Compliance

Die Zeitschrift für Compliance-Verantwortliche

März 2018

Inhalt

Wavebreakmedia Ltd/ Wavebreak Media/Thinkstock

Aufmacher

Preisalgorithmen als Compliance-Risiko
Preisalgorithmen, also Software, die das Internet nach Preisen durchsucht und die eigenen Online-Preise entsprechend anpasst, rücken immer mehr in den Fokus von Kartellbehörden. Mangels Entscheidungspraxis sind jedoch die maßgeblichen Rechtsfragen noch offen, weswegen die hiermit verbundenen kartellrechtlichen Risiken umso größer sind.

Recht

gmac84/iStock/Thinkstock

DSGVO – Die Rechte der Betroffenen
Die Datenschutzgrundverordnung (DSGVO) fordert massive Anpassungen von Unternehmen in der EU. Hinzu kommt, dass betroffene Personen nach Mai 2018 vermutlich vermehrt ihre Rechte einfordern werden. Unternehmen müssen darauf schnell und gut reagieren können.

Praxis

CreativaImages/iStock/Thinkstock

„Der Berater kann im Moment nur ‚viel hilft viel' empfehlen"
„Viel hilft viel", scheint derzeit die sicherste Antwort auf Fragen nach der Umsetzung der Datenschutzgrundverordnung (DSGVO) zu sein. Worauf Unternehmen achten müssen, beschreibt in unserem Interview Dr. Axel-Michael Wagner.

Praxis

ipopba/iStock/Thinkstock

Umfrage: Schutz gegen Cyber-Attacken
Hacker-Angriffe sind das tägliche Brot vieler Unternehmen. Doch eine aktuelle Umfrage zeigt, dass ihre Sicherheitsmaßnahmen noch verbesserungsbedürftig sind.

Veranstaltungen

23.04.2018 | **Münster | Datenschutz im Unternehmen nach der DS-GVO**

24.04.2018 | **Frankfurt | HR-Compliance**

24.04.2018 | **Düsseldorf | Digitalisierung und Compliance**

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

Preisalgorithmen als Compliance-Risiko

Preisalgorithmen, also Software, die das Internet nach Preisen durchsucht und die eigenen Online-Preise entsprechend anpasst, rücken immer mehr in den Fokus von Kartellbehörden. Mangels Entscheidungspraxis sind jedoch die maßgeblichen Rechtsfragen noch offen, weswegen die hiermit verbundenen kartellrechtlichen Risiken umso größer sind.

Wavebreakmedia Ltd/ Wavebreak Media/Thinkstock

Einkaufstour durchs Internet: Nicht selten sind die Online-Preise das Ergebnis von Preisalgorithmen.

Zur Erinnerung: Das Kartellverbot verbietet Vereinbarungen und abgestimmte Verhaltensweisen zwischen Unternehmen, die eine Wettbewerbsbeschränkung bezwecken oder bewirken. Für einen Verstoß gegen das Kartellverbot kann eine bloße „Fühlungnahme" zwischen Unternehmen ausreichen, beispielsweise wenn ein Unternehmen einseitig einem anderen Unternehmen wettbewerblich sensible Informationen kommuniziert und sich das andere Unternehmen nicht ausdrücklich hiervon distanziert. Auch muss eine Abstimmung nicht unmittelbar zwischen den Beteiligten erfolgen, es reicht eine bewusste und gewollte Kommunikation über einen Dritten (sog. Hub-and-Spoke-Konstellationen, wobei die einzelnen Voraussetzungen strittig sind). Abzugrenzen sind diese Fälle vom kartellrechtlich zulässigen Parallelverhalten, wenn also Unternehmen sich aufgrund ihrer eigenen Marktbeobachtungen autonom dem Verhalten der Mitbewerber anpassen.

Stephan Manuel Nagel ist Partner im Düsseldorfer Büro von Taylor Wessing. Er berät zu allen Fragen des deutschen und europäischen Kartellrechts mit einem seiner Tätigkeitsschwerpunkte im Bereich Compliance. Er hat sich u.a. auf die digitale Wirtschaft und die Branchen Energie, Handel, Werbung und Medien spezialisiert.

