TE Dsk BescheidAmtswegigesPruefverfahren 2023/1/30 2023-0.046.014

JUSLINE Entscheidung

Veröffentlicht am 30.01.2023

Norm

WStV §67
WStV §71 Abs1
WStV §71 Abs2
WStV §71 Abs3
WiGev-Statut §1 Abs1
WiGev-Statut §4
WiGev-Statut §7 Abs1
DSGVO Art4 Z12
DSGVO Art4 Z15
DSGVO Art9 Abs1
DSGVO Art33 Abs1
DSGVO Art33 Abs4
DSGVO Art34 Abs1
DSGVO Art34 Abs2
DSGVO Art34 Abs3 lita
DSGVO Art34 Abs3 litb
DSGVO Art34 Abs3 litc
DSGVO Art34 Abs4
DSGVO Art57 Abs1 lita
DSGVO Art57 Abs1 litv
DSGVO Art58 Abs2 lite
DSGVO ErwGr75
DSGVO ErwGr85
DSGVO ErwGr86
EDSA Leitlinien 07/2020 Rz19
EDSA Leitlinien 09/2022 Rz19
EDSA Leitlinien 09/2022 Rz102
EDSA Leitlinien 09/2022 Rz106
EDSA Leitlinien 09/2022 Rz107

EDSA Leitlinien 09/2022 Rz111
EDSA Leitlinien 09/2022 Rz112
EDSA Leitlinien 09/2022 Rz114

Text

GZ: 2023-0.046.014 vom 30. Jänner 2023 (Verfahrenszahl: DSB-D084.4371)

[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.

Der Name der Beschwerdegegnerin, einschließlich der städtischen Unternehmung, wird in diesem Bescheid wiedergegeben. Es handelt sich bei der Betroffenen um eine Körperschaft öffentlichen Rechts, die betreffenden Namen gehen aus mehreren zitierten Rechtsvorschriften eindeutig hervor. Eine sinnvolle und sinnerhaltende Pseudonymisierung des Namens der Beschwerdegegnerin in dieser gemäß § 23 Abs. 2 DSG zu veröffentlichenden Entscheidung war daher nicht möglich.]

BESCHEID

SPRUCH

Die Datenschutzbehörde entscheidet aufgrund der Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO der Stadt Wien – Wiener Gesundheitsverbund (WiGev) (Verantwortliche), vertreten durch den Magistrat der Stadt Wien, vom 11. November 2022 wie folgt:

? Der Verantwortlichen wird aufgetragen, innerhalb einer Frist von zwei Wochen, die betroffene Person von der sich am **. Juni 2022 ereigneten und der Verantwortlichen am 3. November 2022 zur Kenntnis gelangten Sicherheitsverletzung, konkret die Veröffentlichung des elektronischen Krankendekurses der betroffenen Person im Rahmen eines Social-Media-Beitrags einer Mitarbeiterin der Verantwortlichen, im Sinne des Art. 34 Abs. 1 und Abs. 2 DSGVO zu benachrichtigen.

Rechtsgrundlagen: Art. 4 Z 12 und Z 15, Art. 33 Abs. 1 und Abs. 4, Art. 34 Abs. 1, Abs. 2 und Abs. 4, Art. 51 Abs. 1, Art. 57 Abs. 1 lit. a und lit. v sowie Art. 58 Abs. 2 lit. e der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, im Folgenden: DSGVO), ABl. Nr. L 119 vom 04.05.2016, S. 1; § 18 Abs. 1 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999 idgF; § 71 Abs. 1, Abs. 2 und Abs. 2 der Verfassung der Bundeshauptstadt Wien (Wiener Stadtverfassung, im Folgenden: WStV), LGBl. Nr. 28/1968 idgF; § 1 Abs. 1, § 4 sowie § 7 Abs. 1 leg. cit. der Verordnung des Gemeinderates, mit der ein Statut für die Unternehmung „Wiener Gesundheitsverbund“ erlassen wird, ABl 2020/02.

