Anlage 2 zur Dienstvereinbarung Mobiles Arbeiten

Ausführungen zu datenschutzrechtlichen Bestimmungen

**Allgemeines**

Die Vertraulichkeit und Integrität personenbezogener und sensibler Daten müssen gewährleistet sein. Daraus folgt, dass diese Daten gemäß Artikel 5 Abs. 1 Buchstabe f Datenschutzgrundverordnung (DSGVO) vor unbefugter und unberechtigter Verarbeitung sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Beschädigung zu schützen sind. Dies bedeutet vor allem, dass auch ausschließlich die vom Arbeitgeber bereitgestellte Software genutzt werden darf. Das gilt insbesondere auch für das Speichern der von ihnen erstellten Dokumente. Dies darf auf keinen Fall auf privaten Speichermedien wie lokalen Festplatten oder ungesicherten USB-Sticks erfolgen, sondern muss ausschließlich auf Servern oder sonstiger Hardware des Arbeitgebers stattfinden.

**Maßnahmen zur Informationssicherheit**

Um die Einhaltung des notwendigen Datenschutzes und den korrekten Umgang mit sensiblen Daten und Informationen zu gewährleisten, machen Sie sich bitte mit der Richtlinie zur Informationssicherheit „Informationen zur Heimarbeit“ des Landkreises Lüneburg vertraut. Diese finden Sie in den Hausinformationen unter: „Informationssicherheit\Hinweise und Sicherheitsmaßnahmen für die Heimarbeit“. Außerdem beachten Sie bitte auch die „Richtlinie zur Löschung und Vernichtung von Datenträgern jeglicher Art“ und die „Richtlinie zur Nutzung von Informationstechnik“. Diese finden Sie ebenfalls in den Hausinformationen unter: „Informationssicherheit\Richtlinien“.

**Kein Zugang für unbefugte Dritte**

Es muss sichergestellt sein, dass ausschließlich die Beschäftigten Zugang zu den im Zusammenhang mit der Arbeitstätigkeit anfallenden personenbezogenen Daten und sensiblen Informationen haben. Weder Familienangehörige, Mitbewohner noch sonstige Personen dürfen Zugriff auf die zu schützenden Daten erhalten. Aus diesem Grund sollten Sie nach Möglichkeit in einem Raum arbeiten, der für dritte Personen nicht uneingeschränkt zugänglich ist. Auf alle Fälle sollten Bildschirme so positioniert sein, dass eine direkte Einsichtnahme durch Personen, die den Raum betreten, nicht möglich ist. Bei zeitweisem Verlassen des Zimmers, in dem dieTätigkeit stattfindet, muss der Laptop oder der PC ausgeschaltet oder zumindest eine passwortgesicherte Bildschirmsperre aktiviert werden.

**Keine Ausdrucke im Homeoffice**

Das Ausdrucken von Dokumenten im Homeoffice ist nicht gestattet. Bitte benutzen Sie für Ausdrucke im Homeoffice die „Follow me“ Funktion und drucken Sie Ihre Unterlagen bei Ihrer nächsten Anwesenheit in der Dienststelle aus.

**Entsorgung von vertraulichen Informationen**

Keine Entsorgung/Vernichtung von dienstlichen Dokumenten und Datenträgern zu Hause! Entsorgen oder vernichten Sie Datenträger jeglicher Art ausschließlich beim Landkreis Lüneburg, beachten Sie dabei die „Richtlinie zum Löschen und Vernichten von Datenträgern jeglicher Art“.

**Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf**

Wenn Sie dienstliche Unterlagen oder Informationen mit erhöhtem Schutzbedarf bearbeiten müssen, sollten Sie von einem Arbeitsplatz außerhalb der Dienststelle absehen.

**Melden von Datenschutzvorfällen**

Datenschutzvorfälle, insbesondere die unbefugte Kenntnisnahme personenbezogener Daten durch Dritte, melden Sie umgehend an die Datenschutzbeauftragte. Diese muss entscheiden, wie mit diesem Vorfall umzugehen ist, also insbesondere, ob eine Meldepflicht gegenüber den Datenschutzbehörden und den betroffenen Personen besteht. Informationssicherheitsvorfälle melden Sie bitte umgehend gemäß der Richtlinie zur Nutzung von Informationstechnik an den FD 33.

