Homeoffice-Pflicht als Compliance-Herausforderung beim Daten- und Geheimnisschutz

Am 27. Januar 2021 ist mit der Corona-Arbeitsschutzverordnung in Deutschland erstmals eine Homeoffice-Pflicht eingeführt worden. Aber auch schon zuvor haben viele Unternehmen ihren Mitarbeitern die Arbeit im Homeoffice ermöglicht. Die Arbeit im Homeoffice bedingt einen Umgang mit Daten und Dokumenten außerhalb des unmittelbaren Kontrollbereichs des Unternehmens. Dies führt zu einem erhöhten Risiko von Bußgeldern und Haftungsfällen wegen der Verletzung von Datenschutz- und Geheimhaltungspflichten.

Homeoffice-Pflicht: Sie kann in vielerlei Hinsicht herausfordernd sein.

Für eine effektive Arbeit aus dem Homeoffice müssen Unternehmen zulassen, dass ihre Mitarbeiter den Arbeitsplatz nach Hause „verlagern". Arbeit im Homeoffice soll – am besten ohne inhaltliche Beschränkungen – möglich sein. Die Mitarbeiter sollen jederzeit Zugriff auf Dokumente und Daten wie im Büro haben. Auch der Umgang mit sensiblen Daten (personenbezogene Daten – z.B. Kundendaten – und Geschäftsgeheimnisse – z.B. Vertriebsstrategien, Innovationsideen) soll uneingeschränkt möglich bleiben. Im Homeoffice sind diese Daten aber viel größeren Risiken ausgesetzt: Telefonate können einfacher unbefugt mitgehört werden, vertrauliche Papierdokumente sind leichter einsehbar und werden nicht rechtskonform entsorgt, die genutzte technische Infrastruktur ist unsicher und anfällig für Hackerangriffe, um nur einige Beispiele zu nennen. Wenn personenbezogene Daten betroffen sind, kann schnell ein meldepflichtiger sogenannter Data Breach oder ein bußgeldbewehrter Datenschutzverstoß vorliegen. Wenn es um Geschäftsgeheimnisse Dritter (zum Beispiel von Geschäftspartnern) geht, die so unberechtigt nach außen gelangen, kann das Unternehmen gegenüber diesem Dritten für den entstehenden Schaden haften. Aber natürlich sind auch eigene Geschäftsgeheimnisse stärker gefährdet. Datendiebe und Betriebsspione könnten sie unbemerkt abziehen und ein Wettbewerbsvorteil kann dem Unternehmen verloren gehen.

Im Bereich des Datenschutzes sind Unternehmen verpflichtet, auch im Homeoffice durch geeignete Maßnahmen die Integrität und Vertraulichkeit personenbezogener Daten zu schützen. Und das in gleicher Weise wie im Büro. Dasselbe gilt für Geschäftsgeheimnisse Dritter.

Zwar beruht die Notwendigkeit des Schutzes von personenbezogenen Daten einerseits und von Geschäftsgeheimnissen andererseits auf verschiedenen rechtlichen Grundlagen. Da sich eine Vielzahl von Schutzmaßnahmen aber für beide Schutzrichtungen eignen, kann ein umfassendes Homeoffice-Schutzkonzept für beide Bereiche wirken. Das kann sich aufwand- und kostensparend auswirken.

Welche konkreten Schutzmaßnahmen ein Homeoffice-Schutzkonzept vorsehen sollte, hängt grundlegend davon ab, wie sensibel die zu verarbeitenden Daten sind und welche Risikolagen bestehen.

Die Ausarbeitung und Implementierung eines Homeoffice-Schutzkonzepts erfolgt in drei Schritten:

1. Analysephase und Bestandsaufnahme: Die Daten und Informationen sind zu identifizieren und nach Sensibilität, Wichtigkeit und Risikolage zu kategorisieren. Darüber hinaus sind die bestehenden Schutzmaßnahmen auf ihre Eignung und Wirksamkeit hin zu überprüfen und etwaige Schutzlücken sind zu identifizieren (Gap-Analyse).
2. Erstellung und Implementieren eines Schutzkonzepts: Zu jeder Kategorie sind passende rechtliche, technische und organisatorische Schutzmaßnahmen auszuarbeiten und zu implementieren und ihre Einhaltung im Unternehmen sicherzustellen.
3. Regelmäßige Prüfung und Aktualisierung: Da ein Schutzkonzept ein dynamisches System ist, das Änderungen unterlegen ist, muss es regelmäßig geprüft und bei Bedarf angepasst werden.

Konkrete Schutzmaßnahmen sind auf drei Ebenen vorzusehen:

a) Rechtliche Maßnahmenebene: Dazu gehören arbeitsvertragliche Regelungen/Betriebsvereinbarungen, die zu erhöhter Sorgfalt im Homeoffice verpflichten, Auftragsverarbeitungsvereinbarungen mit Dienstleistern, Prüfung von Zertifizierungen, Beteiligung des Betriebsrats u.ä.

b) Technische Maßnahmenebene: Dies sind zum Beispiel die verschlüsselte VPN-Verbindung zum Unternehmensserver, die Ausgabe nur dienstlicher Geräte für die rein dienstliche Nutzung (bestenfalls kein BYOD (Bring Your Own Device) und keine private Nutzung dienstlicher Endgeräte), technische Beschränkung von Zugriff und Druckbarkeit von Dokumenten oder der Nutzung externer Datenträger, Sicherheitsupdates, Nutzung datenschutzkonformer Videokonferenzsysteme u.ä.

c) Organisatorische Maßnahmenebene: Dies beinhaltet insbesondere Arbeitsanweisungen zum Verhalten im Homeoffice (Clean Desk Policy, Dokumentenentsorgung, Schutzmaßnahmen bei Videokonferenzen etc.) und die Festlegung eines Zugriffs- und Berechtigungskonzepts sowie regelmäßige Schulung der Mitarbeiter.

Dr. Michael Kraus und Alexander Leister

CMS

RA Dr. Michael Kraus ist Partner bei CMS Deutschland am Standort Stuttgart. Er berät Unternehmen u.a. zu Fragen der Digitalisierung und des Daten(schutz)rechts.

CMS

RA Alexander Leister, LL.M., ist Counsel bei CMS Deutschland am Standort Stuttgart. Er berät Unternehmen im Gewerblichen Rechtsschutz bei technischen Sachverhalten und im Bereich des Know-how- und Geschäftsgeheimnisschutzes.