DSGVO: 5000 Euro Bußgeld für fehlenden Auftragsverarbeitungsvertrag

Ein kleines Unternehmen wurde mangels Vertrags zur Auftragsverarbeitung zu einem Bußgeld verurteilt. Auslöser war eine Anfrage bei den Datenschutzbehörden.

Seit Anwendung der DSGVO Ende Mai 2018 gab es nur sehr vereinzelte Fälle von Bußgeldern, die von den Aufsichtsbehörden aufgrund von Verstößen gegen den Datenschutz verhängt wurden. Ein erster Verstoß gegen den Social Media Anbieter *Knuddels.de* wurde Ende des Jahres bekannt. Es deutet allerdings einiges darauf hin, dass diese anfängliche Schonfrist nun vorbei ist. Derzeit bearbeiten die Landesdatenschützer viele hundert Beschwerden. Auch wenn nur ein Bruchteil dieser Meldungen verfolgt und mit Bußgeldern geahndet wird, dürfte es 2019 Strafzahlungen für Verstöße jeder Art und in nahezu jeder Höhe geben.
Ein weiterer Fall wurde nun aus Hamburg bekannt. Dort hatte die Datenschutzbehörde mit Datum vom 17.12.2018 einen Bußgeldbescheid an das kleine Versandunternehmen Kolibri Image versandt und dieses aufgefordert, einen Betrag von 5000 Euro zuzüglich 250 Euro Gebühren zu zahlen. Begründet wird dieser Bescheid nach Art. 83 Abs. 4 DSGVO durch das Fehlen eines Auftragsverarbeitungsvertrags.
Ausgangspunkt für dieses Schreiben war eine E-Mail des Unternehmens an den Hessischen Beauftragten für den Datenschutz im Mai 2018. Darin fragte man um Rat hinsichtlich eines beauftragten Dienstleisters, der Kundendaten verarbeitet, aber trotz mehrfacher Anforderung keinen Vertrag zur Auftragsverarbeitung übersandt hatte. Die Behörde antwortete darauf, dass die Pflicht, eine solche Vereinbarung abzuschließen, nicht nur den Dienstleister, sondern auch den Auftraggeber als datenschutzrechtlich Verantwortlichen treffe. Das Unternehmen solle und müsse daher selbst eine entsprechende Vereinbarung verfassen und an den Auftragsverarbeiter zu Unterschrift schicken. Hierfür gäbe es auch entsprechende Vorlagen auf der Seite der Verwaltung.

Beidseitige Verpflichtungen

Darauf antwortete Kolibri Image, dass man sich diese Arbeit nicht machen wolle und dies für eine Pflicht des Auftragnehmers halte. Anfang November beauftragte man einen Anwalt, der ergänzend ausführte, dass man die Frage lediglich vorsorglich gestellt habe. Den Vorschlag, selbst eine entsprechende Vereinbarung mit dem Anbieter im Bereich der Vermittlung von Postdienstleistungen zu verfassen, lehnte der Anwalt ab, da man die internen Prozesse dort nicht kenne und man die teure Übersetzung für den Anbieter aus Spanien ablehnte. Die Behörde aus Hessen gab daraufhin die Sache an die zuständigen Kollegen aus Hamburg ab, die den Bußgeldbescheid verfassten.
Der Beauftrage aus Hamburg sieht in dem Verhalten des Unternehmens einen Verstoß gegen Art. 28 Abs. 3 DSGVO. Nach dieser Vorschrift muss bei jeder Verarbeitung von personenbezogenen Daten durch einen Dritten ein zusätzlicher Vertrag zum Datenschutz geschlossen werden, der unter anderem Details zu den getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Daten enthält. Eine solche Vereinbarung sei zwischen den Parteien nicht geschlossen worden, obwohl der Postdienstleister im Auftrag Kundendaten verarbeitet habe. Die Ausführungen des Anwalts, die Anfrage in Hessen sei nur vorbeugend erfolgt, wollte man in Hamburg nicht glauben. Dies ergäbe sich unter anderem aus Formulierungen in der ursprünglichen ersten E-Mail sowie aus der Tatsache, dass der Dienstleister als Verarbeiter in der Datenschutzerklärung genannt worden sei.

