

## DATENSCHUTZ-PRAXIS

Fortbildungsveranstaltung gemäß  
Art. 38 Abs. 2 DS-GVO, §§ 5, 6, 38 BDSG

# Teleworking unter Beachtung von Datenschutz und Sicherheit

Homeoffice und Mobile Office einrichten, betreiben und effizient nutzen

## TERMINE/ORTE

**5. Mai 2021 Online-Schulung**

**4. November 2021 in Köln**

10:00–17:00 Uhr

## REFERENT



**Dr. Heinrich Kersten**

Consultant, Auditor, Zertifizierer mit langer  
Berufserfahrung beim BSI, bei debis und T-Systems,  
Meckenheim

## ZIELGRUPPE

Datenschutzbeauftragte, IT-Leiter und Mitarbeiter aus dem  
IT-Bereich, Verantwortliche für Personaleinsatz, Compliance  
Manager, IT-Sicherheitsbeauftragte, Sicherheitsberater, Prozess-  
verantwortliche und Business Continuity Manager

## SCHWERPUNKTTHEMEN

- Einführung in aktuelle Teleworking-  
Infrastrukturen
- Compliance- und Sicherheitsrisiken
- Risiken im Hinblick auf den Datenschutz und  
die DS-GVO
- Sinnvolle Maßnahmen zur Behandlung  
der Risiken
- Anforderungen des modernisierten  
IT-Grundschutzes des BSI und der aktuellen  
ISO 27001

## IHR NUTZEN

Das Seminar gibt Ihnen eine Übersicht über die verschiedenen Gestaltungsmöglichkeiten von Teleworking mit mobilen und stationären Geräten (Mobile/Homeoffice). Es werden vorhandene Risiken und entsprechende Lösungsansätze beschrieben. Sie erhalten Tipps und Formulierungshilfen für Richtlinien und Nutzervereinbarungen (inkl. ausformulierter Beispiele) sowie eine Checkliste zur sicheren Einführung von Teleworking.

# TELEWORKING UNTER BEACHTUNG VON DATENSCHUTZ UND SICHERHEIT

Teleworking gehört heute schon zum Alltag und ist bei besonderen Umständen (wie z.B. Pandemie) unerlässlich: Im klassischen Homeoffice oder mobil unterwegs auf Reisen, im Hotel, beim Kunden nimmt man an Tele-Konferenzen teil, verfasst bzw. beantwortet E-Mails, prüft und kommentiert Vertragsentwürfe, erstellt Präsentationen und Texte, beantragt bzw. erteilt Genehmigungen »over-the-air«.

Bei der Gestattung von Teleworking verbleibt die Verantwortlichkeit für die Datenverarbeitung grundsätzlich beim Unternehmen, darunter fällt auch eine evtl. Haftung der Geschäftsführung. Umso wichtiger ist es, sich mit den Risiken bei der Nutzung von Teleworking auseinanderzusetzen: Diese Risiken betreffen vor allem die Themen Compliance, Datenschutz und Informationssicherheit.

## INHALT

### Übersicht über Teleworking

- Ausgangslage und Wünsche für das Teleworking erfassen
- Einsatzszenarien festlegen (Arbeitsplätze, Cloud-Nutzung)
- Rechtliche Vorgaben für das Teleworking ermitteln
- Schutzobjekte identifizieren

### Risiken analysieren und behandeln

- Potenzielle Risiken für die Schutzobjekte systematisch ermitteln
- Geeignete Maßnahmen festlegen
- Verbleibende Risiken bestimmen
- Umsetzung der Maßnahmen planen

### Wichtige konzeptionelle Arbeiten

- Leitlinien überarbeiten
- Konzepte anpassen für die Bereiche des Datenschutzes und der IT-Sicherheit (Fahrplan für Anwendung des SDM, des IT-Grundschutzes und der ISO 27001)
- Teleworking und IT-Notfallkonzepte

Wie lassen sich diese Risiken vermeiden bzw. reduzieren? Wie können Vorgaben einschlägiger Standards und Gesetze – vor allem der DS-GVO und des BDSG – sowie Anforderungen etwa an die Business Continuity erfüllt werden? Welche technischen Voraussetzungen müssen gegeben sein und wie lassen sich diese realisieren? Welche Maßnahmen der Überwachung des Teleworkings sind zu treffen? Welche Vereinbarungen sind mit den Mitarbeitern betreffend Teleworking zu schließen? Sind Schulungs- und Trainingsmaßnahmen aufzusetzen? Erfahren Sie in diesem kompakten Seminar, welche rechtlichen, administrativen und technischen Maßnahmen getroffen werden müssen, um Teleworking im Einklang mit dem Datenschutz und unter Beachtung der Informationssicherheit effektiv nutzen zu können.

