exkulpa

Handreichung zum Homeoffice

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de

Begriffsbestimmung

Homeoffice wird gemeinhin als Oberbegriff für das Arbeiten außerhalb der Dienststätte oder des Dienstsitzes des Arbeitgebers verwendet. Wer nicht im Büro arbeitet, macht Homeoffice. Doch es gibt unterschiede, ob jemand an einigen Tagen in der Woche im Büro arbeitet und an den anderen Tagen von zu Hause aus (sogenannte alternierende Telearbeit), ob jemand unterwegs arbeitet, zum Beispiel in einem Co-Working-Space, in einem Hotel oder Café (sogenanntes mobiles Arbeiten), ob sich jemand auf Dienstreise befindet und hierbei Gelegenheiten zur Produktivität nutzt, z.B. arbeiten im Flugzeug oder der Bahn (sogenannte Entsendung). Der Begriff Homeoffice, also das reine Arbeiten in einem häuslich eingerichteten Büro, wird als Telearbeit bezeichnet.

In den meisten Fällen, in denen Mitarbeitern flexible Arbeitszeit- und Arbeitsortmodelle nutzen, handelt es sich um eine Mischform der oben erwähnten Unterteilungen. Zudem ist der Begriff des Homeoffice eingedeutscht und wird synonym verwendet, weshalb auch diese Handreichung den Begriff allgemein auf das flexible Arbeiten außerhalb der Firma anwendet.

Welche Vorgaben gibt es beim Homeoffice zu beachten?

Das Homeoffice stellt eine Querschnittsmaterie dar, bei der insbesondere folgende Aspekte beachtet werden müssen:

Datenschutz: Wer ist eigentlich für die Daten, die zu Hause oder unterwegs verarbeitet werden verantwortlich? Welche besonderen Datenschutzmaßnahmen müssen beachtet werden, wenn Daten räumlich außerhalb des Unternehmens verarbeitet werden? Und wie kann der Verantwortliche, also die Geschäftsleitung, hierauf Einfluss nehmen?

IT-Sicherheit: Wie wird im Homeoffice die Sicherheit der IT-Infrastruktur gewährleistet? Mit welchen Mitteln kann das erhöhte Aufkommen digitalen Datentransports sichergestellt werden? Wie wird gewährleistet, dass alle Arbeitsgeräte (Laptop, Smartphone, Tablet, USB-Stick usw.) entsprechend ihrer Verwendungszwecke konfiguriert und stets upgedatet werden? Was gilt es hinsichtlich eines Fernzugriffs durch den Arbeitgeber, bzw. durch die IT-Abteilung zu beachten? Welche Gefahren drohen durch Cyber-Angriffe und wie wird im mobilen Arbeiten (z.B. bei Mobilgeräten) für ausreichend Cyber-Security Sorge getragen?

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de

Arbeitssicherheit: Welche Vorgaben stellen die Arbeitsstättenverordnung und das Arbeitsschutzgesetz an einen Homeoffice-Arbeitsplatz? Welche Gefahren oder Beeinträchtigungen drohen dem einzelnen Mitarbeiter an seinem Schreibtisch zu Hause oder beim Arbeiten unterwegs?

Arbeitsrecht: Was gilt hinsichtlich des Arbeitszeitgesetzes, des Geschäftsgeheimnisgesetzes? Ist – sofern vorhanden – der Betriebsrat einzubeziehen? Welche Überwachungs- und Sanktionsmöglichkeiten hat der Arbeitgeber gegenüber seinen sich im Homeoffice befindlichen Angestellten?

Steuern und Kosten: Wer trägt die Kosten für Anschaffungen, etwa eines Monitors oder Bürostuhls im Homeoffice? Wie werden die entstandenen Kosten bei erlaubter Privatnutzung dienstlicher Geräte (z.B. Smartphone) aufgeteilt? Was gilt als geldwerter Vorteil?

Versicherungsschutz: Wann greift welcher Versicherungsschutz, etwa bei Verlust, Defekt oder Diebstahl von Dienstgeräten, Arbeitsunfällen oder Berufskrankheiten des Arbeitnehmers?

EDV-Ausstattung: Welche Hard- und Software ist für das Arbeiten außerhalb des Unternehmens geeignet? Welche Tools uns Apps (z.B. für die Videokonferenz oder das Austauschen von Daten über eine Cloud) können verwendet werden und worauf ist bei der Auswahl zu achten? Was gilt hinsichtlich des Einsatzes von SaaS-Lösungen (Software as a Service) zu berücksichtigen?

