

# Compliance

Februar 2019

Die Zeitschrift für Compliance-Verantwortliche

## Inhalt



### Aufmacher

**„Wir begeben uns in eine Situation wie vor zehn bis zwölf Jahren“**  
Was waren die größten Herausforderungen für Compliance-Verantwortliche im vergangenen Jahr? Worauf müssen sie sich 2019 einstellen? Und bei welchen Themen besteht Nachholbedarf? Das wollten wir von unserem Beiratsmitglied Dr. Katharina Hastenrath wissen.

### Veranstaltung

### Praxis

### News



#### Roundtable Cybercrime

Die zunehmende Digitalisierung bringt viele Vereinfachungen, schafft aber auch neue Einfallstore für Betrüger. Das bekommen jährlich fast 80 Prozent aller deutschen Unternehmen zu spüren. Ein guter Grund für die intensive Diskussion beim Roundtable Cybercrime in den Räumlichkeiten der BEITEN BURKHARDT Rechtsanwältegesellschaft mbH in Frankfurt am Main.

#### Datensicherheit: Doxing betrifft auch Unternehmen

Über Twitter veröffentlichte private Informationen von Prominenten und Politikern rückten Anfang Januar das sogenannte Doxing in den Fokus der Öffentlichkeit. Das Vorgehen ist unter anderem in der Gamer-Szene bereits seit längerem bekannt.

#### 6 Korruptionswahrnehmungsindex 2018

#### Entwurf zu Ethikleitlinien für künstliche Intelligenz

#### 9 Höhere Hürden für Firmenübernahmen

#### 9 Bericht der EU-Kommission zum EU-US-Datenschutzschild

**ANGEBOT  
COMPLIANCE-BERATER: TESTLESEN PRINT**

**Leistungen  
3 Monate gratis  
+ Zugang zur Online-Datenbank**

### Veranstaltungen

21.-22.02.2019 | Berlin | **Steuerkonferenz der deutschen Wirtschaft 2019**

25.02.2019 | Hamburg | **SoCompliance**

01.03.2019 | Winterthur | **3. DACH-Compliance-Tagung**

05.06.2019 | München | **Food Compliance**

06.06.2019 | Frankfurt a.M. | **Deutsche Compliance Konferenz**

# „Wir begeben uns in eine Situation wie vor zehn bis zwölf Jahren“

Was waren die größten Herausforderungen für Compliance-Verantwortliche im vergangenen Jahr? Worauf müssen sie sich 2019 einstellen? Und bei welchen Themen besteht Nachholbedarf? Das wollten wir von unserem Beiratsmitglied Dr. Katharina Hastenrath wissen.



Multitasking: Compliance-Verantwortlichen fehlt oft eine saubere Abgrenzung zu anderen Verantwortungsbereichen.

Geldwäsche, Whistleblowing, Geschäftsgeheimnisse, der Compliance-Faktor Mensch, aber auch immer wieder Themen aus dem weiten Spektrum Informationstechnik beherrschten die Schlagzeilen der Compliance-Welt im Jahr 2018. Im neuen Jahr hat sich daran nicht viel geändert. Die Liste dessen, womit sich Compliance im Jahr 2018 befasst hat und voraussichtlich auch weiterhin im Jahr 2019 befassen wird, scheint schier unerschöpflich. Denn am Ende ist alles irgendwie Compliance-relevant. Das verwundert kaum, wenn man sich auf die ursprüngliche Bedeutung von Compliance zurückbesinnt: Regeltreue. Und diese Regeltreue verlangen und wünschen wir uns natürlich in al-

len Bereichen. Aber ist es effektiv, wenn Compliance-Verantwortliche sich alle Problemfelder zu eigen machen?

Dr. Katharina Hastenrath sieht gerade in diesem umfänglichen Ansatz ein Hauptproblem der Compliance: „Oft fehlt eine klare Risikofokussierung und die saubere Abgrenzung zu internen Kontrollsystemen (IKS), Risikomanagement, Revision und Qualitätsmanagement. Hier müssten sich die Compliance-Verantwortlichen noch einmal ganz klar sortieren können – auch bezüglich der genannten Schnittstellen.“ Dazu gehört auch eine genaue Prüfung wo datenschutzrechtliche Belange hineinspielen und inwiefern sich die

Compliance-Verantwortlichen mit IT-Sicherheit befassen müssen, sagt Hastenrath.

Sicherlich haben die meisten Compliance-Verantwortlichen gerade im Jahr 2018 einen Großteil ihrer Arbeitskraft auf genau diese IT-affinen Themen verwendet. Eine treibende Kraft dafür war und ist die EU-Datenschutzgrundverordnung (DSGVO). Hinzu kommen Cyberangriffe, denen im besten Fall vorgebeugt wird und die im schlechtesten Fall aufgearbeitet werden müssen. Das alles könne Compliance leisten, aber nur, wenn sie auch früh genug mit in die gesamte Unterneh-

mensstrategie aufgenommen wird und einen entsprechenden Stellenwert im Unternehmen hat, warnt Hastenrath. „Gerade im vergangenen Jahr konnte ich beobachten, dass die Themen weiter zunehmen, das Budget der Compliance-Verantwortlichen aber gleichzeitig nicht steigt oder sogar abnimmt. Wir begeben uns damit in eine Situation, in der wir uns nicht mehr richtig auf die Hauptrisiken fokussieren können. So war es auch ganz zu Anfang, als das Thema Compliance vor zehn bis zwölf Jahren an Fahrt aufnahm“.

