Europäische Akademie
für Steuern, Wirtschaft & Recht

Intensivseminar

IT-Sicherheitsrecht in öffentlichen Institutionen und Unternehmen praktisch umsetzen

Einen Weg durch den Paragrafendschungel finden

28. – 29. November 2016, Berlin

Broschüre

Mit Fokus auf:

- **Gebündelter und fundierter Überblick über die geltenden Rechtsvorschriften und ihre Umsetzung**
- **Klare Anleitung bei den brisanten Fragen des IT-Sicherheitsrechts:**
  - **Haftung bei Sicherheitsverstößen**
  - **Rechtliche Grenzen von IT-Sicherheitsmaßnahmen**
  - **Überwachung von Telekommunikation**
  - **Protokollierung**
  - **Outsourcing und Vergabe**
  - **Privatnutzung und BYOD**
  - **Umsetzungsplan KRITIS und Auswirkungen des IT-Sicherheitsgesetzes**

INTERAKTIVES PRAXISSEMINAR

IT-Sicherheitsrecht in öffentlichen Institutionen und Unternehmen praktisch umsetzen

Das IT-Sicherheitsrecht und seine Umsetzung als Herausforderung für die öffentlichen Institutionen

Die IT-Sicherheitsbeauftragten und IT-Verantwortlichen in den öffentlichen Institutionen sind mit den technischen Aspekten ihrer Arbeit bestens vertraut. Bei den rechtlichen Aspekten jedoch haben zahlreiche das Gefühl, sich auf unsicherem Boden zu bewegen. Viele rechtliche Fragen, die u. a. solche Themenfelder wie

- Haftung bei IT-Sicherheitsvorfällen
- rechtliche Grenzen von IT-Sicherheitsmaßnahmen
- Überwachung von Telekommunikation
- Protokollierung
- Sicherheitsaspekte beim Outsourcing und der Vergabe
- Privatnutzung von dienstlicher IT
- BYOD

betreffen, können IT-Sicherheitsbeauftragten und IT-Verantwortlichen, die in der Regel über keine fundierte juristische Ausbildung verfügen, den Schlaf rauben.

Dies ist u. a. auch darauf zurückzuführen, dass es kein einheitliches IT-Sicherheitsrecht gibt und die relevanten rechtlichen Vorgaben über zahlreiche Gesetzestexte, Verordnungen, Verwaltungsanweisungen und Leitlinien verstreut sind. Nicht wenige IT-Sicherheitsbeauftragte und IT-Verantwortliche vermissen in ihrer täglichen Arbeit daher einen gebündelten und klaren Überblick über die aktuellen Rechtsvorschriften für IT-Sicherheitsbeauftragte und eine Experteneinblick in die rechtlich brisanten, komplizierten und aktuellen Themen des IT-Sicherheitsrecht, zu denen bspw. auch die Auswirkungen des IT-Sicherheitsgesetzes und der Umsetzungsplan KRITIS gehören.

Ein solcher Überblick erleichtert die praktische Erarbeitung und den Rollout von Sicherheitsrichtlinien, Sicherheitskonzepten oder Sicherheitsleitlinien enorm, mit denen IT-Sicherheitsbeauftragte das IT-Sicherheitsrecht in ihren öffentlichen Institutionen umsetzen. Das interaktive Praxisseminar wird sich aber nicht nur den aktuellen Gesetzen und Vorschriften widmen, sondern auch einen Einblick in die Umsetzung derselben anbieten. Dabei soll bspw. anhand von Praxisberichten erfahrener IT-Sicherheitsbeauftragter und Datenschützer aufgezeigt werden wie

- Sicherheitsleitlinien, Sicherheitsrichtlinien oder Sicherheitskonzepte rechtskonform erarbeitet und implementiert werden können
- eine Erfolgskontrolle des Standes der Informationssicherheit (in der eigenen öffentlichen Institution) gestaltet werden kann
- IT-Tools (bspw. ein Multinormtool) zur Umsetzung rechtlicher Vorgaben eingesetzt werden können
- Lösungen im Zielkonflikt zwischen optimaler IT-Sicherheit und geltenden Rechtsvorschriften gefunden werden können.

„Die Veranstaltung war insgesamt eine sehr entspannte, runde und interessante Sache.“

Christopher Meyer, IT-Sicherheitsbeauftragter, Stiftung Deutsches Technikmuseum Berlin

An wen richtet sich das Praxisseminar?

IT-Sicherheitsbeauftragte, IT-Sicherheitsrecht- und IT-Recht-Verantwortliche, Leiter der Abteilungen und alle Mitarbeiter, die verantwortlich sind für die Bereiche:

- IT-Sicherheit, IT-Sicherheitsmanagement
- IT-Management
- IT/EDV
- Datenschutz, (technologischer) Datenschutz
- (IT-) Recht
- Compliance
- Zentrale Abteilung
- IT-Revision/Innenrevision
- Informationssicherheit
- Sicherheit
- Geheimschutz
- Sabotageschutz
- eGovernment
- Verwaltungsmodernisierung
- Vergabe

Aus öffentlichen Verwaltungen und Unternehmen in öffentlicher Hand, wie:

- Bundesministerien und nachgeordnete Behörden, Ämter und Betriebe auf Bundesebene
- Landesministerien und nachgeordnete Behörden, Ämter und Betriebe auf Landesebene - inkl. IT-Landesdienstleister
- Kreise und Landkreise
- Städte und Kommunen und nachgeordnete Behörden, Ämter und Betriebe von Städten und Kommunen - inkl. kommunale IT-Dienstleister
- Unternehmen in öffentlicher Hand und des öffentlichen Rechts
- (öffentliche) Rechenzentren, wie bspw. Hochschulrechen-zentren, kommunale Rechenzentren
- Betreiber von kritischer Infrastruktur (bspw. Stadtwerke, Krankenhäuser)
- Sicherheitsbehörden, wie bspw. Polizeibehörden
- Hochschulen und Forschungseinrichtungen
- Kirchlichen Einrichtungen und Non-Profit-Organisationen
- Öffentlichen Banken

Europäische Akademie
für Steuern, Wirtschaft & Recht

Was lernen Sie in diesem Praxisseminar?

