BVwG
Bundesverwaltungsgericht
Republik Österreich

Sitz Wien
Erdbergstraße 192 – 196, 1030 Wien
Tel: +43 1 601 49 - 0
Fax: +43 1 711 23 - 889 15 41
www.bvwg.gv.at

Entscheidungsdatum

20.10.2025

Geschäftszahl

W108 2276075-1/12E

I M N A M E N D E R R E P U B L I K !

Das Bundesverwaltungsgericht hat durch die Richterin Mag. BRAUCHART als Vorsitzende sowie die fachkundige Laienrichterin Dr. FELLNER-RESCH und den fachkundigen Laienrichter Mag. KUNZ als Beisitzerin und Beisitzer über die Beschwerde der XXXX , vertreten durch Rechtsanwalt Dr. Markus ORGLER, gegen den Bescheid der Datenschutzbehörde vom 01.06.2023, Zl. D124.3118 2023-0.315.174, betreffend eine datenschutzrechtliche Angelegenheit (mitbeteiligte Partei: XXXX) zu Recht erkannt:

A)

Die Beschwerde wird gemäß § 28 Abs. 2 VwGVG als unbegründet abgewiesen.

B)

Die Revision ist gemäß Art. 133 Abs. 4 B-VG nicht zulässig.

Entscheidungsgründe:

I. Verfahrensgang und Sachverhalt:

1. In der verfahrensgegenständlichen an die Datenschutzbehörde (belangte Behörde vor dem Bundesverwaltungsgericht) gerichteten Datenschutzbeschwerde gemäß Art. 77 DSGVO sowie § 24 Datenschutzgesetz (DSG) vom 15.10.2020 (datiert mit 16.09.2020 und 12.10.2020) machte die mitbeteiligte Partei bzw. der Mitbeteiligte (ehemaliger Beschwerdeführer im Verfahren vor der belangten Behörde) eine Verletzung im Recht auf Geheimhaltung gemäß § 1 Datenschutzgesetz (DSG) sowie Art. 9 Datenschutz-Grundverordnung (DSGVO) durch die nunmehrige Beschwerdeführerin, die Rechtsträgerin und Betreiberin einer Krankenanstalt (ehemalige Beschwerdegegnerin im Verfahren vor der belangten Behörde), geltend.

Dazu brachte die mitbeteiligte Partei inhaltlich vor, sie sei am 09.06.2019 in der Notaufnahme der von der Beschwerdeführerin betriebenen Klinik behandelt worden, wovon nur diese Klinik und der Hausarzt informiert worden seien. Vor dem Bezirks- bzw. Landesgericht XXXX habe sie am 01.06.2020 erfahren, dass ihre Gesundheitsdaten (so ein Notfall-Bericht der von der Beschwerdeführerin betriebenen Klinik) ohne ihr Einverständnis an Dritte weitergegeben worden seien. Dies stelle einen unzulässigen Eingriff in sein Recht auf Geheimhaltung gemäß § 1 DSG aufgrund einer unrechtmäßigen bzw. ohne hinreichende Rechtfertigungsgründe erfolgten Datenverarbeitung nach Art. 5, 6 und 9 DSGVO dar. Sie sei jener Patient, welcher die „ XXXX Datenaffäre“ ausgelöst habe. Am 16.09.2020 habe sie vom Datenschutzbeauftragten der Beschwerdeführerin das Zugriffsprotokoll für ihre Krankenakte erhalten, danach habe sie eine schriftliche Sachverhaltsdarstellung an die Beschwerdeführerin gerichtet. In der Folge habe die Beschwerdeführerin am 06.10.2020 ihr telefonisch mitgeteilt, dass sich der Verdacht einer Datenschutzverletzung erhärtet habe, und im Rahmen einer Pressekonferenz auch die Medien informiert.

Der Datenschutzbeschwerde waren ein einseitiger medizinischer Notfall-Bericht vom 09.06.2019, die erste Seite eines Protokolls des genannten Landesgerichtes vom 04.06.2020 sowie ein einseitiges Zugriffsprotokoll betreffend die Patientendaten der mitbeteiligten Partei vom 29.09.2020 angeschlossen.

2. Über Aufforderung der belangten Behörde erstattete die Beschwerdeführerin mit Schriftsatz vom 14.01.2021 eine Stellungnahme zur Datenschutzbeschwerde der mitbeteiligten Partei und führte aus, dass ihre Datenschutzbeauftragten dem Anliegen der mitbeteiligten Partei - wie von dieser im Rahmen der Datenschutzbeschwerde beschrieben - nachgekommen seien und dieser eine Zugriffsprotokollierung auf ihre Krankengeschichte bei

einem persönlichen Besprechungstermin ausgehändigt worden sei. In diesem Zusammenhang habe die mitbeteiligte Partei auch die vermutete Weitergabe ihrer personenbezogenen Daten an den gegnerischen rechtsfreundlichen Vertreter in einem Gerichtsverfahren erwähnt. Die Datenschutzbeauftragten der Beschwerdeführerin hätten sich umgehend um die Aufklärung des Sachverhaltes bemüht und eine Data-Breach-Meldung erstattet. Die mitbeteiligte Partei sei mehrfach von den Datenschutzbeauftragen der Beschwerdeführerin über den aktuellen Stand informiert worden und ihr sei zugesichert worden, dass ihr Name im Zusammenhang mit der unrechtmäßigen Datenweitergabe an die Polizei nicht erwähnt werde, da dies von ihr nicht gewünscht gewesen sei. Es habe jedoch nicht festgestellt werden können, von wem tatsächlich der Arztbrief nach außen weitergegeben worden sei, vielleicht würden die staatsanwaltlichen Ermittlungen diesbezüglich noch ein Ergebnis hervorbringen. Intern seien die zwei betroffenen Mitarbeiter, welche für die Datenweitergabe verantwortlich gewesen seien, entlassen worden.

3. Die mitbeteiligte Partei gab zu diesem Schriftsatz ihm Rahmen des ihr hierzu gewährten Parteiengehörs keine Stellungnahme ab.

4. Die belangte Behörde richtete mit Verfahrensanordnung vom 21.05.2021 ein Amtshilfeersuchen an die Landespolizeidirektion XXXX , in der um Auskunft über den Stand der bezughabenden kriminalpolizeilichen Ermittlungen und um Übermittlung aller relevanten Unterlagen ersucht wurde.

Mit Schreiben vom 10.06.2021 teilte die genannte Landespolizeidirektion (konkret das Landeskriminalamt) der belangten Behörde mit, dass der Sachverhalt „Datenschutzskandal XXXX “ vom Bundesamt für Korruptionsbekämpfung und der Staatsanwaltschaft XXXX bearbeitet werde, und verwies diese mit ihrem Amtshilfeersuchen an die beiden genannten Stellen.

5. Über ergänzende Aufforderung der belangten Behörde erstattete die Beschwerdeführerin am 09.06.2021 eine weitere Stellungnahme zu vorformulierten Sachverhaltsfragen der belangten Behörde und teilte mit, dass die beiden Mitarbeiter, von denen sich die Beschwerdeführerin getrennt habe, für die Leitung des Patientenbeschwerdemanagements bzw. des Securitymanagements verantwortlich gewesen seien, wobei deren Zugriffsberechtigung auf die Informationssysteme des Krankenhauses entsprechend den betrieblichen Notwendigkeiten eingerichtet gewesen sei. Jeder Zugriff auf die Krankengeschichte werde über das Krankenhausinformationssystem mitprotokolliert und auf unrechtmäßige Zugriffe (Querzugriffe) überprüft. Ein unrechtmäßiger Zugriff auf eine

Krankengeschichte könne dienstrechtliche bzw. strafrechtliche Konsequenzen nach sich ziehen, worüber die Mitarbeiterinnen und Mitarbeiter auch informiert seien. Einen Zugang zum Klinischen Informationssystem habe nur die Leitung des Patientenbeschwerdemanagements, da für diese Funktionswahrnehmung die Sichtung der Krankengeschichte notwendig sei. Das Patientenbeschwerdemanagement sei der ärztlichen Direktion XXXX zugeordnet. Die Leitung sei bei einer langjährigen Mitarbeiterin bzw. einem langjährigen Mitarbeiter gelegen, wobei es bis zu diesem Vorfall dort nie in irgendeiner Weise datenschutzrechtliche Auffälligkeiten gegeben habe. Der Leiter des Securitymanagements habe keinen Zugriff zum Krankenhausinformationssystem; dies sei explizit abgelehnt worden. Er habe die Patienteninformationen über die Leitung des Patientenbeschwerdemanagements erhalten. Der Leitung des Patientenbeschwerdemanagements obliege die Bearbeitung sämtlicher Patientenbeschwerden am genannten XXXX sowie die Bearbeitung von externen Anfragen zu Krankengeschichten. Dem Securitymanager obliege das Sicherstellen des täglichen Geschäftsablaufs der Beschwerdeführerin auf operationeller Securityebene, das Erheben und Bewerten der Security IST-Situation, die Planung und die Durchführung geeigneter Maßnahmen zur Erreichung der definierten Schutzziele, die Entwicklung eines Service- und Sicherheitskonzeptes und deren effektive Umsetzung, das Mitwirken bei Baumaßnahmen mit Blickrichtung Objekt- Eigentumsschutz, die Weisungsbefugnis gegenüber dem externen Wach- und Sicherheitspersonal, die präventive und repressive Abwehr von Straftaten, gegebenenfalls die Abstimmung mit den Sicherheitsbehörden, die Übernahme von Aufgaben im Risiko-, Krisen-, Ereignis- und Notfallmanagement, die Durchführung von internen Service- und Sicherheitsaudits sowie Schulungen, die Erhebung und statistische Auswertung der Vorfälle und Einsätze, inklusive Erstellung des Sicherheitslageberichts, die Vertretung des Unternehmens in Securityfragen nach außen (Behörden, Firmen, Sicherheitsnetzwerke), die Beratung von Mitarbeitern zu Fragen der Reisesicherheit, die Beratung der Geschäftsführung in allen Securityfragen und die regelmäßige Berichterstattung. Die Zugriffe auf die Krankengeschichte würden regelmäßig von den Datenschutzbeauftragten überprüft. Sollte der Zugriff nicht plausibilisierbar sein, werde eine interne Kommission einberufen und dort über die dienstrechtlichen Konsequenzen entschieden. In diesem speziellen Fachbereich seien bis dato keine datenschutzrechtlichen Vorfälle bekannt gewesen. Datenarten und Kategorien der Verarbeitungstätigkeit seien im Verfahrensverzeichnis der Beschwerdeführerin auf deren Website öffentlich einsehbar. Die Zugriffsrechte auf das Krankenhausinformationssystem würden in einem Berechtigungskonzept dargestellt. Dieses werde regelmäßig durch die interne Datenschutzkommission der Beschwerdeführerin angepasst und freigegeben, wobei sich das Berechtigungskonzept an den

datenschutzrechtlichen Grundsätzen gemäß Art. 5 DSGVO, insbesondere dem Grundsatz der Datenminimierung, orientiere.

6. Mit Amtshilfeersuchen vom 15.06.2021 begehrte die belangte Behörde vom Bundesamt für Korruptionsbekämpfung eine Auskunft über den Stand der kriminalpolizeilichen Ermittlungen zum „Datenschutzskandal XXXX “ und die Übermittlung bezughabender Unterlagen.

