Compliance

Die Zeitschrift für Compliance-Verantwortliche

Februar 2018

Inhalt

LucaZola/iStock/Thinkstock

Aufmacher

Trend 2018:
Wettbewerber-Kontakt-Register
Die Bedeutung von Kartell-Compliance nimmt auch im Jahr 2018 weiter zu. Hohe Bußgelder und gravierende Reputationsschäden rücken das Thema zu Recht in den Fokus. Ein unternehmensinternes „Wettbewerber-Kontakt-Register" könnte Unternehmen vor Kartellabsprachen schützen.

Praxis

Ligorko/iStock/Thinkstock

Tax-Compliance-Systeme müssen sich 2018 an vielfältige Änderungen anpassen
Der Vorteil von Tax-Compliance-Management-Systemen wird in vielen Unternehmen noch unterschätzt. Warum sich das im Jahr 2018 ändern könnte und an welche Entwicklungen das Tax-CMS dieses Jahr unbedingt angepasst werden sollte, erläutern Helmut König und Christian Schenk.

Praxis

carlotofolo/iStock/Thinkstock

Compliance in SAP-Systemen durch Continuous Auditing
SAP-Prüfungen befinden sich im Umbruch: Anstelle jährlicher Stichprobenprüfungen steht inzwischen Continuous Monitoring und damit verbundenes Continuous Auditing im Fokus. Hierzu gibt Jörg Altmeier einen Überblick.

Praxis

Wavebreakmedia Ltd/Wavebreak Media/Thinkstock

Datenschutz-Folgenabschätzungen als Teil wirksamer Compliance
Die Voraussetzungen zur Durchführung der Datenschutz-Folgenabschätzungen (DSFA) sind in der Datenschutz-Grundverordnung (DSGVO) eher schwammig umschrieben. Dr. Michael Widmer und Tanja Juelich erläutern eine Guideline der Artikel-29-Arbeitsgruppe (WP29), die bei der Auslegung helfen soll.

Veranstaltungen

16.02.2018 | **Winterthur | 2. DACH-Compliance-Tagung**

12.-13.04.2018 | **Sao Paulo | Compliance across Americas**

24.04.2018 | **Düsseldorf | Digitalisierung und Compliance**

06.06.2018 | **Frankfurt | Deutsche Compliance Konferenz 2018**

Trend 2018: Wettbewerber-Kontakt-Register

Die Bedeutung von Kartell-Compliance nimmt auch im Jahr 2018 weiter zu. Hohe Bußgelder und gravierende Reputationsschäden rücken das Thema zu Recht in den Fokus. Ein unternehmensinternes „Wettbewerber-Kontakt-Register" könnte Unternehmen vor Kartellabsprachen schützen.

LucaZolaI/iStock/Thinkstock

Unklares Treffen mit dem Konkurrenten: Dem könnten Unternehmen zum Beispiel mit einem Wettbewerber-Kontakt-Register vorbeugen.

Bundeskartellamt und Europäische Kommission haben den Informationsaustausch zwischen Wettbewerbern im Blick. Dabei geht es den Wettbewerbshütern vor allem darum, Preisabsprachen und Marktaufteilungen zu verhindern. Die Unternehmen tun daher gut daran, ihre kartellrechtlichen Compliance-Maßnahmen stetig zu verbessern und auch in die Glaubwürdigkeit ihrer Compliance-Bemühungen zu investieren.

Eric S. Soong, Chief Compliance Officer und Leiter Corporate Security bei der Schaeffler Gruppe, empfiehlt hierzu die Etablierung eines unternehmensintern geführten Wettbewerber-Kontakt-Registers: „Um Kartellvorwürfen zu begegnen, müssen Unternehmen belegen können, dass sie einen kontrollierten Prozess haben, wer mit wem in Sachen Wettbewerbern in Kontakt steht und dass es sich um einen legitimen Dialog handelt. Ein Nachweis mittels eines Wettbewerber-Kontakt-Registers kann dabei helfen zu belegen, dass es nicht um Preisabsprachen geht."