Auch die fehlende Wertschätzung von Compliance im Unternehmen, „Compliance als Business-Verhinderer“, ist einer der größten Hemmschuhe bei der effektiven Weiterentwicklung des Themas. Dazu passt auch, dass viele Compliance-Verantwortliche beklagen, in der Führungsetage nur wenig Gehör zu finden. Hastenrath sieht aber nicht nur innerhalb der Unternehmen Nachholbedarf: „Auf internationalem Level müssten Compliance-Management-Systeme durchgehend zumindest in der Strafzumessung honoriert werden. Das ist in vielen Bereichen, wie zum Beispiel auch beim deutschen Bundeskartellamt, bisher kaum der Fall“, spricht sie ein weiteres Problem für Compliance-Verantwortliche an. Unternehmensleitungen wollen messbare Ergebnisse für ihre Investitionen sehen. Die Vorteile aus der Implementierung eines Compliance-Management-Systems wären für sie eher nachvollziehbar und messbar, wenn eine solche Honorierung durchgehend greifen würde. Dabei sollte aber auch allen Beteiligten bewusst sein, was überhaupt im Rahmen eines effektiven CMS möglich und machbar ist. Für Hastenrath



Dr. Katharina Hastenrath

Dr. Katharina Hastenrath berät zu (strategischen) Compliance-Fragen und ist u.a. Dozentin für Compliance an der ZHAW und der BECK AKADemie; zuvor war sie (C)CO bei mehreren, internationalen Unternehmen.

wäre eine engere Zusammenarbeit zwischen Gesetzgebung, Unternehmen und Gerichten ein erster Schritt für mehr gegenseitiges Verständnis.

chk



School of  
Management and Law

## Win-Win durch Compliance

Von Bußgeld-Reduktionen und anderen Vorteilen eines Compliance-Management-Systems – erfahren Sie das Neueste von Behörden, Verbänden und Unternehmen.

DACH-Compliance-Tagung 2019  
1. März 2019, Winterthur/Zürich (Schweiz)



**Building Competence. Crossing Borders.**

## Roundtable Cybercrime

Die zunehmende Digitalisierung bringt viele Vereinfachungen, schafft aber auch neue Einfallstore für Betrüger. Das bekommen jährlich fast 80 Prozent aller deutschen Unternehmen zu spüren. Ein guter Grund für die intensive Diskussion mit Jörg Bielefeld, Partner, BEITEN BURKHARDT Rechtsanwalts-gesellschaft mbH, Peter Danil, Bundesamt für Sicherheit in der Informationstechnik (BSI), und Peter Zawilla, Geschäftsführer, FMS Fraud & Compliance Management Services GmbH, beim Roundtable Cybercrime in den Räumlichkeiten der BEITEN BURKHARDT Rechtsanwalts-gesellschaft mbH am 22. Oktober 2018 in Frankfurt am Main.



Jörg Bielefeld, Peter Danil und Peter Zawilla (v.l.n.r.)

Peter Danil stellte zunächst den **Bericht zur Lage der IT-Sicherheit 2018** des BSI vor. „Ich möchte Ihnen auf keinen Fall Angst machen“, stieg er angesichts der eher besorgniserregenden Zahlen des Berichts in seinen Vortrag ein und appellierte an die Roundtable-Teilnehmer, „die enormen Chancen der Digitalisierung“ zu sehen. Bis zu neun internetfähige Geräte werde es pro Person in Deutschland in naher Zukunft geben. „Für die Wirtschaft ergeben sich daraus gewaltige Wertschöpfungspotentiale“, sagte Danil. Doch den „sichtbaren Chancen“ stünden eben auch „unsichtbare Bedrohungen“ entgegen: „Statistisch gesehen werden Sie zu 70 bis 80 Prozent in nächster Zeit Opfer eines Cyberangriffs“, sagte Danil und ergänzte: „Wer bisher noch nicht Opfer eines Cyberangriffs war, hat es möglicherweise nur noch nicht bemerkt.“ Durchschnittlich brauche es 243 Tage, um festzustellen, dass man angegriffen wurde. Das ist viel Zeit, in der die Täter z. B. Daten absaugen können. Die Dimension der Cyberkriminalität spiegelt sich auch in den täglich im Durchschnitt rund 390.000 neuen Schadprogrammen wider. Die Bedrohung durch diese sog. Malware

(Trojaner, Viren) wird inzwischen durch einen weiteren Schwachpunkt erhöht: Die Hardware. „Das ist neu“, erklärte Danil. Wie bedeutend die Rolle der Hardware ist, haben jüngst die Prozessorschwachstellen Spectre und Meltdown gezeigt: Diese Sicherheitslücken erlauben es Angreifern, sensible Speicherbereiche des Computers auszulesen. Das Haupteinfallstor sind dennoch nach wie vor E-Mails, über deren Anhänge 80 Prozent aller Angriffe beginnen. „Das ist eine enorme Zahl mit Blick auf den Faktor Mensch, der damit sehr zentral und entscheidend für Ihren Präventionserfolg ist“, verdeutlichte Danil.

Aber nicht nur die Schutzmaßnahmen seien entscheidend, um gegen Cyberangriffe bzw. deren Auswirkungen gewappnet zu sein: „Wir können von Virenschannern keinen 100prozentigen Schutz erwarten. Darum sollten wir keinesfalls Back-up-Lösungen vergessen, die bei der Schadensbegrenzung helfen, indem sie Daten sichern, die für die betrieblichen Abläufe notwendig sind. Zawilla riet darüber hinaus dazu, für den Schadenfall auch eine Art Handlungsanweisung bereit zu halten. „Überlegen Sie sich schon präventiv, an

### Allianz für Cyber-Sicherheit

Über die **Allianz für Cyber-Sicherheit** bietet das BSI der Wirtschaft eine kostenlose Plattform für den Austausch von Informationen und Erfahrungen rund um das Thema Informationssicherheit. Die Initiative zählt derzeit 3.000 teilnehmende Unternehmen.