Vor diesem Hintergrund lassen sich beim Einsatz von Preisalgorithmen drei wesentliche Fallgruppen unterscheiden:

Die erste Fallgruppe, zu der auch bereits Entscheidungspraxis existiert, betrifft die rechtlich einfach gelagerten Fälle, in denen eine kartellrechtswidrige Abstimmung anderweitig erfolgt und die Preisalgorithmen lediglich deren Durchsetzung dienen. Ein Beispiel hierfür ist die Eturas-Entscheidung des EuGH (EuGH, Urt. v. 21.1.2016, C-74/14). In diesem Fall teilte der Administrator eines Online-Reisebuchungssystems den teilnehmenden Reisebüros eine einzuhaltende Obergrenze für Preisnachlässe mit. Bei deren Überschreiten erfolge automatisch eine Preisanpassung. Der EuGH entschied, dass alle Reisebüros, die sich nicht offen von dieser Mitteilung distanzierten oder diese den Kartellbehörden anzeigten, gegen das Kartellverbot verstießen. Ein weiteres US-amerikanisches und britisches Verfahren betraf den Verkauf von Postern über Amazon (DoJ, Case US v. Daniel William Aston and Trod Limited; CMA, 12.8.2016, Case 50228 – Online sales of posters and frames). In diesem Fall entschieden sich die beteiligten Unternehmen, die getroffenen Preisabsprachen mithilfe einer Preisanpassungssoftware umzusetzen.

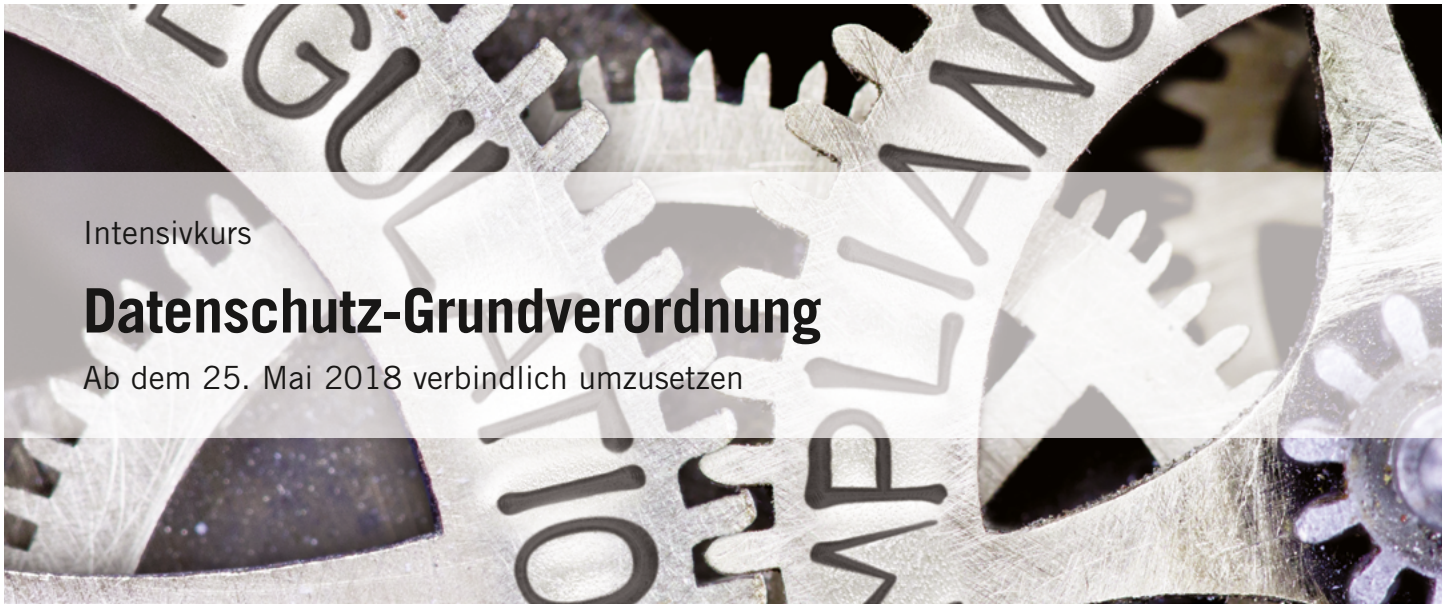
Eine zweite Gruppe betrifft Fälle, in denen Unternehmen bewusst und gewollt dieselben Preisalgorithmen wie ihre Wettbewerber verwenden, um dergestalt Preise abzustimmen. Ein prominenter derzeit in den USA anhängiger Fall ist das Verfahren gegen Travis Kalanick, den ehemaligen CEO und Mitbegründer von Uber (S.D.N.Y., 31.3.2016, 174 F.Supp.3d 817 – Meyer v. Kalanick). Die Uber-Fahrer verpflichten sich, die Uber-App und den damit verbundenen Preisalgorithmus zu benutzen. Die Fahrer melden ihre jeweilige Verfügbarkeit der App, die u.a. auf dieser Grundlage unter Berücksichtigung von Angebotsknappheit den Fahrtpreis berechnet. Während im Fall Uber entscheidend sein könnte, ob es sich bei den Fahrern überhaupt um „Unternehmen" oder nicht vielmehr um Arbeitnehmer handelt, auf die das Kartellrecht keine Anwendung findet, verbieten sich auch in ähnlich gelagerten Konstellationen kartellrechtliche Schnellschüsse. Entscheidend ist eine saubere Abgrenzung zur dritten Fallgruppe, dem zulässigen Parallelverhalten.