- Welche Herausforderungen und Chancen bestehen beim IT-Sicherheitsrecht für öffentliche Institutionen?
- Welche aktuellen Rechtsvorschriften müssen IT-Sicherheitsbeauftragte und IT-Verantwortliche kennen und beachten?
- Was sind die rechtlichen Pflichten und die Rolle des IT-Sicherheitsbeauftragten und welche IT-Sicherheitsstandards müssen in öffentlichen Institutionen beachtet werden?
- Welche Veränderungen wird das kommende IT-Sicherheitsgesetz bringen?
- Was muss bei der Erarbeitung und beim Rollout von Sicherheitsrichtlinien, Sicherheitskonzepten oder Sicherheitsleitlinien beachtet werden?
- Was ist die Erfolgskontrolle des Standes der Informationssicherheit in einer öffentlichen Institution zu gestalten?
- Welche Rolle können IT-Tools (bspw. Multinormtools) bei der Umsetzung rechtlicher Vorgaben spielen?
- Was müssen öffentlichen Institutionen, IT-Sicherheitsbeauftragte und IT-Verantwortliche im Hinblick auf die Haftung bei IT-Sicherheitsverstößen, die rechtlichen Grenzen von IT-Sicherheitsmaßnahmen, die Überwachung von Telekommunikation und Protokollierung beachten?
- Welche Fragen des IT-Sicherheitsrechts müssen beim Outsourcing und bei der Vergabe beachtet werden?
- Welche rechtlichen Fallstricke können die Privatnutzung dienstlicher IT und BYOD (die Nutzung von privater IT für dienstliche Zwecke) mit sich bringen und wie sind diese zu umgehen?

Ihre Vorteile

- Stellen Sie sicher, dass das Ihre öffentliche Institution und auch Sie persönlich (als IT-Sicherheitsbeauftragter) rechtlich geschützt sind.
- Sichern Sie sich das aktuelle rechtliche Wissen, dass Sie für Ihre tägliche Arbeit brauchen.
- Seien Sie darauf vorbereitet, auch in einem rechtlichen Notfall richtig zu handeln.
- Nutzen Sie die Vorteile, die die richtigen Zertifizierungen, Audits und Revisionen bei einem rechtlichen Vorfall für Sie bringen.
- Tauschen Sie Erfahrungen mit Kollegen und unserem Experten aus einem großen Kreis von öffentlichen Institutionen von Bundes-, Landes- und kommunaler Ebene aus.

Fachseminar für Behörden und öffentliche Institutionen

Praktische Umsetzung des IT-Vergabe- und Vertragsmanagements in der öffentlichen Verwaltung *(S-1391)*

30. November – 1. Dezember 2016

Für weitere Informationen, klicken Sie bitte **hier.**

„Masterclass Zentrale Verwaltung“

Dieses Seminar ist Bestandteil der „Masterclass Zentrale Verwaltung“.

Für weitere Informationen **klicken Sie bitte hier.**

PROGRAMM TAG 1

IT-Sicherheitsrecht in öffentlichen Institutionen und Unternehmen praktisch umsetzen

08:30-09:00
Akkreditierung und Ausgabe der Seminarunterlagen

09:00-09:05
Begrüßung durch die Europäische Akademie für Steuern, Wirtschaft & Recht

09:05-09:30
Begrüßung durch den Seminarleiter und Vorstellungsrunde

9:30-10:15
Keynote: IT-Sicherheitsrecht: Herausforderungen und Chancen für die öffentlichen Institutionen und Unternehmen aus der Sicht eines IT-Sicherheitsbeauftragten

- Was muss IT-Sicherheit in öffentlichen Behörden und Unternehmen leisten? Was kann sie in dem gebotenen Rechtsrahmen leisten?
- Paragraphendschungel – Wie komme ich als IT-Sicherheitsbeauftragter durch die rechtlichen Anforderungen und wo nützen sie mir?
- Allein auf weiter Flur? – Wie gestalte ich die Schnittstellen zum Datenschutz und zur Rechtsabteilung effektiv, um gute Ergebnisse zu erhalten?

Andreas Schmidt, IT-Sicherheitsbeauftragter, ISO 27001 Auditor und IS-Revisor, Grundschutzauditor (BSI-ZIG-0255-2012), Bundesministerium für Wirtschaft und Energie (BMWi)

10:15-10:30
Diskussionsrunde

10:30-11:00
Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

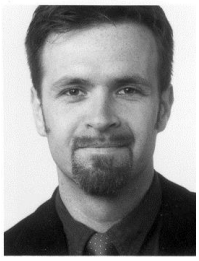
Rechtsvorschriften, Rolle und Pflichten des IT-Sicherheitsbeauftragten

11:00-11:45
Rechtsgrundlagen für IT-Sicherheitsbeauftragte: Gebündelter und klarer Überblick

- Schutzziele für die Datensicherheit
- Gesetze, Verordnungen, Verwaltungsanweisungen, Leitlinien
- Welche Handlungspflichten resultieren aus welchen Vorgaben?
- Aufgaben des Datenschutz- und des IT-Sicherheitsbeauftragten – Gibt es Zielkonflikte?

