

TE Dsk BescheidBeschwerde 2023/6/1 2023-0.315.174

JUSLINE Entscheidung

© Veröffentlicht am 01.06.2023

Norm

DSG §1 Abs1

DSG §1 Abs2

DSG §36 Abs1

DSG §39

DSGVO Art4 Z7

DSGVO Art5 Abs1

DSGVO Art5 Abs1 lita

DSGVO Art5 Abs2

DSGVO Art6 Abs4

DSGVO Art9 Abs1

DSGVO Art9 Abs2

DSGVO Art9 Abs2 litg

DSGVO Art9 Abs2 lith

DSGVO Art9 Abs3

Tir KAG §15 Abs1 lite

Tir KAG §63a

1. DSG Art. 1 § 1 heute
2. DSG Art. 1 § 1 gültig ab 01.01.2014 zuletzt geändert durch BGBl. I Nr. 51/2012
3. DSG Art. 1 § 1 gültig von 01.01.2000 bis 31.12.2013

1. DSG Art. 1 § 1 heute
2. DSG Art. 1 § 1 gültig ab 01.01.2014 zuletzt geändert durch BGBl. I Nr. 51/2012
3. DSG Art. 1 § 1 gültig von 01.01.2000 bis 31.12.2013

1. DSG Art. 2 § 36 heute
2. DSG Art. 2 § 36 gültig ab 29.06.2024 zuletzt geändert durch BGBl. I Nr. 62/2024
3. DSG Art. 2 § 36 gültig von 01.12.2021 bis 28.06.2024 zuletzt geändert durch BGBl. I Nr. 148/2021
4. DSG Art. 2 § 36 gültig von 25.05.2018 bis 30.11.2021 zuletzt geändert durch BGBl. I Nr. 24/2018
5. DSG Art. 2 § 36 gültig von 25.05.2018 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 120/2017
6. DSG Art. 2 § 36 gültig von 01.01.2014 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 83/2013
7. DSG Art. 2 § 36 gültig von 01.07.2010 bis 31.12.2013 zuletzt geändert durch BGBl. I Nr. 133/2009
8. DSG Art. 2 § 36 gültig von 01.01.2010 bis 30.06.2010 zuletzt geändert durch BGBl. I Nr. 133/2009
9. DSG Art. 2 § 36 gültig von 01.01.2000 bis 31.12.2009

1. DSGVO Art. 2 § 39 heute
2. DSGVO Art. 2 § 39 gültig ab 25.05.2018 zuletzt geändert durch BGBl. I Nr. 120/2017
3. DSGVO Art. 2 § 39 gültig von 01.01.2014 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 83/2013
4. DSGVO Art. 2 § 39 gültig von 01.01.2010 bis 31.12.2013 zuletzt geändert durch BGBl. I Nr. 133/2009
5. DSGVO Art. 2 § 39 gültig von 01.01.2000 bis 31.12.2009

Text

GZ: 2023-0.315.174 vom 1. Juni 2023 (Verfahrenszahl: DSB-D124.3118)

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

Die Beschwerdegegnerin konnte hier nicht effektiv pseudonymisiert werden, da ihre Identität aus den in der Begründung zitierten Rechtsvorschriften hervorgeht.]

BESCHEID

SPRUCH

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von Andreas Erich A*** (Beschwerdeführer) vom 16. September 2020 gegen die Tirol Kliniken GmbH (Beschwerdegegnerin, im Firmenbuch eingetragen zu [Anmerkung Bearbeiter/in: Angabe der Firmenbuchnummer fehlt infolge eines Redaktionsversehens bereits im Original] durch das Landesgericht Innsbruck) wegen Verletzung im Recht auf Geheimhaltung wie folgt:

- Der Beschwerde wird Folge gegeben und es wird festgestellt, dass die Beschwerdegegnerin den Beschwerdeführer in seinem Recht auf Geheimhaltung personenbezogener Daten verletzt hat, indem

a) am 4. Oktober 2019 Karl-Josef W*** MSc, der Sicherheitsbeauftragte („Securitymanager“) der Beschwerdegegnerin, um 11:28:17 Uhr eine E-Mail mit folgendem Inhalt an Abteilungsinspektor Richard U***, Beamter der Landespolizeidirektion für Tirol, Stadtpolizeikommando Innsbruck, Kriminalreferat (im Folgenden auch kurz: LPD), sendete, nachdem er sich zuvor eine Kopie der elektronisch gespeicherten Krankengeschichte des Beschwerdeführers (Patienten-ID: *3*4*p*00*32) 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 LKI.

P. 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 Karl-J“;

b) Karl-Josef W*** zu einem nicht näher bekannten Zeitpunkt zwischen dem 4. Oktober 2019 und dem 4. Juni 2020 den Gesundheitsdaten des Beschwerdeführers enthaltenden Notfall-Bericht vom 9. Juni 2019 an die LPD übersendete.

Rechtsgrundlagen: Art. 5 Abs. 1 lit. a, Art. 9 Abs. 1 und Abs. 2 lit. g, Art. 51 Abs. 1, Art. 57 Abs. 1 lit. f sowie Art. 77 Abs. 1 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, im Folgenden: DSGVO), ABl. Nr. L 119 vom 4.5.2016 S. 1; § 1 Abs. 1 und Abs. 2, § 18 Abs. 1 sowie § 24 Abs. 1 und Abs. 5 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999 idgF, iVm § 15 Abs. 1 lit. e des Tiroler Krankenanstaltengesetzes (Tir KAG), LGBl. Nr. 5/1958 idF LGBl. Nr. 152/2016. Rechtsgrundlagen: Artikel 5, Absatz eins, Litera a,, Artikel 9, Absatz eins und Absatz 2, Litera g,, Artikel 51, Absatz eins,, Artikel 57, Absatz eins, Litera f, sowie Artikel 77, Absatz eins, der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, im Folgenden: DSGVO), ABl. Nr. L 119 vom 4.5.2016 Sitzung eins, ; Paragraph eins, Absatz eins und Absatz 2,, Paragraph 18, Absatz eins, sowie Paragraph 24, Absatz eins und Absatz 5, des Datenschutzgesetzes (DSG),

Bundesgesetzblatt Teil eins, Nr. 165 aus 1999, idgF, in Verbindung mit Paragraph 15, Absatz eins, Litera e, des Tiroler Krankenanstaltengesetzes (Tir KAG), Landesgesetzblatt Nr. 5 aus 1958, in der Fassung Landesgesetzblatt Nr. 152 aus 2016,.