BEGRÜNDUNG

A. Vorbringen der Parteien und Verfahrensgang

1. Mit Eingabe vom 11. November 2022 erstattete dieVerantwortliche, vertreten durch die für Datenschutz zuständige Abteilung des Magistrats der Stadt Wien, nachfolgendes Vorbringen:

Die gegenständliche Meldung gemäß Art. 33 DSGVO erfolge lediglich „vorsichtshalber“, da vorerst nicht mit Sicherheit geklärt sei, ob der verfahrensgegenständliche Sachverhalt tatsächlich ihrer datenschutzrechtlichen Verantwortlichkeit unterliege. Angesichts der Judikatur des Bundesverwaltungsgerichtes sei auch die eigenständige Verantwortlichkeit der handelnden Person möglich. Zudem könne ein Risiko derzeit nicht gänzlich ausgeschlossen werden.

Die Verantwortliche habe am 3. November 2022 eine anonyme E-Mail bezüglich der Veröffentlichung von drei Fotos im sozialen Netzwerk „***media“ erhalten. Die internen Meldewege für die Behandlung von „Data Breaches“ habe nicht einwandfrei funktioniert, weshalb die zuständige Abteilung und Vertreterin im gegenständlichen Verfahren erst am 10. November 2022 über den Vorfall informiert worden sei. Dem Inhalt der E-Mail nach, habe eine Studierende in ihren Pflege-Praktika bei der Verantwortlichen Fotos gemacht und auf ***media gepostet. Von diesen Fotos sei lediglich ein im Juni 2022 aufgenommenes Foto der Verantwortlichen zurechenbar. Die anderen Fotos seien in eigener Verantwortung der handelnden Person angefertigt und zudem nach deren Angabe von einer Einwilligung gedeckt gewesen. Das relevante Foto sei im Zeitraum des Praktikums der Studierenden vom **. Mai 2022 bis **. Juli 2022 in der Klinik **** entstanden und vor der Veröffentlichung auf ***media teilweise geschwärzt worden. Auf dem Foto sei

der „elektronische Dekurs“ einer Patientin der genannten Klinik zu sehen. Einige Bereiche seien zwar geschwärzt, ungeachtet dessen seien jedoch folgende personenbezogene Daten erkennbar: Name, Vorname, Patientenzahl, Station, Datum sowie Informationen über Pflegeaktivitäten (Details zur Pflege wie das „Setzen eines Venflons“). Des Weiteren Userkürzel von drei Mitarbeiter*innen der Klinik sowie deren Arbeitsbereich (Akutgeriatrie). Erst nach Veröffentlichung (Teilen) des Posts sei aufgefallen, dass die Schwärzung nicht vollständig gewesen sei. Die betroffenen personenbezogenen Daten – Auszüge aus dem elektronischen Dekurs – seien als Gesundheitsdaten zu qualifizieren. Bezüglich der betroffenen Patientin könne ein Risiko für die Rechte und Freiheiten nicht gänzlich ausgeschlossen werden, da durch die Veröffentlichung des Bildes ein Kontrollverlust eingetreten sei. Mögliche Risiken seien etwa Identitätsdiebstahl, Phishing, Veräußerung der Daten, Veröffentlichung bzw. öffentliche Bloßstellung, finanzielle Verluste, wirtschaftliche oder gesellschaftliche Nachteile. Mit der Studentin sei von der vorgesetzten Stelle ein Gespräch geführt worden. Der Studentin sei es dabei wichtig gewesen zu betonen, dass die Fotos gepostet worden seien, um Erfahrungen und Tätigkeiten im Rahmen des Pflegeberufs positiv darzustellen und sie bedauere den Vorfall zutiefst. Entsprechende dienstrechtliche Maßnahmen seien bereits getroffen worden, insbesondere ein Hinweis auf die Verpflichtungen nach der DSGVO. Aufgrund einer internen Risikoanalyse könne derzeit kein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen erkannt werden. Eine Verständigung iSd. Art. 34 DSGVO sei daher derzeit nicht geplant.

2. Infolge entsprechender Aufforderungen zur ergänzenden Stellungnahme durch dieDatenschutzbehörde erstattete die Verantwortliche am 14. November 2022, am 21. Dezember 2022, am 22. Dezember 2022 sowie abschließend am 18. Jänner 2023 Folgemeldungen.