Wie wichtig dieser Nachweis ist, zeigen diverse Entscheidungen der Kartellbehörden, in denen bereits der reine Informationsaustausch sanktioniert wurde. Die Behörden wollen damit jegliche Einflussnahme auf das Marktverhalten der Wettbewerber unterbinden. Für betroffene Unternehmen kann es daher entscheidend sein, detailliert dokumentiert zu haben, wer wann und mit wem zu welchem konkreten inhaltlichen Zweck in Kontakt getreten ist. Hierbei kann das Register helfen.

Welche Angaben genau in diesem Wettbewerber-Kontakt-Register erfasst werden, kann dabei von Unternehmen zu Unternehmen stark variieren. „Die Angaben müssen zunächst praktikabel sein. Was im Einzelnen erfasst werden muss, sollte mit gesundem Menschenverstand beurteilt werden", sagt Soong. Je nach Anlass oder Beteiligung bestimmter Mitarbeiter könnte daher auch bereits das simple Treffen zum Mittagessen ein Fall für das Register sein. Am Ende muss jeder Mitarbeiter für sich entscheiden, welche Kontakte er im Rahmen bestimmter Unternehmensvorgaben in das Register eingibt. Dieser Schritt dürfte dafür sorgen, dass die Mitarbeiter zur ständigen Reflexion über ihr Kontaktverhalten aufgerufen sind. Allein das kann schon präventiven Charakter haben. Sollte es in Einzelfällen trotz dieser „Hürde" zu kartellrechtlich relevanten Verstößen beim Informationsaustausch kommen, so kann das Unternehmen durch das Register zumindest seine Compliance-Bemühungen nachweisen.

Zur praktischen Umsetzung des Registers dürfte ab einer gewissen Unternehmensgröße eine webbasierte Lösung sinnvoll sein, um das Register unternehmensweit einheitlich zu führen. Ein mögliches Element des Registers wäre eine Vorabgenehmigungspflicht der Wettbewerberkontakte. Das System könnte je nach Risiko- und Sachlage automatisiert eine Freigabe erteilen oder die Freigabe durch die Abteilungen Compliance und/oder Recht vorsehen.

Entscheidend für die Freigabe sollten aber nicht nur die Tagesordnungen bevorstehender Treffen mit Wettbewerbern sein. Soong rät: „Das System sollte auch abfragen, ob der teilnehmende Mitarbeiter bereits hinreichend im Hinblick auf Kartellrecht geschult ist. Wenn nicht, muss vor dem Kontakt nachgeschult werden."

In einem Wettbewerber-Kontakt-Register sieht Soong viele Vorteile. Es könnte nicht nur zur Prävention bei kartellrechtlich kritischen Kontakten beitragen, sondern auch Klarheit zum Beispiel über Mitgliedschaften in Verbänden bringen. „Nicht selten sind unterschiedliche Abteilungen im Unternehmen eigenständig in Verbänden organisiert, ohne zu wissen, dass bereits die Kollegen in der Nachbarabteilung für genau dieselbe Mitgliedschaft zahlen ", beschreibt Soong. Um solche Dopplungen auszuschließen, könnte ein Kontaktregister gleich in Kombination mit einem Verbandsregister aufgelegt werden, um so einen zusätzlichen Mehrwert aus der Investition zu schöpfen.

chk

Schaeffler

Für Eric S. Soong, Chief Compliance Officer und Leiter Corporate Security bei der Schaeffler Gruppe, ist das Wettbewerber-Kontakt-Register ein Trend im Jahr 2018.

Tax-Compliance-Systeme müssen sich 2018 an vielfältige Änderungen anpassen

Der Vorteil von Tax-Compliance-Management-Systemen wird in vielen Unternehmen noch unterschätzt. Warum sich das im Jahr 2018 ändern könnte und an welche Entwicklungen das Tax-CMS dieses Jahr unbedingt angepasst werden sollte, erläutern Helmut König und Christian Schenk.

Ugorkoi/iStock/Thinkstock

Tax-Compliance 2018: Es wird Zeit, das Tax-CMS an die neuen Entwicklungen anzupassen.