BEGRÜNDUNG

A. Vorbringen der Parteien und Verfahrensgang

1. In seiner vom 16. September 2020 datierenden, am 12. Oktober 2020 ergänzten und am 15. Oktober 2020 per Brief bei der Datenschutzbehörde eingelangten Beschwerde hat der Beschwerdeführer Folgendes vorgebracht: Er sei am 9. Juni 2019 in der Notaufnahme der Innsbrucker Klinik behandelt worden. Nur die Klinik und sein Hausarzt Dr. M*** aus H*** seien darüber informiert gewesen. Nun habe er vor Gericht (Bezirks- bzw. Landesgericht Innsbruck) am 1. Juni 2020 davon Kenntnis erlangt, dass Gesundheitsdaten (Notfall-Bericht der von der Beschwerdegegnerin betriebenen Universitätskliniken Innsbruck) ohne sein Einverständnis an Dritte weitergegeben worden seien. Diese sei ein unzulässiger Eingriff in sein Recht auf Geheimhaltung gemäß § 1 DSG unter Verstoß gegen die Art. 5, 6 und 9 DSGVO gewesen. Er sei der Patient, der die „Tirol Klinik Datenaffäre“ ausgelöst habe. Am 16. September habe er bei einem Treffen mit den Datenschutzbeauftragten der Beschwerdegegnerin das Zugriffsprotokoll für seine Krankenakte erhalten und danach eine schriftliche Sachverhaltsdarstellung an die Beschwerdegegnerin gerichtet. Am 6. Oktober 2020 habe er von Seiten der Beschwerdegegnerin telefonisch die Mitteilung erhalten, dass sich der Verdacht erhärtet habe. Am selben Tag seien von Seiten der Beschwerdegegnerin bei einer Pressekonferenz auch die Medien informiert worden. In seiner vom 16. September 2020 datierenden, am 12. Oktober 2020 ergänzten und am 15. Oktober 2020 per Brief bei der Datenschutzbehörde eingelangten Beschwerde hat der Beschwerdeführer Folgendes vorgebracht: Er sei am 9. Juni 2019 in der Notaufnahme der Innsbrucker Klinik behandelt worden. Nur die Klinik und sein Hausarzt Dr. M*** aus H*** seien darüber informiert gewesen. Nun habe er vor Gericht (Bezirks- bzw. Landesgericht Innsbruck) am 1. Juni 2020 davon Kenntnis erlangt, dass Gesundheitsdaten (Notfall-Bericht der von der Beschwerdegegnerin betriebenen Universitätskliniken Innsbruck) ohne sein Einverständnis an Dritte weitergegeben worden seien. Diese sei ein unzulässiger Eingriff in sein Recht auf Geheimhaltung gemäß Paragraph eins, DSG unter Verstoß gegen die Artikel 5, 6, und 9 DSGVO gewesen. Er sei der Patient, der die „Tirol Klinik Datenaffäre“ ausgelöst habe. Am 16. September habe er bei einem Treffen mit den Datenschutzbeauftragten der Beschwerdegegnerin das Zugriffsprotokoll für seine Krankenakte erhalten und danach eine schriftliche Sachverhaltsdarstellung an die Beschwerdegegnerin gerichtet. Am 6. Oktober 2020 habe er von Seiten der Beschwerdegegnerin telefonisch die Mitteilung erhalten, dass sich der Verdacht erhärtet habe. Am selben Tag seien von Seiten der Beschwerdegegnerin bei einer Pressekonferenz auch die Medien informiert worden.

2. Von der Datenschutzbehörde entsprechend aufgefordert (Verfahrensordnung vom 20. Oktober 2020, GZ: 2020-0.669.690), hat die Beschwerdegegnerin in ihrer Stellungnahme vom 14. Jänner 2021 darauf Folgendes erwidert: Die Datenschutzbeauftragten der Beschwerdegegnerin seien dem Anliegen des Beschwerdeführers nachgekommen und hätten ihm die Zugriffsprotokollierung auf seine Krankengeschichte bei einem persönlichen Besprechungstermin ausgehändigt. In diesem Zusammenhang habe der Beschwerdeführer auch die vermutete Weitergabe seiner personenbezogenen Daten an den gegnerischen rechtsfreundlichen Vertreter in einem Arbeitsgerichtsverfahren erwähnt. Die Datenschutzbeauftragten der Beschwerdegegnerin hätten sich umgehend um die Aufklärung des Sachverhaltes bemüht und eine Data Breach Meldung erstattet. Der Beschwerdeführer sei in weiterer Folge mehrfach von den Datenschutzbeauftragten über den aktuellen Stand informiert und es sei ihm auch zugesichert worden, dass sein Name im Zusammenhang mit der unrechtmäßigen Datenweitergabe an die Polizei nicht erwähnt werde, da dies von ihm nicht gewünscht gewesen sei. Es habe nicht festgestellt werden können, von wem tatsächlich der Arztbrief nach außen weitergegeben worden sei. Vielleicht würden hier die staatsanwaltlichen Ermittlungen noch ein Ergebnis hervorbringen. Intern seien die zwei betroffenen Mitarbeiter- bzw. Mitarbeiterinnen, welche für die Datenweitergabe verantwortlich gewesen seien, entlassen worden.

3. Mit Verfahrensordnung vom 18. Jänner 2021, GZ: 2021-0.033.990, hat die Datenschutzbehörde dem Beschwerdeführer erstmals zu den vorliegenden Ergebnissen des Ermittlungsverfahrens Parteiengehör eingeräumt.