Mit Note vom 07.07.2021 lehnte das Bundesamt das Amtshilfeersuchen der belangten Behörde hinsichtlich einer Auskunftserteilung zu einem laufenden Ermittlungsverfahren der Staatsanwaltschaft XXXX ab und verwies diese an die genannte Staatsanwaltschaft.

Mit Amtshilfeersuchen vom 28.07.2021 begehrte die belangte Behörde von der Staatsanwaltschaft XXXX die Übermittlung einer Kopie der Akten des genannten Ermittlungsverfahrens.

Mit Note vom 25.08.2021 lehnte die Staatsanwaltschaft XXXX das Amtshilfeersuchen der belangten Behörde ab, da den Parteien des Datenschutzverfahrens im genannten Ermittlungsverfahren keine Parteistellung zukomme.

Die Verfahrensparteien äußerten sich hierzu ihm Rahmen des ihnen gewährten Parteiengehörs nicht.

7. Über erneute Aufforderung der belangten Behörde unter ausdrücklichem Hinweis auf die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO erstattete die Beschwerdeführerin mit Schriftsatz vom 13.01.2022 eine weitere Stellungnahme zum Data-Breach in der von ihr betrieben Klinik und führte im Wesentlichen aus: Der Securitymanager habe am 04.10.2019 um 11:28 Uhr eine E-Mail als Antwort auf eine Anfrage eines Beamten der Landespolizeidirektion XXXX an letzteren gesendet. Diese sei ohne Anhang (kein Notfall-Bericht im E-Mail enthalten) gesendet worden. Inhaltlich habe der Securitymanager mitgeteilt, dass die mitbeteiligte Partei am 09.06.2019 und am 17.09.2019, jeweils wegen Substanzmissbrauchs, zur ambulanten Notfallbehandlung im XXXX gewesen sei. Er habe dabei jeweils angegeben, dass die Symptome beim bisherigen Konsum von Kokain nicht aufgetreten seien. Weiters habe die mitbeteiligte Partei gesagt, dass die Quelle des aktuell konsumierten Kokains unbekannt sei. Der Securitymanager habe den Polizeibeamten ersucht, für weitere medizinische Informationen „bitte den üblichen Weg (Anfrage per Fax mit Formular)“ zu wählen. Eine andere E-Mail des Securitymanagers mit Anhang des Notfall-Berichtes sei nicht gefunden worden. Es könne aber nicht ausgeschlossen werden, dass der Securitymanager den Notfall-Bericht über einen anderen Weg (anderer E- Mail-Account, Post) an Dritte übermittelt

habe. Erhalten habe der Securitymanager den Notfall-Bericht durch die Leiterin des Beschwerdemanagements im PDF-Format als Teil einer sogenannten Sammelmappe. Deren Abfrage samt Übermittlung sei im Dokumentationsmanagementsystem der Beschwerdeführerin auch protokolliert worden. Die Sammelmappe enthalte den Notfall-Bericht, Arztbericht, Laborbefund, Entlassungsrevers, Konsiliarbefund mit Untersuchung/Therapievorschlag/Übernahme in die Psychiatrie, es handle sich um sehr sensible Gesundheitsdaten der mitbeteiligten Partei, zu welchen diese gegenüber der Beschwerdeführerin immer auf die Verschwiegenheitsverpflichtung hingewiesen habe.

In die Stellungnahme eingefügt waren Wiedergaben des E-Mailverkehrs zwischen dem Beamten der Landespolizeidirektion und dem Leiter des Securitymanagements der Beschwerdeführerin sowie ein Auszug aus den Protokollierungen des Dokumentationsmanagementsystems betreffend die mitbeteiligte Partei vom 03.10.2019, wobei sich aus letzterem ergibt, dass der Leiter des Securitymanagements die Sammelmappe der mitbeteiligten Partei aufgrund einer E-Mailanfrage an die Leitung des Patientenmanagements erhalten hat.

8. Zur Stellungnahme der Beschwerdeführerin äußerte sich die mitbeteiligte Partei nicht.

9. Mit dem nunmehr angefochtenen Bescheid der belangten Behörde wurde der Datenschutzbeschwerde der mitbeteiligten Partei stattgegeben und festgestellt, dass die Beschwerdeführerin die mitbeteiligte Partei in ihrem Recht auf Geheimhaltung personenbezogener Daten verletzt habe, indem

a) am 04.10.2019 der Sicherheitsbeauftrage („Securitymanager“) der Beschwerdeführerin, XXXX , um 11:28:17 Uhr eine E-Mail mit folgendem Inhalt an Abteilungsinspektor XXXX , Beamter der Landespolizeidirektion für XXXX , Stadtpolizeikommando XXXX , Kriminalreferat, gesendet habe, nachdem er sich zuvor eine Kopie der elektronisch gespeicherten Krankengeschichte der mitbeteiligten Partei (Patienten-ID: XXXX) verschafft hatte:

„Guten Morgen,
ug Person war am 09.06.2019 und am 17.09.2019, jeweils wegen Substanzmißbrauch (Kokain; 4-10 Gramm) zur ambulanten Notfallbehandlung im XXXX .
[Der Mitbeteiligte] gab jeweils an, dass die Symptome beim bisherigen Konsum von Kokain nicht aufgetreten sind. Weiters sagte er, dass die Quelle des aktuell konsumierten Kokain unbekannt sei.
Für weitere medizinische Informationen bitte den üblichen Weg (Anfrage per Fax mit Formular) wählen. Für allfällige Fragen stehe ich gerne zur Verfügung.
BG XXXX “;

b) der Sicherheitsbeauftrage („Securitymanager“) der Beschwerdeführerin, XXXX , zu einem nicht näher bekannten Zeitpunkt zwischen dem 04.10.2019 und dem 04.06.2020 den Gesundheitsdaten des Mitbeteiligten enthaltenden Notfall-Bericht vom 09.06.2019 an die Landespolizeidirektion übersendete.

Die belangte Behörde hielt zunächst fest, dass Beschwerdegegenstand die Frage sei, ob die Beschwerdeführerin die mitbeteiligte Partei in ihrem Recht auf Geheimhaltung verletzt habe, indem sie als datenschutzrechtlich Verantwortliche von ihr verarbeitete Daten (Auszüge aus einer Krankengeschichte sowie den Notfall-Bericht vom 09.06.2019 und somit besonders geschützt Daten gemäß Art. 9 DSGVO) an unbefugte Dritte übermittelt habe.

Die belangte Behörde traf folgende Sachverhaltsfeststellungen (auszugsweise; Formatierung nicht originalgetreu wiedergegeben):

„Die [Beschwerdeführerin] ist eine aufgrund gesetzlicher Anordnung … gegründete Gesellschaft mit beschränkter Haftung im wirtschaftlichen Alleineigentum des Landes XXXX , der die Rechtsträgerschaft des XXXX zukommt … .

Am 3. Oktober 2019 um 16:10 Uhr richtetet Abteilungsinspektor XXXX , ein Beamter der Landespolizeidirektion für XXXX , Stadtpolizeikommando XXXX , Kriminalreferat, von der E-Mail-Adresse < XXXX > per E-Mail an XXXX , den Sicherheitsbeauftragten („Securitymanager“) der [Beschwerdeführerin], eine Anfrage mit folgendem Inhalt:

„Hallo XXXX

Die Person heißt XXXX , möglich auch XXXX , geb XXXX und soll eigenen Angaben zu Folge vor ca. 2 Monaten wegen Verdacht auf Kokainüberdosis in die Klinik XXXX eingeliefert worden sein. Vielleicht kannst du mir das unverbindlich überprüfen
Aber nur falls du keine Schwierigkeiten bekommst, ich weiß ja, dass der Weg jetzt anders laufen sollte Vielen Dank im Voraus
XXXX “

XXXX wandte sich daraufhin an XXXX , die Leiterin des Beschwerdemanagements bei der [Beschwerdeführerin], die über die notwendigen Nutzerrechte verfügte, um Patientendaten im Krankenhausinformationssystem/Dokumentationsmanagementsystem der [Beschwerdeführerin] für XXXX , abfragen zu können. Er erhielt von Letzterer noch am 3. Oktober 2019 [den Mitbeteiligten] betreffende Daten in Form einer elektronischen Sammelmappe (Patienten-ID: XXXX) mit Dokumenten im Format PDF, enthaltend den [den Mitbeteiligten] betreffenden Notfallbericht, Arzt-Bericht, Laborbefund, Entlassungsrevers und Konsiliarbefund mit Untersuchung/Therapievorschlag/Übernahme in die Psychiatrie.

Am 4. Oktober 2019 sendete XXXX um 11:28:17 Uhr eine E-Mail mit folgendem Inhalt an XXXX :

„Guten Morgen,

ug Person war am 09.06.2019 und am 17.09.2019, jeweils wegen Substanzmißbrauch (Kokain; 4-10 Gramm) zur ambulanten Notfallbehandlung im XXXX .
XXXX gab jeweils an, dass die Symptome beim bisherigen Konsum von Kokain nicht aufgetreten sind. Weiters sagte er, dass die Quelle des aktuell konsumierten Kokain unbekannt sei.
Für weitere medizinische Informationen bitte den üblichen Weg (Anfrage per Fax mit Formular) wählen. Für allfällige Fragen stehe ich gerne zur Verfügung.
BG XXXX “

Zu einem nicht genau bekannten Zeitpunkt danach übersendete XXXX über einen anderen E-Mail Account oder per Post [den Notfall-Bericht vom 09.06.2019] aus der erwähnten „Sammelmappe“ an die LPD.

In ihrer Beweiswürdigung führte die belangte Behörde aus: Die Feststellungen stützten sich in der Hauptsache auf die Angaben der Beschwerdeführerin in der ausführlichen Stellungnahme und Sachverhaltsdarstellung vom 13.01.2022. Diese Stellungnahme enthalte Faksimiles der zitierten E-Mails sowie Auszüge aus dem Dokumentationsmanagementsystem der Beschwerdeführerin, die die Datenabfragen, deren Hintergrund und die dafür verantwortlichen Personen nachvollziehbar darlegten. Die Kopie des den Mitbeteiligten betreffenden Notfall-Berichts vom 09.06.2019 stamme vom Mitbeteiligten in seiner Datenschutzbeschwerde. Das Dokument stamme, wie aus dem gerichtsüblichen Vermerk der Ordnungsnummer und Aktenseite erkennbar, aus dem Akt XXXX des Landesgerichtes XXXX , in welcher Sache es von der beklagten Partei (Kläger: die mitbeteiligte Partei) als Beweismittel vorgelegt worden sei. Die Feststellung, dass dieses Dokument (ohne entsprechend dokumentierte Anforderung) an die Landespolizeidirektion übermittelt worden sei, beruhe auf einer plausiblen, von der Beschwerdeführerin selbst ausgesprochenen Vermutung (in ihrer Stellungnahme vom 13.01.2022). Erhärtet werde diese durch die aus den E-Mails klar hervorgehende professionelle Bekanntschaft zwischen dem Leiter des Securitymanagements der Beschwerdeführerin XXXX (in der Folge: Sicherheitsmanager) und XXXX (in der Folge: Beamter bzw. Polizeibeamter), einschließlich der erkennbaren Bereitschaft, auch unter Umgehung interner Vorschriften Informationen und Daten auszutauschen (Zitat: „ich weiß ja, dass der Weg jetzt anders laufen sollte“). Eine solche Übermittlung der Daten aus dem Wirkungsbereich der Beschwerdeführerin heraus sei daher plausibler als die von der mitbeteiligten Partei ausgesprochene Vermutung, das Dokument könnte direkt an Rechtsanwalt XXXX , den Vertreter der beklagten Partei in der Sache XXXX , übermittelt worden sein.

