Compliance

Die Zeitschrift für Compliance-Verantwortliche

Oktober 2020

Inhalt

©Schaeffler Group

Aufmacher

DCK 2020: Schaeffler Group setzt auf Integrität in der Unternehmenskultur

Einen anschaulichen Praxisbericht lieferte Dr. Dietmar Deffert, Regional Chief Compliance & Security Officer Europa bei der Schaeffler Group, anlässlich der Deutschen Compliance Konferenz 2020 am 16. September. „Auf dem Weg von regelbasierter Compliance zu einer Integritätskultur" lautete das Thema seines (ersten) Erfahrungsberichts über das Compliance-Projekt „Horizon Next".

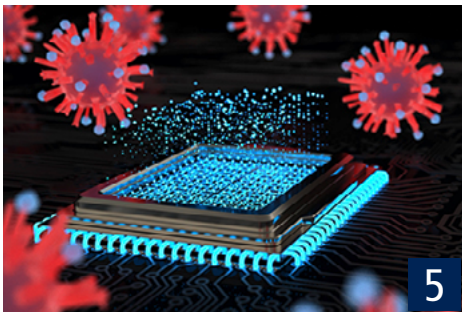
Praxis

© imago images / Panthermedia

Datenschutz zwischen EU und USA: Weder sicherer Hafen, noch Privatsphäre-Schild

Nach einem aktuellen Urteil des Europäischen Gerichtshofs dürfen ab sofort personenbezogene Daten nicht mehr auf Basis bestehender Regelungen in die USA übermittelt werden. In der Konsequenz sehen sich Unternehmen mit erheblichen Reputations- und Rechtsrisiken bis hin zu empfindlichen Bußgeldern und Schadensersatzansprüchen Betroffener konfrontiert.

Veranstaltung



© imago images / Alexander Limbach

Praxisseminar Cyber-Security

„Es gibt nur zwei Arten von Unternehmen: Solche, die gehackt wurden, und solche, die noch gehackt werden", sagte der ehemalige FBI-Chef Robert Mueller bereits 2012 voraus. In der Webinarreihe „Praxisseminar Cyber-Security" referieren praxisnahe Referenten über die zahlreichen rechtlichen Aspekte von Cyber-Security.

Recht

© imago images / Shotshop

Arbeitsrecht als Compliance-Bremse

Ein wichtiger Bestandteil der Compliance-Architektur ist der Mitarbeiter. Erkennt man, dass er keine tragende Säule des Unternehmens mehr ist und hat man Gesetzesverstöße festgestellt, so ist eine rasche Trennung unabänderlich. Doch diese gestaltet sich nicht immer einfach.

Veranstaltungen

16. - 20.11.2020 | **Frankfurt am Main oder via Livestream | 23. Euro Finance Week 2020**

27.10., 03.11., 09.11., 17.11.2020 | **vierteiliges Webinar | Praxisseminar Cyber-Security**

12.11.2020 | **Webinar | Datenschutz in der Praxis**

24.-26.11.2020 | **Düsseldorf oder via Livestream | Datenschutzkonferenz**

28.01.2021 | **Frankfurt am Main oder via Livestream | Praxisseminar zum Geldwäschegesetz**

DCK 2020: Schaeffler Group setzt auf Integrität in der Unternehmenskultur

Einen anschaulichen Praxisbericht lieferte Dr. Dietmar Deffert, Regional Chief Compliance & Security Officer Europa bei der Schaeffler Group, anlässlich der Deutschen Compliance Konferenz 2020 am 16. September. „Auf dem Weg von regelbasierter Compliance zu einer Integritätskultur" lautete das Thema seines (ersten) Erfahrungsberichts über das Compliance-Projekt „Horizon Next".

Schaeffler Group

Dr. Dietmar Deffert ist seit 2016 als Regional Chief Compliance & Security Officer Europa bei der Schaeffler Group tätig und betreut mit seinem Team alle operativen Compliance-Themen in der Region.

„Wir sind als globaler Industrie- und Automobilzulieferer in 50 Ländern unterwegs – auch in Ländern mit Compliance- und Risiko-Hotspots", steckte Deffert den geografischen Rahmen ab, in dem sich die Schaeffler Group mit Compliance konfrontiert sieht. Er selbst ist für Europa, die größte Region des Unternehmens, zuständig. „In der Schaeffler-Welt ist Compliance noch ein bunterer Strauß als woanders", denn außer klassischen Themen gehöre auch die Unternehmenssicherheit dazu, so Deffert.

Schaeffler sei im Compliance-Management inzwischen sehr gut aufgestellt: „Wir ticken wirklich jede Box eines effizienten Compliance-Management-Systems." Als letzten großen Meilenstein hat das Unternehmen zu Beginn des Jahres ein Due-Diligence-Projekt weltweit ausgerollt. Alle Bestandteile eines Compliance-Management-Systems seien implementiert, und auch zertifiziert und testiert. Darum stellte sich dem Compliance-Management die Frage, wo der Ansatzpunkt für eine Weiterentwicklung ist.

„Wir sehen, dass unsere Mitarbeiter das Thema verinnerlicht haben. Aber es gibt Potenzial in diesem Bereich: Verstehe ich Compliance richtig und stehe ich auch wirklich dahinter? Oder tue ich das alles nur, weil ich das muss?", fasste Deffert die Ausgangssituation zusammen.

Die Schaeffler Group hat sich dieser Thematik auf kreative Weise angenommen. Leicht sei das nicht gewesen, denn Vertrauen, Verantwortung, moralisches Verhalten – alles was in Richtung Ethik, Integrität deutet – musste angesprochen werden. Doch allein schon die Definition dieser Begriffe ist schwammig. „All das hat sehr viel mit der Einstellung des Einzelnen zu tun und kann sehr persönlich sein. Wir mussten also genau hier ansetzen: bei den Menschen."