3. Im Rahmen der Folgemeldungen ergänzte dieVerantwortliche zusammengefasst wie folgt:

Es sei davon auszugehen, dass die Veröffentlichung des Fotos auf ***media am **. Juni 2022 erfolgte und der Beitrag („Posting“) nur für drei Stunden online gewesen und danach eine manuelle Löschung durch die Studentin erfolgt sei. Anzumerken sei weiters, dass die Verantwortliche mangels eigener Verantwortung für das Posten auf ***media auf die Angaben der Studentin angewiesen sei. Innerhalb der drei Stunden hätten sich ungefähr 100 Personen den Post in der „Story“ angesehen. Die angegebene Anzahl von 100 Personen entspreche einem Mittelwert betreffend die ***media-Storys der Studentin. Sie habe 630 Follower (bestätigte Abonnenten) und sei das ***media-Profil auf „privat“ eingestellt. Ausschließlich diese Personen hätten somit überhaupt einen (theoretischen) Zugriff auf die ***media-Storys. Im Zeitpunkt der Meldung an die Datenschutzbehörde sei unklar gewesen, ob das Tatbestandselement der unbefugten Offenlegung iSd. Art. 4 Z 12 DSGVO an die Studentin, die das Foto eigenverantwortlich angefertigt und dann auf ***media veröffentlicht habe, erfüllt gewesen sei. Die Studentin sei grundsätzlich zum Aufruf des elektronischen Dekurses für berufliche Zwecke befugt gewesen. Sofern der Aufruf für einen solchen – zulässigen – Zweck erfolgt sei, wäre die Offenlegung an die Studentin nicht unbefugt gewesen. Mangels entsprechender Nachweise werde jedoch im Zweifel mittlerweile von einer unbefugten Offenlegung ausgegangen. Mit Ausnahme von Vor- und Nachname der Patientin seien keine weiteren zur direkten Identifizierung geeigneten personenbezogenen Daten wie z.B. Geburtsdatum, Sozialversicherungsnummer oder Adresse ersichtlich. Insofern sei es nach Ansicht der Verantwortlichen sehr unwahrscheinlich, einen Bezug zu einer konkreten Person herzustellen. Zudem lasse die Angabe der Station „Akutgeriatrie“ keinen Schluss auf das konkrete Alter und den konkreten Gesundheitszustand der Patientin zu. Akutgeriatrie besage lediglich, dass eine betreuungsintensive Pflege erforderlich sei. Aus der Angabe zur pflegerischen Aktivität „Setzen eines Venflons“ lasse sich keine Information auf den sonstigen Gesundheitszustand der Patientin ableiten. Aus dem elektronischen Dekurs seien daher keine weiteren Informationen zum Gesundheitszustand der Patientin ableitbar. Das aus dem Auszug ersichtliche Userkürzel der Mitarbeiter*innen könne ausschließlich durch autorisierte Mitarbeiter*innen der Verantwortlichen aufgelöst werden. Bei der Risikobewertung sei daneben auch die Dauer der Veröffentlichung herangezogen worden. Aufgrund der dargelegten fehlenden Identifizierbarkeit der Patientin (und der drei Mitarbeiter*innen) und der begrenzten Veröffentlichungsdauer sowie des eingeschränkten Personenkreises, denen der Post zugänglich gewesen sei, werde das Risiko für die Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen als gering eingeschätzt. Die Eintrittswahrscheinlichkeit für einen physischen, materiellen oder immateriellen Schaden wie Identitätsdiebstahl oder –betrug, finanziellem Verlust, Rufschädigung, Verletzung der Vertraulichkeit eines Berufsgeheimnisses oder anderen erheblichen gesellschaftlichen oder wirtschaftlichen Nachteilen werde ebenfalls als gering beurteilt und sei folglich auch keine Benachrichtigung der betroffenen Person erforderlich.