4. Der Beschwerdeführer hat sich nicht geäußert.

5. Mit Verfahrensordnungen vom 21. Mai 2021, GZ: 2021-0.367.201, hat die Datenschutzbehörde zum einen ein Amtshilfeersuchen an die LPD gerichtet und um Auskunft über den Stand Bezug habender kriminalpolizeilicher

Ermittlungen und Übermittlung relevanter Unterlagen ersucht, zum anderen die Beschwerdegegnerin zur ergänzenden Stellungnahme und Beantwortung einer Reihe konkreter Fragen aufgefordert.

6. Mit Schreiben (E-Mail) vom 27. Mai 2021 hat die LPD (Landeskriminalamt) die Datenschutzbehörde um nähere Angaben zur Person des Beschwerdeführers und zum Sachverhalt ersucht.

7. Mit Schreiben vom 28. Mai 2021; GZ: 2021-0.382.824, hat die Datenschutzbehörde entsprechende Informationen in Form von Aktenkopien an die LPD übermittelt.

8. Am 9. Juni 2021 hat die Beschwerdegegnerin schriftlich folgende ergänzende Stellungnahme abgegeben: Die beiden Mitarbeiter, von denen man sich getrennt habe, seien für die Leitung des Patientenbeschwerdemanagements bzw. des Securitymanagements verantwortlich gewesen. Ihre Zugriffsberechtigung auf die IKT-Systeme sei entsprechend den betrieblichen Notwendigkeiten eingerichtet gewesen. Bei der Beschwerdegegnerin werde jeder Zugriff auf die Krankengeschichte über das Krankenhausinformationssystem mitprotokolliert. Die Zugriffsprotokollierung werde 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 jene Person gehabt, welcher die Leitung des Patientenbeschwerdemanagements zukam, da für diese Funktionswahrnehmung die Sichtung der Krankengeschichte notwendig sei. Das Patientenbeschwerdemanagement sei der ärztlichen Direktion des Landeskrankenhauses Innsbruck (LKI) 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 oblag die Bearbeitung sämtlicher Patientenbeschwerden am LKI sowie die Bearbeitung von externen Anfragen zu Krankengeschichten. Dem Securitymanager oblag das Sicherstellen des täglichen Geschäftsablaufs der Tirol Kliniken GmbH 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 ggf. 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 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 Verzeichnis der Beschwerdegegnerin auf deren Website öffentlich einsehbar. Die Zugriffsrechte auf das Krankenhausinformationssystem würden in einem Berechtigungskonzept dargestellt. Dieses Berechtigungskonzept werde regelmäßig durch die interne Datenschutzkommission der Beschwerdegegnerin angepasst und freigegeben. Das Berechtigungskonzept orientiere sich an den datenschutzrechtlichen Grundsätzen gemäß Art. 5 DSGVO, insbesondere dem Grundsatz der Datenminimierung. Am 9. Juni 2021 hat die Beschwerdegegnerin schriftlich folgende ergänzende Stellungnahme abgegeben: Die beiden Mitarbeiter, von denen man sich getrennt habe, seien für die Leitung des Patientenbeschwerdemanagements bzw. des Securitymanagements verantwortlich gewesen. Ihre Zugriffsberechtigung auf die IKT-Systeme sei entsprechend den betrieblichen Notwendigkeiten eingerichtet gewesen. Bei der Beschwerdegegnerin werde jeder Zugriff auf die Krankengeschichte über das Krankenhausinformationssystem mitprotokolliert. Die Zugriffsprotokollierung werde 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 jene Person gehabt, welcher die Leitung des Patientenbeschwerdemanagements zukam,

da für diese Funktionswahrnehmung die Sichtung der Krankengeschichte notwendig sei. Das Patientenbeschwerdemanagement sei der ärztlichen Direktion des Landeskrankenhauses Innsbruck (LKI) zugeordnet. Die Leitung sein 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 oblag die Bearbeitung sämtlicher Patientenbeschwerden am LKI sowie die Bearbeitung von externen Anfragen zu Krankengeschichten. Dem Securitymanager oblag das Sicherstellen des täglichen Geschäftsablaufs der Tirol Kliniken GmbH 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 ggf. 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 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 Beschwerdegegnerin auf deren Website öffentlich einsehbar. Die Zugriffsrechte auf das Krankenhausinformationssystem würden in einem Berechtigungskonzept dargestellt. Dieses Berechtigungskonzept werde regelmäßig durch die interne Datenschutzkommission der Beschwerdegegnerin angepasst und freigegeben. Das Berechtigungskonzept orientiere sich an den datenschutzrechtlichen Grundsätzen gemäß Artikel 5, DSGVO, insbesondere dem Grundsatz der Datenminimierung.

9. Mit Schreiben (E-Mail) vom 10. Juni 2021 hat die LPD (Landeskriminalamt) der Datenschutzbehörde mitgeteilt, dass der Sachverhalt „Datenschutzskandal Tirol Kliniken“ vom Bundesamt für Korruptionsbekämpfung (BAK) und der Staatsanwaltschaft Innsbruck (da. AZ: *3 St *5*/20z) bearbeitet und die Datenschutzbehörde mit ihrem Amtshilfeersuchen daher an die beiden letzteren verwiesen werde.

10. Mit Verfahrensordnung vom 15. Juni 2021, GZ: 2021-0.415.676, hat die Datenschutzbehörde ein Amtshilfeersuchen an das BAK gerichtet und um Auskunft über den Stand Bezug habender kriminalpolizeilicher Ermittlungen und Übermittlung relevanter Unterlagen ersucht.

11. Mit Schreiben vom 7. Juli 2021, GZ: PAD/20/*4*67**2, hat das BAK das Amtshilfeersuchen der Datenschutzbehörde hinsichtlich einer Auskunftserteilung zu dem laufenden Ermittlungsverfahren abgelehnt und die Datenschutzbehörde wiederum an die Staatsanwaltschaft Innsbruck verwiesen.

12. Mit Verfahrensordnung vom 28. Juli 2021, GZ: 2021-0.484.705, hat die Datenschutzbehörde ein Amtshilfeersuchen an die Staatsanwaltschaft Innsbruck gerichtet und um Übermittlung einer Kopie der Akten des Ermittlungsverfahrens AZ: *3 St *5*/20z, eventuell unter Angabe entsprechender Sperrvermerke betreffend die Akteneinsicht, ersucht.

