Republik Österreich
Datenschutzbehörde

NEWSLETTER 4/2019

# Die Verantwortlichkeit zur Einhaltung der sich aus der DSGVO ergebenden Pflichten

## ignorantia iuris non excusat – Unwissenheit schützt nicht vor Strafe

**Mag. Samraa El Fohail**

Die Datenschutzbehörde (DSB) hat die (verpflichtende) Eingabe der Verantwortlichen – einem medizinischen Ambulatorium, dessen Unternehmensgegenstand insbesondere die Diagnostik und Therapie allergischer Erkrankungen umfasst – mit welcher sie gemäß Art. 33 DSGVO die Verletzungen des Schutzes personenbezogener Daten gemeldet hat, zum Anlass genommen, ein amtswegiges Prüfverfahren einzuleiten. Im Ergebnis wurde mit (rechtskräftigem) Bescheid vom 16.11.2018, GZ DSB-D213.692/0001-DSB/2018, eine Vielzahl von Verstößen gegen Bestimmungen der DSGVO festgestellt und nach dem „Legalitätsprinzip" im strafprozessualen Sinn nach § 25 Abs 1 Verwaltungsstrafgesetz 1991 – VStG, wonach Verwaltungsübertretungen von Amts wegen zu verfolgen sind, von der DSB ein Verwaltungsstrafverfahren eingeleitet.

Die der Beschuldigten zur Last gelegten Verstöße umfassten dabei Verletzungen in Bezug auf die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und zur Benennung eines Datenschutzbeauftragten gemäß Art. 37 DSGVO sowie Verstöße im Zusammenhang mit den Bedingungen für die Einwilligung in die Datenverarbeitung gemäß Art. 7 DSGVO und den Betroffenenrechten gemäß der Art. 12-14 DSGVO.

Die Beschuldigte hat sich im Rahmen ihrer Vernehmung (vgl. § 40 VStG) im Wesentlichen damit gerechtfertigt, dass sie auf (Fehl-)Informationen Dritter vertraut hätte bzw. sei sie bestrebt gewesen, Informationen in kurzer und prägnanter Form zur Verfügung zu stellen, um Patienten durch überbordende Informationen nicht zu überfordern.

Die DSB hat zum implizit geltend gemachten Rechtsirrtum festgestellt, dass dieser der Verantwortlichen vorwerfbar war, da sich diese – trotz Veranlassung hiezu – über den Inhalt der einschlägigen Normen nicht näher informiert hat. Eine diesbezügliche Erkundigungspflicht hat sich im vorliegenden Fall jedenfalls aus dem Unternehmensgegenstand der Beschuldigten, nämlich dem Betrieb eines medizinischen Ambulatoriums, ergeben. Die sich aus der Verarbeitung personenbezogener Daten ergebenden Pflichten ergeben sich aus der DSGVO und ist für deren Einhaltung jeder Verantwortliche selbst verantwortlich (vgl Art. 5 Abs 2 DSGVO).

Mit (nicht rechtskräftigem) Straferkenntnis vom 12. August 2019 wurde eine Strafe von € 50.000,00 verhängt, da die Beschuldigte folgende Tatbestände verwirklicht hat:

1. Die Beschuldigte, die mehrere Ärzte beschäftigt und deren Kerntätigkeit in der Verarbeitung von Gesundheitsdaten nach Art. 9 Abs 1 DSGVO liegt, hat gegen ihre Pflicht zur Bestellung eines Datenschutzbeauftragten verstoßen.
   Dabei war insbesondere zu berücksichtigen, dass sich das Erfordernis eindeutig aus den einschlägigen Interpretationshilfen zur DSGVO ergibt (vgl. insbesondere die „Leitlinien zum Datenschutzbeauftragten" die bereits vor In-Geltung-Treten der DSGVO mit 25.05.2018 verfügbar waren) und die „Privilegierung" hinsichtlich der Nichtbestellung eines Datenschutzbeauftragten lediglich einzelne Ärzte trifft.
2. Die Beschuldigte hat gegen die Bestimmungen betreffend die Bedingungen für die Einwilligung dadurch verstoßen, indem sie den Patienten in Form eines zu unterfertigenden Formblattes eine Einwilligung abverlangte, die auf unklaren Informationen betreffend die Rechtsgrundlage fußten, einer Einwilligung nicht zugänglich waren, gegen das Widerrufsrecht verstoßen haben oder durch die zum

Nachteil der Betroffenen von Aspekten der Datensicherheit abgewichen werden sollte.
Dies dadurch, dass der Einwilligungserklärung nicht mit der erforderlichen Klarheit zu entnehmen war, für welche Datenverarbeitungen die Einwilligung die Rechtsgrundlage darstellt, mit der Einwilligung von der allfälligen Verpflichtung zur verschlüsselten Übermittlung an Dritte abgegangen werden sollte, die Patienten „unwiderruflich" einzuwilligen hatten, dass zur Durchführung der vereinbarten Dienstleistung Dritte (Auftragsverarbeiter iSd. Art. 28 DSGVO) herangezogen werden können sowie weiters, dass mit der Einwilligung ein Haftungsausschluss für etwaige Datenschutzverletzungen im Zusammenhang mit der Datenübermittlung als vereinbart galt.

