HÄTTEN SIE'S gewusst?

Zehn wichtige To-dos, die Sie bei der Arbeit zu Hause oder unterwegs berücksichtigen müssen.

DR. HERMANN LINDHORST

Der Rechtsanwalt ist Partner bei SCHLARMANNvonGEYSO sowie assoziierter Experte des Deutschen Franchiseverband e.V.

Foto und Illustration: © Followtheflow, M.Style / Shutterstock.com

Früher sprach man von „Telearbeit" oder „Homeoffice", also der Arbeit fern von Kollegen und außerhalb des eigentlichen Büros, als etwas Besonderem. Das ist heute komplett anders. Die Präsenzkultur verschwindet zusehends aus den Unternehmen, und immer häufiger drehen sich schon Vorstellungsgespräche um flexible Arbeitszeiten, VPN-Zugang und mobiles Arbeiten. Längst geht es nicht mehr nur um starre Regelungen wie etwa drei Tage im Unternehmen, zwei Tage zu Hause. Smartphone und Laptop ermöglichen es ja, zu jeder Zeit von überall arbeiten zu können. Ob man an einer Videokonferenz, die sich heutzutage einfach und kostenlos etwa über Skype oder WhatsApp einrichten lässt, nun im Unternehmen, von zu Hause oder unterwegs teilnimmt, spielt keine Rolle. Aber es gibt rechtliche Aspekte, die Unternehmen und Mitarbeiter dabei im Blick haben müssen. Stand früher die steuerliche Absetzbarkeit des Homeoffice im Vordergrund, sind es heute Datenschutz und Datensicherheit die Beachtung finden müssen. Hier die wichtigsten zehn Tipps:

1

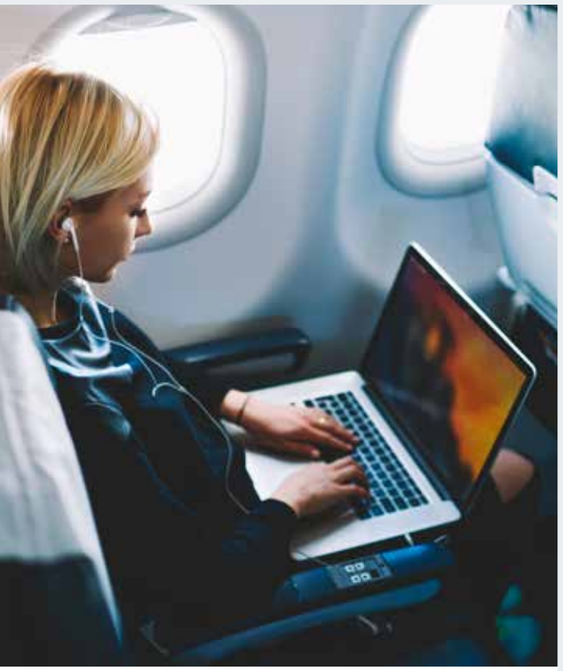
Schulung, Schulung, Schulung!

Man kann gar nicht oft genug darauf hinweisen, denn alle Anweisungen, Richtlinien und Vereinbarungen bringen nichts, wenn Mitarbeiter dennoch vertrauliche Dokumente unterwegs im Flieger oder in der Bahn bearbeiten oder auf andere Art offensichtlich gegen die Vertraulichkeit verstoßen. Dagegen helfen nur Schulungen. Mitarbeiter und übrigens auch Unternehmensinhaber und Geschäftsführer müssen wissen, was datenschutz- und vertraulichkeitsrechtlich geht und was nicht. Das bezieht sich auch auf die IT-Sicherheit: Die meiste Schadsoftware gelangt über die Nutzung privater Computer oder Speichermedien in Unternehmensnetzwerke – oft mit fatalen Auswirkungen.

Achtung Ausland!

So manchem Vielflieger-forum, auch der juristischen Literatur ist zu entnehmen, dass Einreisebeamte an Grenzübergängen gern mal ein neugieriges Auge auf Laptop-Inhalte werfen. Genauso wie viele häufig Reisenden mittlerweile einen zweiten Pass besitzen, empfiehlt es sich auch, insbesondere für Reisen ins außereuropäische Ausland, ein eigens dafür eingerichtetes Laptop mit möglichst wenig Daten zu nutzen.

2



3

Verschlüsselung ist Trumpf!

Kommen Laptop, Smartphone oder kleinere Speichermedien wie USB-Sticks abhanden, ist das eine Datenschutzpanne, die nicht erst seit Einführung der DSGVO meldepflichtig ist. Hiergegen hilft neben höchster Sorgfalt nur eines: Verschlüsselung! Ist der Zugang zum Laptop oder sind die Daten auf dem USB-Stick so sicher verschlüsselt, dass ein Dritter keinerlei Einsicht nehmen kann, ist das im Ernstfall sehr hilfreich und erspart peinliche, rufschädigende und kostenträchtige Diskussionen mit Datenschutzaufsichtsbehörden.