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de

Checkliste

Die folgende Checkliste soll Ihnen einen Überblick darüber geben, was beim Homeoffice zu beachten ist. Wo möglich, werden allgemeine oder konkrete Tipps zur Umsetzung gegeben. Da es sich – wie erwähnt – beim Thema Homeoffice um eine Querschnittsmaterie handelt, sollte die erste Regel lauten: **Beraten Sie sich stets im Einzelfall mit Fachleuten.** Dies sind in der Regel der Arbeitsrechtler, der Datenschutzbeauftragte, die Fachkraft für Arbeitssicherheit und die IT-Abteilung. Sämtliche Maßnahmen zur Ermöglichung des mobilen Arbeitens sollten aufeinander abgestimmt sein, um Haftungsrisiken zu vermeiden und um den organisatorischen und bürokratischen Aufwand so gering, wie möglich zu halten.

Welche Maßnahmen konkret zu ergreifen sind, ist häufig vom Einzelfall und den individuellen Umständen abhängig, also z.B. von der Unternehmensgröße, von branchenspezifischen (gesetzlichen) Anforderungen, von der Unternehmensorganisation und -Philosophie und vielem Weiteren. Bei der Wahl der zu treffenden Maßnahmen ist aber immer auch der Verhältnismäßigkeitsgrundsatz zu wahren; oder anders ausgedrückt: Nicht mit Kanonen auf Spatzen schießen.

Aus all dem zuvor Genannten ergibt sich, dass die Checkliste nicht abschließend sein kann und nicht alle Punkte bei jedem Verwender zu denselben Maßnahmen führen werden.

Thema	Empfehlungen	Eigene Anmerkungen
Verantwortlichkeit	Auch wenn (personenbezogene) Daten räumlich das Unternehmen verlassen, wenn also Daten im Homeoffice verarbeitet werden, bleibt die Geschäftsleitung/der Vorstand für die Daten verantwortlich. Da Daten, die außerhalb des Unternehmens verarbeitet werden in der Regel dem direkten Einflussbereich des Arbeitgebers, also des Verantwortlichen, entzogen werden, ist es umso wichtiger, dass sämtliche technische und organisatorische Maßnahmen vom Arbeitgeber ergriffen werden, die gewährleisten, dass ihm jederzeit umfangreiche Möglichkeiten der Einflussnahme auf die Daten und deren Sicherheit zur Verfügung stehen. **Regel:** Der Verantwortliche ist und muss Herr über „seine“ Daten bleiben.	
Schriftliche Regelung	Stellen Sie schriftlich klare Regelungen auf (z.B. eine Richtlinie zum mobilen Arbeiten/Homeoffice-Richtlinie), welche Voraussetzungen auf Seiten des Arbeitgebers und des Arbeitnehmers vorliegen müssen, damit Homeoffice durchgeführt werden kann. Die Regelungen müssen den betroffenen Mitarbeitern bekannt sein und stets den aktuellsten Stand wiedergeben. Eine solche Regelung schafft Transparenz und Sicherheit bei den Mitarbeitern, die hierdurch erfahren,	

Thema	Empfehlungen	Eigene Anmerkungen
Schriftliche Regelung	was sie konkret zu beachten haben. Die Mitarbeiter werden hierdurch gleichzeitig für etwaige Risiken sensibilisiert. Zugleich ist eine schriftliche Regelung zum Homeoffice wichtig für den Arbeitgeber, um im Streitfall etwaige Ansprüche gegenüber dem Angestellten einfacher geltend machen zu können, bzw. um sich gegen etwaige Ansprüche des Arbeitnehmers zu verteidigen. Im Falle von Verstößen gegen die Regelung stehen dem Arbeitgeber Sanktionsmöglichkeiten zur Verfügung; je nach Regelung etwa eine Abmahnung oder die Versagung des Homeoffices für die Zukunft. Im Datenpannenfall (z.B. durch Fehlverhalten des Arbeitnehmers) kann eine gute Regelung für den Arbeitgeber enthaftende oder haftungsregulierende Wirkung entfalten. Inhalte einer solchen schriftlichen Regelung können die Punkte dieser Checkliste sein.	
Betriebsrat einbinden	Sofern vorhanden, prüfen Sie, ob der Betriebsrat zu involvieren ist. In jedem Fall empfiehlt sich, diesen zumindest vorab über die geplante Einführung des Homeoffice und den zu treffenden Regelungen zu informieren, da dieser eventuell einen Unterrichtungsanspruch nach dem Betriebsverfassungsgesetz hat (etwa nach §§ 80 Abs. 2; 87 Abs. 1; 90 Abs. 1 BetrVG). Dies trifft insbesondere zu bei Maßnahmen zur technischen Einrichtung des Arbeitsplatzes und der Durchführung von Kontrollen.	
Privatnutzung, BYOD, Präventivmaßnahmen	Idealerweise werden Mitarbeiter im Homeoffice mit dienstlichen Geräten ausgestattet, da hierbei der Arbeitgeber Eigentümer der Geräte bleibt und damit seine Hoheit über die Geräte und die sich darauf befindlichen Daten behält. Gestattet der Arbeitgeber zudem die private Nutzung der Dienstgeräte, muss unbedingt darauf geachtet werden, dass dienstliche und private Daten und Informationen voneinander getrennt verarbeitet und gespeichert werden. Für den Umfang der Privatnutzung sollten ebenfalls Regelungen getroffen werden. Die Privatnutzung sollte vom Arbeitgeber immer unter Vorbehalt erteilt werden, etwa unter dem Vorbehalt, die Erlaubnis jederzeit wieder aufheben oder einschränken zu können und dass die Qualität und Quantität der Arbeit sowie die Sicherheit der Daten und Systeme nicht negativ beeinträchtigt oder gefährdet werden. Auf diese Weise wird eine betriebliche Übung vermieden und der Arbeitgeber behält größtmöglichen Handlungs- und Optimierungsspielraum was die Regelung und Umsetzung der Gerätenutzung angeht. Unbedingt vermieden werden sollte eine reine Duldung der Privatnutzung dienstlicher Geräte. Arbeitsrechtlich kann sich aufgrund einer Duldung u.U. ein Anspruch des Arbeitnehmers auf die Privatnutzung dienstlicher Geräte und Einrichtungen ergeben. Daher die wichtige Empfehlung: Geben Sie eindeutig bekannt, ob und in welchem Umfang die Privatnutzung verboten oder erlaubt ist.	

