

Compliance

April 2019

Die Zeitschrift für Compliance-Verantwortliche

Inhalt



© Rudie – stock.adobe.com

Aufmacher

Datenschutz: Die Schonzeit ist vorbei

Ein Jahr nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) legen die Behörden ihre Reißhemmung ab. Obwohl noch viele Fragen ungeklärt sind, wurden in den vergangenen Wochen in Deutschland zahlreiche Bußgelder verhängt. Den Rekord hält aber noch die französische Datenschutzbehörde – er liegt momentan bei 50 Millionen Euro.

Praxis

Recht

Recht



ZHAW



Wavebreakmedia Ltd/Wavebreak Media/Thinkstock



useng/stock/Thinkstock

Die Rolle des Aufsichtsrats bei einer Compliance-gerechten Digitalisierung

Nur wenn Verwaltungs- und Aufsichtsräte die Digitalisierungsprozesse verstehen und das Tempo dieser Transformation richtig einschätzen, können sie ihre Funktionen wahrnehmen. Dabei müssen sie selbst ihre Komfortzone verlassen und sich mit der Digitalisierung auseinandersetzen, wie Martina Klee und Dr. Rita Pikó in einem Workshop anlässlich der 3. DACH-Compliance Tagung der ZHAW am 1. März in Winterthur feststellten.

Gemeinsam Verantwortliche bei der Datenverarbeitung im Konzern

Bei konzerninternen Datenverarbeitungen zwischen einzelnen Gesellschaften innerhalb eines Konzerns ist die richtige Qualifikation dieser Zusammenarbeit entscheidend, um die Compliance mit der Datenschutz-Grundverordnung (DSGVO) sicherzustellen. Vor allem stellt sich die Frage, ob die Zusammenarbeit eine Auftragsverarbeitung oder eine Verarbeitung von gemeinsam Verantwortlichen ist.

Tax Compliance: Folgenreiche Änderungen in den neuen AStBV (St) 2019

Die am 1.1.2019 in Kraft getretenen Anweisungen für das Straf- und Bußgeldverfahren (Steuer), kurz AStBV (St), 2019 beinhalten verschiedene Änderungen im Vergleich zur vorausgegangenen Fassung, die im Wesentlichen Folgen von Gesetzesänderungen sind. Die neuen Anweisungen können weitreichende Folgen für die von ihnen betroffenen Personen und Unternehmen haben.

4 Cyberangriffe in der Realität

Veranstaltungen

ANGEBOT
COMPLIANCE-BERATER: TESTLESEN PRINT

Leistungen
3 Monate gratis
+ Zugang zur Online-Datenbank

14.-16.05.2019 | Düsseldorf |
Datenschutzkonferenz

15.05.2019 | Hamburg |
7. Hanseatischer Compliance Tag

05.06.2019 | München | Food Compliance

06.06.2019 | Frankfurt a.M. |
Deutsche Compliance Konferenz

Datenschutz: Die Schonzeit ist vorbei

Ein Jahr nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) legen die Behörden ihre Reißhemmung ab. Obwohl noch viele Fragen ungeklärt sind, wurden in den vergangenen Wochen in Deutschland zahlreiche Bußgelder verhängt. Den Rekord hält aber noch die französische Datenschutzbehörde – er liegt momentan bei 50 Millionen Euro.



Schreckgespenst DSGVO: Die Behörden haben ihre Reißhemmung abgelegt und verlangen saftige Bußgelder.

Es ist kein Geheimnis: Als am 25. Mai 2018 die DSGVO wirksam wurde, war kaum ein Unternehmen Datenschutz-compliant. Entsprechend ließen die Datenschutz-Aufsichtsbehörden zunächst Milde walten, gaben sich kooperativ, halfen Unternehmen. Seit einigen Wochen hagelt es nun aber Bußgelder, auch gegen kleinere und mittlere Unternehmen, und viele Verfahren laufen noch. Die meisten Bußgelder in Deutschland sind noch mild, aber das wird nicht so bleiben. Die französische Datenschutzbehörde preschte mit einer 50-Millionen-Buße gegen Google vor, das Bundeskartellamt sieht sich ebenfalls für Datenschutz zuständig und knöpfte sich Facebook vor.