### Faktor Mensch

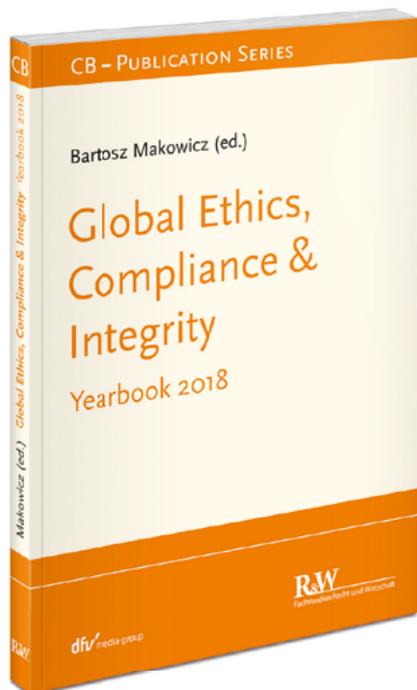
Oft ist nicht die Frage nach dem höchsten Sicherheitsstandard entscheidend, sondern das Augenmerk auf den Menschen. Hier sind meist die einfachsten Dinge wirksam:

- Bei ungewöhnlichen E-Mail-Anfragen stutzig werden und sich rückversichern, wer dahinter steckt: Chief or Thief?
- Keine gefundenen USB-Sticks in den Rechner stecken. Es gibt „Datenschleusen“, durch die man solche USB-Sticks vorher laufen lassen kann.
- Sicherheits-Updates nicht verschieben. Täter werden die Lücke nutzen, sobald sie bekannt ist.
- Dem Passwort-Klau/Phishing über gefälschte Webseiten-Oberflächen vorbeugen.

wen Sie sich wenden, falls Sie zum Opfer eines Cyberangriffs werden. Bauen Sie sich schon vorher ein gutes Netzwerk auf, um den Schaden dann so gering wie möglich zu halten.“ Außerdem sollte dem Thema Cybersicherheit erst noch eine Risikoanalyse vorgeschaltet werden: „Welches Cyberisiko habe ich überhaupt? Wo sind die Schwachstellen in meinem Unternehmen.“ Peter Zawilla verwies darauf, dass zielgerichtete und wirksame Präventionsmaßnahmen nur dann implementiert werden können, wenn zuvor die konkrete unternehmensspezifische Risikosituation erhoben worden und transparent ist. Eine derartige Analyse sei zwar aufwendig, aber lohnend.

Danil appellierte an die Anwesenden: „Cybersicherheit ist Chefsache!“ Es helfe nicht, wenn zwar einige Mitarbeiter im Unternehmen das Thema durchdringen, der Chef aber die notwendigen organisatorischen oder technischen Maßnahmen nicht unterstützt. Jörg Bielefeld riet dazu, die Thematik aus Geschäftsleitersicht zu betrachten. Denn die Verantwortlichen in den Unternehmen müssten sich heutzutage durchaus fragen lassen, ob sie bestimmte Angriffe – etwa auch durch CEO-Fraud – nicht hätten kommen sehen und verhindern können. „Sie müssen Ihrem Chef verdeutlichen, dass Prävention ihn enthaften kann. Dann ist er mit Sicherheit auch eher dazu bereit, Geld für Cybersicherheit auszugeben.“ *chk*

# Compliance-Herausforderungen von Morgen



## Inhalt

- Umfassender, aktueller und kompetenter Überblick über weltweites Know-how und Tendenzen in der Entwicklung von Ethik, Compliance und Integrität in diversen Organisationsarten auf nationaler und globaler Ebene
- Schwerpunkte des Jahrbuchs 2018:
  - grenz- und kulturüberschreitendes Compliance Management
  - Korruptionsbekämpfung, Standardisierung sowie Kommunikation, Whistleblowing und interne Ermittlungen
  - International Trade Compliance
  - Compliance-Herausforderungen der Zukunft
- Über 40 Einzelbeiträge von Fachexperten für Compliance aus diversen Staaten und internationalen Organisationen (u. a. OECD, Weltbank, G20)
- Das Werk erscheint vollständig in englischer Sprache

## Herausgeber

Prof. Dr. **Bartosz Makowicz** arbeitet an der Juristischen Fakultät der Europa-Universität Viadrina Frankfurt (Oder) und ist Direktor des dort interdisziplinär tätigen Viadrina Compliance Center. Er ist Mitglied im wissenschaftlichen Beirat des Deutschen Instituts für Compliance e.V. (DICO) sowie im Beirat von Transparency International Deutschland und Initiator der internationalen Gesellschaft „Global Community for Ethics, Compliance & Integrity“.

