DSB: Auftrag an einen Verantwortlichen - Verlust von Gesundheitsdaten in einem Buch

Verlust des Suchtmittelbuches verpflichtet zur Benachrichtigung der Patienten, wenn nicht sichergestellt ist, dass dasselbe nicht in falsche Hände gerät, oder das Risiko zB durch Pseudonymisierung reduziert wurde.

Data Breach Meldung führt zu einem Auftrag der DSB auch die betroffenen Personen zu verständigen; Bescheid der DSB vom 08.08.2018, DSB-D084.133/0002-DSB/2018

Suchtgiftbuch mit 150 Patientendaten geht verloren – der Verantwortliche meldet es der DSB – das ist nicht genug!

Am 12. Juli 2018 meldete ein Verantwortlicher, dass am 10. Juli 2018 ein **Suchtgiftbuch** während eines Notarzteinsatzes am 10. Juli 2018 „irgendwo im Bezirk U*** auf der Straße“ verloren gegangen sei.

In dem Suchtmittelbuch sind die gemäß Suchtmittelgesetz geforderten Ein- und Ausgänge des Suchtmitteldepots dokumentiert.

Dabei handle es sich um eine **strukturierte Ablage von personenbezogenen Daten** (zum Teil besondere Kategorien von Daten) in **Papierform**. Eine Verschlüsselung der Daten habe nicht stattgefunden.

Das verlorene Suchmittelbuch umfasste **Daten von 150 Patienten**, mit **Vor- und Nachname, körperlicher Gesundheitszustand, verabreichte Menge des Suchtgiftes** sowie die **ausgegebene Menge** betroffen; des weiteren Datensätze von sieben externen Mitarbeitern (Notärzte der S***-Kliniken) sowie von ca. 50 Notfallsanitätern (jeweils Personalnummer und Unterschrift).

Die DSB will mehr Informationen

Am 24. Juli 2018 erteilt die DSB einen Verbesserungsauftrag und ersuchte um Bekanntgabe, weshalb der Verantwortliche davon ausging, dass für die betroffenen Personen kein hohes Risiko bestehen sollte bzw. ob die betroffenen Personen informiert worden sind. Weiters sollten Angaben zum Schutzniveau für das Suchtmittelbuch gemacht werden, und ob dieses auch in einer elektronischen Fassung vorliege. Weiters verlangte die DSB Informationen über die Maßnahmen zur Abmilderung der möglichen nachteiligen Auswirkungen für die betroffenen Personen.

dataprotect
it-recht

Der Verantwortliche ergänzt, und erklärt, warum er die betroffenen Personen seiner Ansicht nach nicht verständigen musste

Im Rahmen der Stellungnahme bezog sich der Verantwortliche dann auf alle möglichen Folgen, die in der DSGVO genannt sind.

Auszug aus dem Bescheid (Hervorhebungen vom Verfasser):

> *„Zu den möglichen Folgen der Sicherheitsverletzung für die Rechte und Freiheiten natürlicher Personen nahm die Verantwortliche wie folgt Stellung:*
>
> *Die Wahrscheinlichkeit der **Bloßstellung**, des **Identitätsdiebstahls** bzw. –**betrugs** wurde als „sehr gering" und die Schwere der möglichen Folgen als begrenzt eingeschätzt. Die Wahrscheinlichkeit des **Verlustes der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten** sei als „gering" einzuschätzen. **Rufschädigende und diskriminierende Folgen**, **finanzielle Verluste**, **erhebliche wirtschaftliche oder gesellschaftliche Nachteile** sowie die **unbefugte Aufhebung der Pseudonymisierung** würden aus der verfahrensgegenständlichen Verletzung nicht resultieren. …*
>
> *Die **Verletzung der Verfügbarkeit** der personenbezogenen Daten beeinträchtige die Betroffenen in keiner Weise, da die personenbezogene Datenverarbeitung lediglich einer gesetzlichen Dokumentationspflicht des Verantwortlichen diene. Die **Verletzung der Vertraulichkeit** könne zwar potentiell die oben beschriebenen Folgen für die Betroffenen haben, die Wahrscheinlichkeit dafür sei jedoch als sehr gering bis gering einzustufen, da es unwahrscheinlich sei, dass das Buch zufällig von jemanden gefunden werde und zu diesem Zeitpunkt aufgrund der Witterungseinflüsse überhaupt noch lesbar sei. Die **verarbeiteten personenbezogenen Daten „in den falschen Händen"** ermöglichten eine Bloßstellung bzw. einen Identitätsdiebstahl/ - betrug nur mit großem Rechercheaufwand und Hinzuziehung weiterer Informationen aus anderen Quellen.*

Die DSB sieht es anders und erteilt einen Auftrag:

> *„Der Verantwortlichen wird aufgetragen, innerhalb einer Frist von vier Wochen jene Personen, deren Gesundheitsdaten von der Sicherheitsverletzung vom 10. Juli 2018 betroffen sind, zu benachrichtigen und einen Nachweis darüber sowie das Schreiben in Kopie an die Datenschutzbehörde zu übermitteln."*

