Homeoffice – Sommer 2021

In der neuen Corona-Arbeitsschutzverordnung vom 25. Juni 2021 ist **nicht** mehr festgehalten, dass der Arbeitgeber Beschäftigten im Fall von Büroarbeiten oder vergleichbaren Tätigkeiten anbieten muss, dass diese Tätigkeiten in deren Wohnung auszuführen sind, wenn keine zwingenden betriebsbedingten Gründe dem entgegenstehen.

Folgendes finden Sie in der Corona-Arbeitsschutzverordnung vom 25. Juni 2021:

§ 3 Kontaktreduktion im Betrieb
Der Arbeitgeber hat alle geeigneten technischen und organisatorischen Maßnahmen zu treffen, um betriebsbedingte Personenkontakte zu reduzieren. Die gleichzeitige Nutzung von Räumen durch mehrere Personen ist auf das betriebsnotwendige Minimum zu reduzieren.

Demzufolge ist es verständlich, dass der Arbeitgeber gern seine teuer bezahlten Büroräume nicht mehr leer stehen lassen möchte, wenn er die - unter § 3 benannten - Bedingungen erfüllt.

Sind Arbeitgeber und Arbeitnehmer sich einig, dass ein Arbeiten im Homeoffice oder dem mobilen Arbeiten gewünscht ist, dann sind jedoch - nach wie vor - die unterschiedlichsten Gesetzgebungen (z. B. Arbeitsschutz und Datenschutz) sowie betriebliche Vereinbarungen zu berücksichtigen.

Das bedeutet vorab:

1. **Der Arbeitgeber muss erst einmal prüfen**, ob Büroarbeiten oder vergleichbare Tätigkeiten in die Wohnstätten der Beschäftigten verlagert werden können. Dabei ist der Arbeitgeber gut beraten, sowohl die Prüfung als solche, als auch die Gründe für oder gegen die Ausführung der Büroarbeiten oder vergleichbaren Tätigkeiten von Zuhause aus zu dokumentieren.

2. Eine abweichende Festlegung des vertraglichen Arbeitsortes bedarf in jedem Fall einer entsprechenden **arbeitsvertraglichen Regelung zwischen Arbeitgeber und Beschäftigten oder einer Betriebsvereinbarung /betriebliche Vereinbarung**.

   Privater Wohnraum der Beschäftigten liegt außerhalb der Einflusssphäre des Arbeitgebers. (Grundrecht der Unverletzlichkeit der Wohnung Artikel 13 GG). Homeoffice ist kein "ausgelagertes Büro". **Auch die häuslichen Verhältnisse der Beschäftigten** (z.B. kein geeigneter Bildschirmarbeitsplatz, räumliche Enge) **können einer Arbeit im Homeoffice entgegenstehen**.

3. **Auch im Homeoffice müssen die Vorgaben der Datenschutzgrundverordnung sorgfältig eingehalten werden.** Es muss sichergestellt sein, dass niemand unbefugt Zugang zu Daten hat. Das betrifft nicht nur das Einsehen von Dokumenten sondern auch das Mithören.

Weitere Informationen zum Homeoffice und zum mobilen Arbeiten finden Sie beim BSI "Homeoffice? – Aber sicher" und bei dem BfDI "Telearbeiten und Mobiles Arbeiten".

Selbst-Check: Datenschutz im Home-Office

Neben technischen Lösungen helfen organisatorische Regelungen, um den Datenschutz einzuhalten und die IT-Sicherheit zu gewährleisten.