**Ja, ich bestelle – auf [www.shop.ruw.de](http://www.shop.ruw.de) oder per Fax unter **08581 754****

\_\_\_\_ Expl. **Global Ethics, Compliance & Integrity**  
Yearbook 2018  
2019, 288 Seiten, Kt., ISBN: 978-3-8005-0009-3  
€ 69,-

\_\_\_\_\_  
Name | Firma | Kanzlei

\_\_\_\_\_  
E-Mail

\_\_\_\_\_  
Straße | Postfach

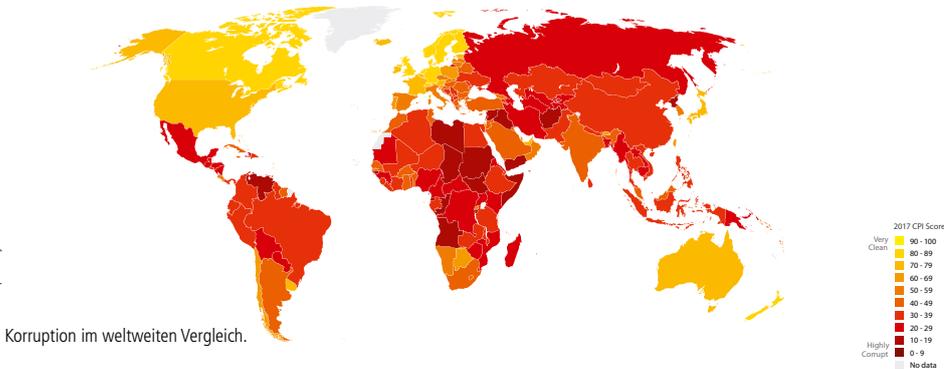
\_\_\_\_\_  
PLZ | Ort

\_\_\_\_\_  
Datum | Unterschrift

# Korruptionswahrnehmungsindex 2018

Die Antikorruptionsorganisation Transparency International hat Ende Januar den Korruptionswahrnehmungsindex (Corruption Perceptions Index, CPI) veröffentlicht. Deutschland verschlechtert sich in der Wahrnehmung von Führungskräften in der Wirtschaft.

Transparency International



Korruption im weltweiten Vergleich.

Deutschland erreicht 80 Punkte – ein Punkt weniger als im Vorjahr. Dennoch rückt Deutschland im Ranking einen Platz nach vorne und teilt sich nun mit Großbritannien, das zwei Punkte verliert, den 11. Rang. Während die meisten für Deutschland relevanten Indizes unverändert bleiben, gibt es bei einem Index eine deutliche Verschlechterung: Der World Economic Forum Executive Opinion Survey (EOS), der jährlich Führungskräfte

aus der Wirtschaft befragt, sinkt von 74 auf 66 Punkte (von 100) – aus Sicht der Wirtschaftschefs nimmt Korruption und Bestechung in Wirtschaft und öffentlichen Institutionen in Deutschland zu. Dr. Edda Müller, Vorsitzende von Transparency Deutschland, nimmt dies zum Anlass, nochmals die zügige Umsetzung der im Koalitionsvertrag bereits vorgesehenen strafrechtlichen Sanktionierung von Unternehmen zu fordern. Zur Korrupti-

onsbekämpfung gehöre darüber hinaus „eine lebendige Zivilgesellschaft und unabhängige Medien als wichtige Kontrollinstanzen, die ohne Angst und Einschränkungen zur Widerstandskraft von pluralistischen Demokratien beitragen“. Dafür brauche es auch die Möglichkeit, Unrechtmäßigkeiten melden zu können. Für Deutschland fordert Müller daher „endlich einen starken, gesetzlichen Hinweisgeberschutz“.

chk

Das tabellarische Ranking, die verwendeten Quellen, Informationen zur Methodik und Antworten auf häufig gestellte Fragen finden Sie [hier](#)

## CPI

Der CPI ist der weltweit bekannteste Korruptionsindex und misst die in Politik, Verwaltung und Wirtschaft wahrgenommene Korruption. Der Index fasst 13 Einzelindizes von 12 unabhängigen Institutionen zusammen, deren Daten auf Expertinnen- und Experteninterviews, Umfragen und weiteren Untersuchungen beruhen. Der CPI ordnet die untersuchten Länder auf einer Skala von 0 (hohes Maß an wahrgenommener Korruption) bis 100 (keine wahrgenommene Korruption) ein. In diesem Jahr wurden 180 Länder und Gebiete aufgenommen.

## Soziale Netzwerke & DSGVO

Neuerscheinung



### Inhalt

- Analyse der Handlungen von Netzwerkbetreibern, Fansite-Betreibern und Nutzern in sozialen Netzwerken und Darstellung der Voraussetzungen sowie datenschutzkonformer und praxistauglicher Möglichkeiten der Datenverarbeitung unter der DSGVO
- Schwerpunkte: Anwendbarkeit der DSGVO, Umfang der Verantwortlichkeit der Akteure und Rechtmäßigkeit der Verarbeitung
- Betrachtung der Besonderheiten sowie Neuheiten der DSGVO und deren spezifische Relevanz für soziale Netzwerke

### Der Autor

Dr. **Alexander Golland** ist zertifizierter Datenschutzbeauftragter sowie Autor zahlreicher Fachveröffentlichungen. Er forscht insbesondere zu datenschutzrechtlichen Grundsatzfragen neuer Technologien.

### Meine Bestellung

#### Expl. Datenverarbeitung in sozialen Netzwerken

2019, 396 Seiten, Kt.,  
ISBN: 978-3-8005-1682-7  
€ 124,-



### Weitere Informationen:

Name | Firma | Kanzlei

E-Mail

Straße | Postfach

PLZ | Ort

Datum | Unterschrift

### Bestellservice

www.shop.ruw.de | info@suedost-service.de  
Tel 08581 9605-0 | Fax 08581 754

# Datensicherheit: Doxing betrifft auch Unternehmen

Über Twitter veröffentlichte private Informationen von Prominenten und Politikern rückten Anfang Januar das sogenannte Doxing in den Fokus der Öffentlichkeit. Das Vorgehen ist unter anderem in der Gamer-Szene bereits seit längerem bekannt. Gemeint ist damit das Veröffentlichen privater Informationen Dritter im Netz, um diese bloßzustellen. Unternehmen sind damit einmal mehr in der Pflicht, ihre IT-Systeme zu schützen.