13. Mit Schreiben vom 25. August 2021, GZ: *3 HSt *4/21t-1, hat die Staatsanwaltschaft Innsbruck das Amtshilfeersuchen mit der Begründung abgelehnt, dass weder dem Beschwerdeführer, noch einer anderen Partei (aus dem parallelen Beschwerdeverfahren Verfahrenszahl DSB-D124.3119) im anhängigen Ermittlungsverfahren Parteistellung zukomme.

14. Mit Verfahrensordnung vom 22. Oktober 2021, GZ: 2021-0.608.978, hat die Datenschutzbehörde beiden Parteien zu den weiteren Ergebnissen des Ermittlungsverfahrens Parteiengehör eingeräumt.

15. Keine der Parteien hat sich innerhalb der gesetzten Frist geäußert.

1 6 . Mit Verfahrensordnung vom 21. Dezember 2021, GZ: 2021-0.899.118, hat die Datenschutzbehörde die

Beschwerdegegnerin unter ausdrücklichem Hinweis auf die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO zu einer nochmaligen genauen Darstellung des Sachverhalts aufgefordert. Mit Verfahrensordnung vom 21. Dezember 2021, GZ: 2021-0.899.118, hat die Datenschutzbehörde die Beschwerdegegnerin unter ausdrücklichem Hinweis auf die Rechenschaftspflicht gemäß Artikel 5, Absatz 2, DSGVO zu einer nochmaligen genauen Darstellung des Sachverhalts aufgefordert.

17. Die Beschwerdegegnerin hat daraufhin am 13. Jänner 2022 folgende schriftliche Stellungnahme abgegeben: Der Securitymanager, Herr Karl-Josef W***, MSc, habe am 4. Oktober 2019, um 11:28 Uhr eine E-Mail als Antwort auf eine Anfrage von AbtInsp Richard U*** von der Landespolizeidirektion Innsbruck an letzteren gesendet. Diese sei ohne Anhang (kein Notfallbericht im E-Mail enthalten) gesendet worden. Inhaltlich habe W*** mitgeteilt, dass der Beschwerdeführer am 9.6.2019 und am 17.9.2019, jeweils wegen Substanzmissbrauch (Kokain, 4-10 Gramm) zur ambulanten Notfallbehandlung im LKI gewesen sei. Er habe dabei jeweils angegeben, dass die Symptome beim bisherigen Konsum von Kokain nicht aufgetreten seien. Weiters habe der Beschwerdeführer gesagt, dass die Quelle des aktuell konsumierten Kokain unbekannt sei. Weiters habe W*** U*** ersucht, für weitere medizinische Informationen „bitte den üblichen Weg (Anfrage per Fax mit Formular)“ zu wählen. Eine andere E-Mail von Herrn W*** mit Anhang des Notfallberichtes sei nicht gefunden worden. Es könne aber nicht ausgeschlossen werden, dass Herr W*** den Notfallbericht über einen anderen Weg (anderer E-Mail-Account, Post) an Dritte übermittelt habe. Erhalten habe Herr W*** den Notfallbericht durch Frau Georgina M***, Leiterin des Beschwerdemanagements, im PDF-Format als Teil einer sogenannten Sammelmappe. Deren Abfrage samt Übermittlung sei im Dokumentationsmanagementsystem der Beschwerdegegnerin auch protokolliert worden. Die Sammelmappe enthalte den Notfallbericht, Arzt-Bericht, Laborbefund, Entlassungsrevers, Konsiliarbefund mit Untersuchung/Therapievorschlag/Übernahme in die Psychiatrie und könne bei Bedarf übermittelt werden, es handle sich jedoch um sehr sensible Gesundheitsdaten des Beschwerdeführers, zu welchen er gegenüber der Beschwerdegegnerin immer auf die Verschwiegenheitsverpflichtung hingewiesen habe. In die Stellungnahme inkludiert waren Wiedergaben der betreffenden E-Mails sowie Auszüge aus dem Dokumentationsmanagementsystem der Beschwerdegegnerin.

18. Mit Verfahrensordnung vom 18. Februar 2022, GZ: 2022-0.030.865, hat die Datenschutzbehörde dem Beschwerdeführer zu diesem weiteren Ergebnis des Ermittlungsverfahrens Parteiengehör eingeräumt.

19. Der Beschwerdeführer hat sich nicht geäußert.

B. Beschwerdegegenstand:

20. Ausgehend vom Vorbringen der Parteien ist Beschwerdegegenstand die Frage, ob die Beschwerdegegnerin den Beschwerdeführer in seinem Recht auf Geheimhaltung verletzt hat, indem sie als datenschutzrechtlich Verantwortliche von ihr verarbeitete Daten (Auszüge aus einer Krankengeschichte, Notfall-Bericht vom 9.6.2019, somit besonders geschützt Daten gemäß Art. 9 DSGVO) an unbefugte Dritte übermittelt hat. Ausgehend vom Vorbringen der Parteien ist Beschwerdegegenstand die Frage, ob die Beschwerdegegnerin den Beschwerdeführer in seinem Recht auf Geheimhaltung verletzt hat, indem sie als datenschutzrechtlich Verantwortliche von ihr verarbeitete Daten (Auszüge aus einer Krankengeschichte, Notfall-Bericht vom 9.6.2019, somit besonders geschützt Daten gemäß Artikel 9, DSGVO) an unbefugte Dritte übermittelt hat.

C. Sachverhaltsfeststellungen:

21. Folgender Sachverhalt steht fest:

22. Die Beschwerdegegnerin ist eine aufgrund gesetzlicher Anordnung (§ 1 Abs. 1 TILAK-Gesetz, LGBl. Nr. 62/2004 idgF) gegründete Gesellschaft mit beschränkter Haftung im wirtschaftlichen Alleineigentum des Landes Tirol, der die Rechtsträgerschaft des A. ö. Landeskrankenhauses (Univ.-Kliniken) Innsbruck zukommt (§ 1 Abs. 2 leg. cit.). Die Beschwerdegegnerin ist eine aufgrund gesetzlicher Anordnung (Paragraph eins, Absatz eins, TILAK-Gesetz, Landesgesetzblatt Nr. 62 aus 2004, idgF) gegründete Gesellschaft mit beschränkter Haftung im wirtschaftlichen Alleineigentum des Landes Tirol, der die Rechtsträgerschaft des A. ö. Landeskrankenhauses (Univ.-Kliniken) Innsbruck zukommt (Paragraph eins, Absatz 2, leg. cit.).