Rechtlich hielt die belangte Behörde im Wesentlichen fest, die gemäß § 15 und § 63a Tir KAG durch die Beschwerdeführerin verarbeiteten Gesundheitsdaten von Patienten fielen nicht unter die im dritten Hauptstück des DSG geregelten Verarbeitungszwecke, sodass die DSGVO anwendbar sei. Die datenschutzrechtliche Verantwortlichkeit der Beschwerdeführerin sei zu bejahen, da sich diese das Handeln des Sicherheitsmanagers in vollem Umfang zurechnen lassen müsse. Die in Beschwerde gezogenen Datenübermittlungen an die Landespolizeidirektion sei jedenfalls in der Form und unter den Umständen, die hier vorgelegen seien, nicht rechtmäßig gewesen, da zwingende Bedingungen der Rechtmäßigkeit der Übermittlung von Gesundheitsdaten gemäß Art. 5 Abs. 1, Art. 9 Abs. 2 DSGVO und § 15 Abs. 1 Tir KAG nicht eingehalten worden seien und damit ohne ausreichende Rechtsgrundlage in das Geheimhaltungsrecht der mitbeteiligten Partei eingegriffen worden sei.

10. Gegen diesen Bescheid erhob die Beschwerdeführerin fristgerecht Parteibeschwerde gemäß Art. 130 Abs. 1 Z 1 B-VG an das Bundesverwaltungsgericht, in welcher sie ihr Vorbringen aus dem behördlichen Verfahren wiederholte und zusammengefasst ausführte, dass der Sicherheitsmanager bereits aufgrund seiner Funktion und Ausbildung bestinformiert gewesen sei. Für die offizielle Kommunikation mit der Polizei sei ein explizit definierter und separater Zugang eingerichtet gewesen, welcher bewusst umgangen worden sei. Auch die Polizeibediensteten hätten inoffiziell und somit außerhalb des Anwendungsbereiches des 3. Hauptstückes des DSG die entsprechenden Informationen angefragt. Die Beschwerdeführerin habe bei Bekanntwerden des Vorfalls umgehend mit der Erhebung aller Informationen begonnen und in der Folge den Sicherheitsmanager fristlos entlassen. Die Beschwerdeführerin könne zudem die Einstellung der strafrechtlichen Ermittlungsverfahren gegen die ehemaligen Mitarbeiter nicht nachvollziehen (und äußerte Mutmaßungen zu den Beweggründen der Staatsanwaltschaft). Zudem habe das Arbeits- und Sozialgericht die zivilrechtliche Klage des Sicherheitsmanagers auf Feststellung des aufrechten Dienstverhältnisses in erster Instanz abgewiesen. Eine datenschutzrechtliche Zurechnung des Sicherheitsmanagers zur Beschwerdeführerin - alleine aufgrund des kategorischen Abstellens auf die Motivlage - sei rechtlich nicht argumentierbar und müsse durch ein Eigeninteresse anderer Art gesprengt werden. Ob ein solches Eigeninteresse in einem Zusammenhang zur Tätigkeit des Datenverantwortlichen stehe, könne nur insofern Beachtung erfahren, als keine entsprechenden Vorkehrungen zur Verhinderung des Missbrauches getroffen worden seien. Die Optimierung der eigenen Dienstabläufe oder eine fehlgeleitete Auslegung der Interessenslagen der Beschwerdeführerin durch den Sicherheitsmanager würden nicht zu einem der Beschwerdeführerin objektiv unterstellbaren Interesse führen. Dieser habe nach seinen eigenen Vorstellungen und in einer nicht vorhersehbaren Dimension optimierte

Kommunikationsabläufe mit den Polizeidienststellen etabliert, Daten an diese herausgeben - ohne dazu angeleitet worden zu sein -, wobei hinsichtlich dieser Vorgänge niemand Kenntnis gehabt und hinsichtlich welcher die Beschwerdeführerin erstmals im Rahmen der durch die mitbeteiligte Partei erhobenen Beschwerde Kenntnis erlangt habe. Der Sicherheitsmanager sei eine erfahrene Sicherheitskraft gewesen und stets - soweit für die Beschwerdeführerin erkennbar - seinen Agenden hervorragend nachgekommen. Das rechtswidrige Handeln der Polizeidienststellen - durch konkrete Anfragen an den Sicherheitsmanager - habe die Beschwerdeführerin nicht erwarten können, der Zweck dieser Vorgänge sei der Beschwerdeführerin weder bekannt gewesen noch sei dies toleriert worden. In der Folge sei es der Beschwerdeführerin nicht möglich gewesen, den Datenschutzvorfall - z.B. durch Belehrungen - zu verhindern. Das Verhalten des Sicherheitsmanagers könne der Beschwerdeführerin nicht zugerechnet werden. Im Ergebnis habe dieser exzessiv gehandelt, was einer privat motivierten Datenschutzverletzung gleichzuhalten sei. Es werde daher beantragt, eine mündliche Verhandlung anzuberaumen, den angefochtenen Bescheid dahingehen abzuändern, dass der gegen die Beschwerdeführerin erhobenen Beschwerde der mitbeteiligten Partei keine Folge gegeben werde, in eventu, den angefochten Bescheid im Anfechtungsumfang aufzuheben und das Verfahren an die Verwaltungsbehörde zurückzuverweisen.

Aus dem der Beschwerde beigefügten erstinstanzlichen Urteil des Arbeits- und Sozialgerichtes XXXX , vom 21.06.2022 ergibt sich, dass der Aufgabenbereich des Sicherheitsmanagers u.a. die Sicherstellung der Kommunikation mit der Polizei umfasste, wobei dieser gemäß der interne Richtlinie Nr. 4464 im Fall einer mündlichen Anfrage der Polizei unter Nennung des Familien-, Vornamen sowie des Geburtsdatums der gesuchten Person Auskunft erteilen durfte, jedoch die Anforderung medizinischer Unterlagen ausschließlich per Mail XXXX zu erfolgen hatte.

11. Die belangte Behörde machte von der Möglichkeit der Beschwerdevorentscheidung nicht Gebrauch und legte die Beschwerde samt den bezughabenden Akten des Verwaltungsverfahrens dem Bundesverwaltungsgericht zur Entscheidung vor, wobei sie den angefochtenen Bescheid verteidigte und insbesondere festhielt, dass die Voraussetzungen für den Entfall einer mündlichen Verhandlung vorlägen und im Beschwerdefall keine Durchbrechung der datenschutzrechtlichen Verantwortlicheneigenschaft der Beschwerdeführerin zu erkennen sei.

12. Die Beschwerdeführerin trat den Ausführungen der belangten Behörde in ihrer Stellungnahme vom 05.09.2023 im Wesentlichen mit der Wiederholung ihres bisherigen Standpunktes zur eigenständigen Verantwortlicheneigenschaft des Sicherheitsmanagers

entgegen und führte ergänzend aus, dass Art. 29 DSGVO im vorliegenden Fall einschlägig sei und der EuGH in der Rechtssache C-40/17 ausgesprochen habe, dass die Entscheidung über die Zwecke und Mittel sich unmittelbar auf den betreffenden Vorgang oder die betreffenden Vorgänge der Datenverarbeitung beziehen müsse. Die erfolgte Datenweitergabe sei durch die betriebsinterne Richtlinie und das 3. Hauptstück des DSG geregelt. Abschließend regte die Beschwerdeführerin die Einleitung eines Vorabentscheidungsverfahrens beim EuGH durch das Bundesverwaltungsgericht, hinsichtlich der Rechtsfrage der Verantwortlicheneigenschaft, an.

13. Nach Gewährung von Parteiengehör wartete das Bundesverwaltungsgericht mit der Entscheidung im vorliegenden Beschwerdeverfahren bis zur Entscheidung des Verwaltungsgerichtshofes über die bei ihm anhängige Revision gegen das Erkenntnis des Bundesverwaltungsgerichtes vom 20.01.2022, W214 2239688-1/35E, in welchem sich im Wesentlichen dieselben Rechtsfragen stellten, zu.

14. Nach Ergehen der Entscheidung des Verwaltungsgerichtshofes, die Anlass für das Zuwarten gegeben hatte, mit Beschluss vom 29.07.2025, Ro 2022/04/0017, setzte das Bundesverwaltungsgericht das Verfahren fort und gab den Verfahrensparteien Gelegenheit, eine ergänzende Stellungnahme einzubringen.

15. Mit Stellungnahme vom 01.10.2025 verwies die Beschwerdeführerin auf ihre Ausführungen im Schriftsatz vom 05.09.2023 und führte ergänzend und zusammengefasst aus, dass der dem genannten Beschluss des Verwaltungsgerichtshofes zugrundeliegende Sachverhalt mit dem beschwerdegegenständlichen Fall nicht ident sei. Der Sicherheitsmanager habe vorsätzlich gehandelt und es bestehe gerade kein dienstlicher Kontext mehr. Es sei strengstens verboten, ohne entsprechende gesetzliche Legitimation personenbezogene sensible Daten weiterzugeben und die Beschwerdeführerin habe über keine objektiven Anhaltspunkte verfügt, dass derartige Datenschutzverstöße durch einen ihrer Bediensteten begangen werden könne. Der durch die belangte Behörde festgestellte E-Mailverkehr belege zudem die Bereitschaft zur vorsätzlichen Umgehung interner Vorschiften. Insoweit unterscheide sich der zu privaten Zwecken erfolgte Missbrauch in keiner Weise von vorsätzlichem Exzedieren eines verbrecherisch handelnden Bediensteten, welcher jedenfalls den Tatbestand der Beihilfe zum Missbrauch der Amtsgewalt erfülle. Die datenschutzrechtliche Zurechnung des Sicherheitsmanagers zur Beschwerdeführerin müsse folglich verneint werden, dies insbesondere deshalb, da dem Verhalten des Bediensteten auch die interne Anweisung „Richtlinien zur Auskunftserteilung gegenüber der Polizei“ entgegengestanden habe. Abschließend wies die Beschwerdeführerin auf europarechtliche Bedenken sowie auf Bedenken bezüglich der Unzulässigkeitserklärung der ordentlichen

Revision hin und beantragte, den Ermittlungsakt XXXX der Staatsanwaltschaft XXXX einzuholen.

II. Das Bundesverwaltungsgericht hat erwogen:

1. Feststellungen:

Es wird von den Ausführungen oben unter Punkt I. zum Verfahrensgang (Verwaltungsgeschehen) und Sachverhalt, insbesondere von den Feststellungen der belangten Behörde im angefochtenen Bescheid, ausgegangen.