Dr. Andreas Lober und Susanne Klein, LL.M., sind Partner bei BEITEN BURKHARDT in Frankfurt. Sie sind überwiegend im Bereich IT und Datenschutz tätig und beraten zahlreiche Unternehmen in Bezug auf DSGVO-Compliance, IT-Verträge und Streitigkeiten aus dem Bereich IT.



Während zahlreiche inhaltliche Fragen noch ungeklärt sind, zeichnen sich einige Tendenzen ab. Die deutschen Datenschutzbehörden nehmen die in der DSGVO enthaltenen Dokumentationspflichten sehr ernst – ein funktionierendes Datenschutz-Compliance-Management ist hierfür essenziell. Auch die technische Sicherstellung des Datenschutzes, also die so genannten technisch-organisatorischen Maßnahmen werden von den deutschen Datenschutzbehörden hochgehalten. Neben Organisation, Dokumentation und Technik spielt die Musik aber auch im originär juristischen Bereich: Die DSGVO lässt zwar zu, Datenverarbeitungen mit einer Notwendigkeit für die Erfüllung des Vertragszwecks zu rechtfertigen. Das Bundeskartellamt schrieb Facebook aber ins Stammbuch, dass dieser Rechtfertigung Grenzen gezogen sind – die Fütterung einer „Datenkrake“ kann damit nicht über einen Vertragszweck gerechtfertigt werden, wenn dasselbe Geschäftsmodell auch weniger datenintensiv betrieben werden kann. Die französische Datenschutzbehörde wiederum begründete ihr Bußgeld gegen Google mit mangelnder Transparenz der Datenschutzerklärung.

Künftig werden die Datenschutzbehörden aller Voraussicht nach gegen Verstöße jeglicher Art noch schärfer vorgehen. Die allermeisten Verfahren werden momentan noch durch Beschwerden der Betroffenen ausgelöst, was auch in Zukunft weiter zunehmen wird. Das Bewusstsein der betroffenen Personen für Datenschutz und ihre damit zusammenhängenden Rechte ist mit der DSGVO gestiegen. Insbesondere Auskunft- und

Das sollten Sie jetzt angehen:

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

- Auftragsverarbeitungsverträge abschließen, Verzeichnis vervollständigen: Für fehlende Auftragsverarbeitungsverträge gab es bereits Bußgelder.
 - Betriebsrat als eigener Verantwortlicher? Die Frage ist ungeklärt, eine Betriebsvereinbarung kann sinnvoll sein.
 - Brexit: Datentransfer ins Vereinigte Königreich evaluieren.
 - Folgeabschätzung: Die Compliance-Organisation muss sicherstellen, dass die Frage der Notwendigkeit einer Folgeabschätzung bei neuen Verarbeitungsvorgängen geprüft wird.
 - Löschkonzepte erstellen und implementieren: Die bayerische Aufsichtsbehörde weist auf Probleme bei SAP hin.
 - Verarbeitungsverzeichnisse aktuell und vollständig zu halten, ist eine fortlaufende Herausforderung.
 - Verschlüsselung von E-Mails: Dringend gewünscht von den Aufsichtsbehörden – personenbezogene Daten in der Betreffzeile sollen vermieden werden.
 - Website-Tracking: Cookies und Tracking-Tools müssen rechtskonform sein – die bayerische Behörde prüft dies umfassend.
 - WhatsApp: Die niedersächsische Aufsichtsbehörde sieht die geschäftliche Nutzung von WhatsApp kritisch. Wenn die Nutzung essentiell ist: Rechtmäßigkeit genau prüfen, technische Lösungen (Sandbox) evaluieren.
- Die Liste ist natürlich nicht vollständig – eine konkrete Handlungsempfehlung für Unternehmen muss sich immer aus einer umfassenden Bestandsanalyse ergeben.

Löschungsanfragen von Betroffenen haben bei Unternehmen deutlich zugenommen. Auch der Gang zur zuständigen Aufsichtsbehörde ist keine Seltenheit mehr, wenn angeschriebene Unternehmen bei der Wahrung der Betroffenenrechte nicht schnell oder umfassend genug reagieren.

Aber die Behörden schauen sich auch einzelne Branchen und Themenbereiche gezielt und proaktiv an. Im Fokus der bayerischen Datenschutzbehörde stehen beispielsweise momentan die Implementierung von Löschkonzepten über SAP und der Einsatz von Tracking-Tools auf Webseiten. Vorläufiges Zwischenfazit der Behörde: Kein einziges der 40 untersuchten Unternehmen war rechtskonform.

