ATS ALLGEMEINE TREUHAND GMBH

Ihr Navigator wird digital!*
Ab Juni 2019

Navigator

Themen, Trends und Tipps für Unternehmer

1. Quartal 2019

CSR-Berichterstattung
Ein Instrument der Unternehmenskommunikation

IT-Sicherheit
Emotet & Co. – warum Sie jetzt vorbeugen sollten

Neues Datenschutzrecht
Bei Verstößen drohen schärfere Sanktionen

Nichtfinanzielle Berichterstattung steigert den Unternehmenswert.

Ihr Navigator wird digital!*
Ab Juni 2019

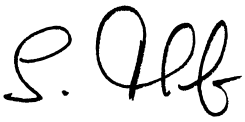
Liebe Leserin, lieber Leser,

der bekannte Satz „Tue Gutes und rede darüber“ gilt ganz besonders im Bereich der Nachhaltigkeit. Immer mehr Kunden wünschen sich nachhaltige Produkte und Dienstleistungen. Doch wie machen Unternehmen ihre entsprechenden Bemühungen sichtbar? Wir stellen mit der freiwilligen CSR-Berichterstattung ein Instrument vor, um Öffentlichkeit und Stakeholder über wahrgenommene unternehmerische Verantwortung zu informieren. Erfahren Sie, wie insbesondere Mittelständler von der nichtfinanziellen Berichterstattung profitieren können.

Emotet, Trickbot und Ryuk – immer ausgefeiltere Malware legt nicht nur Privatpersonen, sondern ganze Unternehmen lahm. Was Emotet & Co. so gefährlich macht, ist die Fähigkeit, gängige Antivirensoftware zu blockieren. Wir zeigen auf, wie Sie richtig vorbeugen.

Lesen Sie außerdem, warum Verstöße gegen das neue Datenschutzrecht künftig richtig teuer werden können. Schließlich stellen wir das mit Beginn dieses Jahres in Kraft getretene Brückenteilzeitgesetz vor.

Es grüßt Sie



StB Susanne Tschöpe
Geschäftsführung
Fachbereich Steuerberatung
E susanne.tschoepe@a-t-s.de

***PS: Bitte beachten Sie**

Auch wir übernehmen Verantwortung für unsere Umwelt. Daher: **Ihr Navigator wird digital!** Die gedruckte Ausgabe wird es in Zukunft nicht mehr geben. Wenn Sie weiterhin regelmäßig spannende Themen, Tipps und Trends aus unserem Unternehmen lesen möchten, abonnieren Sie gleich den digitalen Navigator unter **www.a-t-s.de/wissen/anmeldung/**. Ab kommenden Juni erhalten Sie dann automatisch die aktuelle Ausgabe im umweltfreundlichen PDF-Format von uns.

INHALT

CSR-Berichterstattung S. 4–6
IT-Sicherheit S. 7–8
Brückenteilzeitgesetz S. 9
Datenschutz S. 10

Nutzen Sie freiwillige CSR-Berichterstattung als Instrument der Unternehmenskommunikation

Das Thema Nachhaltigkeit ist in aller Munde. Dabei ist der Begriff Nachhaltigkeit trotz seines inflationären Gebrauchs weitgehend unbestimmt. Viele Menschen verbinden damit die Reduktion von CO_2-Emissionen und das Einsparen von natürlichen Ressourcen. Doch der Begriff Sustainability, der im englischsprachigen Raum in diesem Zusammenhang verwendet wird, schließt auch unternehmerische Gesellschaftsverantwortung (Corporate Social Responsibility – CSR) und somit viele weitere Aspekte, wie den Umgang mit Arbeitnehmern, die Umweltverträglichkeit des eigenen Produkts, Korruptionsbekämpfung oder die Stärkung der Menschenrechte mit ein.

Viele Unternehmen setzen auf ein nachhaltiges Wirtschaften, weil sie rücksichtsvolles Handeln als selbstverständlich ansehen. Sie achten daher verstärkt darauf, vornehmlich mit Geschäftspartnern zu handeln, die ein ähnliches Interesse an einer verantwortungsvollen Erbringung von Dienstleistungen und Produkten haben wie sie selbst. Auf der anderen Seite finden sich auch zahlreiche Kunden, die ein stärkeres Bewusstsein für nachhaltig hergestellte Produkte entwickelt haben und deshalb bereit sind, hierfür einen höheren Kaufpreis zu bezahlen.