Thema	Empfehlungen	Eigene Anmerkungen
Privatnutzung, BYOD, Präventivmaßnahmen	Nach Möglichkeit sollte die Nutzung privater Geräte zu dienstlichen Zwecken (sogenanntes Bring Your Own Device, kurz: BYOD) vermieden werden. BYOD ist zwar grundsätzlich möglich, bedarf aber besonderer technischer und organisatorischer Regelungen, z.B. um dienstliche von privaten Daten zu trennen oder um Zugriff und Kontrollen (etwa durch Fernwartung) auf den privaten Geräten durchführen zu dürfen. In bestimmten Situationen, etwa in unerwarteten Krisensituationen, in denen schnelles Handeln notwendig ist (etwa im „Corona-Fall“) und eine Beschaffung dienstlicher Geräte für alle Mitarbeiter logistisch und/oder finanziell nicht zu stemmen ist, die Gesundheit der Mitarbeiter aber erhöhte Priorität besitzt, kann der Verhältnismäßigkeitsgrundsatz herangezogen werden, weshalb auch der Einsatz von BYOD ggf. unter vereinfachten Bedingungen zu ermöglichen ist. Wichtig aber ist, dass auch in solchen Fällen sämtliche zumutbaren Maßnahmen getroffen werden müssen, um die Einhaltung des Datenschutzes umfänglich zu gewährleisten. Während die Privatnutzung des dienstlichen Laptops oder Smartphones noch recht gut zu regeln ist, sieht dies bei der privaten Nutzung des dienstlichen E-Mail-Postfachs anders aus. Aufgrund von Aufbewahrungspflichten von Schriftverkehr, dem Persönlichkeitsschutz des Mitarbeiters in Bezug auf private E-Mails sowie erschwerten Zugriffs- und Kontrollmöglichkeiten des Arbeitgebers, sollte die Privatnutzung des dienstlichen E-Mail-Postfachs grundsätzlich (schriftlich) verboten sein. Vertiefende Informationen hierzu finden Sie auch in unserem Blog-Artikel „Zugriff auf E-Mails von Kollegen in deren Abwesenheit“ unter https://exkulpa.de/datenschutz/zugriff-auf-e-mails-von-kollegen/ Mitarbeiter sollten regelmäßig (es empfiehlt sich mindestens jährlich) zu Datenschutz und Datensicherheit geschult werden. Wenn mobiles und Arbeiten im Homeoffice zur Regel gehört, sollten diesbezüglich Sensibilisierungen und Schulungen auch themen-/schwerpunktbezogen stattfinden, etwa zu Risiken, Gefahren und Vorsichtsmaßnahmen beim mobilen Arbeiten und im Homeoffice. Schulungen dieser Art können z.B. als Live-, Online- oder Webinar-Schulung stattfinden. Gerne sind wir Ihnen bei der Organisation und Durchführung von Schulungen und Sensibilisierungsmaßnahmen behilflich und finden die für Sie und Ihre Mitarbeiter passende Lösung. Sprechen Sie uns einfach an unter https://exkulpa.de/akademie/	
Technische Maßnahmen & IT-Sicherheit	Dienstgeräte sollten von einer zentralen Stelle (i.d.R. der IT-Abteilung) nach einem einheitlichen Konzept vorkonfiguriert werden, bevor diese an die Mitarbeiter ausgehändigt werden. Die einzelnen und konkreten Sicherheits-Konfigurationen sind abhängig von a) der Entscheidung, ob das Gerät auch für private Zwecke genutzt werden darf. In diesem Fall ist insbesondere auf eine saubere Trennung dienstlicher und privater Daten zu achten. Hierunter zählen etwa	

