1 Jahr DSGVO –

erste Erfahrungen im Vollzug

Senatsrat Dr. Leopold-Michael Marzi

11. ÖGSV Fachtagung Hafnersee

13.06.2019

Ziel der Datenschutz-Grundverordnung der EU

- Einheitliche, EU-weit geltende Standards
- Anpassung an die sich rasch wandelnde Realität
- Ausweitung der Schutzrechte
- Sanktionen für Pflichtverletzungen

Inkrafttreten der DSGVO mit 25. Mai 2018

- Die markantesten Trends seit Mai 2018
- Erste Entscheidungen der Datenschutzbehörde
- Tipps und Tricks vom Juristen

Das Grundrecht auf Datenschutz

Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.

Starker Anstieg der anhängigen Fälle

Prüfung der Dokumentation durch die Datenschutzbehörde

Tendenziell strenge Auslegung

Verarbeitungsverzeichnis: was muss es können?

Grundsatz der Datensparsamkeit

- Das Verarbeiten von Daten ist unzulässig, wenn kein Rechtfertigungsgrund vorliegt („Verbot mit Ausnahmen“).
- Zweck der Verarbeitung (eng auszulegen)
- Verpflichtung zur Löschung, wenn der Zweck nicht mehr gegeben ist

Speicherdauer

Zulässigkeit der Speicherdauer ist grundsätzlich auf die gesetzliche Aufbewahrungsfrist beschränkt (Datenschutzbehörde, Entscheidung vom 28.05.2018).

Aufbewahrungsfristen für Ärzte

Grundsätzlich sind niedergelassene Ärzte verpflichtet, Patientendaten mindestens 10 Jahre aufzubewahren, allerdings können bis zur absoluten Verjährung (30 Jahre) Schadenersatzansprüche gestellt werden.

Bei einer allfälligen Prüfung durch die Datenschutzbehörde sollte daher sofort Auskunft gegeben werden können, welche Patientendaten in welchem technischen System zu welchem Zweck wie lange gespeichert sind.

Was ist in Hinblick auf die DSGVO primär zu beachten?

Praxistipps vom Juristen

Sensibler Umgang mit Patientendaten, vor allem bei der ersten Anmeldung (diskrete Atmosphäre)

Sensibilisierung des gesamten Personals in Bezug auf den Datenschutz

Einmal jährlich nachweisliche Kenntnisnahme der wesentlichen Regeln

Technische Ausstattung (insbesondere der IT)

Schriftliche Bestätigung durch den IT-Dienstleister, dass die technischen Anforderungen an den Datenschutz (insbesondere in Hinblick auf den Virenschutz) gewährleistet sind.

- Nicht mehr benötigte schriftliche Aufzeichnungen auf Papier sollten unbedingt mit Hilfe eines Shredders (Crosscut) vernichtet werden oder einem befugten Entsorger übergeben werden.

Laufend benötigte sensible Daten

Sensible Daten sollten nach Betriebsende unbedingt in einem versperrten Kasten oder Schrank verwahrt werden, der Raum ist nach Betriebsende zu versperren.

Datenverlust

Der Verlust von Daten an Endgeräten (etwa durch Cyberattacken) oder aber auch der Verlust eines USB-Sticks u.ä. ist umgehend der Datenschutzbehörde zu melden, sofern für die Betroffenen (Patienten) ein Risiko besteht.

Versand von Newslettern

Der Versand von Newslettern, Einladungen oder allen anderen Formen von Verständigungen, die nicht in einem unmittelbaren Zusammenhang mit dem Behandlungsvertrag stehen, bedürfen der ausdrücklichen Zustimmung der betroffenen Personen.

Praxisgemeinschaften und Unternehmen

Zwischen den Partnern sollte schriftlich vereinbart werden, dass sämtliche personenbezogene Daten, die sich auf jeweils andere Partner beziehen (etwa Terminvereinbarungen in gemeinsam geführten Kalendern) vertraulich zu behandeln sind.

Vielen Dank für Ihre Aufmerksamkeit!

marzi@moser-marzi.at