Aus unserer Sicht bedarf es beim Einsatz von Preisalgorithmen wie bei klassischen Hub-and-Spoke-Konstellationen eines Vorsatzes, sich mit anderen Unternehmen mittels dieser Algorithmen abzustimmen, um gegen das Kartellverbot zu verstoßen. Hiernach liegt jedenfalls dann ein zulässiges Parallelverhalten vor, wenn Unternehmen Preisalgorithmen einsetzen, ohne zu wissen, dass auch ihre Mitbewerber dieselben Algorithmen benutzen. Auch wenn der jeweilige Nutzer die eingesetzte Software individuell anpassen und so eine autonome Preissetzungsstrategie verfolgen kann, ist nicht von einer abgestimmten Verhaltensweise auszugehen. Dies gilt erst recht, wenn Unternehmen selbst entwickelte Preisalgorithmen einsetzen. Hierbei handelt es sich lediglich um eine autonome Anpassung an das beobachtete Marktverhalten der Wettbewerber. Es bleibt allerdings abzuwarten, ob die Kartellbehörden und Gerichte dieser Auffassung folgen werden.

Schließlich sei darauf hingewiesen, dass Preisalgorithmen nicht nur im Rahmen des Kartellverbots kartellrechtlich relevant sein können, sondern auch beim Verbot des Missbrauchs einer marktbeherrschenden Stellung. So ermittelt das Bundeskartellamt derzeit gegen Lufthansa wegen angeblich überhöhter Preise nach der Insolvenz von Air Berlin. Den Verweis von Lufthansa auf eine automatische Preissetzung durch einen Algorithmus hat Kartellamtspräsident Mundt mit der Aussage gekontert, dass „solche Algorithmen" nicht „vom lieben Gott geschrieben" würden.

Stephan Manuel Nagel

Mehr zu kartellrechtlicher Compliance bei digitalen Geschäftsmodellen und zu weiteren Compliance-Themen in Zusammenhang mit Digitalisierung erfahren Sie bei der Konferenz „**Digitalisierung & Compliance, Datenschutz 2.0 – Chance und Risiko**" am 24. April 2018 in Düsseldorf.



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

DSGVO – Die Rechte der Betroffenen

Die Datenschutzgrundverordnung (DSGVO) fordert massive Anpassungen von Unternehmen in der EU. Hinzu kommt, dass betroffene Personen nach Mai 2018 vermutlich vermehrt ihre Rechte einfordern werden. Unternehmen müssen darauf schnell und gut reagieren können. Wie sie sich in Bezug auf die Betroffenenrechte vorbereiten sollten, beschreibt Dr. Axel-Michael Wagner, Rechtsanwalt und Partner der Kanzlei Peters, Schönberger & Partner mbB.

Erfahrungsgemäß ist die Einhaltung sämtlicher datenschutzrechtlicher Anforderungen gerade für den Mittelstand mit besonderen Schwierigkeiten verbunden. Angesichts knapper personeller Ressourcen, insbesondere im Bereich von Compliance-Management-Systemen, und der Konzentration auf die Kern-Wertschöpfungsprozesse führte das Thema Datenschutz in der Praxis bislang häufig ein Nischendasein. Die ab Mai 2018 geltende Datenschutzgrundverordnung der EU vereinfacht die Sache nicht. Denn sie sieht massive Konsequenzen bei Verstößen vor und macht die Überarbeitung bestehender oder sogar die Einführung neuer unternehmensinterner Prozesse notwendig. Als Beispiel soll hier das Thema Betroffenenrechte dargestellt werden.

Zum einen bestehen Informationspflichten des Unternehmens, das personenbezogene Daten verarbeitet, gegenüber den Betroffenen, deren Daten verarbeitet werden. Dies ist landläufig unter dem Stichwort „Datenschutzerklärung" bekannt. Zum anderen haben die Betroffenen nach der Erhebung ihrer Daten Rechte gegenüber dem datenverarbeitenden Unternehmen. Diese Rechte umfassen insbesondere das Recht auf Auskunft, auf Berichtigung, auf Löschung („Vergessenwerden"), auf eingeschränkte Verarbeitung, auf Datenübertragbarkeit und auf Widerspruch. Unverzüglich, spätestens aber binnen eines Monats, muss das Unternehmen dem Betroffenen „Informationen über die ergriffenen Maßnahmen" mitteilen. Entscheidet das Unternehmen, nicht tätig zu werden, muss auch dies dem Betroffenen spätestens nach einem Monat mitgeteilt werden, damit der Betroffene ggf. behördliche oder gerichtliche Hilfe in Anspruch nehmen kann. Die Bearbeitung der Betroffenenrechte durch das Unternehmen muss im Regelfall für den Betroffenen unentgeltlich erfolgen.