Andreas Lichtenfeld
Eichenstr. 88
93164 Laaber

Teil.: 09498-7227071
E-Mail: info@agqus.de
www.agqus.de

5000 Euro Geldbuße

Die Geldbuße wurde auf einen Betrag von 5000 Euro festgesetzt. Dies ergebe sich daraus, dass nach Ansicht der Behörde schützenswerte Daten ohne Rechtsgrundlage an den Dienstleister übermittelt wurden. Erschwerend wirke sich aus, dass man diese Praxis aufrechterhalten habe, obwohl dem Unternehmen die Datenverarbeitungsprozesse des Verarbeiters explizit nicht bekannt waren. Auch der Hinweis auf hohe Kosten für eine Übersetzung wirke nicht strafmildernd.

Vielmehr hätte man zwingend von der Beauftragung des Dienstleisters absehen müssen. Man habe aber im Gegenteil spätestens nach der Auskunft aus Hessen von der Rechtslage Kenntnis gehabt und sich vorsätzlich dagegen entschieden, rechtskonform zu handeln. Weder habe man das Schreiben ernst genommen, noch sei die Verwendung der vorgeschlagenen Formulierungshilfe in Betracht gezogen worden. Vielmehr habe man durch widersprüchlichen Vortrag versucht, sich der Verantwortung zu entziehen. Schließlich fehle es auch an einer Zusammenarbeit mit der Behörde, die sich strafmildernd auswirken könne.

Kritik an wirklichkeitsfernen Regelungen

Dirk Maass von Kolibri Image kritisierte das Vorgehen der Behörden. Nachdem der Postdienstleister auf seine Anfrage nicht reagiert hatte, habe er sich hilfesuchend an den Datenschutzbeauftragten in Hessen gewandt. Diesem sei nichts Anderes eingefallen, als ihn auf einige PDF-Vorlagen zum Download hinzuweisen. Das sei vollkommen realitätsfern, da er naturgemäß nicht wisse, welche Datenprozesse und Verantwortlichkeiten auf Seiten des Auftragnehmers bestehen. Es sei auch nicht realistisch, einen teuren IT-Anwalt zu beauftragen, das Ergebnis anschließend auf eigene Kosten ins Spanische übersetzen zu lassen und dies dann an den Hauptsitz des Auftragsdienstleisters in Madrid zu senden, mit der Aufforderung, doch gefälligst zu unterschreiben. Also habe man notgedrungen auf die weitere Zusammenarbeit verzichtet.

Maass: „Wir sind für Datenschutz, aber so wie es hier gelaufen ist, kann es doch nicht gemeint sein. Hier erweist sich der Datenschutz einen Bärendienst“. Er kündigte an, gegen den Bußgeldbescheid Widerspruch einzulegen.

Andreas Lichtenfeld
Eichenstr. 88
93164 Laaber

Teil.: 09498-7227071
E-Mail: info@agqus.de
www.agqus.de

DS-GVO Artikel 83, Abs. 4
(Allgemeine Bedingungen für die Verhängung von Geldbußen)

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist: a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43; b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43; c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4. 4.5.2016 L 119/82 Amtsblatt der Europäischen Union DE

DS-GVO Artikel 28, Abs. 3 (Auftragsverarbeiter)

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet; b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift; d)die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält; e)angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen; f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt; g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht; h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt. 4.5.2016 L 119/49 Amtsblatt der Europäischen Union DE Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

Informationen in allen Fragen des Datenschutzes und Unterstützung zur Umsetzung der Informationssicherheit finden Sie bei uns!

www.agqus.de

Andreas Lichtenfeld
Eichenstr. 88
93164 Laaber

Teil.: 09498-7227071
E-Mail: info@agqus.de
www.agqus.de