2. Beweiswürdigung:

Die Feststellungen ergeben sich aus den vorgelegten Verwaltungsakten sowie dem gegenständlichen Gerichtsakt, insbesondere aus dem angefochtenen Bescheid. Die für die Entscheidung wesentlichen Umstände im Tatsachenbereich sind geklärt und die relevanten Ermittlungsergebnisse und Urkunden liegen in den vorgelegten Verwaltungsakten ein. Die belangte Behörde hat ein mängelfreies, ordnungsgemäßes Ermittlungsverfahren durchgeführt und in der Begründung des angefochtenen Bescheides den maßgeblichen Sachverhalt in Übereinstimmung mit der Aktenlage mit einer schlüssigen Beweiswürdigung richtig festgestellt. Diesem Sachverhalt und der Beweiswürdigung trat die Beschwerdeführerin in ihrer Parteibeschwerde nicht bzw. mit bloß unsubstantiiertem Vorbringen entgegen. Damit steht der entscheidungswesentliche Sachverhalt aber fest. Einer weiteren Klärung des Sachverhaltes unter Aufnahme weiterer Beweise und Durchführung einer mündlichen Verhandlung bedarf es daher nicht. Damit konnte auf die beantragte Beischaffung des von der Beschwerdeführerin begehrten staatsanwaltschaftlichen Ermittlungsaktes verzichtet werden.

3. Rechtliche Beurteilung:

Zu A)

3.1. Gemäß Art. 130 Abs. 1 Z 1 B-VG erkennen die Verwaltungsgerichte über Beschwerden gegen den Bescheid einer Verwaltungsbehörde wegen Rechtswidrigkeit.

Gemäß § 6 BVwGG entscheidet das Bundesverwaltungsgericht durch Einzelrichter, sofern nicht in Bundes- oder Landesgesetzen die Entscheidung durch Senate vorgesehen ist. Gemäß § 27 Datenschutzgesetz (DSG) idgF entscheidet das Bundesverwaltungsgericht in Verfahren über Beschwerden gegen Bescheide, wegen Verletzung der Unterrichtungspflicht gemäß § 24 Abs. 7 und der Entscheidungspflicht der Datenschutzbehörde durch Senat. Der Senat besteht aus einem Vorsitzenden und je einem fachkundigen Laienrichter aus dem Kreis der Arbeitgeber und aus dem Kreis der Arbeitnehmer.

Das Verfahren der Verwaltungsgerichte mit Ausnahme des Bundesfinanzgerichtes ist durch das VwGVG, BGBl. I 2013/33 idF BGBl. I 2013/122, geregelt (§ 1 leg.cit.). Gemäß § 58 Abs. 2 VwGVG bleiben entgegenstehende Bestimmungen, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bereits kundgemacht wurden, in Kraft.

Gemäß § 17 VwGVG sind, soweit in diesem Bundesgesetz nicht anderes bestimmt ist, auf das Verfahren über Beschwerden gemäß Art. 130 Abs. 1 B-VG die Bestimmungen des AVG mit Ausnahme der §§ 1 bis 5 sowie des IV. Teiles, die Bestimmungen der Bundesabgabenordnung – BAO, BGBl. Nr. 194/1961, des Agrarverfahrensgesetzes – AgrVG, BGBl. Nr. 173/1950, und des Dienstrechtsverfahrensgesetzes 1984 – DVG, BGBl. Nr. 29/1984, und im Übrigen jene verfahrensrechtlichen Bestimmungen in Bundes- oder Landesgesetzen sinngemäß anzuwenden, die die Behörde in dem dem Verfahren vor dem Verwaltungsgericht vorangegangenen Verfahren angewendet hat oder anzuwenden gehabt hätte.

Gemäß § 28 Abs. 1 VwGVG hat das Verwaltungsgericht die Rechtssache durch Erkenntnis zu erledigen, sofern die Beschwerde nicht zurückzuweisen oder das Verfahren einzustellen ist.

Gemäß § 28 Abs. 2 VwGVG hat das Verwaltungsgericht über Beschwerden gemäß Art. 130 Abs. 1 Z 1 B-VG dann in der Sache selbst zu entscheiden, wenn (1.) der maßgebliche Sachverhalt feststeht oder (2.) die Feststellung des maßgeblichen Sachverhalts durch das Verwaltungsgericht selbst im Interesse der Raschheit gelegen oder mit einer erheblichen Kostenersparnis verbunden ist.

3.2. Zu den Prozessvoraussetzungen:

Die Beschwerde wurde fristwahrend erhoben und es liegen auch die sonstigen Prozessvoraussetzungen vor.

3.3. In der Sache:

3.3.1. Rechtsgrundlagen:

3.3.1.1. Art. 4 DSGVO lautet auszugsweise:

„Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu

Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

15. „Gesundheitsdaten“ 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;“

3.3.1.2. Art. 5 DSGVO lautet:

„Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;

personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“

3.3.1.3. Art. 9 DSGVO lautet auszugsweise:

„(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,“

3.3.1.4. § 1 DSG lautet auszugsweise:

„(1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die

aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden."

3.3.1.5. § 36 Abs. 1 DSG lautet:

„Die Bestimmungen dieses Hauptstücks gelten für die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung."

3.3.1.6. § 39 DSG lautet auszugsweise:

„Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person für die in § 36 Abs. 1 genannten Zwecke ist nur zulässig, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und

1. die Verarbeitung gemäß § 38 zulässig ist oder

2. sie sich auf Daten bezieht, die die betroffene Person offensichtlich selbst öffentlich gemacht hat."

3.3.1.7. § 15 Tiroler Krankenanstaltengesetz, Tir KAG, lautet auszugsweise:

„Führung von Krankengeschichten und sonstigen Vormerkungen

(1) Die Träger der Krankenanstalten haben

b) Krankengeschichten anzulegen, in denen

> 1. die Vorgeschichte der Erkrankung (Anamnese), der Zustand des Patienten zur Zeit der Aufnahme (status praesens), der Krankheitsverlauf (decursus morbi), die angeordneten Maßnahmen sowie die erbrachten ärztlichen und gegebenenfalls zahnärztlichen Leistungen einschließlich Medikation (insbesondere hinsichtlich Name, Dosis und Darreichungsform) und Aufklärung des Patienten und
>
> 2. sonstige angeordnete sowie erbrachte wesentliche Leistungen, insbesondere der pflegerischen und einer allfälligen psychologischen bzw. psychotherapeutischen Betreuung, sowie Leistungen der medizinisch-technischen Dienste, darzustellen sind;

e) den Gerichten und Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist, weiters den Versicherungsträgern im Sinne des § 52 und den Organen des Tiroler Gesundheitsfonds oder den von ihnen beauftragten Sachverständigen, soweit dies zur Wahrnehmung der ihnen obliegenden Aufgaben erforderlich ist, sowie den einweisenden oder weiterbehandelnden Ärzten, Zahnärzten oder Krankenanstalten auf Verlangen kostenlos Abschriften oder Ablichtungen von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Patienten zu übermitteln;

f) den mit Aufgaben des öffentlichen Gesundheitsdienstes betrauten Behörden alle Mitteilungen zu erstatten, die zur Einhaltung zwischenstaatlicher Verpflichtungen und zur Überwachung der Einhaltung bestehender Vorschriften erforderlich sind;

(5) Für ambulante Untersuchungen und Behandlungen gilt Abs. 1 sinngemäß mit der Maßgabe, daß die Aufbewahrungsfrist mindestens zehn Jahre beträgt."

3.3.1.8. § 63a Tir KAG lautet auszugsweise:

„Verarbeitung personenbezogener Daten

(3) Die Rechtsträger von Krankenanstalten sind Verantwortliche nach Art. 4 Z 7 der Datenschutz-Grundverordnung bei der Erfüllung der ihnen nach diesem Gesetz übertragenen Aufgaben.

(11) Die nach Abs. 3 Verantwortlichen dürfen die im Rahmen des Betriebes einer Krankenanstalt nach den Bestimmungen dieses Gesetzes erforderlichen personenbezogenen Daten zum Zwecke der Dokumentation und Auskunftserteilung (§ 15) und der Abrechnung (§§ 39 bis 44) verarbeiten.

(12) Die nach Abs. 3 Verantwortlichen sind berechtigt, Daten nach Abs. 11 zur Erfüllung ihrer gesetzlichen Verpflichtungen nach diesem Gesetz und nach dem Bundesgesetz über die Dokumentation im Gesundheitswesen sowie Daten nach Abs. 11 die für die Wirtschaftsaufsicht und die Abrechnung erforderlich sind, an den für das Gesundheitswesen zuständigen Bundesminister, die Gerichte, die Verwaltungsbehörden, die Versicherungsträger nach § 52, den Landeshauptmann, die Landesregierung, den Tiroler Gesundheitsfonds oder an beauftragte Sachverständige und Angehörige von Gesundheitsberufen zu übermitteln.

(14) Hinsichtlich der Verarbeitung personenbezogener Daten nach Abs. 11 sind die Pflichten und Rechte gemäß Art. 13, 14, 18 und 21 Datenschutz-Grundverordnung ausgeschlossen. Personenbezogene Daten gemäß Abs. 11, die der Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen dienen, dürfen jedenfalls bis zu 30 Jahre gespeichert und gegebenenfalls verarbeitet werden."

3.3.2. Umgelegt auf den gegenständlichen Fall bedeutet dies Folgendes:

3.3.2.1. Vorauszuschicken ist, dass Sache des vorliegenden Beschwerdeverfahrens - wie die belangte Behörde zu Recht ausführte - die Frage ist, ob die Beschwerdeführerin die mitbeteiligte Partei dadurch, dass sie von ihr verarbeitete Patientendaten (Auszüge aus der Krankengeschichte sowie einen Notfall-Bericht) an unbefugte Dritte übermittelt hat, in ihrem

Recht auf Datenschutz bzw. Geheimhaltung gemäß § 1 DSG verletzt hat (vgl. auch VwGH 08.02.2022, Ro 2021/04/0033).

Nicht Gegenstand dieses Beschwerdeverfahrens sind die durch die Beschwerdeführerin aufgeworfenen Vermutungen im Zusammenhang mit strafbaren Handlungen bzw. rechtswidrigen Vorgehensweisen durch die - an der Datenübermittlung - beteiligten Akteure.

3.3.2.2. Unstrittig ist, dass es sich bei den – in der E-Mail des Sicherheitsmanagers vom 04.10.2019 und im Notfallbericht vom 09.06.2019 enthaltenen - Informationen, dass die mitbeteiligte Partei sich im Zusammenhang mit einer Kokainintoxikation (mehrmals) in der Klinik der Beschwerdeführerin aufgehalten hat, der erhobenen Anamnese, den aufgetreten Symptomen, gewonnenen Untersuchungswerten sowie dem Behandlungsverlauf um „Gesundheitsdaten“ iSd Art. 4 Z 15 DSGVO handelt.

