# Hinweise zum Datenschutz im Homeoffice (Stand: 27.03.2020)

Üblicherweise ist die Einrichtung eines Heim-Arbeitsplatzes mit Vorbereitungen verbunden, um am heimischen Arbeitsplatz Datenschutz in gleichem Maße wie im Büro zu gewährleisten.

Im Zuge der Corona-Pandemie verändert sich derzeit jedoch vieles im Alltagsleben. Dazu gehört auch ein verstärktes Arbeiten von Zuhause aus (Homeoffice, Telearbeit), das gegenwärtig häufig unter improvisierten Bedingungen realisiert wird.

Nachfolgend sind daher einige Hinweise für den Umgang mit personenbezogenen Daten im Homeoffice zusammengestellt, die Sie auch bei provisorischen Heimarbeitssituationen beherzigen sollten.

**Inhalt:**



## 1. Arbeitsplatz im Homeoffice

Die Arbeit im Homeoffice muss von Ihrem Arbeitgeber, gegebenenfalls unter Auflagen, genehmigt sein.

Achten Sie bei der Einrichtung Ihres häuslichen Arbeitsplatzes nicht nur darauf, dass Sie ungestört und effektiv arbeiten können, sondern auch auf folgende Punkte:

- Wenn Sie regelmäßig personenbezogene Daten verarbeiten ist ein Arbeitsplatz in einem eigenen Raum am besten, ansonsten in einem hinreichend separierten Bereich. Wählen Sie den Platz so, dass andere den Bildschirm nicht einsehen können.

- Wenn Sie Ihren privaten Internet-Anschluss verwenden: Richten Sie Ihren Computer so ein, dass er mit dem privaten Netzwerk durch ein Kabel oder ein verschlüsseltes WLAN verbunden ist. Ihr WLAN sollte so eingerichtet sein, dass man sich nur mit einem Passwort einwählen kann.

- Für Papierdokumente muss ein unbefugter Zugriff bei Transport und Nutzung ausgeschlossen werden. Lassen Sie diese daher nicht unbeaufsichtigt! Finden Sie einen geeigneten Platz, um dienstliche Unterlagen mit personenbezogenen Daten geschützt vor unbefugten Zugriff aufzubewahren.

- Organisieren Sie Ihren häuslichen Arbeitsplatz so, dass sich private und dienstliche Daten nicht mischen.

## 2. IT-Geräte, Datenträger, Netzwerkzugang

- Beim Wechsel ins Homeoffice nehmen Sie vermutlich Dokumente und IT-Geräte vom Arbeitsplatz mit nach Hause. Achten Sie dabei darauf, dass Ihr Laptop nicht nur mit einem sicheren Passwort o.ä. geschützt ist, sondern die Festplatte und etwaige Speichermedien (z.B. USB-Stick, Festplatte) auch verschlüsselt sind.

- Stellen Sie sicher, dass die Geräte und Speichermedien nicht für andere Personen zugänglich sind, wenn Sie nicht damit arbeiten.

    - Hat Ihr Arbeitgeber keine Dienst- oder Betriebsanweisung zum Thema „Bring your own device“, sollten Sie vorrangig IT-Geräte Ihres Unternehmens bzw. Ihrer Behörde und keine privaten Geräte nutzen. Ist Letzteres unvermeidlich, benötigen Sie dafür die Genehmigung Ihres Arbeitgebers. Weiterhin müssen die Geräte über essentielle Sicherheitsmaßnahmen verfügen (aktuelle System- und Anwendungssoftware, Schutz vor Schadsoftware, aktivierte Firewall, sowie ein wirksamer Zugangsschutz (Passwort, Fingerabdruck/Gesichtserkennung, Token).