Die bereits im Dezember bekannt gewordenen Daten enthielten öffentlich zugängliche Informationen, wie berufliche E-Mail-Adressen und Telefonnummern, die wohl über einen längeren Zeitraum zusammengetragen wurden. Daneben wurden aber auch passwortgeschützte oder private Inhalte wie Chatprotokolle, Familienfotos oder private Adressen und Telefonnummern publik.

Wie genau der kurz nach Bekanntwerden des Angriffs vorläufig verhaftete 20-jährige mutmaßliche Täter an die geschützten Daten gelangen konnte, ist noch unklar. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erklärte in einer Meldung kurz nach Beginn der Ermittlungen, dass die Passwörter gestohlen oder erraten worden seien. Seitdem hält es sich aber mit Informationen zurück. Auch ob der mutmaßliche Täter tatsächlich alleine handelte oder doch – mangels eigenem technischem Sachverstand – Mittäter hatte, ist nach wie vor unklar.

Das das Verwenden von Standard-Passwörtern wie zum Beispiel „Passwort“ oder „123456“ eine Gefahr für die Datensicherheit darstellt, dürfte sich inzwischen herumgesprochen haben. Wie jedoch ein kürzlich bekannt gewordener Vorfall zeigt, machen Hacker auch vor Zugangsgeschützten Systemen nicht Halt. Konkret wurden nach Auskunft des BSI circa 773 Millionen E-Mail-Adressen und 21 Millionen Passwörter im Klartext im Internet veröffentlicht. Deutlich wird dadurch auch, dass sich Angreifer wie der mutmaßliche Täter der Doxing-Attacke die technischen Fähigkeiten Dritter zunutze machen können, indem sie auf Zugangsdaten zurückgreifen, die von anderen im Internet oder im Darknet veröffentlicht werden.

Einmal mehr dürften die Vorfälle Internet-Nutzern vor Augen führen, dass die Veröffentlichung privater Daten im Internet zu unerwünschten Spätfolgen führen kann. Aber auch die Bedeutung von IT-Sicherheit ist wieder in den Fokus der Öffentlichkeit gerückt. Ulrich Kelber, der neue Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, sieht die Unternehmen in der Pflicht, „überhaupt die Chance einer sicheren



Datensicherheit: Die aktuellen Doxing-Fälle nehmen Unternehmen einmal mehr in die Pflicht, ihre IT-Systeme zu schützen.

Nutzung ihrer Dienste zu ermöglichen“. Dass neben den Internetnutzern selbst auch und gerade Unternehmen die Pflicht haben, IT-Systeme sowie darin enthaltene personenbezogene Daten zu schützen, ist allerdings kein Novum.

Das 2015 in Kraft getretene IT-Sicherheitsgesetz nimmt neben den Betreibern kritischer Infrastrukturen, wie Unternehmen der Energie-, Wasser- und Gesundheitsversorgung auch Betreiber von Webangeboten, Apps und Telekommunikationsunternehmen in die Pflicht. Die betroffenen Unternehmen müssen einen Mindeststandard an IT-Sicherheit einhalten, der dem Stand der Technik entsprechen muss. Kritische Infrastrukturen und Telekommunikationsunternehmen müssen bestimmte Störungen zudem dem BSI melden.

Bereits im ersten Halbjahr 2019 soll das IT-Sicherheitsgesetz 2.0 folgen, das unter anderem den Aspekt der Zertifizierung noch stärker in den Fokus rücken soll.

Aber auch Unternehmen, die nicht in den Anwendungsbereich des IT-Sicherheitsgesetzes fallen, haben nach der im Mai letzten Jahres in Kraft getretenen Datenschutzgrundverordnung (DSGVO) die Pflicht zur Umsetzung technischer und organisatorischer Maßnahmen, die für Datenverarbeitungen „ein dem Risiko angemessenes Schutzniveau“ gewährleisten müssen. Auch hierbei ist der aktuelle Stand der Technik zu beachten. Eine Meldepflicht bei Datenschutzverlet-

zungen existiert ebenfalls bereits. Wenn nicht der drohende Vertrauens- und Rufverlust, so dürften doch jedenfalls die drohenden Strafen bei einem Verstoß gegen genannte Pflichten der DSGVO, die Geldbußen von bis zu 10 Millionen Euro oder bis zu zwei Prozent des weltweit erzielten Jahresumsatzes betragen können, Unternehmen zur Einhaltung entsprechender Vorgaben veranlassen.

Der Ruf nach strengeren Vorgaben für Unternehmen, der im Zusammenhang mit Vorkommnissen wie dem Vorliegenden beinahe reflexartig laut wird, ist somit letztlich unangebracht. Vielmehr sollten Unternehmen dazu angehalten werden, die bereits bestehenden Vorgaben einzuhalten.

Daneben aber müssen sich Nutzer darüber im Klaren sein, dass es gänzliche Sicherheit wohl nie geben wird. Gene Spafford, einer der führenden IT-Sicherheitsexperten der USA, schrieb bereits 1989: „Das einzig sichere System müsste ausgeschaltet, in einem versiegelten und von Stahlbeton ummantelten Raum und von bewaffneten Schutztruppen umstellt sein – und selbst dann hätte ich meine Zweifel.“ Dieser Satz behält in der heutigen Zeit des rasanten technischen Fortschritts uneingeschränkt Geltung.