Fehlerhafte Steuererklärungen werden in der Praxis überwiegend erst im Rahmen von Betriebsprüfungen entdeckt. In diesem Zusammenhang hat das Bundesministerium der Finanzen mit dem Anwendungserlass zu § 153 AO vom 23. Mai 2016 angedeutet, dass ein innerbetriebliches Kontrollsystem für steuerliche Zwecke („Steuer-IKS") ggf. ein Indiz gegen ein vorwerfbares Verhalten darstellen kann.

Schon 2017 wurden die Geschäftsleitungen in Einzelfällen von Betriebsprüfern zu Beginn der Betriebsprüfung gefragt, ob das Unternehmen ein Steuer-IKS eingerichtet hat. Für 2018 sind solche Nachfragen häufiger zu erwarten, da der AEAO zu § 153 mittlerweile nicht mehr so neu ist. Es bleibt abzuwarten, ob sich durch den Nachweis eines eingerichteten Steuer-IKS der Umfang der Prüfung verringert. Sollte dies der Fall sein, würde ein positiver Anreiz für Unternehmen geschaffen, den auf die Erfüllung der steuerlichen Pflichten gerichteten Prozessen mehr Aufmerksamkeit zukommen zu lassen. In der Praxis ist zu beobachten, dass Unternehmen den Vorteil eines wirkungsvollen Steuer-IKS bzw. Tax-Compliance-Management-Systems („Tax-CMS") noch nicht vollständig erkannt haben.

Angesichts sich stetig verändernder technischer und regulatorischer Rahmenbedingungen für das unternehmerische Handeln muss sich ein Tax-CMS immer weiterentwickeln und in das Gesamtsystem des Unternehmens integriert sein (wobei die Prozesse zur Erkennung der geänderten Rahmenbedingungen bereits Teil des Systems sind!). Zum anderen wird klar, dass steuerliche Prozesse nicht isoliert im Unternehmen ablaufen.

So wird beispielswiese 2018 der fiskalische Druck auf grenzüberschreitend tätige Unternehmen der Digitalwirtschaft im Bereich der Umsatzsteuer weiter zunehmen: Seit einigen Jahren wenden viele Staaten für elektronische Dienstleistungen umsatzsteuerlich das Empfängerortprinzip an. Danach unterliegen Unternehmen in dem Staat der Umsatzsteuer, in dem der private Endverbraucher ansässig ist. Für EU-Fälle galt dies ab 2015. Weltweit wenden über 40 Staaten das Empfängerortprinzip für elektronische Dienstleistungen im B2C-Bereich an. Unternehmen mit entsprechenden Leistungen müssten sich ohne Sondervorschriften in diesem Staat registrieren und zumindest Umsatzsteuererklärungen abgeben. Viele nichteuropäische Staaten sehen allerdings lediglich Umsatzgrenzen vor, ab denen Deklarationspflichten bestehen. Solche Umsatzgrenzen können sich verändern. In der Schweiz bestand z.B. bis 2017 erst eine Registrierungspflicht, wenn die in der Schweiz ausgeführten Umsätze CHF 100.000 überstiegen. Seit 2018 bezieht sich diese Grenze auf den weltweiten Umsatz, sodass auf einmal Unternehmen steuerlichen Pflichten in der Schweiz nachkommen müssen, für die dieser Markt von vollkommen untergeordneter Bedeutung ist.

Auch auf EU-Ebene wird bereits konkret an einer tiefgreifenden Neuordnung des Mehrwertsteuersystems gearbeitet. Die Schlagwörter sind hier: One-Stop-Shop, Reihengeschäfte, Konsignationslager und mehr. Auch durch die US-Steuerreform ergeben sich mögliche steuerliche Implikationen für die fiskalische Risikoexposition deutscher Unternehmen mit entsprechenden Geschäftsbeziehungen und/oder Beteiligungsverhältnissen in den US-Markt.