23. Am 3. Oktober 2019 um 16:10 Uhr richtet Abteilungsspektor Richard U***, ein Beamter der Landespolizeidirektion für Tirol, Stadtpolizeikommando Innsbruck, Kriminalreferat, von der E-Mail-Adresse per E-Mail

an Karl-Josef W***, MSc, den Sicherheitsbeauftragten („Securitymanager“) der Beschwerdegegnerin, eine Anfrage mit folgendem Inhalt: ***@polizei.gv.at>

„Hallo Karl-Josef

Die Person heißt Aa***, möglich auch A*** Andreas, geb 2*. *5.199* und soll eigenen Angaben zu Folge vor ca. 2 Monaten wegen Verdacht auf Kokainüberdosis in die Klinik Innsbruck 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

Richard U***, AbtInsp“

24. Karl-Josef W*** wandte sich daraufhin an Georgina M***, die Leiterin des Beschwerdemanagements bei der Beschwerdegegnerin, die über die notwendigen Nutzerrechte verfügte, um Patientendaten im Krankenhausinformationssystem/Dokumentationsmanagementsystem der Beschwerdegegnerin für das Landeskrankenhaus Innsbruck, Universitätsklinik für Innere Medizin, abfragen zu können. Er erhielt von Letzterer noch am 3. Oktober 2019 den Beschwerdeführer betreffende Daten in Form einer elektronischen Sammelmappe (Patienten-ID: *3*4*p*00*32) mit Dokumenten im Format PDF, enthaltend den den Beschwerdeführer betreffenden Notfallbericht, Arzt-Bericht, Laborbefund, Entlassungsrevers und Konsiliarbefund mit Untersuchung/Therapievorschlag/Übernahme in die Psychiatrie.

25. Am 4. Oktober 2019 sendete Karl-Josef W*** um 11:28:17 Uhr eine E-Mail mit folgendem Inhalt an Richard U***:

„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 LKI.

P. 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 Karl-J“

26. Zu einem nicht genau bekannten Zeitpunkt danach übersendete Karl-Josef W*** über einen anderer E-Mail Account oder per Post folgendes Dokument aus der erwähnten „Sammelmappe“ an die LPD:

[Anmerkung Bearbeiter: Dokument Notfall-Bericht betreffend Behandlung des Bf. am 9.6.2019 in der Universitätsklinik Innsbruck, Faksimile, entfernt, da Gesundheitsdaten enthaltend und nicht bzw. nicht mit vertretbarem Aufwand pseudonymisierbar]

27. Beweiswürdigung: Diese Feststellungen stützen sich in der Hauptsache auf die Angaben der Beschwerdegegnerin in der ausführlichen Stellungnahme und Sachverhaltsdarstellung vom 13. Jänner 2022, einliegend als Eingangsstück in GZ: 2022-0.030.865. Diese Stellungnahme enthält Faksimiles der zitierten E-Mails sowie Auszüge aus dem Dokumentationsmanagementsystem der Beschwerdegegnerin, die die Datenabfragen, deren Hintergrund und die dafür verantwortlichen Personen nachvollziehbar darlegen. Die Kopie des den Beschwerdeführer betreffenden Notfall-Berichts vom 9.6.2019 stammt vom Beschwerdeführer selbst (Beilage zur Beschwerde vom 16. September 2020, einliegend als Eingangsstück in GZ: 2020-0.669.690). Das Dokument stammt, wie aus dem gerichtlichen Vermerk der Ordnungsnummer und Aktenseite erkennbar, aus dem Akt *3 Cga 8*3/19f des Landesgerichts Innsbruck, in welcher Sache es von der beklagten Partei (Kläger: der Beschwerdeführer) als Beweismittel vorgelegt wurde. Die Feststellung, dass dieses Dokument (ohne entsprechend dokumentierte Anforderung) an die Landespolizeidirektion übermittelt wurde, beruht auf einer plausiblen, von der Beschwerdegegnerin selbst ausgesprochenen Vermutung (Stellungnahme vom 13. Jänner 2022, Seite 2). Erhärtet wird diese durch die aus den E-Mails klar hervorgehende professionelle Bekanntschaft zwischen Karl-Josef W*** und Richard U***, 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 Beschwerdegegnerin heraus ist daher plausibler als die vom Beschwerdeführer ausgesprochene Vermutung, das Dokument könnte direkt

an Rechtsanwalt Dr. V***, den Vertreter der beklagten Partei in der Sache *3 Cga 8*3/19f, übermittelt worden sein.

D. In rechtlicher Hinsicht folgt daraus

D.1. Summe:

2 8 . Die Beschwerde hat sich als berechtigt erwiesen, 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 und damit ohne ausreichende Rechtsgrundlage in das Geheimhaltungsrecht des Beschwerdeführers eingegriffen worden ist. Die Beschwerde hat sich als berechtigt erwiesen, da zwingende Bedingungen der Rechtmäßigkeit der Übermittlung von Gesundheitsdaten gemäß Artikel 5, Absatz eins, Artikel 9, Absatz 2, DSGVO und Paragraph 15, Absatz eins, Tir KAG nicht eingehalten und damit ohne ausreichende Rechtsgrundlage in das Geheimhaltungsrecht des Beschwerdeführers eingegriffen worden ist.

D.2. Anwendung der DSGVO:

2 9 . Nach § 1 Abs. 1 DSG hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Die DSGVO und insbesondere auch die darin verankerten Grundsätze sind bei der Auslegung des Rechts auf Geheimhaltung zu berücksichtigen (vgl. DSB 31.10.2018, GZ: DSB-D123.076/0003-DSB/2018, RIS). Nach Paragraph eins, Absatz eins, DSG hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Die DSGVO und insbesondere auch die darin verankerten Grundsätze sind bei der Auslegung des Rechts auf Geheimhaltung zu berücksichtigen (vergleiche DSB 31.10.2018, GZ: DSB-D123.076/0003-DSB/2018, RIS).

