

Datensicherheit aufrechterhalten

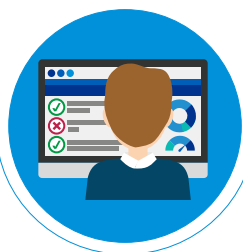
Aktuelle Herausforderungen: Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten sicherstellen



Die Auswirkungen des COVID-19-Virus selbst und damit einhergehende Folgemaßnahmen stellen Unternehmen vor zahlreiche Herausforderungen, wie bspw. im Umgang mit Gesundheitsdaten. Für Sie in der Unternehmensleitung oder als Governance-Verantwortliche geht es in der jetzigen Situation vor allem darum, datenschutzrelevante Prozesse aufrechtzuerhalten, auch unter dieser besonderen Belastungssituation (Stabilität der Systeme, Homeworking, usw.).



- Datenschutzkonformer Umgang mit Gesundheitsdaten von Mitarbeitern und Dritten (z. B. Kontaktpersonen der infizierten Person), insbes. auch Weitergabe von Gesundheitsdaten
- Sicherstellung eines fristgerechten Umganges mit Betroffenenanfragen und Datenschutzverletzungen



- Technische Maßnahmen zum Schutz personenbezogener Daten im Homeoffice, z. B. Verhinderung des Zugriffs durch Dritte (Mitbewohner, Hacker, etc.), Wahrung eines sicheren Datentransfers
- Überprüfung bzw. Erstellung von Homeoffice-Regelungen (organisatorische Maßnahmen)



- (Digitale) Awareness Schulungen zum datenschutzkonformen Umgang mit personenbezogenen Daten im Homeoffice
- Prüfung der privaten Umgebung hinsichtlich „Datenschutz-Gefährdern“, z. B. virtuelle Sprachassistenten, wie das „Mithören“ von Alexa

10 Sofortmaßnahmen:

- Datenschutzkonformen internen Prozess für COVID-19-(Verdachts-) Meldungen sicherstellen
- Berücksichtigung der Rechte und Interessen Dritter (Kontaktpersonen) im (Verdachts-) Meldeprozess
- Sicherstellung der datenschutzkonformen Weitergabe der Gesundheitsdaten von Infizierten
- Festlegung von klaren Vertretungsregelungen für die Bearbeitung von Betroffenenanfragen und Meldung von Datenschutzverletzungen
- Rollen- und Berechtigungskonzepte überprüfen
- Bei Bedarf Homeoffice-Regelungen erstellen bzw. bestehende Regelungen überprüfen
- Mitarbeiter über Homeoffice-Regelungen informieren
- Überprüfung der elektronischen Datenübermittlung auf den aktuellen Stand der Technik
- Aufrechterhaltung der Betriebssicherheit (z. B. Updates, Virenschutz, Firewall)
- Durchführung von kurzfristigen Awareness Schulungen

Ihre Ansprechpartner

Barbara Scheben

Partner,
Head of Forensic, Head of Data Protection
Corporate Governance Services, Forensic
T +49 69 9587-3737
bscheben@kpmg.com

Katharina Sundermann

Manager,
Corporate Governance Services, Forensic
T +49 211 475-7345
ksundermann@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia



Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2020 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.