Ein Tax-CMS kann somit vor dem Hintergrund dieser Beispiele nur wirksam sein, wenn es Prozesse vorsieht, solche Änderungen zu erkennen und dann die Bestandteile des Tax-CMS laufend an die sich ändernden Rahmenbedingungen angepasst werden. Andernfalls droht die Gefahr, dass das Tax-CMS schleichend unwirksam wird. Die von der Finanzverwaltung angedachte protektive Wirkung eines Steuer-IKS tritt aber nur dann ein, wenn dieses IKS angemessenen und wirksam ist.

Eine wesentliche ab dem Jahr 2018 (nämlich ab dem 25. Mai) verpflichtend anzuwendende Vorschrift ist die EU Datenschutz-Grundverordnung. Viele Unternehmen arbeiten gerade noch mit Hochdruck daran, die notwendigen Prozesse aufzusetzen und zu dokumentieren. Beispielsweise sind geeignete Löschkonzepte für persönliche Daten aufzustellen und umzusetzen. Das auf den Datenschutz gerichtete Compliance-Management-System und das Tax-CMS überschneiden sich in diesem Fall. Die Konzentration nur auf das eine, ohne das andere ebenfalls im Blick zu haben, birgt die Gefahr zumindest gegen die gesetzlichen Vorschriften eines Bereichs zu verstoßen.

Helmut König und Christian Schenk

Beiten Burkhardt

Helmut König, Wirtschaftsprüfer/Steuerberater, ist Partner bei BEITEN BURKHARDT in Düsseldorf und Leiter der Praxisgruppe Steuern. Sein Tätigkeitsbereich umfasst insbesondere steuerliche Strukturierungen und Umwandlungen wie auch Beratungstätigkeiten im Bereich der Umsatzsteuer, des steuerlichen Verfahrensrechts, Restrukturierung und Sanierung.

Beiten Burkhardt

Christian Schenk, Wirtschaftsprüfer/Steuerberater, ist Partner bei BEITEN BURKHARDT in Düsseldorf und Mitglied der Praxisgruppe Steuern. Sein Tätigkeitsbereich umfasst die steuerliche und betriebswirtschaftliche Beratung von Unternehmen unterschiedlicher Rechtsformen, Größen und Branchen.

Mehr zu den aktuellen Entwicklungen und gezielte Praxishinweise zur Tax-Compliance können Sie als Teilnehmer der **Deutschen Compliance Konferenz** 2018 am 6. Juni 2018 in Frankfurt am Main erfahren.

Intensivkurs

Datenschutz-Grundverordnung

Ab dem 25. Mai 2018 verbindlich umzusetzen

Wichtiges Hintergrundwissen und praktische Hilfestellungen für die Umsetzung

Highlights aus dem Programm

- Compliance-Druck und Kontrolldichte: Ohne und mit DSGVO
- Sanktionen bei Verstoß gegen die DSGVO
- Verarbeitung personenbezogener Daten: Einwilligung, Vertrag, Interessenabwägung
- Datenschutz-Folgenabschätzung: Risiken identifizieren und bewerten
- Steuerung von Risiken durch technisch-organisatorische Maßnahmen
- Inhalte eines Verarbeitungsverzeichnisses und weitere Dokumentationspflichten
- Ernennung eines Datenschutzbeauftragten: Aufgaben, Verantwortung, Haftungsrisiken
- Der unternehmensinterne Prozess zur Bearbeitung der Betroffenenrechte
- Datenschutzerklärung und Mitteilungspflicht bei „Datenpannen“
- Wann liegt Auftragsdatenverarbeitung vor und was ist dann zu beachten?
- Datenübermittlung in Drittländer: Was geht, was geht nicht?

Termine

25. April 2018 in Frankfurt am Main

14. Mai 2018 in Bonn

05. Juni 2018 in München

Mehr Informationen und Anmeldung unter vereon.ch/dsg

Compliance in SAP-Systemen durch Continuous Auditing

SAP-Prüfungen befinden sich im Umbruch: Anstelle jährlicher Stichprobenprüfungen steht inzwischen Continuous Monitoring und damit verbundenes Continuous Auditing im Fokus. Nachdem insbesondere SAP-ERP-Systeme gründlich unter die Lupe genommen werden, sorgt das automatisierte Verarbeiten von regelbasierten Prüfungen für viel Zeitersparnis. Hierzu gibt Jörg Altmeier einen Überblick.