Heiko Behrendt, Gutachter und Berater für Datenschutzaudits, ISO 27001 Grundschutzauditor, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

11:45-12:00
Diskussionsrunde



ANDREAS SCHMIDT

IT-Sicherheitsbeauftragter, ISO 27001 Auditor und IS-Revisor, Grundschutzauditor (BSI-ZIG-0255-2012), Bundesministerium für Wirtschaft und Energie (BMWi)

Andreas Schmidt ist seit 2011 im Bundesministerium für Wirtschaft und Energie als IT-Sicherheitsbeauftragter tätig und in dieser Funktion für das Ministerium und den Geschäftsbereich verantwortlich. Weiterhin leitet er das IT-Projektmanagement im BMWi. Davor hat er unter anderem die Sicherheit und den Geheimschutz für den Digitalfunk der BOS-Behörden verantwortet und war als Referent für IT-Sicherheit im BMI tätig. Als ISO 27001 Auditor und IS-Revisor führt Andreas Schmidt darüber hinaus Audits und Revisionen nach der Methodik des IT-Grundschutz des BSI durch.

HEIKO BEHRENDT

Gutachter und Berater für Datenschutzaudits, ISO 27001 Grundschutzauditor, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Heiko Behrendt ist beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) in leitender Funktion für die Durchführung datenschutzrechtlicher und sicherheitstechnischer Audits zuständig. Als zertifizierter ISO 27001 Grundschutzauditor hat er Organisationen auf dem Weg der Grundschutzeinführung bis zur Zertifizierung erfolgreich begleitet und unterstützt. Die Ausbildung von Datenschutzbeauftragten, die methodische Durchführung von Audits und die komplexe IT-Grundschutzthematik gehören zu seinen Schwerpunkten.

„Interessanter Erfahrungsaustausch."

12:00-12:45

Rolle und Pflichten des IT-Sicherheitsbeauftragten

- Was muss? Was kann?
- Informations- und Meldeplichten bei Sicherheitsvorfällen
- Orientierung an etablierten Standards für IT-Sicherheit
  - ISO 27001 nativ
  - BSI Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
  - BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
  - IT-Grundschutz-Kataloge
- Business Continuity Management (BCM)
- IT-Sicherheitskonzept, IT-Sicherheitsleitlinie und IT-Sicherheitsrichtlinien
- Überwachung und Aktualisierung des IT-Sicherheitskonzepts

Heiko Behrendt, Gutachter und Berater für Datenschutzaudits, ISO 27001 Grundschutzauditor, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

12:45-13:00

Diskussionsrunde

13:00-14:00

Mittagspause mit Gelegenheit zum Erfahrungsaustausch und Networking

14:00-14:45

Umsetzungsplan KRITIS und Auswirkungen des IT-Sicherheitsgesetzes

- Empfehlung oder schon verbindliche Vorschrift?
- Ziel des Gesetzes – Schutz der Bürgerinnen und Bürger?
- Betroffene Branchen/Sektoren/Unternehmen
- Einhaltung eines Mindestniveaus an IT-Sicherheit
- Regelmäßiger Nachweis der Erfüllung durch Sicherheitsaudits
- Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI
- Betreiben einer Kontaktstelle

Heiko Behrendt, Gutachter und Berater für Datenschutzaudits, ISO 27001 Grundschutzauditor, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

14:45-15:00

Diskussionsrunde

15:00-15:30

Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

Praktische Erfahrungen bei der Umsetzung des IT-Sicherheitsrechts

15:30-16:15

Erarbeitung und Rollout von Sicherheitsleitlinien, Sicherheitsrichtlinien oder Sicherheitskonzepten in öffentlichen Institutionen

- Welche Bereiche sollten geregelt werden?
- Best Practices:
  - Privatnutzung der IT- und TK-Infrastruktur
  - Nutzung privater IT für dienstliche Zwecke (BYOD)
  - Protokollierung
  - Kopier- und Installationsverbote
  - Umgang mit externen Datenträgern und/oder mobilen Datenträgern
  - Abwesenheits- und Vertretungsregeln
  - Verpflichtungen zur Meldung von Sicherheitsvorfällen
- Lösungen im Zielkonflikt zwischen:
  - IT-Sicherheit
  - Datenschutz
  - Staatlichem Geheim- und Sabotageschutz
  - Fernmeldegeheimnis etc.

