BENEKE.CO.
CONSULTING GMBH

Coronavirus (COVID-19) & Datenschutz / Datensicherheit

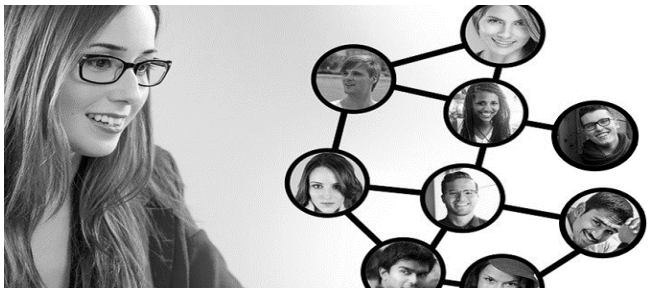
Das Coronavirus führt zu einer starken Veränderung unserer Arbeitswelt- mobiles Arbeiten und Videokonferenzen haben bei vielen Firmen Einzug gehalten. Doch welche Auswirkungen hat dies auf Sicherheitsmaßnahmen beim Umgang mit Geschäftsgeheimnissen und personenbezogenen Daten? Wir geben Ihnen im Rahmen dieses Infobriefes einen praxisorientierten Leitfaden an die Hand!

Die Festlegung von „Technisch-Organisatorischen Maßnahmen“ (kurz „TOM‘s“) dient der Sicherstellung von **Vertraulichkeit**, Verfügbarkeit und Integrität- unter anderem bei **Dokumenten mit Firmen-Know-how**, **Patenten**, **Umsatz- und Bilanzdaten**, aber auch **Kundenadressen** oder **Personalakten**.
Vor der Coronakrise wurden solche schützenswerten Informationen überwiegend innerhalb des Betriebsgeländes und damit eines **gesicherten Netzwerkes** eingesehen und bearbeitet. Aufgrund der aktuellen Veränderungen der Arbeitswelt werden **Zugriffe von außerhalb** beim mobilen Arbeiten häufiger und selbstverständlicher - z.B. im Home-Office -. Entsprechend müssen Sie das mobile Arbeiten bei der (Neu-) Gestaltung der TOM‘s In Ihrem Unternehmen stärker berücksichtigen.

Um Sie hierbei praxisorientiert zu unterstützen haben wir Ihnen **diesen Leitfaden** mit den nachfolgenden **Praxistipps** für die Identifizierung der zugehörigen TOM‘s erstellt. Dieser Leitfaden gilt sowohl für Aktivitäten innerhalb des Betriebsgeländes als auch für das mobile Arbeiten (gekennzeichnet mit einem roten Thermometer). Sie finden die zugehörige **Gesamtliste der TOM’s** auf unserer Internetseite: https://www.ims-schulung.de/downloads

Wichtige Sicherungsmaßnahmen beim mobilen Arbeiten

7 Praxistipps, inklusive Verknüpfung zum Leitfaden (Buchstabe in der Überschrift)



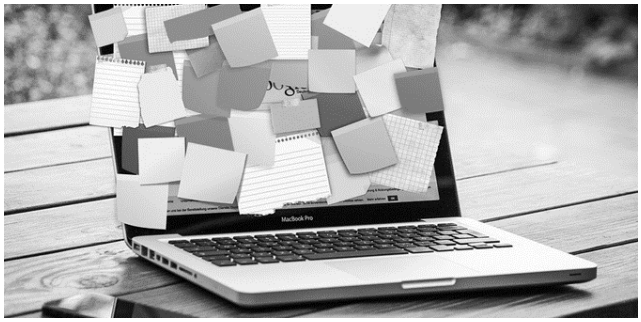
A. Datensicherheit bei Online-Meetings.

Verwenden Sie nur seriöse Online-Meeting-Tools von anerkannten Firmen. Sichern Sie sich gegen unerwünschten Zugriff von Fremden ab, indem Sie für jedes Online-Meeting ein Passwort vergeben. Holen Sie sich im Fall der Aufzeichnung des Online-Meetings eine datenschutzkonforme Einwilligung der Beteiligten ein.

B. Vertraulichkeit bei Online-Meetings.

Wer in einem Online-Meeting seinen Bildschirm teilt, sollte sicherstellen, dass die anderen Teilnehmer keine vertraulichen Daten wie Emails anderer Kunden oder Verzeichnisnamen fremder Projekte einsehen können. Achten Sie (wie auch beim Telefonieren) darauf, dass Personen in Hörreichweite keine vertraulichen Informationen erhalten.