Lisa Hondl



Lisa Hondl ist Anwältin bei der internationalen Wirtschaftskanzlei CMS. Ihre Schwerpunkte sind das Datenschutzrecht, insbesondere die Umsetzung der Datenschutzgrundverordnung im Unternehmen und die Direktwerbung unter Aspekten des Wettbewerbsrechts (UWG).

## IMPRESSUM

**Verlag**  
Deutscher Fachverlag GmbH, Mainzer Landstraße 251,  
60326 Frankfurt am Main  
Registergericht AG Frankfurt am Main HRB 8501  
UStIdNr. DE 114139662

**Geschäftsführung:** Angela Wisken (Sprecherin), Peter Esser, Markus Gotta, Peter Kley, Holger Knapp, Sönke Reimers

**Aufsichtsrat:** Klaus Kottmeier, Andreas Lorch, Catrin Lorch, Peter Ruß  
**Redaktion:** Christina Kahlen-Pappas (verantwortlich),  
Telefon: 069 7595-1153, E-Mail: christina.kahlen-pappas@dfv.de

**Verlagsleitung:** RA Torsten Kutschke,  
Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de

**Anzeigen:** Lena Moneck, Telefon: 069 7595-2713, E-Mail: lena.moneck@dfv.de

### Mitherausgeber:

BEITEN BURKHARDT Rechtsanwaltskanzlei mbH  
**Fachbeirat:** Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, thyssenkrupp Steel Europe AG; Ralf Brandt, divient patch Beteiligungs GmbH; Otto Geiß, Fraport AG; Mirko Haase, Hilti Corporation; Dr. Katharina Hastenrath, Frankfurt School of Finance & Management; Olaf Kirchhoff, Schenker AG; Torsten Krumbach, Bosch Sicherheitssysteme GmbH; Dr. Karsten Leffriang, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Corpus Sireo Holding GmbH; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, BSH Hausgeräte GmbH; Jörg Siegmund, Getzner Textil AG; Elena Späth, AXA Assistance Deutschland GmbH; Dr. Martin Walter, selbstständiger Autor, Berater und Referent für Compliance- Themen; Heiko Wendel, Rolls-Royce Power Systems AG; Dietmar Will, Audi AG.

**Jahresabonnement:** kostenlos

**Erscheinungsweise:** monatlich (10 Ausgaben pro Jahr)

**Layout:** Uta Struhalla-Kautz, SK-Grafik.de

Jede Verwertung innerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Keine Haftung für unverlangt eingesandte Manuskripte. Mit der Annahme zur Alleinveröffentlichung erwirbt der Verlag alle Rechte, einschließlich der Befugnis zur Einspeicherung in eine Datenbank.

Gemäß § 5 Abs. 2 ff. des Hessischen Gesetzes über Freiheit und Recht der Presse wird mitgeteilt: Gesellschafter der Deutscher Fachverlag GmbH sind Herr Andreas Lorch, Heidelberg (42,1908%); Frau Catrin Lorch, Königswinter (10,9385%); Frau Annette Lorch, Büdingen (10,9367%); Frau Britta Lorch, Berlin (10,9367%) sowie die Deutscher Fachverlag GmbH, Frankfurt am Main (25%).

## 6. Praxis-Dialog Internationales Steuerrecht

# Tax goes Future

## Digitalisierung und Verschärfung des Steuerwettbewerbs der Länder

9. und 10. Mai 2019,  
Deutscher Fachverlag,  
Frankfurt am Main

**Brennpunkthemen 2019**

Die mit der Digitalisierung einhergehende Umstellung auf digitale Geschäftsmodelle, der verschärfte Steuerwettbewerb, als auch die Maßnahmen des Anti-BEPS-Projekts führen dazu, dass die Agenda der Steuerverantwortlichen in den Unternehmen immer umfangreicher wird. So liegen z.B. auf Ebene der OECD und der EU Vorschläge zur Besteuerung digitaler Geschäftsmodelle vor, die Ansatzpunkte für eine Abgrenzung der nationalen Besteuerungsrechte enthalten. Wir geben Ihnen einen umfangreichen Überblick über die aktuellen Handlungsfelder für Steuerpraktiker.

Freuen Sie sich auf hochkarätige Praxisexperten aus namhaften Unternehmen sowie aus Wissenschaft und Verwaltung. Sie vermitteln die wichtigsten Details und präsentieren in bewährter Manier Lösungen für neuartige Fragestellungen.

Hier ein Überblick über unsere Schwerpunkthemen:

- **Impulsvortrag: Komplexität internationaler Steuersysteme**
- **Auswirkungen von Digitalisierung und Industrie 4.0 auf konzerninterne Wertschöpfungsketten und zugrundeliegende Verrechnungspreissysteme**
- **Anzeige und Meldepflichten steuerrelevanter Sachverhalte im Dialog mit der Finanzverwaltung**
- **Digitale Geschäftsmodelle am Beispiel einer Handelsplattform und deren umsatzsteuerliche Behandlung**
- **Vielfältige Quellensteuerfragen an Hand eines international agierenden Mobilitätsunternehmens**
- **Digitalisierung der Steuerabteilung: Bedeutung, Handlungsfelder und praktische Lösungsansätze insbesondere für international agierende Unternehmen**

**Veranstalter:**

**Warth & Klein  
Grant Thornton**

An instinct for growth™

**Veranstaltungsort**

Deutscher Fachverlag GmbH  
Mainzer Landstraße 251 | 60326 Frankfurt am Main

**Kontakt**

Torsten Kutschke  
Deutscher Fachverlag GmbH | Mainzer Landstraße 251,  
60326 Frankfurt am Main | Telefon: 069 7595-1151  
E-Mail: torsten.kutschke@dfv.de

**Anmeldeschluss**

Eine frühzeitige Anmeldung wird empfohlen,  
Anmeldeschluss ist der 3. Mai 2019.

