Republik Österreich
Datenschutz behörde

Barichgasse 40-42
A-1030 Wien
Tel.: +43-1-52152

E-Mail: dsb@dsb.gv.at

GZ: ***

[Adressierung entfernt]

Datenschutzbeschwerde (Recht auf Geheimhaltung)
A/GIS Gebühren Info Service GmbH

B E S C H E I D

S P R U C H

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von A (beschwerdeführende Partei) vom 28.01.2023 gegen die GIS Gebühren Info Service GmbH (Beschwerdegegnerin) wegen Verletzung im Recht auf Geheimhaltung wie folgt:

- Der Beschwerde wird Folge gegeben und es wird festgestellt, dass die Beschwerdegegnerin die beschwerdeführende Partei im Recht auf Geheimhaltung verletzt hat, indem die Beschwerdegegnerin es mangels geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO („Sicherheit der Verarbeitung“) ermöglicht hat, dass personenbezogene Daten der beschwerdeführenden Partei (jedenfalls Vor- und Nachname, Geburtsdatum und postalische Anschrift) zumindest einer dritten Person (Hacker) unrechtmäßig zugänglich wurden.

Rechtsgrundlagen: Art. 4, Art. 5 Abs. 1 lit. a und lit. f, Art. 6 Abs. 1, Art. 28, Art. 32, Art. 34, Art. 51 Abs. 1, Art. 57 Abs. 1 lit. f, Art. 58 Abs. 2 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, Abs. 2 Z 5 und Abs. 5 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999; § 17 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 (AVG), BGBl. Nr. 51/1991 idgF.

B E G R Ü N D U N G

A. Vorbringen der Parteien und Verfahrensgang

A.1. Mit Eingabe vom 28.01.2023 behauptete die beschwerdeführende Partei (in Folge: bP) eine Verletzung im Recht auf Geheimhaltung. Zusammengefasst wurde vorgebracht, dass die Beschwerdegegnerin (in Folge: BG) durch eine Lücke dazu beigetragen habe, dass ihre persönlichen Meldedaten weitergegeben worden seien.

A.2. Aufgrund der Vielzahl der gegen die BG gerichteten Datenschutzbeschwerden, denen derselbe Sachverhalt zugrunde liegt, wurde ein Hauptverfahren zur GZ: 123*** geführt. Im Hauptverfahren wurden alle wesentlichen Ermittlungsschritte gesetzt. Die Ermittlungsergebnisse werden in allen gegen die BG gerichteten Verfahren herangezogen. Hintergrund dieser Vorgehensweise ist eine effiziente Abarbeitung der anhängigen „GIS-Datenschutzbeschwerden“, zumal es nicht zweckmäßig war, dieselben Ermittlungsschritte mehrfach zu wiederholen.

A.3. Die BG brachte im genannten Hauptverfahren zur GZ: 123*** am 14. März 2023 eine Stellungnahme ein. Darin führte die BG zusammengefasst aus, dass die BG keinen Zugriff auf den beim Täter sichergestellten Datenbestand habe. Die BG stehe mit der Staatsanwaltschaft in Abklärung des Erhalts der beim Täter sichergestellten Daten. Der Datensicherheitsvorfall im Jahre 2020 habe einen Datenbestand aus dem Jahr 2019 betroffen. Weiters setze eine individuelle Benachrichtigung (gemeint offenbar: über den gegenständlichen Vorfall) die Kenntnis voraus, dass die zu benachrichtigende Person tatsächlich betroffen gewesen sei. Die BG habe gegenüber der APA aber im Mai 2020 eine schriftliche Stellungnahme erstattet, die in den Medien breiten Widerhall gefunden habe. Es sei auf den Link https://xyz.at/ hinzuweisen. Die Umstände seien auch auf der Website der BG veröffentlicht worden. Seither seien polizeiliche Ermittlungen hinsichtlich des unbekannten Täters im Gange, welcher für den Datendiebstahl verantwortlich sei.

A.4. Im Rahmen des Hauptverfahren zur GZ: 123*** wurde am 25. Mai 2023 eine mündliche Einvernahme der BG in den Räumlichkeiten der Datenschutzbehörde durchgeführt. Gegenstand der Einvernahme war ein Vorfall, der sich im Mai 2020 ereignet hat. Im Rahmen dieses Vorfalls wurden u.a. Meldedaten von Personen mit Unterkunft in Österreich im Internet zum Verkauf angeboten. Die Datenschutzbehörde teilte der BG mit, dass die gegenständliche Niederschrift in allen Datenschutzbeschwerden, die mit dem gegenständlichen Vorfall von Mai 2020 im Zusammenhang stehen, für die Feststellung des Sachverhalts herangezogen wird. Eine geschwärzte Version der Niederschrift der Einvernahme befindet sich u.a. auch im gegenständlichen Akt zur GZ: D124***.

