DATA AGENDA PLUS
powered by GDD

DataAgenda - das Lösungsportal
zum Datenschutzrecht

Präsentiert von DATAKONTEXT

www.DataAgenda.de

Checkliste „Mobiles Arbeiten“

Die Ausübung der beruflichen Tätigkeit von zu Hause und das Arbeiten unterwegs unter Einsatz von Informationstechnologien hat in den vergangenen Jahren eine wesentliche Bedeutung in der Arbeitswelt erlangt. Beide Arbeitsformen werden nachfolgend unter dem Begriff „Mobiles Arbeiten“ subsummiert.

Um ein datenschutzkonformes Arbeitsumfeld zu schaffen, ist der Arbeitgeber verpflichtet, den Schutz personenbezogener Daten auch außerhalb seiner stationären Arbeitsplätze und Standorte sicherzustellen. Der Arbeitnehmer ist zur Einhaltung besonderer Verhaltensregelungen angehalten.

Nachfolgend sind i.S. eines Best-Practise-Ansatzes wesentliche Aspekte für ein datenschutzkonformes mobiles Arbeiten zusammengestellt.

Allgemeine Anforderungen

- Im Rahmen einer **Risikobetrachtung** hat der Arbeitgeber - vor Aufnahme des mobilen Arbeitens bzw. bei Veränderungen der Verarbeitungssituation - das aus dem mobilen Arbeiten resultierende Risiko zu ermitteln und zu bewerten (z.B. beschränkte Kontrollmöglichkeit aufgrund räumlicher Trennung oder Nutzung technischer Einrichtungen außerhalb des Einflussbereichs). Es empfiehlt sich den Datenschutz- und den Informations-/IT-Sicherheits-Beauftragten hinzuzuziehen.
- Wenn eine geplante Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist eine **Datenschutz-Folgenabschätzung** gem. Art. 35 DS-GVO durchzuführen. So können bspw. besondere Risiken des Datenverlusts, Datenmissbrauchs oder Zugriffs durch unbefugte Dritte existieren, die Gefahren für die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten bedeuten können. Wenn die Risiken für die Rechte und Freiheiten betroffener Personen nicht hinreichend eingedämmt werden können, ist ein mobiles Arbeiten nicht zulässig.
- Es ist ein **Datenschutz- und Datensicherheitskonzept** zu erarbeiten, welches auf spezifische Anforderungen des mobilen Arbeitens eingeht, regelmäßig aktualisiert und mit bereits bestehenden Konzepten zum stationären Arbeiten harmonisiert wird. Die datenschutzrechtlichen Regelungen sind den Beschäftigten nachweislich bekannt zu machen, zur Verfügung zu stellen und die Inhalte sind durch regelmäßige, verpflichtende Schulungen und Sensibilisierungsmaßnahmen zu vermitteln.
- Der Arbeitgeber muss die **Einhaltung der Regelungen** zum mobilen Arbeiten gewährleisten können. Dies ist bspw. über vom Arbeitnehmer bestätigte Checklisten und/oder Vor-Ort-Kontrollen (bei Arbeiten im Homeoffice) möglich. Ein Zutrittsrecht des Arbeitgebers muss vertraglich mit den mobil arbeitenden Beschäftigten vereinbart werden, wobei auch das Einverständnis der in häuslicher Gemeinschaft mit ihnen zusammenlebenden Personen umfasst sein muss.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

- Technische Anwendungen, die eine weitreichende – präventive - **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.
- Der Arbeitgeber hält **Übersichten** über die Tätigkeiten mit Verarbeitung personenbezogener Daten, die im Rahmen des mobilen Arbeitens erbracht werden, über die Beschäftigten und die zur Verfügung gestellten Geräte samt Konfigurationen vor.
- Da viele der nachfolgenden organisatorischen und technischen Maßnahmen ein aktives Mitwirken der Beschäftigten erfordern, sind **regelmäßige Schulungen/Fortbildungen** zum datensicheren und datenschutzgerechten mobilen Arbeiten wichtig.