Thema	Empfehlungen	Eigene Anmerkungen
Technische Maßnahmen & IT-Sicherheit	Container-Lösungen, das Verbot der Nutzung bestimmter Apps, die Zugriffe auf andere Apps benötigen (z.B. Telefonbuch, Kamera, Foto-App, Standortabfrage). b) der Möglichkeit des Fernzugriffs, z.B. durch die eigene IT-Abteilung oder durch einen externen IT-Dienstleister für Wartungsleistungen. Durch den Fernzugriff ist es i.d.R. technisch möglich, auf sämtliche sich auf dem Gerät befindlichen Daten zuzugreifen, bzw. diese einzusehen, also auch auf die privaten Daten des Mitarbeiters. c) den Datenkategorien, die durch die Mitarbeiter im Homeoffice verarbeitet werden. Grundsätzlich gilt: Je sensibler die Daten, desto höher müssen die getroffenen Schutzmaßnahmen sein. Diese sind dann bereits bei der Anschaffung und der Konfiguration der Geräte sowie dem Umfang einer etwaigen Privatnutzungserlaubnis zu berücksichtigen. Bitte beachten Sie: Daten können nicht nur aufgrund ihres Informationsgehaltes (z.B. Zahlungsdaten) als sensibel einzustufen sein, sondern auch aufgrund ihres Umfangs (z.B. eine hohe Anzahl an E-Mail-Adressen) oder per Gesetz (z.B. alle personenbezogenen Daten nach Art. 9 DSGVO, etwa Gesundheitsdaten). Technische Maßnahmen sollten hierbei so gewählt werden, dass sie a) die mit Hilfe des Gerätes verarbeiteten Daten b) schützen und c) die allgemeine IT-Infrastruktur schützen. Es sollten die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität gewährleistet sein. Hierbei kann sich an den Grundschutzkatalogen des Bundesamt für Sicherheit in der Informationstechnik (BSI) orientiert werden, die auf der Webseite des Bundesamtes frei verfügbar sind, etwa unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html und konkret zum Homeoffice unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_2_4_Telearbeit.html Beispiele für technische Maßnahmen: ○ VPN-Verbindung ○ Remote-Zugriff für schnelle technische Unterstützung ○ Systemseitige Sperrungen (einzelner Systeme/des Geräte) bei Inaktivität ○ Ausreichender Passwortschutz; 2-Faktor-Authentifizierung; passwortgeschützter Bildschirmschoner ○ Keine lokale Datenspeicherung, bzw. regelmäßige Synchronisierung ○ Verschlüsselung von Hardware und Datenträgern (Festplatten, USB-Sticks usw.), eventuell auch Verschlüsselung einzelner Daten/Datensätze, Ablageverschlüsselung auf mobilen Geräten ○ Nutzung von Black- und Whitelists ○ Sperrung von Ports ○ Virenschutz, Firewall	