B. Beschwerdegegenstand

Gegenständlich ist die Frage zu klären, ob im Verfahren 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

1. Beim Wiener Gesundheitsverbund handelt es sich um eine Unternehmung der Stadt Wien, dessen Statut durch die Verordnung des Gemeindesrats der Stadt Wien GZ: V001/285/2020 erlassen worden ist. Der Wiener Gesundheitsverbund betreibt als Gesundheitsdienstleister u.a. acht Krankenanstalten (Kliniken), im Rahmen dessen eine Vielzahl medizinischer und gesundheitsbezogener Dienstleistungen erbracht werden.

2. Eine zur Verantwortlichen in einem Ausbildungsverhältnis stehende und bei einer der unter Punkt C.1. genannten Kliniken (konkret: „Klinik ****“) im verfahrensrelevanten Zeitpunkt tätige Mitarbeiterin (Praktikantin) hat im Rahmen ihrer Tätigkeit elektronisch vorhandene Daten einer Patientin (betroffene Person) der Verantwortlichen abgefragt und in weiterer Folge ein Lichtbild des elektronisch dokumentierten Krankheitsverlaufes derselben („elektronischer Dekurs“) im Rahmen ihres Social-Media Profils auf der Plattform „***media“ des Betreibers N*** Ltd im Juni 2022 veröffentlicht. Es handelt sich dabei um einen Beitrag in Form einer „***media Story“, welcher laut Standardeinstellung 24 Stunden nach dessen Veröffentlichung automatisiert gelöscht wird. Verfahrensgegenständlich war der Beitrag für rund drei Stunden sichtbar und wurde nachfolgend durch die Mitarbeiterin selbst gelöscht. Social-Media Beiträge der Mitarbeiterin werden durchschnittlich von rund 100 Personen angesehen.

3. Dem genannten Lichtbild waren folgende Informationen der Patientin (betroffene Person) zu entnehmen: Vor- und Nachname, Patientenzahl, Station (namentlich „Akutgeriatrie“) sowie Informationen über sie betreffende Pflegeaktivitäten (namentlich „Setzen eines Venflons“). Des Weiteren Namenskürzel und Arbeitsbereich von drei Mitarbeiter*innen der Verantwortlichen.

4. Eine Einwilligung betreffend die Veröffentlichung der unter Punkt C.3. genannten Informationen durch die betroffene Person lag zu keinem Zeitpunkt vor.

5. Der Verantwortlichen wurde die unter Punkt C.2. genannte Veröffentlichung am 3. November 2022 durch einen anonymen Hinweis zur Kenntnis gebracht, dieser wurde jedoch erst am 10. November 2022 an die intern zuständige Abteilung weitergeleitet, weshalb die verfahrenseinleitende (Erst-)Meldung an die Datenschutzbehörde am 11. November 2022 erstattet worden ist. Konkret erfolgt diese durch die für Datenschutz zuständige Abteilung des Magistrats der Stadt Wien. In weiterer Folge wurden mehrere ergänzende Meldungen und Stellungnahme durch die Verantwortliche eingebracht.

6. Bis zum Abschluss des gegenständlichen Verfahrens erfolgte keine Benachrichtigung und Information der von der unter Punkt C.2. genannten Veröffentlichung betroffenen Person.

Beweiswürdigung: Die getroffenen Feststellungen beruhen im Wesentlichen auf dem stringenten und insofern durchwegs glaubwürdigen Vorbringen der Verantwortlichen, vertreten durch die zuständige Abteilung des Magistrats Wien, im Rahmen der Erstmeldung vom 11. November 2022 sowie der Folgemeldungen. Die Feststellungen zu den Punkten C.1. sowie C.2. gründen sich darüber hinaus auf einer amtswegigen Abfrage der Webseiten des Wiener Gesundheitsgesundheitsverbundes unter www.gesundheitsverbund.at sowie der Nutzungsbedingungen von ***media unter www.***media.org, beides abgefragt am 20. Jänner 2023.

D. In rechtlicher Hinsicht folgt daraus:

D.1. Allgemeines und Rechtsgrundlagen

Gemäß Art. 33 Abs. 1 DSGVO meldet der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine

Begründung für die Verzögerung beizufügen. Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen (Abs. 4 leg. cit.).

