

Datenschutzbeauftragter für Ärzte und Tageskliniken – Entscheidung der DSB

Art 37 DSGVO verpflichtet zur Bestellung eines DSBA, insbes. wenn die Kerntätigkeit in der umfangreichen Verarbeitung von Art 9 DSGVO Daten besteht.

Gesundheitsdaten sind jedenfalls Daten nach Art 9 DSGVO. Wo aber ist die Grenze der „Umfangreichheit“?

Amtswegiges Prüfverfahren bei Tagesklinik

Nach Meldungen von Sicherheitsverletzungen, vermutlich daher Meldungen von Datenschutzvorfällen iSd Art 33 DSGVO am 18.06.2018 und 22.06.2018 hat die DSB ein amtswegiges Prüfverfahren gegen eine Tagesklinik eingeleitet. Thema war auch, weshalb kein Datenschutzbeauftragter bestellt wurde.

Tagesklinik verarbeitet Gesundheitsdaten – aber wann ist das umfangreich?

Die DSB bezieht sich insbes. auch auf die **Leitlinien zum Datenschutzbeauftragten der Art. 29-Datenschutzgruppe (WP 243 rev.01)**, und verweist darauf, dass ein die Datenverarbeitung dann nicht als umfangreich gilt, wenn dies durch **einen einzelnen Arzt** oder einen sonstigen Angehörigen der Gesundheitsberufe erfolgt.

WEiters wird auf die Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev.01 hingewiesen, die auch Festlegungen dazu enthalten, und auf

- a) Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe;
 - b) verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente;
 - c) Dauer oder Dauerhaftigkeit der Datenverarbeitung;
 - d) geografisches Ausmaß der Datenverarbeitung
- Bezug nehmen.

In der Tagesklinik waren zum Zeitpunkt der Entscheidung **„zwölf Büro- bzw. Labormitarbeiter, siebzehn Ärzte und zwei Ernährungsberater“** beschäftigt

Die DSB kommt zum Schluss, dass aufgrund der Größe der Tagesklinik, und der gesetzlichen Speicherfrist von 10 Jahren gem. § 51 ÄrzteG die Kerntätigkeit (Verarbeitung von Gesundheitsdaten) als umfangreich zu beurteilen ist.

Aussagen zur genauen Abgrenzung bei Ärzten oder Tageskliniken zur Personenanzahl, die personenbezogene

Daten verarbeiten, und dann die umfangreiche Verarbeitung begründen gibt es im Bescheid der DSB nicht.

Die Ärztekammer geht davon aus, dass – in Anlehnung an die Bestimmungen des BDSG – bei Gruppenpraxen, ein DSBA zu bestellen ist, wenn mehr als zehn Mitarbeiter (Vollzeitäquivalente) Zugriff auf personenbezogene Daten/Patientenkarteien haben

Dieses Kriterium hatte die Tagesklinik jedenfalls erfüllt bzw. überschritten.



dataprotect
it-recht