Es habe nahe gelegen, sich in erster Linie die Führungskräfte vorzunehmen. Denn nur, was „oben" verstanden wird und funktioniert, kann auch nach unten weitergereicht werden. Dabei stand fest: „Wir wollten weg von den klassischen Schulungsthemen und dahin kommen, dass die Menschen sich inhaltlich mit dem Thema Integrität auseinandersetzen."

Die Compliance-Abteilung hat hierzu eigens eine neue Form des Workshops kreiert: „Horizon Next". „Wir wollen unsere Mitarbeiter damit nicht zu ‚besseren Menschen' erziehen", betonte Deffert. In klassischen Workshop-Formaten, die etwa drei Stunden dauern, kann jeder Compliance Officer, der einen Workshop moderiert, aus einem „bunten Potpourri" aus verschiedenen Modulen wählen. „Jeder CO nimmt aus diesem Koffer die Teile, von denen er glaubt, dass sie am besten funktionieren."

Ein Beispiel ist eine eigens entwickelte Dilemma-Situation: „Ein Sachverhalt mit fünf Personen und jeder hat etwas falsch gemacht – aber auf unterschiedlichem Niveau und mit unterschiedlicher Motivation. Dabei spielen auch kulturelle Hintergründe eine Rolle. Die Aufgabe der Teilnehmer besteht darin, in Gruppen zu diskutieren, welche dieser Personen sich am verwerflichsten verhalten hat", beschrieb Deffert. In der Gruppe sollen sich die Teilnehmer auf eine Reihenfolge der Schwere einigen. Das führe zu interessanten Diskussionen und bringe die Teilnehmer dazu, darüber nachzudenken, was für sie falsches Verhalten ist. „Hier ist der Weg das Ziel", fasste Deffert zusammen.

Ein weiteres Beispiel ist eine Intranet-Umfrage zu verschiedenen Fragen, etwa was Integrität für die Mitarbeiter bedeutet. „Die Ergebnisse können nun bei den Workshops diskutiert oder auch spielerisch aufgearbeitet werden, indem man in Anlehnung an eine frühere Fernsehshow eine Art ‚Familien-Duell' macht, z.B.: Was waren die häufigsten Antworten?"

Sogenannte Black-Stories, die auch als Gesellschaftsspiel bekannt sind, eigneten sich ebenfalls für die Workshops, so Deffert. Dabei werde das Ende einer Geschichte erzählt und dann diskutiert, wie es dazu gekommen ist. Diese eher verspielten Ansätze würden allerdings auf der Führungsebene manchmal auch skeptisch betrachtet. „Die Leute sind hier nüchterner unterwegs. Das sollte man von der Zielgruppe abhängig machen", rät Deffert.

Die Dauer der „Horizon Next"-Workshops von drei Stunden sei anfänglich nicht leicht zu vermitteln gewesen. „Das ist relativ lang, hat sich aber trotzdem mittlerweile recht gut gefügt, was vermutlich auch mit den Inhalten zu tun hat."

Die „Horizon Next"-Workshops setzt die Schaeffler Group bislang vor allem in Deutschland ein. Das Feedback sei insgesamt erstaunlich gut. Bedenken wie „zu lange, muss das sein, noch etwas Zusätzliches – wir machen ja auch unsere regulären Schulungen weiter" hätten sich nicht bewahrheitet. Vereinzelt gebe es nach wie vor die Skepsis gegenüber „Erziehung" durch das Unternehmen, was als anmaßend empfunden werde. „Aber wer den Workshop mitgemacht hat, sieht, dass das gerade nicht Ziel der Veranstaltung ist", resümiert Deffert.

„Der Fluch der guten Tat" sei indes, dass die Mitarbeiter zum Teil enttäuscht reagierten, wenn sie keinen „Horizon Next"-Workshop besuchen, sondern eine der selbstverständlich weiterhin notwendigen regulären Compliance-Schulungen absolvieren.

In Zeiten von Corona nutzt die Schaeffler Group auch die Möglichkeit „Horizon Next"-Workshops virtuell durchzuführen. „Das funktioniert mit nicht allzu großen Gruppen – mehr als acht bis zehn Leute sollten es dann nicht sein." Die bessere Variante sei aber der Austausch „face to face".

Deffert zeigte sich überzeugt von „Horizon Next": „Das ist ein wichtiger Beitrag hin zu einer von Integrität geprägten Unternehmenskultur. Aber es ist herausfordernd, allein schon, weil die Inhalte der Workshops immer weiterentwickelt werden müssen." *chk*

Die Deutsche Compliance Konferenz 2020 fand in diesem Jahr vor dem Hintergrund der Corona-Pandemie erstmals rein digital im Livestream statt. Dem anspruchsvollen Programm tat dies keinen Abbruch. Außer vielfältigen Schilderungen aus der täglichen Compliance-Praxis der Referenten wurden auch die aktuell wichtigsten Compliance-Themen behandelt. Darunter der viel diskutierte Entwurf des Verbandssanktionengesetzes mitsamt seinen Fallstricken und Auswirkungen, aber zum Beispiel auch die zunehmenden Bußgeldverfahren bei DSGVO-Verstößen. Ein Veranstaltungsbericht zur Deutschen Compliance Konferenz erscheint in der November-Ausgabe von Compliance.

Compliance Berater | Betriebs Berater | Compliance – Die Zeitschrift für Compliance-Verantwortliche

Praxisseminar zum Geldwäschegesetz

28. Januar 2021 - Frankfurt am Main

Januar 2021

Mo	Di	Mi	Do	Fr	Sa	So
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	**28**	29	30	31

Veranstaltungsort:
Gleiss Lutz
Taunusanlage 11
60329 Frankfurt am Main

Teilnahmegebühr:

Abonnenten CB/BB + Übersendung des Kaufbelegs des Kommentars GwG, Zentes/Glaab	699,- €
Übersendung des Kaufbelegs des Kommentars GwG, Zentes/Glaab	749,- €
Abonnenten CB/BB	799,- €
regulär	899,- €

Rabatte – So sparen Sie intelligent:

Frühbucherrabatt
5 % bei Buchung bis zum 02.11.2020

Mehrbucherrabatt
5 % bei Anmelden von 3 oder mehr Teilnehmern einer Institution ab dem 3. Teilnehmer

Anmeldeschluss:
Eine frühzeitige Anmeldung wird empfohlen.
Anmeldeschluss ist der 26.01.2021.