A.5. Zwischenzeitig stellte die Datenschutzbehörde im Rahmen des Hauptverfahrens zur GZ: 123*** mehrere Amtshilfeersuchen an öffentliche Stellen, um den Sachverhalt möglichst rasch aufzuklären. Als Resultat eines dieser Amtshilfeersuchen wurde ein Datenbestand in der Form, wie er seitens einer öffentlichen Stelle sichergestellt wurde, über einen gesicherten Kanal an die Datenschutzbehörde übermittelt. Der Datenbestand wurde laut der öffentlichen Stelle zum damaligen Zeitpunkt unter dem Titel „Austria gis.at [8.9M] television and radio licensing company“ im Internet zum Verkauf angeboten.

A.6. Darüber hinaus teilte das ***-Amt im Hauptverfahren zur GZ: 123*** – als Folge eines Amtshilfeersuchens der Datenschutzbehörde – mit, dass der Datenbestand im Zeitraum 24. Mai 2023 [Hinweis der Datenschutzbehörde: Hierbei handelt es sich um einen Tippfehler und es handelt sich richtigerweise um das Datum 24. Mai 2020] bis 25. Mai 2020 angekauft und vom Verdächtigen (gemeint: jener Hacker, der die Daten kompromittiert hat) übermittelt worden sei. In Folge sei das Angebot des Verdächtigen offline genommen worden. Am 25. Jänner 2021 sei erneut ein Datenbestand

mit dem Titel „Austria gis.at [8.9M] television and radio licensing company“ im Internet angeboten worden. Kurz darauf sei das Angebot wieder verschwunden. Am 25. Jänner 2022 sei wiederum dasselbe Angebot zum Verkauf angeboten und spätestens am 11. Februar 2022 offline genommen worden. Auf Rückfrage der Datenschutzbehörde teilte das ***-Amt mit, dass es sich bei diesen Informationen um „open source“ Informationen handle. Jedermann habe diese öffentlichen Angebote – zumindest zum damaligen Zeitpunkt – wahrnehmen können.

A.7. In weiterer Folge hat die Datenschutzbehörde in allen Beschwerdeverfahren, die mit dem gegenständlichen Vorfall von Mai 2020 im Zusammenhang stehen, einen Abgleich der Daten der jeweiligen bP anhand des Datenbestands durchgeführt. Der Abgleich erfolgte immer im Vieraugenprinzip von (entsprechend geschulten) Bediensteten der Datenschutzbehörde. Auch für die bP des gegenständlichen Verfahrens zur GZ: D124*** wurde ein Abgleich durchgeführt. Die Recherche ergab, dass die bP des gegenständlichen Verfahrens im Datenbestand aufscheint (Treffer).

A.8. Die BG brachte im Hauptverfahren zur GZ: 123*** am 8. August 2023 eine Stellungnahme ein. Darin führte die BG zusammengefasst aus, dass der Hacker zwischenzeitig in den Niederlanden strafgerichtlich verurteilt worden sei. Das Strafurteil enthalte keinen Hinweis darauf, dass die erbeuteten Daten tatsächlich von der BG gekommen seien. Die Daten der bP könnten auch aus einem anderen erbeuteten Datenbestand stammen. Die Handlung, durch welches ein Geheimhaltungsinteresse verletzt worden sei, habe nicht die BG, sondern der Hacker gesetzt. Eine Verletzung des Rechts auf Geheimhaltung sei der BG nicht zuzurechnen. Die BG habe die gebotenen technischen und organisatorischen Maßnahmen eingehalten.

A.9. Im Rahmen des Hauptverfahrens zur GZ: 123*** wurde am 25. August 2023 eine mündliche Einvernahme des IT-Dienstleisters der BG in den Räumlichkeiten der Datenschutzbehörde durchgeführt. Eine geschwärzte Version der Niederschrift der Einvernahme befindet sich u.a. auch im gegenständlichen Akt zur GZ: D124***.