Dr. Andreas Lober und Susanne Klein, LL.M.

Die Rolle des Aufsichtsrats bei einer Compliance-gerechten Digitalisierung

Nur wenn Verwaltungs- und Aufsichtsräte die Digitalisierungsprozesse verstehen und das Tempo dieser Transformation richtig einschätzen, können sie ihre Funktionen wahrnehmen, wie Martina Klee und Dr. Rita Pikó in einem Workshop anlässlich der 3. DACH-Compliance Tagung der ZHAW am 1. März in Winterthur feststellten.



Dr. Rita Pikó (li.), Dozentin der ZHAW School of Management, und Martina Klee (r.), Mitglied des Aufsichtsrats der Deutschen Bank AG, erläuterten die Bedeutung der Digitalisierung für den Aufsichtsrat.

„Die Digitalisierung hat einen besonderen Störfaktor, der heißt: Mensch“, stellte Dr. Rita Pikó, Dozentin an der ZHAW School of Management, gleich zu Beginn des Workshops mit Martina Klee, Mitglied des Aufsichtsrats der Deutschen Bank AG, eine provokante, aber nicht ganz unbekannte These in den Raum. Doch während bisher vor allem die Mitarbeiter im operativen Geschäft im Fokus der Digitalisierung standen, lenkten Pikó und Klee die Aufmerksamkeit auf den Verwaltungs- bzw. Aufsichtsrat. „Wer sich heute im Aufsichtsrat für das Thema Technologie und Digitalisierung nicht interessiert, ist wahrscheinlich in seinem Job falsch“, konstatierte Klee. Denn Digitalisierung sei kein Phänomen, dass sich auf bestimmte Geschäftsbereiche eingrenzen lässt.

Selbst die HR-Abteilung sei massiv gefordert, da Bewerbungsverfahren zunehmend digitalisiert werden. Da gelte es, Diversität, Gleichstellung und die Vermeidung von Günstlingswirtschaft zu beachten, führte Klee als Beispiele an: „Der Aufsichtsrat kann das alles nur im Blick behalten und seine Funktion erfüllen – also beurteilen, ob etwas compliant ist oder nicht –, wenn er die Prozesse versteht.“ Der Aufsichtsrat der Deutschen Bank hat darum einen Technologieausschuss gebildet, der regelmäßig auch Fachkollegen z.B. aus den Bereichen IT oder Compliance involviert. Klee selbst bringt einen beruflichen Background als Programmiererin mit, doch auch für sie sei es eine Herausforderung, die rasante Entwicklung der Technik mitzugehen. Die Deutsche Bank arbeitet daher mit Kompetenzprofilen. Aufsichtsratsmitglieder, die bestimmte Kompetenzen nicht erfüllen, müssen diese in Fortbildungen „nacharbeiten“, beschreibt Klee. Ein Grundverständnis für Digitalisierung verlange bereits die Arbeitsweise des Aufsichtsrats: „Wir nutzen einen gemeinsamen Datenraum, der natürlich für Dritte geschlossen ist. Das ist wie eine riesige Wissensdatenbank, an die ich gezielte Anfragen stellen kann.“ *chk*

Die 4. DACH-Compliance-Tagung findet am 6. März 2020 in Winterthur statt.



360°
ganzheitliche Ethik &
Compliance
im
#BestPracticeShowroom

Kamera ab –
Wir freuen uns auf Ihr
Wissen.

Compliance meets
Web-TV @
compliancechannel.tv

Cyberangriffe in der Realität

Manche betrachten Cybersicherheit als Synonym für IT-Security-Compliance, also der Einhaltung anerkannter Standards wie der ISO 27001 oder dem BSI Grundschutzkatalog. Ist der Compliance-Audit bestanden und das Zertifikat erteilt, sollte man als Unternehmen vor Hackern geschützt sein – könnte man meinen. Die Realität sieht allerdings anders aus, denn gute Vorgaben, Dokumentationen und unterzeichnete Risikoübernahmen halten Angreifer leider nicht aus dem Netzwerk fern. Was also können Unternehmen heute tun, um sich wirksam gegen Cyberangriffe zu schützen?



