Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

noch immer beschäftigt die Unternehmen die Auswirkungen der Corona-Pandemie. Viele von Ihnen werden Ende Juni, Anfang Juli mit der Umstellung der Buchhaltungs- und Warenwirtschaftssysteme auf die geänderten Umsatzsteuersätze sowie der Berichtigung von Rechnungen beschäftigt gewesen sein. Trotz alle der administrativen Belastungen dieser Sondersituation sind die rechtlichen Anforderungen an den Datenschutz weiter in Kraft. Die Einhaltung wird durch die Aufsichtsbehörden geprüft. Folge: Die Anzahl der verhängten Bußgelder steigt. Wir geben Ihnen eine Übersicht zu den wesentlichen deutschen Bußgeldverfahren der ersten Jahreshälfte 2020.

In dieser Ausgabe finden Sie unseren Hinweis zu den Folgen der EuGH-Entscheidung zur Ungültigkeit des „EU US Privacy Shield“ sowie auf ein Urteil des Landesarbeitsgerichts (LAG) Mecklenburg-Vorpommern zur Frage der Verantwortlichkeit des betrieblichen Datenschutzbeauftragten bei der Umsetzung der Datenschutzgrundverordnung (DSGVO). Außerdem wollen wir Sie weiterhin zu Datenschutz-Themen auf dem Laufenden halten, die im Zusammenhang mit der Corona-Pandemie stehen.

Für unsere Kunden aus dem Gesundheitswesen haben wir ein *„Special“* zu aktuellen Themen zum Gesundheitsdatenschutz zusammengestellt.

Das mip Datenschutzteam wünscht Ihnen eine anregende Lektüre. Zögern Sie nicht, Ihre Berater zu den Themen anzusprechen.

Ihr

Asmus Eggert

Inhalt

Entwicklung der Bußgelder in den letzten Monaten

Mit Wirksamwerden der Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018 hat der Datenschutz radikal an Bedeutung gewonnen. Grund für den Bedeutungszuwachs sind nicht etwa geänderte Grundbedingungen für die Datenverarbeitungen, sondern dass die Zeiten der „verschmerzbaren“ Bußgeldverhängung mit einer grundsätzlichen Deckelung von 300.000 EUR der Vergangenheit angehören. Die DSGVO erlaubt den Aufsichtsbehörden bereits beim ersten Verstoß Bußgelder von bis zu 20 Millionen Euro zu verhängen. So ein Verstoß kann etwa eine Datenverarbeitung ohne Rechtsgrundlage oder eine fehlende Datenschutzinformation sein. Dabei spielt die Größe des Unternehmens keine Rolle. Folglich sind auch kleine und mittelständische Unternehmen (KMUs) und Vereine Bußgeldern potenziell ausgesetzt.

Inzwischen hat die Umsetzung der DSGVO in vielen Unternehmen den Projektstatus verloren und ist erfolgreich, wenn auch nicht immer abschließend, umgesetzt. Daneben gibt es noch immer Unternehmen, die die Anforderungen der DSGVO bisher noch nicht umgesetzt haben, weil sie das Bußgeldrisiko als eher gering einschätzen und daher aus ihrer Warte die Kostenersparnis der Nichtumsetzung die Umsetzungsaufwände überwog. In den letzten Jahren ist die Bußgeldliste nun jedoch peu à peu gewachsen. Das hat auch mit dem voranschreitenden personellen, fachlichen und technischen Ausbau der Aufsichtsbehörden zu tun. Das potenzielle Risiko von Bußgeldern steigt.

Hier eine Liste mit Beispielen in Deutschland verhängter Bußgelder aus dem 1. Halbjahr 2020:

30.06.2020	1.240.000 €	AOK Baden-Württemberg	Verwendung der Daten von 500 Gewinnspielteilnehmern für Werbezwecke »Details
03.04.2020	6.000 €	Berliner Landesverband der NPD	Veröffentlichung der Kontaktdaten von Flüchtlingshelfern über Google Maps. »Details
24.03.2020	50.000 €	Unternehmen	Fehlender AV-Vertrag und Verstoß gegen Transparenz- und Verständlichkeitsgebot. »Details
24.03.2020	12.000 €	Betreiber eines Schwimmbades	Unerlaubte Videoüberwachung in Schwimmbad, fehlender AV-Vertrag und keine Benennung eines DSB. »Details
14.03.2020	229 €	LKW-Fahrer	Betrieb einer Dashcam im Straßenverkehr und Veröffentlichung von Aufnahmen über Youtube. »Details
11.03.2020	2.000 €	Restaurant	Unerlaubte Kameraüberwachung des Gastraumes eines Restaurants. »Details
13.02.2020	51.000 €	Facebook Germany GmbH	Unterlassene Mitteilung über den Wechsel des Datenschutzbeauftragten. »Details
13.02.2020	20.000 €	Hamburger Verkehrsverbund GmbH	Verspätete Meldung einer Datenpanne an betroffene Personen und Aufsichtsbehörde. »Details
30.01.2020	100.000 €	Lebensmittelhandwerksunternehmen	Unzureichender Schutz personenbezogener Daten in einem Bewerberportal. »Details

Praxishinweis: Die Verstöße sind vielfach in nicht oder nicht hinreichend umgesetzten technischen und organisatorischen Maßnahmen (TOMs) begründet. Daher ist dringend zu empfehlen, neben der Liste der Verarbeitungstätigkeiten geeignete technische und organisatorische

Datensicherheitsmaßnahmen (TOMs) umzusetzen und zu dokumentieren. Bestehende Dokumentationen sind regelmäßig zu evaluieren und ggf. zu aktualisieren.

Betrieblicher Datenschutzbeauftragter: Aufgabe und Qualifikation

„Ja, Datenschutz ist wichtig, ABER ….!“ Das ist der Tenor, der in vielen Unternehmen vorherrscht. Da die Umsetzung des Datenschutzes den Unternehmen personelle wie finanzielle Ressourcen abfordert, ist eine effektive und effiziente Herangehensweise geboten. Dazu zählt auch die Frage, wer sich im Unternehmen um den Datenschutz in welchem Umfang kümmert. Dies erfordert diverse unternehmerische Entscheidungen, die eine gewisse Kenntnis der datenschutzrechtlichen Situation voraussetzt. Wesentlich ist dabei ein klares Verständnis der Rollen im Unternehmen: Die Umsetzungsverantwortung bleibt stets bei der Geschäftsführung. Das gilt auch dann, wenn für das Unternehmen nach DSGVO bzw. BDSG ein Datenschutzbeauftragter benannt werden muss. Der Datenschutzbeauftragte (DSB) hat hingegen eine Kontroll- und Beratungsfunktion. Zur Erfüllung dieser Aufgabe muss die Geschäftsleitung dem DSB die notwendigen Ressourcen zur Verfügung stellen. Auch ist sicherzustellen, dass er die notwendige Qualifikation für diese Aufgabe hat.

Hinweise zu diesem Thema lassen sich einem aktuellen Urteil des LAG Mecklenburg-Vorpommern entnehmen (Urteil vom 25.02.2020 Az.: 5 Sa 108/19). Dieses hatte den Fall zu entscheiden, ob ein Arbeitgeber dem bei ihm angestellten Datenschutzbeauftragten zu Recht als Fehlverhalten vorhalten durfte, das in einer möglichen fehlerhaften Beratung im Blick auf die frühzeitige Umsetzung der DSGVO bestand. Als Folge der nicht rechtzeitigen Umsetzung wurde das Unternehmen durch die Datenschutzaufsichtsbehörde gerügt. Der Arbeitgeber sah darin eine massive Verletzung der Pflichten des Datenschutzbeauftragten und seine mangelnde Fachkenntnis.

Dieser Ansicht des Arbeitgebers ist das Gericht nicht gefolgt. Die Einhaltung der geltenden datenschutzrechtlichen Bestimmungen sei Aufgabe des Arbeitgebers. Der Datenschutzbeauftragte habe als Kontrollorgan Kontrollpflichten und insoweit keine Umsetzungsverantwortung. Pflichtverletzungen eines Datenschutzbeauftragten lägen zum Beispiel dann vor, wenn der Datenschutzbeauftragte seine Arbeitszeit nicht voll ausschöpfe, um seinen Kontrollpflichten nachzukommen bzw., wenn er seine Aufgaben durch die Nichtausschöpfung seiner Arbeitszeit nicht ausreichend abgeschlossen habe. Das LAG weist darauf hin, dass die Tätigkeit des Datenschutzbeauftragten keine bestimmte Ausbildung oder näher bezeichnete Fachkenntnisse erfordere. Vielmehr richte sich die erforderliche Sachkunde des Datenschutzbeauftragten nach der jeweiligen Organisation. Der DSB müsse daneben über die nötige Zuverlässigkeit für die Tätigkeit als Datenschutzbeauftragter verfügen. Er müsse also die Gewähr bieten, dass er seinen Aufgaben gewissenhaft nachkommt und nicht gegen die gesetzlich auferlegten Pflichten eines Datenschutzbeauftragten verstößt. Eine Verletzung allgemeiner arbeitsrechtlicher Pflichten (z. B. Diebstahl, Unterschlagung, vorsätzliche Rufschädigung) könne ebenfalls die Zuverlässigkeit in Frage stellen.

