

Unsere Experten haben sorgfältig Dokumente erstellt, die den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprechen. Diese Vorlagen können jederzeit abgespeichert, bearbeitet und an Mitarbeiter, Kunden oder Geschäftspartner weitergegeben werden.

Wir verstehen, dass jedes Unternehmen einzigartige Anforderungen hat. Deshalb sind unsere Vorlagen flexibel und können an Ihre individuellen Bedürfnisse angepasst werden. Sie bieten eine solide Grundlage, auf der Sie aufbauen können, um sicherzustellen, dass Ihre Datenschutzpraktiken den aktuellen gesetzlichen Vorgaben entsprechen.

Die Verwendung unserer Dokumente erleichtert Ihnen die Einhaltung der DSGVO und trägt dazu bei, den Datenschutz in Ihrem Unternehmen effizient zu gestalten.

Wenn Sie spezifische Anpassungen oder Beratung benötigen, stehen unsere Experten Ihnen gerne zur Verfügung.

Fon 0231 / 95 29 805

Mail info@lexallawconsultings.de

Richtlinien für den Home-Office Bereich zwischen Arbeitgeber und Arbeitnehmer

Soll ein Arbeitnehmer die Möglichkeit haben zeitweise mobil arbeiten zu können, muss dies vertraglich vereinbart werden. Eine Klausel im Arbeitsvertrag, nach der der Arbeitgeber den Arbeitnehmer von einem anderen Ort arbeiten lassen kann, genügt dafür nicht.

Achtung: Sofern die Arbeitstätigkeit regelmäßig im Auftrag des Arbeitgebers im Home-Office ausgeübt wird, kann diese Tätigkeit rechtlich als Heimarbeit eingestuft werden und fällt dann unter den Schutz des Heimarbeitsgesetzes (HAG). Da der Arbeitgeber grundsätzlich auch im Home-Office für die Einhaltung der Arbeitsschutzvorschriften und des Datenschutzes verantwortlich bleibt, sollte sich der Arbeitgeber ein Zutrittsrecht zur Privatwohnung des Arbeitnehmers einräumen lassen. Ein solches Zutrittsrecht bedarf der fortwährenden Zustimmung aller im fraglichen Haushalt lebenden volljährigen Bewohner. Das Zutrittsrecht sowohl in zeitlicher als auch in räumlicher Hinsicht auf das unbedingt Erforderliche beschränkt und an eine vorherige Ankündigung gekoppelt werden sollte.

Es ist denkbar sich vom Arbeitnehmer eine Beschreibung der im Home-Office bestehenden Datensicherheitsmaßnahmen geben zu lassen. Sofern begründete Zweifel vorliegen, gewährt der Arbeitnehmer dem Arbeitgeber das Recht zur Kontrolle des Telearbeitsplatzes die Wohnung des Arbeitnehmers zu betreten.

Richtlinienvereinbarung für den Home-Office Bereich

Zwischen

Unternehmen (Kontaktdaten)

Und

Mitarbeiter/In (Kontaktdaten, Geburtsdatum)

Ort der Tätigkeitsausübung im Home-Office

Straße/Hausnummer: _____

PLZ/Ort: _____

wird folgende Richtlinienvereinbarung für den Homeoffice Bereich vereinbart:

1. Bestimmung

Die in dieser Richtlinie festgelegten Bestimmungen legen die praktischen Anforderungen und Regeln für die Umsetzung von Home-

Office fest. Es ist wichtig zu beachten, dass diese Bestimmungen dem/der Mitarbeiter/in nicht automatisch das Recht geben, seine Arbeitsleistung von einem anderen Ort als dem vertraglich vereinbarten Arbeitsplatz zu erbringen. Um außerhalb des vertraglichen Arbeitsplatzes zu arbeiten, ist eine separate Erlaubnis erforderlich. Dies bedeutet, dass der Arbeitnehmer oder die Arbeitnehmerin in der Regel die ausdrückliche Genehmigung des Arbeitgebers einholen muss, bevor sie von zu Hause aus arbeiten dürfen. Die genauen Bedingungen und Anforderungen für diese Erlaubnis sollten in der Richtlinie oder in einem separaten Dokument festgelegt werden. Dies dient dazu, die Arbeitsbeziehung und die Erfüllung der Arbeitspflichten in einem solchen Umfeld klar zu regeln und sicherzustellen, dass die Arbeitgeberinteressen sowie die Arbeitnehmerrechte gewahrt werden.

2. Zweck

Diese Richtlinie regelt die Grundsätze der Verrichtung der Arbeitstätigkeit in den eigenen Wohnräumen (Home-Office) des/der Mitarbeiters/ Mitarbeiterin zur Einhaltung des Datenschutzes

außerhalb der Geschäftsräume. Eine sichere Verarbeitung von personenbezogenen Daten muss, wie im Unternehmen auch, bei der Verrichtung der Tätigkeit an einem Home-Office-Arbeitsplatz gewährleistet sein.

