

6 Maßnahmen zum Datenschutz im Home- und Mobileoffice



**DATENSCHUTZ
EXPERTE.DE**

Ein Service der Proliance GmbH

Die aktuelle Debatte um die Förderung von Home- und Mobileoffice durch die deutsche Regierung ist ein möglicher Schritt zur Entlastung der Städte und Metropolen. Der Verkehr durch Pendler auf den Straßen nimmt ab, die Mietsituation in den Metropolen entspannt sich und die Menschen nutzen ihre Zeit sinnvoller, als im Auto oder in der Bahn zu sitzen. Soweit die Hoffnung. Doch mit den neuen Arbeitsmodellen gehen auch erhebliche Herausforderungen einher – insbesondere im Bereich Datenschutz. Denn während die Vorteile des flexiblen Arbeitens auf der Hand liegen, ist die Sicherheit sensibler Daten zunehmend gefährdet.



Datenschutz im Home- und Mobileoffice sicherstellen

In einer Zeit, in der **Cyberangriffe und Datenschutzverletzungen** zur alltäglichen Bedrohung geworden sind, ist es für Unternehmen unerlässlich, effektive Maßnahmen zu ergreifen, um die Privatsphäre ihrer Mitarbeitenden und Kunden zu schützen. Dieses Whitepaper bietet Ihnen praxisnahe Lösungen und fundierte Empfehlungen, wie Sie den Datenschutz im Home- und Mobileoffice wirksam sicherstellen können.

Sie werden **sechs konkrete Maßnahmen** kennenlernen, die Ihnen helfen, den Schutz personenbezogener Daten zu gewährleisten – von klaren Hardware-Richtlinien bis hin zur ordnungsgemäßen Vernichtung von Papierakten. Unsere Empfehlungen sind praxisorientiert und einfach umsetzbar, sodass Sie Ihre Datenschutzstrategie im Handumdrehen optimieren können.

Lassen Sie sich inspirieren, wie Sie in Ihrem Unternehmen eine **sichere und zukunftsorientierte Arbeitsumgebung** schaffen können – egal, wo Ihre Mitarbeiter sich befinden. Neugierig geworden? Dann erfahren Sie jetzt mehr über die entscheidenden Schritte, die Ihre Daten vor unbefugtem Zugriff schützen und die **Einhaltung gesetzlicher Vorschriften** sicherstellen.

Ihre Reise in eine sichere, flexible Arbeitswelt beginnt hier.

1

Kein Zugang Dritter zu personenbezogenen Daten

Die zur Verarbeitung im Homeoffice genutzten personenbezogenen Daten dürfen nur dem betreffenden Arbeitnehmer zugänglich sein. Das bedeutet, dass der Arbeitnehmer die Akten und auch die betrieblichen Geräte nur selbst nutzen und einsehen darf. Er muss deshalb dafür sorgen, dass andere Personen, die sich ebenfalls in der Wohnung aufhalten, weder Einsicht in die Akten oder die Geräte haben, noch an deren Zugangsdaten gelangen.

Der Arbeitnehmer muss daher bei Anwesenheit anderer Personen in der Wohnung die betrieblichen **Geräte sperren und Papierakten einschließen**, z. B. wenn er seinen Arbeitsplatz verlässt.

Falls er selbst die Wohnung verlässt und die anderen Personen weiterhin anwesend sind, muss er die Akten und die betrieblichen Geräte unzugänglich einschließen. Um die Sicherheit zu gewährleisten, wenn der Mitarbeiter die Wohnung verlässt, sind außerdem die Fenster zu schließen und die Wohnungstür abzuschließen. Dies soll die erhöhte Gefahr des unbefugten Zugriffs auf Daten durch Einbrüche minimieren.

 **Wichtig:** Gerade im Mobileoffice sollten zusätzliche Maßnahmen getroffen werden, um das Einsehen von Daten durch Dritte zu verhindern. Hierzu können z.B. Sichtschutzfolien für Laptops genutzt werden.