3 0 . Die Beschwerdegegnerin ist eine in der Rechtsform einer Gesellschaft mit beschränkter Haftung eingerichtete Trägerorganisation für öffentliche Krankenanstalten. Die unter ihrer datenschutzrechtlichen Verantwortung gemäß § 15 und § 63a Tir KAG verarbeiteten Gesundheitsdaten von Patienten unterliegen deren Verarbeitungszweck entsprechend, der nicht unter die im 3. Hauptstück des DSG geregelten Verarbeitungszwecke fällt (siehe § 36 Abs. 1 DSG), den Regeln der DSGVO. Dies gilt auch für die Frage der Rechtmäßigkeit einer Übermittlung solcher Daten. Die Beschwerdegegnerin ist eine in der Rechtsform einer Gesellschaft mit beschränkter Haftung eingerichtete Trägerorganisation für öffentliche Krankenanstalten. Die unter ihrer datenschutzrechtlichen Verantwortung gemäß Paragraph 15 und Paragraph 63 a, Tir KAG verarbeiteten Gesundheitsdaten von Patienten unterliegen deren Verarbeitungszweck entsprechend, der nicht unter die im 3. Hauptstück des DSG geregelten Verarbeitungszwecke fällt (siehe Paragraph 36, Absatz eins, DSG), den Regeln der DSGVO. Dies gilt auch für die Frage der Rechtmäßigkeit einer Übermittlung solcher Daten.

3 1 . Die Verarbeitung der Gesundheitsdaten des Beschwerdeführers durch die Beschwerdegegnerin war für den Zweck seiner Behandlung („Versorgung oder Behandlung im Gesundheits- oder Sozialbereich“) und der gesetzmäßigen medizinischen Dokumentation („Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich“) auf Grundlage von § 1 Abs. 2 DSG und Art. 9 Abs. 1 lit. h [Anmerkung Bearbeiter/in: offenkundiges Redaktionsversehen, gemeint ist Art. 9 Abs. 2 lit. h] und Abs. 3 DSGVO iVm § 15 Abs. 1 lit. b und Abs. 5 sowie § 63a Tir KAG zulässig. Die Verarbeitung der Gesundheitsdaten des Beschwerdeführers durch die Beschwerdegegnerin war für den Zweck seiner Behandlung („Versorgung oder Behandlung im Gesundheits- oder Sozialbereich“) und der gesetzmäßigen medizinischen Dokumentation („Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich“) auf Grundlage von Paragraph eins, Absatz 2, DSG und Artikel 9, Absatz eins, Litera h, [Anmerkung Bearbeiter/in: offenkundiges Redaktionsversehen, gemeint ist Artikel 9, Absatz 2, lit. h] und Absatz 3, DSGVO in Verbindung mit Paragraph 15, Absatz eins, Litera b und Absatz 5, sowie Paragraph 63 a, Tir KAG zulässig.

D.3. Verantwortlichkeit der Beschwerdegegnerin:

3 2 . Es ist die Frage zu prüfen, ob durch das Handeln von Karl-Josef W*** nicht Grenzen der Verantwortlichkeit der Beschwerdegegnerin überschritten worden sind, weil sie sich dessen - unbestritten regelwidriges - Verhalten nicht mehr zurechnen lassen muss. Eine solche Durchbrechung der Grenzen der Verantwortlichkeit liegt dann vor, wenn ein Mitarbeiter eines datenschutzrechtlich Verantwortlichen personenbezogene Daten für eigene Zwecke entfremdet, etwa um die Daten wirtschaftlich zu verwerten, seine persönliche Neugier zu befriedigen oder etwas zum Tratsch im eigenen Bekanntenkreis beizutragen (Übermittlung durch Zweckänderung, vgl. auch Art. 6 Abs. 4 DSGVO). Die Beschwerdegegnerin würde in diesem Fall nur für die Entfremdung, nicht jedoch für die eigentliche Übermittlung

haften. Es ist die Frage zu prüfen, ob durch das Handeln von Karl-Josef W*** nicht Grenzen der Verantwortlichkeit der Beschwerdegegnerin überschritten worden sind, weil sie sich dessen - unbestritten regelwidriges - Verhalten nicht mehr zurechnen lassen muss. Eine solche Durchbrechung der Grenzen der Verantwortlichkeit liegt dann vor, wenn ein Mitarbeiter eines datenschutzrechtlich Verantwortlichen personenbezogene Daten für eigene Zwecke entfremdet, etwa um die Daten wirtschaftlich zu verwerten, seine persönliche Neugier zu befriedigen oder etwas zum Tratsch im eigenen Bekanntenkreis beizutragen (Übermittlung durch Zweckänderung, vergleiche auch Artikel 6, Absatz 4, DSGVO). Die Beschwerdegegnerin würde in diesem Fall nur für die Entfremdung, nicht jedoch für die eigentliche Übermittlung haften.

33. Aus dem Sachverhalt ist jedoch nicht ableitbar, dass Karl-Josef W*** unmittelbar vor oder bei der gegenständlichen Datenübermittlung eigene Zwecke verfolgt hätte und nicht der Meinung gewesen wäre, im Interesse der Beschwerdegegnerin und ihm Rahmen seiner dienstlichen Aufgaben zu handeln. Daher muss sich die Beschwerdegegnerin sein Verhalten in vollem Umfang bis zu jenem Punkt zurechnen lassen, an dem die Daten des Beschwerdeführers in den Verantwortungsbereich der LPD gelangt sind.

D.4. Rechtmäßigkeit der Übermittlung:

34. Zu prüfen ist nun, ob es einen gesetzmäßigen Grund gegeben hat, Gesundheitsdaten des Beschwerdeführers für andere Zwecke zu verarbeiten, hier an einen Beamten der regionalen Sicherheits- und Kriminalpolizeibehörde (LPD) zu übermitteln.