Thema	Empfehlungen	Eigene Anmerkungen
Technische Maßnahmen & IT-Sicherheit	○ Rollen und Berechtigungen nach dem kneed-to-know-Prinzip einrichten ○ Container-Lösung o.Ä. bei erlaubter Privatnutzung ○ Sicherstellung von regelmäßigen Updates ○ Für das Arbeiten unterwegs sollten Laptopbildschirme vor der Einsichtnahme Unbefugter geschützt sein, z.B. mittels einer entsprechenden Display-Blickschutzfolie. Je nach Anzahl der mobilen Geräte empfiehlt sich die Nutzung eines Asset Managements zur Dokumentation der Geräte sowie eines Mobile Device Managements zur Verwaltung mobiler Endgeräte. Gerne sind wir Ihnen bei der Bewertung und Umsetzung von IT-Sicherheitsmaßnahmen im Homeoffice behilflich. Sprechen Sie uns gerne an unter https://exkulpa.de/it-sicherheit-leistungsuebersicht/	
Organisatorische Maßnahmen	Eine der wichtigsten organisatorischen Maßnahmen stellt die eingangs erläuterte schriftliche Regelung (Richtlinie) dar. Administratorenrechte und Fernzugriffsmöglichkeiten für Geräte, die im Homeoffice genutzt werden, sollten klar definiert und geregelt werden. Bei erlaubter Privatnutzung der Geräte sollte klar geregelt sein, ob und welche zusätzliche Software/Apps der Nutzer aufspielen und nutzen darf. Hierbei bietet sich ein Freigabeprozess an, der sicherstellt, dass nur durch die IT-Abteilung freigegebene Tools verwendet werden dürfen. Nach Möglichkeit sollte auf den Einsatz von privaten mobilen Datenträgern (z.B. USB-Sticks) verzichtet werden. Stattdessen sollten betriebsseitig Speichermedien angeschafft und verwendet werden; idealerweise solche, die besondere Sicherheitsvorkehrungen aufweisen, etwa eine Verschlüsselung. Mitarbeiter sollten zur Arbeit im Homeoffice, den damit verbundenen Risiken und den vom Unternehmen vorgegebenen Verhaltensregeln sensibilisiert werden. Dies könnte mittels Live- oder Online-Schulung oder Ausgabe eines Merkblatts geschehen. Onboarding: Wichtig ist, dass auch neue Mitarbeiter informiert und sensibilisiert werden, bevor ihnen die Arbeit im Homeoffice ermöglicht wird. Offboarding: Es sollte einen zentralen Prozess geben, der sicherstellt, dass ausscheidende Mitarbeiter alle Geräte, Ausdrucke u.Ä. rechtzeitig zurückgeben und dass ihnen Berechtigungen entzogen werden. Es sollten Regelungen für den Fall von Datenpannen, Verlust, Diebstahl und Defekt von Geräten getroffen werden. Mitarbeitern sollte für diese Fälle ein einheitlicher, zentraler Kommunikationsweg und entsprechende Ansprechpartner (z.B. IT-Abteilung, Datenschutzbeauftragter) bekannt sein. Zutritts-, Zugriffs- und Kontrollmöglichkeiten (z.B. Vor-Ort-Kontrolle im Homeoffice, Remote Stichprobenkontrollen) des Arbeitgebers sollten unbedingt geregelt werden.	

Thema	Empfehlungen	Eigene Anmerkungen
	Fehlverhalten, Verstöße gegen getroffenen Regelungen und etwaige Sanktionen sollten ebenfalls transparent geregelt und allen Mitarbeitern im Homeoffice bekannt gegeben werden.	
Ausstattung des Homeoffice	Bei der Ausstattung des Homeoffice ist auch auf die Umsetzung und Einhaltung der Datenschutz-Grundsätze zu achten, das heißt insbesondere: ○ Fremden (hierzu gehören auch Familienmitglieder) muss der Zugriff auf dienstliche Daten und Dokumente verwehrt werden. Das gilt für physische Daten, wie z.B. Papierdokumente und Akten, als auch für digitale Daten. ○ Laptops und Monitore sind bei Verlassen des Arbeitsplatzes zu sperren. ○ Mobilgeräte sollten über ausreichenden Zugriffsschutz verfügen, z.B. Passworteingabe zur Entsperrung, Abschaltzeit bei Inaktivität möglichst kurz halten usw. ○ Werden Geräte auch von Familienmitgliedern genutzt, ist sicherzustellen, dass die dienstlichen Daten so abgelegt und geschützt sind, dass auf diese nicht zugegriffen werden kann. ○ Ausdrucke sollten so sparsam wie möglich getätigt werden. ○ Nicht mehr benötigte Papierdokumente sollten so vernichtet werden, dass sie nicht oder nur unter größten Anstrengungen wiederherstellbar sind. Papier geknüddelt in den Papierkorb zu verfrachten stellt keine ordentliche Datenvernichtung dar. Achtung gilt auch bei der Entsorgung im Papierhausmüll. Wenn nötig, sollte der Homeoffice-Arbeitsplatz über einen abschließbaren Schrank oder Rollcontainer verfügen, um Akten und Papierdokumente zugriffssicher aufzubewahren. Auch im Homeoffice sollten so wenige Daten anfallen, wie möglich. Es gilt das kneed-to-know-Prinzip, das heißt, Mitarbeiter sollten auch im Homeoffice nur mit denjenigen Daten arbeiten können, die sie zur Erfüllung ihrer Aufgaben unbedingt benötigen. Ein bestehendes Rollen- und Berechtigungskonzept sollte daher auch im Homeoffice Anwendung finden. Es sollte eine stabile Internetverbindung bestehen, gerade wenn aus dem Homeoffice heraus an Telefon- und Videokonferenzen teilgenommen wird. Die Internetverbindung im Homeoffice muss nach dem Stand der Technik geschützt sein (z.B. Passwortschutz). Besondere Vorsicht gilt demnach insbesondere bei offenen Netzwerken und Internetzugängen, die mit der Familie, Nachbarn, der WG oder der Hausgemeinschaft geteilt und gemeinsam genutzt werden.	
Software, Apps, Tools	Bei der Arbeit im Homeoffice wird häufig bekannte, mobile, einfach einzurichtende und/oder kostenlose Software, beispielsweise aus dem App-Store, verwendet. Tools für die Videokonferenz, Cloud-Storage zum Austausch von Daten und weitere oft cloudbasierte Programme sind meist praktisch, intuitiv zu bedienen und geräteübergreifend nutzbar. Bei der Verwendung solcher Software sind jedoch einige wichtige Punkte zu beachten:	