2

Hardware - Richtlinien und Vereinbarungen

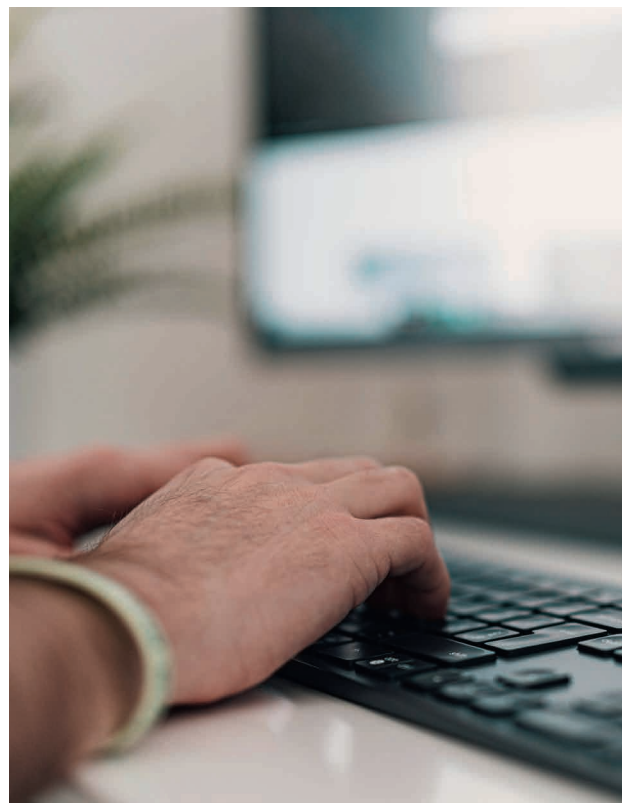
Dokumentation der Ausgabe unternehmenseigener Hardware

Die Ausgabe von vom Betrieb bereitgestellten Geräten jeglicher Art sollte dokumentiert werden, damit etwa im Falle eines Verlustes oder Diebstahls genau nachvollzogen werden kann, welche Ausmaße eine mögliche Datenschutzverletzung hat und wo der Verlust auftrat.

Private Nutzung der Hardware und private Nutzung von Internet und E-Mail-Postfächern

Die für das Homeoffice bereitgestellte Hardware sollte nicht für die private Nutzung zugelassen sein. Dies wird auch hinsichtlich der privaten Nutzung von Internet und E-Mail-Postfächern empfohlen - grundsätzlich auch unabhängig von Home-/Mobile-office-Tätigkeiten.

Hierzu sollten **verbindliche Richtlinien oder Vereinbarungen** getroffen werden. Sollte die Privatnutzung in einem bestimmten Umfang und unter bestimmten Vorgaben erlaubt sein, sollte dies auch für die Homeoffice-Tätigkeit gelten und den Mitarbeitern entsprechend kommuniziert werden.



Einsatz privater Geräte

Der Einsatz privater Geräte zur Verarbeitung oder Speicherung von Daten sollte vermieden werden. Dazu gehört beispielsweise die Nutzung privater Computer oder Smartphones zum Abrufen betrieblicher E-Mails oder auch die Verwendung privater USB-Sticks. Die Nutzung privater Geräte für die berufliche Tätigkeit ist nur dann zu empfehlen, wenn eine **geeignete technische Lösung** auf dem Gerät implementiert werden kann, die die privaten und die beruflichen Daten vollständig trennt.

Bei der Verwendung von Web-Logins kann ein Zugriff auch über private Geräte erfolgen, falls eine automatische Verschlüsselung gewährleistet werden kann. Es wird zudem empfohlen, die Nutzung (entweder Verbot oder Erlaubnis) privater Endgeräte zu beruflichen Zwecken durch **Richtlinien oder Vereinbarungen** zu regeln.

3

Software - Unbefugten den Zugriff auf Daten erschweren

Zwei-Faktor-Authentifizierung

Um das Risiko des Zugriffs eines Unbefugten auf unternehmenseigene Daten zu minimieren, sollte eine Zwei-Faktor-Authentifizierung eingerichtet sein, die dem **Identitätsnachweis des Nutzers** (Mitarbeiters im Homeoffice) dient.

Bei dieser Form der Authentifizierung muss sich ein Nutzer mittels einer Kombination aus zwei unterschiedlichen und voneinander unabhängigen Authentifizierungsmethoden ausweisen, z.B. mit Benutzername/Passwort und einem über ein externes Programm versendeten Code.

