenen Verpflichtungen (Auftragsverarbeitungs-verträge im Sinne von Art. 28 DS-GVO) daraufhin überprüfen, ob die Verarbeitung personenbezogener Daten im Rahmen des mobilen Arbeitens möglicherweise ausgeschlossen ist.

- ⇨ Leitlinien des EDSA zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO
- ⇨ Kurzpapier Nr. 13 der DSK zur Auftragsverarbeitung, Art.28 DS-GVO

Mit Blick auf die Thematik des mobilen Arbeitens steht für Verantwortliche insbesondere der Grundsatz der **Integrität und Vertraulichkeit** des Art. 5 Abs. 1 Buchstabe f DS-GVO im Vordergrund, der durch Art. 32 DS-GVO konkretisiert wird.

Nach Art. 32 Abs. 1 DS-GVO treffen Verantwortliche und Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des

Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten**.

Bei der Bestimmung der zu ergreifenden technischen und organisatorischen Maßnahmen gem. Art 32 Abs. 1 DS-GVO ist – trotz fehlender spezieller Regelung – den besonderen, mit dem mobilen Arbeiten einhergehenden Gefahren Rechnung zu tragen. Im Rahmen der Risikobetrachtung ist daher zunächst das aus dem mobilen Arbeiten resultierende Risiko zu ermitteln und zu bewerten. Als konkrete Beispiele sind etwa die beschränkte Einwirkungs- und Kontrollmöglichkeit der Arbeitgeber (aufgrund der räumlichen Trennung) sowie die Nutzung technischer Einrichtungen außerhalb ihres Einflussbereichs (z.B. Gebrauch des privaten Internetanschlusses der Beschäftigten) zu nennen.

Weiterhin ist zu prüfen, ob aufgrund des mit dem mobilen Arbeiten einhergehenden Risikos für die Rechte und Freiheiten betroffener Personen eine **Datenschutz-Folgenabschätzung** gem. Art. 35 DS-GVO durchzuführen ist. Zu denken ist in diesem Zusammenhang an die besonderen Risiken des Datenverlustes, Datenmissbrauchs oder des Zugriffs durch unbefugte Dritte, wodurch Gefahren für die Vertraulichkeit, die Integrität und die Verfügbarkeit personenbezogener Daten entstehen können.

- ⇨ Kurzpapier Nr. 18 der DSK Risiko für die Rechte und Freiheiten natürlicher Personen
- ⇨ Kurzpapier Nr. 5 der DSK Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
- ⇨ Leitlinien des EDSA zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“

Vor dem Hintergrund der datenschutzrechtlichen Anforderungen an das mobile Arbeiten empfiehlt sich insbesondere die Berücksichtigung der nachfolgenden Hinweise.

Technische Maßnahmen, um im Zusammenhang mit dem mobilen Arbeiten ein dem Risiko angemessenes Schutzniveau zu gewährleisten

- Den Beschäftigten ist, soweit möglich, die für ihre Arbeit notwendige Ausstattung (Laptop, Mobiltelefon, Drucker etc.) in Form von **Firmengeräten** zur Verfügung zu stellen.

- Bei allen genutzten Endgeräten (Laptop, Mobiltelefon, Tablet etc.) müssen angemessene und wirksame Sicherheitseinrichtungen umgesetzt sein. Hierzu zählen bspw. die **Verschlüsselung von Speichermedien**, **Firewalls** und **Virenschutzprogramme**. Ferner muss sichergestellt werden, dass **Sicherheits-updates** auf allen Endgeräten unverzüglich eingespielt werden. Mobil genutzte Endgeräte sollten aus der Ferne verwaltet bzw. kontrolliert werden können, etwa mittels eines Mobile Device Management-Systems.