**Stornierung**

Die Anmeldung ist übertragbar. Bei Stornierung bis zum 25. April 2019 (Eingangsdatum) wird eine Bearbeitungsgebühr von 50,00 Euro zzgl. MwSt erhoben. Danach ist die volle Teilnahmegebühr zu entrichten.

**Teilnahmegebühr Abonnenten EWS/RIW/BB:**

369,00 EUR (zzgl. MwSt.)

**Teilnahmegebühr Normalpreis:**

449,00 EUR (zzgl. MwSt.)

**Rabatte:**

**Frühbucherrabatt** 5 % bis Buchung zum 1. Februar 2019.

**Mehrbucherrabatt** 5 % bei Anmeldung von 3 oder mehr Teilnehmern einer Kanzlei/einer Institution/einer Behörde/einer Kammer ab dem 3. Teilnehmer (unabhängig vom Frühbucherrabatt).

**Vorabendempfang am 9. Mai 2019****Sie haben EWS, RIW oder den BB noch nicht im Abo?**

- Ja, ich möchte die „EWS – Europäisches Wirtschafts- und Steuerrecht“ abonnieren.**

Bitte liefern Sie die zweimonatlich erscheinende EWS zum Jahresbezugspreis Inland: 608,99 EUR (inkl. Vertriebskosten und MwSt.).

- Ja, ich möchte die „RIW – Recht der internationalen Wirtschaft“ abonnieren.**

Bitte liefern Sie den monatlich erscheinende RIW zum Jahresbezugspreis Inland: 799,00 EUR (inkl. Vertriebskosten und MwSt.).

- Ja, ich möchte den „Betriebs-Berater“ abonnieren.**

Bitte liefern Sie den wöchentlich erscheinenden BB zum Jahresbezugspreis Inland: 699,00 EUR (inkl. Vertriebskosten und MwSt.).

**zurück per Fax: 069 7595 1150**

Name/Vorname

Kanzlei/Firma

Ich nehme am Vorabendempfang teil

Straße

PLZ/Ort

Abo-/Kundennummer

Telefon

E-Mail

Datum/Unterschrift

**Weitere Informationen zum Programm finden Sie unter [www.wkgt-praxisdialog.de](http://www.wkgt-praxisdialog.de)**

Veranstalter:



**Warth & Klein  
Grant Thornton**  
An instinct for growth™

In Zusammenarbeit mit:



# Entwurf zu Ethikleitlinien für künstliche Intelligenz

Die von der EU-Kommission im Juni eingesetzte Expertengruppe für Künstliche Intelligenz (KI) hat am 18. Dezember 2018 den ersten Entwurf ihrer **Ethikleitlinien** veröffentlicht, auf deren Grundlage KI entwickelt und eingesetzt werden soll. Darin legen die 52 Experten aus Wissenschaft, Wirtschaft und Zivilgesellschaft dar, wie Entwickler und Nutzer sicherstellen können, dass die KI die Grundrechte, die geltenden Vorschriften und Grundprinzipien respektiert. Bis zum 18. Januar 2019 konnten dazu Kommentare eingesendet werden. Im März 2019 wird die Sachverständigenkommission ihre endgültigen Leitlinien vorlegen.



Brian Jackson/Stock/Thinkstock

Künstliche Intelligenz: Sie macht mehr möglich, als ethisch vertretbar ist.

# Höhere Hürden für Firmenübernahmen



Rainald/Stock/Thinkstock

Ausländische Investoren: Die Bundesregierung will sie künftig genauer unter die Lupe nehmen.

Wenn deutsche Unternehmen durch ausländische Investoren übernommen werden sollen, wird das künftig strenger geprüft. So soll die Bundesregierung frühzeitig mitentscheiden können, ob legitime Sicherheitsinteressen Deutschlands betroffen sind. Das Kabinett hat dazu eine Änderung der Außenwirtschaftsverordnung beschlossen. Mit der Änderung der Außenwirtschaftsverordnung werden die Hürden für

Übernahmen in besonders sensiblen Bereichen höher. Will künftig ein außereuropäischer Investor mindestens zehn Prozent der Anteile eines deutschen Unternehmens erwerben, kann die Bundesregierung den Vorgang prüfen. Bislang betrug die Prüfschwelle 25 Prozent der Firmenanteile. Der abgesenkte Schwellenwert bezieht sich nur auf Unternehmen, die für die Sicherheit Deutschlands entscheidend sind –

etwa im Bereich der Verteidigung oder der sogenannten kritischen Infrastrukturen. Dazu zählen Energieversorger, aber auch Lebensmittelproduzenten ab einer bestimmten Größe. Auch für Unternehmen der Medienwirtschaft gelten künftig die verschärften Regeln. Das soll verhindern, dass deutsche Medien bei Übernahme durch ausländische Investoren für Desinformation genutzt werden können.