3. Geltungsbereich

Die vorliegende Richtlinie hat Gültigkeit für das gesamte Unternehmen und ist für sämtliche Mitarbeiter bindend, sofern sie dazu angehalten oder autorisiert werden, ihre Tätigkeit außerhalb der betrieblichen Geschäftsräume auszuüben. Es ist gestattet, Aufgaben im Home-Office zu erledigen, sofern keine rechtlichen Einschränkungen durch Gesetz oder Vertrag bestehen. Alle Daten sind ausschließlich gemäß den Vorgaben und Anweisungen des Arbeitgebers zu verarbeiten.

4. Rahmenbedingungen der Nutzung betrieblicher IT-Systeme im Home-Office

- a) Home-Office ist ausschließlich mit den hierfür vom Arbeitgeber bereitgestellten Mitteln (u.a. Hardware, Anwendungen, Verbindungsmöglichkeiten) erlaubt.
- b) Es ist ausschließlich die Nutzung durch die IT-Abteilung vorinstallierter oder durch diese im Einzelfall freigegebener Anwendungen zulässig. Dies gilt ausdrücklich auch für portable Software oder Betriebssysteme von Wechseldatenträgern.
- c) Die lokalen Laufwerke eines Computers sind für den Start von Anwendungen und den Betrieb während des Arbeitstages gedacht. Lokal verarbeitete Daten sind auch im Home-Office spätestens am Ende des Arbeitstages entsprechend zu sichern, z.B. auf durch Ablage serverbasierenden Laufwerken. Eine Ausnahme besteht nur dann, wenn die Verbindung zu den serverbasierenden Laufwerken o.ä. vorübergehend nicht gegeben ist. In diesem Falle ist die Sicherung bei nächstmöglicher Gelegenheit nachzuholen.
- d) Ausdrücke, die personenbezogene Daten beinhalten, dürfen im Home-Office nur erfolgen, wenn sichergestellt ist, dass diese sicher

vernichtet werden können (z.B. durch einen Shredder der Schutzklasse 2 oder höher gem. DIN66399).

Anmerkung: Ausdrucke sollten möglichst unterlassen werden oder sicher aufbewahrt und vor allem vernichtet (Schredder) werden.

e) Der Arbeitgeber trägt Sorge für die technische Absicherung der zum Home-Office bereitgestellten Arbeitsmittel.

f) Alle Störungen oder Auffälligkeiten bei der Tätigkeitsdurchführung im Home-Office sind dem Arbeitgeber unverzüglich zu melden.

5. Sicherungsvorkehrungen in den Wohnräumen des Arbeitnehmers

a) Die Durchführung von Home-Office, selbst innerhalb der eigenen Wohnräume, erfordert äußerste Sorgfalt und Beachtung bestimmter Sicherheitsaspekte, um sicherzustellen, dass die Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmensdaten gewährleistet sind. Dies schließt die strikte Einschränkung des Zugriffs auf die verarbeiteten Daten ein, sodass Dritte zu keiner Zeit in der Lage sind,

Kenntnis von diesen Daten zu erlangen. Als "Dritte" gelten in diesem Zusammenhang nicht nur externe Personen, sondern auch solche, die sich im gleichen Haushalt wie der Arbeitnehmer befinden.

Vertraulichkeit gewährleisten: Die Vertraulichkeit von Unternehmensdaten hat oberste Priorität. Die Arbeitnehmer sollten sicherstellen, dass sie an einem Ort arbeiten, an dem keine unautorisierten Personen, einschließlich Familienmitglieder oder Mitbewohner, Zugang zu den vertraulichen Informationen haben. Dies kann bedeuten, dass ein dedizierter Arbeitsplatz eingerichtet wird, der von anderen Räumen isoliert ist.

Sichere Arbeitsumgebung: Die physische Umgebung, in der das Home-Office eingerichtet ist, sollte sicher und frei von Risiken sein, die die Integrität von Geräten oder Daten gefährden könnten. Dies schließt die Vermeidung von Gefahren wie Wasserschäden, unsichere Stromquellen oder Sturzgefahren ein.

Zugriffskontrollen: Der Zugriff auf Arbeitsmittel und -daten sollte durch angemessene Zugriffskontrollen geschützt werden. Dies kann durch die Verwendung von Passwörtern, PIN-Codes oder biometrischen Identifikationsmethoden erreicht werden.

Sichere Datenübertragung: Wenn Daten zwischen dem Home-Office und dem Unternehmensnetzwerk übertragen werden, müssen verschlüsselte Verbindungen verwendet werden, um sicherzustellen, dass die Daten während der Übertragung nicht kompromittiert werden.

Datenvernichtung: Die sichere Vernichtung von vertraulichen Dokumenten oder Datenträgern ist ebenso wichtig wie der Schutz vor unbefugtem Zugriff. Arbeitsmittel sollten ordnungsgemäß gelöscht oder vernichtet werden, wenn sie nicht mehr benötigt werden.