Praxishinweis: Die Geschäftsleitung eines Unternehmens kann sich nicht durch die Benennung eines Datenschutzbeauftragten seiner Umsetzungsverantwortung entziehen. Die Pflicht zur Umsetzung des Datenschutzes kann also nicht auf den betrieblichen Datenschutzbeauftragten „abgewälzt“ werden. Die Geschäftsleitung trägt stets die Verantwortung für die Datenschutzorganisation und das Datenschutzmanagements.
Sollten Sie Fragen zu den Themen haben, sprechen Sie Ihren Datenschutzberater der mip an.

Corona-Pandemie und Datenschutz

Die veränderten Arbeitsbedingungen als Folge der Corona-Pandemie hat weiterhin direkt oder indirekt Auswirkung auf den Datenschutz im Unternehmen. Daher wollen wir Sie auch in dieser Ausgabe der mip Beratungsinformation auf zwei Themen in diesem Kontext hinweisen:

BMAS: „SARS-CoV-2-Arbeitsschutzstandard“ vorgestellt

Am 16.4.2020 hat das Bundesministerium für Arbeit und Soziales (BMAS) ein Papier mit dem Titel „SARS-CoV-2-Arbeitsschutzstandard“ vorgestellt. Hier sind umfassende, verbindliche Regeln zum Arbeitsschutz für alle Unternehmen aufgestellt worden. Geregelt werden unter anderem organisatorische und personenbezogene Maßnahmen im Hinblick auf den Gesundheits- und Infektionsschutz von Mitarbeitern. Daneben haben diese neuen Arbeitsschutzstandards auch datenschutzrechtliche Implikationen hinsichtlich der Dokumentation von Kontaktdaten betriebsfremder Personen für den Fall der Infektionskettenverfolgung.

Der Standard kann unter folgendem Link auf der Seite des BMAS heruntergeladen werden:
SARS-CoV-2-Arbeitsschutzstandard

LDI NRW: Betriebliche Datenschutzbeauftragte sind auch bei Corona-bedingter Kurzarbeit unverzichtbar im Unternehmen

Dass die veränderten Arbeitsbedingungen, die als Folge der Corona-Pandemie in den Unternehmen einzuführen und zu bewältigen sind, auch datenschutzrechtliche Auswirkungen haben, dürfte den Geschäftsleitungen der Unternehmen inzwischen bekannt sein. Diese haben auch Auswirkungen auf die Tätigkeit der Datenschutzbeauftragten. Diese sind mit vielen neuen datenschutzrechtlichen Fragestellungen konfrontiert, die sich aus der Corona-bedingten Änderung bisheriger Arbeitsabläufe im Unternehmen ergeben. Dazu zählen zum Beispiel die Neuorganisation von Arbeitsprozessen, die Zunahme der elektronischen Datenverarbeitung, das Arbeiten im Home-Office oder in Telearbeit und den Einsatz von Videokonferenzsystemen. Auch Fragen des Gesundheitsdatenschutzes bei Beschäftigen, Kundinnen und Kunden erfordern die Einbindung des Datenschutzbeauftragten.

Umso wichtiger ist es, dass auch das verantwortliche Unternehmen der oder dem Datenschutzbeauftragten die Wahrnehmung der Kontroll- und Beratungsaufgaben ermöglicht. Eine entsprechende Pflicht ist in Artikel 38 Absatz 2 DSGVO gesetzlich verankert. Danach unterstützt der Verantwortliche bzw. der Auftragsverarbeiter den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39 DSGVO, indem die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und der Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zur Verfügung gestellt werden. Dem betrieblichen Datenschutzbeauftragten muss der Arbeitgeber auch erforderliche Ressourcen zur Erhaltung seines Fachwissens gewähren.