In der Literatur werden „Gesundheitsdaten“ als personenbezogene Daten definiert, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen, einschließlich der Gesundheitsdienstleistungen (Hödl in Knyrim, DatKomm Art. 4 DSGVO Rz 156 [Stand 01.12.2018, rdb.at]). Unstrittig ist, dass medizinische Daten (als Teilmenge) unter den Begriff der Gesundheitsdaten fallen, letzterer aber viel mehr erfasst (Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art. 9 DSGVO Rz 28 [Stand 07.05.2020, rdb.at]). Der EuGH hat bereits im Zusammenhang mit der DS-RL festgehalten, dass angesichts deren Zweck der in Art. 8 Abs. 1 DS-RL verwendete Begriff „Daten über Gesundheit“ in dem Sinne weit auszulegen ist, dass er sich auf alle Informationen bezieht, die die Gesundheit einer Person unter allen Aspekten (körperlichen wie psychischen) betreffen. Die Angabe, dass sich eine Person den Fuß verletzt hat und partiell krankgeschrieben ist, ist bereits als personenbezogenes Datum über die Gesundheit zu qualifizieren (vgl. EuGH 06.11.2003, C-101/01, Lindqvist). Dies steht auch im Einklang mit der Rechtsprechung des Verwaltungsgerichtshofes, wonach ein mittelbares Hervorgehen der sensiblen Information bzw. indirekte Hinweise auf sensible Merkmale für die Anwendbarkeit von Art. 9 Abs. 1 DSGVO ausreichend sind (vgl. VwGH 17.05.2024, Ra 2023/04/0005, Rz 30; 14.12.2021, Ro 2021/04/0007; vgl. auch EuGH 01.08.2022, C-184/20, Vyriausioji tarnybinės etikos komisija).

Vor diesem Hintergrund kann bezüglich der Qualifikation der beschwerdegegenständlichen Daten als „Gesundheitsdaten“ iSd Art. 4 Z 15 DSGVO kein Zweifel bestehen.

3.3.2.3. Bezüglich der Anwendung der DSGVO hat die belangte Behörde zutreffend ausgeführt, dass die Beschwerdeführerin eine in der Rechtsform einer Gesellschaft mit

beschränkter Haftung eingerichtete Trägerorganisation für öffentliche Krankenanstalten ist und die unter ihrer datenschutzrechtlichen Verantwortung gemäß § 15 und § 63a Tir KAG verarbeiteten Gesundheitsdaten von Patienten - und die Frage der Rechtmäßigkeit einer Übermittlung solcher Daten - den Regeln der DSGVO unterliegen, da der Verarbeitungszweck nicht unter die im 3. Hauptstück des DSG geregelten Verarbeitungszwecke fällt (§ 36 Abs. 1 DSG). Dies wurde von der Beschwerdeführerin auch nicht (substantiiert) in Abrede gestellt.

3.3.2.4. Strittig ist jedoch die datenschutzrechtliche Verantwortlicheneigenschaft der Beschwerdeführerin für die in Beschwerde gezogenen Datenverarbeitung, die von der belangten Behörde und der mitbeteiligten Partei bejaht, von der Beschwerdeführerin hingegen verneint wird.

Die belangte Behörde begründet ihre Ansicht damit, dass aus dem Sachverhalt nicht ableitbar sei, dass der (ehemalige) Sicherheitsmanager der Beschwerdeführerin unmittelbar vor oder bei der gegenständlichen Datenübermittlung eigene Zwecke verfolgt hätte und nicht der Meinung gewesen wäre, im Interesse der Beschwerdeführerin ihm Rahmen seiner dienstlichen Aufgaben zu handeln. Daher müsse sich die Beschwerdeführerin das – wenngleich rechtswidrige und unter Überschreitung seiner datenschutzrechtlichen Befugnisse erfolgte – Verhalten des Sicherheitsmanagers in vollem Umfang bis zu jenem Punkt zurechnen lassen, an dem die Daten der mitbeteiligten Partei in den Verantwortungsbereich der Landespolizeidirektion gelangt seien.

Die Argumentation der Beschwerdeführerin geht demgegenüber dahin, dass sie für die Weiterleitung der Gesundheitsdaten der mitbeteiligten Partei durch den Sicherheitsmanager nicht (mehr) als Verantwortliche gemäß Art. 4 Z 7 DSGVO anzusehen sei, da dieser eigenmächtig, vorsätzlich und ohne Konnex zu seiner dienstlichen Tätigkeit gehandelt habe.

Dem Standpunkt der Beschwerdeführerin kann allerdings nicht beigetreten werden:

Der zentrale Anknüpfungspunkt im Regime der DSGVO ist der Verantwortliche. Beim Verantwortlichen handelt es sich um jene Person oder Einrichtung, die dafür zu sorgen hat, dass die Datenschutzbestimmungen der DSGVO eingehalten werden. Damit gilt der Verantwortliche als Adressat der Pflichten aus der DSGVO und der Begriff dient der Zuweisung von Verantwortlichkeiten. Sowohl natürliche als auch juristische Personen und vergleichbare Personenmehrheiten können Verantwortliche nach der DSGVO sein, unabhängig davon, ob sie öffentlich-rechtlich oder privatrechtlich organisiert sind (vgl. Hödl in Knyrim, DatKomm Art. 4 DSGVO Rz 77, 81 [Stand 01.12.2018, rdb.at]).

Die Verantwortung wird dem übertragen, der die Entscheidungsmacht hat. Entscheidend für die Zuweisung der Verantwortlichkeit ist daher, wer über die wesentlichen Aspekte der Mittel der Verarbeitung entscheidet. Für die Zuschreibung der Verantwortlichen-Eigenschaft ist es nicht erforderlich, dass der Verantwortliche selbst Daten verarbeitet, sich im Besitz der verarbeiteten Daten befindet oder über die physische Herrschaft verfügt. Trifft er die Entscheidung, dass Daten zu verarbeiten sind, sind ihm sämtliche Personen und Stellen funktional zuzurechnen, die unter seiner Aufsicht bzw. Anweisung Schritte einer Datenverarbeitung vornehmen (Hilfsorgane) (vgl. Hödl in Knyrim, DatKomm Art. 4 DSGVO Rz 83 [Stand 01.12.2018, rdb.at]).

Der gemäß Art. 68 DSGVO eingerichtete Europäische Datenausschuss (EDSA) führt in seinen „Leitlinien 07/2020“ über das Konzept von Verantwortlichen und Auftragsverarbeitern nach der Datenschutzgrundverordnung aus, dass Angestellte, die Zugriff zu personenbezogenen Daten innerhalb einer Organisation haben, grundsätzlich nicht als Verantwortliche oder als Auftragsverarbeiter zu sehen sind (Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, angenommen am 07.07.2021, 10 f). In Ausnahmesituationen kann es jedoch vorkommen, dass ein Beschäftigter beschließt, personenbezogene Daten für seine eigenen Zwecke zu verwenden, wodurch die ihm erteilte Befugnis unrechtmäßig überschritten wird (z.B. Gründung eines eigenen Unternehmens o. ä.). Daher hat die Organisation als Verantwortlicher dafür zu sorgen, dass angemessene technische und organisatorische Maßnahmen, wie z. B. Schulungen und Informationen für Mitarbeiter, ergriffen werden, um die Einhaltung der DSGVO sicherzustellen.

Unstrittig ist, dass die Beschwerdeführerin als Rechtsträgerin der beschwerdegegenständlich involvierten Krankenanstalt gemäß § 63a Abs. 3 Tir KAG als Verantwortliche nach Art. 4 Z 7 DSGVO für die bei der Erfüllung der ihr nach dem genannten Gesetz übertragenen Aufgaben anzusehen ist. Bei den über die mitbeteiligte Partei verarbeiteten sensiblen Daten liegt ein solcher Konnex gemäß § 15 Abs. 1 lit. b und Abs. 5 Tir KAG vor, da die mitbeteiligte Partei als Patient in der Notaufnahme der Klinik XXXX behandelt wurde und somit die rechtliche Verpflichtung bestand, ihre Krankengeschichte zu verarbeiten. Darüber hinaus ist es die gesetzliche Aufgabe der Beschwerdeführerin gemäß § 15 Abs. 1 lit. e Tir KAG u.a. den Gerichten und Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist, auf Verlangen kostenlos Abschriften oder Ablichtungen von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Patienten zu übermitteln.

Darüber hinaus kann eine Verantwortlichenstellung (etwa einer Gebietskörperschaft) auch in der - der Weiterverarbeitung durch einen Bediensteten zugrundeliegenden - Speicherung der Daten begründet sein kann (vgl. VwGH 29.07.2025, Ro 2022/04/0017). Im vorliegenden Fall wurden personenbezogene Daten des Mitbeteiligten von der Beschwerdeführerin jedoch selbst im Rahmen ihrer gesetzlichen Aufgaben, zum Zweck der „Führung von Krankengeschichten und sonstigen Vormerkungen“ nach § 15 Tir KAG, verarbeitet.

Der Verwaltungsgerichtshof hat sich zuletzt im Erkenntnis vom 27.03.2025, Ro 2022/04/0023, ausführlich mit dem Begriff des „Verantwortlichen“ gemäß Art. 4 Z 7 DSGVO auseinandergesetzt. Unter Verweis auf die hier einschlägige Rechtsprechung des EUGH (07.03.2024, C-604/22, IAB Europe/Gegevensbeschermingsautoriteit; 05.12.2023, C-807/21, Deutsche Wohnen SE; 10.07.2018, C-25/17, Zeugen Jehovas) sowie die Leitlinien des EDSA 07/2020 sprach der Verwaltungsgerichtshof aus, dass die Frage der Verantwortlichenstellung unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalles zu beurteilen ist. Um zu klären, ob eine Person als Verantwortliche im Sinn des Art. 4 Z 7 DSGVO (bzw. allenfalls als gemeinsam Verantwortliche gemäß Art. 26 Abs. 1 DSGVO) angesehen werden kann, ist zu prüfen, ob sie unter Berücksichtigung der besonderen Umstände des Falles aus Eigeninteresse auf die betreffende Verarbeitung personenbezogener Daten Einfluss genommen und - allenfalls gemeinsam mit anderen - die Zwecke der und die Mittel zur fraglichen Bearbeitung festgelegt hat. Es kommt daher darauf an, welche natürliche oder juristische Person jeweils die Entscheidung sowohl über den Zweck - das „warum“ - als auch über die Mittel - „auf welche Weise“ - in Bezug auf die konkrete Handlung getroffen hat (VwGH 29.07.2025, Ro 2022/04/0017).

Dem - mit dem zitierten Erkenntnis Ro 2022/04/0023 entschiedenen - Fall lag zu Grunde, dass Bedienstete einer Gemeinde, die kraft ihrer Stellung Zugang zur ZMR-Abfrage hatten, diese Abfragemöglichkeit zu anderen als zu dienstlichen Zwecken nutzten. Der Verwaltungsgerichtshof sah hier die Gemeinde nicht als Verantwortliche im Sinn des Art. 4 Z 7 DSGVO an. Die für die Verantwortlichenstellung im Sinn des Art. 4 Z 7 DSGVO ausschlaggebende Entscheidung darüber, dass die (von der Gemeinde zur Verfügung stehenden) Mittel für die konkreten Abfragen eingesetzt wurden, und zu welchem Zweck dieser Einsatz erfolgte, wurde nämlich von den Personen - den Bediensteten der Gemeinde - getroffen, die die Abfragen für ihre eigenen privaten Zwecke tätigten. Für den Verwaltungsgerichtshof korrelierte dieses Ergebnis auch mit den Leitlinien des EDSA, dass die betreffenden Bediensteten fallbezogen auch nicht als Personen zu verstehen sind, die „unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftraggebers befugt sind, personenbezogene Daten zu verarbeiten“, weil sie als solche nur insoweit anzusehen sind, als

sie zur Verarbeitung personenbezogener Daten befugt sind. Eine bei der Gemeinde beschäftigte Person, die Kraft ihrer Stellung Zugang zur Abfragemöglichkeit hatte - oder sich diese verschaffte - und die ZMR-Abfragemöglichkeit zu anderen als zu dienstlichen Zwecken, die der Gemeinde zuordenbar wären, durchführte, ist in Zusammenhang mit der vorgenommenen Verarbeitung gegenüber der Gemeinde als Dritter zu betrachten, wobei diese(r) Dritte in Bezug auf die relevante Verarbeitung allenfalls selbst als Verantwortlicher zu betrachten ist (VwGH 29.07.2025, Ro 2022/04/0017).