Angriffe von Internetkriminellen: Unternehmen sollten einige einfache Schutzmaßnahmen ergreifen.

Um diese Frage zu beantworten, sollten Unternehmen vor allen Dingen „unmotivierte Hacker“ in den Fokus nehmen. Also solche, die nicht ein konkretes Unternehmen im Auge haben, sondern denen es allgemein darum geht, für ihre kriminellen Machenschaften Systeme zu übernehmen, um zum Beispiel Spam zu versenden oder Schadsoftware wie Erpressungstrojaner zu verteilen. Diese Internetkriminellen machen in etwa 95% aller Angreifer aus. Durch einige sehr einfache Prinzipien kann man die Cybersicherheit bereits so weit steigern, dass man derartige Angreifer möglichst wirksam aus dem eigenen Netzwerk draußen hält:

- Inventarisierung: Viele Unternehmen sind sich heute gar nicht bewusst, welche IT-Systeme sie im Einsatz haben und wie diese genau miteinander zusammenhängen. Eine gute Inventarisierung von Hard- und Software kann dabei helfen, das Risiko

von Schwachstellen besser einzuschätzen, Fremdgeräte aus dem Netzwerk fernzuhalten und die nächsten vier Punkte wirksam zu erfüllen.

- Update/Patch Management: Nichts ist so anfällig für einen Hacker wie veraltete Software. Auf dem Markt gibt es eine Vielzahl so genannter Schwachstellenscanner, die ganze Netzwerke innerhalb kürzester Zeit auf veraltete Software und die zugehörigen Sicherheitslücken abgrasen. Derartige Software kann man sich im eigenen Netzwerk zu Nutze machen, um Schwachstellen zu identifizieren und durch entsprechende Updates abzustellen.

- Sichere Konfiguration: Um die IT sicher zu betreiben, macht es Sinn, für strategisch eingesetzte Kernsoftware (z.B. Betriebssysteme, Office-Produkte) einen Mindeststandard für die sichere Konfiguration zu etablieren.

- Berechtigungsvergabe nach Minimalprinzip: Mitarbeiter sollten stets nur über die Berechtigungen verfügen, die sie tatsächlich zur Ausführung ihrer Arbeit benötigen. Die Nutzung administrativer Benutzerkonten für normale Alltagsaufgaben sollte niemals das Mittel der Wahl sein. Auch unnötige Zugriffsberechtigungen auf eine Vielzahl von Abteilungslaufwerken sollten noch einmal überdacht werden.

- Backups: Es klingt so banal und wie eine alte Leier, aber viele Unternehmen scheitern bei der

Umsetzung ordentlicher Backup-Pläne. Sich darüber bewusst zu sein, welche IT-Systeme kritisch für den Betrieb und das geistige Eigentum des Unternehmens sind, kann dabei helfen, Datensicherungen und Zielvorgaben zu deren Wiederherstellung passend zu definieren. Auch helfen sie bei der Abwehr der mittlerweile sehr häufig vorkommenden Erpressungstrojaner.

Sind diese fünf grundlegenden Punkte ordentlich umgesetzt, ist man als Unternehmen im Hinblick auf die Cybersicherheit bereits besser aufgestellt als die meisten anderen und hat sich das Geld für die allseits beliebte ISO 27001 Zertifizierung dabei gespart.

Die Sinnhaftigkeit internationaler Standards wie der ISO 27001 soll mit diesen Worten natürlich nicht in Abrede gestellt werden. Es handelt sich dabei um ein gutes Regelwerk, das, technisch und organisatorisch gut implementiert, ebenfalls ein hohes Cybersicherheitsniveau herstellt. Nur krankt es leider häufig genau an dieser besagten Implementierung, da der Fokus bei Zertifizierungen zu stark auf die Dokumente als auf die reale technische Umsetzung gelegt wird. Und so schützt das Hochglanzzertifikat an der Wand am Ende nicht davor, selbst Opfer eines erfolgreichen Angriffs zu werden.

Holger Ahrend

Der ausführliche Beitrag von Holger Ahrend „Cyberangriffe in der Realität“ ist im **Compliance-Berater** Ausgabe 4/2019 nachzulesen. Der Beitrag beschreibt auch für „Nicht-ITler“ verständlich, welche Angriffswege genutzt werden und wie Unternehmen sich dagegen schützen können.