Vertraulichkeit bei Bildschirmfreigaben und Videokonferenzen	B
Laptops / Monitore sichtgeschützt aufstellen	
Vertraulichkeit bei Telefonaten / Videokonferenzen in der Öffentlichkeit	B
Clean-Desk-Policy (Aufgeräumter Arbeitsplatz	

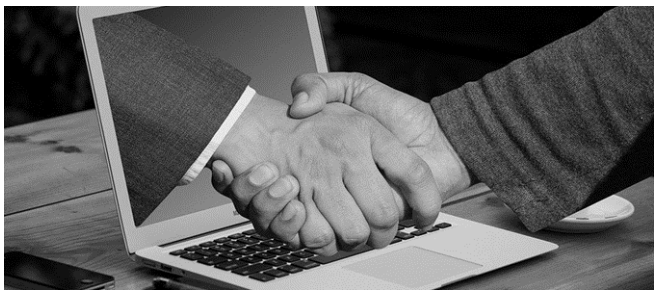


C. Sicherer Umgang mit Papierakten.

Stellen Sie den sicheren Umgang mit Papierakten, Notizen und anderen vertraulichen Ausdrucken im Home-Office sicher.
Maßnahmen sind absperrbare Zimmer und Schränke, ein aufgeräumter Schreibtisch und die Vernichtung mittels Aktenvernichters.

D. Sicherer Einsatz von Passwörtern

Um den Zugriff Fremder zu verhindern müssen IT-Systeme durch Passwörter abgesichert sein. Die Passwörter müssen ausreichend komplex sein (mind. 8 Zeichen, Verwendung von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen). Ein Passwort darf nicht weitergegeben werden und darf auch nicht für mehrere Systeme bzw. Benutzerkonten verwendet werden.

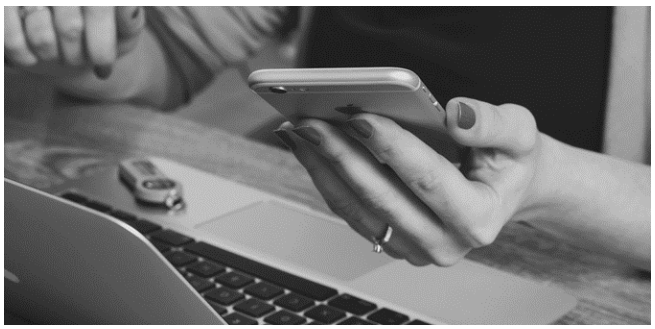


E. Sicheres Speichern und Übertragen von Daten

Daten sollten nie lokal auf dem IT-Gerät gespeichert werden, sondern soweit technisch möglich immer direkt im Firmennetzwerk. IT-Geräte, die sich außerhalb des Firmennetzwerks befinden, dürfen nur mittels abgesicherter Verbindungen (z.B. VPN) Zugriff erhalten. Emails sind kein sicheres Mittel für Dateitransfers.

F. Software-Updates nicht vergessen.

Betriebssystem und installierte Programme benötigen regelmäßige Updates- dies ist aus der Ferne mittels Internetverbindung meist nur teilweise oder gar nicht möglich. Klären Sie mit Ihrem Administrator die technischen Voraussetzungen für Updates im Home-Office. Eventuell ist es einfacher und günstiger, die IT-Geräte zu Aktualisierungszwecken regelmäßig in das Firmennetzwerk vor Ort einzubinden.



G. Zweistufige Anmeldung für kritische Bereiche.

Sichern Sie besonders kritische IT-Bereiche zusätzlich mit einem zweistufigen Anmeldeverfahren (Zwei-Faktor-Authentifizierung). Dies bedeutet, dass der Anwender bei der Anmeldung nicht nur seine Benutzerkennung und Passwort eingeben muss, sondern zusätzlich per SMS oder App ein nur einmal verwendbares Passwort („One-time password“) erhält.

Bildquellen: Pixabay

Aus Gründen der Zustellbarkeit senden wir diese Praxishilfe als pdf.
Wenn Sie die Vorlage als Excel-Datei wünschen um sie mit Ihrem eigenen Branding zu versehen schreiben Sie uns.
info@beneke-co.de – info@ims-zert.de

Stand: 27.04.2020