  - ⇨ Empfehlungen des BSI zur Firewall
  - ⇨ Empfehlungen des BSI zum Patch und Änderungsmanagement

- Um einen sicheren Zugriff auf die Unternehmensinfrastruktur zu gewährleisten, bedarf es sicherer, autorisierter und authentifizierter Verbindungen. Es empfiehlt sich die Nutzung eines über entsprechende Zertifikate abgesicherten **VPN-Tunnels**. Die gesamte (Daten-) Kommunikation sollte, soweit möglich, über dieses VPN und damit die gesicherte IT-Infrastruktur des Verantwortlichen geleitet werden. Nur in begründeten Ausnahmefällen sollte auf einzelne IT-Dienste oder Anwendungen direkt über das Internet zugegriffen werden, wobei stets eine Risikoabwägung durchzuführen ist. Sollen Cloud-Speicher

verwendet werden, so ist bei diesen darauf zu achten, dass sie den datenschutzrechtlichen Anforderungen genügen.

⇨ Empfehlungen des BSI zu Virtuellen Privaten Netzwerken
⇨ Kurzpapier Nr. 18 der DSK Risiko für die Rechte und Freiheiten natürlicher Personen

- Zusätzlich bietet es sich an, den Zugriff auf Anwendungen und Kommunikationskanäle über einen **Terminalserver** oder eine **Remote-Client-Umgebung** laufen zu lassen.

- Bei der Nutzung von privaten Internetanschlüssen der Beschäftigten ist darauf zu achten, dass auch diese sicher eingerichtet sind, analog zu firmeneigenen Endgeräten hinsichtlich sicherheitsrelevanter Updates auf dem aktuellen Stand gehalten werden und bestenfalls eine Verbindung per LAN oder über ein (zumindest) mit WPA2, besser mit WPA3, verschlüsseltes **WLAN-Netzwerk** hergestellt wird.

- Es sollten nur Endgeräte genutzt werden, die von den Herstellern unterstützt werden.

- Besondere Vorsicht ist bei der Nutzung **öffentlicher Internetzugänge** geboten, z.B. in Hotels oder an Flughäfen. Eine Nutzung sollte nur in Ausnahmefällen und unter der Voraussetzung erfolgen, dass entsprechende technische und organisatorische Maßnahmen umgesetzt wurden, z.B. die ausschließliche Netzwerkkommunikation über VPN-Tunnel (s.o.).

  ⇨ Sicherheitstipps im privaten und öffentlichen WLAN des BSI

- Die Zugriffskontrolle für die IT-Infrastruktur des Unternehmens ist mittels einer **Multi-Faktor-Authentifizierung** vorzunehmen. Gängig ist hier bislang die Zwei-Faktor-Authentifizierung (2FA), welche in der Regel aus einem sicheren Passwort, für das es eine Passwortrichtlinie geben muss, und einem weiteren Authentifizierungsfaktor besteht. Grundsätzlich stehen die folgenden Arten von Authentifizierungsfaktoren zur Verfügung:

  - Wissensfaktoren (z.B. Passwörter, PIN-Codes)
  - Besitzfaktoren (z.B. TAN-Geräte, SIM-Karte für SMS, Chipkarte, Token)
  - Inhärenzfaktoren (z.B. Fingerabdruck, Gesichtserkennung), sofern deren Einsatz datenschutzrechtlich zulässig ist.

  Für eine wirksame 2FA ist es erforderlich, dass die eingesetzten Faktoren von unterschiedlicher Art sind.

  ⇨ Handlungsempfehlung der LfD Niedersachen zur sicheren Authentifizierung
  ⇨ Empfehlungen des BSI zur Zwei-Faktor-Authentisierung
  ⇨ Empfehlungen des BSI zur Erstellung sicherer Passwörter
  ⇨ Empfehlungen des BSI zum Identitäts- und Berechtigungsmanagement

- Alle **Geräte** (Laptop, Mobiltelefon, Tablet etc.) sowie alle weiteren **Datenträger** (USB-Sticks, externe Festplatten etc.) sind nach dem Stand der Technik zu **verschlüsseln**.

