DSGVO-Geldbußen – ein (un)kalkulierbares Risiko für Unternehmen?

RA Jan Spittka*

Am 24. 5. 2023 hat der Europäische Datenschutzausschuss (EDSA), das Koordinationsgremium der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten, ein Update seiner Leitlinien für die Berechnung von Geldbußen für Datenschutzverstöße zur öffentlichen Konsultation veröffentlicht (EDSA, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.0, v. 24. 5. 2023). Obwohl sich an der grundsätzlichen Methodik nichts geändert hat, verdeutlicht die neue Version noch einmal, dass gerade bei umsatzstarken Unternehmen ein erhebliches Risiko deutlich höherer Geldbußen besteht. Grund hierfür ist, dass der EDSA den Umsatz eines Unternehmens nicht nur für die Bestimmung der Obergrenze der Geldbuße (je nach Verstoß 2 % oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs) für relevant hält, sondern auch für die Bestimmung des Ausgangswertes für die Bußgeldberechnung heranziehen möchte. Je nach Schwere des Verstoßes soll dieser Ausgangswert im Falle leichter Verstöße bereits bei bis zu 0,2 % bzw. 0,4 % und im Falle schwerer Verstöße bereits bei bis zu 2 % bzw. 4 % liegen. Nach diesem Ansatz könnte z. B. die Geldbuße gegen ein Unternehmen mit einem Umsatz von zwei Milliarden Euro bei einem DSGVO-Verstoß der höheren Kategorie selbst bei einem leichten Verstoß bereits bei vier Millionen Euro liegen. Der Ausgangswert kann dann im weiteren Verfahren anhand der Punkte in Art. 83 Abs. 2 DSGVO, z. B. Grad des Verschuldens, einschlägige frühere Verstöße oder Nachtatverhalten, erhöht oder abgesenkt und auch noch einmal unter Berücksichtigung der Kriterien Wirksamkeit, Verhältnismäßigkeit und Abschreckung korrigiert werden.

Die große Unbekannte bei der Berechnung von Geldbußen ist jedoch immer noch die Frage, auf wessen Umsatz abzustellen ist. Der EDSA vertritt unter Berufung auf Erwägungsgrund 150 der DSGVO die Auffassung, dass der Unternehmensbegriff aus Art. 101, 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) herangezogen werden könne, also die im Unionskartellrecht entwickelte Rechtsfigur der wirtschaftlichen Einheit. Dieser funktionale Unternehmensbegriff meint nicht nur die Gesellschaft, welche die personenbezogenen Daten als Verantwortlicher oder Auftragsverarbeiter verarbeitet, sondern kann auch die Muttergesellschaft und ggf. sogar den gesamten Konzern erfassen. Ob sich diese weite Auslegung durchsetzen wird, ist noch nicht geklärt. Erwägungsgründe sind nicht rechtlich verbindlich. Zudem würde die Übertragung des kartellrechtlichen Unternehmensbegriffs zu erheblichen Widersprüchen mit dem Verständnis von „Unternehmen“ und „Unternehmensgruppe“ im rechtlich bindenden Teil der DSGVO führen. Im Verfahren *Deutsche Wohnen* hat der Generalanwalt jedoch bereits vertreten, dass der funktionale Unternehmensbegriff durchaus zur Festsetzung der Höhe der Geldbußen angewendet werden könne (Schlussanträge v. 27. 4. 2023, Az. C-807/21, Rn. 48). Ein Urteil steht jedoch noch aus. Sollte sich die weite Auslegung des Unternehmensbegriffs durchsetzen, dürfte die Bußgeldhöhe in vielen Fällen erheblich ansteigen.

Es ist jedoch auch fraglich, ob der Umsatz überhaupt zur Berechnung der Bußgeldhöhe herangezogen werden kann. Die DSGVO nennt den Umsatz lediglich im Zusammenhang mit der Bestimmung der Obergrenze der Geldbuße, nicht aber als Kriterium zur Entscheidung über die Höhe. Der Umsatz kann auch nicht unter die „anderen erschwerenden oder mildernden Umstände“ i. S. d. Art. 82 Abs. 2 lit. k DSGVO subsumiert werden, da der Umsatz zunächst einmal wertungsneutral ist. Auch das LG Bonn, welches als erstes deutsches Gericht zu einer DSGVO-Geldbuße urteilte und hierbei auf den funktionalen Unternehmensbegriff abstellte, hat entschieden, dass für die Bemessung der Geldbuße in erster Linie auf tatbezogene Gesichtspunkte abzustellen und dass eine Fokussierung auf den Unternehmensumsatz problematisch sei (LG Bonn, Urt. v. 11. 11. 2020, Az. 29 OWi 1/20). Selbstverständlich könne der Umsatz vor dem Hintergrund der Ahndungsempfindlichkeit eine Rolle spielen, jedoch seien auch andere Kriterien, wie Bilanzgewinn und sonstige Kennzahlen der wirtschaftlichen Leistungsfähigkeit des Unternehmens zu berücksichtigen. Die starke Umsatzfokussierung im Bußgeldberechnungsmodell des EDSA ist daher abzulehnen. Die derzeit unklare Rechtslage macht Geldbußen für Unternehmen zu einem nur schwer kalkulierbaren Risiko. Umso wichtiger ist es für die Unternehmensleitung, effektive Risikomanagementmaßnahmen zur Einhaltung der DSGVO zu implementieren und deren Umsetzung zu überwachen.

* ist Rechtsanwalt und Partner in der Kanzlei Clyde & Co in Düsseldorf und auf Datenschutzrecht und Cybersecurity, insbesondere im Versicherungssektor, spezialisiert. Nach dem Studium in Münster mit Schwerpunkt im Informationsrecht war er als wiss. Mitarbeiter am ITM (zivilrechtliche Abteilung) tätig. Im Anschluss an das Referendariat, das er u. a. bei einer Datenschutzbehörde absolvierte, ist er seit 2012 als Anwalt tätig.