Andreas Schmidt, IT-Sicherheitsbeauftragter, ISO 27001 Auditor und IS-Revisor, Grundschutzauditor (BSI-ZIG-0255-2012), Bundesministerium für Wirtschaft und Energie (BMWi)

16:15-16:30

Diskussionsrunde

16:30-17:15

Erfolgskontrolle zum Stand der Informationssicherheit in der eigenen Institution

- Rechtliche, normative und konzeptionelle Vorgaben
- Erfolgskontrolle im PDCA-Zyklus („Plan, Do, Check, Act“)
- Messen der Effizienz und Effektivität von IT-Sicherheitsmaßnahmen
- Gestaltung interner Audits (Anforderungen, Praxisberichte)
- IS-Revisionen, Audits, Zertifizierungen

Andreas Schmidt, IT-Sicherheitsbeauftragter, ISO 27001 Auditor und IS-Revisor, Grundschutzauditor (BSI-ZIG-0255-2012), Bundesministerium für Wirtschaft und Energie (BMWi)

17:15-17:30

Diskussionsrunde

17:30

Ende des ersten Tages des interaktiven Praxisseminars

PROGRAMM TAG 2

IT-Sicherheitsrecht in öffentlichen Institutionen und Unternehmen praktisch umsetzen

Praktische Erfahrungen bei der Umsetzung des IT-Sicherheitsrechts

08:30-10:00

Technische Umsetzung rechtlicher Vorgaben leicht gemacht: BSI-Grundschutz-Tool – Best Practice mit einem Multinormtool

- Rechtliche und technische Rahmenbedingungen
- Normen: 27001, ISIS12, IDW-Standards, usw.
- Komplexitätsreduktion – Vorgehensmodell/Tailoring
- Organisatorische und personelle Hürden
- Controlling des Sicherheitsstatus
- Umsetzungsbeispiele

Frank Moses, Landesbeauftragter für Informationssicherheit, Ministerium für Finanzen und Europa des Saarlandes

10:00-10:15

Diskussionsrunde

10:15-10:45

Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

Haftung bei Sicherheitsverstößen, rechtliche Grenzen von IT-Sicherheitsmaßnahmen und weitere rechtlich brisante Themen

10:45-11:30

Haftung bei IT-Sicherheitsverstößen, rechtliche Grenzen von IT-Sicherheitsmaßnahmen, Überwachung von Telekommunikation, Protokollierung

- Haftung der öffentlichen Institution; persönliche Haftung des IT-Sicherheitsbeauftragten
  - gegenüber der Behörde
  - gegenüber den Geschädigten
- Spannungsfeld IT-Sicherheit und
  - Grundrechte
  - Datenschutz
  - Fernmeldegeheimnis
  - Arbeitnehmerrechte
- Optimale IT-Sicherheit vs. die Rechte Dritter
- Überwachung von Telekommunikation
- Protokollierung

Thomas H. Fischer, M.B.L.-HSG, Rechtsanwalt und Partner bei Waldeck Rechtsanwälte PartmbB, Fachanwalt für Informationstechnologierecht

11:30-11:45

Diskussionsrunde

11:45-13:00

Mittagspause mit Gelegenheit zum Erfahrungsaustausch und Networking

FRANK MOSES

Landesbeauftragter für Informationssicherheit, Ministerium für Finanzen und Europa des Saarlandes

Frank Moses verantwortet als Landesbeauftragter für Informationssicherheit den Aufbau und die Etablierung eines Informationssicherheits-Managementsystem (ISMS) im Ministerium für Finanzen und Europa des Saarlandes, wo er seit 1995 Referent ist. In der Rolle als Landesbeauftragter für Informationssicherheit vertritt er das Land in den Arbeitsgruppen AG-InfoSic und AG-Cybersicherheit des IT-Planungsrats. Davor war er Projektleiter für unterschiedliche Projekte wie die Einführung eines Dokumentenmanagementsystems, eines landeseinheitlichen Business-Intelligence- und Controllingsystems und unterstützte in den vergangenen fünf Jahren den CIO bei strategischen Planungen zur Verwaltungsmodernisierung.

THOMAS H. FISCHER, M.B.L.-HSG

Rechtsanwalt und Partner bei Waldeck Rechtsanwälte PartmbB, Fachanwalt für Informationstechnologierecht

Thomas Fischer ist Rechtsanwalt und Partner der Sozietät Waldeck Rechtsanwälte in Frankfurt am Main. Die Kanzlei gründete er 2004 mit Partnern renommierter Großsozietäten. Zuvor war er in internationalen Sozietäten in Frankfurt und Hamburg tätig. Seit vielen Jahren begleitet Thomas Fischer Vergabeverfahren im IT-Umfeld sowie komplexe Outsourcing Projekte. 2014 wurde er vom Handelsblatt zu einem der besten Rechtsanwälte im Bereich IT Recht gekürt. Er berät den Branchenverband BITKOM bei den Verhandlungen zur Ausgestaltung der EVB-IT Verträge. Im WHO'S WHO LEGAL, dem offiziellen Research Partner der International Bar Association, wurde er als „einer der führenden Experten unter den Vergaberechtsanwälten" für Deutschland aufgenommen. Die Sozietät Waldeck Rechtsanwälte wurde von der britischen Zeitschrift ACQ-Magazin zur besten „Public Procurement Law Firm of the Year 2014" in Deutschland gewählt.