IMPRESSUM

Verlag

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

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

Aufsichtsrat: Klaus Kottmeier, Andreas Lorch, Catrin Lorch, Peter Ruß

Redaktion: Christina Kahlen-Pappas (verantwortlich),
Telefon: 069 7595-1153, E-Mail: christina.kahlen-pappas@dfv.de

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

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

Mitherausgeber:

BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH

Fachbeirat: Gregor Barendregt, Carl Zeiss AG, Andrea Berneis, thyssenkrupp Steel Europe AG, Ralf Brandt, divini patch Beteiligungs GmbH, Otto Geiß, Fraport AG; Mirko Haase, Hilti Corporation; Dr. Katharina Hastenrath, Frankfurt School of Finance & Management; Olaf Kirchhoff, Schenker AG; Torsten Krumbach, Bosch Sicherheitssysteme GmbH; Dr. Karsten Leffring, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Corpus Sireo Holding GmbH; Dr. Dietmar Pechtel, 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, www.SK-Grafik.de

Jede Verwertung innerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen. Keine Haftung für unverlangt eingesandte Manuskripte. Mit der Annahme zur Alleinveröffentlichung erwirbt der Verlag alle Rechte, einschließlich der Befugnis zur Einspeicherung in eine Datenbank.

© 2019 Deutscher Fachverlag GmbH, Frankfurt am Main



Holger Ahrend ist unabhängiger Cyber Security-Berater. Er hat mehr als zehn Jahre Erfahrung in der IT sowie über sieben Jahre in Security-Projekten. Durch Stationen bei Deloitte, KPMG und Accenture hat er abseits der tiefen technischen IT-Expertise das notwendige Wissen über konzernrelevante Geschäftsprozesse.

Compliance
Berater



Deutsche ComplianceKonferenz

6. Juni 2019

dfv Mediengruppe, Frankfurt am Main

Compliance der Zukunft

Die richtungsweisende Konferenz für alle Compliance Officer

5% Mehrbucherrabatt
sowie attraktive Konditionen für
CB-Abonnenten und Unternehmensjuristen!

Themen

- Wirtschaftsstrafrecht (Überblick, aktuelle Entwicklungen)
- Internal Investigation – Was kommt durch die im Koalitionsvertrag geplanten gesetzlichen Änderungen auf uns zu bzw. welche ersten Schritte hat die GroKo inzwischen eingeleitet?
- Compliance und Zertifizierung im mittelständischen Industrieunternehmen
- Erfüllung von Compliance Anforderungen im industriellen Wachstum Compliance als Schlüssel im internationalen Geschäft
- Kartellbehördliche Durchsuchung: Die ersten 48 Stunden
- Hinweisgeberstelle als zentrales und effektives Element der Compliance-Kommunikation
- Panel-Diskussion „Compliance-Kommunikation“

Philipp Blumenstein

dfv Mediengruppe | Compliance Berater
Tel.: 069 7595-2772 | Fax: 069 7595-1150
philipp.blumenstein@dfv.de

www.deutsche-compliance-konferenz.de

dfv Mediengruppe

Gemeinsam Verantwortliche bei der Datenverarbeitung im Konzern

Bei konzerninternen Datenverarbeitungen zwischen einzelnen Gesellschaften innerhalb eines Konzerns ist die richtige Qualifikation dieser Zusammenarbeit entscheidend, um die Compliance mit der Datenschutz-Grundverordnung (DSGVO) sicherzustellen. Vor allem stellt sich die Frage, ob die Zusammenarbeit eine Auftragsverarbeitung oder eine Verarbeitung von gemeinsam Verantwortlichen ist.



Auftragsverarbeitung oder nicht? Im Zweifelsfall sollten eine gemeinsame Verantwortlichkeit angenommen und die entsprechenden Verträge entworfen werden.

Als Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle zu qualifizieren, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet. Diese drei Kriterien müssen gegeben sein, damit die Stellung als Verantwortlicher angenommen werden kann. Von großer praktischer Bedeutung ist das dritte Kriterium „über die Zwecke und Mittel entscheiden“. Es ist zu identifizieren, wer der „Herr der Daten“ ist und somit in beabsichtigter Weise auf das Ergebnis und auf die Art und Weise, wie dieses Ergebnis erreicht werden kann, entscheidend einzuwirken vermag.