4

Arbeitsschutz ernst nehmen!

Die Arbeitsstättenverordnung und das Arbeitsschutzgesetz sind sperrig und unbeliebt. Nach einhelliger rechtlicher Auffassung gilt aber zumindest das Arbeitsschutzgesetz auch im heimischen Büro, sodass das Unternehmen grundsätzlich verpflichtet ist, für die Einhaltung der erforderlichen Maßnahmen des Arbeitsschutzes zu sorgen und entsprechende Mittel bereitzustellen. Detailfragen sind hier umstritten, z. B. ob der Arbeitgeber zur Überprüfung des Homeoffices seines Mitarbeiters auch ein Zutrittsrecht hat. Wie in Bezug auf die private Nutzung von Internet und E-Mail ist auch hier der Gesetzgeber gefordert, endlich der digitalen Realität genügende Rahmenbedingungen zu schaffen, um Unternehmen und ihren Mitarbeitern mehr Rechtssicherheit zu bieten.

5

Forget BYOD!

Bring Your Own Device – vor Jahren groß in Mode: Mitarbeiter nutzten ihre eigenen teuren iPhones & Co. am Arbeitsplatz, was Unternehmen die Anschaffung solcher Geräte und reichlich Kosten ersparte. Mittlerweile setzt sich die Erkenntnis durch, dass dies datenschutz- und lizenzrechtlich, vor allem aber auch mit Blick auf die IT-Sicherheit ein Supergau ist: Unternehmen haben keinerlei Kontrolle über die eingesetzten Geräte und sind permanent dem Risiko von Sicherheitspannen und Lizenzabmahnungen ausgesetzt.

6

Private Nutzung von Smartphone und Computer

Auch für mobiles Arbeiten und Homeoffice gilt nach wie vor: Nur wenn Unternehmen die private Nutzung von Internet und E-Mail vertraglich untersagt haben und dies auch einigermaßen regelmäßig kontrollieren, sind sie grundsätzlich berechtigt, auf Festplatten und E-Mail-Konten zugreifen zu können. Das betrifft etwa Konstellationen, in denen ein Vertretungszugriff nicht geregelt wurde oder der Verdacht besteht, dass ein Mitarbeiter Knowhow an Wettbewerber weitergibt oder andere Rechtsverletzungen begeht, z. B. Filesharing und Arbeitszeitklau durch exzessives Surfen im Internet. Häufig wünschen sich Unternehmen eine modernere, liberalere Lösung; Rechtsprechung und Gesetzgebung lassen das zur Zeit aber nicht zu – ebenso wie der Gesetzgeber –, sodass Unternehmen nach wie vor zu raten ist, die private Nutzung von Internet und E-Mail weitestgehend zu untersagen.

7

Statussymbol VPN-Zugang: Klar festlegen, wer berechtigt ist!

Ein VPN-Zugang, der das Arbeiten von unterwegs oder zu Hause ermöglicht, gilt gerade in Sekretariaten zunehmend als Privileg: Früher nach Hause gehen zu dürfen und flexibel zu sein, dort noch E-Mails zu schreiben, ist praktisch, auch mit Blick auf familiäre Verpflichtungen. Ungünstig ist es, wenn Entscheidungen, wer diesen Zugang bekommt, nicht transparent und willkürlich getroffen werden. Das ist nicht gut fürs Betriebsklima und kann Neid und Missgunst schüren.

8

Widerrufsvoraussetzungen festlegen!

Es ist ein offenes Geheimnis, dass nicht jeder Mitarbeiter mit den Freiheiten, die mobiles Arbeiten ermöglicht, umgehen kann. Häufen sich z. B. Beschwerden über die Erreichbarkeit eines Mitarbeiters oder sinkt die Arbeitseffizienz, sollten Unternehmen und Mitarbeiter klipp und klar festlegen, unter welchen Umständen VPN-Zugang und Homeoffice-Berechtigung wieder entzogen werden können.

9

Wichtiger Geheimtipp: Aktenvernichter und Schredder!

Die Anschaffung effektiven Geräts zur Vernichtung nicht mehr benötigter Unterlagen wird häufig vergessen. Um betriebsbezogene Dokumente sicher vor unbefugter Einsichtnahme zu schützen, dürfen sie nicht in frei zugänglichen Altpapiertonnen landen. Für manche Personenkreise, z. B. Journalisten oder Wirtschaftsdetekteien kann dies ein gefundenes Fressen sein.

10

Last but not least: Schutz vor Katzen und Kindern!

Auch dem Verfasser dieser Zeilen ist schon mal seine Hauskatze über die Tastatur gelaufen. Fatale Folge: Eine noch gar nicht dafür bestimmte E-Mail wurde versandt, da halfen selbst umständlichste Erklärungsversuche nichts mehr. Insofern: Sichern Sie Ihre unmittelbare Arbeitsumgebung zu Hause oder von unterwegs so, dass Sie uneingeschränkter Herrscher über die Tastatur bleiben!