Updates, Virenschutz, Firewall und Bootschutz

Um eine umfassende Datensicherheit zu gewährleisten, sind Virenschutz, Firewall und Bootschutz selbstverständlich auch im Homeoffice unerlässlich. Diese sollten **immer auf dem neuesten Stand und aktiv** sein.

Der Mitarbeiter sollte technisch gar nicht erst die Möglichkeit haben, diese Systeme selbst zu deaktivieren. Zudem sollte der Mitarbeiter darauf sensibilisiert sein, mit der IT-Abteilung in Kontakt zu treten, sobald eine dieser Sicherheitsmaßnahmen nicht ordnungsgemäß funktioniert.



Passwortgeschützter automatischer Bildschirmschoner

Eine automatische Sperrung des Bildschirms bei Abwesenheit und eine Verpflichtung des Mitarbeiters zur **manuellen Sperrung** sollte immer bestehen. Dies gilt natürlich auch für die Arbeit im Homeoffice und im Mobileoffice.

Ausschluss der lokalen Speicherung von Daten auf dem Rechner

Es sollten generell keine Daten auf dem lokalen Rechner gespeichert werden, sondern ausschließlich **über Terminalserver, eine Virtual Desktop Infrastruktur oder per Webanwendung** auf zentral gespeicherte Daten zugegriffen werden, um im Falle eines Verlustes oder Diebstahls des Computers den unbefugten Zugriff auf Daten zu erschweren.

Sichere Aufbewahrung verkörperter Daten

Auch am Heimarbeitsplatz muss die Aufbewahrung verkörperter Daten vor der Einsicht Unbefugter geschützt sein und dem **Sicherheitsniveau gem. Art. 32 DSGVO** entsprechen. Personenbezogene Daten in Papierform, wie z.B. Akten, sollten daher in einem Schrank verschlossen werden.



Sichere Übertragung und sicherer Transport von Daten

Es muss sichergestellt sein, dass der Mitarbeiter im Homeoffice und im Mobileoffice auf sicherem Wege mit den Daten arbeiten kann. In diesem Punkt kann bereits der Arbeitgeber Vorkehrungen treffen. Es sollte zunächst darauf geachtet werden, dass es eine **sichere Verbindung zu dem Firmennetzwerk** gibt. So kann zum Beispiel durch eine VPN-Verbindung sichergestellt werden, dass der Mitarbeiter nur unter Verwendung einer sicheren Verbindung auf personenbezogene Daten zugreifen und diese übermitteln kann.

Bei der Übertragung von Daten mittels Datenträger sollten diese sowie der Datenträger, aufgrund der hohen Verlustgefahr von mobilen Speichergeräten, **verschlüsselt** sein. Beim Transport verkörperter Daten sollten sich diese in einem **verschlossenen Behältnis** befinden (z.B. in einem verschlossenen Aktenkoffer o.Ä.) und zu keiner Zeit unbeobachtet sein.

4

Ordnungsgemäße Vernichtung von Papierakten

Papierakten müssen auch im Home-/Mobile-office ordnungsgemäß vernichtet werden. Hierfür sollte ein **Aktenvernichter mit angemessener Sicherheitsstufe** verwendet werden. Alternativ können Papierakten zunächst sicher aufbewahrt und anschließend zum Unternehmen verbracht und dort sicher vernichtet werden.

50 %

aller Akten in deutschen Büros wurden bereits digitalisiert und jedes zwölfte Unternehmen arbeitet komplett papierlos

Quelle: Bitkom Digital Office Index 2022

Auch bei Papierakten stellt sich die Frage, ob deren Verarbeitung für die Arbeit im Mobileoffice geeignet ist. In jedem Fall sollten entsprechende Sicherheitsvorkehrungen getroffen werden.

Aufgrund der erhöhten Gefahr von Diebstählen und Spionage im Mobileoffice sollten Papierakten nie unbeobachtet gelassen werden.



5 Kontrolle der Einhaltung des Datenschutzes

Der Arbeitgeber muss als Verantwortlicher für die Datenverarbeitung auch dann die Möglichkeit zur **Kontrolle der Einhaltung des Datenschutzes** durch den Mitarbeiter haben, wenn dieser sich im Homeoffice befindet. Dazu muss der Arbeitgeber die Wohnung seines Arbeitnehmers betreten dürfen. Da die Wohnung jedoch grundrechtlich geschützt ist, muss sich der Arbeitgeber vom Arbeitnehmer (und evtl. von dessen Mitbewohnern) das Recht zur Kontrolle des Datenschutzes in der Wohnung einräumen lassen.