A.10. Die Datenschutzbehörde hat der BG im Rahmen des Hauptverfahrens zur GZ: 123*** Gelegenheit gegeben, allfällige Schwärzungen der Niederschriften anzuregen. Die Anregungen wurden allerdings nicht übernommen, da die für eine Schwärzung vorgeschlagenen Stellen aus Sicht der Datenschutzbehörde für den Sachverhalt maßgeblich sind. Die Datenschutzbehörde hat jedoch Schwärzungen durchgeführt, soweit Teile der Niederschriften entweder nicht für den Beschwerdegegenstand relevant sind oder die Teile ermittlungstaktische Maßnahmen öffentlicher Stellen betreffen.

A.11. Die Datenschutzbehörde räumte der bP zu diesen Ermittlungsergebnissen – auch zu jenen, die bis dahin nur im Hauptverfahren zur GZ: 123*** vorhanden waren – Parteiengehör ein. Die Niederschriften wurden gemäß § 17 Abs. 3 AVG in geschwärzter Fassung übermittelt.

A.12. Die bP gab trotz eingeräumter Möglichkeit in Form von Parteiengehör keine Stellungnahme mehr ab. Es sind keine Anhaltspunkte für eine fehlerhafte Zustellung vorhanden.

B. Beschwerdegegenstand

B.1. Für Parteieingaben ist nicht bloß der Wortlaut der Beschwerde, sondern auch der Wille der Partei beachtlich. Das Vorliegen von Voraussetzungen ist nicht streng formal zu interpretieren, sofern der Gegenstand des Verfahrens – wenn auch nach Auslegung des Vorbringens iSd §§ 6 u. 7 ABGB – zweifelsfrei, also ohne Möglichkeit einer Verwechslung zu erkennen ist (VwSlg. 18968 A/2014). Für die Beurteilung eines Anbringens kommt es nicht auf Bezeichnungen und zufällige Verbalformen an, sondern auf den Inhalt des Anbringens, also das erkennbare oder zu erschließende Ziel eines Parteischrittes (vgl. das Erkenntnis des VwGH vom 27. November 1998, Zl. 95/21/0912).

Dem Wortlaut von Art. 77 Abs. 1 DSGVO iVm § 24 Abs. 2 Z 1 DSG kann nicht entnommen werden, dass die bP ganz konkrete Normen oder gar Anspruchsketten anführen muss. Ziel dieser Bestimmung ist es – im Gegenteil – einer betroffenen Person einen einfachen und unentgeltlichen Rechtsschutzweg zu gewährleisten, was sich u.a. aus Art. 57 Abs. 2 und Abs. 3 DSGVO ergibt.

Zudem ist die Datenschutzbehörde nicht an die wörtliche Formulierung gestellter Anträge gebunden, sondern hat vielmehr amtswegig zu prüfen, ob eine Verletzung im geltend gemachten Recht – hier: Geheimhaltung – vorliegt oder nicht. Das geltend gemachte Recht stellt somit die äußerste Grenze der Prüfbefugnis der Datenschutzbehörde in einem antragsgebundenen Beschwerdeverfahren dar. Daher ist es der Datenschutzbehörde auch möglich, die Anträge entsprechend umzuformulieren.

Für den gegenständlichen Fall bedeuten diese Überlegungen Folgendes:

B.2. Die bP verfolgt mit ihren Eingaben das erkennbare Ziel, gegen die Offenlegung ihrer Daten durch die BG an einen Dritten vorzugehen. Es ist erkennbar, dass diese Offenlegung nach Ansicht der bP nicht zulässig war und die Verantwortung hierfür die BG trägt. Die bP hat zudem einen Feststellungsantrag gestellt, indem sie beim elektronischen Beschwerdeformular der Datenschutzbehörde das entsprechende Feld angekreuzt hat. Somit ergibt sich als Beschwerdegegenstand die Frage, ob die BG die bP im Recht auf Geheimhaltung gemäß § 1 Abs. 1 DSG verletzt hat, da es die BG – mangels geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO („Sicherheit der Verarbeitung“) – ermöglicht hat, dass personenbezogene Daten der bP (jedenfalls Vor- und Nachname, Geburtsdatum und postalische Anschrift) zumindest einer dritten Person (Hacker) unrechtmäßig zugänglich wurden.

