GZ: DSB-D084.133/0002-DSB/2018 vom 8.8.2018

[Anmerkung Bearbeiter: Namen und Firmen, Rechtsformen und Produktbezeichnungen, Adressen (inkl. URLs, IP- und E-Mail-Adressen), Aktenzahlen (und dergleichen), etc., sowie deren Initialen und Abkürzungen können aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein. Offenkundige Rechtschreib-, Grammatik- und Satzzeichenfehler wurden korrigiert.]

B E S C H E I D

S P R U C H

Die Datenschutzbehörde entscheidet aufgrund des durch die Meldung einer Datenschutzverletzung des N*** Hilfs- und Rettungsverbandes, Landesverband **** (Verantwortliche), vom 12. Juli 2018 eingeleiteten Verfahrens betreffend eine Verletzung des Schutzes personenbezogener Daten wie folgt:

- 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.

Rechtsgrundlagen: Art. 4 Z 12 und Z 13, Art. 33, Art. 34 und Art. 58 Abs. 2 lit. e der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), ABl. Nr. L 119 S. 1.

B E G R Ü N D U N G

A. Verfahrensgang

1. Mit Schreiben vom 12. Juli 2018 meldete der N*** Hilfs- und Rettungsverband, Landesverband **** (Verantwortlicher), die Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO.

Demnach sei während eines Einsatzes des Notarzteinsatzfahrzeuges R*** am 10. Juli 2018 das Suchtgiftbuch „irgendwo im Bezirk U*** auf der Straße“ verloren gegangen. In dem Suchtmittelbuch seien die gemäß Suchtmittelgesetz geforderten Ein- und Ausgänge des Suchtmitteldepots dieser Einsatzressource dokumentiert worden. 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.

Von der Verletzung seien ca. 150 Datensätze der Patienten des Rettungsdienstes der Kategorien 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) der Verantwortlichen sowie von ca. 50 Notfallsanitätern der Kategorie Personalnummer und Unterschrift.

Die Suche nach dem Suchtgiftbuch durch die Mannschaft sowie durch die Sachbearbeiterin „P**“ am 10. bzw. 11. Juli 2018 sei erfolglos geblieben. Die zuständige stützpunktkoordinierende Notärztin, der Landes-Notarzt-Koordinator sowie die zuständige Krankenhaus-Apotheke seien über den Vorfall informiert worden.

2. Mit Verbesserungsauftrag der Datenschutzbehörde vom 24. Juli 2018 wurde die Verantwortliche aufgefordert ihre Meldung binnen zwei Wochen zu ergänzen. Insbesondere fehle Information darüber, ob die betroffenen Personen von der Sicherheitsverletzung informiert worden seien bzw. eine Begründung, warum die Verantwortliche davon ausgehe, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem hohen Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen führe. Aus der Meldung gehe nicht hervor, ob eine Verlustmeldung erstattet worden sei, ob über die Suche des Suchtgiftbuches hinausgehende Maßnahmen zur Behebung der Verletzung sowie über die Information der zuständigen Ärzte und Krankenhausapotheke hinausgehende Maßnahmen zur Abmilderung der möglichen nachteiligen Auswirkungen für die betroffenen Personen gesetzt worden seien. Darüber hinaus, ob das Suchtgiftbuch auch in einer elektronischen Fassung vorliege oder eine Kopie desselben vorhanden sei bzw. welche Vorkehrungen generell getroffen würden, um sicherzustellen, dass die Daten eines Suchtgiftbuches in einer Weise verarbeitet würden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleisteten.

3. Mit Schreiben vom 30. Juli 2018 ergänzte die Verantwortliche ihre Meldung der Sicherheitsverletzung gemäß Art. 33 DSGVO. Insbesondere führte sie aus, dass das Suchtgiftbuch nicht mehr wiedergefunden worden sei und keine Kopie oder elektronische Fassung vorliege. Eine Pseudonymisierung der Daten sei nicht erfolgt.

In Bezug auf generelle Vorkehrungen zur Gewährleistung einer angemessenen Sicherheit der Verarbeitung personenbezogener Daten wurde ausgeführt, das Suchtgiftbuch werde im Einsatzfahrzeug in der Dokumentationsmappe gelagert; Zutritt in das Fahrzeug habe nur das diensthabende Personal (Sanitäter, Notarzt und Auszubildende). Es gebe keine Datensicherung und nur eine Möglichkeit der Wiederherstellung über andere Quellen (Einsatz- und Notarztdokumentation sowie andere Suchtgiftbücher, in welchen ein

Übertrag in das betroffene Depot vermerkt sei). Dies könne händisch mit einigem Aufwand durchgeführt werden.

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.

Diese Risikobewertung ergebe, dass zwar eine Behördenmeldung zwingend zu erfolgen habe; jedoch keine Betroffeneninformation. Die Benachrichtigung an die betroffenen Personen sei nicht erfolgt, weil die Risikobewertung auf Basis der vorliegenden Daten und Fakten kein potentiell hohes Risiko ergebe. 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.

B. Verfahrensgegenstand

Gegenständlich ist die Frage zu klären, ob im Verfahren betreffend die Sicherheitsverletzung gemäß Art. 33 DSGVO unter Berücksichtigung der Wahrscheinlichkeit mit der die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko gemäß Art. 34 DSGVO führt, die Datenschutzbehörde der Verantwortlichen den Auftrag zu erteilen hat, die Benachrichtigung der betroffenen Personen nachzuholen.