Das Unternehmen ist daher gehalten, im Rahmen eines umfassenden Datenschutzkonzeptes einen unternehmensinternen Prozess zu definieren, in dessen Rahmen Betroffenenrechte bearbeitet werden. Dieser Prozess ist (einschließlich z. B. der unternehmensintern zuständigen Personen) schriftlich niederzulegen. Am Beginn des Prozesses steht die Eingabe des Betroffenen, die das Unternehmen auf unterschiedlichen Kommunikationskanälen erreichen kann. In diesem Zusammenhang ist ggf. die Identität des Betroffenen sicherzustellen, d. h. dass die Person tatsächlich der Betroffene ist. Daran anschließend ist – auch unter Einbeziehung des Datenschutzkonzepts des Unternehmens insgesamt bzw. des vom Unternehmen vorzuhaltenden Verarbeitungsverzeichnisses – zu klären, ob das Recht, das der Betroffene geltend macht, besteht und wie es zu bearbeiten ist. Im Regelfall wird dies den Zugriff auf die vom Unternehmen gespeicherten personenbezogenen Daten des Betroffenen erfordern. Diese Daten sollten demnach für denjenigen, der das Betroffenenrecht im Unternehmen bearbeitet, zentral zugänglich sein. Die Notwendigkeit, diese erst aus verschiedenen Quellen „zusammensuchen" zu müssen, wird zu erheblichem Mehraufwand im Unternehmen führen.

gmac84/iStock/Thinkstock

Daten löschen: Das ist eins der Betroffenenrechte gegenüber dem datenverarbeitenden Unternehmen.

Möglicherweise ist dann im Rahmen des Prozesses eine Änderung dieser Daten bzw. der Zugriffsrechte hierzu (Sperrung etc.) zu veranlassen. Dies betrifft etwa die Rechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung sowie das Widerspruchsrecht. In jedem Fall ist dem Betroffenen Bericht über die ergriffenen Maßnahmen zu erstatten und dieser Bericht zu protokollieren. Im Falle des Auskunftsrechts sind diesem Bericht beispielsweise die personenbezogenen Daten selbst sowie Verarbeitungszwecke, Empfänger, Dauer der Speicherung, Herkunft der Daten etc. beizufügen. Die Übermittlung des Berichts sollte auf einem sicheren Übertragungsweg stattfinden, vorzugsweise über einen gesicherten Online-Zugriff.

Die Behandlung der Betroffenenrechte enthält viele weitere Fallstricke und Besonderheiten. Als Beispiel kann hier der Fall dienen, dass das Unternehmen die personenbezogenen Daten einem Dritten zur Verfügung gestellt hat und die Daten nun aufgrund der Ausübung von Betroffenenrechten geändert oder gelöscht werden müssen. Diese Dritten müssen dann vom datenverarbeitenden Unternehmen benachrichtigt werden, ausgenommen „dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden". Es liegt nahe, dass hier schon im Vorhinein für jedes personenbezogene Datum, das vom Unternehmen „gesammelt" wurde, eine Art Register derjenigen Weiterleitungsempfänger geführt werden sollte, die dann von der entsprechenden Änderung benachrichtigt werden. Wurden die Daten veröffentlicht, etwa auf der Internet-Seite des Unternehmens, so sind sie damit auch über Suchmaschinen etc. zugänglich, obwohl die Daten nicht zielgerichtet an die Suchmaschine übermittelt wurden. In diesem Fall besteht die Verpflichtung, zumindest die gängigen Suchmaschinen (oder andere „Datenwiederverwerter") über das Verlangen der Löschung zu benachrichtigen, um die Löschung von Links und Kopien zu erreichen. Der Betroffene kann die Mitteilung verlangen, welche Dritten infolge der Änderung benachrichtigt wurden.

Es ist damit zu rechnen, dass Betroffene nach Mai 2018 die Reaktionszeiten und -qualitäten verantwortlicher Unternehmen „testen" werden. Die Zugriffs- und Sanktionsmöglichkeiten der Behörden, an welche die Betroffenen Beschwerden richten können, sind immens. Es empfiehlt sich daher gerade für mittelständische Unternehmen dringend – trotz knapper Ressourcen und immer neuer Compliance-Pflichten – auf die korrekte Umsetzung der DSGVO besondere Aufmerksamkeit zu legen. *Dr. Axel-Michael Wagner*

Lesen Sie auch unser Interview zum Thema mit Dr. Axel-Michael Wagner auf Seite 6.

