Sind „interne Empfänger“ von Daten zu beauskunften?

In einem Auskunftsverfahren (noch unter DSG 2000) hat ein Krankenhaus einer Auskunftswerberin (einer Angestellten) zwar mitgeteilt, dass es Zugriffe auf ihre Daten gegeben hat, aber die konkreten Empfänger der Daten wurde nicht beauskunftet.

Ist eine derartige Auskunft zu erteilen?

Es wurde der Auskunftswerberin vom Verantwortlichen mitgeteilt, dass auf ihre **Patientendaten mehrere Male zugegriffen** wurde und diese **Zugriffe** als „**nicht plausibel**“ bezeichnet. Eine Angabe über die Personen / Empfänger der Daten erfolgte nicht.

In einem „Vorverfahren“ vor der DSB (DSB-D122.831/0003-DSB/2018, Bescheid vom 04.06.2018) hat der Verantwortliche mitgeteilt:

> *„Vom Datenverantwortlichen des Krankenhauses **** wurden dementsprechend die Zugriffsprotokolle ausgewertet, wobei unplausible Zugriffe von einer Person festgestellt wurden. Gemäß den Krankenhaus ****-internen Prozessabläufen wurde eine Stellungnahme von der/dem betreffenden Krankenhaus ****-MitarbeiterIn eingeholt. Die Bewertung der Stellungnahme ergab, dass diese Zugriffe nicht auf Basis eines Behandlungs- bzw. Betreuungsverhältnisses oder einer sonstigen rechtlichen Grundlage erfolgten und somit unzulässig waren.“*

Unerlaubte Zugriffe verletzten die betroffene Person im Recht auf Geheimhaltung

In diesem Vorverfahren wurde festgestellt, dass der Verantwortliche die Auskunftswerberin dadurch in ihrem **Recht auf Geheimhaltung verletzte**, indem es **unerlaubte Zugriffe** zumindest am 28. November 2016 (Zeit: 14:10:10), am 3. Jänner 2017 (Zeit: 08:44:47), 28. März 2017 (Zeit: 18:46:28 und 20:56:21) und am 12. April 2017 (Zeit: 09:05:51) auf ihren elektronischen Gesundheitsakt (ihre elektronische Krankengeschichte) gab.

Im Verfahren verwies die DSB darauf, dass der Verantwortliche die Zugriffe selbst als „unzulässig“ bezeichnet hatte, und diese auch nicht erklären konnte. Daher wurde der Eingriff in das Grundrecht auf Datenschutz von der DSB bescheidmäßig festgestellt.

Gibt es ein Recht auf Auskunft, wer (innerhalb der Organisation des Verantwortlichen) auf die Daten zugegriffen hat?

Das Verfahren war dadurch jedoch nicht beendet, da die Auskunftswerberin nicht nur in ihrem Recht auf Geheimhaltung verletzt wurde, sondern der Verantwortliche auch nicht mitgeteilt hat, wer auf die Daten zugegriffen hatte.

Der Verantwortliche stellte sich auf den Standpunkt, dass „**Protokolldateien**“ **nicht zu beauskunften** seien.

Die DSB hat 06.06.2018 (DSB-D122.829/0003-DSB/2018, rk) dazu (in einem Verfahren, dass vor dem 25.05.2018 begonnen hatte) entschieden:

> „Nach dem Erkenntnis des Bundesverwaltungsgerichts zur GZ W214 2117640-1 vom 11. Juli 2017 zur Frage, ob Protokolldaten nach § 14 DSG 2000 zu beauskunften sind, unterliegen **Abfragen von Mitarbeitern des Verantwortlichen, die sich innerhalb des ursprünglichen Aufgabengebietes bewegen, nicht der Auskunftspflicht, solange sie keine Übermittlungen darstellen**.

Keine Auskunft bei „berechtigten“ Zugriffen

Wenn daher **Daten im bisherigen Aufgabengebiet verwendet** werden, und **keine „Zweckänderung“** vorliegt, dann stellte dies nach DSG 2000 keine „Übermittlung“ dar, sodass eine **Auskunft nicht erfolgen** musste.

Auskunftspflicht bei „unberechtigten“ Zugriffen

Die DSB führt diese Rechtsprechung des BVwG fort:

> „Auch nach Art. 15 Abs. 1 lit. c DSGVO sind Empfänger, gegenüber denen Daten offengelegt worden sind, zu beauskunften.
>
> Nach Art. 4 Z 9 DSGVO ist „**Empfänger**“ eine **natürlich oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.**
>
> Art. 4 Z 10 DSGVO definiert „**Dritter**“ als eine natürlich oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den **Personen, die unter unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind**, die personenbezogenen Daten zu verarbeiten.“

Die DSGVO geht daher nicht davon aus, dass Empfänger von Daten nur Organisationen oder Personen sind, die vom Verantwortlichen verschieden sind. Auch **„Stellen“ in der Organisation** sind daher **Empfänger** von personenbezogenen Daten, sobald sie Zugriff auf diese Daten haben.

Die DSGVO definiert als „Dritte“ auch Personen in der Organisation des Verantwortlichen / Auftragsverarbeiters, die nicht befugt sind, auf die Daten zuzugreifen (Argument aus Art 4 Z

10 DSGVO: „befugt“ sind. Unzulässige Zugriffe, für die es keine rechtliche Begründung gibt, sind daher Zugriffe von „Dritten“, weil die Person, die Zugriff hat, „nicht befugt war, die personenbezogenen Daten zu verarbeiten.“

Wenn daher **unberechtigte Zugriffe auf personenbezogene Daten** (in der Organisation eines Verantwortlichen) erfolgen, dann sind die **Protokolldateien** darüber auch zu **beauskunften**, und die betroffene Person hat das Recht, konkret zu erfahren, wer (unberechtigt) auf die Daten zugegriffen hat.

dataprotect
it-recht