    - Dokumente, an denen Sie arbeiten und Ihre Arbeitsergebnisse sind auch bei der Nutzung privater Geräte auf dienstlichen Systemen im Netz Ihres Arbeitgebers oder auf dienstlich bereitgestellten Datenträgern zu speichern (z.B. USB-Stick, Festplatte). Letztere sind durch eine Verschlüsselung zu schützen. Entsprechende Möglichkeiten sind z.B. hier beschrieben:
      https://www.datenschutz.rlp.de/de/themenfelder-themen/7zip/
      https://www.heise.de/download/product/veracrypt-95747

  Von einer Speicherung personenbezogener dienstlicher/geschäftlicher Daten in privaten Cloud-Speichern ist abzusehen. Soweit dies im Einzelfall unvermeidbar ist, darf dies nur vorübergehend erfolgen und die Daten müssen verschlüsselt werden. Hinweise hierzu finden Sie unter:
  https://www.datenschutz.rlp.de/de/themenfelder-themen/cloud-speicher-sicher-nutzen/

- Wenn Sie an einem dienstlichen Computer arbeiten, schließen Sie an diesem Gerät keine private Hardware (z. B. externe Festplatten oder USB-Sticks) an. So verringern Sie das Risiko, dass Schadsoftware Ihren Computer befallen und Daten kompromittiert werden.

- Ein externer Zugang in das Netzwerk Ihres Unternehmens bzw. Ihrer Verwaltung darf nur über eine geschützte Verbindung erfolgen (VPN; Verschlüsselung der Verbindung, Authentifizierung (möglichst 2-Faktor Authentifizierung über Passwort und Zertifikat/SMS-PIN/OTP/Token).

- Wenn Sie Ihren Arbeitsplatz kurzzeitig verlassen, aktivieren Sie den Bildschirmschoner mit Kennwortschutz, damit niemand unberechtigt auf Ihre dienstlichen Daten zugreifen kann.

- Wenn Sie Dokumente an Ihrem häuslichen Arbeitsplatz ausdrucken müssen, dann achten Sie darauf, dass andere Personen im Haushalt keine Kenntnis davon nehmen können. Achten Sie auch darauf, dass Sie, wenn Sie z. B. über VPN in Ihrem dienstlichen Netz arbeiten, keine Druckaufträge auf allgemein zugängliche Drucker abschicken, da in diesem Fall unberechtigte Personen Einblick in diese Dokumente nehmen könnten.

- Entsorgen Sie dienstliche Papierdokumente nicht in Ihren privaten Papiermüll.

### 3. Telefon

- Wenn Sie am häuslichen Arbeitsplatz dienstlich telefonieren, dann achten Sie darauf, dass Sie dafür einen ungestörten Bereich aufsuchen, wenn dabei personenbezogene Daten Dritter zur Sprache kommen, damit andere Personen im Haushalt keine Kenntnis von diesem nehmen können. Sollte es sich um ein Telefonat unter Kollegen ohne die Nennung von personenbezogenen Daten Dritter handeln, informieren Sie den Gesprächspartner, wenn im Hintergrund eine andere Person im Haushalt das Telefonat hören kann.

- Werden private Telefone verwendet, müssen Sie sicherstellen, dass gespeicherte Kontakte von Kunden, Klienten o.ä. nicht dauerhaft auf dem privaten Telefon verbleiben. In der Regel ist es nicht erforderlich, dass Ihre private Nummer bei Ihren Anrufen erscheint. Aktivieren Sie deshalb gegebenenfalls die Rufnummernunterdrückung (Achtung: Einige Telefonkonferenzsysteme funktionieren nur mit übertragener Rufnummer).

- Zur Frage, inwieweit Arbeitgeber private Kontaktdaten von Beschäftigten verarbeiten dürfen und inwieweit diese dies dulden müssen hat der LfDI entsprechende Hinweise zusammengestellt. Diese finden Sie unter:
  https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Beschaeftigtendatenschutz_-_Heimarbeit_und_private_Erreichbarkeitsangaben.pdf

## 4. E-Mail

- Soweit im Homeoffice die Möglichkeit besteht, auf das dienstliche/geschäftlicher Postfach zuzugreifen, ist dieses zu nutzen. Eine Nutzung privater Mailadressen ist nur ausnahmsweise, vorübergehend, mit Zustimmung des Arbeitgebers und bei ausreichendem Schutz dienstlicher Daten zulässig. Auf außereuropäische Anbieter sollte dabei nicht zurückgegriffen werden. Ist ein Rückgriff auf US-Anbietern zwingend notwendig dürfen nur solche Anbieter ausgewählt werden, die dem EU-US-Privacy-Shield-Abkommen beigetreten sind (vgl. https://www.privacyshield.gov/list).