Betroffene Person

Die DSGVO schützt „die Grundrechte und Grundfreiheiten natürlicher Personen", nämlich der betroffenen Personen. Jede Information, die sich auf eine identifizierte oder (direkt oder indirekt) identifizierbare Person bezieht, wird von der DSGVO als personenbezogenes Datum dieser betroffenen Person erfasst. Auch vordergründig rein maschinengenerierte Daten können durchaus einen Personenbezug aufweisen: Der Fahrer eines Fahrzeugs etwa, das Telematikdaten erfasst, ist „betroffene Person", weil die Daten Auskunft über seine Fahrweise geben.

„Der Berater kann im Moment nur ‚viel hilft viel' empfehlen"

„Viel hilft viel", scheint derzeit die sicherste Antwort auf Fragen nach der Umsetzung der Datenschutzgrundverordnung (DSGVO) zu sein. Welchen Nutzen Unternehmen aus der Verordnung ziehen können und an welcher Stelle nur die Gerichte und entsprechende konkretisierende Leitlinien bzw. Empfehlungen des Europäischen Datenschutzausschusses endgültige Klarheit bringen werden, beschreibt in unserem Interview Dr. Axel-Michael Wagner.

CreativeImages/iStock/Thinkstock

Mit Datenschutz Vertrauen schaffen: So können Unternehmen einen Nutzen aus der DSGVO ziehen.

» Große Unternehmen haben das Thema Datenschutz inzwischen als Marketing-Instrument für sich entdeckt. Wie können auch Mittelständler die Sorge ihrer Kunden vor Datenmissbrauch als Werbeinstrument nutzen und das Thema so erfolgversprechend aus der Nische holen?

« Zunächst einmal können sämtliche Unternehmen damit punkten, dass sie die DSGVO, insbesondere die vorgesehenen Aufklärungspflichten und die Wahrung der Betroffenenrechte, einhalten. Dies ist dann auch von außen, insbesondere durch die Betroffenen, wahrnehmbar. Unabhängig davon können sich Unternehmen irgendwann in der Zukunft zertifizieren lassen und mit dem Zertifikat, Siegel oder Prüfzeichen werben. Gerade beim Thema Zertifizierung sieht die DSGVO vor, dass „den besonderen Bedürfnissen von [...] kleinen und mittleren Unternehmen [...] Rechnung getragen" wird, was immer das bedeutet. Über diese von der DSGVO vorgesehenen Mechanismen hinaus ist es natürlich auch nicht verboten, über die Anforderungen hinauszugehen und den Betroffenen (bzw. auf der Website) genauer zu beschreiben, was konkret wo mit ihren Daten passiert. Damit kann – über Marketing-Gemeinplätze hinaus – zusätzliches Vertrauen geschaffen werden.

» Die DSGVO legt den Unternehmen – unabhängig von ihrer Größe – klare Pflichten auf. Ist es hier überhaupt möglich, einen „Minimalweg" zur Umsetzung der Verordnung zu beschreiten?

« Im Grundsatz ist es richtig, dass der DSGVO ein „one size fits all"-Ansatz zugrunde liegt. Gleichwohl gibt es die, wenn auch halbherzige, Bestrebung, für kleine und mittlere Unternehmen den Maßstab zu reduzieren – wenn auch keinesfalls auf einen „Minimalweg". So hat man beispielsweise die Verpflichtung, ein Verarbeitungsverzeichnis zu führen, eigentlich auf Unternehmen mit über 250 Mitarbeitern beschränken wollen, aber diesen guten Ansatz durch die diffuse Rückausnahme relativiert, dass doch ein Verarbeitungsverzeichnis zu führen ist, wenn die Verarbeitung personenbezogener Daten „nicht nur gelegentlich" erfolgt. Welches Unternehmen verarbeitet denn „nur gelegentlich" personenbezogene Daten in seinen EDV-Systemen? Das Beispiel zeigt, dass gerade für den Mittelstand die Frage besonders schwer zu beantworten ist, wie die Pflichten der DSGVO nun zu lesen und wie granular sie zu erfüllen sind. Hier werden erst die Gerichte im Laufe der Zeit Klarheit schaffen. Der Berater kann im Moment nur „viel hilft viel" empfehlen. Das macht weder den Berater noch die DSGVO sympathisch.

» Lässt sich abschätzen, wie hoch der Bearbeitungsaufwand pro Bearbeitung der Betroffenenrechte sein wird? Wie lässt sich dieser Bearbeitungsaufwand möglichst gering halten?