Laut Art. 4 Z 12 DSGVO ist unter „Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zurunbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

In ErwG 85 DSGVO werden als mögliche Folgen einer Verletzung des Schutzes personenbezogener Daten – wenn nicht rechtzeitig und angemessen reagiert wird – u.a. ein physischer, materieller oder immaterieller Schaden durch Verlust der Kontrolle über personenbezogene Daten, Diskriminierung, Identitätsdiebstahl oder etwa Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person genannt. Aus diesen Gründen sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde unverzüglich unterrichten.

Hat die Verletzung des Schutzes personenbezogener Datenvoraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche gemäß Art. 34 Abs. 1 DSGVO die betroffene Person unverzüglich von der Verletzung. Die genannte Benachrichtigung der betroffenen Person beschreibt gemäß Abs. 2 leg. cit. in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Abs. 3 Buchstaben b, c und d leg. cit. genannten Informationen und Maßnahmen.

Laut Art. 34 Abs. 4 DSGVO kann die Aufsichtsbehörde, wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte Voraussetzungen erfüllt sind.

Die Benachrichtigung der betroffenen Person soll laut ErwG 86 dazu dienen, dass diese die erforderlichen Vorkehrungen treffen können. Solche Benachrichtigungen sollten stets so rasch wie möglich nach allgemeinem Ermessen und in enger Absprache mit der Aufsichtsbehörde erfolgen.

Gesundheitsdaten sind gemäß Art. 4 Z 15 DSGVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Sie sind laut Art. 9 Abs. 1 DSGVO als Daten besonderer Kategorie („sensible Daten") qualifiziert und ist bei deren Verarbeitung laut ErwG 75 leg. cit. mit einem gewissen (erhöhten) Risiko zu rechnen.

Laut § 71 Abs. 1 WStV handelt es sich bei „Unternehmungen" im Sinne dieses Gesetzes um jene wirtschaftlichen Einrichtungen, denen der Gemeinderat (der Stadt Wien) die Eigenschaft einer Unternehmung zuerkennt. Die Unternehmungen besitzen gemäß Abs. 2 leg. cit. keine Rechtspersönlichkeit. Ihr Vermögen wird vom übrigen Vermögen der Gemeinde gesondert verwaltet. Soweit eine Eintragung der Unternehmungen in das Firmenbuch erfolgt, muss aus der Bezeichnung ersichtlich sein, dass es sich um eine Unternehmung der Stadt Wien handelt.

Gemäß § 71 Abs. 3 WStV hat der Gemeinderat insbesondere unter Bedachtnahme auf den zweiten Absatz des § 67 leg. cit. für die Unternehmungen durch Verordnung ein Statut zu beschließen. Laut diesem obliegt dem Magistratsdirektor, der dem Bürgermeister unmittelbar unterstellt ist, die Leitung des inneren Dienstes des Magistrats und die Besorgung der ihm in der Geschäftseinteilung vorbehaltenen Aufgaben.

Laut Verordnung des Gemeinderates, mit der ein Statut für die Unternehmung „Wiener Gesundheitsverbund" erlassen wird, ist die Unternehmung „Wiener Gesundheitsverbund" eine wirtschaftliche Einrichtung, der der Gemeinderat die Eigenschaft einer Unternehmung zuerkannt hat (§ 1 Abs. 1 leg. cit.). Dem Gemeinderat steht die Oberaufsicht über die Unternehmung „Wiener Gesundheitsverbund" zu (§ 4 leg. cit.). Dem Bürgermeister ist der Magistratsdirektor sowie alle Bediensteten der Unternehmung „Wiener Gesundheitsverbund" untergeordnet (§ 7 Abs. 1 leg. cit.).

D.2. Zum Vorliegen einer Sicherheitsverletzung und zur diesbezüglichen Verantwortlichkeit

Dem unter Punkt D.1. zitierten Art. 33 Abs. 1 DSGVO ist ausdrücklich zu entnehmen, dass sich die darin normierte Meldeverpflichtung ausschließlich an den jeweiligen Verantwortlichen richtet. Da die Verantwortlicheneigenschaft im Laufe des Verfahrens mehrfach von der Verantwortlichen in Zweifel gezogen wurde, ist näher darauf einzugehen:

Eingangs kann der Verantwortlichen zwar insoweit zugestimmt werden, als dass aus (zweckwidrigen und unternehmensfremden) Datenabfragen uÄ durch Mitarbeiterinnen und Mitarbeiter – insbesondere zu rein privaten Zwecken – im Einzelfall eine eigenständige (uU ausschließliche) datenschutzrechtliche Verantwortlichkeit der natürlichen Person abgeleitet werden kann (vgl. etwa den Bescheid der DSB vom 25. November 2020, GZ: 2020-0.764.719).