Im vorliegenden Fall wurde das Fehlverhalten des Sicherheitsmanagers der Beschwerdeführerin hingegen im Rahmen seiner dienstlichen Aufgaben, so der „Sicherstellung der Kommunikation mit der Polizei“, gesetzt. Die Beschwerdeführerin legte im verwaltungsbehördlichen Verfahren ausdrücklich dar, dass es die dienstliche Aufgabe des Sicherheitsmanagers war, im Zusammenhang mit der präventiven und repressiven Abwehr von Straftaten eine Abstimmung mit den Sicherheitsbehörden vorzunehmen. Dies steht im Einklang mit dem von der Beschwerdeführerin vorgelegten Urteil des Landesgerichtes XXXX als Arbeits- und Sozialgericht, XXXX , betreffend die Entlassung des Sicherheitsmanagers u.a. im Zusammenhang mit der verfahrensgegenständlichen Datenübermittlung, wonach diesem die Aufgabe der Kommunikation mit der Polizei zukam, wobei die interne Richtlinie Nr. 4464 die Funktion des Sicherheitsmanagers als Ansprechpartner für mündliche Anfragen durch die Polizei vorgesehen hat und dieser eingeschränkte Auskünfte zum Aufenthalt von Patienten erteilen durfte, während die Anforderung medizinischer Unterlagen durch die Polizei ausschließlich per E-Mail über eine bestimmte E-Mailadresse zu erfolgen hatte.

In diesem Kontext ist darüber hinaus zu berücksichtigen, dass der Sicherheitsmanager, obwohl diesem kein elektronsicherer Zugang zu sensiblen Patienteninformationen erteilt bzw. ein solcher Zugang explizit abgelehnt wurde und eine vollständige Protokollierung aller Zugriffe auf Patientendaten in der Klinik der Beschwerdeführerin erfolgte, ohne Schwierigkeiten die vollständige Krankengeschichte der mitbeteiligten Partei für die Beantwortung von einer an ihn gerichteten Anfrage eines Beamten der Landespolizeidirektion, welche die Frage des Aufenthalts der mitbeteiligten Partei im Zusammenhang mit einer Kokainintoxikation in der Klinik der Beschwerdeführerin betraf, bei der Leitung des Patientenbeschwerdemanagements durch eine E-Mail-Anfrage beschaffen konnte.

Für das Bundesverwaltungsgericht ist nicht ersichtlich, dass der Sicherheitsmanager nach der einschlägigen (bereits genannten) Rechtsprechung des EuGH und VwGH ein erkennbares Eigeninteresse an der verfahrensgegenständlichen Datenverarbeitung entwickelte hätte und außerhalb seiner dienstlichen Agenden - der Kommunikation mit den Sicherheitsbehörden

bzw. der Polizei - tätig geworden wäre. Dieser mag zwar (wie unten in Punkt 3.3.2.5. noch ausgeführt werden wird) sowohl nach dem Gesetz als auch nach den internen Regeln der Beschwerdeführerin sowie unter Überschreitung seiner Befugnisse im Bereich der Datenverarbeitung rechtswidrig gehandelt haben und, sei es aufgrund einer fehlgeleiteten Interpretation seiner Aufgabe, exzessiv und – wie die Protokollierung des Zugriffes bzw. das E-Mail an die Leitung des Patientenbeschwerdemanagements zeigt – auf unüblichem Weg die Patientendaten der mitbeteiligten Partei beschafft haben, dies jedoch nur im Zusammenhang mit der festgestellten Anfrage eines Beamten der Landespolizeidirektion, deren Bearbeitung - unabhängig vom verwendeten Medium - grundsätzlich in seinen Aufgabenbereich gefallen ist und auch gemäß § 15 Abs. 1 lit. e Tir KAG eine gesetzlich übertragene Aufgabe der Beschwerdeführerin darstellen kann.

Es ist gerade nicht erkennbar, dass die für die Verantwortlichenstellung im Sinn des Art. 4 Z 7 DSGVO ausschlaggebende Entscheidung darüber, dass die (von der Beschwerdeführerin zur Verfügung stehenden) Mittel, welche für die konkrete Übermittlung eingesetzt wurden, und zu welchem Zweck dieser Einsatz erfolgte, vom Sicherheitsmanager zu privaten Zwecken getroffen wurde (vgl. VwGH 27.03.2025, Ro 2022/04/0023). Der belangten Behörde ist zuzustimmen, dass nach Lage des Falles nicht gesagt werden kann, dass der Sicherheitsmanager die hier in Rede stehenden personenbezogenen Daten der mitbeteiligten Partei für eigene Zwecke entfremdet hat, etwa um die Daten wirtschaftlich zu verwerten, seine persönliche Neugier zu befriedigen oder etwas zum Tratsch im eigenen Bekanntenkreis beizutragen, der Sicherheitsmanager unmittelbar vor oder bei der gegenständlichen Datenübermittlung eigene Zwecke verfolgt hätte und nicht der Meinung gewesen wäre, im Interesse der Beschwerdeführerin und im Rahmen seiner dienstlichen Aufgaben zu handeln. Die Beschwerdeführerin hat kein Vorbringen erstattet, das eine andere Sichtweise nahelegen würde. Eine Durchbrechung der Grenzen der datenschutzrechtlichen Verantwortlichkeit der Beschwerdeführerin liegt daher im vorliegenden Fall nicht vor.

Soweit die Beschwerdeführerin dieser Beurteilung entgegenhält, dass der Datenexzess durch den Sicherheitsmanager einer privaten Zweckverfolgung gleichzuhalten sei, da dieser sich im Klaren über seine - auch in einer internen Richtline vorgesehenen -Tätigkeitsbeschränkungen sein musste, übersieht die Beschwerdeführerin, dass sie für die Art und Weise der Verarbeitung bzw. Verwendung durch ihre Bediensteten verantwortlich ist, auch soweit es sich um eine überschießende Datenverarbeitung handelt. Aus dem Umstand, dass sich nach den Feststellungen der Sicherheitsmanager die - für die polizeiliche Anfragebeantwortung verwendete - Krankengeschichte der mitbeteiligten Partei durch eine einfache E-Mail-Anfrage bei der Leitung des Patientenmanagements beschaffen konnte, folgt, dass Grundsätze der

Datenverarbeitung, insbesondere die organisatorischen Datensicherheitsmaßnahmen, durch für die Beschwerdeführerin tätige Bedienstete verletzt wurden. Auch die Handlungen bzw. Unterlassungen, die zu dieser Verletzung führten, muss sich die Beschwerdeführerin zuzurechnen lassen. Daran ändern auch die von der Beschwerdeführerin ins Treffen geführten und implementierten Datensicherheitsmaßnahmen nichts, da sich diese gegen eine einfache E-Mail-Anfrage als offensichtlich unzureichend erwiesen haben bzw. die durch die Beschwerdeführerin eingeführten Kontrollmöglichkeiten nicht genutzt wurden (Monitoring der Zugriffe auf Patientendaten z.B. in Verbindung mit einer Plausibilitätsprüfung). Dass diesbezügliche Schulungen oder Überprüfungen stattfanden, wurde von der Beschwerdeführerin bloß unsubstantiiert behauptet, überdies kann auch bei langjährigen Mitarbeitern nicht davon ausgegangen werden, dass auf wiederholte datenschutzrechtliche Schulungs- und Überprüfungsmaßnahmen verzichtet werden kann. Die Beschwerdeführerin führte in ihrer Beschwerde dahingehend sogar ausdrücklich aus, dass „auch ohne Belehrung“ der Sicherheitsmanager die Rechtswidrigkeit seines Handelns erkennen hätte müssen. Die hier vorliegende Art und Weise der Datenverwendung ist der Beschwerdeführerin somit jedenfalls als der gemäß Art. 4 Z 7 DSGVO, für die Verarbeitung der Daten der mitbeteiligten Partei für Zwecke der Beantwortung von polizeilichen Anfragen, Verantwortlichen zuzurechnen.

Darüber hinaus ist klarzustellen, dass nicht jedes Fehlverhalten, unabhängig von der Frage einer möglichen Strafbarkeit oder eines schuldhaften Verhaltens beteiligter Personen, augenblicklich die Zurechnung der Verarbeitung zu dem bis zu diesem Zeitpunkt für die Verarbeitung Verantwortlichen unterbricht. Eine solche Unterbrechung der Zurechnung tritt vielmehr erst dann ein, wenn der Verantwortliche die Kontrolle über den regelwidrigen Verarbeitungsvorgang verliert, weil dieser sich nunmehr „außerhalb des Tätigkeitsbereichs und der möglichen Kontrolle“ seiner Organisation entfaltet (vgl. Hödl in Knyrim, DatKomm Art. 4 DSGVO Rz 86 [Stand 01.12.2018, rdb.at], unter Berufung auf Hartung in Kühling/Buchner, DS-GVO Art. 4 Nr 7 Rz 10). Gerade dies ist hier aber nicht der Fall gewesen, da der Sicherheitsmanager als für die Beschwerdeführerin agierender Mitarbeiter im Rahmen seines Aufgabenbereiches tätig war, wenngleich er exzessive Übermittlungen von sensiblen Daten an Dritte vorgenommen hat (vgl. etwa auch BVwG 30.09.2020, W274 2225135-1/3E, wonach eine Datenweitergabe durch einen Lehrer an Klassensprecher nicht diesem, sondern der Schule zuzurechnen war).