**Telefonate und Videokonferenzen**

Führen Sie Telefonate und Videokonferenzen mit vertraulichem Inhalt so, dass andere Haushaltsmitglieder oder andere unbefugte Personen den Inhalt des Gesprächs nicht mithören können. Hierbei sind auch geöffnete Fenster zu berücksichtigen. Balkon, Terrasse oder Garten eignen sich gegebenenfalls nicht für solche Gespräche. Auch evtl. vorhandene digitale Assistenten, welche über Sprache reagieren, sind auszuschalten bzw. zu entfernen. Machen Sie sich vor einer Videokonferenz mit der Checkliste für externe Videokonferenzen vertraut. Diese finden Sie in den Hausinformationen unter „Informationssicherheit\ Checkliste für externe Videokonferenzen“.

**Transport und Aufbewahrung von Dokumenten und Akten**

Transportieren Sie dienstliche Papierdokumente/Akten zwischen der Arbeitsstätte und dem gewählten Ort in verschlossenen Behältern/Taschen. Lassen Sie Datenträger und Unterlagen während des Transportes nicht unbeaufsichtigt. Zum Mobilen Arbeiten benötigen Sie einen geeigneten Arbeitsplatz, an dem Dokumente mit personenbezogenen Daten sicher aufbewahrt werden können. Empfehlenswert ist ein eigener abschließbarer Raum, der nach Feierabend oder in Pausen für dritte Personen nicht zugänglich ist. Ist das räumlich nicht möglich, verwahren Sie sämtliche Unterlagen zumindest in einem abschließbaren Schrank oder Rollcontainer. Am Ende des Arbeitstages müssen Sie alle Unterlagen sicher verwahren.

**Umgang mit dienstlichen Geräten**

Dienstliche Geräte werden nicht für private Zwecke benutzt. Die Richtlinie zur Nutzung von Informationstechnik ist zu beachten.

**Voraussetzungen für den Einsatz von privater IT-Technik**

Sollten Sie private IT-Technik nutzen, muss diese einige Voraussetzungen erfüllen. Dies ist zwingend notwendig, um ein sicheres Arbeiten von Ihrem privaten Gerät zu gewährleisten. Versichern Sie sich bitte vor der ersten Nutzung privater IT-Technik, ob die im Folgenden aufgeführten Voraussetzungen erfüllt sind.

* Eine Absicherung Ihres privaten Netzes muss vorhanden und aktuell sein.
* Ihre Router Einstellungen sind zu überprüfen und Updates hierfür zu pflegen.
* Optimaler Weise nutzen Sie zum Arbeiten eine LAN-Verbindung. Sollte dies nicht möglich sein und Sie nutzen eine WLAN-Verbindung, muss diese mindestens eine WPA2 Verschlüsselung haben in Verbindung mit einem sicheren Passwort. Ein offenes WLAN darf nicht genutzt werden.
* Ihr Betriebssystem muss aktuell sein und es muss ein gültiger Support für das Betriebssystem zur Verfügung stehen.
* Für den Zugriff auf Ihr System muss eine Benutzerauthentifizierung eingerichtet sein.
* Es muss bei Ihrem Gerät ein aktueller Virenschutz vorhanden sein.
* Updates, insbesondere Sicherheitsupdates müssen aktuell sein und von Ihnen gepflegt werden.

Nur wenn Sie alle diese Voraussetzungen bejahen können, ist die Nutzung Ihrer privaten Geräte zulässig.

**Möchten Sie kontrollieren, ob Sie an die wichtigsten Punkte zum Thema Datenschutz gedacht haben? Hier für Sie die Checkliste zum Selbstcheck:**

**Datenschutzrechtliche Regelungen Mobiles Arbeiten**

**Checkliste mit Prüfkriterien nach DS-GVO Anlage**

Stand: 10.06.2022

**Selbst-Check: Datenschutzrechtliche Regelungen beim mobilen Arbeiten**

**Arbeitsumgebung**

Die Arbeitsplatzumgebung zu Hause soll so ausgestaltet sein, dass vom Grundsatz her die Vertraulichkeit und Verfügbarkeit der Daten wie im Büro sichergestellt ist.

