21. Juli 2026 · 13:00–17:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

Datensicherheit und Data Governance zwischen DSGVO und DORA

Banken-Praxis-Seminar · 4,5 CPE-Punkte

- Zusammenspiel von DSGVO, DORA und anderen Rechtsnormen
- Zielkonflikte und Synergien u. a. in den Bereichen IKT-Risiko-management, Meldepflichten und Dienstleistersteuerung/TPRM
- Technische und organisatorische Maßnahmen (TOMs) und deren DORA- bzw. DSGVO-konforme Umsetzung
- Besondere Anforderungen an Dienstleistungs- und Drittparteien-Verträge nach DSGVO und DORA
- Operationalisierung in der Praxis: Hinweise und Umsetzungs-Tipps

Referent

Stefan Kountouris
Senior Consultant für Datenschutz, Governance,
Informationssicherheit & IT-Compliance
BridgingIT, Stuttgart

Datensicherheit und Data Governance zwischen DSGVO und DORA

Programm

Stefan Kountouris · 13:00–17:00 Uhr inkl. 15 Min. Pause nach 90 Min.

Regulatorischer Rahmen

- Überblick über das Zusammenspiel der relevanten Rechtsakte: DSGVO, DORA, Data Act, NIS2, EU AI Act, MaRisk, ggf. BAIT/VAIT/KAIT/ZAIT, Digitaler Omnibus
- DORA und NIS2: Wann greift NIS2?
- Integrationsmodell als integriertes Compliance-Modell

Verhältnis DSGVO zu DORA: Zielkonflikte und Synergien in den Bereichen IKT-Risikomanagement, Meldepflichten und Dienstleistersteuerung/TPRM

- Risikobasierter Ansatz als gemeinsame Grundlage von DSGVO und DORA – Abgrenzung personenbezogener Daten (Art. 24, 32, DSGVO) zu IKT-Risiken nach DORA – Schaffung eines gemeinsamen Risiko-Frameworks
- Synergie der Governance-Strukturen durch Integration der Datenschutzorganisation (DPO, TOMs) in die DORA-Governance (IKT-Risikomanagementfunktion)
- Konflikt zwischen Datenminimierung (DSGVO) und digitalen Resilienzanforderungen mit umfangreiche Log-, Monitoring- und Telemetriedaten zur Detektion und Abwehr von IKT-Vorfällen (DORA)
- Spannungsfeld Speicherbegrenzung vs. forensische Nachvollziehbarkeit – DSGVO-Löschfristen kollidieren mit DORA-Anforderungen an langfristige Incident-Analyse, Audit-Trails und Threat-Intelligence-Nutzung
- Konfliktpotential Drittlandtransfers zu IKT-Outsourcing
- Mögliche Synergie bei Incident Management
- Unterschiedliche Schutzobjekte: Schutz der Grundrechte natürlicher Personen nach DSGVO gegenüber dem Schutz der Systemstabilität und Finanzmarktintegrität nach DORA
- Zielkonflikte bei Penetration Testings (TLPT)
- Konflikte zwischen Transparenz und Sicherheits-geheimhaltung
- Synergie bei Zugriffskontrollen und IAM

Technische und organisatorische Maßnahmen (TOMs) und Umsetzungen unter Berücksichtigung von DSGVO und DORA

- Vertragliche Operationalisierung von Art. 32 DSGVO in Abgrenzung zu Art. 9 DORA
- Durchgriffstiefe bei (IKT-)Drittanbietern: DORA verlangt explizite Prüf- und Weisungsrechte (inkl. Subdienstleister-Ketten), die über typische DSGVO-Auftragsverarbeitungs-verträge hinausgehen
- Auditrechte und Prüfregime: DSGVO-Audits fokussieren Datenschutz-Compliance und TOM-Wirksamkeit, DORA auf umfassende IKT-Audits inklusive operativer Resilienz
- DSGVO-konforme Aufbereitung der DORA-Test-Daten
- Kontinuierliche Wirksamkeitsüberwachung der TOMs: Kombination aus DSGVO-Reviewpflichten und DORA-Resilienzmetriken (KPIs/KRIs) ermöglicht ein integriertes Control-Monitoring inklusive automatisierter Überwachung von Sicherheitsmaßnahmen, Incident Response und Wiederherstellungszeiten (RTO/RPO)

Besondere Anforderungen an Dienstleistungs- und Drittparteien-Verträge nach DSGVO und DORA

- Erweiterung des AVV zum IKT-Drittparteienvertrag: Art. 28 DSGVO im Vergleich zu Art. 29/30 der DORA
- Risiko- und Kritikalitätsklassifizierung
- Verstärkte Exit- und Substitutionspflichten: Während Art. 28 DSGVO primär Löschung/Rückgabe personenbezogener Daten regelt, verlangen Art. 29/30 DORA belastbare Exit-Strategien inkl. technischer Portabilität, Übergangsunterstützung und Vermeidung von Lock-in-Effekten – erhebliche Erweiterung der vertraglichen DORA-Anforderungen an Anbieterwechsel und Betriebsfortführung

Praxis-Hinweise und Umsetzungs-Tipps

- Konkrete Handlungsanweisungen und Best Practices für die effiziente Operationalisierung im Banken- und Dienstleisterumfeld

Seminarziel

Das Seminar vermittelt eine vertiefte, praxisnahe Analyse des Zusammenspiels von DSGVO und DORA mit Fokus auf konkrete Umsetzungs- und Steuerungsherausforderungen in der Banken- und Finanzdienstleistungs-Praxis.

Die Teilnehmenden entwickeln ein integriertes Verständnis für Zielkonflikte und Synergien beider Regime, insbesondere im Bereich technischer und organisatorischer Maßnahmen (TOMs), IKT-Drittparteienrisiken sowie vertraglicher Ausgestaltung.