Vor diesem Hintergrund bleibt für die gegenteiligen Ausführungen der Beschwerdeführerin im Zusammenhang mit der eigenständigen Verantwortlicheneigenschaft des Sicherheitsmanagers kein Raum. Die angeführte Norm des Art. 29 DSGVO erfasst - wie die

Beschwerdeführerin zutreffend vorbringt - Angestellte bzw. Mitarbeiter eines Verantwortlichen und legt fest, dass diese ausschließlich auf dessen Weisung personenbezogene Daten verarbeiten dürfen. Art. 29 DSGVO steht in Relation zu Art. 32 Abs. 4 DSGVO, da Verantwortliche und Auftragsverarbeiter entsprechende Schritte zu unternehmen haben, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten (vgl. Bogendorfer in Knyrim, DatKomm Art. 29 DSGVO Rz 3 [Stand 01.12.2022, rdb.at]). Für die Beurteilung, ob die „Rolle“ einer „unterstellten Person“ angenommen werden kann, ist eine konkret vorliegende Weisung aber nicht entscheidend. Die rechtliche Eingriffsmöglichkeit in einen grundsätzlich vorgegebenen Verarbeitungsrahmen ist erforderlich (vgl. Bogendorfer in Knyrim, DatKomm Art. 29 DSGVO Rz 22 [Stand 01.12.2022, rdb.at]). Dies wird in einem Arbeitsverhältnis bzw. Dienstverhältnis, gerade bei Verarbeitungen im Rahmen einer neu geschaffenen Ansprechperson für Dritte (konkret: der Polizei), welche zu von der Beschwerdeführerin vorgegebenen Zwecken Auskünfte erteilt, stets dazu führen, dass nicht der Bedienstete selbst Verantwortlicher ist, sondern der Arbeit- bzw. Dienstgeber. Eine Ausnahme wird nur dann in Frage kommen, wenn ein Bediensteter seine Befugnisse insofern unrechtmäßig überschreitet als er beschließt, die Daten für seine eigenen privaten Zwecke zu verarbeiten (vgl. dazu auch BVwG 05.07.2022, W252 2246278-1/4E). Ein solcher Fall von privater Zweckverfolgung bzw. unvereinbarer Durchbrechung des vorgegebenen Verarbeitungszweckes des Verantwortlichen liegt jedoch - wie oben bereits ausgeführt - nicht vor. Zuletzt kann auch aus dem zitierten Judikat des EuGH vom 29.07.2019, C-40/17 (Fashion ID) für den Standpunkt der Beschwerdeführerin nichts gewonnen werden, da es diesem Fall an einem vergleichbaren Sachverhalt - einer Datenverarbeitungen durch Bedienstete zu privaten Zwecken - fehlt. Auch die Hinweise der Beschwerdeführerin auf die Haftungsregeln des ABGB und auf schadenersatzrechtliche Erwägungen sind aufgrund der unmittelbaren Anwendbarkeit und unionsrechtlichen Auslegung der DSGVO nicht stichhaltig. Denn, wie die belangte Behörde in ihrer Stellungnahme zu Recht ausgeführt hat, fordert die DSGVO für die Zurechnung eines rechtswidrigen Verarbeitungsvorganges weder, dass dem Handelnden besondere Befugnisse (wie eine Vollmacht, sonstige Vertretungsmacht oder besondere technische Nutzerprivilegien für ein Datenverarbeitungssystem) eingeräumt waren, noch, dass das rechtswidrige Handeln durch Verschulden des Verantwortlichen verursacht oder ermöglicht wurde. Darauf, ob die Beschwerdeführerin einen Grund hatte, vorab an der Zuverlässigkeit und Rechtstreue des Sicherheitsmanagers zu zweifeln, oder ob sie die Möglichkeit hatte, seine Handlungen zu verhindern, kommt es daher nicht an.

Im Ergebnis hat nach den Umständen dieses Falles der Sicherheitsmanager Gesundheitsdaten der mitbeteiligten Partei enthaltende Informationen/Unterlagen zwar rechtswidrig übermittelt, jedoch ohne Verfolgung von Eigeninteressen im Rahmen seiner beruflichen Tätigkeit, zu der auch die Aufgabe der „Sicherstellung der Kommunikation mit der Polizei“ gehörte, sodass keine Durchbrechung des Zwecks der Datenverarbeitung stattgefunden hat.

Der belangten Behörde kann daher bei der Einstufung der Beschwerdeführerin als Verantwortliche im Zusammenhang mit der verfahrensgegenständlichen Datenverarbeitung nicht entgegengetreten werden.

3.3.2.5. Der belangten Behörde ist auch dahin zu folgen, dass die in Beschwerde gezogene Datenverarbeitung (Datenübermittlung) nicht rechtmäßig nach dem DSG und der DSGVO war.

Eine zulässige Beschränkung des Geheimhaltungsanspruchs nach § 1 DSG ergibt sich grundsätzlich aus dem zweiten Absatz dieser Bestimmung, die DSGVO und insbesondere auch die dort (in Art. 5 DSGVO) verankerten Grundsätze sind jedoch zur Auslegung des Rechts auf Geheimhaltung jedenfalls zu berücksichtigen (vgl. Thiele/Wagner, Praxiskommentar zum Datenschutzgesetz [DSG]² § 1, Rz 39 [Stand 01.02.2022, rdb.at]).

Art. 5 DSGVO legt die Grundsätze für die Verarbeitung personenbezogener Daten fest (Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz [Art. 5 Abs. 1 lit. a], Grundsatz der Zweckbindung [Art. 5 Abs. 1 lit. b], Grundsatz der Datenminimierung [Art. 5 Abs. 1 lit. c], Grundsatz der Richtigkeit [Art. 5 Abs. 1 lit. d], Grundsatz der Speicherbegrenzung [Art. 5 Abs. 1 lit. e], Grundsatz der Integrität und Vertraulichkeit [Art. 5 Abs. 1 lit. f], Grundsatz der Rechenschaftspflicht [Art. 5 Abs. 2], vgl. Jahnel, Kommentar zur Datenschutz-Grundverordnung Art. 5 DSGVO [Stand 01.12.2020, rdb.at]).

Die Anforderungen für eine rechtmäßige Datenverarbeitung von Gesundheitsdaten sind in Art. 9 Abs. 2 DSGVO konkretisiert. Im vorliegenden Fall ist der Rechtsfertigungsgrund des Art. 9 Abs. 2 lit. g DSGVO einschlägig, wonach die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

Art. 9 Abs. 2 lit. g DSGVO ist kein eigenständiger Zulässigkeitstatbestand, es handelt sich um eine „Öffnungsklausel“ zugunsten unionsrechtlicher und mitgliedstaatlicher Regelungen. Kernvoraussetzung ist, dass die Verarbeitung aus Gründen eines erheblichen öffentlichen

Interesses (Art. 8 Abs. 4 DS-RL verlangte ein „wichtiges öffentliches Interesse“) erforderlich sein muss, wie z.B. die Strafverfolgung, Sicherstellung der öffentlichen Gesundheit oder Gefahrenabwehr (vgl. Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art. 9 DSGVO Rz 49 und 50 [Stand 07.05.2020, rdb.at]).

Eine auf Art. 9 Abs. 2 lit. a bis h DSGVO gestützte Verarbeitung von zB Gesundheitsdaten ist nach der Rechtsprechung des EuGH zudem nur dann rechtmäßig, wenn sie sowohl die sich aus dieser Bestimmung ergebenden Anforderungen als auch die sich aus Art. 5 Abs. 1 lit. a und Art. 6 Abs. 1 DSGVO ergebenden Pflichten einhält und insbesondere eine der in Art. 6 Abs. 1 DSGVO genannten Rechtmäßigkeitsvoraussetzungen erfüllt (vgl. EuGH 21.12.2023, C-667/21, Krankenversicherung Nordrhein, Rz 76-79). Nicht erforderlich ist hingegen, dass die rechtfertigende Rechtsgrundlage die strittige Datenverarbeitung selbst bezeichnet (vgl. VwGH 21.12.2023, Ro 2021/04/0010 mit Verweis auf EuGH C-136/17).

Nach Art. 6 Abs. 1 lit. c DSGVO ist die Verarbeitung von Daten unter anderem dann rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Nach Art. 6 Abs. 1 lit. e DSGVO ist dies zudem dann der Fall, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Damit gilt (weiterhin), dass eine den (Verfahrens)Gesetzen entsprechende Verwendung von (sensiblen) Daten auch aus datenschutzrechtlicher Sicht zulässig ist (vgl. OGH 27.11.2019, 6Nc30/19t; siehe auch Jahnel, Kommentar zur Datenschutz-Grundverordnung Rz 61 zu Art. 6 DSGVO [Stand 01.12.2020, rdb.at]).

Vorauszuschicken ist des Weiteren, dass eine Erhebung (Art. 4 Z 2 DSGVO) von Gesundheitsdaten durch die Sicherheitsbehörden gemäß § 39 DSG nur für die in § 36 Abs. 1 DSG genannten Zwecke (insbesondere der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit) zulässig ist, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und die Verarbeitung gemäß § 38 DSG zulässig ist oder sie sich auf Daten bezieht, die die betroffene Person offensichtlich selbst öffentlich gemacht hat.

Zum Kriterium der Erforderlichkeit hat der EuGH mehrfach ausgeführt, dass eine Verarbeitung nur jene Daten enthalten darf, die auch erforderlich sind, und sich grundsätzlich auf das

absolut Notwendige beschränken muss (EuGH 09.11.2010, C-92/09 und C-93/09 [Schecke] Rz 86; 07.11.2013, C-473/12 [IPI] Rz 39; 11.12.2014, C-212/13 [Ryneš] Rz 28).

Ebenso verpflichtet § 15 Abs. 1 lit. e Tir KAG die Beschwerdeführerin ausschließlich in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist, auf Verlangen von Gerichten oder Verwaltungsbehörden kostenlos Abschriften oder Ablichtungen von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Patienten zu übermitteln.

Es ist die ständige Judikatur des EuGH, dass grundsätzlich jede Verarbeitung personenbezogener Daten den in Art. 6 DS-RL (nunmehr Art. 5 DSGVO) aufgestellten Grundsätzen, vorbehaltlich der nunmehr in Art. 23 DSGVO zulässigen Ausnahmen, in Bezug auf die Qualität der Daten und einem der in Art. 7 DS-RL (jetzt Art. 6 DSGVO) angeführten Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten genügen muss (vgl. Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art. 6 DSGVO Rz 1 [Stand 07.05.2020, rdb.at]; in diesem Sinne EuGH 20.05.2003, C-465/ 00, C-138/ 01 und C-139/ 01, Österreichischer Rundfunk; EuGH 16.12.2008, C-524/ 06, Huber; EuGH 02.03.2023, C-268/21, Norra Stockholm Bygg AB).

Vor diesem rechtlichen Hintergrund liegt aber eine Verletzung des Rechtes auf Geheimhaltung gemäß § 1 DSG durch die Beschwerdeführerin bzw. den für sie handelnden Sicherheitsmanager fallgegenständlich vor, weil die beschwerdegegenständliche Übermittlung und dadurch bewirkte Offenlegung der (sensiblen) Daten der mitbeteiligten Partei gegenüber der Landespolizeidirektion nicht entsprechend § 15 Abs. 1 lit. e Tir KAG erfolgte und aufgrund keiner die Beschwerdeführerin treffenden rechtlichen (gesetzlichen) Verpflichtung bzw. in Wahrnehmung einer im erheblichen öffentlichen Interesse gelegenen Aufgabe datenschutzrechtlich gerechtfertigt war. Die Beschwerdeführerin bzw. der für sie handelnde Sicherheitsmanager war aufgrund der anzuwendenden (Verfahrens)Gesetze weder berechtigt noch verpflichtet, aufgrund der bloß informellen Anfrage des Beamten der Landespolizeidirektion diesem die festgestellten Informationen aus der elektronisch gespeicherten Krankengeschichte der mitbeteiligten Partei und den Gesundheitsdaten der mitbeteiligten Partei enthaltenden Notfall-Bericht an die Landespolizeidirektion zu übermitteln.