Thema	Empfehlungen	Eigene Anmerkungen
Software, Apps, Tools	○ Nicht jede frei verfügbare Software ist vom Herausgeber für den kommerziellen/gewerblichen Gebrauch freigegeben. Oft sind sie nur für den privaten Gebrauch zugelassen. Daher sollte sich der erste Blick vor dem Download oder dem Erwerb auf die Nutzungsvereinbarung oder die AGBs richten. ○ Viele Anbieter bekannter Software bieten eine separate, meist kostenpflichte, Business-Version an. In vielen Fällen ist diese der kostenlosen Version vorzuziehen, da mehr Funktionen zur Verfügung stehen, die im gewerblichen Umfang besonders sinnvoll sind. Zudem sind Business-Versionen meist nicht auf die private Nutzung beschränkt (dies deutet bereits die Verwendung des Begriffs „Business“ an). Nicht selten bieten kostenpflichtige Tools auch mehr Sicherheit, z.B. bei der Datenverarbeitung oder der Datenspeicherung, als kostenlose Versionen. ○ Achten Sie bei der Auswahl unbedingt darauf, wer hinter einer Software steckt. Viele Big Player und Software-Giganten bieten unter verschiedenen Namen eine Vielzahl von Apps an. Hierbei sollte ein besonderes Augenmerk darauf liegen, wo der Anbieter seinen Firmensitz hat, wo er die Daten verarbeitet/speichert, und auf welche Subdienstleister (z.B. Hoster) er zurückgreift. An die strengen Anforderungen der Datenschutzgrundverordnung (DSGVO) sind nur EU-Staaten gebunden, und solche, die außerhalb der EU über ein anerkanntes, angemessenes Datenschutzniveau verfügen. Drittländer, zu denen auch die USA gehören, haben keine oder deutlich schwächere Datenschutzgesetze. Auch IT-Sicherheitsgesetze, die manche Anbieter von Software oder Hoster zu beachten haben, sind längst nicht überall auf der Welt Standard. Als Faustregel gilt: Anbieter aus dem Inland oder der EU müssen in der Regel einen besonders hohen Sicherheitsstandard einhalten. ○ Insbesondere mobile Anwendungen erfassen, und werten oft das Benutzerverhalten und sogar den Standort aus. Dies geschieht z.B. über diverse Sensoren (etwa GPS, Bewegungssensoren). In aller Regel trägt der Arbeitgeber auch die Verantwortung für derartige Datenverarbeitungen, die mitunter auch eine Auswertung des Arbeitnehmers darstellen kann. Zudem greifen mobile Anwendungen häufig Daten anderer Apps ab und benötigen (häufig unnötige) Zugriffsberechtigungen auf andere Anwendungen. Schon deshalb sollte Software, die für den dienstlichen Gebrauch gedacht ist, zuvor von zentraler Stelle (z.B. der IT-Abteilung) freigegeben werden müssen. ○ Sofern über Software personenbezogene Daten verarbeitet werden (z.B. bei der Verwendung eines Tools für die Durchführung von Videokonferenzen), sind diese i.d.R. im Verzeichnis von Verarbeitungstätigkeiten (VVT; Art. 30 DSGVO) aufzunehmen. Unter Umständen ist für einzelne Tools auch eine Risikobewertung, die sogenannte Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen, bei der zwingend der DSB zu involvierend ist. ○ Bei SaaS-Produkten (Software as a Service; also über das Internet bereitgestellte Anwendungen/Cloud-Lösungen) wird i.d.R. ein	