35. Es sind [...] aus der Richtlinie 2016/680 keinespezifischen Verfahrensregeln, die die Rechtmäßigkeit des Zugangs zu [...] gespeicherten Daten gewährleisten, abzuleiten, sondern es gelten die nationalen Rechtsvorschriften zur Regelung von Durchsuchungen und Sicherstellungen im Rahmen strafrechtlicher Ermittlungen (Schlussanträge des Generalanwalts Manuel Campos Sanchez-Bordona vom 20. April 2023 in der Rechtssache C-548/21, Rz. 86, Unterstreichungen nicht im Original).

36. Das Gesetz erlaubt solche Übermittlungen bei Gesundheitsdaten jedoch nur ausnahmsweise. Gemäß Art. 9 Abs. 1 DSGVO besteht ein grundsätzliches Verbot, besonders geschützte Daten zu verarbeiten. Daraus folgt, dass ihre Verarbeitung nur dann zulässig ist, wenn alle gesetzlichen Bedingungen dafür erfüllt werden. Das Gesetz erlaubt solche Übermittlungen bei Gesundheitsdaten jedoch nur ausnahmsweise. Gemäß Artikel 9, Absatz eins, DSGVO besteht ein grundsätzliches Verbot, besonders geschützte Daten zu verarbeiten. Daraus folgt, dass ihre Verarbeitung nur dann zulässig ist, wenn alle gesetzlichen Bedingungen dafür erfüllt werden.

37. Gemäß § 39 DSG durfte die LPD Gesundheitsdaten des Beschwerdeführers nur verarbeiten, demnachermitteln und speichern, wenn die „Verarbeitung unbedingt erforderlich“ war und „wirksame Maßnahmen zum Schutz der Rechte und Freiheiten“ des Beschwerdeführers getroffen waren. Gemäß Paragraph 39, DSG durfte die LPD Gesundheitsdaten des Beschwerdeführers nur verarbeiten, demnach ermitteln und speichern, wenn die „Verarbeitung unbedingt erforderlich“ war und „wirksame Maßnahmen zum Schutz der Rechte und Freiheiten“ des Beschwerdeführers getroffen waren.

38. Aus dem Blickwinkel der Beschwerdegegnerin folgt daraus, dass die Beschwerdegegnerin selbst verpflichtet war zu überprüfen, ob bei dieser Verarbeitung die Grundsätze gemäß Art. 5 Abs. 1 lit. a) bis c) DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz; Zweckbindung und Datenminimierung), die Bedingung des Art. 9 Abs. 2 lit. g) DSGVO und die Bestimmungen des § 15 Abs. 1 lit. e) Tir KAG eingehalten werden. Aus dem Blickwinkel der Beschwerdegegnerin folgt daraus, dass die Beschwerdegegnerin selbst verpflichtet war zu überprüfen, ob bei dieser Verarbeitung die Grundsätze gemäß Artikel 5, Absatz eins, Litera a,) bis c) DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz; Zweckbindung und Datenminimierung), die Bedingung des Artikel 9, Absatz 2, Litera g, DSGVO und die Bestimmungen des Paragraph 15, Absatz eins, Litera e, Tir KAG eingehalten werden.

39. Der EuGH hat in seiner Rechtsprechung mehrfach festgehalten, dass bei jeder Verarbeitung personenbezogener Daten, vorbehaltlich der nach Art. 23 DSGVO zulässigen Ausnahmen, die in Kapitel II der DSGVO aufgestellten Grundsätze für die Verarbeitung personenbezogener Daten sowie die in ihrem Kapitel III geregelten Rechte der betroffenen Person beachtet werden müssen. Insbesondere muss jede Verarbeitung personenbezogener Daten zum einen mit den in Art. 5 DSGVO aufgestellten Grundsätzen im Einklang stehen und zum anderen die in Art. 6 DSGVO aufgezählten Rechtmäßigkeitsvoraussetzungen erfüllen (vgl. in diesem Sinne EuGH 2.3.2023, C-268/21, Rn 43, unter Hinweis auf EuGH 6.10.2020, C-511/18, C-512/18 und C-520/18, ECLI: EU:C:2020:791, Rn. 208 und die dort angeführte

Rechtsprechung). An die Stelle des Art. 6 tritt bei der Verarbeitung von Gesundheitsdaten der Art. 9 DSGVO. Der EuGH hat in seiner Rechtsprechung mehrfach festgehalten, dass bei jeder Verarbeitung personenbezogener Daten, vorbehaltlich der nach Artikel 23, DSGVO zulässigen Ausnahmen, die in Kapitel römisch zwei der DSGVO aufgestellten Grundsätze für die Verarbeitung personenbezogener Daten sowie die in ihrem Kapitel römisch drei geregelten Rechte der betroffenen Person beachtet werden müssen. Insbesondere muss jede Verarbeitung personenbezogener Daten zum einen mit den in Artikel 5, DSGVO aufgestellten Grundsätzen im Einklang stehen und zum anderen die in Artikel 6, DSGVO aufgezählten Rechtmäßigkeitsvoraussetzungen erfüllen vergleiche in diesem Sinne EuGH 2.3.2023, C-268/21, Rn 43, unter Hinweis auf EuGH 6.10.2020, C-511/18, C-512/18 und C-520/18, ECLI: EU:C:2020:791, Rn. 208 und die dort angeführte Rechtsprechung). An die Stelle des Artikel 6, tritt bei der Verarbeitung von Gesundheitsdaten der Artikel 9, DSGVO.

40. Eine derartige Übermittlung hätte daher ein begründetes Ersuchen der LPD vorausgesetzt, was den beteiligten Personen offenkundig auch bewusst war. Die festgestellten Tatsachen lassen nicht einmal einen klaren Schluss hinsichtlich der Frage zu, ob der Vertreter der LPD gegenüber dem Mitarbeiter der Beschwerdegegnerin offengelegt hat, gegen wen und in welcher Sache ermittelt wurde, ob etwa der betroffene Patient selbst einer Straftat verdächtigt wurde, oder ob seine Daten zu dem Zweck benötigt wurden, ein Ermittlungsverfahren gegen (unbekannte) Dritte einzuleiten oder voranzutreiben.