SAP-Systeme sind die wohl am häufigsten auditierten Informatiksysteme weltweit. Das liegt zum einen daran, dass diese oftmals das Herzstück der Business-Software eines Unternehmens darstellen und damit besondere Anforderungen an die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien erfüllen müssen. Zum anderen sind die von Wirtschaftsprüfungen aufgestellten Prüfregeln für SAP-Systeme am besten dokumentiert. Regelmäßig einmal im Jahr, im Herbst oder am Jahresende, steht daher bei zahlreichen Unternehmen die Informatik-Revision an. Diese führt zu manchmal hektischen, meist zumindest arbeitsintensiven Aktivitäten, um die von den Revisoren geforderten Informationen und Belege bereit zu stellen. Häufig wird mit „Shopping Lists" gearbeitet, mehr oder weniger umfangreichen Listen von SAP-Tabellen, Belegauszügen und Dokumentationen, die für das betreffende SAP-System extrahiert und für die Prüfung bereit gestellt werden müssen.

Auf Basis der in den bereitgestellten Tabellen und Belegen enthaltenen Informationen werden von Prüfern manuell oder toolgestützt Abweichungen zu bestehenden Vorgaben oder Mustern ermittelt, die auf eine nicht vorgabegerechte Systemeinstellung oder unsachgemäßes Bearbeiten von Geschäftsvorfällen schließen lassen könnten. Überall dort, wo eine Abweichung ermittelt wurde, sind von den Verantwortlichen der IT-Abteilung Aussagen gefordert, woher die Abweichung resultiert und wie sie sachlich begründet werden kann. Für die IT-Verantwortlichen und Mitarbeitenden produziert diese Unsicherheit einen teilweise großen Stressfaktor, insbesondere auch, weil die täglich zu bewältigenden Betriebsaufgaben kaum Zeit für intensive Nachforschungen lassen. Auf der Seite der Prüfer ist es ähnlich, stehen diese doch vor der Herausforderung, mit möglichst geringem Personal und Zeit-Aufwand korrekt zu prüfen.

Neue Prüfsoftware fokussiert nicht mehr ausschließlich auf zeitpunktbezogene Stichprobenprüfungen, sondern überwacht automatisiert und kontinuierlich die definierten Vorgabewerte. Abweichungen werden aufgezeigt, dokumentiert und per Workflow den zuständigen Personen im IT-Betrieb, in den Fachabteilungen oder im Sicherheits- und Risikomanagement übermittelt. Dort werden sie zeitnah analysiert und (falls erwünscht) auditgerecht begründet oder im Falle einer ungewollten Veränderung via Change-Management-Prozess wieder auf den Vorgabewert zurückgeführt. Die verwendeten Best-Practise-Prüfregeln decken dabei alle zu überwachenden Bereiche ab, die Kontrollen auf Geschäftsprozessebene, auf SAP-Anwendungsebene (prozessbezogen und applikationsübergreifend), sowie Kontrollen für die SAP-Basissysteme und für die SAP-Infrastruktur. Durch das automatisierte kontinuierliche Überprüfen sämtlicher Prozesse und Einstellungen (Continuous Monitoring) und auch durch die automatisierte Korrektur oder Begründung von Abweichungen, ist die Nachvollziehbarkeit und Revisionssicherheit garantiert (Continuous Auditing). Wesentlich ist der Einbezug der Fachabteilungen in den Prozess. Sie entscheiden für die applikations- und prozessbezogenen Kontrollen, ob eine erkannte Abweichung zur von ihnen verantworteten Vorgabe toleriert und begründet, das Risiko also akzeptiert wird, oder ob die erkannte Abweichung korrigiert werden soll. Bislang waren es häufig die IT-Mitarbeitenden, die dies häufig in Unkenntnis der betriebswirtschaftlichen Sachverhalte entscheiden mussten und dies im Rahmen der jährlichen IT-Revision gegenüber den Prüfern zu rechtfertigen hatten.

carlotoffolo/iStockfinkstock

SAP-System: Das Herzstück der Business-Software vieler Unternehmen.