« Je besser der entsprechende unternehmensinterne Prozess vorab strukturiert wird, desto effizienter lassen sich Betroffenenrechte später bearbeiten. Es macht einen sehr großen Unterschied, ob ein Unternehmen, das mit einem Betroffenenrecht konfrontiert wird, darauf systematisch vorbereitet oder „kalt erwischt" wird und dann jeden Fall einzeln unstrukturiert behandeln muss. Dabei spielt auch die unternehmensinterne Strukturierung der personenbezogenen Daten selbst eine erhebliche Rolle: Je mehr datenschutzrelevante Metadaten angelegt und gepflegt werden und je besser bei der Bearbeitung von Betroffenenrechten zentral auf sämtliche relevanten Datenbestände zugegriffen werden kann, desto geringer ist der Bearbeitungsaufwand pro Einzelfall.

» Schwierig dürfte es immer dann werden, wenn das Unternehmen die Daten der Betroffenen „aus der Hand gegeben", also Dritten (z.B. Suchmaschinen) zur Verfügung gestellt hat. Wie weit muss das Unternehmen hier gehen, um seine Pflichten zu erfüllen, und wo ist die Grenze „zum unverhältnismäßigen Aufwand" zu ziehen?

« Hier sind zwei Fälle zu unterscheiden: Hat das Unternehmen die Daten an bestimmte Dritte übermittelt und sind die Daten zu berichtigen oder zu löschen, muss dieser Umstand diesen Dritten mitgeteilt werden. Die Grenzen sind hier „Unmöglichkeit" (z. B. ein unbekannt verzogener oder liquidierter Dritter) und „unverhältnismäßiger Aufwand", etwa im Verhältnis zu den Interessen der betroffenen Person, wenn eine unbedeutende Korrektur der Daten vorzunehmen ist und eine große Menge an Empfängern die Daten erhalten haben. Der zweite Fall betrifft das Löschen von Daten, die öffentlich gemacht wurden, insbesondere also auf eine Website gestellt wurden. Hier muss eine Informierung der unbestimmten Anzahl und Identität von Unternehmen, die personenbezogene Daten verarbeiten, stattfinden, und zwar durch „angemessene Maßnahmen unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten". Hier werden – wie auch in vielen anderen Fällen – entsprechende konkretisierende Leitlinien bzw. Empfehlungen des Europäischen Datenschutzausschusses abzuwarten sein. Ich könnte mir vorstellen, dass es in Zukunft sogar Dienstleister gibt, die solche „Löschmitteilungen" fachgerecht im Auftrag abwickeln.

chk

Dr. Axel-Michael Wagner ist Rechtsanwalt und Partner der Kanzlei Peters, Schönberger & Partner mbB in München. Zur DSGVO hat Herr Dr. Wagner bereits verschiedene Seminarveranstaltungen, Workshops und Webinare abgehalten, aktuelle Termine finden Sie u. a. hier: **www.vereon.ch/dsg**

Umfrage: Schutz gegen Cyber-Attacken

Das Problem der Cyber-Attacken ist jüngst durch den Angriff auf das hochgesicherte Regierungsnetzwerk IVBB wieder stärker in das mediale Bewusstsein gerückt. Hacker-Angriffe sind auch das tägliche Brot vieler Unternehmen. Doch eine aktuelle Umfrage zeigt, dass ihre Sicherheitsmaßnahmen noch verbesserungsbedürftig sind.

ipopba/iStock/Thinkstock

Hochspezialisierte Hacker-Angriffe: Viele Unternehmen ändern auch nach einem Angriff wenig an ihren Sicherheitsvorkehrungen.

Cyber-Attacken sind an sich nichts Neues oder gar Außergewöhnliches. Die Bundesregierung registriert nach eigenen Angaben täglich etwa 20 hochspezialisierte Hacker-Angriffe auf ihre Computer. Die Angriffe werden in aller Regel rechtzeitig erkannt und abgewehrt. Brisant ist die aktuelle Attacke auf das Regierungsnetzwerk, weil es den Hackern offenbar gelungen ist, über längere Zeit in das Netz einzudringen.

Zum echten Problem werden Hacker-Angriffe auch für Unternehmen, wenn sie nicht rechtzeitig erkannt werden, und durch die Attacke Daten abfließen oder Schadsoftware eingeschleust wird, die dafür sorgt, dass ein Unternehmen praktisch lahmgelegt ist. Dies kann ernsthafte wirtschaftliche Einbußen nach sich ziehen.