Das sind die Überlegungen der DSB:

Die Behörde zog daraus folgenden Schluss:

a) Es liegt eine Verletzung des Schutzes von personenbezogenen Daten vor, nämlich ein Verlust von Daten (Art 4 Nr 12 DSGVO inkludiert auch den Verlust)

b) Es sind **Gesundheitsdaten** betroffen.

c) Die **Prognoseentscheidung** eines Verantwortlichen im Rahmen einer Datenschutzvorfallmeldung, dass kein hohes Risiko für die Rechte und Grundfreiheiten der betroffenen Personen gegeben ist, kann im Rahmen der Prüfung der Benachrichtigungspflicht gem. Art 34 DSGVO (Benachrichtigung der betroffenen Personen) **überprüft** werden.

d) Schon **150 Datensätze** bei Gesundheitsdaten bewirken ein hohes Risiko, da dies typischerweise bei **umfangreichen Verarbeitungen** von besonderen Datenkategorien verwirklicht wird.

e) Eine **Eintrittswahrscheinlichkeit** ist dann gegeben bzw. wird von der DSB vermutet, wenn nicht auszuschließen ist, dass sich das Risiko verwirklicht und der Verantwortliche keine Präventivmaßnamen (zB Pseudonymisierung) gesetzt hat.

f) **Nachfolgende Sicherheitsmaßnahmen**, die nicht geeignet sind, das Risiko zu minimieren, sind für die DSB in der Entscheidung, ob die betroffenen Personen zu benachrichtigen sind, unbeachtlich.

g) Es ist der „**normale Gang der Dinge**“ zu berücksichtigen, wenn dargelegt wird, weshalb davon ausgegangen wird, dass ein Risiko sich nicht realisiert, wobei der Verantwortliche die Behauptungs- und Beweislast dafür trägt, dass der Schaden nicht eintritt.

Die DSB führt dazu aus (Hervorhebungen durch den Verfasser):

> „Die **Schwere des Risikos** (Schadensschwere) für die Rechte und Freiheiten beurteilt sich nach dem **Gewicht des bedrohten Rechts bzw. der bedrohten Freiheit** sowie danach, **welche Schäden** den betroffenen Personen aus der Verarbeitung erwachsen können. […]. Ein **hohes Risiko** besteht demnach insbesondere und jedenfalls t**ypischerweise bei umfangreichen Verarbeitungen besonderer Kategorien personenbezogener Daten** iSd Art. 9 Abs. 1 DSGVO, worunter auch Gesundheitsdaten fallen (vgl. Paal/Pauly, Datenschutz-Grundverordnung, Kommentar, Art. 34, Rn. 30).
>
> Im gegenständlichen Fall ist von der Sicherheitsverletzung eine **umfangreiche Verarbeitung von Gesundheitsdaten** umfasst. Die drohende Schadensschwere ist demnach hoch.
>
> Die **Eintrittswahrscheinlichkeit** für einen möglichen Schaden ist gegeben, da das Suchtgiftbuch nicht gefunden wurde. Es entbehrt nicht jeder Lebensrealität, dass das Suchtgiftbuch von einem Unbefugten gefunden wurde bzw. noch gefunden wird.

Die Voraussetzungen für die Benachrichtigung der Verletzung an die betroffenen Personen sind folglich gegeben. Es liegt auch keine Ausnahme der Benachrichtigungspflicht gemäß Art. 34 Abs. 3 DSGVO vor:

Die Verantwortliche hat keine geeigneten präventiven Sicherheitsvorkehrungen gemäß Art. 34 Abs. 3 lit. a DSGVO getroffen, die das Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen deutlich reduziert hätten. Eine Vorkehrung, durch die die betroffenen Daten für Unberechtigte unzugänglich gemacht werden, etwa durch Verschlüsselung bzw. Pseudonymisierung, wurde von der Verantwortlichen nicht getroffen.

Auch die **nachfolgenden Sicherheitsmaßnahmen**, nämlich das Suchen des Suchtgiftbuches und die Information bzw. Aufklärung der Mitarbeiter der Verantwortlichen, waren jedenfalls **nicht geeignet, das anfänglich hohe Risiko zu minimieren**. Auch der Hinweis auf die witterungsbedingte Unlesbarkeit des Suchtgiftbuches stützt sich lediglich auf Vermutungen der Verantwortlichen, die nicht geeignet sind zu widerlegen, dass bei einem **normalen Gang der Dinge** damit gerechnet werden muss, dass sich ein Schadensereignis realisiert (vgl. Art. 34 Abs. 3 lit. b DSGVO).

Die **Benachrichtigung** der betroffenen Personen ist schließlich **nicht mit einem unverhältnismäßigen Aufwand** gemäß Art. 34 Abs. 3 lit. c DSGVO verbunden. Von der Sicherheitsverletzung sind die Gesundheitsdaten von ca. 150 Personen betroffen.

Die **Wiederherstellung der Daten** ist laut Vorbringen der Verantwortlichen – wenn auch mit Aufwand – möglich.