Continuous Monitoring und Auditing sorgt für eine deutliche Effizienzsteigerung im Compliance Monitoring, sowohl auf Kunden- als auch auf Prüfungsseite. Manuelle, aufwändige Prüfungen werden in Bruchteilen der bisher benötigten Zeit toolgestützt abgearbeitet und sind durch den Einsatz abgenommener Regeln auch fehlerfrei. Das eingesetzte Regelwerk beschränkt sich dabei nicht ausschließlich auf Anforderungen der Revision. Es beinhaltet auch Vorgaben zu unternehmensinternen Weisungen wie Stellvertretungsregeln oder Governance-Richtlinien wie Systembereinigungen. Dadurch haben die Fachabteilungen und die IT jederzeit die Gewissheit, dass ihr jeweiliger Verantwortungsbereich vorgabenkonform ist. Eine Sicherheit, die sehr stark auch dazu beitragen kann, den IT-Revisionen immer noch anhaftenden Stressfaktor zu reduzieren und eine konstruktive Kooperation zwischen IT-Verantwortlichen und Prüfern zu ermöglichen – zum Nutzen des Unternehmens.

Jörg Altmeier

Jörg Altmeier, Diplom-Kaufmann, MTQ (Universitäten Saarbrücken und Kaiserslautern), seit über 20 Jahren beratend im Umfeld Projects, Processes, Quality, Information und Security tätig.
Zu Compliance in SAP Systemen hat Jörg Altmeier bereits zahlreiche Seminare geleitet, aktuelle Termine finden Sie hier: **www.vereon.ch/scc**

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251,
60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. 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
Unter Mitwirkung von CAD-Institut für Compliance, Arbeitsrecht und Datenschutz
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 Rechtsanwaltsgesellschaft mbH
Fachbeirat der Online-Zeitschrift Compliance: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, thyssenkrupp Steel Europe AG; Ralf Brandt, divieni patch Beteili- gungs GmbH; Otto Geiß, Fraport AG; Mirko Haase, Hilti Corporation; Dr. Katharina Hastenrath, Frankfurt School of Finance & Management; Olaf Kirchhoff, Mitutoyo Europe GmbH; Torsten Krumbach, Bosch Sicherheitssysteme GmbH; Dr. Karsten Leffrang, 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; 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

Fit für die Praxis

Digitalisierung & Compliance

Datenschutz 2.0 – Chance und Risiko

In Kooperation mit TaylorWessing und KLDiscovery

Medienpartner: BVDW Wir sind das Netz, Kommunikation & Recht, Compliance Berater und Recht innovativ