Anmeldung:
Frau Maria Belz
Deutscher Fachverlag GmbH
Mainzer Landstr. 251
60326 Frankfurt am Main
Tel.: +49 69 7595-1157
Fax: +49 69 7595-1150
E-Mail: Maria.Belz@dfv.de

Stornierung:
Die Anmeldung ist übertragbar. Bei Stornierung bis zum 08.01.2021 (Eingangsdatum) wird eine Bearbeitungsgebühr von 75,- EUR zzgl. MwSt. erhoben. Danach ist die volle Teilnahmegebühr zu entrichten.

Der Preis schließt Veranstaltungsunterlagen und die Pausenverpflegung mit ein. Die Teilnahmegebühr bitten wir erst nach Erhalt der Rechnung zu überweisen.

Anmeldung

per Mail an Maria.Belz@dfv.de
per Fax an +49 69 7595-1150
www.ruw.de/gwg

Kanzlei/Firma: _____

Name, Vorname: _____

Position: _____

Straße, Nr.: _____

PLZ, Ort: _____

Tel.: _____ E-Mail: _____

Abo-Nummer CB/BB: _____

Datum: _____ Unterschrift: _____

Ich nehme teil

- ☐ regulär
- ☐ als Abonnent CB/BB
- ☐ mit Kaufbeleg des Kommentars GwG
- ☐ als Abonnent CB/BB mit Kaufbeleg des Kommentars GwG

Jetzt gleich vorbestellen:

GwG-Kommentar, Zentes/Glaab, 2. Auflage
GeldtransferVO, relevante Vorgaben aus AO, KWG, StGB, VAG und ZAG

☐ Bitte senden Sie mir den neuen Kommentar zum GwG von Zentes/Glaab für 259,- € zu.

Datenschutz zwischen EU und USA: Weder sicherer Hafen, noch Privatsphäre-Schild

Nach einem aktuellen Urteil des Europäischen Gerichtshofs dürfen ab sofort personenbezogene Daten nicht mehr auf Basis bestehender Regelungen in die USA übermittelt werden. In der Konsequenz sehen sich Unternehmen mit erheblichen Reputations- und Rechtsrisiken bis hin zu empfindlichen Bußgeldern und Schadensersatzansprüchen Betroffener konfrontiert. Zudem berühren Verstöße auch unternehmensinterne Compliance-Vorschriften.

Privacy Shield: Auch dieses Konstrukt zur Datenübertragung zwischen der EU und den USA hat der EuGH nun zu Fall gebracht.

Mit einer Klage gegen Facebook Ireland Ltd. hatte ein österreichischer Datenschutzaktivist die gängige Praxis zum Austausch personenbezogener Daten mit den USA durch Soziale Netzwerke wie auch andere Unternehmen grundsätzlich unterbinden wollen. Seiner Auffassung nach waren personenbezogene Daten in den USA nicht ausreichend vor dem Zugriff der dortigen Sicherheitsbehörden geschützt. Daran ändere auch das zu diesem Zwecke verabschiedete Abkommen („Safe-Harbour") zwischen der EU und den USA nichts. Der Europäische Gerichtshof (EuGH) folgte dieser Argumentation und erklärte es 2015 für ungültig.

Auf der Grundlage des als Nachfolgeregelung genutzten „Privacy Shield" sowie auf Basis sogenannter Standarddatenschutz-Klauseln wurden personenbezogene Daten weiter in die USA übermittelt. Der Datenschutzaktivist klagte erneut und bekam wieder vor dem EuGH Recht. In seinem Urteil vom 16. Juli 2020 hat der EuGH den Beschluss der EU-Kommission, dass das EU-US-Datenschutzschild (Privacy Shield) ein angemessenes Schutzniveau biete, für ungültig erklärt. Dabei stützt sich der EuGH vor allem auf die weitreichenden Eingriffsbefugnisse für Sicherheitsbehörden in den USA, die nach seiner Ansicht nicht auf das zwingend erforderliche Maß beschränkt sind. Insbesondere eröffne der implementierte Ombuds-Mechanismus keine ausreichenden Rechtsschutzgarantien.

Nach dem EuGH kann eine Datenübermittlung zwar grundsätzlich weiterhin auf sog. Standarddatenschutzklauseln zwischen dem Übermittler und dem Empfänger in den USA gestützt werden. Jedoch kann es je nach der in einem bestimmten Drittland gegebenen Lage erforderlich sein, dass der Verantwortliche zusätzliche Maßnahmen ergreift, um die Einhaltung eines angemessenen, das heißt eines der DSGVO-vergleichbaren, Schutzniveaus zu gewährleisten.

Kann ein solches angemessenes Schutzniveau nicht garantiert werden, muss die Übermittlung personenbezogener Daten in die USA unverzüglich ausgesetzt bzw. beendet werden.

Die Entscheidung des EUGH bedeutet daher für Unternehmen:

1. Eine Übermittlung personenbezogener Daten in die USA ist ab sofort nicht mehr auf Basis des Privacy Shields erlaubt. Daten müssen ggf. sogar zurückgeholt werden.
2. Standardschutzklauseln als alleinige Grundlage für den Datenaustausch sind ohne zusätzliche Garantien nicht mehr zulässig. Ähnliches dürfte auch für Verbindliche Interne Datenschutzvorschriften (Binding Corporate Rules) gelten.
3. Absolute Rechtssicherheit lässt sich derzeit wohl nur durch eine ausschließliche Verarbeitung personenbezogener Daten innerhalb der EU gewährleisten – ohne Zugriff einer US Konzernmutter.