Während sich die diesbezügliche Judikatur jedoch in erster Linie auf die im Rahmen von Individualbeschwerdeverfahren nach Art. 77 Abs. 1 DSGVO iVm. § 24 Abs. 1 DSG geltend gemachte Verantwortlichkeit für Verletzungen der Rechte von Betroffenen (in erster Linie im Recht gem. § 1 Abs. 1 DSG) bezieht, ist Gegenstand des vorliegenden Verfahrens vielmehr die – gewissermaßen vorgelagerte – Melde- und Benachrichtigungsverpflichtungen der (möglicherweise bloß ursprünglichen) Verantwortlichen.

Sinn und Zweck dieser Bestimmungen (Art. 33 und 34 DSGVO) ist nämlich in erster Linie die Prävention und Begrenzung möglich materieller und immaterieller Schäden für betroffene Personen (vgl. Martini in Paal/Pauly, Datenschutz-Grundverordnung (2017) Art. 33 Rz. 10-11).

Zudem führen die Guidelines 07/2020 des EDPB zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" aus, dass, selbst wenn ein Beschäftigter seine Befugnis iZm der Verarbeitung von Daten (unzulässigerweise) überschreitet, die Organisation als Verantwortlicher – ungeachtet dessen – angemessene technische und organisatorische Maßnahmen implizieren muss, um die Einhaltung der DSGVO sicherzustellen (EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, angenommen am 7. Juli 2021, Rz. 19).

Auch das Bundesverwaltungsgericht hielt iZm der eigenmächtigen Datenverwendung durch einen Bediensteten fest, dass die dahinterstehende Organisation (konkret: Behörde) weiterhin für die Art und Weise der Verarbeitung bzw. Verwendung durch deren Bedienstete verantwortlich sei, auch soweit es sich um eine sorgfaltswidrige Verwendung oder überschießende Akteneinsicht handle. In diesem Zusammenhang wurde darauf hingewiesen, dass rechtlich zwischen dem datenschutzrechtlich relevanten Verhalten der Behörde (als ursprüngliche Verantwortliche) und dem datenschutzrechtlich relevanten Verhalten eines/einer allfälligen Dritten zu unterscheiden sei. Abschließend wurde angemerkt, dass bei einer gegenteiligen Sichtweise eine Organisation jedwedes datenschutzrechtliches Fehlverhalten auf Bedienstete abwälzen und sich so ihrer Verantwortung gegenüber dem Rechtsschutzsuchenden entziehen könne (vgl. das Erkenntnis des BVwG vom 20. Jänner 2022, GZ: W214 2239688-1).

Schließlich ist noch der Wortlaut des Art. 4 Z 12 DSGVO zu beachten, wonach der Begriff „Verletzung des Schutzes personenbezogener Daten" jedenfalls so weit zu verstehen ist, dass auch vom Daten Verarbeitenden nicht beeinflussbare bzw. zumindest nicht auf dessen schuldhaftes Verhalten rückführbare (arg: „unbeabsichtigt") Sicherheitsverletzungen, welche zu einer unbefugten Offenlegung oder zu einem unbefugten Zugang führen, erfasst sein sollen.

Die korrespondierenden Guidelines 9/2022 des EDPB führen zum Begriff der „Verletzung" iSd Art. 33 DSGVO ausdrücklich den „Verlust der Kontrolle oder des Zugangs" durch den (ursprünglichen) Verantwortlichen an (vgl. EDPB Guidelines 9/2022 on personal data breach notification under GDPR, angenommen am 10. Oktober 2022, Rn. 19).