- Der Anschluss **privater Hardware** (auch Drucker und Scanner) sollte verboten und – soweit technisch möglich – **blockiert** werden.
- Aufgrund der größeren Verlustgefahr mobiler Geräte und Datenträger sind Dateien vorzugsweise auf den Unternehmensservern und **nicht lokal zu speichern**. Ist eine lokale Speicherung unumgänglich, können **regelmäßige Backups** der größeren Gefahr des

Datenverlustes entgegenwirken, um hierdurch dem Schutzziel der Verfügbarkeit Rechnung zu tragen.

- Um bei dem Verlust oder Diebstahl von Geräten die Vertraulichkeit der Daten sicherzustellen, sind auf diesen **Remote-Wipe-Lösungen** zu installieren. Auch Hardware-Token sollten eine **Sperrung** im Verlustfall ermöglichen. Ebenfalls kann – neben der Verschlüsselung – eine automatisierte Löschung des Geräts bei wiederholter Falscheingabe von Passwörtern z.B. zur Verhinderung erfolgreicher Brute-Force-Attacken eine sinnvolle Maßnahme sein.

- Werden mobile Endgeräte (z.B. das Mobiltelefon) auch zur privaten Nutzung freigegeben, so ist eine strikte Trennung (d.h. separierte Bereiche ohne Möglichkeit der Interaktion) von privaten und beruflichen Dateien, Dokumenten und Programmen sicherzustellen, z.B. mittels einer **Container-Lösung**.

- **Messenger** zur dienstlichen Kommunikation sind ausschließlich über die Firmengeräte zu nutzen. Dabei ist auf den Einsatz datenschutzrechtskonformer Lösungen zu achten. So muss neben einer Ende-zu-Ende-Verschlüsselung z.B. auch ausgeschlossen werden, dass der Anbieter Informationen darüber erhält, speichert oder verarbeitet, wer mit wem kommuniziert hat.

  ⇨ „Whitepaper“ der DSK Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich

- Beim Einsatz von **Videokonferenzsystemen** sind über die allgemeinen datenschutzrechtlichen Anforderungen hinaus die besonderen Umstände des mobilen Arbeitens zu berücksichtigen. Dies gilt insbesondere auch hinsichtlich des etwaigen Einsatzes aus dem privaten Bereich von Beschäftigten heraus, etwa aus Privatwohnungen. Hier sind angemessene und wirksame technische und organisatorische Maßnahmen zu ergreifen.

  ⇨ Orientierungshilfe der DSK Videokonferenzsysteme
  ⇨ Checkliste der DSK Datenschutz in Videokonferenzsystemen
  ⇨ Handreichung „Videokonferenzsysteme – Hinweise zur praktischen Nutzung“ des LfDI Baden-Württemberg
  ⇨ Webseite des HBDI „Videokonferenzsysteme“

Organisatorische Maßnahmen, um im Zusammenhang mit dem mobilen Arbeiten ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

- Bei der **räumlichen Gestaltung** des Arbeitsplatzes haben Beschäftigte darauf zu achten, dass von ihnen verarbeitete **Daten nicht einsehbar** sind. Wird von unterwegs und nicht im privaten häuslichen Umfeld gearbeitet, so ist hierbei neben Passantinnen und Passanten auch auf Überwachungskameras zu achten. Grundsätzlich empfiehlt sich beim mobilen Arbeiten der Einsatz von **Sichtschutzfolien** auf den Bildschirmen der genutzten Endgeräte.

  ⇨ Empfehlungen des BSI zum häuslichen Arbeitsplatz
  ⇨ Empfehlungen des BSI zum mobilen Arbeitsplatz

- Bei Telefonaten und Videokonferenzen ist einem potentiellen **Mithören entgegenzuwirken**. Generell empfiehlt sich die Verwendung von Kopfhörern. Telefonate und Videokonferenzen, in denen es um personenbezogene Daten geht, sind in einem geschlossenen Raum bzw. in Abwesenheit unbefugter Personen zu führen. Auch **Sprachassistenten**, unabhängig davon, ob in Form von Smart Speakern oder in Laptop oder Mobiltelefon verbaut, sind im häuslichen Bereich zu entfernen bzw. zu **deaktivieren**.

