



27.09.2024  
online

[jetzt anmelden](#)

# Technisches Basiswissen für Datenschutz und Informationssicherheitsbeauftragte

Funktionen von Hard- und Software, Gefährdungen sowie technische und organisatorische Maßnahmen einfach erklärt



Heiko Behrendt

ISO 27001 Auditor  
Datenschutz- und IT-Sicherheitsexperte  
einer Landes-Prüfbehörde

Das Praxisseminar befähigt Sie, die IT-Infrastruktur in Ihrem Umfeld besser zu verstehen. Sie sind in der Lage, die Zusammenhänge der Datenverarbeitungsprozesse zu beurteilen und können Datenschutz- und Informationssicherheitsschwachstellen auf IT-Systemen und IT-Komponenten erkennen sowie mit geeigneten technischen und organisatorischen Maßnahmen beseitigen.

Die Überwachung der automatisierten Datenverarbeitung auf die Einhaltung der DSGVO können Sie mit Hilfe von Checklisten anwendungsbezogen durchführen.



## Inhaltsübersicht

- IT-Systeme und IT-Komponenten in einer Organisation sicherheitstechnisch prüfen
- Funktionen und Besonderheiten bei
  - PC, Notebook, Thin-Client, Server
  - Tablets, Mobiltelefon
  - USB-Sticks, Speicherkarten
  - Router, Switches, Firewall
  - Speichersysteme
  - Multifunktionsgeräte
  - Betriebssysteme
  - Benutzerkonten und Berechtigungen
  - Fachanwendungen und Datenbanken
  - Datensicherung
  - Datenlöschung
  - Protokollierung und Monitoring
  - Virtualisierung
  - Clouddienste
- Ansatzpunkte für die Überprüfung der IT-Systeme und IT-Komponenten
- Auswahl technischer und organisatorischer Maßnahmen (TOM)
- Hilfsmittel zur Dokumentation und Nachvollziehbarkeit



08:45

### Login

09:00

### Begrüßung und Vorstellungsrunde

- Vorstellung des Referenten und der Teilnehmenden

09:15

### PC, Notebook, Thin-Client, Server, Tablets, Mobiltelefon, USB-Stick, Speicherkarten

- Merkmale: z.B. Hard- und Software, lokale Datenspeicherung, mobiler Einsatz möglich
- Schwachstellen: z.B. offene Schnittstellen, Apps, private Nutzung, externe Speichermedien
- Sicherheitsmaßnahmen: z.B. Patch Management, Verschlüsselung, Softwareverteilung
- Checkliste: Was sollte ich vor dem Einsatz der Medien beachten?

10:30

### Kaffeepause

11:00

### Router, Switches, Firewall, Speichersysteme, Multifunktionsgeräte

- Merkmale: z. B. Kabelverbindung, Interfaces, Firewall-Regeln, Festplattensubsysteme
- Schwachstellen: z. B. Protokollierung, Angriffe über Netzanschlusssdosen und Internetdienste, mangelnde Datenabschottung
- Sicherheitsmaßnahmen: Prozesse für die Administration von Firewall-Regeln, demilitarisierte Zone, Segmentierung des Netzes, Kennwörter, etc.
- Checkliste: Was sollte ich vor dem Einsatz der Medien beachten?

12:30

### Mittagessen

13:30

### Betriebssysteme, Benutzerkonten und Berechtigungen

- Merkmale: z.B. Nutzerkonto, Berechtigungen, Benutzerverwaltung, Verfügbarkeitsanforderungen
- Schwachstellen: z.B. Härtung, Rechtevergabe, zu weitgehende Datenprofile
- Sicherheitsmaßnahmen: Gruppenrichtlinien, komplexe Kennwörter, Datensicherungskonzept etc.
- Checkliste: Was sollte ich vor dem Einsatz beachten?



14:30

### **Fachanwendungen und Datenbanken, Datensicherung**

- Merkmale: z. B. Standardsoftware, SQL-Datenbanken, inkrementelle Datensicherung, Datensicherungsroboter
- Schwachstellen: z. B. Datensicherung, Inventarisierung
- Sicherheitsmaßnahmen: Test- und Freigabeverfahren, Löschrufen, Übung von Datenrekonstruktionen, etc.
- Checkliste: Was sollte ich vor dem Einsatz beachten?

15:30

### **Kaffeepause**

15:45

### **Datenlöschung, Protokollierung und Monitoring, Virtualisierung, Clouddienste**

- Merkmale: z. B. Löschttools, Syntax der Protokolle, Wirt- und Gastsysteme, Rechenzentren
- Schwachstellen: Ausfallrisiko, weitgehende Zugriffsberechtigungen, keine Revisionsfähigkeit, keine Kontrolle über die Datenverarbeitung beim Dienstleister, etc.
- Sicherheitsmaßnahmen: z. B. geeignete Tools, Syslog-Server, Ticketsystem, AV-Vertrag
- Checkliste: Was sollte ich vor dem Einsatz beachten?