Umso erstaunlicher ist es daher, dass mehr als ein Drittel der deutschen Unternehmen auch nach einer Cyber-Attacke die Sicherheitsstrategie kaum ändert. So zumindest das Ergebnis einer aktuellen Untersuchung von CyberArk , einem weltweit agierenden Anbieter von Sicherheitssystemen. Die globale Umfrage „Advanced Threat Landscape" wurde inzwischen zum elften Mal durchgeführt. Befragt wurden 1.300 IT-Verantwortliche und Geschäftsbereichsleiter weltweit, darunter 200 aus Deutschland.

Offenbar sehen die befragten deutschen Unternehmen sich selbst als unzureichend vor Cyber-Bedrohungen geschützt. So räumen 53% ein, dass sie den Zugriff von Angreifern auf das interne Netzwerk nicht in jedem Fall verhindern können. Fast ebenso viele (47%) deutsche Unternehmen erklären, dass Kunden- oder generell personenbezogene Daten Sicherheitsrisiken ausgesetzt sind. „Angesichts der bevorstehenden EU-Datenschutz-Grundverordnung kann sich eigentlich kein Unternehmen mehr einen laxen Umgang mit personenbezogenen Daten leisten", betont Michael Kleist, Regional Director DACH bei CyberArk in Düsseldorf. Unternehmen müssten sich daher mit den zentralen Einfallstoren auseinandersetzen. Ein großes Risiko seien Administratorenrechte oder weitreichende Benutzerrechte auf Endgeräten. Viele Unternehmen seien sich dieses Risikos aber nicht bewusst oder ließen es außer Acht. Denn die Befragten bestätigten, dass die Zahl der Anwender, die über lokale administrative Privilegien auf ihren Endgeräten verfügen, von 64% in der letztjährigen Untersuchung auf jetzt 83% gestiegen ist.

Deutsche Unternehmen sehen die größten Gefahren in zielgerichteten Phishing-Attacken und in Insider-Bedrohungen (51 %). Aber auch die Sicherheit von in der Cloud gespeicherten Daten sehen viele kritisch (38%). Dennoch vertrauen mehr als zwei Drittel (72%) auf die Sicherheitsmaßnahmen ihres Cloud-Providers. *chk*

Die Veröffentlichung der Untersuchung finden Sie in drei Teilen unter den folgenden Links:

- **Einbindung von Privileged Account Security in DevOps-Prozesse**
- **Sichtweise von Führungskräften auf die IT-Sicherheit**
- **Unternehmensaktivitäten rund um Privileged Account Security und Endpunktsicherheit**

Sicherheit für Smartphone und Tablet

Die Nutzung von Smartphones und Tablets ist in Unternehmen mittlerweile an der Tagesordnung. Doch häufig entstehen Probleme, wenn mobile Endgeräte sowohl für berufliche Aufgaben als auch privat verwendet werden. Die geltenden Compliance-Vorgaben und IT-Sicherheitsrichtlinien einzuhalten, kann dann für Unternehmen zur echten Herausforderung werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nennt verschiedene Lösungsmöglichkeiten: Im einfachsten Fall könne auf den Geräten eine Applikation installiert werden, die einen Datencontainer mit allen dienstlichen Daten und Zugängen verwaltet. Diese Applikation müsse für sämtliche dienstliche Tätigkeiten ausgelegt sein, einen eigenen Browser beinhalten und selbsttätig eine verschlüsselte Verbindung zur Institution aufbauen. Als weitere Möglichkeit, private und dienstliche Bereiche auf Endgeräten zu trennen, schlägt das BSI vor, die Informationen auch bei der Verarbeitung auf den Unternehmens-Servern zu belassen. Dann könne über eine abgesicherte Netzverbindung die Anwendung auf einem Server der Institution bedient werden. Das entsprechende Programm auf dem Endgerät muss dabei so konfiguriert werden, dass die Daten nicht lokal gespeichert werden können. Diese Lösung setzt allerdings bei jeder Nutzung eine ausreichende Internetverbindung voraus. Schließlich könnten der private und der berufliche Bereich auch als unterschiedliche virtuelle Maschinen auf einem Gerät betrieben werden. Anders als bei der Lösung über eine Datencontainer-Variante werden die Bereiche nicht auf Anwendungsebene, sondern auf Betriebssystemebene getrennt. *chk*

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
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: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, thyssenkrupp Steel Europe AG; Ralf Brandt, divieni patch Beteiligungs 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 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

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 2.0 – Chance und Risiko

Die Digitalisierung ist nicht mehr aufzuhalten und hat mittlerweile sämtliche Bereiche der Wirtschaft erfasst. Sie stellt Unternehmen und insbesondere auch Rechts- und Compliance-Abteilungen vor große Herausforderungen, bietet aber auch ungeahnte Chancen. Zugleich wird das regulatorische Umfeld immer komplexer und Verstöße gegen rechtliche Vorgaben immer risikoreicher. Compliance ist das Gebot der Stunde.