13:00-13:45

Outsourcing und Vergabe als besondere rechtliche Herausforderung im IT-Sicherheitsrecht

- Auftragsvergabe an Dritte: Kontrollverlust bei gleichzeitiger Verantwortung des Auftraggebers (für Datenschutz und IT-Sicherheit)
- Vergabe: Geheimhaltungsbedürftige Aufträge
- Sicherheitsfragen im Vergabeverfahren
- Möglichkeiten der Risikominimierung durch eine geschickte Vertragsgestaltung

Thomas H. Fischer, M.B.L.-HSG, Rechtsanwalt und Partner bei Waldeck Rechtsanwälte PartmbB, Fachanwalt für Informationstechnologierecht

13:45-14:00
Diskussionsrunde

14:00-14:30
Kaffeepause mit Gelegenheit zum Erfahrungsaustausch und Networking

14:30-15:15

Privatnutzung und BYOD als rechtliche Herausforderungen

- Private Nutzung dienstlicher IT: rechtliche Herausforderungen und Lösungen
- Nutzung privater IT für dienstliche Zwecke (BYOD): Fallstricke und Chancen

Thomas H. Fischer, M.B.L.-HSG, Rechtsanwalt und Partner bei Waldeck Rechtsanwälte PartmbB, Fachanwalt für Informationstechnologierecht

15:15-15:30
Diskussionsrunde

15:30
Ende des interaktiven Praxisseminars und Ausgabe der Zertifikate

THOMAS H. FISCHER, M.B.L.-HSG

Rechtsanwalt und Partner bei Waldeck Rechtsanwälte PartmbB, Fachanwalt für Informations-technologierecht

Thomas Fischer ist Rechtsanwalt und Partner der Sozietät Waldeck Rechtsanwälte in Frankfurt am Main. Die Kanzlei gründete er 2004 mit Partnern renommierter Großsozietäten. Zuvor war er in internationalen Sozietäten in Frankfurt und Hamburg tätig. Seit vielen Jahren begleitet Thomas Fischer Vergabeverfahren im IT-Umfeld sowie komplexe Outsourcing Projekte. 2014 wurde er vom Handelsblatt zu einem der besten Rechtsanwälte im Bereich IT Recht gekürt. Er berät den Branchenverband BITKOM bei den Verhandlungen zur Ausgestaltung der EVB-IT Verträge. Im WHO'S WHO LEGAL, dem offiziellen Research Partner der International Bar Association, wurde er als „einer der führenden Experten unter den Vergaberechtsanwälten" für Deutschland aufgenommen. Die Sozietät Waldeck Rechtsanwälte wurde von der britischen Zeitschrift ACQ-Magazin zur besten „Public Procurement Law Firm of the Year 2014" in Deutschland gewählt.

„Hochinteressant. Viel Inhalt unterhaltsam vermittelt."

„Sehr gelungen. Fachlich und inhaltlich sehr gut rübergebracht."

IT-Sicherheitsrecht in öffentlichen Institutionen und Unternehmen praktisch umsetzen

Veranstaltungstermin
28. – 29. November 2016, Berlin

Buchungsnummer
S-1383 MC3

Veranstaltungssprache
Die Veranstaltungssprache ist Deutsch.

Veranstaltungspreis
1.389,- Euro

Im Veranstaltungspreis inbegriffen sind:
- Umfangreiche Veranstaltungsunterlagen, die als Druckerzeugnis im Rahmen der Veranstaltung übergeben werden
- Seminar-Zertifikat bei voller Anwesenheit
- Getränke und abwechslungsreiche Pausenversorgung während der ganzen Veranstaltung
- Mittagessen an beiden Tagen

Auf Wunsch erhalten Sie nach der Veranstaltung die **digitale Version** der Tagungsunterlagen zum Preis von **zzgl. 60,- Euro** zusätzlich zum Seminar.

Alle Preise zzgl. 19% MwSt.

Fachseminar für Behörden und öffentliche Institutionen

Praktische Umsetzung des IT-Vergabe- und Vertragsmanagements in der öffentlichen Verwaltung *(S-1391)*

30. November – 1. Dezember 2016

Für weitere Informationen, klicken Sie bitte **hier.**

BUCHUNG
E-Mail: buchung@euroakad.eu
Tel.: +49 (0)30 802080-20
Fax: +49 (0)30 802080-22250
Für Online-Buchungen besuchen Sie bitte unsere Internetseite:
www.euroakad.eu

Kontakt
Europäische Akademie für Steuern, Wirtschaft & Recht
am Potsdamer Platz, Eingang Leipziger Platz 9
10117 Berlin
Tel.: +49 (0)30 80 20 80 230
Fax: +49 (0)30 80 20 80 250
E-Mail: info@euroakad.eu
Internet: www.euroakad.eu

Ihre AnsprechpartnerInnen zum Programm:

Regina Lüning, M. Sc. econ.
Leiterin Marketing & Sales
Tel.: +49 (0)30 80 20 802 2300
Fax: +49 (0)30 80 20 802 2250
E-Mail: regina.luening@euroakad.eu

Pascal Dumont du Voitel, M.A.
Conference Manager
Tel.: +49 (0)30 80 20 80 21 349
Fax: +49 (0)30 80 20 80 22 259
E-Mail: pascal.dumont@euroakad.eu

(Programmänderungen vorbehalten)

Veranstaltungsort
RAMADA Hotel Berlin-Alexanderplatz
Karl-Liebknecht-Straße 32
10178 Berlin
Tel.: +49 (0)30 30 10 411 750
Fax: +49 (0)30 30 10 411 759
E-Mail: berlin.alex@h-hotels.com

Bitte nehmen Sie die Zimmerreservierung direkt im Hotel unter dem Stichwort „Europäische Akademie für Steuern, Wirtschaft & Recht“ vor, wenn Sie im Veranstaltungshotel auf ein begrenzt verfügbares Zimmerkontingent zurückgreifen möchten. Selbstverständlich können Sie auch ein anderes Hotel für Ihre Übernachtung wählen.