Insgesamt kann daher in einem Zwischenergebnis festgehalten werden, dass ein ursprünglich datenschutzrechtlicher Verantwortlicher – selbst bei Verlust der Verfügungsmacht über oder bei unberechtigtem Zugriff Dritter auf dessen Datenbestand – Verpflichteter iSd Art. 33 und 34 DSGVO ist bzw. bleibt und sich das diesbezügliche Vorbringen der Verantwortlichen daher als unbeachtlich erwies.

Wie den Feststellungen zu entnehmen ist, wurde die verfahrensgegenständlichen Daten der betroffenen Person (Patientin) im Rahmen einer medizinischen Behandlung in einer Krankenanstalt erhoben, welche vom „Wiener Gesundheitsverbund" – als Unternehmung – betrieben wird. Dieser wiederum ist – wie den unter Punkt D.1. zitierten Bestimmungen der WStV sowie der korrespondierenden Verordnung unzweideutig zu entnehmen ist – der Stadt Wien

zuzuordnen (vgl. insb. die Weisungshoheit des Bürgermeisters laut § 7 Abs. 1 der Verordnung des Gemeinderates), welche im gegenständlichen Verfahren durch den Magistrat der Stadt Wien vertreten ist (vgl. hierzu das Erkenntnis des BVwG vom 27. Mai 2020, GZ: W214 2228346-1).

Vor diesem Hintergrund kommt die Datenschutzbehörde zum Ergebnis, dass für die im Rahmen der verfahrensgegenständlichen Krankenanstalt („Klinik ****“) verarbeiteten Daten die Stadt Wien als datenschutzrechtlich Verantwortliche – und im Sinne der obigen Ausführungen – als Melde- und ggf. Benachrichtigungsverpflichtete (zu Letzterem siehe Punkt D.3.) zu qualifizieren war.

D.3. Zur Benachrichtigungspflicht gegenüber der betroffenen Person

Das Vorliegen einer Verletzung des Schutzes personenbezogener Daten durch den zweckwidrigen Zugriff auf Daten der betroffenen Person (Patientin) sowie die anschließende unbefugte Offenlegung durch die Mitarbeiterin der Verantwortlichen im Rahmen ihres Social-Media Profils (vgl. Punkt C.2.) steht außer Zweifel und wurde im Übrigen zu keinem Zeitpunkt von der Verantwortlichen, welche überdies eine ausdrücklich als solche bezeichnete Meldung gemäß Art. 33 Abs. 1 DSGVO erstattete, in Frage gestellt.

Eine Benachrichtigungspflicht der betroffenen Person nach Art. 34 Abs. 1 DSGVO besteht in jenen Fällen, in welchen voraussichtlich – somit im Sinne einer Prognoseentscheidung – ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen zu erwarten ist.

Wie die Verantwortliche im Rahmen ihrer Stellungnahme selbst ausführte, bedeutet der Begriff „Akutgeriatrie“, dass eine betreuungsintensive (medizinische) Pflege erforderlich ist und war überdies eine konkrete medizinische Behandlung („Setzen eines Venflons“) ersichtlich.

In diesem Zusammenhang ist daher anfänglich darauf hinzuweisen, dass es sich – entgegen dem Vorbringen im Rahmen der Folgeeingaben – bei den verfahrensgegenständlichen Informationen der betroffenen Person (Patientin) aus dem „elektronischen Dekurs“ sowohl nach dem – weit gefassten – Wortlaut des Art. 4 Z 15 DSGVO als auch nach der Spruchpraxis der Datenschutzbehörde (vgl. etwa den Bescheid der DSB vom 19. November 2020, GZ: 2020-0.743.659) unzweifelhaft um Gesundheitsdaten („Gesundheitsdienstleistungen“) handelt, welche nach dem Willen des Verordnungsgebers einer erhöhten Schutzwürdigkeit unterliegen sollen (vgl. Art. 9 Abs. 1 DSGVO).

Die Datenschutzbehörde hat bereits ausgesprochen, dass Sicherheitsverletzungen iZm Gesundheitsdaten in der Regel ein hohes Risiko darstellen (vgl. Bescheid der DSB vom 8. August 2018, GZ: DSB-D084.133/0002-DSB/2018).