Das Urteil dürfte erhebliche Auswirkungen auf die alltägliche Arbeit in Unternehmen, nicht zuletzt in Personalabteilungen, haben. Man denke nur an Arbeitsverträge, Gehaltsabrechnungen, Vergütungsvergleiche bis hin zu Angaben der betrieblichen Altersversorgung. Dabei scheinen einfache Lösungen zur Übertragung von Daten in die USA bislang nicht in Sicht. Die erweiterten Prüfpflichten vor der Übermittlung von Daten an potenziell betroffene Dritte wie beispielsweise Dienstleister können nicht nur erhebliche Reputations- und Rechtsrisiken – bis hin zu empfindlichen Bußgeldern und Schadensersatzansprüchen Betroffener – auslösen, sondern berühren bei Verstößen auch unternehmensinterne Compliance-Vorgaben.

Dr. Jan Dörrwächter und Johannes Brinkkötter

hkp

Dr. Jan Dörrwächter ist Rechtsanwalt und seit April 2017 Senior Partner und Mitglied der Geschäftsleitung der hkp/// group. Seit seinem Wechsel aus der Industrie berät er Unternehmen unter anderem in allen Fragen der Vorstandsvergütung, aber auch zur Vergütung von Führungskräften und sonstigen Mitarbeitern einschließlich des Tarifbereichs.

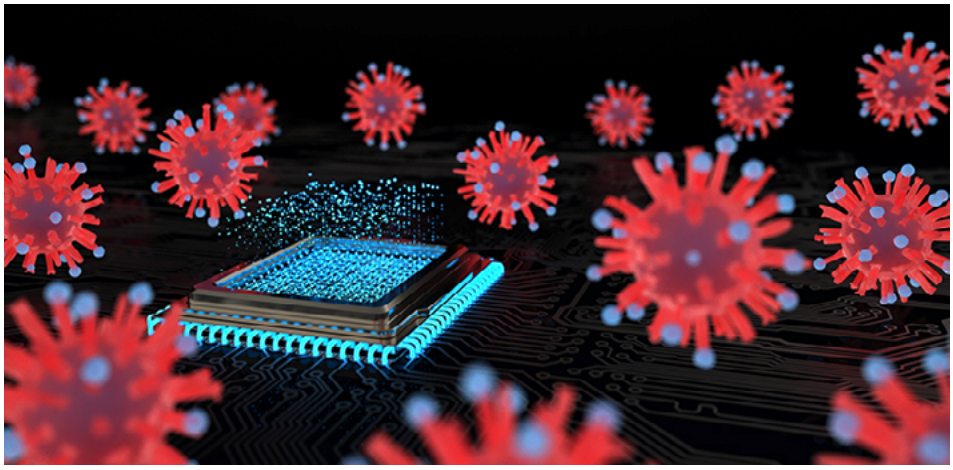
hkp

Johannes Brinkkötter ist seit Juli 2018 Partner und Mitglied der Geschäftsleitung der hkp/// group. Er zählt zu den führenden Shared Service Beratern in Deutschland und blickt auf eine themenspezifisch geprägte Laufbahn im BASF- und EON-Konzern zurück, wo er verschiedene Fach- und Führungspositionen innehatte.

Ein ausführlicher Beitrag zum Thema erscheint in der November-Ausgabe des Compliance-Beraters.

Praxisseminar Cyber-Security

„Es gibt nur zwei Arten von Unternehmen: Solche, die gehackt wurden, und solche, die noch gehackt werden", sagte der ehemalige FBI-Chef Robert Mueller bereits 2012 voraus. In der Webinarreihe „Praxisseminar Cyber-Security" referieren praxisnahe Referenten über die zahlreichen rechtlichen Aspekte von Cyber-Security – sowie über „klassische" Compliance-Materien wie Datenschutz und IT-Sicherheit.



Infektionsgefahr: Sie besteht auch virtuell und kann gravierende Folgen für Unternehmen haben.

Mit der steigenden Anzahl an Cyber-Angriffen in den vergangenen Jahren steigt auch die Notwendigkeit, auf einen solchen Vorfall vorbereitet zu sein und geeignete Reaktionen auf den Ernstfall zu kennen. In seinem aktuellen Bericht über „Die Lage der IT-Sicherheit in Deutschland 2019" benennt das Bundesamt für Sicherheit in der Informationstechnik (BSI) „Infektionen" durch Schadprogramme als eine der größten IT-Bedrohungen für Privatanwender, Unternehmen und Behörden. Darüber hinaus seien Identitätsdiebstähle an der Tagesordnung, bei denen personenbezogene Daten in hoher Anzahl missbräuchlich durch Dritte genutzt werden. „Um Cyber-Sicherheit erfolgreich gewährleisten zu können, ist die Abwehr von Angriffen der wesentliche Aspekt. Wirksamer Schutz ist aber nur möglich, wenn die allgemeine wie auch die konkrete Gefährdungslage zumindest im Überblick bekannt sind. Eine regelmäßige und gezielte Neubewertung der bestehenden Risiken ist aufgrund der dynamischen Entwicklung der Cyber-Sicherheitslage unabdingbar, um geeignete präventive und reaktive Maßnahmen auszuwählen", heißt es im BSI-Bericht.

Wie sich Unternehmen im Detail auf den Ernstfall vorbereiten können und welche rechtlichen Aspekte beim Thema Cyber-Security zu beachten sind, erfahren Sie darum in der Seminarreihe Cyber Security.

Teilnehmer des Praxisseminars können an den vier aufeinander abgestimmten Terminen am 27. Oktober, 3., 9. und 17. November per digitalem Livestream in Echtzeit das gesamte Tagungsprogramm verfolgen und im virtuellen Plenum Fragen und Anmerkungen platzieren.