C. Sachverhaltsfeststellungen

C.1. Die BG ist mit der der Einbringung und Abrechnung der Rundfunkgebühr in Österreich beauftragt und vollzieht das Rundfunkgebührengesetz. Zur Wahrnehmung dieser Aufgabe erhält sie Meldedaten aus lokalen Melderegistern von den jeweiligen lokalen Meldebehörden. Hierzu gehören in der Regel

zumindest der Vor- und Nachname, das Geburtsdatum und die postalische Anschrift von in Österreich gemeldeten Personen.

In der Vergangenheit wurde ein sog. Customer-Relationship-Management-Systems (CRM-Systems) eingeführt. Für die Einführung des CRM-Systems wurde ein IT-Unternehmen herangezogen. Konkret wurde das IT-Unternehmen mit der Systemgestaltungsentwicklung und -implementierung beauftragt. Die BG hatte das Ziel, eine Normierung der Datenbestände (Meldedaten) zu erreichen, da diese aus unterschiedlichen Quellen stammten und daher eine unterschiedliche Struktur aufwiesen.

*Beweiswürdigung zu C.1.: Die getroffenen Feststellungen zur grundsätzlichen Tätigkeit der BG sind allgemein bekannt und unstrittig. Der Umstand, dass die BG Meldedaten aus lokalen Melderegistern von den jeweiligen lokalen Meldebehörden erhält und dass es sich hierbei regelmäßig um Vor- und Nachname, Geburtsdatum und postalische Anschrift handelt, sowie die Feststellungen zur Heranziehung des IT-Unternehmens, beruhen auf der Aussage der BG im Rahmen der mündlichen Einvernahme vom 25. Mai 2023 im Hauptverfahren zur GZ: 123***, S. 3 und S. 5(Hinweis: In der genannten Niederschrift wird das IT-Unternehmen als „Subunternehmen" bezeichnet).*

C.2. Bei einem Teilschritt des genannten Projekts (Einführung eines CRM-Systems) kam es zu folgendem Vorfall:

Das IT-Unternehmen hat die seitens der BG zur Verfügung gestellten Daten – im Wesentlichen Meldedaten – auf eine Testumgebung geladen. Auf diese Testumgebungen haben Mitarbeiter der BG und des IT-Unternehmens zugegriffen (Remote Access). Grundlage für die Testumgebung war der sog. *** [Hinweis der Datenschutzbehörde: Technische Details wurden entfernt].

Das IT-Unternehmen hat in der Folge im Rahmen von Entwicklungs- bzw. Testtätigkeiten eine Re-Konfiguration am Server der Testumgebung vorgenommen und einen Zugangs-Port zum Server geöffnet und offengelassen. Ein Remote Access ermöglicht es einem Nutzer, von der Ferne auf Netzwerkressourcen (im gegenständlichen Fall die Testumgebung) zuzugreifen, als wäre der Nutzer direkt an einem Rechner angemeldet, der mit diesem Netzwerk verbunden ist.

Einer dritten Person (Hacker) gelang es im Mai 2020, durch eine gezielte Suche die Ziel-IP-Adresse und den Ziel-Port des Servers der Testumgebung, konkret: der verfahrensgegenständlichen ***-Datenbank, herauszufinden. Danach gelang es der dritten Person (Hacker), über die offene Netzwerk-Schnittstelle auf die Datenbank zuzugreifen und den Datenbank-Bestand zu exfiltrieren. Durch die offene Netzwerk-Schnittstelle war es für den Zugriff auf die ***-Datenbank nicht mehr notwendig, sich mittels Remote Access mit dem Server der Testumgebung zu verbinden. Andere Vorkehrungen bzw. Sicherheitsmechanismen, um unautorisierten Zugriff auf die ***-Datenbank zu verhindern (wie etwa eine zusätzliche Zugangsbeschränkung durch Authentifizierung mittels Nutzername und Passwort), waren bei der Konfiguration nicht getroffen worden.

Die dritte Person (Hacker) hat den exfiltrierten Datenbestand (die Meldedaten, die die BG dem IT-Unternehmen zur Verfügung gestellt hat) in der Folge im Internet im sog. „RaidForums“ zumindest im Mai 2020 zum Verkauf angeboten.

Der genannte Datenbestand wurde von einer öffentlichen Stelle in Österreich zwischen 24. und 25. Mai 2020 angekauft und wurde der Datenbestand nach Datenübermittlung offline genommen. Die Daten im exfiltrierten Datenbestand waren jedenfalls nicht aktueller als zum Zeitpunkt des Jahres 2019.