Die Möglichkeit des Arbeitgebers die Wohnung bezüglich der Einhaltung datenschutzrechtlicher Grundsätze zu kontrollieren sollte jedoch **nur im konkreten Verdachtsfall** herangezogen werden. Eine andauernde oder anlasslose Überprüfung könnte einen schweren Eingriff in die Privatsphäre des Arbeitnehmers bedeuten und arbeitsrechtliche Konsequenzen mit sich ziehen.





6

Regelungen gegenüber den Mitarbeitern

Die zuvor erwähnten Punkte sollten so vereinbart werden, dass der Mitarbeiter rechtlich an die Einhaltung gebunden ist.

Dies kann zum Beispiel dadurch geschehen, dass die datenschutzrechtlichen Richtlinien für die Arbeit im Homeoffice oder im Mobileoffice in die **Homeoffice-Vereinbarung** mit dem Mitarbeiter aufgenommen werden. Es empfiehlt sich, solch eine Vereinbarung zusätzlich zu dem Arbeitsvertrag zu schließen, um diesen entsprechend zu erweitern.

In einer solchen Vereinbarung können beispielsweise folgende Punkte geregelt werden und durch konkrete Maßnahmen zum Datenschutz bzw. einen Verweis auf eine entsprechende Richtlinie individuell ergänzt werden:

1. Genehmigung im Homeoffice / Mobileoffice zu arbeiten

2. Arbeitszeiten

- An wie vielen Tagen darf im Homeoffice gearbeitet werden?
- Pausenzeiten und Zeiteinteilung (z.B. hinsichtlich Kernarbeitszeiten)

3. Arbeitsbereich

- Gestaltung des Arbeitszimmers
- Möglichkeit privater Nutzung von Hardware (optimalerweise ausschließen)

4. Erreichbarkeit für Vorgesetzte, Kollegen oder Kunden

5. Möglichkeit zur Besichtigung des Heimarbeitsplatzes



Sie haben Fragen? Wir helfen Ihnen weiter!

Sie wünschen eine unverbindliche Beratung zum Datenschutz Management in Ihrem Unternehmen und dem Thema externer Datenschutzbeauftragter?

Rufen Sie uns gerne an oder schreiben Sie uns eine E-Mail!

datenschutzexperte.de
+49 (0)89 2500 392 20
info@datenschutzexperte.de



Alexander Ingelheim
Geschäftsführung

datenschutzexperte.de ist Ihr Partner im Datenschutz.

Wir glauben, dass Datenschutz nicht teuer und komplex sein muss. Mit unseren auf KMU zugeschnittenen Lösungen beraten wir Sie als externer Datenschutzbeauftragter. Alternativ unterstützen wir sowohl interne oder externe Datenschutzbeauftragte mit unserer smarten SaaS-Plattform Proliance 360. So lässt sich Datenschutz einfach & pragmatisch umsetzen. Wir sind ein junges Münchner Unternehmen mit mehr als 70 Mitarbeitern und helfen bereits über 2.000 Unternehmen, die Herausforderungen der DSGVO zu meistern. Sprechen Sie uns gerne an.

Copyright © 2024 PROLIANCE GmbH

Wir behalten uns alle Rechte an diesem Dokument vor. Dieses Whitepaper sowie Teile davon dürfen nicht ohne schriftliche Einwilligung der PROLIANCE GmbH reproduziert oder in kommerzieller Weise verwendet werden. Diese Checkliste dient lediglich als Leitfaden und erhebt keinen Anspruch auf Vollständigkeit und/oder Rechtsverbindlichkeit. Trotz höchster Sorgfalt bei der Erstellung des Textes übernehmen wir keine Haftung oder Verantwortung dafür, dass dieser fehlerfrei ist. Diese Checkliste ersetzt keine individuelle Rechtsberatung; für eine persönliche Beratung kontaktieren Sie bitte einen unserer Legal Consultants oder einen Rechtsanwalt.



**DATENSCHUTZ
EXPERTE.DE**

Ein Service der Proliance GmbH

Join the movement
Wir sind Mitglied



We take
**Climate
Action**

ifca.earth/co2