Thema	Empfehlungen	Eigene Anmerkungen
	Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO mit dem Anbieter zu schließen sein. Der Anbieter muss zudem ein ausreichendes Datensicherheitskonzept vorhalten können.	
Arbeitssicherheit	Auch im Homeoffice trifft den Arbeitgeber die Pflicht, Arbeitsunfälle, gesundheitliche Beeinträchtigungen und etwaige Folgerisiken, wie etwa Berufskrankheiten usw. zu erkennen und zu vermeiden, bzw. Mitarbeitern diesen Risiken nicht unnötig auszusetzen. Dies betrifft demnach auch die Ausstattung des Homeoffices (vgl. §§ 1 ff. ArbSchG und § 2 Abs. 7 ArbStättVO). Hierzu zählen insbesondere Anforderungen an die Beleuchtung des Arbeitsplatzes, der Größe und Position des Monitors, des Sitzkomforts und etwaige weitere Gefährdungen nach dem Arbeitsschutzgesetz (z.B. §§ 3, 4 ArbSchG) und der Arbeitsstättenverordnung (ArbStättV). Ein Homeoffice-Arbeitsplatz am Küchentisch entspricht demnach in aller Regel nicht den gesetzlichen Vorschriften über einen ordentlichen Arbeitsplatz. Es empfiehlt sich eine Gefährdungsbeurteilung (§ 5 Abs. 1 ArbSchG, § 3 ArbStättV) mit der Fachkraft für Arbeitssicherheit zu erstellen, diese zu dokumentieren und ggf. eine Arbeitssicherheitsunterweisung zum Arbeiten im Homeoffice durchzuführen. Mit dieser Beurteilung kann durch den Arbeitgeber und den Arbeitnehmer eingeschätzt werden, welche besonderen gesundheitlichen Risiken vorhanden und wie diese einzudämmen sind. Ergibt die Gefährdungsbeurteilung, dass der Telearbeitsplatz (Homeoffice) aus Gründen der Arbeitssicherheit oder des Gesundheitsschutzes des Mitarbeiters nicht geeignet ist (u.a. ungeeignete Möbel, fehlende Beleuchtung), sind durch den Arbeitgeber Maßnahmen einzuleiten und ggf. zu finanzieren. In einer schriftlichen Vereinbarung zwischen Arbeitgeber und Arbeitnehmer sollten Regelungenwie die folgenden aufgenommen werden: ○ Der Telearbeitsplatz muss erforderlichen Arbeits- und Gesundheitsschutzvorgaben entsprechen. ○ Arbeitgeber und Arbeitnehmer einigen sich, dass im Falle der Verweigerung zur Mitwirkung geeigneter Arbeitsschutz- und Gesundheitsschutzmaßnahmen durch den Arbeitnehmer, der Arbeitgeber die Vereinbarung zum Telearbeitsplatz widerrufen kann. Da es i.d.R. nicht möglich ist, jeden Homeoffice Arbeitsplatz persönlich zu besichtigen, um die dortigen Gegebenheiten und das Arbeitsumfeld zu bewerten, empfiehlt sich die Verwendung einer detaillierten Checkliste. Eine solche Checkliste sollte folgendes beinhalten: a) Einen ersten Teil, in dem der Arbeitgeber konkrete Voraussetzungen an den Arbeitsplatz und das Umfeld vorgibt, z.B. einen separaten Raum und Schreibtisch (anstelle des Arbeitens am Küchentisch o.Ä.), eine stabile Internetverbindung mit einer Mindestbandbreite, dass der Internetzugang gesichert und nur einem eingeschränkten	

Thema	Empfehlungen	Eigene Anmerkungen
Arbeitssicherheit	Personenkreis zur Verfügung steht, ein abschließbarer Schrank oder Rollcontainer usw. b) Einen zweiten Teil, in dem der Arbeitnehmer seinen Arbeitsplatz im Homeoffice beschreibt, z.B. wo sich dieser befindet (im Keller, Erdgeschoss, Dachgeschoss), wer Zutritt hat, evtl. um was für eine Art der Wohngemeinschaft es sich handelt (Ein- oder Mehrpersonenhaushalt, Wohngemeinschaft), ob eine ausreichende Belichtung vorhanden ist, wie die Papierentsorgung stattfindet u.a. c) Einen vierten Teil, der als Inventarliste zu führen ist über die dem Arbeitnehmer überlassenen Arbeitsmittel. d) Einen vierten Teil, in dem sich der Mitarbeiter dazu verpflichtet, die Vorgaben des Arbeitgebers in Bezug auf den Homeoffice Arbeitsplatz einzuhalten, relevante (räumliche) Veränderungen dem Arbeitgeber mitzuteilen und dem Arbeitgeber ein Kontroll-, bzw. Besuchsrecht einzuräumen. Gerne sind Ihnen hierbei unsere Kollegen aus dem Bereich Arbeitssicherheit behilflich. Sie können Sie unter https://exkulpa.de/arbeitssicherheit/ erreichen.	
Arbeitsrecht	Einen generellen Anspruch auf Homeoffice haben Arbeitnehmer nicht. Je nachdem, wie das Arbeiten im Homeoffice geregelt werden soll, sind auch Vorgaben aus dem Arbeitsrecht zu beachten, etwa bzgl. Erreichbarkeit und Arbeitszeiten nach dem Arbeitszeitgesetz (ArbZG). Geregelt werden sollte, wie mit Überstunden zu verfahren ist: Wie werden Überstunden im Homeoffice dokumentiert? Unter welchen Voraussetzungen werden diese vergütet (z.B. nur nach vorheriger Anordnung von Überstunden durch den Arbeitgeber)? Arbeitsrechtlich besonders relevant ist auch die Kontrolle der sich im Homeoffice befindlichen Arbeitnehmer. Die seit 2017 gültige Arbeitsstättenverordnung (ArbStättV) schreibt vor, dass bestimmte Aspekte und Regelungen für das Homeoffice im Arbeitsvertrag oder in einem Zusatz zu diesem vereinbart und festgehalten werden müssen. Hierin sollte auch ein Kontroll-, bzw. Besichtigungsrecht des Arbeitgebers (oder eines anderen Kontrollorgans, etwa Betriebsrat oder DSB) enthalten sein. Festgelegt werden sollte auch die Dauer der Möglichkeit des Homeoffice, ob dieses unbefristet oder befristet gewährt wird und unter welchen Bedingungen die Möglichkeit des Homeoffice von beiden Parteien beendet werden kann oder muss, z.B. wenn aufgrund innerbetrieblicher Organisation alle Mitarbeiter in der Firma arbeiten sollen oder wenn aufgrund von Verstößen oder Fehlverhalten der Arbeitgeber die Möglichkeit zum Homeoffice entziehen möchte. Um arbeitsrechtliche Haftungsfallen zu vermeiden, empfiehlt sich die Rücksprache mit einem entsprechend fachkundigen juristischen Beistand, z.B. einem Fachanwalt für Arbeitsrecht.	