- Bei Verlassen des Arbeitsplatzes sind die dienstlichen **Arbeitsmaterialien** zu **verschließen**. Steht kein separates und abschließbares Büro für den mobilen Arbeitsplatz zur Verfügung, so sind die Arbeitsmaterialien im Sinne einer **Clean-Desk-Policy** in einem verschließbaren Behälter zu sichern.

- Auch bei kurzer Abwesenheit sind die Endgeräte zu sperren (es empfiehlt sich eine manuelle Sperrung – das Abwarten einer automatischen Sperrung, bspw. durch einen zeitgesteuerten Bildschirmschoner, ist nicht ratsam).

- Es ist organisatorisch festzulegen, ob und welche personenbezogenen Daten nach Art, Umfang und Kategorie der Daten im Rahmen des mobilen Arbeitens verarbeitet werden dürfen. Hierbei sind die Risiken für Rechte und Freiheiten betroffener Personen, der potentielle Schaden sowie die Eintrittswahrscheinlichkeit zu berücksichtigen. An der auch im Rahmen des mobilen Arbeitens notwendigen Erstellung des **Rollen- und Berechtigungskonzepts** ist die oder der betriebliche oder behördliche Datenschutzbeauftragte zu beteiligen.

  ⇨ Kurzpapier Nr. 17 der DSK Besondere Kategorien personenbezogener Daten
  ⇨ Kurzpapier Nr. 18 der DSK Risiko für die Rechte und Freiheiten natürlicher Personen

- Müssen personenbezogene Daten transportiert werden, so sind diese in Abhängigkeit vom Transportmedium technisch **verschlüsselt** bzw. physisch **verschlossen** zu **transportieren**.
  ⇨ Orientierungshilfe der DSK Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail
  ⇨ Webseite des HBDI „Zur Übermittlung personenbezogener Daten per Fax“

- Ein **Medienbruch** bei der Verarbeitung von personenbezogenen Daten im Zuge des mobilen Arbeitens ist möglichst zu **vermeiden**. Ein privater Drucker oder Scanner darf nicht verwendet werden. Sofern erforderlich, ist ein solcher von Arbeitgebern zu stellen. Beim Drucken ist darauf zu achten, dass der richtige Drucker angesteuert und nicht versehentlich das falsche Gerät mit der Folge ausgewählt wird, dass personenbezogene Daten gegenüber unbefugten Dritten offengelegt werden. Grundsätzlich ist papierlosem Arbeiten im Home-Office der Vorzug zu geben.

- Hinsichtlich der Entsorgung von Papierdokumenten bedarf es einer festgelegten **Regelung zur Vernichtung**. Diese dürfen nicht einfach im Hausmüll entsorgt werden, sondern sind mit einem dem erforderlichen Schutzniveau des Dokuments angemessenen Aktenvernichter zu zerkleinern. Deshalb sind sie in das Unternehmen zu transportieren und dort einer angemessenen Entsorgung (Aktenvernichtung) zuzuführen. Für lokal auf Firmengeräten (z. B. Mobiltelefone oder Laptops) gespeicherte digitale Dokumente und personenbezogene Daten bedarf es darüber hinaus eines **Löschprogramms**, welches sicherstellt, dass die Dokumente und personenbezogenen Daten vollständig von den Geräten entfernt sind.

⇨ Standarddatenschutzmodell der DSK, Baustein 60 "Löschen und Vernichten"

- Die Festlegung von **klaren betriebsinternen Kommunikationswegen** ermöglicht eine leichtere Identifikation von Kommunikationspartnern und verringert somit deutlich die Gefahr von erfolgreichen Betrugsversuchen (z.B. Phishing-Mails). Im Zuge dessen ist auch die Nutzung von oder Weiterleitung an private E-Mail-Konten für die dienstliche Kommunikation zu untersagen und – soweit möglich – technisch zu unterbinden. Dies gilt in besonderem Maße auch für den Zugriff auf und den Abruf von beruflichen E-Mail-Konten von privaten oder öffentlichen Endgeräten.