Unsere Konferenz widmet sich den Schnittstellen dieser beiden Mega-Trends. So werden von führenden Experten ausgewählte Compliance-Themen der Digitalisierung beleuchtet – Cybersecurity, die DSGVO und die neuen verbraucherschutzrechtlichen Kompetenzen des Bundeskartellamts in der digitalen Wirtschaft. Aber auch die Erleichterungen, die die Digitalisierung in der Form von Legal Tech bei der täglichen Umsetzung von Compliance Programmen bietet, sind Thema unserer Konferenz. Schließlich werden Vertreter der Wirtschaft, Verwaltung und Wissenschaft die Compliance-Herausforderungen der Digitalisierung in einer Podiumsdiskussion erörtern. Sie sollten diese hochkarätig besetzte Konferenz zu den großen rechtlichen Themen unserer Zeit nicht verpassen.

KLDiscovery

KLDiscovery ist weltweiter Marktführer für Services und Technologien im Bereich Ediscovery, Document Review und Computer Forensik. Mit preisgekrönter Review -Software und Expertenwissen als Branchenpionier unterstützen wir Unternehmen und Anwaltskanzleien bei internen Untersuchungen, Litigation/Arbitration und Due Diligence/Merger Control. In Deutschland ist das Unternehmen seit 1994 am Standort Böblingen vertreten. Das Rechenzentrum für das Datenhosting befindet sich in Frankfurt/Main.

www.kldiscovery.com

Veranstaltungsort:

Taylor Wessing
Benrather Str. 15
40213 Düsseldorf

Teilnahmegebühr:

349,00 Euro (zzgl. MwSt.) Abonnenten K&R, CB, Ri, DSB
499,00 Euro (zzgl. MwSt.) Normalpreis

Die Teilnahmegebühr bitten wir nach Erhalt der Rechnung zu überweisen.

Rabatte:

So sparen Sie intelligent:

Frühbucherrabatt
5 % bis Buchung zum 28. Februar 2018.

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

Anmeldeschluss:

Eine frühzeitige Anmeldung wird empfohlen, Anmeldeschluss ist der 18. April 2018.

Stornierung:

Die Anmeldung ist übertragbar. Bei Stornierung bis zum 30. März 2018 (Eingangsdatum) wird eine Bearbeitungsgebühr von 50,00 Euro zzgl. MwSt. erhoben. Danach ist die volle Teilnahmegebühr zu entrichten.

Hotelempfehlung:

Me and all Hotel
Immermannstr. 23
40210 Düsseldorf
Tel. 0211/542590

Das Carls Hotel
Benrather Str. 7a
40213 Düsseldorf
Tel. 0211/90993100

Leonardo Royal Hotel
Graf-Adolf-Platz 8-10
40213 Düsseldorf
Tel. 0211/38490

Weitere Informationen:
Wir sind berechtigt, unsere Veranstaltungen aus wichtigem Grund abzusagen oder zeitlich zu verlegen, insbesondere bei unzureichender Teilnehmerzahl oder Absage bzw. Erkrankung der Referenten. Die Teilnehmer werden hiervon umgehend schriftlich oder per E-Mail in Kenntnis gesetzt. Bereits gezahlte Gebühren werden zur Teilnahme an anderen Veranstaltungen gutgeschrieben oder zurückerstattet. Ein weiterer Schadensersatzanspruch besteht nicht, außer in Fällen von Vorsatz und grober Fahrlässigkeit.

zurück per Fax: 069 7595 1150

Name/Vorname

Kanzlei/Firma

Straße

PLZ/Ort

Telefon E-Mail

K&R, Ri, CB oder DSB Kundenummer

Datum/Unterschrift

Sie haben noch kein Abo?

Ich möchte
❑ die K&R (für € 447,99 inkl. MwSt und Versandkosten)

❑ die Recht innovativ (für € 259,00 inkl. MwSt und Versandkosten)

❑ den Compliance Berater (für € 489,00 inkl. MwSt und Versandkosten)

❑ den DATENSCHUTZ-BERATER (für € 300,00 inkl. MwSt. und Versandkosten)

im jährlichen Abonnement beziehen.

Kontakt
Deutscher Fachverlag GmbH · Torsten Kutschke · Gesamtverlagsleiter Fachmedien Recht & Wirtschaft
Mainzer Landstraße 251 · 60326 Frankfurt · Tel: 069 7595 1151 · Fax: 069 7595 1150 · Torsten.Kutschke@dfv.de