Weitere Infos und den Link zur Anmeldung finden Sie hier. *chk*

Arbeitsrecht als Compliance-Bremse

Ein wichtiger Bestandteil der Compliance-Architektur ist der Mitarbeiter. Erkennt man, dass er keine tragende Säule des Unternehmens mehr ist und hat man Gesetzesverstöße festgestellt, so ist eine rasche Trennung unabänderlich. Doch diese gestaltet sich nicht immer einfach.

© imago images / Shotshop

Weggelobt: Gerade bei fristlosen Kündigungen wegen Compliance-Verstößen werden Arbeitszeugnisse häufig „gerichtlich weichgespült".

Da ist zum einen die strenge Frist des § 626 Abs. 2 BGB für die fristlose Kündigung. Ist der Arbeitgeber zunächst bemüht, trotz eines Verstoßes gegen arbeitsrechtliche Pflichten auch im Interesse des Arbeitnehmers eine außergerichtliche Lösung zu finden, so ist die Zweiwochenfrist schnell vertan. Im Zeitraum zwischen der Feststellung einer Pflichtverletzung durch einen Mitarbeiter und den Bemühungen zur friedlichen Klärung bis zur Aussprache der fristlosen Kündigung kann diese Frist schnell verstrichen sein. Das zunächst positive Bemühen um eine außergerichtliche Einigung fällt dem Arbeitgeber auf die Füße. Je nach Ausrichtung des zuständigen Arbeitsgerichtes kann der Arbeitgeber später nur selten Verständnis für die Verletzung dieser Frist erwarten.

Aus arbeitsrechtlicher Sicht mag dies im Sinne des Arbeitnehmers sein, erweist aber dem Unternehmen und seinen übrigen Mitarbeitern einen Bärendienst. Kann sich der Arbeitgeber nicht von einem Arbeitnehmer trennen, der auf die Einhaltung von Compliance pfeift, ist dies das denkbar schlechteste Zeichen an die gesamte Belegschaft. Denn die Details der arbeitsrechtlichen Auseinandersetzung werden den Mitarbeitern nur selten bekannt und nachvollziehbar sein. Es besteht die Gefahr, dass bei einem Verbleib im Unternehmen oder einer Trennung mit unangemessen hoher Abfindung der Eindruck entsteht, Compliance-Verstöße werden nicht geahndet und lohnen sich sogar.

HDH

Dr. Malte Passarge ist Rechtsanwalt und Fachanwalt für Handels- und Gesellschaftsrecht und Partner in der Kanzlei HUTH DIETRICH HAHN Rechtsanwälte PartGmbB, Vorstand des Instituts für Compliance im Mittelstand (ICM) und Geschäftsführer von Pro Honore e. V. sowie Chefredakteur des Compliance-Beraters.

Tatsächlich liegt einige irritierende Rechtsprechung vor, wonach eine Kündigung trotz Compliance-Verstößen unzulässig sei, etwa wenn ein unmittelbarer Vorgesetzter den Verstoß gegen Compliance-Vorgaben angeordnet hat. Dabei übersehen Gerichte gelegentlich, dass Strafgesetze auch für Arbeitnehmer gelten, und zwar unabhängig von einer mehr oder weniger wirksam umgesetzten Anti-Korruptions-Richtlinie.

Diese Problematik setzt sich auch nach Beendigung des Arbeitsverhältnisses fort. Neben der Frage, was die Trennung kosten soll, kommt es für den Arbeitnehmer gerade bei einer fristlosen Kündigung besonders darauf an, trotzdem ein ordentliches Zeugnis zu bekommen. Die Praxis zeigt, dass die Arbeitsgerichte gelegentlich den Arbeitnehmern ein nicht immer angemessenes Wohlwollen zum Ausdruck bringen und zum Teil der Ansicht zu sein scheinen, dass das Zeugnis allein den Arbeitnehmer betrifft. Dies mag aus Sicht des Arbeitnehmers auch so sein, jeder sollte eine zweite Chance erhalten.

Aber denken wir dies einmal zu Ende – denn Adressat des Zeugnisses ist ja der künftige Arbeitgeber. Die ausufernde Rechtsprechung zu Zeugnisformulierungen hat zu vermeintlichen Zeugnis-Codes geführt, bei denen in jede Formulierung eine besondere Bedeutung hineininterpretiert wird – die nicht immer allen Beteiligten bekannt ist. Dass jeder Arbeitnehmer stets zur vollen oder vollsten Zufriedenheit gearbeitet hat, ist schlicht absurd. Die Zeugnisse sprechen aber eine andere Sprache. Dies hat allerdings für die Allgemeinheit eine unerfreuliche Folge. Denn der künftige Arbeitgeber weiß von den Pflichtverletzungen nichts und läuft so möglicherweise die Gefahr, einen unredlichen oder gar kriminellen Mitarbeiter einzustellen. Der Altarbeitgeber will die arbeitsrechtliche Auseinandersetzung rasch beenden und sich nicht mehr um einen Zeugnistext streiten, der ihn ohnehin nichts kostet.

Tatsächlich besteht für den Altarbeitgeber das Risiko der Haftung für ein fehlerhaftes Arbeitszeugnis gegenüber dem neuen Arbeitgeber. Die Rechtsprechung stützt dies zu Recht auf §§ 311 Abs. 3, 241 Abs. 2 BGB. Doch ist die Durchsetzung eines solchen Anspruches gewiss kein Selbstgänger und nicht immer ist ein Schaden gerichtsfest darzulegen.

Jüngst hat diese Frage besondere Dramatik erlangt. So wurde der Krankenpfleger Högel aus Oldenburg, dem mehr als 300 Morde zuzurechnen sind, sowohl innerhalb der Kliniken als auch von Klinik zu Klinik mit positiven Zeugnissen weggelobt. Trotz klarer Hinweise wurden keinerlei arbeitsrechtliche Maßnahmen eingeleitet. Ein eindeutiges Vorgehen hätte Leben retten können. So auch kürzlich die Tötung eines Kindes durch eine Erzieherin in Viersen. Auch hier war die Pflegerin bereits bei vorangegangenen Arbeitgebern auffällig geworden. Dass dies Niederschlag im Zeugnis gefunden hat, ist wohl eher nicht anzunehmen.