Der Auftragsverarbeiter ist gemäß Art. 4 Ziffer 8 DSGVO eine natürliche oder juristische Person, die Personendaten im Auftrag des Verantwortlichen oder eines weiteren Auftragsverarbeiters verarbeitet. Der Auftragsverarbeiter qualifiziert sich dadurch, dass er nur Verarbeitungen nach der strikten Anweisung des Verantwortlichen durchführt und somit so stark weisungsgebunden ist, dass er keine selbstständigen Entscheide über Zweck und Mittel der Verarbeitung treffen kann. Allerdings ist hierbei zu beachten, dass die Art. 29-Datenschutzgruppe festgehalten hat, dass die Entscheidung über die technischen und organisatorischen Mittel ohne weiteres an den Auftragsverarbeiter delegiert werden kann, solange der Verantwortliche über die wesentlichen Mittel (die sich insbesondere auf das Wie der Verarbeitung z.B. hinsichtlich Zugriffsrechten oder Speicherfristen beziehen) entscheiden kann.

Art. 26 DSGVO zufolge ist von gemeinsam Verantwortlichen auszugehen, wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke und die Mittel der Datenverarbeitung festlegen. Die Verantwortlichen müssen dazu nicht im gleichen Verhältnis mitwirken, sondern es reicht, wenn ein minimaler Beitrag an der Festlegung des Zwecks und der Mittel geleistet wird. In der Fanpage-Entscheidung des EuGH vom 5. Juni 2018 zeigt sich, dass eine gemeinsame Verantwortlichkeit nur eine geringfügige Einwirkung auf die Datenverarbeitung voraussetzt.

Im Bereich der DSGVO gibt es kein Konzernprivileg, weshalb auch hier jede Datenübermittlung zwischen den Konzerngesellschaften gesondert auf ihre Zulässigkeit zu prüfen ist. In Konzernen wird häufig einer der Konzerngesellschaften als zentrale Dienstleistungsgesellschaft durch Organisationsreglemente oder interne Weisungen die

Datenverarbeitung von Kunden- oder Mitarbeiterdaten ganz oder teilweise übertragen. Sofern eine solche Dienstleistungsgesellschaft in die Entscheidung über die Mittel und Zwecke oder Datenverarbeitung miteinbezogen oder ihr die Verfolgung eigener Interessen zugestanden wird, ist von einer gemeinsamen Verantwortlichkeit auszugehen. Von einem konzerninternen Auftragsverarbeitungsverhältnis wird man jedoch ausgehen müssen, wenn eine konzerninterne Gesellschaft nur die technischen Mittel der Datenverarbeitungen bestimmt, jedoch auf die wesentlichen Mittel und auf den Zweck der fraglichen Verarbeitungstätigkeiten keinen Einfluss hat.

Aufgrund der weitergehenden Pflichten des Verantwortlichen in der DSGVO ist es anzuraten, im Zweifelsfall eine gemeinsame Verantwortlichkeit anzunehmen und die entsprechenden Verträge zu entwerfen. Eine bei gemeinsamer Verantwortlichkeit geforderte Vereinbarung könnte folgenden Inhalt aufweisen:

- Festlegung der Zwecke und Dauer der Datenverarbeitung
- Beschreibung der Art der Personendaten und Kategorie der betroffenen Personen
- Beschreibung der Datenströme und Beziehungen zwischen den Verantwortlichen
- Beschreibung der Rechtfertigungsgründe für die Verarbeitung gemäß Art. 6 und 9 DSGVO und deren Zuteilung zu den Verantwortlichen
- Festlegung, welche Pflichten weiterhin von allen Verantwortlichen wahrgenommen werden müssen (Grundsätze der Datenverarbeitung und Rechtfertigungsgründe)
- Festlegung der Anlaufstelle für betroffene Personen
- Aufteilung der organisatorischen Erfüllung der Betroffenenrechte
- Aufteilung der externen Kommunikation mit betroffenen Personen (insb. Informationen über die Vereinbarung und über die Datenverarbeitung) und mit den Aufsichtsbehörden (ins. Datenschutz-Folgenabschätzung und Meldungen bei Datenschutzverletzungen)
- Vereinbarung über die Bestellung des Vertreters i.S.v. Art. 27 Abs. 3 DSGVO
- Vereinbarungen über die technische Ausgestaltung der Betroffenenrechte
- Vereinbarungen über die technischen Maßnahmen für die Datensicherheit und für die Maßnahmen zu Privacy by Design and by Default
- Vereinbarungen über Prozesse im Bereich der Meldungen von Datenschutzverletzungen
- Vereinbarungen über die Führung der Verarbeitungsverzeichnisse
- Vorgehen bei Datenübermittlungen in ein Drittland ohne adäquates Schutzniveau
- Gegenseitige Informationspflichten bei relevanten organisatorischen Änderungen der gemeinsam Verantwortlichen
- Vereinbarungen über die Haftung im Innenverhältnis, wenn ein oder mehrere gemeinsam Verantwortliche den gesamten Schaden beglichen haben.