41. Gemäß § 15 Abs. 1 lit. e Tir KAG wäre die Beschwerdegegnerin jedenfalls verpflichtet gewesen, sich zu vergewissern, Gemäß Paragraph 15, Absatz eins, Litera e, Tir KAG wäre die Beschwerdegegnerin jedenfalls verpflichtet gewesen, sich zu vergewissern,

a. in welcher Sache („Angelegenheit“) die LPD Auskunft verlangt und

b. für welche „Entscheidung oder Verfügung im öffentlichen Interesse“ die LPD die Daten benötigt. Gemäß Art. 9 Abs. 2 lit. g DSGVO muss es sich überdies um ein erhebliches öffentliches Interesse handeln. für welche „Entscheidung oder Verfügung im öffentlichen Interesse“ die LPD die Daten benötigt. Gemäß Artikel 9, Absatz 2, Litera g, DSGVO muss es sich überdies um ein erhebliches öffentliches Interesse handeln.

42. Ein solches Ersuchen hätte nach Eingang bei der Beschwerdegegnerin 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 nicht in jenem Umfang geschehen, den die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO geboten hätte. Ein solches Ersuchen hätte nach Eingang bei der Beschwerdegegnerin 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 Artikel 32, DSGVO zu beachten ist) hätte dokumentiert werden müssen. Dies ist nicht in jenem Umfang geschehen, den die Rechenschaftspflicht gemäß Artikel 5, Absatz 2, DSGVO geboten hätte.

43. Es ist daher festzuhalten, dass die Beschwerdegegnerin gegen die Grundsätze der Rechtmäßigkeit (Art. 5 Abs. 1 lit. a 1. Fall DSGVO) und Transparenz (Art. 5 Abs. 1 lit. a 3. Fall DSGVO) bei der Verarbeitung personenbezogener Daten verstoßen hat. Es ist daher festzuhalten, dass die Beschwerdegegnerin gegen die Grundsätze der Rechtmäßigkeit (Artikel 5, Absatz eins, Litera a, 1. Fall DSGVO) und Transparenz (Artikel 5, Absatz eins, Litera a, 3. Fall DSGVO) bei der Verarbeitung personenbezogener Daten verstoßen hat.

44. Daraus folgt wiederum, dass die Datenübermittlungen an die LPD, jedenfalls in der Form und unter den Umständen, die hier vorlagen, nicht rechtmäßig waren. Es handelt sich hierbei um keine bloße Verletzung von Formalitäten, sondern um einen Verstoß gegen materielles Datenschutzrecht. Einerseits legt die Unionsgesetzgebung in Art. 5 Abs. 1 lit. a DSGVO klar fest, dass dem Beschwerdeführer ein (in Art. 15 Abs. 1 lit. c DSGVO konkretisiertes) Recht auf die Nachvollziehbarkeit von Übermittlungsvorgängen zukommt. Andererseits verlangt Art. 9 Abs. 2 lit. g DSGVO als denkmögliche Grundlage für die hier erfolgte Übermittlung besonders geschützter Daten ausdrücklich, dass eine solche Verarbeitung „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht“ (vgl. dazu auf der Seite der Datenempfängerin LPD auch § 39 DSG, welche Bestimmung „wirksame Maßnahmen zum Schutz der Rechte und Freiheiten“ der betroffenen Person verlangt). Zu solchen Maßnahmen ist auch die Einhaltung entsprechender Formalitäten zu zählen, die den beteiligten Personen u.a.

die Bedeutung und den Ausnahmecharakter des Vorgangs vor Augen führen sollen. Beide Bedingungen für die Rechtmäßigkeit der Verarbeitung sind hier nicht eingehalten worden. Daraus folgt wiederum, dass die Datenübermittlungen an die LPD, jedenfalls in der Form und unter den Umständen, die hier vorlagen, nicht rechtmäßig waren. Es handelt sich hierbei um keine bloße Verletzung von Formalitäten, sondern um einen Verstoß gegen materielles Datenschutzrecht. Einerseits legt die Unionsgesetzgebung in Artikel 5, Absatz eins, Litera a, DSGVO klar fest, dass dem Beschwerdeführer ein (in Artikel 15, Absatz eins, Litera c, DSGVO konkretisiertes) Recht auf die Nachvollziehbarkeit von Übermittlungsvorgängen zukommt. Andererseits verlangt Artikel 9, Absatz 2, Litera g, DSGVO als denkmögliche Grundlage für die hier erfolgte Übermittlung besonders geschützter Daten ausdrücklich, dass eine solche Verarbeitung „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht“ vergleiche dazu auf der Seite der Datenempfängerin LPD auch Paragraph 39, DSG, welche Bestimmung „wirksame Maßnahmen zum Schutz der Rechte und Freiheiten“ der betroffenen Person verlangt). Zu solchen Maßnahmen ist auch die Einhaltung entsprechender Formalitäten zu zählen, die den beteiligten Personen u.a. die Bedeutung und den Ausnahmecharakter des Vorgangs vor Augen führen sollen. Beide Bedingungen für die Rechtmäßigkeit der Verarbeitung sind hier nicht eingehalten worden.

D.6. Schlussfolgerungen:

4 5 . Durch die oben festgestellten Verstöße gegen Bestimmungen des Kapitels II der DSGVO hat die Beschwerdegegnerin ungerechtfertigt in das Grundrecht auf Geheimhaltung personenbezogener Daten des Beschwerdeführers eingegriffen. Durch die oben festgestellten Verstöße gegen Bestimmungen des Kapitels römisch zwei der DSGVO hat die Beschwerdegegnerin ungerechtfertigt in das Grundrecht auf Geheimhaltung personenbezogener Daten des Beschwerdeführers eingegriffen.

4 6 . Es waren daher gemäß § 24 Abs. 2 Z 4 und Abs. 5 Satz 2 DSG die spruchgemäßen Feststellungen zu treffen. Es waren daher gemäß Paragraph 24, Absatz 2, Ziffer 4 und Absatz 5, Satz 2

Quelle: Datenschutzbehörde Dsb, <https://www.dsb.gv.at>

© 2026 JUSLINE

JUSLINE® ist eine Marke der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH.

www.jusline.at