Thema	Empfehlungen	Eigene Anmerkungen
Steuern & Kosten **Steuern & Kosten**	Viele Anschaffungen fürs Homeoffice sind vom Arbeitgeber zu tragen. Anschaffungen in diesem Sinne können vom Drucker und Monitor bis hin zum Bürostuhl, Schreibtisch und der Beleuchtung sein. Sofern Dienstliche Geräte und Einrichtungen vom Arbeitnehmer auch privat genutzt werden dürfen, ist zu prüfen, ob hierin ein geldwerter Vorteil zu sehen ist. In jedem Fall sollten Kosten und Aufwendungen für Anschaffungen, Geräte, Internet- und Telefongebühren (z.B. für Festnetz und DSL) und eine etwaige Beteiligung des Arbeitgebers geregelt werden. Hierbei sollten auch Kosten durch die Nutzung mobilen Datenvolumens oder kostenintensiven Auslandsgesprächen berücksichtigt werden.	
Cyber-Security & Risiken	Unter Umständen eröffnet das Arbeiten im Homeoffice besondere Risiken durch Cyberangriffe. Die gewohnten Abwehrmechanismen, die im Büro durch die IT-Abteilung initiiert sind, fehlen häufig im heimischen Netz, so dass die Anzahl von Spam und Cyberangriffen durchaus erhöht sein kann. Kriminelle machen auch vor Krisen keinen Halt, weshalb auch in Zeiten von „Corona“ besondere Vorsicht geboten ist vor Cyber-Kriminellen. So warnt das Landeskriminalamt Niedersachsens derzeit vor betrügerischen Fakeshops, die den Medienhype um den Corona-Virus ausnutzen https://www.polizei-praevention.de/aktuelles/fakeshop-nutzt-medienhype-um-corona-virus-aus.html Social Engineering, also das Ausspähen sozialer Gegebenheiten, um zielgerichtet Schwachstellen bei Mitarbeitern auszunutzen, stellt im Homeoffice ein besonderes Risiko dar, da Kriminelle häufig die Aktivitäten der Mitarbeiter in den sozialen Netzwerken nutzen. Auf diese Weise kommen sie an authentische Informationen, die sie ausnutzen, um z.B. per Telefon, Besuch der privaten Wohnung oder per E-Mail-Informationen zu streuen, abzufangen, oder um Schadsoftware ins Unternehmen einzuspielen.	
Versicherungsschutz	Auch im Homeoffice sind Mitarbeiter grundsätzlich über den Arbeitgeber unfallversichert. Jedoch nur im Rahmen ihrer tatsächlichen dienstlichen Tätigkeit. Bei einem Sturz auf dem Weg zum Briefkasten oder zur Wohnungstüre, um dem Paketboten zu öffnen, kann schon entscheidend sein, ob mit dem Gang zum Briefkasten oder zur Türe ein dienstlicher oder privater Zweck verfolgt wird. Anders als in der Firma sind Unfälle bspw. auf dem Weg zur Toilette oder zur Küche i.d.R. nicht über den Arbeitgeber versichert. Auch im Homeoffice gilt im Falle eines Unfalls eine Meldepflicht an den Arbeitgeber, da bei einem Arbeitsausfall ab drei Tagen ebenfalls eine Meldepflicht an die zugehörige Berufsgenossenschaft gesendet werden muss. Der Unfall muss zudem detailliert in einem Unfallmeldebogen erfasst werden.	