Dr. Lukas Lezzi und Jutta-Sonja Oberlin



Jutta Sonja Oberlin, CIPP/E, CIPM, zertifizierte Datenschutzbeauftragte, zertifizierte Compliance Officer (Universität Augsburg), arbeitet als Unternehmensberaterin im Security Team der PWC in Zürich.



Dr. Lukas Lezzi, CIPP/E, hat in Zürich Rechtswissenschaften studiert und im Finanzmarktrecht promoviert. Er war als betrieblicher Datenschutzverantwortlicher einer großen schweizerischen Finanzmarktinfrastuktur tätig. Zurzeit bereitet er sich auf die Zürcher Anwaltsprüfung vor.

Soziale Netzwerke & Datenschutz-Grundverordnung – aktuell und praxistauglich!



Inhalt

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

Der Autor

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

Für

Betriebliche Datenschutzbeauftragte, Unternehmensjuristen, externe Datenschutzexperten, Rechtsanwälte, Mitarbeiter in Compliance-Abteilungen, Geschäftsführer und Manager, in deren Verantwortungsbereich Datenschutz und IT fallen, Unternehmen, Vereine

Ja, ich bestelle – auf www.shop.ruw.de oder per Fax unter 08581 754

Expl. **Datenverarbeitung in sozialen Netzwerken**

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

Weitere Informationen:



Name | Firma | Kanzlei

E-Mail

Straße | Postfach

PLZ | Ort

Datum | Unterschrift

Tax Compliance: Folgenreiche Änderungen in den neuen AStBV (St) 2019

Die am 1. Januar 2019 in Kraft getretenen Anweisungen für das Straf- und Bußgeldverfahren (Steuer), kurz AStBV (St), 2019 beinhalten verschiedene Änderungen im Vergleich zur vorausgegangenen Fassung, die im Wesentlichen Folgen von Gesetzesänderungen sind. Die neuen Anweisungen können weitreichende Folgen für die von ihnen betroffenen Personen und Unternehmen haben.

ueang/Stock/Thinkstock



Tax Compliance: Die neuen Anweisungen für das Straf- und Bußgeldverfahren können weitreichende Folgen haben.

Beispielsweise wurde in Nr. 136 Abs. 1 Nr. 6 AStBV eine Anweisung über die Mitteilungspflicht rechtskräftiger Verurteilungen wegen Steuerhinterziehung (§ 370 AO) an das Bundeskartellamt zum Zwecke der Eintragung in das Wettbewerbsregister aufgenommen. Diese Pflicht gilt auch bzgl. rechtskräftiger Unternehmensgeldbußen (§ 30 OWiG), wenn diesen eine Steuerhinterziehung zugrunde liegt. Dies ist auch der Fall, wenn die Unternehmensgeldbuße an eine Aufsichtspflichtverletzung (§ 130 OWiG) anknüpft, deren Anknüpfungspunkt wiederum eine Steuerhinterziehung ist.

Eine neue und über die gesetzlichen Vorgaben hinausgehende Anweisung enthält Nr. 131 Abs. 1 Satz 2 AStBV. Danach sind im Zuge einer laufenden Außenprüfung abgegebene Nacherklärungen grundsätzlich der BuStra zur Prüfung vorzulegen.