Was folgt hieraus? Auch die Personalabteilung hat Compliance-Pflichten nicht nur gegenüber ihren ehemaligen Mitarbeitern zu beachten, sondern auch gegenüber deren künftigen Arbeitgebern. Im Interesse aller Beteiligten sollte man sich in arbeitsgerichtlichen Vergleichsverhandlungen nicht zu schnell auf eine bequeme Zeugnisformulierung drängen lassen. Wir sollten die Gerichte durchaus auf die Problematik der Haftung für ein fehlerhaftes Arbeitszeugnis nach § 311 BGB und die langfristigen Auswirkungen bequemer Vergleichsregelungen hinweisen. Vergessen Sie nicht, das nächste falsche positive Zeugnis könnte auf Ihrem Schreibtisch liegen.

Dr. Malte Passarge

IMPRESSUM

Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. DE 114139662
Geschäftsführung: Peter Esser (Sprecher), Sönke Reimers (Sprecher), Markus Gotta, Peter Kley
Aufsichtsrat: Andreas Lorch, Catrin Lorch, Peter Ruß, Angela Wisken
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: Eva Triantafillidou, Telefon: 069 7595-2713, E-Mail: Eva.Triantafillidou@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; Joern-Ulrich Fink, Central Compliance Germany, Deutsche Bank AG; James H. Freis, Jr., Chief Compliance Officer, Deutsche Börse AG; Otto Geiß, Fraport AG; Mirko Haase, Hilti Corporation; Dr. Katharina Hastenrath, Frankfurt School of Finance & Management; Corina Käsler, Head of Compliance, State Street Bank International GmbH; Olaf Kirchhoff, Schenker AG; Torsten Krumbach, Bosch Sicherheitssysteme GmbH; Dr. Karsten Leffrang, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Corpus Sireo Holding GmbH; Stephan Niermann; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, BSH Hausgeräte GmbH; Hartmut T. Renz, Citi Chief Country Compliance Officer, Managing Director, Citigroup Global Markets Europe AG; Dr. Barbara Roth, Chief Compliance Officer, UniCredit Bank AG; Jörg Siegmund, Getzner Textil AG; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG; 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, www.sk-grafik.de

2020 als Webinar
Datenschutz in der Praxis

» Donnerstag, 12. November 2020 | 10.00 - 12.00 Uhr

In Kooperation mit Linklaters

Dr. Daniel Pauly,
Linklaters LLP

Betroffenenrechte - praxisrelevante Entwicklungen in 120 Minuten

Detailgrad der Informationspflicht // Reichweite des Auskunftsanspruchs // Recht auf Kopien // Ausnahmen vom Recht auf Vergessenwerden // Umfang des Rechts auf Datenübertragbarkeit // Erkenntntisse aus Gerichts- und Verwaltungsverfahren // weitere spannende Themen

» jeweils mit praktischen Beispielen

Prof. Dr. Boris Paal,
Universität Freiburg

Format:
Im Webinar „Datenschutz in der Praxis", das dieses Jahr ausnahmsweise an Stelle der jährlichen Präsenztagung stattfinden wird, referieren Dr. Daniel Pauly und Prof. Dr. Boris Paal zu praxisrelevanten datenschutzrechtlichen Themen. Nach und während des Vortrags haben Sie die Möglichkeit, via Chatfunktion Fragen zu stellen, die sodann beantwortet werden.

Teilnahmegebühr:
139,00 Euro zzgl. MwSt.
Die Teilnahmegebühr bitten wir nach Erhalt der Rechnung zu überweisen.

Rabatte:
Frühbucherrabatt: 5 % bei Buchung bis zum 6. Juli 2020.

Anmeldeschluss:
Eine frühzeitige Anmeldung wird empfohlen. Anmeldeschluss ist der 11. November 2020.

Stornierung:
Die Anmeldung ist übertragbar. Bei Stornierung bis zum 9. Oktober 2020 (Eingangsdatum) wird eine Bearbeitungsgebühr von 25,00 Euro zzgl. MwSt. erhoben. Danach ist die volle Teilnahmegebühr zu entrichten.

Zugangsdaten:
Die Zugangsdaten erhalten Sie rechtzeitig vor der Veranstaltung per E-Mail. Bitte geben Sie Ihre E-Mailadresse unbedingt gut leserlich an.

Anmeldung

zurück per Mail an: Stephen.Hain@dfv.de
oder per Fax: 069 7595-1150

Name/Vorname

Kanzlei/Firma

Straße PLZ/Ort

Telefon E-Mail

Datum/Unterschrift

Medienpartner: DATENSCHUTZ-BERATER | Kommunikation & Recht | Compliance Berater | Betriebs Berater

Deutscher Fachverlag GmbH · Ansprechpartner: Stephen Hain
Mainzer Landstraße 251 · 60326 Frankfurt · Tel: 069 7595 2712 · Fax: 069 7595 1150 · Stephen.Hain@dfv.de

Compliance in Zeiten von #MeToo

Fälle sexueller Belästigungen sind Compliance-Vorfälle, die als ernstzunehmende Compliance-Risiken einzustufen sind.

In den letzten Jahren haben sich Organisationen vermehrt mit Diskriminierungen, insbesondere sexuellen Übergriffen, auseinandersetzen müssen. Eine maßgebliche Rolle spielt dabei die #MeToo-Bewegung als weltweite Kampagne gegen jede Form sexueller Übergriffe. Diese erlaubt den Betroffenen, aus der Opferrolle heraus zu treten und sich zu wehren. Mit dem Öffentlichmachen einhergehend verschwindet mehr und mehr das bisherige stillschweigende Tolerieren des Ausnutzens von Machtpositionen zur sexuellen Diskriminierung und Bagatellisierung solchen Verhaltens.