Damit Sie als Unternehmer diesen immer größer werdenden Interessentenkreis erreichen und über die von Ihnen wahrgenommene ökonomische, ökologische und soziale Verantwortung informieren können, benötigen Sie einen transparenten Zugang zu den Stakeholdern Ihres Unternehmens.

Doch wie erreichen Sie diese am effizientesten? Die Antwort lautet: durch CSR-Berichterstattung.

Diese wird aktuell vor allem mit großen börsennotierten Kapitalgesellschaften und Kreditinstituten in Verbindung gebracht. Doch schon seit vielen Jahren nutzen auch mittelständische und familiengeführte Unternehmen eine freiwillige CSR-Berichterstattung als zusätzliches Instrument ihrer Unternehmenskommunikation.

Vorteile der freiwilligen Bereitstellung nichtfinanzieller Informationen

Durch CSR sollen im Rahmen der Publizität nichtfinanzielle Bezüge des Unternehmens, insbesondere zur Umwelt und zu seinen Mitarbeitern, aufgezeigt werden. Dadurch wird auch der Unternehmenswert gesteigert, da nachhaltiges Wirtschaften für eine langfristige Ressourcenerhaltung steht.

Diese Aspekte sind aber nicht nur großen kapitalmarktorientierten Unternehmen vorbehalten, sondern spiegeln auch die Werte vieler kleiner und mittelständischer Unternehmer wider. Anders als die großen Gesellschaften, sind die meisten Unternehmen jedoch nicht verpflichtet, über CSR-Belange zu berichten, obgleich ein Großteil von ihnen diese jedoch sicherlich umsetzen und beispielsweise durch ISO-Zertifizierungen viel Aufwand betreiben, um das eigene unternehmerische Handeln nachhaltig zu gestalten. Die Informationen dazu finden sich jedoch oft nur sehr verstreut auf der eigenen Homepage wieder.

Mit einer zentralen CSR-Berichterstattung können Sie der Öffentlichkeit die Möglichkeit bieten, sich schnell und übersichtlich über das Verantwortungsbewusstsein Ihres Unternehmens zu informieren. Dieses Mittel der Darstellung wird in Ländern wie Großbritannien, den USA, den Niederlande oder Australien bereits seit vielen Jahren genutzt, um Kunden, Mitarbeiter, potenzielle Investoren und Geschäftspartner ▸

über das eigene Handeln zu informieren und eine aktive Abgrenzung gegenüber dem Wettbewerb zu erreichen.

Rahmenwerk ist wichtig

Eine freiwillige CSR-Berichterstattung kann die unterschiedlichsten Ausprägungen haben, da sie keinen gesetzlichen Vorgaben unterliegt. Es ist jedoch zu empfehlen, sich an ein Rahmenwerk zu halten. Ohne diesen Rahmen läuft das Unternehmen Gefahr, sich in Detailfragen zu verlieren und das Ziel der CSR-Berichterstattung nicht mehr im Blick zu behalten, nämlich, die Stakeholder durch eine fokussierte und prägnante Berichterstattung über die eigene Wahrnehmung der unternehmerischen Verantwortung zu informieren. Unstrukturierte Hochglanzbroschüren mit wenig aussagekräftigen Werbetexten wirken in diesem Zusammenhang eher kontraproduktiv.

Die beiden in Deutschland gebräuchlichsten Rahmenwerke sind die GRI Sustainability Reporting Standards (Global Reporting Initiative) und der Deutsche Nachhaltigkeitskodex (DNK). Beide Konzepte sind empfehlenswert, da die Leistungsindikatoren vergleichbar, konsistent und messbar sind. Außerdem werden hierdurch die Anforderungen an Transparenz- und Informationsbedürfnisse des Adressatenkreises erfüllt.

