LLR.
Rechtsanwälte
Köln | Brüssel | Helsinki

Leitfaden für Arbeitgeber

Datenschutz und Datensicherheit im Home-Office

24. März 2020

Im Rahmen der Umsetzung behördlicher Empfehlungen oder Verfügungen, aber auch unternehmensinterner Notfallmaßnahmen zur **Eindämmung der Ausbreitung von Covid19** kann es erforderlich sein, Beschäftigte, deren Tätigkeit – zumindest eingeschränkt – auch außerhalb der Arbeitsstätte erbracht werden kann, bis auf Weiteres in Telearbeit (Home-Office) einzusetzen.

Für alle Beteiligten ist es dann unerlässlich, u.a. für die Beschäftigung außerhalb der betrieblichen Arbeitsstätte **verbindliche Regeln zur Aufrechterhaltung der IT-Sicherheitsziele wie Schutz, Vertraulichkeit und Integrität von Informationen** sowie den gesetzlichen und internen **Regelungen zum Datenschutz** aufzustellen. Einige Aufsichtsbehörden haben bereits Pressemitteilungen veröffentlicht, in denen sie auf fortbestehende Erfordernisse zur Einhaltung datenschutzrechtlicher Maßgaben auch bei Telearbeit aufmerksam machen. Daher sollten – ungeachtet anderer rechtlicher Implikationen, die mit Telearbeit einhergehen mögen – folgende Sicherheitsaspekte beachtet werden:

1. Die Pflicht des Arbeitgebers, ein **angemessenes Datensicherheitsniveau** bei der Verarbeitung personenbezogener Daten zu gewährleisten, besteht **auch bei der Entsendung von Beschäftigten ins Home-Office** fort. Alle im Home-Office Beschäftigten müssen daher die gleichen Mindestanforderungen an **technische und organisatorische Maßnahmen** sicherstellen. Dabei gilt: Je sensibler und umfangreicher die verarbeiteten Daten sind, desto höher sind die Datensicherheitsanforderungen an den Arbeitsplatz.

2. Es empfiehlt sich daher, eine **ausdrückliche Richtlinie oder schriftliche Arbeitsanweisung** (auch „Policy“ genannt) zum Arbeiten im Home-Office einzuführen. Ziel ist es, eine verbindliche Regelung zu schaffen, die Beschäftigten Orientierung bietet, und zudem Risiken einer Organisationshaftung für mögliche Datenpannen, die sich gerade durch eine Tätigkeit im Home-Office realisieren, minimiert.

3. Grundsätzlich gelten alle arbeitsvertraglichen oder sonstige betriebliche **Regelungen, Richtlinien, Arbeitsanweisungen sowie Kollektiv- bzw. Betriebsvereinbarungen** zur Nutzung der **IT-Infrastruktur** im Allgemeinen oder zum konkreten **Einsatz von bestimmter Software oder Hardware** (Endgeräten) auch für den Betrieb in Telearbeit, soweit diese Regeln auf die Tätigkeit im Home-Office anwendbar sind. Insbesondere das **IT-Notfall-Management wie Anweisungen für den Umgang mit IT-Sicherheitsvorfällen und Datenschutzverletzungen** sind unbedingt

Per Kristian Stöcker
Rechtsanwalt
ext. Datenschutzbeauftragter
(TÜV cert.)
per.stoecker@llr.de

Prof. Klaus Gennen
Rechtsanwalt
FA für IT-Recht & Arbeitsrecht
betriebl. Datenschutzbeauftragter
(GDD cert.)
klaus.gennen@llr.de

Haben Sie Fragen?
Gerne stehen unsere Experten für IT-Recht und Datenschutz zu Ihrer Verfügung:

Telefon: +49 221 55400-170
Telefax: +49 221 55400-192

LLR Legerlotz Laschet und Partner Rechtsanwälte Partnerschaft mbB
Mevissenstraße 15
50668 Köln
Deutschland
Telefon: +49 221 55400-0
Telefax: +49 221 55400-190
www.llr.de

Sitz: Köln
Registrierung:
AG Essen PR 3609

aufrechtzuerhalten. Soweit diese Regeln das Arbeiten im Home-Office nicht ausdrücklich regeln, kann eine separate Regelung diese für die besondere Arbeitssituation zumindest konkretisieren.