Organisatorische Maßnahmen im Zusammenhang mit mobilen Arbeiten

- Sämtliche **Regelungen** des Arbeitgebers zur Organisation des mobilen Arbeitsplatzes und der mit dem mobilen Arbeiten verbundenen Anforderungen an bestimmte Arbeitsprozesse sind schriftlich zu dokumentieren, den Beschäftigten zu kommunizieren und zu schulen sowie regelmäßig zu überprüfen und ggf. anzupassen.
- Bei der **räumlichen Gestaltung des Arbeitsplatzes** haben die Beschäftigten darauf zu achten, dass die von ihnen verarbeiteten personenbezogenen Daten – weder von Familienmitgliedern noch sonstigen Dritten - nicht einsehbar sind. Beim mobilen Arbeiten im öffentlichen Bereich ist auch auf Überwachungskameras zu achten und es sollten Sichtschutzfolien auf den Bildschirmen der genutzten Endgeräte genutzt werden.
- Beim **Verlassen** des häuslichen **Arbeitsplatzes** oder auch eines Hotelzimmers etc. hat der Beschäftigte darauf zu achten, dass Fenster und Türen geschlossen werden. Alle Arbeitsmaterialien sind i.S.e. Clean-Desk-Policy verschlossen aufzubewahren. Alle Endgeräte werden – auch bei kurzer Abwesenheit - manuell gesperrt.
- Bei Telefonaten und Videokonferenzen ist einem potenziellen **Mithören** entgegenzuwirken (z.B. geschlossen Räume, Kopfhörer). **Sprachassistenten** sind im häuslichen Umfeld zu entfernen bzw. zu deaktivieren.
- Ein **Medienbruch** sollte bei der Verarbeitung personenbezogener Daten im Zuge des mobilen Arbeitens möglichst vermieden werden. Grundsätzlich ist papierlosem Arbeiten der Vorzug zu geben. Sofern technisch eine Unterbindung nicht möglich ist, sollte die Verwendung privater Drucker oder Scanner sowie Speichermedien verboten werden.
- Bei einem **Transport von Dokumenten und Datenträgern** mit personenbezogenen Daten sind sicher verschlossene (Transport-)Behältnisse zu verwenden, welche gegen Entnahme und Einsichtnahme geschützt sind. Zudem sollte geregelt sein, dass Unterlagen und Datenträger beim Transport nicht erhöhten Risikosituationen (z. B. Rücksitz beim Einkaufen, Rucksack im Restaurant usw.) ausgesetzt werden.
- Die **Entsorgung von Dokumenten und Datenträgern** erfolgt nicht über den Restmüll oder die häusliche Papiertonne, sondern – entsprechend der im Unternehmen festzulegenden Regelungen zur Vernichtung - entweder im Büro oder zu Hause durch einen Aktenvernichter mit geeigneter Sicherheitsstufe nach DIN 66399. Fehlausdrucke oder nicht mehr benötigte Dokumente sollten zudem nicht anderweitig (z.B. als Notizzettel) genutzt werden.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

- Eine **Nutzung von oder Weiterleitung von Informationen an private E-Mail-Konten** für die dienstliche Kommunikation ist zu untersagen und - soweit möglich – technisch zu unterbinden. Dies gilt auf für den Zugriff auf und den Abruf von beruflichen E-Mail-Konten von (nicht autorisierten) privaten oder öffentlichen Endgeräten.
- Es sind klare **betriebsinterne Kommunikationswege** festzulegen und Ansprechpartner für datenschutzrechtliche und -technische Fragen (z.B. im Fall potenzieller Datenschutzverletzungen) zu benennen. Die Abläufe für solche Fälle sind klar und transparent zu regeln.
- Beim **Einsatz von Videokonferenzsystemen** ist darauf zu achten, dass z.B. durch Einblicke in die Privatsphäre oder das Erscheinen weiterer Personen im Bild keine datenschutzrecht-lichen Risiken entstehen. Der Arbeitgeber sollte die Beschäftigten über Regelungen zu Bildschirmfreigaben, Hintergrundbildern und Speicherung von Aufnahmen informieren und sie im Umgang mit den eingesetzten Systemen schulen und trainieren.
- Für die im Rahmen des mobilen Arbeitens zugelassenen Tätigkeiten sind die **Berechtigungs- und Zugangsregelungen** zu den IT-Systemen, IT-Anwendungen und Datenbanken auf das notwendige Minimum zu beschränken, um das Risiko von Datenlecks zu minimieren.

Technische Maßnahmen im Zusammenhang mit mobilem Arbeiten

- Den Beschäftigten ist, soweit möglich, die für ihre Arbeit notwendige **technische Ausstattung** (Laptop, Mobiltelefon, Ausgabe- und Speichergeräte etc.) in Form von **Firmengeräten zur Verfügung zu stellen**. Es existiert zudem eine Anweisung, dass zur Verfügung gestellte dienstliche Geräte auch zu Hause nicht für private Zwecke genutzt werden.
- 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**.
- **USB- und sonstige Zugänge** sind soweit möglich **technisch zu sperren**, ebenso sollte eine Anbindung von **Druckern/Scannern** technisch unterbunden werden.
- 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**.
- **PIN-Sperre** bei dienstlichen Smartphones, jedoch auch bei privaten Geräten, wenn hierüber eine Synchronisation mit Mail/Kontakte/Kalender oder weiterer Datenaustausch mit dem Unternehmensnetz möglich ist.
- Um bei dem Verlust oder Diebstahl von Geräten die Vertraulichkeit der Daten sicherzustellen, sind auf diesen **Remote-Wipe-Lösungen** zu installieren.
- Die **Verbindung ins Unternehmensnetzwerk** und die gesamte Kommunikation erfolgen ausschließlich mit **verschlüsselten VPN-Verbindungen** (oder ähnlichen Technologien) nach dem Stand der Technik. **WiFi-Zugänge** müssen **mit einem sicheren Passwort abgesichert** sein.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

- Der Zugang der Berechtigten zu den sensiblen personenbezogenen Daten erfolgt ausschließlich mit **Multi-Faktor-Authentifizierung**, nebst PIN/Passwort, oder Nutzung von **Passkeys**.
- 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).
- **Messenger** zur dienstlichen Kommunikation sind ausschließlich über die Firmengeräte zu nutzen. Neben einer Ende-zu-Ende-Verschlüsselung muss technisch auch ausgeschlossen werden, dass der Anbieter Informationen darüber erhält, speichert oder verarbeitet, wer mit wem kommuniziert hat.

Autor

Uwe Bargmann
Freiberuflicher Berater Datenschutzmanagement, Kooperationspartner der DMC Datenschutz Management + Consulting GmbH & Co KG