3. Die Beschuldigte hat gegen ihre Informationspflichten nach Kapitel III, Abschnitt 2 DSGVO dadurch verstoßen, dass der zur Verfügung gestellten Information nicht zweifelsfrei entnommen werden konnte, ob diese nach Art. 13 oder Art. 14 DSGVO erteilt wird. Dabei wurde zudem – obwohl die Verantwortliche unstrittig besondere Kategorien personenbezogener Daten (nämlich Gesundheitsdaten) gemäß Art. 9 DSGVO verarbeitet – als Rechtsgrundlage ausschließlich Art. 6 DSGVO angeführt und die Patienten nicht auf ihr Recht auf jederzeitigen Widerruf der Einwilligung hingewiesen.
4. Die Beschuldigte hat gegen ihre Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO verstoßen, obwohl sich das Erfordernis durch einen Umkehrschluss sowohl aus den „Leitlinien zum Datenschutzbeauftragten" als auch aus der DSFA-AV ergibt, die beide lediglich einzelne Ärzte von der Pflicht ausnehmen.

Die vorgeworfenen Zuwiderhandlungen waren jedenfalls der juristischen Person zurechenbar. Das pflichtwidrige Verhalten war der juristischen Person zuzurechnen, weil die für die Zuwiderhandlungen verantwortlichen natürlichen Personen zu der wirtschaftlichen Einheit gehören, die durch die Verantwortliche als juristische Person gebildet wird. Die Handlungen wurden von natürlichen Personen begangen, die für die juristische Person handlungsbefugt waren und folglich Handlungen im Namen der Beschuldigten setzen konnten.

Unter Beachtung des Art. 83 Abs 3 DSGVO – welcher in Abweichung zum mit § 22 Abs 2 VStG normierten Kumulationsprinzip – das Absorptionsprinzip anordnet, wonach bei einem Verstoß gegen gleiche oder miteinander verbundene Verarbeitungsvorgänge gegen mehrere Bestimmungen der DSGVO der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß übersteigt, wurde – unter Berücksichtigung der „Erschwerungs- und Milderungsgründe" eine, den verwirklichten Tatunwert tat- und schuldangemessene „Gesamtstrafe" von € 50.000,00 verhängt.

## Im Fokus

Mag. Andreas Zavadil

### Überwachungsstellenakkreditierungs-Verordnung (ÜstAkk-V)

Die Systematik der DSGVO geht von einer durchaus weitreichenden Selbstverantwortung von datenschutzrechtlich Verantwortlichen aus und sieht mit der Schaffung von Verhaltensregeln („Codes of conduct") gemäß Art. 40 DSGVO eine Methode zur Selbstregulierung vor, um Rechtsunsicherheiten im Zusammenhang mit der DSGVO innerhalb einer spezifischen Branche zu beseitigen.

Ein wesentlicher Bestandteil dieser Selbstverantwortung im Rahmen der Schaffung von solchen Verhaltensregeln ist die obligatorische Überwachung von Verhaltensregeln, die einer Überwachungsstelle („monitoring body") obliegt. Allerdings ist zu beachten, dass nur eine durch die Datenschutzbehörde akkreditierte Stelle als Überwachungsstelle eingesetzt werden kann. Eine Überwachungsstelle muss daher zunächst einen Antrag auf Akkreditierung stellen.

Die Anforderungen an eine solche Akkreditierung wurden auf nationaler Ebene gemäß Art. 40 Abs. 3 DSGVO, Art. 57 Abs. 1 lit. p DSGVO und § 21 Abs. 3 DSG in der Überwachungsstellenakkreditierungs-Verordnung (ÜStAkk-V), BGBl. II Nr. 264/2019 konkretisiert.

Die Akkreditierung als Überwachungsstelle erfolgt auf Grund eines schriftlichen Antrages an die Datenschutzbehörde unter Einhaltung der in der ÜStAkk-V normierten Voraussetzungen. Demnach hat eine Überwachungsstelle insbesondere ihre Unabhängigkeit und ihr Fachwissen nachzuweisen, Maßnahmen zur Verhinderung von Interessenkonflikten zu treffen und geeignete Überwachungs- und Streitbeilegungsverfahren im Zusammenhang mit den Verhaltensregeln zu implementieren.

Zu beachten ist, dass die Antragstellung als Überwachungsstelle auch für eine Organisationseinheit innerhalb jener Verbände und anderen Vereinigungen, welche die Verhaltensregeln gemäß Art. 40 Abs. 2 DSGVO ausgearbeitet, geändert oder erweitert haben, zulässig ist („interne Stellen"). Eine solche interne Stelle hat jedoch zusätzlich durch Erläuterung ihrer Organisationsstruktur darzulegen, weshalb eine Aufgabenerfüllung ohne Einflussnahme durch den Verband oder die Vereinigung möglich ist.

Zur effizienten Abwicklung der Verfahren ist es sinnvoll, dass sich Antragsteller auf Genehmigung von Verhaltensregeln und Antragsteller, die die Akkreditierung der entsprechenden Überwachungsstelle beantragen, koordinieren und zeitgleich ihre Anträge bei der Datenschutzbehörde einbringen. Im Hinblick auf jene Verhaltensregeln, die bereits unter der Bedingung der (späteren) Akkreditierung einer Überwachungsstelle genehmigt wurden, ist festzuhalten, dass die mit der Unterwerfung unter die Verhal-