Sicherheitsbewusstsein: Alle in einem Haushalt lebenden Personen sollten über die Notwendigkeit informiert werden, die Vertraulichkeit

von Unternehmensdaten zu wahren, und darauf hingewiesen werden, keine unbefugten Zugriffe vorzunehmen.

b) Die Sicherheit von eingesetzten Geräten und Informationen ist nicht auf die bloße Arbeitszeit beschränkt, sondern erstreckt sich auch auf den Transport und die Aufbewahrung innerhalb der Wohnräume des Mitarbeiters. Dies ist von entscheidender Bedeutung, um sicherzustellen, dass vertrauliche Informationen nicht gefährdet werden und dass Arbeitsmittel geschützt sind.

Transport innerhalb der Wohnräume: Wenn Sie Geräte wie Notebooks oder USB-Sticks innerhalb Ihrer Wohnräume bewegen, ist besondere Vorsicht geboten. Diese Geräte können sensible Unternehmensdaten enthalten, die nicht in falsche Hände geraten dürfen. Daher sollten Sie sicherstellen, dass Sie solche Geräte immer sicher transportieren, zum Beispiel in einer verschlossenen Tasche oder einem verschlossenen Behälter. Vermeiden Sie es, diese Gegenstände unbeaufsichtigt in Bereichen zu lassen, in denen andere Personen Zugang haben.

Sicherer Transport von Arbeitsmitteln: Es ist auch die Verantwortung des Arbeitgebers sicherzustellen, dass die bereitgestellten Geräte, wie Notebooks und USB-Sticks, angemessen verschlüsselt sind. Die Verschlüsselung stellt sicher, dass selbst im Falle eines Verlusts oder Diebstahls der physische Zugriff auf die Daten verhindert wird. Dies ist eine wichtige Schutzmaßnahme, um sicherzustellen, dass vertrauliche Informationen geschützt sind, selbst wenn die physische Sicherheit des Geräts gefährdet ist.

c) Die Sicherheit sensibler Informationen und Arbeitsmittel ist von höchster Wichtigkeit. Daher sind bestimmte Maßnahmen zu ergreifen, um diese zu schützen:

Kurzzeitige Abwesenheit: Wenn Sie Ihren Arbeitsplatz nur kurzzeitig verlassen, sollten Sie alle genutzten Geräte, wie Computer oder Laptops, durch Bildschirmsperren oder Passwortschutz sichern. Dies stellt sicher, dass niemand unbefugt auf Ihre laufenden Anwendungen oder Daten zugreifen kann, während Sie nicht anwesend sind. Es ist

eine einfache, aber effektive Methode, um die Sicherheit zu gewährleisten.

Längerfristige Abwesenheit: Wenn Sie für längere Zeit abwesend sind, sollten Sie sämtliche Informationen und Arbeitsmittel sicher aufbewahren. Idealerweise sollten diese in verschlossenen Schränken oder Schubladen untergebracht werden. Dies schützt nicht nur vor unbefugtem Zugriff, sondern auch vor physischen Schäden oder Diebstahl. Es ist ratsam, keine vertraulichen Informationen oder Arbeitsmittel unbeaufsichtigt und ungesichert zu lassen.

Unterstützung durch die IT-Abteilung oder den Administrator: Wenn Sie unsicher sind, wie Sie die genannten Sicherheitsmaßnahmen umsetzen sollen oder technische Hilfe benötigen, sollten Sie sich an die IT-Abteilung oder den Administrator Ihres Unternehmens wenden. Diese Fachleute können Sie bei der Einrichtung von Passwortschutz, Bildschirmsperren oder anderen Sicherheitsvorkehrungen unterstützen und sicherstellen, dass Ihre Arbeitsmittel angemessen geschützt sind.

Anmerkung: Zentral gesteuerter Bildschirmsperre reicht nicht aus, da diese oftmals erst nach 15 min greift. Der Arbeitgeber muss beim Verlassen des Arbeitsplatzes die Bildschirmsperre manuell aktivieren.

7. Folgen von Verstößen

a) Die Nichteinhaltung dieser Richtlinie kann schwerwiegende arbeitsrechtliche Konsequenzen nach sich ziehen. Solche Konsequenzen könnten Disziplinarmaßnahmen, Abmahnungen, Suspendierungen oder im schlimmsten Fall sogar die Kündigung des Arbeitsverhältnisses sein. Es ist von größter Bedeutung, dass alle Mitarbeiterinnen und Mitarbeiter sich dieser Richtlinie bewusst sind und ihre Bestimmungen gewissenhaft einhalten, um arbeitsrechtliche Probleme zu vermeiden.

b) Je nach Art und Umfang des Verstoßes können auch weitere rechtliche Konsequenzen drohen. Im Zivilrecht könnten Schadensersatzforderungen von betroffenen Parteien oder

Organisationen erhoben werden, wenn durch den Verstoß Schäden entstehen. Im Strafrecht könnten Verstöße gegen Datenschutzbestimmungen zu strafrechtlichen Ermittlungen und möglicherweise zu Geldstrafen oder Freiheitsstrafen führen. Es liegt im Interesse aller Beteiligten, die Einhaltung dieser Richtlinie ernst zu nehmen, um rechtliche Konsequenzen zu vermeiden.

Ort,Datum: _____

Mitarbeiter/in: _____

Unternehmen: _____