

In diesem Monat jährt sich die Geltung der Datenschutz-Grundverordnung (DSGVO) und damit deren praktische Anwendung zum ersten Mal. In den zwei Jahren zwischen Inkrafttreten und Geltung des neuen EU-Datenschutzrechts waren Unternehmen damit beschäftigt, ihre internen Prozesse und Dokumentationen sowie Verträge, Datenschutzhinweise und Einwilligungserklärungen anzupassen. Die Datenschutzbehörden waren – und sind immer noch – bemüht, auf deutscher und EU-Ebene, mit diversen Orientierungshilfen, Kurzpapieren und Anwendungshinweisen Hilfestellung

„Data Breach Notification“ nach Art. 33 DSGVO bekannt wurden. Interessant ist hier, dass die Behörde anscheinend das Verwendungsverbot in § 43 Abs. 4 BDSG für solche Meldungen wegen vermeintlicher Gemeinschaftsrechtswidrigkeit nicht angewendet hat. In beiden Fällen wurde betont, dass die Kooperation der jeweiligen Unternehmen mildernd berücksichtigt wurde. Weitere interessante Bußgelder wurden in Hamburg verhängt: € 20 000 für eine verspätete Meldung nach Art. 33 DSGVO i. V. m. der unterbliebenen Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO sowie € 5000 gegen



RA Jan Spittka, Köln

Ein Jahr Geltung der DSGVO – Die ersten Schritte zur Durchsetzung

zu geben, aber auch die Deutungs-
hoheit über die Auslegung des neuen Rechts zu erlangen. Nunmehr hat die praktische Durchsetzung der DSGVO durch die Aufsichtsbehörden begonnen. Die DSGVO und das „unterstützende“ neue Bundesdatenschutzgesetz (BDSG) enthalten nicht nur eine Vielzahl per se auslegungsbedürftiger Rechtsbegriffe wie „berechtigtes Interesse“ oder „ein dem Risiko angemessenes Schutzniveau“, sondern sind zudem in einigen Punkten unklar. So ist hoch umstritten, welcher Unternehmensbegriff bei der Verhängung von Geldbußen zugrunde zu legen ist. Ist das Unternehmen das jeweilige verstößende Rechtssubjekt oder aber die „wirtschaftliche Einheit“ bis hin zum Konzern? Inwieweit können durch den pauschalen Verweis aus dem BDSG auf das Ordnungswidrigkeitengesetz Bußgelder gegen einzelne im Unternehmen tätige Personen verhängt werden?

Betrachtet man die bisherige Praxis der Sanktionsverhängung durch die deutschen Datenschutzbehörden, kann man feststellen, dass sich die Behörden im breiten Spektrum zwischen einer Verwarnung und Geldbußen in Höhe von bis zu 4 % des weltweiten Umsatzes eher moderat verhalten. Der Durchschnittsbetrag der mittlerweile bekanntgewordenen Bußgelder liegt im mittleren vierstelligen Bereich. Das derzeit höchste Bußgeld wurde vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg verhängt: € 80 000 wegen der versehentlichen digitalen Veröffentlichung von Gesundheitsdaten aufgrund unzureichender interner Kontrollmechanismen. Dieselbe Behörde verhängte zudem ein Bußgeld in Höhe von € 20 000 gegen das Social-Media-Unternehmen Knuddels wegen unzureichender IT-Sicherheitsmaßnahmen, die im Rahmen einer

eine kleine GbR für eine fehlende Auftragsverarbeitungsvereinbarung nach Art. 28 Abs. 3 DSGVO. Die Behörde hat aber auch 25 Verwarnungen ausgesprochen, z. B. wegen verspäteter Auskunft oder Missachtung von Werbewidersprüchen. Einige deutsche Behörden haben aber bereits Geldbußen im sechsstelligen Bereich angekündigt. In Portugal wurden bereits € 400 000 wegen eines mangelhaften Datenzugriffskonzepts und in Polen rund € 220 000 wegen fehlenden Datenschutzhinweises verhängt.

Diese Beträge stehen natürlich allesamt hinter den € 50 Millionen zurück, welche die französische Datenschutzaufsicht CNIL gegen die Google LLC verhängt hat. Hier wurden aber anscheinend die rund € 96 Milliarden Jahresumsatz der Google-Mutter Alphabet Inc. zugrunde gelegt, also der weite Unternehmensbegriff angewendet. In der Sache wird Google vorgeworfen, gegen die Transparenzpflichten nach Art. 12, 13 DSGVO verstoßen und personenbezogene Daten ohne Rechtsgrundlage verarbeitet zu haben, da die erforderlichen Einwilligungen unwirksam seien. Der Online-Datenschutz rückt auch bei den deutschen Datenschutzbehörden in den Fokus. Das Bayerische Landesamt für Datenschutzaufsicht hat 40 Webseiten geprüft. Ergebnis war, dass – nach Auffassung der Behörde – auf keiner der Webseiten eine wirksame Einwilligung eingeholt wurde. Vor diesem Hintergrund wurden Sanktionsmaßnahmen angekündigt. In der jüngst veröffentlichten Orientierungshilfe für Anbieter von Telemedien sind die Datenschutzbehörden jedoch von einem strikten Einwilligungserfordernis für Online-Tracking abgewichen, sodass bestimmte Formen der Analyse des Nutzerverhaltens auch auf eine Interessenabwägung gestützt werden können. Die praktische Anwendung der DSGVO bleibt somit spannend.