- Personenbezogene und in anderer Hinsicht sensible Daten sind bei der Übertragung durch eine ausreichende Verschlüsselung zu schützen. Hinweise hierzu finden Sie unter: https://www.datenschutz.rlp.de/de/themenfelder-themen/e-mail-inhalte-schuetzen/

- Über die dienstliche/geschäftliche E-Mail-Adresse geführte Kommunikation ist zeitnah in das dienstliche Postfach zu überführen und im privaten Postfach zu löschen.

## 5. Messenger-Dienste, Telefon-/Videokonferenzsysteme

Die Auswahl von Messenger Diensten, Telefon- oder Videokonferenzsystemen sollte sich an folgenden Kriterien orientieren:

- Die Kommunikation zwischen den beteiligten Endgeräten wird durch eine Ende-zu-Ende-Verschlüsselung gesichert, die Vertraulichkeit gegenüber dem Anbieter des Dienstes gewährleistet.

- Die Bestands-, Verbindungs- und Nutzungsdaten der Teilnehmer werden ohne Einwilligung ausschließlich für die Erbringung des Dienstes und nicht für andere Zwecke genutzt; insbesondere nicht für weitere kommerzielle Zwecke. Dies gilt insbesondere bei der Nutzung kostenfreier Dienste.

- Art- und Umfang der im Rahmen des Dienstes verarbeiteten Daten und deren Verwendung müssen ersichtlich sein (Datenschutzerklärung, Nutzungsbestimmungen etc.).

- Soweit auf Dienst von US-Anbietern zurückgegriffen werden soll, dürfen nur solche Anbieter ausgewählt werden, die dem EU-US-Privacy-Shield-Abkommen beigetreten sind (vgl. https://www.privacyshield.gov/list).

- Für die Nutzung entsprechender Dienst sollten keine privaten Accounts genutzt werden (z.B. private Facebook-, Google- oder Microsoft-IDs, Mail-Adressen etc.)

- Die Möglichkeit pseudonymer Zugangskennungen sollte genutzt werden.

- Achten Sie darauf, in Messenger-Kommunikationen keine sensiblen Informationen auszutauschen.

## 6. Sonstiges

Für den Fall eines Datenverlusts (z. B. Verlust von Papierunterlagen oder Datenträgern) oder eines Datenschutzverstoßes (z. B. Zugang von Unbefugten an den Computer) oder eine sonstige Verletzung des Schutzes personenbezogener Daten besteht eine Meldepflicht gegenüber der Datenschutzaufsichtsbehörde. Hier muss auch für das Arbeiten im Homeoffice geregelt sein, wem der Beschäftigte dies im Unternehmen oder der Behörde unverzüglich mitteilen muss.

Mussten Sie sich sehr kurzfristig in den häuslichen Arbeitsbereich begeben, kann es sein, dass es in Ihrem Unternehmen bzw. in Ihrer Behörde noch kein Konzept für die Heimarbeit gibt. In dieser besonderen Situation müssen Sie, auch in Bezug auf den datenschutzkonformen Umgang mit Daten im häuslichen Bereich, versuchen, die Anforderungen mit Hilfe von mündlichen oder E-Mail-Anweisungen Ihrer Vorgesetzten oder durch die Berücksichtigung dieser Regeln umzusetzen.

Sollte sich jedoch eine unvorbereitete Homeoffice-Situation über einen längeren Zeitraum hinziehen, ist es notwendig, dass dafür in Ihrem Unternehmen bzw. in Ihrer Behörde ein schriftliches Konzept erstellt wird. In diesem Konzept müssen insbesondere die technischen und organisatorischen Maßnahmen beschrieben werden, um Daten sicher und datenschutzgerecht im Homeoffice verarbeiten zu können.

## 7. Quellen und weiterführende Informationen

**„Plötzlich im Homeoffice – und was nun?“**
Hinweise des ULD Schleswig-Holstein
https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf

**„Telearbeit und Mobiles Arbeiten“**
Information des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)
Stand: Januar 2019, 20 Seiten, deutsch
https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html

**„Top Tips for Cybersecurity when Working Remotely“**
Artikel der European Union Agency for Cybersecurity (ENISA)
Stand: März 2020, englisch
https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely

**„Home-Office? – Aber sicher!“**
Information des Bundesamts für Sicherheit in der Informationstechnik (BSI)
Stand: März 2020
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html