BUCHUNG
E-Mail: buchung@euroakad.eu
Tel.: +49 (0)30 802080-20
Fax: +49 (0)30 802080-22250
Für Online-Buchungen besuchen Sie bitte unsere Internetseite:
www.euroakad.eu

Europäische Akademie
für Steuern, Wirtschaft & Recht

Buchung

Buchungsnummer: S-1383 MC3 (DMW) 28. – 29. November 2016, Berlin

Hiermit möchten wir die folgenden Personen verbindlich für das Intensivseminar: „IT-Sicherheitsrecht in öffentlichen Institutionen und Unternehmen praktisch umsetzen“ anmelden.

Teilnehmer 1 ☐ Frau ☐ Herr

Vorname _____ Tel. _____
Nachname _____ Fax _____
Organisation _____ **E-Mail** _____
Abteilung _____
U-Abt. / Referat _____ ☐ Hiermit bestelle ich die digitale Version der kostenpflichtigen Tagungsunterlagen zusätzlich zum Seminar.
Position _____
Straße _____
PLZ / Stadt _____
Land _____

Teilnehmer 2 ☐ Frau ☐ Herr

Vorname _____ Tel. _____
Nachname _____ Fax _____
Organisation _____ **E-Mail** _____
Abteilung _____
U-Abt. / Referat _____ ☐ Hiermit bestelle ich die digitale Version der kostenpflichtigen Tagungsunterlagen zusätzlich zum Seminar.
Position _____
Straße _____
PLZ / Stadt _____
Land

Rechnungsanschrift, falls abweichend ☐ Frau ☐ Herr

Vorname _____ Straße _____
Nachname _____ PLZ / Stadt _____
Organisation _____ Land _____
Abteilung _____ Tel. _____
U-Abt. / Referat _____ Fax _____
Position _____
E-Mail _____

Mit meiner Unterschrift bestätige ich die rechtsverbindliche Anmeldung und akzeptiere die Allgemeinen Geschäftsbedingungen.

HINWEIS
Die Anmeldung ist nur mit Stempel und Unterschrift gültig.

☐ Hiermit stimme ich zu, weitere Information von der Europäischen Akademie für Steuern, Wirtschaft & Recht zu erhalten.

Bei Anmeldung von mehreren Teilnehmern wünschen Sie:
☐ Einzelrechnung? ☐ Sammelrechnung?

Ort, Datum **Unterschrift Bevollmächtigter und Stempel**

Allgemeine Geschäftsbedingungen

für die Angebote der Europäische Akademie für Steuern, Wirtschaft & Recht

§ 1 Geltungsbereich - Vertragsgegenstand - Vertragspartner
(1) Die AGB gelten für die Teilnahme an allen von der Europäische Akademie für Steuern, Wirtschaft & Recht (folgend EA) angebotenen und durchgeführten Bildungsmaßnahmen wie Kurse, Seminare, Workshops, Trainings („Veranstaltung“) einschließlich aller damit verbundenen Waren- und Dienstleistungen, sofern nichts Anderes vereinbart ist - etwa im Rahmen von Sonderbedingungen.
(2) Rechtlicher Anbieter der Angebote der EA und alleiniger Vertragspartner sämtlicher Leistungen ist die Brauner Klingenberg GmbH, vertreten durch den Geschäftsführer Christoph Brauner Leipziger Straße 9 in 10178 Berlin, eingetragen beim AG Charlottenburg, HRB 15132B.
(3) EA erbringt seine Leistungen ausschließlich gegenüber Unternehmern gemäß § 14 BGB, juristische Personen des öffentlichen Rechts sowie gegenüber öffentlich-rechtlichen Sondervermögen („Kunde“). Alleine diese werden Vertragspartner der EA. Die von den Kunden für die Veranstaltung benannten und angemeldeten Personen („Teilnehmer“) werden nicht Vertragspartner der EA. Das Angebot richtet sich nicht an Verbraucher.
(4) Diese Geschäftsbedingungen gelten ausschließlich; entgegenstehende oder von den Geschäftsbedingungen abweichende Bedingungen des Kunden erkennt EA nicht an, es sei denn, EA hat ihrer Geltung ausdrücklich schriftlich zugestimmt. Diese Bedingungen gelten auch dann, wenn EA in Kenntnis entgegenstehender oder von den Geschäftsbedingungen abweichende Bedingungen des Kunden die Leistung an diesen vorbehaltlos erbringt.

§ 2 Angebot - Anmeldung - Vertragsschluss
(1) Der Kunde kann sich per Buchungsformular über Internet, Post, Telefax oder E-Mail für Veranstaltungen anmelden. Die Buchung gilt als angenommen und es kommt der Vertrag rechtsverbindlich zustande, wenn EA die Anmeldung des Kunden ausdrücklich annimmt oder nicht binnen sieben Tagen nach Eingang des vollständig ausgefüllten und unterschriebenen Buchungsformulars eine schriftliche Ablehnung erklärt. Spätestens kommt der Vertrag aber mit Eingang des vollen Veranstaltungspreises für die Veranstaltung auf dem Konto der EA zustande. Zusätzlich erhält der Kunde in jedem Fall von der EA eine Buchungsbestätigung per E-Mail. Eine Teil-Buchung ist nur für als selbständig buchbar ausgeschriebene Veranstaltungsteile möglich.
(2) Anmeldungen werden grundsätzlich in der Reihenfolge ihres Eingangs berücksichtigt. Kann eine Anmeldung nicht berücksichtigt werden, so wird dies umgehend mitgeteilt.