Bisher bestand und besteht nach Nr. 130 Abs. 1 und 2 AStBV eine Pflicht zur unverzüglichen Unterrichtung der BuStra und Steufa bei Vorliegen des Verdachts einer Straftat (z. B. Steuerhinterziehung nach § 370 AO) oder Ordnungswidrigkeit (z. B. leichtfertige Steuerverkürzung nach § 378

Abs. 1 AO). In Bezug auf Ordnungswidrigkeiten kann die Durchführung eines Bußgeldverfahrens und damit die Mitteilung an die BuStra und Steufa ausnahmsweise aus Opportunitätsgründen (§ 47 Abs. 1 OWiG) unterbleiben, insb. wenn das steuerliche Mehrergebnis insgesamt unter 5.000 Euro liegt (vgl. Nr. 130 Abs. 1 Satz 2 AStBV).

Zudem besteht im Falle von Nacherklärungen, die als Selbstanzeige bezeichnet oder als solche erkennbar sind, eine Pflicht der Finanzbehörde

zur Weiterleitung an die BuStra. Dies gilt insbesondere für Erklärungen, bzgl. derer Anhaltspunkte dafür vorliegen, dass zuvor eine leichtfertige Steuerverkürzung oder eine Steuerhinterziehung begangen wurde (vgl. Nr. 132 Abs. 1 AStBV).

Derartige Anhaltspunkte oder einen Verdacht sieht die nun neu eingeführte Anweisung (Nr. 131 Abs. 1 Satz 2 AStBV) in Bezug auf Nacherklärungen im Rahmen von Außenprüfungen nicht vor. Sie geht damit über die bisherigen Anweisungen weit hinaus. Die Vorlage an die BuStra erfolgt allein aus dem Umstand, dass die Nacherklärung i. R. e. Außenprüfung erfolgt ist. Zwar soll die Vorlage nur

AStBV (St) 2019

Die Anweisungen für das Straf- und Bußgeldverfahren (Steuer), kurz AStBV (St), sind, wie ihr Name es sagt, eine verwaltungsinterne Anweisung an die Finanzbehörden bzw. deren Mitarbeiter. Sie bezwecken eine einheitliche Handhabung des Gesetzes und die reibungslose Zusammenarbeit der zur Verfolgung von Steuerstraftaten und Steuerordnungswidrigkeiten berufenen Stellen. Neben der Steuerfahndung (Steufa) und den Bußgeld- und Strafsachenstellen (BuStra) haben auch alle anderen Stellen der Finanzbehörden die Vorgaben der AStBV zu beachten, jedenfalls sofern sie mit der Steufa oder BuStra zusammenarbeiten oder selbst Maßnahmen im Straf- oder Bußgeldverfahren treffen.

„grundsätzlich“ erfolgen, jedoch ist zu befürchten, dass eine Art Automatismus der Weiterleitung einsetzen wird. Die BuStra wird dann prüfen, ob es sich bei der Nacherklärung um eine bloße Berichtigung im Sinne des § 153 AO, oder aber eine Selbstanzeige nach § 371 AO (Achtung: Gefahr der Unwirksamkeit!) oder § 378 Abs. 3 AO handelt und ggf. weitere Schritte einleiten.

Die Neuregelung verdeutlicht einmal mehr die Notwendigkeit einer qualifizierten steuerlichen, aber auch steuerstrafrechtlichen Beratung, wenn der Steuerpflichtige – in Vorbereitung auf eine Außenprüfung oder während einer solchen – Fehler aus der Vergangenheit identifiziert. Dies galt und gilt auch dann, wenn zwischen dem Steuerpflichtigen und dem Außenprüfer ein vermeintlich „gutes Verhältnis“ besteht, das bereits „seit Jahren“ anhält, man also „nichts zu befürchten“ habe, da der Prüfer dem Unternehmen „wohlgesonnen“ sei. Denn nur so können Risiken rechtzeitig erkannt und ihnen durch wohl überlegtes Verhalten begegnet werden.

Timo Handel



Timo Handel ist Rechtsanwalt und Mitglied des Bereichs Wirtschafts- und Steuerstrafrecht der BEITEN BURKHARDT Rechtsanwaltskanzlei mbH in Frankfurt a. M. Er berät sowohl Unternehmen als auch Individualpersonen in sämtlichen Bereichen des Steuerstrafrechts und der Tax Compliance.

Der ausführliche Beitrag von Timo Handel „Generalverdacht in der Außenprüfung? – Neue Mitteilungsregelungen in den Anweisungen für das Straf- und Bußgeldverfahren (Steuer)“ erscheint demnächst im **Compliance-Berater**.