C. Sachverhaltsfeststellungen

Am 12. Juli 2018 meldete der Verantwortliche eine Sicherheitsverletzung gemäß Art. 33 DSGVO, demnach am 10. Juli 2018 das verfahrensgegenständliche Suchtgiftbuch verloren wurde.

Im Suchtgiftbuch werden die Ein- und Ausgänge des Suchtmitteldepots dokumentiert. Bei den Ausgängen in Form von Verabreichungen am Patienten sind der Patientenname sowie der Wirkstoff bzw. das Präparat und die Anzahl der Ampullen (maximal verabreichte Dosis) notiert. Eine Verschlüsselung bzw. Pseudonymisierung der Daten ist nicht erfolgt.

Von der Verletzung der Verfügbarkeit sind Datensätze von ca. 150 Patienten umfasst, welche Daten der Kategorien Vor- und Nachname, körperlicher Gesundheitszustand sowie verabreichtes Suchtgift und ausgegebene Menge desselben betreffen. Darüber hinaus sind die Personalnummer und Unterschrift von sieben externen Mitarbeitern (Notärzte der S***-Kliniken) und ca. 50 Mitarbeitern der Verantwortlichen (Notfallsanitäter) von der Verletzung umfasst.

Die Wiederherstellung der Daten ist möglich. Die personenbezogenen Einträge der Verabreichung können aus der Einsatz- und Notarztdokumentation sowie den Aus- und Eingängen des Suchtgiftdepots der Krankenhausapotheke extrahiert werden.

Eine Benachrichtigung der von der Verletzung betroffenen Personen gemäß Art. 34 Abs. 1 DSGVO erfolgte nicht.

Beweiswürdigung: Die getroffenen Feststellungen beruhen auf dem Vorbringen der Verantwortlichen in der Meldung vom 12. Juli 2018 sowie in der ergänzenden Stellungnahme vom 30. Juli 2018.

D. In rechtlicher Hinsicht folgt daraus:

Gegenständlich liegt durch das Verlieren des personenbezogene Daten aufzeichnenden Suchtgiftbuches eine Verletzung des Schutzes personenbezogener Daten aufgrund Verlust vor (vgl. Art. 4 Z 12 DSGVO).

Da im Suchtgiftbuch die Vor- und Nachnamen, der körperliche Gesundheitszustand sowie das verabreichte Suchtgift und die ausgegebene Menge desselben aufgezeichnet wurde, sind von der Verletzung auch Gesundheitsdaten gemäß Art. 4 Z 15 DSGVO betroffen.

Gemäß Art. 34 Abs. 1 DSGVO hat der Verantwortliche die betroffene Person dann unverzüglich von der Verletzung zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte

und Freiheiten natürlicher Personen zur Folge hat und keine Ausnahme nach Art. 34 Abs. 3 DSGVO vorliegt. Ob „voraussichtlich ein hohes Risiko“ vorliegt, hat die Verantwortliche selbst in einer Prognoseentscheidung zu treffen, wobei zur Beurteilung, ob ein solches vorliegt, auf die Leitlinien der Art. 29-Gruppe über die Meldung einer Verletzung des Schutzes personenbezogener Daten gemäß der Verordnung 2016/679 (WP250rev.01), abrufbar über die Website der Datenschutzbehörde, zurückgegriffen werden kann.

Die Benachrichtigungspflicht kann gemäß Art. 34 Abs. 4 DSGVO von der Datenschutzbehörde überprüft werden.

Gegenständlich kam die Verantwortliche in ihrer Prognoseentscheidung zu dem Schluss, dass „aufgrund der vorliegenden Daten und Fakten kein potentiell hohes Risiko“ gegeben sei.

Dieser Einschätzung kann jedoch aus folgendem Grund nicht gefolgt werden:

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. Einige mögliche Schadensereignisse sind im Erwägungsgrund ErwGr 75 der DSGVO ausdrücklich hervorgehoben. Ein hohes Risiko besteht demnach insbesondere und jedenfalls typischerweise 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.

Im Ergebnis ist davon auszugehen, dass die Benachrichtigung Betroffener geeignet ist, pro futuro weitere Verletzungen für die persönlichen Rechte und Freiheiten Betroffener zu vermeiden. Die Verantwortliche hat demnach alle Personen (ca. 150), deren Gesundheitsdaten von der Sicherheitsverletzung betroffen sind, zu benachrichtigen.

In zeitlicher Hinsicht hat die Benachrichtigung betroffener Personen von der Verletzung grundsätzlich unverzüglich zu erfolgen (vgl. auch ErwGr. 86). Im konkreten Einzelfall ist die Benachrichtigung innerhalb einer Frist von vier Wochen angemessen, da die vom Verlust betroffenen Daten händisch mit einigem Aufwand aus anderen Aufzeichnungen extrahiert werden müssen, bevor eine individuelle Benachrichtigung der Betroffenen stattfinden kann.

Es war daher spruchgemäß zu entscheiden.

Abschließend wird darauf hingewiesen, dass eine individuelle Adressierung der Betroffenen, etwa durch E-Mail, auf dem Postweg oder auf andere, sie individuell adressierenden Weise zu erfolgen hat. Die Benachrichtigung muss in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten enthalten und zumindest die in Art. 33 Abs. 3 lit. b, c und d DSGVO genannten Informationen und Empfehlungen umfassen.