Ziel ist es, bestehende Datenschutz- und IKT-Risikomanagementstrukturen fachlich zu harmonisieren, regulatorische Anforderungen effizient zu operationalisieren und belastbare Governance-, Kontroll- und Vertragsmodelle für eine resiliente und zugleich datenschutzkonforme Organisation zu etablieren.

Zielgruppe

Aus der Praxis für die Praxis!
Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche

- Interne Revision und IT-Revision
- Data Governance und Datenmanagement
- Risk-Data-Management und Data-Compliance
- Informationssicherheit (ISB), Datenschutz (DSB) und IKT-Risikokontrollfunktion
- IKT-Risikomanagement und Informationsrisikomanagement
- IT-Grundsatz und IT-Regulatorik

Sowie weitere interessierte Fachbereiche, Vorstandsmitglieder, Geschäftsleitung, externe Prüfer*innen sowie (Bank-)Dienstleister.

Gute Gründe für Ihre Teilnahme

- Sie erarbeiten sich aktuelles Know-how zu spezifischen Ansätzen für die Harmonisierung der Anforderungen aus DSGVO und DORA
- Sie erhalten sofort anwendbare Umsetzungstipps für Ihr Institut und Ihren Bereich
- Sie klären offene Fragen für Ihren Bereich oder Ihr Institut mit dem erfahrenen Referenten und anderen Expert*innen
- Sie erhalten wertvolle Praxis- und Anwendungs-Tipps im Erfahrungsaustausch mit anderen Praktiker*innen und Teilnehmenden

Unser Referent

Stefan Kountouris
Senior Consultant für Datenschutz, Governance, Informationssicherheit & IT-Compliance, BridgingIT, Stuttgart

Stefan Kountouris ist bei der BridgingIT in den Bereichen Datenschutz, Compliance, Governance und Informationssicherheit tätig. Davor war er u. a. in den Bereichen Auslagerungsmanagement, Konzerndatenschutz, Informationssicherheit, IT-Compliance und KI für verschiedene Banken und Finanzdienstleister tätig. Stefan Kountouris besitzt langjährige Expertise und Praxis-Erfahrungen zu den genannten Themen, die er u. a. im Rahmen von Praxis- und Fach-Vorträgen an die Teilnehmenden weitergibt.

Herausforderungen im Umgang mit KI-Dienstleistern durch DORA/MaRisk/KI-VO
10. Juni 2026, Online-Veranstaltung

Fachtagung IKT-Aufsicht
15./16. Juni 2026, Online-Veranstaltung

Zertifizierter KI-Governance-Officer
17. bis 19. Juni 2026, Online-Veranstaltung

IKT Spezial für Compliance & Governance
23. Juni 2026, Online-Veranstaltung

Anforderungen an IT-Infrastruktur und IT-Betrieb unter DORA
23. Juni 2026, Online-Veranstaltung

Praxis-Umsetzung IT-Sicherheit & Cyber-Sicherheit unter DORA
29. Juni 2026, Online-Veranstaltung

DORA- und Praxis-Anforderungen an die SOD-Matrix
13. Juli 2026, Online-Veranstaltung

IKT Spezial – Identity- & Access-Management (IAM)
22. Juli 2026, Online-Veranstaltung

▶ Diese und weitere Seminar-Angebote finden Sie bei uns online unter *www.akademie-heidelberg.de/online-seminare*

Zusätzliche Informationen

Fragen zu diesen Schulungen oder unserem gesamten Seminar-Programm beantworte ich Ihnen sehr gerne.

Björn Wehling
Telefon 06221/65033-44
b.wehling@akademie-heidelberg.de

Anmeldeformular

Datensicherheit und Data Governance zwischen DSGVO und DORA

Name

Vorname

Position

Firma

Straße / Nr.

PLZ / Ort

Telefon

E-Mail

Name der Assistenz

Datum / Unterschrift

Senden Sie Ihre Anmeldung bitte an: **anmeldung@akademie-heidelberg.de**

Termin und Seminarzeiten

Dienstag, 21. Juli 2026
13:00–17:00 Uhr
Online-Zugang ab 12:45 Uhr

Seminar-Nr. 26 07 BA221 W

Teilnahmegebühr

€ 220,– (zzgl. gesetzl. USt)

Die Gebühr beinhaltet die Teilnahme am Online-Seminar sowie die Präsentation als PDF-Datei.
Im Anschluss an das Seminar erhalten Sie ein Zertifikat, das Ihnen die Teilnahme an der Fortbildung bestätigt.

Allgemeine Geschäftsbedingungen

Es gelten unsere Allgemeinen Geschäftsbedingungen (Stand: 01.01.2010), die wir Ihnen auf Wunsch gerne zusenden. Diese können Sie jederzeit auch auf unserer Website einsehen: www.akademie-heidelberg.de/agb

Zum Ablauf

- Vor dem Seminartag erhalten Sie von uns eine E-Mail mit einem Link, über den Sie sich direkt in die Online-Veranstaltung einwählen können.
- Für Ihre Teilnahme ist es nicht notwendig, ein Programm herunterzuladen. Sie können am Seminar direkt per *Zoom* im Browser teilnehmen.
- Über Ihr Mikrofon und Ihre Kamera können Sie jederzeit Fragen stellen und mit den Referierenden und weiteren Teilnehmenden diskutieren. Alternativ steht auch ein Chat zur Verfügung.

AKADEMIE HEIDELBERG

AH Akademie für Fortbildung Heidelberg GmbH
Maaßstraße 32/1 · 69123 Heidelberg
Telefon 06221/65033-0
info@akademie-heidelberg.de
www.akademie-heidelberg.de

05.26 / 26 07 BA221