Düsseldorf | Dienstag, 24. April 2018

09.30 - 10.00 Uhr	**Registrierung**
10.00 - 10.15 Uhr	**Begrüßung** Torsten Kutschke, dfv Mediengruppe Detlef Klett, Taylor Wessing
10.15 - 11.00 Uhr	**IT-Compliance: Cybersecurity** • Aktuelle Bedrohung aus dem Cyberraum • IT-Sicherheitsrecht vor und nach 2015 • Konsequenzen für Unternehmen in Deutschland Detlef Klett, Taylor Wessing
11.00 - 11.30 Uhr	Kaffeepause
11.30 - 12.30 Uhr	**IT-Compliance: Endspurt DS-GVO** • Kurzer Überblick über die DS-GVO • Umsetzung: Aufgaben, Herausforderungen, Risiken • Hilfestellungen und Praxistipps Mareike Gehrmann, Taylor Wessing
12.30 - 13.30 Uhr	Mittagspause (inkl. Breakout-Session mit KLDiscovery)
13.30 - 14.30 Uhr	**Kartellrechtliche Compliance bei digitalen Geschäftsmodellen** • Kartellrechtliche Grenzen beim Einsatz von Digital Pricing Tools / Preissetzungsalgorithmen • Neue Entwicklungen im Bereich E-Commerce: Plattformverbote und selektiver Vertrieb (insbes. Coty-Urteil des EuGH), Paritätsklauseln, Best-Preis-Klauseln (Booking & Co.), wesentliche Ergebnisse der Sektoruntersuchung der EU-Kommission im Bereich E-Commerce Stephan Manuel Nagel, Taylor Wessing
14.30 - 14.45 Uhr	Kaffeepause
14.45 - 15.30 Uhr	**Verbraucherschutzkompetenzen des Bundeskartellamts in der digitalen Wirtschaft** • Darstellung der neuen Verbraucherschutzkompetenzen des BKartA durch die 9. GWB-Novelle • Zusammenspiel zwischen Verbraucherschutz durch BKartA und Verbraucherzentralen • Aktuelles Vorgehen des BKartA im Bereich SmartTVs Dr. Markus Böhme, Taylor Wessing
15.30 - 15.45 Uhr	Kaffeepause
15.45 - 17.15 Uhr	**Podiumsdiskussion: Compliance-Herausforderungen in der digitalen Welt** Moderator: Stephan Manuel Nagel, Taylor Wessing Teilnehmer: Oliver Hahne, Leiter Legal + Compliance, Haufe Gruppe Dr. André Uhlmann, Head of Compliance, thyssenkrupp Industrial Solutions AG Michael Neuber, Bundesverband Digitale Wirtschaft (BVDW) e.V.
ab 17:15 Uhr	**Sundowner auf Einladung von** TaylorWessing


Detlef Klett


Torsten Kutschke


Mareike Gehrmann


Stephan Manuel Nagel


Dr. Markus Böhme


Dr. André Uhlmann


Michael Neuber


Oliver Hahne

Datenschutz-Folgenabschätzungen als Teil wirksamer Compliance

Die Voraussetzungen zur Durchführung der Datenschutz-Folgenabschätzungen (DSFA) sind in der Datenschutz-Grundverordnung (DSGVO) eher schwammig umschrieben. Dr. Michael Widmer und Tanja Juelich erläutern nachfolgend eine **Guideline** der **Artikel-29-Arbeitsgruppe** (WP29), die bei der Auslegung helfen soll.

Wavebreakmedia Ltd/Wavebreak Media/Thinkstock

Besteht ein Datenschutzrisiko? Die Datenschutz-Folgenabschätzung soll das klären.

Die Datenschutz-Grundverordnung (DSGVO) sieht als Instrument zur Identifikation von Datenschutzrisiken die Durchführung von Datenschutz-Folgenabschätzungen (DSFA) vor. Die DSFA ist ein Prozess der Compliance, welcher der Erfüllung grundsätzlicher Anforderungen der DSGVO dient. Dadurch sollen Risiken identifiziert und bewertet werden, die durch den Einsatz von Technologien und Systemen im Rahmen der Datenverarbeitung entstehen. Gemäß Art. 35 Abs. 1 DSGVO muss eine DSFA durchgeführt werden, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge" hat. Die Voraussetzungen zur Durchführung einer DSFA werden in der DSGVO eher schwammig umschrieben. Die Aufsichtsbehörden haben deshalb eine Liste von Verarbeitungsvorgängen zu erstellen, für welche eine DSFA durchzuführen ist (schwarze Liste). Ferner können sie eine Liste von Verarbeitungsvorgängen erstellen, für die keine DSFA erforderlich ist (weiße Liste). Darüber hinaus enthält Art. 35 Abs. 7 DSGVO zwar gewisse Mindestanforderungen betreffend den Inhalt der DSFA. Hinsichtlich weiterer Anforderungen, der Methodologie zur Durchführung von DSFA und der Verpflichtung zur vorherigen Konsultation der Aufsichtsbehörde sind die Regelungen aber vage.