## Bericht der EU-Kommission zum EU-US-Datenschutzschild

Die Europäische Kommission hat am 19. Dezember 2018 ihren Bericht über die zweite jährliche Überprüfung der Funktionsweise des EU-US-Datenschutzschildes veröffentlicht. Aus dem diesjährigen Bericht geht hervor, dass die Vereinigten Staaten nach wie vor ein angemessenes Schutzniveau für die personenbezogenen Daten gewährleisten, die aus der EU im Rahmen des Datenschutzschildes an teilnehmende Unternehmen in den USA übermittelt werden. Die von den US-Behörden ergriffenen Maßnahmen zur Umsetzung der Empfehlungen der Kommission aus ihrem letztjährigen Bericht haben das Funktionieren des Rahmens verbessert. Die Kommission erwartet jedoch von den US-Behörden noch, dass sie bis zum 28. Februar 2019 eine ständige Ombudsperson benennen, die an die Stelle der derzeit amtierenden tritt. Eine ständige Ombudsperson stelle einen wichtigen Mechanismus dar, der gewährleistet, dass Beschwerden über den Zugriff von US-Behörden auf personenbezogene Daten behandelt werden. Zu den bereits eingeführten Verbesserungen gehören der Ausbau der Zertifizierungsverfahren durch das US-Handelsministerium und die Intensivierung seiner proaktiven Überwachung des Rahmens. Wie die Kommission in ihrer ersten jährlichen Überprüfung empfahl, hat das Handelsministerium mehrere Mechanismen eingerichtet, z. B. eine Systemkontrolle („Stichprobenkontrolle“), für die Unternehmen nach dem Zufallsprinzip ausgewählt werden, um zu überprüfen, ob sie die Grundsätze des Datenschutzschildes einhalten. Von 100 kontrollierten Unternehmen wurden bei 21 Problemen festgestellt, die inzwischen gelöst wurden. Weitere Verfahren zur Überprüfung der Einhaltung umfassen auch die Analyse der Websites der Datenschutzschild-Teilnehmer, um sicherzustellen, dass die Links zu den Datenschutzbestimmungen korrekt sind. Das Handelsministerium hat ein System zur Ermittlung falscher Behauptungen eingerichtet, das verhindert, dass Unternehmen, die nicht zertifiziert wurden, von sich behaupten, sie würden das Datenschutzschild einhalten.

# 32. DEUTSCHER LEBENSMITTELRECHTSTAG

## Lebensmittelrecht zwischen Renationalisierung und Harmonisierung in Europa

Europäische Entwicklungen | Transparenz in der Krise? | Nationale Kontrolle  
Trends in Deutschland und den USA | Neue Technologien

20. bis 22. März 2019 | Wiesbaden, Kurhaus

### Referenten:

- Dr. Mario Stein** | Landratsamt Erzgebirgskreis  
**Dr. Jörg W. Rieke** | Milchindustrieverband  
**Peter Röhrig** | Bund Ökologische Landwirtschaft  
**Dr. Sabine Jülicher** | Europäische Kommission  
**Dr. Bernhard Url** | Geschäftsf. Direktor der EFSA  
**Dr. Markus Kraus** | Weiss Walter Fischer-Zernin RAe  
**Prof. Dr. Markus Möstl** | Universität Bayreuth  
**MD Bernhard Kühnle** | BMEL  
**Prof. Dr. Dr. Michael Kühne** | Nds. Ministerium f.  
Ernährung, Landwirtschaft und Verbraucherschutz  
**Dr. Marcus Girnau** | Bund f. Lebensmittelrecht  
und Lebensmittelkunde e. V.  
**Dr. Katharina Kluge** | BMEL  
**Dr. Christine Bothmann** | Nds. Landesamt f.  
Verbraucherschutz u. Lebensmittelsicherheit  
**Prof. Franz-Theo Gottwald** | Schweisfurth Stiftung  
**Dr. Anna Glinke** | Hogan Lovells International  
**Christian Ballke, LL.M.** | Meisterernst RAe  
**Dr.-Ing. Volker Heinz** | Deutsches Institut f.  
Lebensmitteltechnik e.V.

### Rabatte! So sparen Sie intelligent:

Frühbucherrabatt 5 % bei Buchung bis 12.11.2018,  
Mehrbucherrabatt 5 % bei Anmeldung von mehr als  
2 Teilnehmern einer Kanzlei/eines Unternehmens ab  
dem 3. Teilnehmer (unabhängig vom Frühbucherrabatt)

### ANMELDUNG

- Behördenvertreter/Abo ZLR  
 Behördenvertreter/Normalpreis  
 Mitglied WGL       ZLR-Abonnent  
 Vorabend (Mi)       Abendessen (Do)

### SEMINARGEBÜHR\*

- € 529,00 f. Behördenvertreter bei Abo ZLR  
 € 569,00 f. Behördenvertreter Normalpreis  
 € 769,00 f. Abonnenten ZLR  
 € 819,00 f. Mitglieder WGfL  
 € 1.299,00 Normalpreis

\*alle Preise zzgl. MwSt.

\_\_\_\_\_  
Name/Vorname

\_\_\_\_\_  
Kanzlei/Firma

\_\_\_\_\_  
Straße

\_\_\_\_\_  
PLZ

\_\_\_\_\_  
Ort

\_\_\_\_\_  
E-Mail

\_\_\_\_\_  
Datum

\_\_\_\_\_  
Unterschrift

### INFORMATIONEN

Deutscher Fachverlag GmbH

**Torsten Kutschke**

60264 Frankfurt am Main

Tel.: 069 7595-1151 | Fax: 069 7595-1150

E-Mail: torsten.kutschke@dfv.de

# ZLR / WGfL

Deutscher Lebensmittelrechtstag

Im Internet anmelden unter  
[www.lebensmittelrechtstag.de](http://www.lebensmittelrechtstag.de)  
 oder per Fax an **069 7595-1150**