Wie bereits die belangte Behörde zutreffend ausgeführt hat, hätte eine derartige Übermittlung ein begründetes Ersuchen der Landespolizeidirektion vorausgesetzt. Ein solches lag aber offenkundig nicht vor, da daraus nicht einmal hervorging, gegen wen und in welcher

Sache ermittelt wurde, ob etwa die mitbeteiligte Partei selbst einer Straftat verdächtigt wurde, oder ob dessen Daten zu dem Zweck benötigt wurden, ein Ermittlungsverfahren gegen (unbekannte) Dritte einzuleiten oder voranzutreiben. Gemäß § 15 Abs. 1 lit. e Tir KAG wäre die Beschwerdeführerin bzw. der für sie handelnde Mitarbeiter jedenfalls verpflichtet gewesen, sich zu vergewissern, in welcher Sache („Angelegenheit“) die Landespolizeidirektion Auskunft verlangt und für welche „Entscheidung oder Verfügung im öffentlichen Interesse“ die Landespolizeidirektion die Daten benötigte, wobei gemäß Art. 9 Abs. 2 lit. g DSGVO ein erhebliches öffentliches Interesse bestehen musste. Die Anfrage des Beamten der Landespolizeidirektion vom 03.10.2019 enthält keine Informationen oder auch nur Hinweise darauf, inwiefern die der Beschwerdeführerin zurechenbaren Übermittlungen von Gesundheitsdaten der mitbeteiligten Partei für den Zweck der Strafverfolgung oder anderer in § 36 Abs. 1 DSG genannten Zwecke erforderlich gewesen wäre. Spiegelbildlich wäre die Beschwerdeführerin bzw. der für sie handelnde Mitarbeiter verpflichtet gewesen, das Vorliegen dieser gesetzlichen Voraussetzungen zu prüfen, wobei die (unbedingte) Erforderlichkeit erst vorliegt, wenn der verfolgte Zweck nicht auf andere Weise mit gleicher Sicherheit erreicht werden kann oder es keine milderen Mittel gibt (vgl. Thiele/Wagner, Praxiskommentar zum Datenschutzgesetz [DSG]^2 § 39 Rz 15 [Stand 01.02.2022, rdb.at]). Es ist jedoch evident, dass der verfahrensgegenständlichen Datenübermittlung keine Prüfung der unbedingten Erforderlichkeit durch die Beschwerdeführerin bzw. den für sie handelnden Mitarbeiter vorausgegangen ist und eine solche auch nicht vorliegt, da anhand der polizeilichen Anfrage vom 03.10.2019 bereits der heranzuziehende Mindestmaßstab (Aktenzahl des Ermittlungsverfahrens, der zugrundeliegende Sachverhalt, die fehlende Alternative zur begehrten Informationsbeschaffung, die Stellung der mitbeteiligten Partei als Beschuldigter oder Zeuge und eine mögliche Gefahr im Verzug) nicht festgestellt werden kann. Vor diesem Hintergrund war bereits die Erforderlichkeit der Übermittlung von Gesundheitsdaten der mitbeteiligten Partei auszuschließen bzw. von einer datenschutzrechtlich überschießenden Übermittlung/Offenlegung von Daten auszugehen, die dem Grundsatz der Datenminimierung des Art. 5 Abs. 1 lit. c DSGVO nicht entsprochen hat.

Ebenso ist die Beschwerdeführerin bzw. der für sie handelnde Mitarbeiter gemäß § 15 Abs. 1 lit. e Tir KAG verpflichtet, ausschließlich in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist, eine Übermittlung von Kopien der Krankengeschichte und ärztlichen Äußerungen über den Gesundheitszustand der mitbeteiligten Partei an Verwaltungsbehörden vorzunehmen. Wie bereits zuvor ausgeführt, fehlte es der Beschwerdeführerin jedoch an den notwendigen Informationen, um eine solche Angelegenheit sowie das öffentliche Interesse

identifizieren bzw. beurteilen zu können und ist dies auch durch das Bundesverwaltungsgericht nicht zu erblicken.

Darüber hinaus wurden nach den eigenen Angaben der Beschwerdeführerin ihre vorgegebenen Arbeitsabläufe (insbesondere die organisatorischen und technischen Sicherheitsmaßnahmen) nicht eingehalten und in der Folge keine datenschutzkonforme Dokumentation der Datenübermittlung durchgeführt (Art. 5 Abs. 2 DSGVO), um Betroffenenrechte wahrnehmen zu können. Die polizeiliche Anfrage vom 03.10.2019, aber auch das Ersuchen des Sicherheitsmanagers an die Leiterin des Beschwerdemanagements hätte nach Eingang bei der Beschwerdeführerin dokumentiert, von den dafür zuständigen Organen geprüft und die Entscheidung samt Angabe der ausschlaggebenden Gründe wiederum dokumentiert werden müssen. Auch der genaue Umfang der an die anfragende Behörde übermittelten Daten (Dokumente, bei deren Übermittlung überdies Art. 32 DSGVO zu beachten ist) hätte dokumentiert werden müssen. Dies ist im vorliegenden Fall jedenfalls nicht in jenem Umfang geschehen, den die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO geboten hätte. Dies widerspricht wiederum den gemäß Art. 9 Abs. 2 lit. g DSGVO geforderten angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person.

Es ist den Ausführungen der belangten Behörde somit nicht entgegenzutreten, wenn sie schlussfolgert, dass die Datenübermittlungen an den Beamten der Landespolizeidirektion, jedenfalls in der Form und unter den Umständen, die gegenständlich vorlagen, nicht rechtmäßig waren und zumindest die Verarbeitungsgrundsätze des Art. 5 Abs. 1 lit. a - c DSGVO verletzt und der Erlaubnistatbestand des Art. 9 Abs. 2 lit. g DSGVO - mangels des Erfüllens des Tatbestandes einer geeigneten Rechtsgrundlage - nicht vorgelegen hat. Für das Bundesverwaltungsgericht sind auch keine anderen Rechtsgrundlagen für die vorgenommenen Datenübermittlungen ersichtlich, solche wurden von der Beschwerdeführerin auch nicht behauptet.

Im Ergebnis hat die Beschwerdeführerin bzw. der für sie handelnde Sicherheitsmanager die Gesundheitsdaten der mitbeteiligten Partei nicht den anzuwendenden (Verfahrens)Gesetzen entsprechend verwendet. Zwingende Bedingungen der Rechtmäßigkeit der Übermittlung von Gesundheitsdaten gemäß der DSGVO und dem Tir KAG wurden nicht eingehalten, womit ohne ausreichende Rechtsgrundlage in das Geheimhaltungsrecht der mitbeteiligten Partei eingegriffen wurde. Sohin ist die Zulässigkeit der in Beschwerde gezogenen, der Beschwerdeführerin zurechenbaren Datenverarbeitung aus datenschutzrechtlicher Sicht nicht gegeben.

3.3.3. Die behauptete Rechtswidrigkeit des Bescheides liegt daher nicht vor. Das Verfahren hat auch nicht ergeben, dass der Bescheid aus anderen, nicht geltend gemachten Gründen rechtswidrig wäre. Da dem angefochtenen Bescheid eine Rechtswidrigkeit iSd Art. 130 Abs. 1 Z 1 B-VG somit nicht anhaftet, war die Beschwerde abzuweisen.

3.3.4. Das Bundesverwaltungsgericht sieht sich aufgrund der gegenständlichen Beschwerde nicht veranlasst, einen Antrag gemäß Art. 267 AEUV an den Gerichtshof der Europäischen Union zu richten. Im Übrigen ist das Bundesverwaltungsgericht - im vorliegenden Fall - auf Grund der Möglichkeit, gegen seine Entscheidungen eine ordentliche oder außerordentliche Revision an den Verwaltungsgerichtshof zu erheben, kein letztinstanzliches Gericht im Sinne des Art. 267 AEUV (vgl. VfSlg. 19.896/2014).

3.4. Gemäß § 24 Abs. 1 VwGVG hat das Verwaltungsgericht auf Antrag oder, wenn es dies für erforderlich hält, von Amts wegen eine öffentliche mündliche Verhandlung durchzuführen.

Gemäß § 24 Abs. 4 VwGVG kann – soweit durch Bundes- oder Landesgesetz nichts anderes bestimmt ist – das Verwaltungsgericht ungeachtet eines Parteiantrags von einer Verhandlung absehen, wenn die Akten erkennen lassen, dass die mündliche Erörterung eine weitere Klärung der Rechtssache nicht erwarten lässt, und einem Entfall der Verhandlung weder Art. 6 Abs. 1 EMRK noch Art. 47 GRC entgegenstehen.

Ein solcher Fall liegt hier vor: Im vorliegenden Fall hat die Beschwerdeführerin die Durchführung einer Verhandlung beantragt. Es konnte jedoch gemäß § 24 Abs. 4 VwGVG ungeachtet dieses Parteiantrags von einer Verhandlung abgesehen werden, da nicht zu erkennen ist, dass eine mündliche Erörterung eine weitere Klärung der Rechtssache erwarten lässt, und es ist auch im Hinblick auf Art. 6 Abs. 1 EMRK und Art. 47 GRC die Notwendigkeit der Durchführung einer Verhandlung nicht ersichtlich. Der entscheidungsrelevante Sachverhalt ist anhand der Aktenlage feststehend und geklärt. Zu einer Lösung von Rechtsfragen ist im Sinne der Judikatur des EGMR eine mündliche Verhandlung nicht geboten. Im Hinblick auf die dem Beschwerdefall zu Grunde liegenden Rechtsfragen ist eine besondere Komplexität nicht ersichtlich. Die EMRK und die GRC stehen der Abstandnahme von einer mündlichen Verhandlung daher nicht entgegen. Aus diesen Gründen war es nicht erforderlich, eine öffentliche mündliche Verhandlung durchzuführen.

Zu B)

Gemäß § 25a Abs. 1 VwGG hat das Verwaltungsgericht im Spruch seines Erkenntnisses oder Beschlusses auszusprechen, ob die Revision gemäß Art. 133 Abs. 4 B-VG zulässig ist. Der Ausspruch ist kurz zu begründen.

Die vorliegende Entscheidung hängt nicht von der Lösung einer Rechtsfrage ab, der grundsätzliche Bedeutung zukommt. Weder fehlt es an einer Rechtsprechung des Verwaltungsgerichtshofes noch weicht die gegenständliche Entscheidung von der Rechtsprechung des Verwaltungsgerichtshofes ab; weiters ist die vorliegende Rechtsprechung des Verwaltungsgerichtshofes auch nicht als uneinheitlich zu beurteilen. Es liegen auch keine sonstigen Hinweise auf eine grundsätzliche Bedeutung der zu lösenden Rechtsfragen vor. Das Bundesverwaltungsgericht kann sich bei allen erheblichen Rechtsfragen auf eine ständige Rechtsprechung des Verwaltungsgerichtshofes bzw. auf eine ohnehin klare Rechtslage stützen. Es ist auch nicht ersichtlich, dass sich im konkreten Fall eine Rechtsfrage stellt, die über den (hier vorliegenden konkreten) Einzelfall hinaus Bedeutung entfaltet. Ausgehend davon kann eine Rechtsfrage im Sinn des Art. 133 Abs. 4 B-VG von grundsätzlicher Bedeutung auch insofern nicht bejaht werden. Es ist daher auszusprechen, dass die Revision gemäß Art. 133 Abs. 4 B-VG nicht zulässig ist.