PRAXISHINWEIS

Die erstmalige Erstellung eines Berichtskonzepts und die daraus folgende Aufstellung eines Nachhaltigkeitsberichts sind eine nicht zu unterschätzende Herausforderung. Mit unserer Erfahrung sowohl aus der freiwilligen als auch aus der gesetzlich vorgeschriebenen CSR-Berichterstattung können wir Ihnen in allen Phasen des Reportings mit Rat und Tat zur Seite stehen.

Unser Serviceangebot reicht dabei von der Erstellung eines umfänglichen Berichts- und Nachhaltigkeitskonzepts bis hin zur gezielten Beratung in einzelnen Teilaspekten. Eine freiwillige Prüfung der von Ihnen erstellten Nachhaltigkeitsberichterstattung (entweder ganz oder in ausgewählten Teilaspekten) erhöht die Aussagefähigkeit und Glaubwürdigkeit und fördert die Wahrnehmung am Markt. Auch hier können wir Sie unterstützen.

Wir beraten Sie gerne über unser Serviceangebot und erstellen ein individuell auf Sie zugeschnittenes Konzept. Sprechen Sie uns an!

WP/StB Niclas Rauscher

WP/StB Manuel Selchow

Sheridan Kindler

Emotet & Co.: Jetzt richtig vorbeugen

Emotet, Trickbot und Ryuk – dieses Dreiergespann legt nicht nur Privatpersonen, sondern ganze Unternehmen lahm. Aufgrund seiner Fähigkeit, andere Schadsoftware nachzuladen und gängige Antivirenlösungen zu deaktivieren, zählt Emotet wohl zur bisher kostspieligsten und zerstörerischsten Malware. Auch das Bundesamt für Sicherheit in der Informationstechnik hat bereits mehrere Sicherheitswarnungen herausgegeben.

Warum ist Emotet so gefährlich?

Ist ein System erst mit Emotet infiziert, versucht die Schadsoftware, sich im gesamten Netzwerk zu verbreiten. Dazu werden eine Reihe unterschiedlicher Angriffsvektoren ausgenutzt – mitunter die als EternalBlue bekannte Windowsschwachstelle und sogenannte Brute-Force-Angriffe. Bei Letzteren wird eine Passwortliste systematisch abgearbeitet, um erweiterte Systemrechte zu erhalten. Um dies unbemerkt tun zu können, werden gängige Antivirenprogramme deaktiviert, der Windows-Defender wird sogar gänzlich gelöscht. Ist mindestens einer der Angriffe erfolgreich, werden neue Module von infizierten Servern nachgeladen, die speziell auf das System angepasste Aufgaben erfüllen. So werden sogenannte Backdoor-Programme installiert, die es Hackern direkt ermöglichen, auf die Systeme zuzugreifen. Anmeldedaten des Windows-Systems können gesammelt, Bankdaten abgegriffen und weitere Spam-E-Mails an ausgelesene Kontaktlisten versendet werden, teils sogar von der eigenen E-Mail-Adresse. Hinzu kommt das Nachladen weiterer Schadsoftware, wie etwa des Trojaners Trickbot und der Ransomware Ryuk.

Dabei ist die Infektion selbst nur schwer zu erfassen, da Module, die nicht mehr benötigt werden, sofort gelöscht werden und schadhafter Code in Systemdateien versteckt wird. Aufgrund seiner polymorphen Struktur kann Emotet auch von signaturbasierten Antivirenlösungen nur schwer erkannt werden. Laut einer Studie von Malwarebytes werden die Module serverseitig so oft geändert, dass zwei Infektionen niemals identisch sind. Schließlich ist die Schadsoftware äußerst persistent und übernimmt Hintergrundprozesse, welche selbst nach einer erfolgreichen Bereinigung des Systems Emotet erneut nachladen. Daher auch die Empfehlung des BSI, infizierte Systeme komplett neu zu installieren.

Ein Vorfall aufgrund einer Emotet-Infektion kann laut BSI einen Schaden in Millionenhöhe auslösen.

Worauf hat Emotet es abgesehen?