17:00

### **Ende des Seminars**



### Heiko Behrendt

Als zertifizierter ISO 27001 Auditor für Informationssicherheit begleitet Heiko Behrendt Behörden und Firmen bei der Einführung und Sicherstellung von IT-Grundschutz- und Datenschutzstandards. Darüber hinaus führt er in seiner Funktion als Datenschutz- und IT-Sicherheitsexperte einer Aufsichtsbehörde Datenschutz-Audits sowie datenschutzrechtliche und sicherheitstechnische Kontrollen der Einhaltung der Datenschutzgrundverordnung durch.

### Zielgruppe – An wen richtet sich dieses Seminar?

Das Intensiv-Praxisseminar richtet sich nicht nur an Datenschutz- und Informationssicherheitsbeauftragte, sondern auch an Führungskräfte, MitarbeiterInnen und SachbearbeiterInnen, die an technischen und rechtlichen Aspekten des Datenschutzes interessiert sind.



## Termin:

**27.09.2024**

**online**

### **TEILNAHMEGEBÜHR:**

Online-Teilnahme: 427,- Euro zzgl. MwSt.

### **DIE TEILNAHMEGEBÜHR BEINHALTET:**

- Schulungsunterlagen (digital)
- Teilnahmezertifikat

### **ANMELDUNG:**

Bitte verwenden Sie zur Anmeldung unser Online-Anmeldeformular unter: [www.fortbildungskampagne.de/anmeldung](http://www.fortbildungskampagne.de/anmeldung)

### **KONTAKT FÜR RESERVIERUNGEN UND BUCHUNGEN:**

Haben Sie Fragen zum Seminar oder zu Reservierungen und Buchungen?

Schreiben Sie uns einfach eine Email oder rufen Sie uns unter der folgenden Rufnummer an:

Email: [team@fortbildungskampagne.de](mailto:team@fortbildungskampagne.de) | Telefon: +49 (0) 30 89 56 27 16

### **TEILNAHME- UND STORNIERUNGSKONDITION (AUSZUG):**

Die verbindliche Anmeldung erfolgt über unser Online-Anmeldeformular und wird durch Zusendung einer Anmeldebestätigung sowie der Rechnung bestätigt. Stornierungen sind bis vier Wochen vor Veranstaltungsbeginn kostenfrei, bereits gezahlte Beträge werden erstattet. Bei kurzfristiger Stornierung oder beispielsweise krankheitsbedingter Abwesenheit ist die Benennung eines Ersatzteilnehmers jederzeit möglich. Sofern sich kein Ersatzteilnehmer findet, kann nach Absprache ein Gutschein ausgestellt werden, der zur Teilnahme an einem Nachfolgetermin oder einem ähnlichen Seminar berechtigt. Bitte beachten Sie unsere AGB, die unter dem folgenden Link aufgerufen werden können:

[www.fortbildungskampagne.de/agb](http://www.fortbildungskampagne.de/agb)

### **DATENSCHUTZHINWEISE:**

Wir weisen darauf hin, dass Sie die Verwendung Ihrer Daten gemäß unserer Datenschutzbestimmungen durch eine Nachricht an [datenschutz@fortbildungskampagne.de](mailto:datenschutz@fortbildungskampagne.de) selbstverständlich jederzeit widerrufen können. Bitte beachten Sie unsere Datenschutzbestimmungen, die unter dem folgenden Link aufgerufen werden können:

[www.fortbildungskampagne.de/privacy](http://www.fortbildungskampagne.de/privacy)

### **HINWEISE ZUM DATENSCHUTZ BEI ONLINE-TEILNAHME:**

Details zur technischen Umsetzung der Online-Teilnahme erhalten Sie im Anschluss an Ihre Anmeldung. Ein wirksamer Auftragsverarbeitungsvertrag mit dem technischen Dienstleister liegt vor. Durch die Fortbildungskampagne als Veranstalter erfolgt während der Online-Teilnahme keine Speicherung von schriftlichen, akustischen oder visuellen Daten der Teilnehmenden. Eine temporäre Protokollierung des Chat-Verlaufes einer Online-Veranstaltung wird binnen zwei Arbeitstagen nach der Veranstaltung gelöscht. Bitte beachten Sie, dass Sie im Rahmen Ihrer Online-Teilnahme möglicherweise unfreiwillig Daten und Informationen übertragen, etwa durch weitere Personen in Ihrem Raum. Eine mögliche Übertragung derartiger Informationen liegt in Ihrem Verantwortungsbereich.