§ 3 Leistung der EA
(1) Inhalt, Umfang, Dauer und sonstige Einzelheiten der Veranstaltung und der Leistung ergeben sich aus den von der EA veröffentlichten Publikationen oder Angaben auf der Internetseite zu den Veranstaltungen.
(2) Der Veranstaltungspreis versteht sich pro Person und Veranstaltungstermin. Er beinhaltet - soweit angekündigt - Veranstaltungsunterlagen, Mittagessen und Pausengetränke. Des Weiteren ist die Ausstellung eines Teilnahmezertifikates eingeschlossen. Eine Hotelunterbringung/Übernachtung/Anreise ist nicht geschuldet.

§ 4 Veranstaltungspreis und Entgelte - Zahlungsbedingungen - Aufrechnung
(1) Sofern nichts Anderes vereinbart ist, gilt der in den Publikationen zu den Veranstaltungen angegebene Veranstaltungspreis. Des Weiteren berechnet EA je nach Anfall Zusatzentgelte für Zusatzleistungen (bsw. Visainvitationhandling, Umschreibung von Rechnungen, Versand von Rechnungen per Post usw.) gemäß der auf der Internetseite der EA zum Zeitpunkt des Vertragsschlusses veröffentlichten Preisliste. Alle Preise verstehen sich zuzüglich der am Tage der Rechnungsstellung geltenden Umsatzsteuer.
(2) Der Kunde ist verpflichtet, den vereinbarten Veranstaltungspreis sowie etwaige Zusatzentgelte im Voraus, das heißt vor Beginn einer Veranstaltung zu bezahlen. Rechnungen sind sofort nach Zugang ohne jeden Abzug zur Zahlung fällig. Rechnungen werden elektronisch versandt. Der Kunde kommt spätestens sieben Tage nach Fälligkeit in Verzug. Kommt der Kunde in Zahlungsverzug, ist EA berechtigt, Verzugszinsen i.H.v. 8 % über dem Basiszinssatz der Europäischen Zentralbank p.a. zu fordern. Wenn EA einen höheren Verzugsschaden nachweist, kann dieser geltend gemacht werden.
(4) Ratenzahlungen werden nur ausnahmsweise und nur aufgrund besonderer schriftlicher Vereinbarung akzeptiert. Zahlungen erfolgen nur auf Rechnung oder durch bargeldlose Überweisung. Bar- oder Kreditkartenzahlungen werden nur nach vorheriger Vereinbarung mit der EA akzeptiert. Zahlungen durch Wechsel/Scheck werden nicht akzeptiert.
(5) Die Aufrechnung durch den Kunden ist nur möglich mit Ansprüchen, welche rechtskräftig festgestellt sind, von der EA anerkannt oder mit der Hauptforderung der EA synallagmatisch verknüpft sind.
(6) Die Abrechnung auf der Webseite via Kreditkarte erfolgt durch: HUELLEMANN & STRAUSS ONLINESERVICES S.à r.l.; 1, Place du Marché; L-6755 Grevenmacher; R.C.S. Luxembourg B 144133; E-Mail: info @ hso-services.com; Geschäftsführer: Ramona Spies Heiko Strauß. Dies gilt nicht für telefonisch ausgelöste Kreditkartenzahlungen.

§ 5 Rücktritt des Kunden - Stornierung
(1) Stornierungen müssen schriftlich oder in Textform erfolgen. Bei Stornierung der Teilnahme bis 30 Tage vor Veranstaltungsbeginn wird eine Bearbeitungsgebühr von 80,00€ zzgl. Umsatzsteuer sofort fällig. Der unter Verrechnung der Bearbeitungsgebühr verbleibende Veranstaltungspreis wird erstattet. Bei Stornierungen bis zwei Wochen vor Beginn der Veranstaltung werden 50% des Veranstaltungspreises und der Zusatzentgelte zzgl. Umsatzsteuer fällig. Bei Nichterscheinen oder Stornierung später als zwei Wochen vor dem Veranstaltungstermin wird der gesamte Veranstaltungspreis zzgl. der Umsatzsteuer fällig. Dem Kunden steht der Nachweis frei, dass der EA kein oder ein nierdrigerer Schaden entstanden ist. Gerne akzeptiert die EA ohne zusätzliche Kosten einen Ersatzteilnehmer statt des ursprünglich angemeldeten Teilnehmers, sofern dieser bis spätestens drei Tage vor Veranstaltungsbeginn gemeldet wird.
(2) Ein teilweiser/ tageweiser Rücktritt von einer Veranstaltung sowie die Meldung nur tageweiser Ersatzteilnehmer ist nicht möglich.
(3) Ist der Veranstaltungspreis einschließlich etwaiger Zusatzentgelte am Tag der Veranstaltung nicht bezahlt oder kann die Zahlung nicht eindeutig nachgewiesen werden, so kann der Teilnehmer von der Veranstaltung ausgeschlossen werden. Der Veranstaltungspreis ist dennoch sofort fällig und wird durch die EA gegebenenfalls im Mahnverfahren oder gerichtlich geltend gemacht.