Emotet bleibt eine Gefahr, da die Malware ständig weiterentwickelt wird. Ursprünglich war die Malware ein Banking-Trojaner und auf das Abgreifen von sensiblen Zugangsdaten zu Bankkonten spezialisiert. Seit der Spam-Mail-Welle 2018 wurde er jedoch um die oben beschriebenen Module erweitert und wirkt nun vielmehr als Verteiler und Wegbereiter für weitere Bedrohungen, wie Trickbot und Ryuk. Trickbot war ursprünglich ebenfalls ein Banking-Trojaner, der nun aber um Module erweitert wurde, welche die vollständige Kontrolle über ein infiziertes System ermöglichen und Daten aus FTP-Verbindungen, Browserhistorien und insbesondere aus Outlook abgreift. Ryuk hingegen ist wie die 2017 aus den Schlagzeilen bekannte Schadsoftware WannaCry eine sogenannte Ransomware, welche ganze Dateisysteme verschlüsselt und diese erst nach Zahlung eines Lösegelds in Form der Kryptowährung Bitcoin wieder entschlüsselt. Das perfide an Ryuk ist, dass gezielt nach Backups gesucht wird und diese gelöscht werden. Ryuk konnte so nach Angaben des Nachrichtenmagazins „Der Spiegel“ bereits umgerechnet über zwei Millionen Euro „erwirtschaften“, wobei die Dunkelziffer wohl viel höher liegt.

Was muss bei einem Befall getan werden?

Im Ernstfall empfiehlt es sich, befallene Rechner sofort zu isolieren, nicht herunterzufahren und nicht auszuschalten. Sollten im Nachgang forensische Untersuchungen stattfinden, um beispielsweise den Diebstahl von personenbezogenen Daten, Unternehmensgeheimnissen oder anderen sensiblen Daten zu bestätigen oder zu widerlegen, würden wichtige Indizien und Informationen verlorengehen. Eine solche Untersuchung kann im Rahmen der EU-Datenschutz-Grundverordnung, der BSI-Kritisverordnung, vertraglicher Vereinbarungen oder weiterer Vorschriften notwendig sein. Im nächsten Schritt sind alle Verbindungen nach außen zu trennen, damit die Schadsoftware keinen weiteren Code nachladen kann. Gleichzeitig sollten auch alle Netzwerksegmente voneinander getrennt werden, um eine weitere Ausbreitung zu verhindern. Wenden Sie sich im Zweifel an das BSI oder an ein Incident-Response-Team. ▶

PRAXISHINWEIS

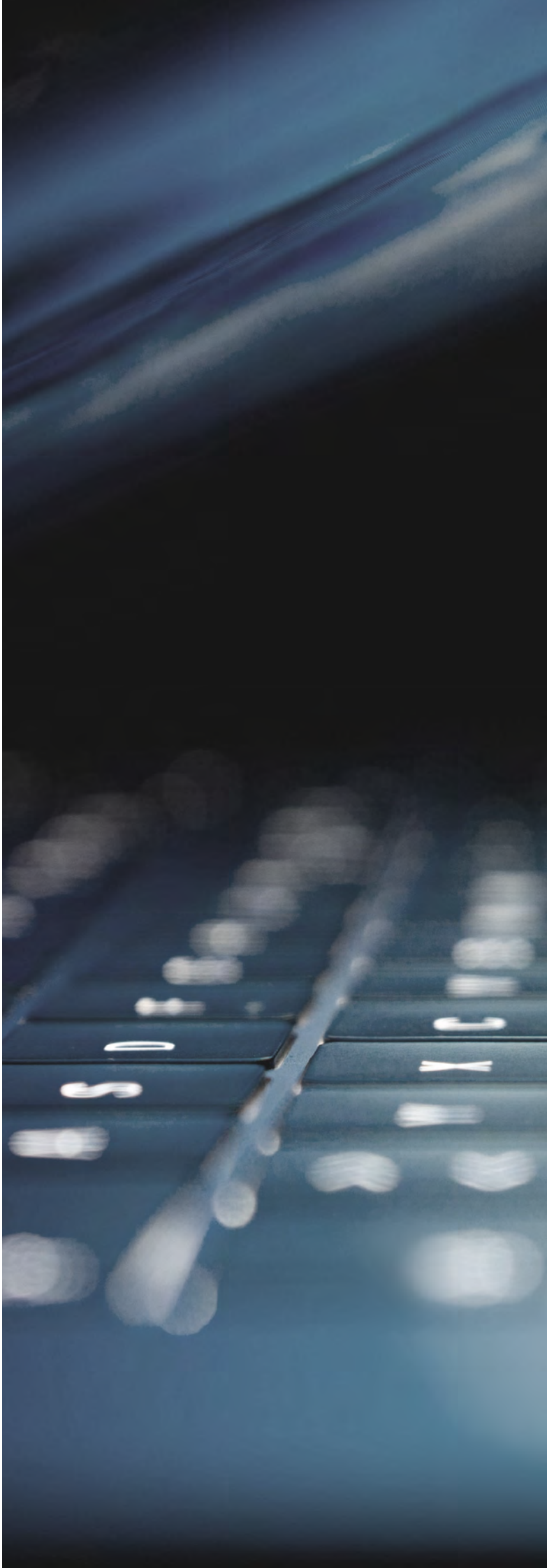
Emotet & Co. werden ständig um neue gefährliche Funktionen erweitert und bleiben damit eine ständige Gefahr auch für Unternehmen. Um Nachteile für den Betrieb zu verhindern, sollten beispielsweise folgende Sicherheitsmaßnahmen umgesetzt werden:

- Auf allen Servern und End-Points sind aktuelle Antivirenlösungen zu betreiben.
- Auf allen Systemen ist ein aktueller Update- und Patchstand unerlässlich.
- Es ist ein aktives Firewall-Logging zu implementieren, welches auch ausgehende Verbindungen überwacht.
- Mitarbeiter sind durch jährliche Schulungen für die Gefahren zu sensibilisieren.
- Es sollten Intrusion-Detection-Systeme eingesetzt werden, die auffälligen Netzwerkverkehr überwachen.
- Eine Netzwerksegementierung sollte implementiert werden, wobei die Netzübergänge durch eine Firewall überwacht werden.

Wir verfügen über eine umfassende Expertise im Bereich IT-Security und Incident Response. Gerne unterstützen wir Sie bei Cyber Vorfällen, sowie bei der Umsetzung von Maßnahmen zur Gefährdungsreduzierung.

Helmut Brechtken

Chris Lichtenthäler



Ihr Navigator wird digital!*
Ab Juni 2019

Neuer gesetzlicher Rückkehranspruch zur Vollzeit

Zum Beginn dieses Jahres ist § 9a des Teilzeit- und Befristungsgesetzes (TzBfG) in Kraft getreten, der die „Brückenteilzeit“ einführt. Danach haben Arbeitnehmer grundsätzlich einen motivationsunabhängigen Anspruch auf Verringerung der Arbeitszeit für einen Zeitraum von ein bis fünf Jahren. Nach Ablauf des beanspruchten Zeitrahmens erfolgt eine automatische Rückkehr zur vertraglich vereinbarten (Voll-)Arbeitszeit.

Die „Teilzeit“ stellt somit die Brücke zwischen den beiden „Vollzeiten“ dar. Der Arbeitgeber muss sicherstellen, dass der Arbeitnehmer mit Ablauf der zeitlich begrenzten Teilzeit zu seiner ursprünglich vertraglich vereinbarten Arbeitszeit zurückkehren kann. Um ausufernde Teilzeitanträge und folglich wirtschaftliche Risiken der Arbeitgeber aufgrund des Vorhaltens von Vollzeitarbeitsplätzen für „Rückkehrer“ zu vermeiden, enthält § 9a TzBfG Arbeitgeberschutzmechanismen.

Zum Schutz vor wirtschaftlicher Überlastung von Kleinstunternehmen besteht ein Anspruch auf „Brückenteilzeit“ erst, wenn der Arbeitgeber in der Regel mehr als 45 Arbeitnehmer beschäftigt. Des Weiteren bestehen in Unternehmen mit 45 bis 200 Mitarbeitern abgestufte Höchstzahlen für Arbeitnehmer, die zur selben Zeit „Brückenteilzeit“ beanspruchen können. Bei Erreichen der Grenze kann der Arbeitgeber weitere Anträge ablehnen.