*Beweiswürdigung zu C.2.: Die getroffenen Feststellungen zur Beauftragung des IT-Unternehmens durch die BG und zum Verkauf der Daten im „RaidForums“ durch einen Hacker ergeben sich aus den Aussagen der BG im Rahmen der mündlichen Einvernahme vom 25. Mai 2023 im Hauptverfahren zur GZ: 123***, S. 5 ff. Die getroffenen Feststellungen zu den Details des IT-Projekts, insbesondere zum offen gelassenen Port und den darauffolgenden Zugriff durch eine dritte Person (Hacker), ergeben sich aus der Stellungnahme des IT-Unternehmens vom 8. September 2020 im Rahmen des amtswegigen Verfahrens zur GZ: D213.1087, 2020-0.457.209, S. 2, S. 4 sowie S. 6. Die BG hat zum damaligen Zeitpunkt Parteiengehör zur Stellungnahme des IT-Unternehmens vom 8. September 2020 erhalten. Das Thema des offen gelassenen Ports wurde auch im Rahmen der mündlichen Einvernahme vom 25. Mai 2023 im Hauptverfahren zur GZ: 123*** mit der BG erörtert. Zur Funktionsweise des *** wurde eine amtswegige Recherche unter *** durchgeführt. Wie sich noch aus der rechtlichen Beurteilung ergibt, spielt das Verschulden für ein datenschutzrechtliches Beschwerdeverfahren keine Rolle (vgl. D.4.), weshalb diesbezügliche Feststellungen nicht erforderlich waren. Die Feststellungen zum Ankauf des Datenbestands ergeben sich aus der Beantwortung des gestellten Amtshilfeersuchens durch die öffentliche Stelle, die den Datenbestand angekauft hat und sind unstrittig.*

C.3. Die Daten der bP waren im Datenbestand, welcher seitens der dritten Person (Hacker) exfiltriert und in Folge zum Verkauf angeboten wurde, vorhanden (Treffer). Konkret waren folgende Daten der bP betroffen (Formatierung nicht 1:1 wiedergegeben):

[Auszug entfernt. Es handelt sich um Meldedaten, d.h. insbesondere Name, Geburtsdatum und Adresse]

Bei diesem Datenbestand handelt es sich um jenen Datenbestand, den die dritte Person (Hacker) vom IT-Unternehmen der BG exfiltriert hat.

Der bP wurde im Rahmen des gegenständlichen Verfahrens seitens der Datenschutzbehörde mitgeteilt, dass ihre Daten in dieser Datenbank vorhanden waren.

*Beweiswürdigung zu C.3.: Der Datenschutzbehörde wurde der exfiltrierte Datenbestand – als Folge eines Amtshilfeersuchens im Hauptverfahren zur GZ: 123*** – seitens des *** übermittelt. Die Datenschutzbehörde hat im Rahmen aller anhängigen Datenschutzbeschwerden eine Recherche in diesem Datenbestand durchgeführt. Im gegenständlichen Fall wurden die Daten der bP mit dem*

Datenbestand abgeglichen, was zu einem Treffer geführt hat. Die Recherche wurde im Vieraugenprinzip von (entsprechend geschulten) Bediensteten der Datenschutzbehörde durchgeführt.

*Die Feststellung, dass es sich bei dem Datenbestand um jenen Datenbestand handelt, den die dritte Person (Hacker) vom IT-Unternehmen der BG exfiltriert hat, ergibt sich zunächst aus der Stellungnahme des ***-Amts im Hauptverfahren zur GZ: 123***. Nach Angaben des ***-Amts wurde der exfiltrierte Datenbestand mehrfach mit dem Titel „*Austria gis.at [8.9M] television and radio licensing company*“ zum Verkauf angeboten. Der enge zeitliche Zusammenhang zwischen Datenexfiltration vom IT-Unternehmen der BG und Verkaufsangebot der Daten durch den Hacker im Internet spricht ebenso dafür, dass es sich hierbei um den Datenbestand der BG handelt. Darüber hinaus handelt es sich bei den betroffenen Datenkategorien um Daten, die typischerweise in Melderegistern vorhanden sind, aus welchen die BG ihre Daten erhält. Umgekehrt sind keine Datenkategorien betroffen, die nicht typischerweise in Melderegistern vorhanden sind. Soweit die BG in ihrer Stellungnahme vom 8. August 2023 im Hauptverfahren zur GZ: 123*** vorbringt, dass das zwischenzeitig gegen den Hacker ergangene Strafurteil keinen Hinweis enthalte, dass die Daten von der BG gekommen seien, ist ihr entgegenzuhalten, dass sich das genannte Strafurteil mit der Datenquelle gar nicht auseinandersetzt. Darüber hinaus setzt sich das Strafurteil mit einer Vielzahl unterschiedlicher Vorwürfen auseinander. Das genannte Strafurteil ist abrufbar unter https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2023:3748. Auch sonst sind keinerlei Anhaltspunkte vorhanden, dass der Hacker die Daten der bP aus einem völlig anderen Datenbestand erhalten hätte. Insgesamt betrachtet ist die Datenschutzbehörde daher davon überzeugt, dass es sich beim zum Verkauf angebotenen Datenbestand um jenen des IT-Unternehmens der BG handelt.*