Auch im Rahmen der bereits zitierten Guidelines 9/2022 des EDPB wird ausdrücklich darauf hingewiesen, dass gerade bei Gesundheitsdaten regelmäßig von einem hohen Risiko auszugehen sei und dieses nur in besonderen Ausnahmefällen ausgeschlossen werden könne (vgl. Guidelines 9/2022 des EDPB, Rn. 102 und 107 „nature, sensitivity, and volume of personal data“). Des Weiteren sei gerade bei medizinischen Daten zwischen einem „bloßen“ Verlust oder der – verfahrensgegenständlichen – Offenlegung gegenüber unberechtigten Dritten zu unterscheiden und sei bei Letzterer jedenfalls von einer erhöhten Schwere der Verletzung auszugehen (vgl. Guidelines 9/2022 des EDPB, Rn. 106 „type of breach“). Zu beachten sei ferner, ob die Daten – wie verfahrensgegenständlich betreffend die Mitarbeiterinnen und Mitarbeiter (vgl. Punkt C.3.) – verschlüsselt uÄ oder – wie verfahrensgegenständlich betreffend die Patientin – unverschlüsselt und aufgrund von Name und Adresse unmittelbar identifizierbar offengelegt worden seien (vgl. Guidelines 9/2022 des EDPB, Rn. 111-112 „Ease of identification of individuals“).

Die Datenschutzbehörde übersieht dabei nicht, dass die Offenlegung für einen begrenzten Zeitraum und gegenüber einem beschränkten Personenkreis erfolgte. Dabei ist jedoch festzuhalten, dass nach allgemeiner Lebenserfahrung bereits ein kurzer Zeitraum dazu führen kann, dass Informationen – insbesondere durch deren einfache Weiterverbreitung im Onlinekontext – einer Vielzahl und besonders der Verantwortlichen unbekannter Personen (vgl. Guidelines 9/2022 des EDPB, Rn. 114, wonach die Unmöglichkeit der Einschätzung der Intentionen bei nicht bekannten Personen ein erhöhtes Risiko darstelle) zur Kenntnis gebracht wird.

Abschließend ist noch darauf hinzuweisen, dass die Verantwortliche im Rahmen des vorliegenden Verfahrens keine (etwa geeigneten technischen oder organisatorischen) Maßnahmen im Sinne des Art. 34 Abs. 3 lit. a und b DSGVO anführte und alleine die anschließende Löschung des Social-Media Beitrags durch die Mitarbeiterin das potenzielle hohe Risiko nicht wesentlich vermindern mag. Ein unverhältnismäßiger Aufwand iZm der Benachrichtigung (lit. c leg. cit.) liegt ebenso wenig vor.

Als Ergebnis ist daher festzuhalten, dass die Benachrichtigung der betroffenen Person (Patientin) nicht nur pro futuro zur Vermeidung weiterer Verletzung ihrer persönlichen Rechte und Freiheiten geeignet, sondern – aufgrund des festgestellten Risikopotenzials – überdies obligatorisch ist und der Verantwortlichen infolgedessen die Nachholung der Benachrichtigung gemäß Art. 58 Abs. 2 lit. e DSGVO aufzutragen war.

In zeitlicher Hinsicht hat die Benachrichtigung betroffener Personen von der Verletzung grundsätzlich unverzüglich zu erfolgen (vgl. auch ErwGr. 86). Im konkreten Einzelfall erscheint die Benachrichtigung innerhalb einer Frist von zwei Wochen als angemessen. Betreffend die Art und Form wird der Vollständigkeit halber auf Art. 34 Abs. 2 DSGVO verwiesen.

Es war daher spruchgemäß zu entscheiden.

Schlagworte

Anweisung an Verantwortlichen, Benachrichtigung, Datenschutzverletzung, Data Breach, Gesundheitsdiensteanbieter, Verantwortlichenrolle, Gemeinde, Krankenhaus, Krankenanstalt, Klinik, Träger einer Krankenanstalt, Offenlegung von Daten, besondere Kategorien, Gesundheitsdaten, hohes Risiko, Soziale Medien

European Case Law Identifier (ECLI)

ECLI:AT:DSB:2023:2023.0.046.014

Zuletzt aktualisiert am

15.03.2023