

# LEGALNEWS

Richtig (re)agieren in der Corona-Krise | März 2020

## Corona-Krise – Arbeiten im Mobile Office datenschutzgerecht gestalten

### Was genau ist das Problem?

Zunehmend mehr Unternehmen gehen aus Gründen des Gesundheitsschutzes und zur Aufrechterhaltung des Geschäftsbetriebs dazu über, ihren Mitarbeiter das Arbeiten außerhalb des Büros zu ermöglichen. Ferner drohen möglicherweise ab Sonntag oder Montag Ausgangssperren, so dass ein Arbeiten im Büro des Arbeitgebers gar nicht mehr möglich sein könnte. Unsere Empfehlung: Bereiten Sie sich auf einen möglichen Shut down vor und vereinbaren, soweit sinnvoll, mit Ihren Mitarbeitern das mobile Arbeiten.

Das Mobile Office bringt indes nicht nur technische Herausforderungen mit sich – alle Mitarbeiter müssen mit geeigneter IT ausgestattet werden – sondern wirft auf rechtliche Fragestellungen auf.

### Was Sie jetzt tun müssen

Arbeitgeber können mobiles Arbeiten grundsätzlich nicht einseitig anordnen, wenn gleich von diesem Grundsatz möglicherweise in der Corona-Krise und behördlichen Schließungsanordnungen Ausnahmen zulässig sein dürften/sollten. Allerdings ist in jedem Fall eine individualvertragliche oder kollektivrechtliche Rechtsgrundlage, wie etwa eine Betriebsvereinbarung oder ein Tarifvertrag, sehr sinnvoll, eventuell auch zwingend erforderlich abhängig von den Inhalten.

### Datenschutz nicht vergessen!

Neben den arbeitsrechtlichen Rahmenbedingungen sind dabei vor allem auch datenschutzrechtliche Regelungen festzulegen, wie bei einer Tätigkeit im Büro. Werden personenbezogene Daten im Mobile Office verarbeitet, muss sichergestellt sein, dass die Daten sicher verarbeitet und übermittelt und nicht von Dritten eingesehen werden können. So dürfen etwa Geschäftsunterlagen nicht auf dem Küchentisch ausgebreitet und der Laptop offenstehen gelassen werden, während gleichzeitig die Familie und vielleicht sogar Dritte anwesend sind.

Falls möglich, sollten personenbezogene Daten in einem separaten, abschließbaren Raum verarbeitet werden. Ist das nicht möglich, sollte zumindest die Aufbewahrung dieser Daten in einem abschließbaren Schrank organisiert werden.

Die vom Arbeitgeber für die Tätigkeit im Mobile Office zur Verfügung gestellte IT-Infrastruktur darf grundsätzlich nicht privat genutzt werden. In diesem Zusammenhang haben die meisten Unternehmen IT-Richtlinien erlassen bzw. IT-Betriebsvereinbarungen abgeschlossen, die den Umgang mit betrieblicher IT detailliert regelt und insbesondere die rein dienstliche oder eventuell private Nutzung festlegt. Diese Regelungen gelten uneingeschränkt auch im Mobile

1

BEI FRAGEN WENDEN SIE SICH GERNE AN:



Dr. Thomas Block, MBA  
[thomas.block@actlegal-act.com](mailto:thomas.block@actlegal-act.com)  
+49 69 247097-11



Dr. Florian Wäßle, LL.M.  
[florian.waessle@actlegal-act.com](mailto:florian.waessle@actlegal-act.com)  
+49 69 247097-28

# LEGALNEWS

Richtig (re)agieren in der Corona-Krise | März 2020

Office. Insbesondere ist darauf zu achten, dass

- der Laptop passwortgeschützt und bei auch nur kurzer Abwesenheit gesperrt ist,
- berufliche E-Mails nicht zur Bearbeitung an private E-Mail-Postfächer weitergeleitet oder auf privaten Speichermedien (z.B. USB-Sticks) gespeichert werden,
- das vom Arbeitgeber zur Verfügung gestellte Mobiltelefon gesperrt und passwortgeschützt ist und
- Ausdrücke von personenbezogenen Daten und anderen sensiblen Inhalten sicher verwahrt und nach Gebrauch ebenso sicher vernichtet werden.

Der Arbeitgeber sollte in diesem Zusammenhang sicherstellen, dass die von ihm zur Verfügung gestellte IT-Infrastruktur für den Einsatz im Mobile Office geeignet d.h. verschlüsselt und passwortgeschützt ist. Auf jedem System sollten geeignete Anwendungen installiert sein, die eine sichere Datenübermittlung gewährleisten und Zugriffe auf die Systeme des Arbeitgebers lediglich über ein Virtual Private Network ermöglichen.

## Wichtig!

**Zur vertraglichen Absicherung ist in jedem Fall eine Zusatzvereinbarung zum Arbeitsvertrag über (zeitlich befristetes) Arbeiten im Mobile Office oder eine vergleichbare Betriebsvereinbarung abzuschließen.**

Diese sollte flankiert sein von einer *IT-Richtlinie* bzw. *IT-Betriebsvereinbarung*, die den generellen Umgang mit betrieblicher IT regelt, sowie einem geeigneten

Datenschutzkonzept (*Datenschutz-Richtlinie* bzw. *Betriebsvereinbarung*).

Nicht zu vergessen ist auch in diesem Rahmen ein geeignetes *Informationsmanagement* zum effektiven Schutz von Geschäftsgeheimnissen im Mobile Office.

Gerne unterstützen wir Sie.

Sprechen Sie uns an!

BEI FRAGEN WENDEN SIE SICH GERNE AN:



Dr. Thomas Block, MBA  
[thomas.block@actlegal-act.com](mailto:thomas.block@actlegal-act.com)  
+49 69 247097-11



Dr. Florian Wäßle, LL.M.  
[florian.waessle@actlegal-act.com](mailto:florian.waessle@actlegal-act.com)  
+49 69 247097-28