- Sinnvolle Richtlinien/Regelwerke für das Teleworking entwickeln und in Kraft setzen

### Wichtige Aufgabenbereiche beim Teleworking

- Personalmanagement: Genehmigungen/Vereinbarungen, Aus- und Fortbildung der Teleworker, Abgrenzung dienstliche/private Nutzung
- Technischer Support: detaillierte Darstellung der Support-Aktivitäten, insbesondere (remote) Management der Teleworking-Systeme
- Überwachung des Teleworkings: Monitoring, Inspektionen, Audits

### Technische Voraussetzungen und Maßnahmen für das Teleworking

- Maßnahmen zur Absicherung der Teleworking-Systeme, der Arbeitsumgebung und des Netzwerkzugangs
- Einsatz von Kryptografie/Verschlüsselung
- Sichere Formen der Authentisierung nutzen
- Alternativen für die sichere Kommunikation (Algorithmen, Protokolle, Architekturen) zwischen Teleworker und Unternehmen (bzw. Cloud)

## ANMELDUNG unter [datakontext.com](http://datakontext.com) oder per Fax +49 2234 98949-44

Wir melden an:

### Teleworking unter Beachtung von Datenschutz und Sicherheit

- 05.05.2021 Online-Schulung
- 04.11.2021 in Köln

Jeweils 5,5 Nettostunden

#### Teilnahmegebühr:

700 € zzgl. gesetzl. MwSt.  
(Präsenz-Schulung)

495 € zzgl. gesetzl. MwSt.  
(Online-Schulung)

**Enthalten sind:** Tagungsunterlagen, Teilnahmebescheinigung und bei Präsenz-Veranstaltungen Pausengetränke und Mittagessen. Das Tagungshotel der Präsenz-Veranstaltung teilen wir Ihnen in der Anmeldebestätigung mit. Stornierungen ab 14 Tage vor Veranstaltungsbeginn müssen mit 50 % der Gebühren, Absagen am Veranstaltungstag mit der vollen Gebühr belastet werden. Stornierungen werden nur schriftlich akzeptiert. Der Veranstalter behält sich vor, das Seminar bis 14 Tage und die Online-Schulung bis 2 Tage vor Beginn zu stornieren. Die Veranstaltungsgebühr ist 14 Tage nach Rechnungserhalt ohne Abzug fällig.

### DATAKONTEXT GmbH

Postfach 41 28 · 50217 Frechen

Tel.: +49 22 34 98949-40 · Fax: + 49 2234 98949-44

[datakontext.com](http://datakontext.com) · [tagungen@datakontext.com](mailto:tagungen@datakontext.com)

Änderungen bei Terminen, Preisen und Orten bleiben vorbehalten.

### RECHNUNGSANSCHRIFT:

1. Name: .....	Firma: .....
Vorname: .....	Abt.: .....
Funktion**:	Name: .....
Abteilung**:	Straße: .....
E-Mail*:	PLZ/Ort: .....
2. Name: .....	Telefon (geschäftlich): .....
Vorname: .....	Rechnungszustellung standardmäßig per E-Mail (unverschlüsselt) wie links angegeben oder an:
Funktion**:	<input type="checkbox"/> Auf Wunsch per Fax: .....
Abteilung**:	
E-Mail*:	Unterschrift: ..... Datum: .....

**Datenschutzinformation:** Wir, die DATAKONTEXT GmbH, Augustinusstr. 9d, 50226 Frechen, verwenden Ihre oben angegebenen Daten für die Bearbeitung Ihrer Bestellung, die Durchführung der Veranstaltung sowie für Direktmarketingzwecke. Dies erfolgt evtl. unter Einbeziehung von Dienstleistern und der GDD. Eine Weitergabe an weitere Dritte erfolgt nur zur Vertragserfüllung oder wenn wir gesetzlich dazu verpflichtet sind. Soweit Ihre Daten nicht als freiwillige Angaben mit \*\* gekennzeichnet sind, benötigen wir sie für die Erfüllung unserer vertraglichen Pflichten. Ohne diese Daten können wir Ihre Anmeldung nicht annehmen. Weitere Informationen zum Datenschutz erhalten Sie unter [datakontext.com/datenschutzinformation](http://datakontext.com/datenschutzinformation). Falls Sie keine Informationen mehr von uns erhalten wollen, können Sie uns dies jederzeit an folgende Adresse mitteilen: DATAKONTEXT GmbH, Augustinusstr. 9d, 50226 Frechen, Fax: 02234/98949-44, [werbewiderspruch@datakontext.com](mailto:werbewiderspruch@datakontext.com). \* Sie können der Verwendung Ihrer E-Mail-Adresse für Werbung jederzeit widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

### DATAKONTEXT-Repräsentanz

Postfach 20 03 03 · 08003 Zwickau

Tel.: +49 375 291728 · Fax: + 49 375 291727

[zwickau@datakontext.com](mailto:zwickau@datakontext.com)

INTERNET