C.4. Die BG hat daraufhin im Mai 2020 eine allgemeine Benachrichtigung über den Vorfall – konkret in Form von Presseaussendungen – durchgeführt. Eine individuelle Benachrichtigung (also die Benachrichtigung konkreter Person) wurde nicht durchgeführt. Konkret wurde im Mai 2020 der folgende Text veröffentlicht (Formatierung nicht 1:1 wiedergegeben):

*„**Verdacht auf Datendiebstahl bei GIS***

****-Amts und Verfassungsschutz ermitteln*

Wien (APA) - Die ORF-Tochter Gebühren Info Serivce (GIS) könnte von einem Datendiebstahl betroffen sein. Wie die für die Abwicklung der Rundfunkgebühren zuständige Firma der APA sagte, laufen derzeit Ermittlungen der Behörden dazu. Anlass sind dem Vernehmen nach auf einem Darknet-Marktplatz angebotene österreichische Daten, deren Zusammensetzung auf die von der GIS gespeicherten Informationen hinweist.

"Wie heute bekannt wurde, dürfte es zu einem Diebstahl von größeren Mengen an Daten gekommen sein, wobei nicht ausgeschlossen werden kann, dass diese Daten aus dem Einflussbereich der GIS stammen", hieß es in einer schriftlichen Stellungnahme der GIS gegenüber der APA. Geschäftsführer C betont, mit den Behörden zusammenzuarbeiten und die Systeme der GIS für Überprüfungen zur Verfügung gestellt zu haben. "Wie uns unsere Datenschutzexperten versichern, ist es seitens der GIS zu keinerlei Versäumnissen gekommen. Dies wird auch durch die im Februar erneuerte ISO-Zertifizierung der GIS-IT-Systeme untermauert", betonte C.

*"Das ***-Amt geht seit kurzem dem Verdacht eines Datendiebstahls nach", bestätigte Sprecher D auf APA-Anfrage. Geführt werden die Ermittlungen demnach vom Cyber Crime Competence Center (C4) des ***-Amts mit Unterstützung des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT). Man arbeite eng mit der GIS zusammen.*

Wie viele Personen von dem möglichen Datendiebstahl betroffen sind und um welche Daten es sich genau handelt, war vorerst nicht zu erfahren. Anlass für die Ermittlungen war dem Vernehmen nach, dass auf einem Darknet-Marktplatz Daten angeboten wurden, deren Zusammensetzung auf die (teils aus dem Zentralen Melderegister abgefragten, Anm.) Kundendaten der GIS hinweist. Offiziell bestätigt wurde das allerdings nicht.

Der NEOS-Abgeordnete E hatte zuvor von einem einschlägigen Darknet-Angebot berichtet, auf dem behauptet wird, Adressen, Telefonnummern und Kontodaten von österreichischen Beamten, Richtern, Staatsanwälten und Journalisten zu verkaufen. Ob es sich dabei um jene Plattform handelt, die auch die aktuellen Ermittlungen ausgelöst hat, war vorerst unklar. E hielt auf Anfrage der APA auch einen Zusammenhang mit dem "Ergänzungsregister" auf der Seite des Wirtschaftsministeriums für möglich und forderte Aufklärung darüber, ob hier Daten abgeflossen sein könnten.“

*Beweiswürdigung zu C.4.: Die getroffenen Feststellungen beruhen auf der Stellungnahme der BG im Hauptverfahren zur GZ: 123*** und sind unstrittig. Konkret abgefragt wurden die Websites https://xyz.at/ sowie https://***-Amt.at/, die die BG in ihrer Stellungnahme angeführt hat.*