Allgemeine Regelungen	
Ein Überblick über die Mitarbeiter im Homeoffice besteht.	
Ein Überblick über die Geräte der Mitarbeiter im Homeoffice ist vorhanden.	
Die Mitarbeiter werden vorab über die Homeoffice-Regelungen geschult.	
Die Mitarbeiter haben eine schriftliche Verpflichtung unterzeichnet, dass diese sich an die Regelungen halten, inkl. Verschwiegenheitsverpflichtung. Eine Vor-Ort-Kontrolle kann so i.d.R. entfallen, anderenfalls sollte es schriftlich geregelt werden.	
Eine Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten ist untersagt (und auch in der schriftlichen Vereinbarung aufgenommen).	
Bei sensiblen Dokumenten verhindern Regelungen zum Ausdruck von Dokumenten auf den Druckern im Büro die Einsicht durch andere Mitarbeiter.	
Arbeitsumgebung	
Familienmitglieder oder Besucher können keinen Blick auf das Notebook und in die Papierunterlagen werfen.	
Es werden Sichtschutzfolien angeboten, wenn dies erforderlich ist (bspw. Schreibtisch am Fenster in Parterrewohnung).	
Es wird darauf geachtet, dass Telefongespräche nicht von unbefugten Personen mitgehört werden (z.B. offenes Fenster, laufende andere Videokonferenz).	
Papierunterlagen können sicher verschlossen werden (z.B. Schränke).	
Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages.	
Fenster und Türen werden geschlossen, so dass kein unbefugter Zugang zu den Unterlagen und Daten möglich ist.	
Sperrung des Notebooks bei Verlassen des Arbeitsplatzes	
Genutzte Hardware Es sollten dienstliche Geräte bereitgestellt werden und eine Nutzung von Privatgeräten nur in Ausnahmefällen gestattet sein.	
Dienstliche Notebooks sind verfügbar und werden gestellt.	
Diensttelefone sind verfügbar und werden gestellt.	
Remoteverbindungen auf Terminalserver werden verwendet (ausdrücklich bei Privatgeräten)	
Dienstlich zur Verfügung gestellte Geräte werden nicht für private Zwecke genutzt	
Umgang mit Papierdokumenten	
Mit dem Vorgesetzten ist genau abgestimmt, welche Unterlagen mit nach Hause genommen werden dürfen. Die Unterlagen werden ausschließlich in verschlossenen Behältern / Aktenkoffern transportiert.	
Regelungen zur Risiko-Minimierung beim Transport bestehen (z.B. Rücksitz im Auto während des Einkaufens, leicht zugänglicher Rucksack)	
Papierunterlagen werden nicht über den Hausmüll entsorgt, sondern fachgerecht entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 3 (nach DIN 66399).	
Sicherheit	
Die Hard- und Software entspricht den hohen Sicherheitsstandards des Unternehmens.	
Es werden regelmäßige Sicherheitsupdates installiert.	
Die Anbindung an das Firmennetz mit verschlüsselten VPN- Verbindungen nach aktuellem Stand der Technik ist vorhanden.	
Es ist geregelt, ob öffentliche WLAN-Hotspots verwendet werden dürfen – wenn ja, dann nur über sichere VPN-Verbindungen.	
Die Nutzung vom heimischen WLAN ist mit starken Passwörtern versehen. Die Passwörter werden geheim gehalten.	
Neue Software auf dem Dienstgeräten darf nur mit ausdrücklicher Erlaubnis des Unternehmens installiert werden (nach Zustimmung - z.B. durch den IT- und Datenschutzbeauftragten).	

Regelungen zum Umgang mit USB-Ports (z.B. Deaktivierung oder Verbot des Anschlusses privater Sticks) wurden getroffen	
Ein Zugriff vom Homeoffice nur auf erforderliche Server, Dateiablagen und Anwendungen ist nur über die VPN-Verbindung zum Firmennetzwerk gestattet.	
Die dienstlichen Geräte (z.B. Smartphones, Tablet) sind alle mit einem PIN versehen.	
Die Nutzung der privaten IT-Ausstattung darf nur mit ausdrücklicher Erlaubnis des Unternehmens und unter besonderen technischen und organisatorischen Maßnahmen genutzt werden.	
Es wurden detaillierte Regelungen zum Umgang der IT-Ausstattung, mobile Endgeräte und das Arbeiten im Homeoffice in entsprechenden Nutzungsanweisungen oder Dienst-vereinbarungen festgehalten und unterzeichnet.	
Nutzung von Cloud-Diensten	
Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO ist abgeschlossen und geprüft	
Verwendung starker Passwörter für Nutzer	
Sensibilisierung der Mitarbeiter für Risiken von Phishing- Attacken auf Cloud-Konten	
Verwendung von Verfahren zur Zwei-Faktor-Authentifizierung bei administrativen Konten	
Wirksame Löschung von Daten (z.B. bei Beendigung des Vertrages)	
Nutzung von Videokonferenzsystemen	
Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO ist abgeschlossen und geprüft	
Verwendung einer Transportverschlüsselung (z.B. TLS) nach Stand der Technik	
Verwendung einer Ende-zu-Ende-Verschlüsselung, sofern Daten mit hohem Risiko besprochen bzw. übertragen werden	
Deaktivierung von biometrischen Features wie Aufmerksamkeitserkennung, sofern eine solche Verarbeitung angeboten wird	
Keine Aufzeichnung der Videokonferenzen durch das Unternehmen und der Mitarbeiter	
Regelungen zum Zweck und der Speicherdauer (z.B. Löschung bei Beendigung der Konferenz) von Chat-Funktionen sind vorhanden	
Es gibt die Möglichkeit eines virtuellen Warteraumes, in dem Teilnehmer bis zu Beginn der Konferenz ohne Audio-/Video-übertragung warten können.	
Nutzung von Messenger-Diensten	
Die Kommunikation der Inhalte und der Transport erfolgt verschlüsselt (Ende-zu-Ende-Verschlüsselung. Dies gilt auch für Anhänge wie z.B. Bilder.	
Daten werden nicht in Drittländer weitergeleitet, die nicht der Norm der EU-DSGVO entsprechen	

Nach einer individuellen Überprüfung Ihres Unternehmens gibt es evtl. noch sehr viel mehr Punkte, die berücksichtigt werden müssen.

Eine Nutzungs- bzw. Betriebsvereinbarung, die genau auf Ihr Unternehmen angepasst ist, ist ein sehr wichtiges Dokument, um die IT-Sicherheit und den Datenschutz zu regeln.

Sie wollen das Arbeiten im "Homeoffice" für Ihre Beschäftigten ermöglichen und benötigen Unterstützung bei der Prüfung, Dokumentation und Umsetzung?

Dann rufen Sie uns an oder schreiben eine Mail.
Wir unterstützen Sie gern.

Telefon: 033200 639904
Mail: info@pro-dat.de