Deshalb hat die Artikel-29-Arbeitsgruppe (WP29) eine Guideline erstellt. Diese ausführliche, immerhin 22 Seiten lange Guideline soll helfen, die schwammigen Begriffe zu klären.

Dr. Michael Widmer, LL.M., ist als Rechtsanwalt in Zürich tätig. Zudem ist er Dozent für Datenschutz an der ZHAW School of Management and Law.

Tanja Juelich, MSc., LL.M., ist wissenschaftliche Assistentin an der ZHAW School of Management and Law. Sie ist im Bereich des Datenschutzes tätig.

Sie enthält u.a. Hilfestellungen hinsichtlich der Methodologie zur Durchführung von DSFA und der Verpflichtung zur vorherigen Konsultation der Aufsichtsbehörde.

Vor allem aber enthält die Guideline diverse Kriterien zur Beantwortung der Frage, wann ein hohes Risiko vorliegt, da die in Art. 35 Abs. 3 DSGVO enthaltenen Beispiele nicht abschließend sind und auch andere Verarbeitungen zu einem „hohen Risiko" führen können.

Als Kriterien nennt die Richtlinie:

- Evaluation oder Scoring
- Automatisierte Einzelfallentscheidungen
- Systematische Überwachung
- Verarbeitung sensitiver Daten oder von Daten hoch persönlicher Art
- Verarbeitung von Daten in großem Umfang
- Datenbestände, welche abgeglichen oder kombiniert wurden
- Verarbeitung von Daten betreffend schutzbedürftige Personen
- Neuartige Anwendung oder Gebrauch von technischen oder organisatorischen Lösungen
- Verarbeitungen, welche die Ausübung von Rechten oder die Inanspruchnahme von Leistungen oder den Abschluss von Verträgen durch die betroffene Person verhindern.

Je mehr dieser Kriterien erfüllt sind, desto eher liegt ein „hohes Risiko" vor, wobei in Fällen, in welchen nur ein Kriterium erfüllt ist, in der Regel keine DSFA durchgeführt werden muss. Wenn ein Verantwortlicher hingegen der Ansicht ist, es liege kein „hohes Risiko" vor, obschon mehr als zwei der oben genannten Punkte erfüllt sind, wird er wohl gute Gründe dafür haben müssen, keine DSFA durchzuführen und sollte dies entsprechend dokumentieren.

Keine DSFA ist durchzuführen, wenn kein „hohes Risiko" vorliegt, wenn für äußerst ähnliche Verarbeitungsvorgänge mit ähnlich hohen Risiken bereits eine DSFA durchgeführt wurde oder wenn die entsprechende Verarbeitung auf einer „weißen Liste" der Aufsichtsbehörde enthalten ist. Eine Pflicht zur DSFA besteht grundsätzlich nur für künftige Verarbeitungen, also nur für solche, mit denen am 25. Mai 2018 noch nicht begonnen wurde. Dennoch muss eine DSFA auch für bereits bestehende Verarbeitungen durchgeführt werden, wenn eine Änderung des damit verbundenen Risikos auftritt.

Ferner ist in gewissen Fällen eine Vorab-Konsultation der Aufsichtsbehörde erforderlich. Gemäß dem Wortlaut gilt dies „wenn aus einer DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft". Damit gemeint ist, dass eine Konsultation demnach nur dann erforderlich ist, wenn das hohe Risiko durch die Maßnahmen des Verantwortlichen voraussichtlich nicht ausreichend eingedämmt werden kann. Auch die WP29 bestätigt diese Ansicht. Darüber hinaus stellt die Guideline klar, dass keine rechtliche Pflicht zur Veröffentlichung von DSFA besteht – obschon eine solche Publikation zumindest von Teilen stark empfohlen wird.

Im besten Fall kann die DSFA demnach als Frühwarnsystem die rechtzeitige Identifikation und angemessene Reaktion auf Datenschutzrisiken unterstützen und so zu einem besseren Datenschutzniveau beitragen.

Dr. Michael Widmer und Tanja Juelich

Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung wird gemäß Art. 35 **DSGVO** durchgeführt, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.