

DATENSCHUTZ-ORGANISATION

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

IT-Sicherheitsmanagement aus Sicht des/der Datenschutzbeauftragten

TERMIN/ORT

16. April 2024 in Köln

10:00–17:00 Uhr

REFERENTEN



Dr. Jens Eckhardt

Fachanwalt für Informationstechnologierecht,
Derra, Meyer & Partner Düsseldorf, Ulm, Berlin;
Datenschutzauditor und Compliance-Officer



Dr. Niels Lepperhoff

Geschäftsführer, XAMIT Bewertungsgesellschaft mbH;
DSZ Datenschutzauditor, Düsseldorf

SCHWERPUNKTTHEMEN

- Grundsätzliches zur DS-GVO
- Anforderungen der DS-GVO an das IT-Sicherheitsmanagement
- Wirksamkeitstest & Protokollierung
- Meldepflichten

ZIELGRUPPE

Datenschutzbeauftragte, Compliance Manager/innen,
Datenschutzverantwortliche der Personal- und DV-Abteilung,
IT-Sicherheitsbeauftragte

IHR NUTZEN

In komprimierter Form erhalten Sie einen Überblick über Haftungsrisiken im Zusammenhang mit Sicherheitsmaßnahmen. Es wird Handwerkszeug zur Beurteilung der Rechtmäßigkeit und Angemessenheit von Sicherheitsmaßnahmen vermitteln.

Zunehmende Cyberangriffe insbesondere mit Ransomware bedrohen Unternehmen. Innentätern kommt dabei eine besondere Bedeutung zu, da Ransomware-Banden teilweise Innentäter rekrutieren, um die Angriffe wirkungsvoller auszugestalten. Aber auch schlicht fehlende Vorsicht von Mitarbeitenden führt zu Sicherheitsrisiken und damit zum Erfolg von Cyberangriffen. Zusätzliche Sicherheitsmaßnahmen sind das Gebot der Stunde. Doch der Grat zwischen nicht genug und zuviel in der DS-GVO ist schmal. Denn Sicherheitsmaßnahmen – ob präventiv oder reaktiv – erfordern die Verarbeitung personenbezogener Daten. Beide

Pflichten müssen in Balance gebracht werden. Auf beiden Seiten lauern damit auch Bußgelder und Schadensersatzansprüche nach der DS-GVO. Cyber Security ist damit eine Frage der persönlichen Haftung und Organhaftung – sowohl für zu viel als auch für zu wenig Cyber Security. Als Lotse ist der/die Datenschutzbeauftragte gefragt, nicht Cyber Security zu fordern, sondern auch die Rechtmäßigkeit zu bewerten und vor allem die Angemessenheit in den Blick zu nehmen. Komplexe Sicherheitsmaßnahmen, wie KI-basierende Security Appliance und Big Data Analyse Verfahren, stellen dabei besondere Herausforderungen dar.

INHALT

- Haftung sowohl bei fehlenden Sicherheitsmaßnahmen als auch bei Missachtung der datenschutzrechtlichen Anforderungen
- Die Pflicht zur Meldung von Datenschutzpannen
- Rechtmäßigkeit von Sicherheitsmaßnahmen
- Hilfe des DSB bei Bewertung ausgewählter Sicherheitsmaßnahmen zum Schutz (Zweck heiligt nicht die Mittel)
- Besondere Anforderungen an Sicherheit von Internetdiensten durch § 19 TTDSG
- Anonymisierung als Bestandteil von Sicherheitsmaßnahmen (inkl. Bewertung ob Anonymisierung vorliegt)
- Unterscheidung zwischen Maßnahmen mit Personenbezug und solchen ohne
- Besondere Herausforderungen bei KI-basierten Security Appliances und Produkten
- Beurteilung der Angemessenheit von Sicherheitsmaßnahmen unter Bezugnahme auf Risikobeurteilung nach Art. 32, 35 DS-GVO

ANMELDUNG unter **datakontext.com** oder per Fax +49 2234 98949-44

Wir melden an:

IT-Sicherheitsmanagement aus Sicht des Datenschutz- beauftragten

☐ 16.04.2024 Köln

Jeweils 5,5 Nettostunden

Teilnahmegebühr:

790 € zzgl. gesetzl. MwSt.

Enthalten sind: Tagungsunterlagen, Pausengetränke, Mittagessen und Teilnahmebescheinigung. Das Tagungshotel teilen wir Ihnen in der Anmeldebestätigung mit.

Stornierungen sind bis 15 Tage vor Veranstaltungsbeginn kostenfrei, ab 14 bis 8 Tage vor Veranstaltungsbeginn werden 50 % der Gebühr berechnet. Ab 7 Tage vor Veranstaltungsbeginn bzw. nach Versand der Zugangsdaten wird die gesamte Veranstaltungsgebühr fällig. Stornierungen werden nur schriftlich akzeptiert. Der Veranstalter behält sich vor, die Präsenz-Veranstaltung bis 14 Tage und die Online-Veranstaltung bis 2 Tage vor Beginn zu stornieren. Die Veranstaltungsgebühr ist 14 Tage nach Rechnungserhalt ohne Abzug fällig. Sollten sich nicht genügend Teilnehmer für die Präsenz-Veranstaltung melden, behalten wir uns vor, das Seminar digital durchzuführen.

DATAKONTEXT GmbH

Postfach 41 28 · 50217 Frechen

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

datakontext.com · tagungen@datakontext.com

Änderungen bei Terminen, Preisen und Orten bleiben vorbehalten.

RECHNUNGSANSCHRIFT:

1. Name:

Vorname:

Funktion**:

Abteilung**:

E-Mail*:

2. Name:

Vorname:

Funktion**:

Abteilung**:

E-Mail*:

Firma:

Abt.:

Name:

Straße:

PLZ/Ort:

Telefon (geschäftlich):

Rechnungszustellung standardmäßig per E-Mail (unverschlüsselt) wie links angegeben oder an:

☐ Auf Wunsch per Fax:

Unterschrift: Datum:

Datenschutzinformation: Wir, die DATAKONTEXT GmbH, Augustinusstr. 11 A, 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

Falls Sie keine Informationen mehr von uns erhalten wollen, können Sie uns dies jederzeit an folgende Adresse mitteilen: DATAKONTEXT GmbH, Augustinusstr. 11 A, 50226 Frechen, Fax: 02234/98949-44, 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