DSGVO Bußgeld verhängt

DSGVO: Portugiesische Aufsichtsbehörde verhängt Bußgeld in Höhe von 400.000 EUR gegen Krankenhaus

Die portugiesische Datenschutzaufsichtsbehörde hat gegen ein Krankenhaus ein Bußgeld in Höhe von 400.000 EUR verhängt. Es handelt sich dabei – jedenfalls soweit bekannt – um das europaweit erste Bußgeld in signifikanter Höhe nach dem Inkrafttreten der Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018.

Hintergrund

Die portugiesische Datenschutzbehörde CNPD (Comissão Nacional de Protecção de Dados) hat bekanntgegeben, dass ein Großteil des Bußgeldes darauf beruht, dass in dem betroffenen Krankenhaus zu viele Personen Zugriff auf Patientendaten hatten. So sei bei Daten, die eigentlich nur für Ärzte einsehbar sein sollten, auch für Techniker der Zugriff möglich gewesen. Darüber hinaus waren im System nahezu 1.000 Nutzer als „Arzt“ registriert, obwohl das Krankenaus eigentlich nur knapp 300 Ärzte beschäftigt habe.

Rechtliche Einordnung

Personenbezogene Daten müssen – und das eigentlich nicht erst seit Inkrafttreten der DSGVO – so geschützt werden, dass nur die Mitarbeiter Zugriff erhalten, die mit genau diesen Daten auch wirklich arbeiten müssen und somit den Zugriff benötigen. Dieser Grundsatz ist unter dem Stichwort „privacy by design“ (oder „Datenschutz durch Technikgestaltung“) nunmehr auch ausdrücklich im Gesetz verankert.

Dieser Grundsatz gilt in ganz besonderem Maße im Krankenhausbereich, da es sich hier um besonders sensible Daten handelt, die im Übrigen in Deutschland auch strafrechtlich geschützt sind. Ein Vorfall wie in Portugal könnte daher in Deutschland auch die Strafverfolgungsbehörden auf den Plan rufen.

Bewertung

Dem Vernehmen nach will das Krankenhaus gerichtlich gegen das Bußgeld vorgehen. Insoweit bleibt abzuwarten, ob die zuständigen Gerichte die rechtliche Würdigung der Datenschutzbehörde teilen und insbesondere die Höhe des Bußgeldes für angemessen erachten.

Grundsätzlich handelt es sich hier nach dem bekannten Sachverhalt um einen gravierenden Fall, der noch dazu besonders sensible Daten betrifft. Er zeigt allerdings auch, dass die Behörden bereit sind, nicht nur nach ganz

offensichtlichen Verstößen zu suchen, sondern durchaus auch tiefer in die Systeme der Verantwortlichen einzutauchen.

Empfehlung

Die deutschen Datenschutzaufsichtsbehörden haben bereits vor Jahren Orientierungshilfen für den Einsatz von Krankenhausinformationssystemen herausgegeben. Ein Fokus dieser Orientierungshilfen liegt auf der Gestaltung von Zugriffsrechten. Es kann davon ausgegangen werden, dass die in den Orientierungshilfen enthaltenen Empfehlungen weit überwiegend auch nach Inkrafttreten der DSGVO gültig sind.

Verantwortliche – nicht nur aus dem Gesundheitsbereich – sind daher gut beraten, ihre Berechtigungskonzepte auf den Prüfstand zu stellen. Im Fall von behördlichen Kontrollen muss der Verantwortliche ein Berechtigungskonzept nachweisen, bei dem der Zugriff auf das tatsächlich Erforderliche beschränkt ist. Der Verantwortliche muss damit auch begründen können, warum eine Person Zugriff auf bestimmte Daten benötigt. Dabei kann schon der fehlende Nachweis (unter dem Stichwort „Rechenschaftspflicht“) ein Bußgeld auslösen.

Ansprechpartner:

Sebastian Hoegl, LL.M. (Wellington)
Tel: +49 761 769999-20
shoegl@kpmg-law.com