Vorwürfe sexueller Belästigungen können heute auf Grund der damit einhergehenden Reputationsschäden ein mit Korruption oder anderen wirtschaftskriminellen Compliance-Vorfällen (wie Betrug oder Wettbewerbsabsprachen) vergleichbares Schadenspotential entwickeln. Die prominenten Fälle von Harvey Weinstein und Fox News illustrieren dies beispielhaft: Weinstein verlor im Zuge des Skandals seine Anstellung, seine Produktionsfirma ist insolvent, er sitzt derzeit seine Gefängnisstrafe ab und ist Entschädigungs- und Vergleichszahlungen in bisher zweifacher Millionenhöhe ausgesetzt. Fox News verlor aufgrund des Skandals (zumindest vorübergehend) zentrale Werbekunden und zahlte Entschädigungen an Opfer und Aktionäre von über 110 Mio. USD.

Im Zusammenhang mit sexuellen Übergriffen am Arbeitsplatz treffen Arbeitgeber gesetzliche Vorgaben. Sowohl das Allgemeine Gleichbehandlungsgesetz (AGG in § 3 Abs. 4) für Deutschland wie das Gleichstellungsgesetz (CH-GlG in Art. 4) für die Schweiz enthalten jeweils eine spezifische Definition von sexueller Belästigung am Arbeitsplatz. Die Form sexueller Belästigung ist dabei nicht abschließend definiert. Ausschlaggebend für die Beurteilung des Verhaltens ist letztlich, ob die betroffene Person das Verhalten objektiv erkennbar als unerwünscht erlebt. Die Voraussetzung, dass das unerwünschte Verhalten die Würde der betroffenen Person verletzt oder verletzen will, wirkt dabei als objektivierendes Kriterium. Es schützt entsprechend vor Überempfindlichkeiten und Missbrauch.

© imago images / blickwinkel

#MeToo: Sexuelle Belästigung am Arbeitsplatz ist kein Kavaliersdelikt.

Arbeitgeber in Deutschland wie der Schweiz sind gesetzlich verpflichtet, ihre Mitarbeitenden an ihrem Arbeitsplatz vor sexueller Belästigung durch andere Mitarbeitende bzw. Dritte zu schützen (§ 12 Abs. 1 AGG bzw. Art. 328 CH-OR). So müssen Arbeitgeber einem glaubhaften Hinweis auf sexuelle Belästigung angemessen nachgehen, den Sachverhalt (soweit möglich) aufklären und Maßnahmen ergreifen, die weitere Belästigungen verhindern. Dazu zählt auch das Ergreifen von Sofortmaßnahmen bei weiter andauernden Belästigungen. Maßnahmen zur Prävention sind nicht zwingend gesetzlich vorgeschrieben. Diese ist Arbeitgebern allerdings dringend zu empfehlen – schon allein aus dem Grundgedanken der Schutzpflicht den Mitarbeitenden gegenüber, der äquivalenten Behandlung des Risikos vor sexuellen Belästigungen mit anderen Compliance-Risiken, und um die Möglichkeit zu wahren, sich gemäß den gesetzlichen Bestimmungen exkulpieren zu können.

Ein zeitgemäßes Compliance-Management-System (CMS) umfasst somit nicht nur die Prävention und Bekämpfung von Wirtschaftskriminalität, sondern auch die von Diskriminierungsfällen und insbesondere sexueller Belästigungen. Eine der wichtigsten präventiven Maßnahmen zum Schutz vor sexuellen Belästigungen ist das Vorleben einer wertebasierten Unternehmenskultur durch die Führungskräfte („tone from the top"). Das bedeutet, zur Sorgfaltspflicht des Arbeitgebers und seiner Führungskräfte gehört es auch, bei Diskriminierungen hinzusehen und verantwortlich zu agieren.

Weitere Maßnahmen zur Prävention und Bekämpfung von sexueller Belästigung am Arbeitsplatz umfassen insbesondere spezifische Schulungen zu sexueller Belästigung, das Ergreifen von Diversity & Inclusion-Maßnahmen zur Herstellung einer wertebasierten Unternehmenskultur, das Ausweiten der regelmäßig unternehmensintern durchzuführenden Compliance-Risikoanalyse auf die Risiken sexueller Belästigungen im Unternehmen, das Implementieren und Kommunizieren eines Hinweisgebersystems oder Meldestelle, das Erheben entsprechender Daten und ein transparenter Umgang mit dem Thema im Unternehmen.

Einem glaubhaften Hinweis auf eine sexuelle Belästigung am Arbeitsplatz muss der Arbeitgeber in angemessener Weise nachgehen, am zweckmäßigsten mittels einer internen Untersuchung. Untersuchungen von sexuellen Belästigungsfällen stellen den Arbeitgeber vor spezielle Herausforderungen: Zum einen gibt es im Unterschied zu Compliance-Vorfällen wirtschaftskrimineller Natur ein persönlich, in seiner Privat- bzw. Intimsphäre betroffenes Opfer. Der Arbeitgeber ist somit gefordert, die richtige Balance zwischen Schutz des Opfers vor weiteren Belästigungen und Schutz der beschuldigten Person vor falschen Anschuldigungen zu finden. Bestätigt die interne Untersuchung den Hinweis auf sexuelle Belästigung, so hat der Arbeitgeber die im Einzelfall geeigneten, erforderlichen und angemessenen Maßnahmen zur Unterbindung der Diskriminierung wie Abmahnung, Umsetzung, Versetzung oder Kündigung zu ergreifen.

Dr. Rita Pikó, RAin, LL.M. und Dr. Laurenz Uhl, RA, LL.M.

privat

Dr. Rita Pikó, LL.M. (Exeter), ist Rechtsanwältin und Partnerin in der Kanzlei Pikó Uhl Rechtsanwälte AG in Zürich mit Zulassungen in Deutschland und der Schweiz. Sie doziert an verschiedenen Hochschulen zu Compliance.

privat

Dr. Laurenz Uhl, LL.M. (Exeter), ist Rechtsanwalt/Fürsprecher und Partner in der Kanzlei Pikó Uhl Rechtsanwälte AG in Zürich mit Zulassungen in Deutschland und der Schweiz.