Darüber hinaus können Arbeitgeber weiterhin Teilzeitbegehren aus betriebsbedingten Gründen entsprechend der bisherigen Regelung zur unbefristeten Teilzeit zurückweisen. Ferner kann ein Arbeitnehmer, dessen Antrag auf Teilzeit zu Recht abgelehnt wurde, erst nach Ablauf einer Sperrfrist erneut einen Antrag auf „Brückenteilzeit“ stellen.

Neuregelung stellt Arbeitgeber künftig vor weitere Herausforderungen

Arbeitsplatzkontingente müssen über einen längeren Zeitraum vorgehalten werden. Zugleich müssen die Unternehmen ihre wirtschaftliche Leistungsfähigkeit während der Abwesenheit der Arbeitnehmer sicherstellen und dabei gewährleisten, dass zu dem Zeitpunkt, wenn der Arbeitnehmer in „Brückenteilzeit“ automatisch wieder in Vollzeit zurückkehrt, keine Überbesetzung eintritt. Dies wird durch flexible Personaleinsatzplanung und vermehrten Einsatz befristeter Arbeitsverhältnisse in Teilzeit ermöglicht, was angesichts der aktuellen Arbeitsmarktsituation eine weitere Herausforderung für Arbeitgeber sein dürfte.

Fazit

Es wird sich zeigen müssen, welche Relevanz der neue Anspruch neben den weiter bestehenden Teilzeitansprüchen in der betrieblichen Praxis erlangen wird. Die Eintrittsschwelle ist mit der „Kleinstunternehmerklausel“ ungewöhnlich hoch gesteckt worden. Eine Regelung über das Verhältnis zu anderen Teilzeitansprüchen fehlt und wird zu rechtlichem Klärungsbedarf führen. Den Arbeitsvertragsparteien ist zu empfehlen, von ihrer Dispositionsfreiheit Gebrauch zu machen und die „Brückenteilzeit“ vertraglich eingehend zu regeln; außerdem ist es ratsam, in den Arbeitsverträgen durch Leistungsbestimmungsrechte des Arbeitgebers Vorsorge zu treffen, um Leistungslücken und langwierige Streitigkeiten auszuschließen.

RA Kathrin Reitner

RA Marc Schwarz

Neues Datenschutzrecht: Unternehmen müssen bei Verstößen mit hohen Geldbußen rechnen

In Frankreich ist Google eine Geldbuße in Höhe von 50 Millionen Euro auferlegt worden, weil der Konzern gegen die EU-Datenschutz-Grundverordnung (DSGVO) verstoßen haben soll. Es ist das erste Mal, dass eine europäische Behörde einen globalen Internetkonzern auf Basis der DSGVO bestraft – auch wenn Google dagegen in Berufung gegangen ist.

In Deutschland wurden bisher nur vereinzelt Geldstrafen verhängt, doch jetzt scheint auch hierzulande die Schonfrist abgelaufen. Viele Landesdatenschutzbeauftragte haben in der „Umstellungsphase" primär auf Beratung und weniger auf Sanktionen gesetzt. Denn Beratungen galten in dieser Phase zunächst als zielführender und Sanktionen eher als hemmend, wenn es darum gehe, dass Unternehmen ihr Datenschutzmanagement anpassten. Ein weiterer Grund für die derzeit noch überschaubare Anzahl an Bußgeldbescheiden ist laut dem Landesbeauftragten für den Datenschutz in Baden-Württemberg die Tatsache, dass die Aufsichtsbehörden einen gewissen Vorlauf benötigten. Denn solche Bußgeldverfahren sind häufig komplex und in weniger als drei bis vier Monaten nicht abzuwickeln. Zukünftig werden Bußgelder regelmäßig verhängt, in größerem Umfang und auch mit höheren Beträgen. Ein fünfstelliges Bußgeld wird keine Seltenheit mehr sein und auch Gerichte müssen lernen, mit ungewöhnlichen Bußgeldhöhen, beispielsweise in Millionenhöhe, umzugehen.

