Weiteres Millionen-Bußgeld nach der DSGVO

Autoren: Arbeitskreis Datenschutz I Stand: Juli 2020

Die Nachricht lässt aufhorchen: Zum Ende des ersten Halbjahres 2020 wurde eine Krankenkasse mit einem Bußgeld in Höhe von 1,24 Millionen Euro belegt.

Diese hatte im Rahmen von Gewinnspielen in den Jahren 2015 bis 2019 personenbezogene Daten der jeweiligen Teilnehmer, darunter deren Kontaktdaten und Krankenkassenzugehörigkeit, erhoben. Dabei sollten die Daten der Gewinnspielteilnehmer auch zu Werbezwecken genutzt werden, sofern die Teilnehmer hierzu eingewilligt hatten. Mithilfe technischer und organisatorischer Maßnahmen sollte gewährleistet werden, dass nur Daten solcher Gewinnspielteilnehmer zu Werbezwecken verwendet werden, die zuvor wirksam hierin eingewilligt hatten.

Die zum Zwecke des Datenschutzes festgelegten Maßnahmen – dabei handelte es sich unter anderem um interne Richtlinien und Schulungsmaßnahmen – genügten jedoch nicht den gesetzlichen Anforderungen. In der Folge wurden die personenbezogenen Daten von mehr als 500 Gewinnspielteilnehmern ohne deren Einwilligung zu Werbezwecken verwendet. Insbesondere bemängelte der LfDI Baden-Württemberg fehlende regelmäßige Kontrollen hinsichtlich der Datensicherheit und entsprechende Anpassungen der technischen und organisatorischen Maßnahmen, um ein angemessenes Schutzniveau sicherzustellen.

Die Botschaft der Behörde ist eindeutig: Der vorhandene verwaltungsrechtliche Sanktionsrahmen wird konsequent angewandt, um durch abschreckende Geldbußen eine Einhaltung der sich aus der DSGVO ergebenen datenschutzrechtlichen Pflichten sicherzustellen. Der LfDI Baden-Württemberg hat bei der Festlegung des Bußgelds das Bußgeldmodell der deutschen Aufsichtsbehörden angewendet, bei dem der Bußgeldrahmen basierend auf den Umsätzen des betreffenden Unternehmens und der Schwere des Verstoßes bestimmt wird.

Das Modell lässt allerdings auch die Möglichkeit zu, bußgeldmindernde Umstände anzuerkennen. Insoweit wurde auch hier die Kooperation mit der Behörde bei der Bemessung der Bußgeldhöhe berücksichtigt.

Datenschutzrisiken stellen seit geraumer Zeit ein echtes Unternehmensrisiko dar. Zwar können Datenschutzverstöße zum Beispiel aufgrund individuellen menschlichen Versagens nie gänzlich ausgeschlossen werden, jedoch sind systemimmanente Defizite und prozessuale Schwachstellen vermeidbar.

Die Aufsichtsbehörden legen verstärkt einen Fokus auf die Einhaltung von Datensicherheitsanforderungen. Die Verarbeitung von personenbezogenen Daten mit Erlaubnisvorbehalt sieht vor, dass Datenverarbeitungen nur mit einer passenden Rechtsgrundlage stattfinden dürfen. Verantwortliche im Sinne der DSGVO müssen zudem geeignete technische und organisatorische Maßnahmen treffen, welche die Datensicherheit bei der Verarbeitung zu jeder Zeit sicherstellt, von der Erhebung der Daten bis hin zu deren Löschung. Dabei sollten die Verantwortlichen die Kontrolle der getroffenen Maßnahmen stets im Blick behalten.

Was bedeutet dies für die Praxis?

Unternehmen sollten folgerichtig Sorge dafür tragen, dass in einem ganzheitlichen Datenschutz-Managementsystem die Verarbeitungslandschaft vollständig erfasst ist. Mit ihr geht auch die Risikobewertung und die korrespondierende Auswahl der technischen und organisatorischen Maßnahmen einher. Diese sind fortlaufend und regelmäßig zu kontrollieren und bei Bedarf entsprechend anzupassen, um auf Dauer ein angemessenes Schutzniveau sicherzustellen.

Am Ende gewinnen diejenigen Unternehmen das nachhaltige Vertrauen ihrer Geschäftspartner, die dafür Sorge tragen, dass ein verantwortungsvoller Umgang mit deren Daten aktiv gelebt wird.