4. Vermieden werden sollte das **Arbeiten auf lokalen Laufwerken**, da diese regelmäßig von implementierten IT-Sicherheitsmaßnahmen wie Updates, Virenschutz und Firewall, aber auch dem Erstellen von Back-Ups nicht umfasst sind. Es empfiehlt sich daher, zumindest alle Systeme für das Verarbeiten von sensiblen Informationen (personenbezogene Daten, Geschäfts- oder Berufsgeheimnisse) auf **virtuellen Server-Umgebungen** zu speichern, auf die Beschäftigte nur über einen **verschlüsselten VPN-Tunnel** zugreifen können.

5. Nach Möglichkeit sollten die im Home-Office genutzten Geräte über **verschlüsselte Festplatten** verfügen, sodass auch im Falle eines Geräteverlusts (Einbruchsdiebstahl u.a.) ein Zugriff auf sensible Daten nicht ohne Weiteres zu befürchten ist.

6. Auch im Home-Office gilt: **Keine Nutzung privater Endgeräte** in der betrieblichen IT-Infrastruktur (kein „Bring your own device“). Das betrifft alle Geräte, die über einen internen Gerätespeicher verfügen oder Zugriff zu externen, virtuellen Speichern herstellen wie insbesondere PCs, Laptops, Smartphones und Tablets oder Speichermedien wie USB-Sticks. Auch Drucker, Scanner oder diese Funktionen beinhaltende Kombigeräte können dem Verbot unterliegen, wenn diese über einen eigenen Arbeitsspeicher verfügen. Ausnahmen sollten nur in **Absprache mit dem Arbeitgeber** und gegebenenfalls durch **Freigabe der Geräte durch die IT-Administratoren** erfolgen.

7. Die Beschäftigten haben auch im Home-Office **wirksame Maßnahmen für eine Zutritts -und Zugangskontrolle** umzusetzen. Soweit auch andere Personen im Haushalt leben, sollten neben einer in (auch nur kurzfristiger) Abwesenheit stets abzuschließenden Haus- oder Wohnungstür gegebenenfalls weitere Zutrittsmaßnahmen innerhalb des Hauses oder der Wohnung umgesetzt werden, so z.B. eine abschließbare Arbeitszimmertür, abschließbare Schränke zur Dokumenten- oder Geräteaufbewahrung, Vermeidung von offenliegenden Dokumenten und Passwörtern, sowie aktivierte automatische Bildschirmsperren. Sensible Date sollten zudem niemals in gemeinsam genutzten Sozialräumen von Haus- und Wohnungsgemeinschaften verarbeitet werden.

8. Ein großes Risiko für Datenpannen stellt die unsachgemäße **Dokumentenvernichtung** dar, soweit diese nicht im Rechtssinne vernichtet, sondern bloß „entsorgt“ werden. Vertrauliche Dokumente und papiergebundene personenbezogene Informationen sind stets mit einem **Shredder (mindestens Schutzklasse 2 / DIN 66399)** zu vernichten oder in dafür gesondert vorgesehene **verschlossene Entsorgungsbehälter** zu geben. Soweit im Home-Office keine solchen Einrichtungen verfügbar sind, sollten Beschäftigte zu vernichtende Dokumente in einem abschließbaren Schrank aufbewahren und beim nächsten Aufsuchen des Arbeitsplatzes dort zur fachgerechten Entsorgung abgeben. Alternativ muss der Arbeitgeber die Abholung von Dokumenten beim Arbeitnehmer organisieren, beispielsweise

durch einen zertifizierten Dienstleister. Der **Grundsatz des papierlosen Arbeitens** sollte daher insbesondere für die Home-Office-Situation befolgt werden.

9. Es besteht für das Home-Office **kein gesetzliches Betretungsrecht des Arbeitgebers**. Besonders bei **kritischen, risikogeneigten Verarbeitungstätigkeiten** oder **IT-Administratoren** sollte aber das Recht auf eine **Vorabbesichtigung** eingeräumt werden, sowie ein **anlassbezogenes Zutrittsrecht** zur Behandlung eines akuten IT-Sicherheitsvorfalls, wenn dieser nicht remote behoben werden kann. Hierzu sind ausdrückliche kollektive oder individuelle Vereinbarungen zwingend.

Haben Sie Fragen?

Gerne stehen unsere Experten für IT-Recht und Datenschutz zu Ihrer Verfügung:

LLR.

Per Kristian Stöcker
per.stoecker@llr.de

Prof. Klaus Gennen
klaus.gennen@llr.de

T: +49 221 55 400 170
F: +49 221 55 400 192
www.llr.de