§ 6 Rücktritt /Änderungen des Veranstalters/Ausschluss Teilnahme der Veranstaltung
(1) EA ist berechtigt, aus wichtigem Grund vom Vertrag zurückzutreten, ungeachtet sonstiger Gründe, insbesondere, wenn:
- für eine Veranstaltung nicht genügende Anmeldungen vorliegen;
- die Veranstaltung aus nicht von der EA zu vertretenden Umständen abgesagt werden muss (z.B. höhere Gewalt, Streik, wegen Verhinderung eines Referenten, wegen Störungen am Veranstaltungsort)

In den vorgenannten Fällen werden bereits bezahlte Teilnahmeentgelte vollständig zurückerstattet. Die Kunden werden durch die EA frühzeitig informiert. Die Absage wegen nicht genügender Anmeldungen erfolgt nicht später als zwei Wochen vor der Veranstaltung.
(2) Schadensersatzansprüche stehen den Teilnehmern in diesen Fällen nicht zu, es sei denn, solche Kosten entstehen aufgrund grob fahrlässigen oder vorsätzlichen Verhaltens seitens der EA oder deren Erfüllungsgehilfen. EA verpflichtet sich, bei eventuell auftretenden Leistungsstörungen alles Zumutbare zu unternehmen, um zu einer Behebung oder Begrenzung der Störung beizutragen. Sollten in bestimmten Fällen aus Kulanz dennoch Reisekosten erstattet werden, so stellt dies eine Ausnahme dar.
(3) Die EA behält sich vor, angekündigte Referenten durch andere zu ersetzen und notwendige Änderungen im Veranstaltungsprogramm oder Verlegung des Tagungsortes unter Wahrung des Gesamtcharakters der Veranstaltung bei Bedarf vorzunehmen.

§ 7 Urheberechte, Datenschutz und Listen
(1) Die im Rahmen der Veranstaltung ausgehändigten Unterlagen/Dokumente sind urheberrechtlich geschützt. Die Vervielfältigung, Weitergabe oder anderweitige kommerzielle Nutzung und/oder kommerzielle Verwertung der Unterlagen - auch auszugsweise - ist nur mit ausdrücklicher schriftlicher Zustimmung durch EA gestattet. Die Teilnehmer dürfen ohne ausdrückliche, schriftliche Einwilligung der EA auch keine sonstigen Lichtbild-, Ton- und/oder Videoaufzeichnungen der Veranstaltungen anfertigen. Die EA behält sich alle Rechte vor.
(2) Die Namen der Teilnehmer und Namen der Kunden, nebst Anschriften können von der EA über die Teilnehmerliste den anderen Veranstaltungsteilnehmern zugänglich gemacht und an das mit dem Postversand beauftragte Unternehmen zuzüglich der entsprechenden Adressdaten übermittelt werden. Kunden und oder Teilnehmer haben keinen Anspruch auf Herausgabe der Teilnehmerliste der besuchten Veranstaltung.
(3) Kunde und Teilnehmer sind mit der Aufnahme (Video, Foto, Audio u.s.w.) ihrer Person auf einer Veranstaltung einverstanden und willigen ein, dass diese Aufnahmen von der EA verwandt, verwertet und / oder veröffentlicht werden dürfen.
(4) Es gilt die auf der Internetseite der EA abrufbare Datenschutzerklärung. Im Übrigen gelten die gesetzlichen Regelungen.

§ 8 Haftung
(1) Die Veranstaltungen werden von qualifizierten Referenten sorgfältig vorbereitet und durchgeführt. Die EA übernimmt keine Haftung für die Aktualität, Richtigkeit und Vollständigkeit in Bezug auf die Tagungsunterlagen und die Durchführung der Veranstaltung und/oder sonstige Inhalte der Veranstaltungen, sofern kein vorsätzliches oder grob fahrlässiges Verschulden der EA oder eines Erfüllungsgehilfen besteht.
(2) Unsere Haftung für vertragliche Pflichtverletzungen sowie aus Delikt ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Dies gilt nicht bei Verletzung von Leben, Körper und Gesundheit des Teilnehmers, Ansprüchen wegen der Verletzung von Kardinalpflichten, d.h. von Pflichten, die sich aus der Natur des Vertrages ergeben und bei deren Verletzung die Erreichung des Vertragszwecks gefährdet ist, sowie dem Ersatz von Verzugsschäden (§ 286 BGB). Insoweit haften die EA für jeden Grad des Verschuldens. Soweit es um Schäden geht, die nicht aus der Verletzung von Leben, Körper und Gesundheit des Kunden resultieren, haftet die EA aber nur für den typischerweise entstehenden Schaden.

§ 9 Erfüllungsort - Rechtswahl - Gerichtsstand - Sonstiges
(1) Soweit sich aus dem Vertrag nichts Anderes ergibt, ist Zahlungsort der Geschäftssitz der EA in Berlin. Erfüllungsort ist Berlin.
(2) Für diesen Vertrag gilt das Recht der Bundesrepublik Deutschland. Die Anwendung des UN-Kaufrechts wird ausgeschlossen.
(3) Ausschließlicher Gerichtsstand ist bei Verträgen mit Kaufleuten, juristischen Personen des öffentlichen Rechts oder öffentlich-rechtlichen Sondervermögen das für unseren Geschäftssitz zuständige Gericht. EA ist auch berechtigt, den Kunden an seinem allgemeinen Gerichtsstand zu verklagen.
(4) Rechtserhebliche Erklärungen und Anzeigen, die der Kunde gegenüber der EA oder einem Dritten abzugeben hat, bedürfen der Text- oder Schriftform, sofern in diesen AGB nicht abweichend geregelt.

Stand: Juli 2016