CB-EDITORIAL

DSGVO-Schadensersatz als Compliance-Risiko

Die Einhaltung gesetzlicher und damit auch datenschutzrechtlicher Vorgaben ist nicht nur aus Gründen gesetzeskonformen Handelns für Unternehmen wichtig. FCPA, UK Bribery Act, KWG, GWG, OWiG und der Deutsche Corporate Governance Kodex (DCGK) verpflichten zu bzw. verlangen eine verantwortungsvolle und rechtsförmige Unternehmensführung auf Basis anwendbarer Rechtsnormen und entsprechender Corporate Governance Kodizes. Bestandteil dieses Pflichtenkanons sind ebenfalls die Implementierung, Aufrechterhaltung und Weiterentwicklung einer Datenschutz-Governance-Struktur. Überdies bzw. vielmehr zunehmend gerät eine bestehende gute Datenschutz-Compliance zu einem wichtigen unternehmerischen Reputationsaspekt: „Verlorene" sensitive Daten, Datenlecks mit der Folge im Internet „herumgeisternder" personenbezogener Daten, unverhältnismäßige arbeitgeberseitige Überwachungsmaßnahmen der Belegschaft oder Hackerangriffe aufgrund systembedingter IT-Schwachstellen sorgen für große mediale Beachtung und enden überdies regelmäßig in Bebußungen durch die datenschutzrechtlichen Aufsichtsbehörden gem. Art. 83 DSGVO in aufsehenerregenden Höhen. Fünfstellige Geldbußen sind an der Tagesordnung, sechsstellige Geldbußen keine Seltenheit mehr.

Daneben nimmt auch die Inanspruchnahme von Unternehmen durch Klagen auf immateriellen Schadensersatz wegen Datenschutzverstößen durch Individualpersonen zu. Eine Klageindustrie für Massenklagen formt sich bereits. Anwälte treten werbend mit Angeboten entsprechender Interessenvertretung am Markt auf, um potentielle Anspruchsteller „einzusammeln"[1]. Aus Klägersicht praktikabel und recht einfach möglich macht dies Art. 82 DSGVO, wonach immaterieller Schadensersatz nahezu für jedwede Verletzung datenschutzrechtlicher Vorgaben geltend gemacht werden kann. Zwar hat der EuGH in einigen Entscheidungen den Anwendungsbereich der Norm zurückgeschnitten, indem die Luxemburger Richter den Nachweis eines konkreten Schadens einfordern[2]. Eine Bagatellgrenze darf es aber weiter nicht geben[3], so dass auch der bloße Kontrollverlust über die eigenen Daten einen ersatzfähigen immateriellen Schaden darstellen kann[4].

Mit zwei jüngeren Urteilen[5] bestätigt der EuGH dies: Ein Verstoß gegen die DSGVO allein begründet zwar weiterhin keinen Schadensersatz, ein konkreter Schaden muss folglich dargelegt werden. Allerdings reicht dafür „die Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen diese Verordnung an Dritte weitergegeben wurden, ohne dass nachgewiesen werden kann, dass dies tatsächlich der Fall war […], sofern diese Befürchtung samt ihrer negativen Folgen ordnungsgemäß nachgewiesen ist". Mit anderen Worten: Eine glaubhaft dargelegte Furcht kann ausreichen, um Schadensersatzansprüche zu begründen, es muss nicht wirklich etwas „passieren". Immerhin betont der EuGH, dass der Schadensersatz keinen abschreckenden Charakter hat, sondern „ausschließlich eine Ausgleichsfunktion erfüllt", so dass der Schweregrad und die Frage der Vorsätzlichkeit bei der Bemessung des Schadensersatzes nicht berücksichtigt werden müssen. Demnach dürfen nationale Gerichte die fehlende Schwere eines Schadens durch die Verurteilung zur Zahlung eines geringfügigeren Schadenersatzanspruchs berücksichtigen.

Für Unternehmen ist dies allenfalls ein sehr kleiner Lichtblick am datenschutzrechtlichen Entschädigungshorizont. Das Risiko der Inanspruchnahme wegen behaupteter Datenschutzverstöße und vermeintlicher daraus resultierender Schäden bleibt bestehen. Rechtssicherheit in Form einer praktischen Begrenzung ausufernder Entschädigungsansprüche wird nur die nationale Rechtsprechung herbeiführen können. Diese ist von einer einheitlichen Linie aber weit entfernt und zeichnet sich eher durch einen „kasuistischen Wildwuchs" aus. Die einzige Strategie der Risikomitigierung für Unternehmen ist es daher, den Datenschutz ernst zu nehmen und im Rahmen einer guten Corporate Governance zu einer prioritären Aufgabe der Unternehmenscompliance zu machen. Wie für andere bedeutende Compliance-Themen in Unternehmen (u.a. Anti-Corruption) gilt es damit auch für den Datenschutz ein effektives Management-System zu implementieren und fortlaufend weiterzuentwickeln.

„Datenschutz ist prioritäre Aufgabe der Compliance."

Autor

Prof. Dr. Michael Fuhlrott *ist Partner bei FUHLROTT Arbeitsrecht in Hamburg. Er berät Unternehmen zu sämtlichen individual- und kollektivrechtlichen Fragestellungen mit einem Schwerpunkt im Arbeitnehmerdatenschutz.*

1 S. auch *Barrein/Fuhlrott*, NZA 2024, 443.
2 EuGH, Urt. v. 4.5.2023 – C-300/21, BB 2023, 1106.
3 EuGH, Urt. v. 14.12.2023 – C-456/22, K&R 2024, 112.
4 EuGH, Urt. v. 14.12.2023 – C-340/21, CB 2024, 124.
5 EuGH, Urt v. 20.6.2024 – C-590/22, CB 2024, 343, sowie verb. Rs. C-182/22 und C-189/22.