So kann es nach den jeweils aktuellen Umständen geboten sein, den Arbeitsumfang einer oder eines zuvor in Vollzeit als Datenschutzbeauftragten tätigen Beschäftigten zu reduzieren. Dies darf nach der Ansicht der Aufsichtsbehörde jedoch keinesfalls zum vollständig „brachliegen“ des Arbeitsfeldes führen. Datenschutzbeauftragte sind daher unverzichtbar für das Unternehmen.

Praxishinweis: Datenschutzbeauftragte müssen nach wie vor vom Unternehmen ordnungsgemäß und frühzeitig und in alle mit dem Schutz personenbezogener Daten zusammenhängende Fragen eingebunden werden. Betriebliche Datenschutzbeauftragte müssen daher die Möglichkeit haben, regelmäßig ihre Posteingänge sichten zu können sowie telefonisch und/oder per E-Mail als Ansprechpartner für die Beschäftigten, Kundinnen und Kunden oder andere betroffene Personen erreichbar sein.

Um dies sicherzustellen, sollten geeignete Maßnahmen vorgesehen werden: beispielsweise regelmäßiger Zugang zum Büro, Einrichtung eines Telearbeitsplatzes, Bereitstellen eines Diensthandys, Vereinbaren bestimmter Sprechzeiten o.ä.

"Privacy Shield" - EuGH kippt Datendeal zwischen USA und EU

Der EuGH erklärt die Datenschutzvereinbarung zwischen der EU und den USA "Privacy Shield" für ungültig. Wir haben dazu bereits eine Beratungsinformation EXTRA versandt. Da die Diskussion der daraus abzuleitenden Folgen erst gestartet ist, werden wir Sie in dieser Sache durch Blogs auf unserer Seite „Sofortdatenschutz.de“ auf dem Laufenden halten.

Special: Aktuelles zum Gesundheitsdatenschutz

Die aktuelle Corona-Pandemie macht deutlich, wie wichtig ein funktionierendes Gesundheitssystem ist. Krankenhäuser, Arztpraxen und medizinische Labore stellen sich der Herausforderung, die medizinische Versorgung der Bevölkerung sicherzustellen. Die Funktionsfähigkeit einer medizinischen Einrichtung hängt immer mehr von der Verfügbarkeit und Einsatzfähigkeit digitaler Systeme und IT-Anwendungen ab. Damit steigt die Gefahr für die Anfälligkeit durch Cyberangriffe. Bereits ein erfolgreicher Cyberangriff kann für Tage oder Wochen das Funktionieren medizinischer Einrichtungen massiv beeinträchtigen oder im schlimmsten Fall diese sogar komplett lahmlegen.

Zur Überprüfung der Cybersicherheitsmaßnahmen haben der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) und das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) daher medizinischen Einrichtungen in Bayern eine Best-Practice-Checkliste zur Verfügung gestellt. Diese kann selbstverständlich auch von Einrichtungen aus den anderen Bundesländern genutzt werden.

Oft braucht es jedoch leider nicht mal einen Cyberangriff, um eine Datenpanne zu erzeugen: Eine Celler Gemeinschaftspraxis hatte höchst private Daten zehntausender Patienten über einen ungesicherten Praxisserver gespeichert. Damit waren diese für jedermann einsehbar. Nach dem Datenschutzskandal prüft die zuständige Landesbeauftragte für den Datenschutz nun die Einleitung eines Ordnungswidrigkeitenverfahrens. Wir rechnen mit der Verhängung einer erheblichen Geldbuße.

Praxishinweis: Prüfen Sie Ihre Systemlandschaft sowie die Umsetzung und Wirksamkeit der TOMs! Sprechen Sie bei Unterstützungsbedarf Ihren Datenschutzberater an.

Impressum

mip Consult GmbH
Wilhelm-Kabus-Straße 9
10829 Berlin
Tel: +49 (0) 30 – 20 88 999 – 00
Fax: +49 (0) 30 – 20 88 999 – 88
Redaktion: Stefan Ax, Asmus Eggert

Internet: www.sofortdatenschutz.de und www.blog.sofortdatenschutz.de
E-Mail: sofortdatenschutz@mip-consult.de

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider
Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 121869
USt.-Identnr.: DE249276018
Verantwortlich nach § 55 Abs. 2 RStV: Asmus Eggert