Dies bestätigt auch eine Umfrage des „Handelsblatts" unter den Datenschutzbeauftragten der Länder; danach laufen derzeit „sehr viele" weitere Bußgeldverfahren. Die Aufsichtsbehörden recherchieren im Internet oder kontrollieren vor Ort. Der Landesdatenschutzbeauftragte von Rheinland-Pfalz plant laut „Handelsblatt" derzeit „exemplarische Umfrageaktionen" und „eine Phase stichprobenhafter Prüfungen und Untersuchungen" und bei festgestellten Defiziten „eine verstärkte Nutzung der Abhilfebefugnisse". Zugleich machen zahlreiche Betroffene bei den Aufsichtsbehörden auf Probleme aufmerksam. Dadurch hat sich etwa in Sachsen die Zahl der Beschwerden in 2018 gegenüber 2017 verdreifacht, die Anzahl der gemeldeten Datenpannen hat sich in Baden-Württemberg sogar verzehnfacht.

Zudem ist zu berücksichtigen, dass Unternehmen zukünftig auch vermehrt Schadenersatzklagen ausgesetzt sein werden. Denn mit dem neuen Datenschutzrecht besteht zusätzlich die Möglichkeit, als Betroffener einen immateriellen Schaden geltend zu machen. Zusätzlich können Verbraucherverbände nun auch Verbandsklagen oder Musterfeststellungsklagen erheben. In allen Fällen geht es um Schmerzensgeld, dass in seiner Höhe zunächst einmal unbegrenzt ist. Und gerade dort, wo der Schadensersatzklage ein Bußgeldverfahren vorausgegangen ist, wird die erfolgreiche Abwehr solcher Schadensersatzansprüche kaum noch möglich sein. Hiervon betroffen ist im Übrigen jedes Unternehmen, das seine Waren oder Dienstleistungen innerhalb der EU anbietet, ganz gleich, wo es seinen Sitz hat.

PRAXISHINWEIS

Man kann es nicht oft genug betonen: Ein wirksames Datenschutzmanagementsystem ist für Unternehmen von zentraler Bedeutung. Unser Netzwerk steht Ihnen bei allen Fragen rund um das Thema Datenschutz mit Rat und Tat zur Seite. Ganz gleich, ob Sie Unterstützung beim Aufbau eines Datenschutzmanagementsystems benötigen, Ihr bestehendes System prüfen lassen möchten oder einen externen Datenschutzbeauftragten bestellen wollen: Unsere Experten können Sie in allen Datenschutzbelangen unterstützen.

RA Dr. Matthias Bauer

Ihr Navigator wird digital!*
Ab Juni 2019

„Seit über 50 Jahren unterstützen wir mittelständische Unternehmen sowie Freiberufler, ihre Ziele zu erreichen.“

Unsere Service-Bereiche:

· Steuerberatung
· Wirtschaftsprüfung und -beratung
· Finanz- und Personalbuchhaltung
· Existenzgründung

Impressum
Alle Angaben erfolgen nach bestem Wissen, jedoch ohne Gewähr,
und können eine umfassende Beratung im Einzelfall nicht ersetzen.
Sämtliche Bezeichnungen richten sich an alle Geschlechter.

Redaktionsstand: 03/2019

Herausgeber
ATS Allgemeine Treuhand GmbH
Buchprüfungsgesellschaft Steuerberatungsgesellschaft
Johannstraße 37
40476 Düsseldorf

T +49 211 6878 44 0
F +49 211 6878 44 50

V. i. S. d. P.: Susanne Tschöpe
E navigator@a-t-s.de

Geschäftsführung
Dipl.-Kfm. Arnd Zimmermann
Vereidigter Buchprüfer Steuerberater
Ansprechpartner Fachbereich Wirtschaftsprüfung

Dipl.-Kfm. Susanne Tschöpe
Steuerberaterin
Ansprechpartnerin Fachbereich Steuerberatung

Gestaltung
Seele und UNIMAK GmbH

ATS ALLGEMEINE TREUHAND GMBH

www.a-t-s.de