* Der Arbeitsplatz ist so gewählt, dass Familienmitglieder oder Besucher keinen Blick auf das Notebook und in die Papierunterlagen werfen können
* Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages
* Es werden Sichtschutzfolien angeboten, wenn dies erforderlich ist (bspw. Schreibtisch am Fenster in Parterrewohnung)
* Papierunterlagen können in Dokumentenmappen oder
* Schränken verschlossen werden
* Fenster werden in Erdgeschosswohnungen bei Verlassen des Arbeitsplatzes immer geschlossen.
* Sperrung des Bildschirms bei Verlassen des Arbeitsplatzes, falls ein anderer Zugriff – egal ob gewollt oder ungewollt
* z. B. durch Kinder oder Haustiere – nicht ausgeschlossen ist
* Es wird darauf geachtet, dass Telefongespräche nicht von unbefugten Personen mitgehört werden (z. B. offenes Fenster, laufende andere Videokonferenz)

**Genutzte Hardware**

Es wird die Bereitstellung von dienstlichen Geräten empfohlen. Privatgeräte sollten nur in Ausnahmefällen eingesetzt werden.

* Dienstliche Notebooks/PC werden gestellt
* Dienstliche Smartphones oder Softphones werden gestellt
* Bei Verwendung von Privatgeräten werden Remoteverbindungen auf Terminalserver verwendet
* Dienstlich zur Verfügung gestellte Geräte werden auch zu Hause nicht für private Zwecke genutzt

**Umgang mit Papierdokumenten**

In vielen Betrieben sind noch nicht alle Arbeitsabläufe komplett digital nutzbar. Beim Umgang mit Papierdokumenten entstehen neue Risiken, die in den Räumlichkeiten des Büros nicht auftraten.

* Papierunterlagen werden in geeigneten Mappen (u. a. mit Name des Unternehmens im Falle eines Verlusts) mit nach Hause genommen
* Regelungen bestehen, dass Papierunterlagen beim Transport nach/von zu Hause nicht erhöhten Risikosituationen (z. B. Rücksitz beim Einkaufen, Rucksack im Restaurant) ausgesetzt werden sollen
* Entsorgung von Papierunterlagen erfolgt nicht über den eigenen Hausmüll, sondern fachgerecht entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 3 (nach DIN 66399)
* Es wurde über die Risiken der Schädigung von wichtigen Papierdokumenten (z. B. Kinder bemalen ein Originaldokument) sensibilisiert – es wird bei solchen Dokumenten, sofern möglich, mit Kopien gearbeitet

**Allgemeine organisatorische Regelungen**

Die Anbindung von Mitarbeitern im Zu-Hause-Modus muss durchdacht und sicher ausgestaltet werden. Neben technischen Lösungen helfen organisatorische Regelungen, um Einfallstore für tiefgreifende Cyberangriffe zu verhindern.

* Überblick über die Mitarbeiter im Homeoffice
* Überblick über die Geräte der Mitarbeiter im Homeoffice
* Schulung/Informationen für Mitarbeiter über die Homeoffice-Regelungen
* Schriftliche Verpflichtung der Mitarbeiter, dass diese sich an die Regelungen halten – eine Vor-Ort-Kontrolle kann so i. d. R. entfallen
* Keine Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten
* Bei sensitiven Dokumenten verhindern Regelungen zum Ausdruck von Dokumenten auf den Druckern im Büro die Einsicht durch andere Mitarbeiter

**5 Sicherheit**

Das eigene Homeoffice gilt als virtuelles Büro. Durch die Anbindung an das Internet erhöhen sich dabei die Sicherheitsrisiken enorm. Technische Lösungen helfen, diese Risiken zu minimieren.

* Anbindung an das Firmennetz mit verschlüsselten VPN-
* Verbindungen nach Stand der Technik
* Einsatz von Verfahren zur Zwei-Faktor Authentifizierung nebst PIN/Passwort (z. B Hardwaretoken
* Nutzung vom heimischen WLAN mit starken Passwörtern
* Nutzung öffentlicher WLAN-Hotspots nur bei durchgängiger Absicherung sämtlicher Kommunikation durch VPN-Anbindung
* Speicherung von Daten auf über die VPN-Verbindung
* erreichbare Netzlaufwerke im Unternehmen
* Regelmäßiges Patch Management erfolgt auch auf dem Homeoffice-Notebook/PC durch Konfiguration von automatischen Sicherheitsupdates
* Täglich Updates der Virensignaturen auf den Homeoffice-Notebooks/PC

**Bei Fragen zur Datensicherheit wenden Sie sich bitte an den FD 33 Informations- und Kommunikationstechnik oder an unsere Datenschutzbeauftragte.**