Ein ausführlicher Beitrag zum Thema ist erschienen in BB 2020, 1204-1214.

+++ NEUE WEBINARREIHE +++ NEUE WEBINARREIHE +++ NEUE WEBINARREIHE +++

Praxisseminar Cyber-Security

Cyber Attack & Data Breach – Preparedness & Response

4-teiliges Webinar: 27.10. | 03.11. | 09.11. | 17.11.

In Kooperation mit WHITE & CASE

Modul 1 | Dienstag, 27.10. | 11.00 Uhr bis 12.30 Uhr
Cyber-Security und Legal Risk Management – eine unternehmensrechtliche Kernaufgabe in Zeiten der Digitalisierung
Prof. Dr. Igor Podebrad, Group Chief Information Security Officer, Commerzbank AG
Dr. Detlev Gabel, Partner, White & Case LLP

Modul 2 | Dienstag, 03. 11. | 11.00 Uhr bis 12.30 Uhr
Cyberrisk Governance, Resilienz und Versicherbarkeit
Prof. Dr. Igor Podebrad, Group Chief Information Security Officer, Commerzbank AG
Dr. Alexander Kiefner, Partner, White & Case LLP
Christian Wirth, Partner, White & Case LLP

Modul 3 | Montag, 09.11. | 11.00 Uhr bis 12.30 Uhr
Mitarbeiterführung und Cyber-Security
Hendrik Röger, Partner, White & Case LLP
Suntka von Halen, Director, Brunswick Group

Modul 4 | Dienstag, 17.11. | 11.00 Uhr bis 12.30 Uhr
Response: Die richtige Reaktion im Ernstfall
Prof. Dr. Igor Podebrad, Group Chief Information Security Officer, Commerzbank AG
Dr. Detlev Gabel, Partner, White & Case LLP
Suntka von Halen, Director, Brunswick Group


Prof. Dr. Igor Podebrad


Dr. Detlev Gabel


Dr. Alexander Kiefner


Christian Wirth


Hendrik Röger


Suntka von Halen

Medienpartner: DATENSCHUTZ-BERATER | Kommunikation & Recht | Compliance Berater | und

Praxisseminar Cyber-Security

„Es gibt nur zwei Arten von Unternehmen: Solche, die gehackt wurden, und solche, die noch gehackt werden", sagte der ehemalige FBI-Chef Robert Mueller bereits 2012 voraus. Mit der steigenden Anzahl an Cyber-Angriffen in den letzten Jahren steigt auch die Notwendigkeit, auf einen solchen Vorfall vorbereitet zu sein und geeignete Reaktionen auf den Ernstfall zu kennen.

Praxisnahe Referenten geben Ihnen in dieser Webinarreihe einen Überblick über die zahlreichen rechtlichen Aspekte von Cyber-Security – von der Verantwortlichkeit der Geschäftsleitung für Organisation und Fortbestand des Unternehmens über „klassische" Compliance-Materien wie Datenschutz und IT-Sicherheit bis hin zu Fragen der Transaktions- und Aufsichtspraxis.

Verfolgen Sie per digitalem Livestream in Echtzeit das gesamte Tagungsprogramm und platzieren Sie im virtuellen Plenum Fragen und Anmerkungen – ganz so, als wären Sie live dabei! Teil des Referenten-Teams werden der Chief Information Security Officer einer großen Geschäftbank und eine auf Krisenintervention spezialisierte Kommunikationsberaterin einer der in diesem Bereich führenden Adressen sein.

Sie haben noch kein Abo?

Ich möchte

- ❑ den DATENSCHUTZ-BERATER
  für € 329,90 inkl. MwSt. und Versandkosten
- ❑ die K&R
  für € 524,90 inkl. MwSt. und Versandkosten
- ❑ den Compliance Berater
  für € 534,50 inkl. MwSt. und Versandkosten

im jährlichen Abonnement beziehen.

Teilnahmegebühr (zzgl. MwSt.):

Regulärer Preis 149,– €

Die Teilnahmegebühr bitten wir nach Erhalt der Rechnung zu überweisen.

Rabatte - So sparen Sie intelligent:

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

Anmeldeschluss:

Eine frühzeitige Anmeldung wird empfohlen, Anmeldeschluss ist der 26.10.2020.

Stornierung:

Die Anmeldung ist übertragbar. Bei Stornierung bis zum 12.10.2020 (Eingangsdatum) wird eine Bearbeitungsgebühr in Höhe von 25,–€ (zzgl. MwSt.) erhoben. Danach und bei Nicht-Teilnahme ist die volle Teilnahmegebühr zu entrichten.

Eine Fortbildungsbescheinigung in Höhe von 6 Stunden für Ihre berufliche Weiterbildung wird erteilt.

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.

Gabel/Heinrich/Kiefner (Hrsg.)
Rechtshandbuch Cyber-Security

- ❑ Bitte senden Sie mir das Rechtshandbuch Cyber-Security von Gabel/Heinrich/Kiefner für 98,– € (inkl. MwSt.) zu.

Anmeldung Praxisseminar Cyber-Security

» www.ruw.de/cybersecurity

per E-Mail: Vittorio.Loparco@dfv.de
oder zurück per Fax: 069 7595-1150

Name/Vorname

Kanzlei/Firma

Straße

PLZ/Ort

Telefon E-Mail

Datum/Unterschrift

Veranstalter: Deutscher Fachverlag GmbH · Ansprechpartner: Vittorio Loparco
Mainzer Landstraße 251 · 60326 Frankfurt am Main · Tel.: 069 7595-2863 · Fax: 069 7595-1150 · Vittorio.Loparco@dfv.de