- Die **private E-Mail- und Internetnutzung** am Arbeitsplatz sollte **ausdrücklich geregelt** werden. Hierbei bietet es sich an, sie in einem ersten Schritt grundsätzlich zu untersagen, um zu verhindern, dass diese im Sinne einer betrieblichen Übung ungeregelt stattfindet. In einem zweiten Schritt können Arbeitgeber dann die Privatnutzung unter bestimmten Voraussetzungen gestatten.

  ⇨ Orientierungshilfe der DSK zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

- Schließlich ist die **Benennung von Ansprechpartnerinnen und Ansprechpartnern**, sowohl für datenschutzrechtliche als auch datenschutztechnische Fragen notwendig. Gerade im Falle einer (potenziellen) Verletzung des Schutzes personenbezogener Daten, z. B. durch Verstoß oder Datenverlust, ist es zur Minimierung etwaiger Risiken elementar, dass den Beschäftigten die fachlich kompetenten Ansprechpartnerinnen und Ansprechpartner bekannt sind. Darüber hinaus müssen die Abläufe für solche Fälle klar und transparent geregelt sein.

  ⇨ 48. Tätigkeitsbericht des HBDI, 4.3 Datenschutz im Umgang mit Phishing Vorfällen, Seite 16

- Durch **regelmäßige, verpflichtende Schulungs- und Sensibilisierungs-maßnahmen** sind die Beschäftigten auf die einzuhaltenden datenschutz-rechtlichen Vorgaben und Regelungen hinzuweisen. Hierzu bieten sich beispielsweise E-Learnings mit abschließenden Tests, Merkblätter mit Bestätigung der Kenntnisnahme und praktische Übungen an. Die Teilnahme an Schulungs- und Sensibilisierungsmaßnahmen sollte dokumentiert werden. Durch die Schulungsmaßnahmen lassen sich die Beschäftigten für die generellen datenschutzrechtlichen Gefahren, Bedrohungen und Risiken sensibilisieren. Ihnen kann z.B. die Klassifizierung von Daten sowie die Differenzierung hinsichtlich der Vertraulichkeit dieser nähergebracht und es können gegenwärtig erkennbare Gefahren gesondert hervorgehoben werden.

  ⇨ Kurzpapier Nr. 19 der DSK Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO

- Technische Anwendungen, die eine weitreichende Überwachung der Beschäftigten ermöglichen, stellen einen erheblichen Eingriff in das Recht der Beschäftigten auf informationelle Selbstbestimmung dar, der durch den Überwachungszweck häufig nicht gerechtfertigt werden kann und somit nicht den Anforderungen des Datenschutzrechts genügt.

  ⇨ 50. Tätigkeitsbericht des HBDI, 11.2 Nutzung von digitalen Instrumenten zur Mitarbeiterüberwachung, Seite 131

- Alle datenschutzrechtlichen Regelungen sind entweder in einer separaten **Richtlinie für mobiles Arbeiten** festzuhalten oder in die bestehende, generelle IT- oder Datenschutzrichtlinie zu integrieren. Sie ist den Beschäftigten nachweislich bekannt zu machen und zur Verfügung zu stellen.

Weitere Veröffentlichungen zu dem Thema

- ⇨ Selbst-Check: Datenschutzrechtliche Regelungen bei Homeoffice des BayLDA
- ⇨ Tipps für sicheres mobiles Arbeiten des BSI
- ⇨ Telearbeit und Mobiles Arbeiten des BfDI
- ⇨ Technische und organisatorische Maßnahmen zur Umsetzung des Datenschutzes bei Heimarbeit des LDA Brandenburg
- ⇨ Hilfestellung zum Datenschutz im Homeoffice der LfD Niedersachsen