D. In rechtlicher Hinsicht folgt daraus:

D.1. Zur Feststellungskompetenz der Datenschutzbehörde

Nach Judikatur des VwGH und des BVwG kommt der Datenschutzbehörde eine Feststellungskompetenz im Hinblick auf Verletzungen des Rechts auf Geheimhaltung gemäß § 1 Abs. 1 DSG in Beschwerdeverfahren zu (vgl. das Erkenntnis des BVwG vom 20. Mai 2021, Zl. W214 222 6349-1/12E; das Erkenntnis des VwGH vom 19. Oktober 2022, Ro 2022/04/0001; implizit auch das Erkenntnis des VwGH vom 23. Februar 2021, Ra 2019/04/0054, worin sich dieser mit der Feststellung einer in der Vergangenheit liegenden Geheimhaltungspflichtverletzung auseinandergesetzt hat, ohne die Unzuständigkeit der belangten Behörde aufzugreifen).

Es bestehen keine sachlichen Gründe, die Überlegungen des BVwG nicht auch auf den gegenständlichen Fall zu übertragen. Gegenständlich ist nämlich das Vorliegen einer in der Vergangenheit liegenden Verletzung zu überprüfen und scheidet ein Leistungsauftrag gemäß Art. 58 Abs. 2 DSGVO – als primäre Abhilfemaßnahme – aus.

Als Zwischenergebnis ist daher festzuhalten, dass eine Feststellungskompetenz gemäß Art. 58 Abs. 6 DSGVO iVm § 24 Abs. 2 Z 5 und Abs. 4 DSG gegeben ist.

D.2. Zur Präklusion des Beschwerderechts

Nach § 24 Abs. 4 DSG erlischt der Anspruch auf Behandlung einer Beschwerde, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behaupteter Maßen stattgefunden hat. Verspätete Beschwerden sind zurückzuweisen.

In der Literatur wird diesbezüglich von der subjektiven einjährigen Frist und der objektiven dreijährigen Frist gesprochen. Beide Fristen müssen eingehalten werden, damit ein Anspruch auf Behandlung der Beschwerde besteht (vgl. *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG [2018] § 24 Rz 2).

Wie festgestellt, erfolgte der Datendiebstahl durch eine dritte Person im Mai 2020 und wurden die Daten der bP daraufhin im Internet zum Verkauf angeboten (siehe Sachverhaltsfeststellung C.3). Da die

gegenständliche Beschwerde am 28.01.2023 eingebracht wurde, wurde die objektive Frist von drei Jahren jedenfalls eingehalten.

Zu überprüfen ist in weiterer Folge aber, ob auch die subjektive Frist von einem Jahr eingehalten wurde:

Im vorliegenden Fall hat die BG feststellungsgemäß über das beschwerende Ereignis – also den Datendiebstahl durch eine dritte Person und das darauffolgende Anbieten der Daten der bP im Internet – im Mai 2020 eine allgemeine Benachrichtigung gemäß Art. 34 Abs. 3 lit. c DSGVO durchgeführt. Es stellt sich in diesem Zusammenhang daher die Frage, ob die Benachrichtigung bereits als „Kenntniserlangung“ zu werten ist.

Weder aus dem Wortlaut von § 24 Abs. 4 DSG, noch aus den ErlRV zur Pendantbestimmung des früheren § 34 Abs. 1 DSG 2000 (vgl. 1613 BlgNR 20. GP 50) kann abgeleitet werden, ab wann von einer Kenntnis eines Einschreiters über das beschwerdende Ereignis auszugehen ist.

Anhaltspunkte für eine Auslegung bietet die Judikatur des VwGH zu § 42 AVG, der – in vergleichbarer Weise zu § 24 Abs. 4 DSG – bei Vorliegen gewisser Voraussetzungen eine Präklusion normiert. Konkret ist nach gefestigter Judikatur des VwGH zu überprüfen, ob eine bestimmte Kundmachungsform eine hohe Wahrscheinlichkeit dafür begründet, dass ein Beteiligter von der Anberaumung der Verhandlung tatsächlich Kenntnis erlangt (vgl. VwSlg 17384 A/2008).

Diese Anforderungen können auch auf die in § 24 Abs. 4 DSG normierte Präklusionsfrist übertragen werden.

Demzufolge muss eine hohe Wahrscheinlichkeit vorliegen, dass die bP bereits vor Ablauf der subjektiven Frist von einem Jahr Kenntnis von dem beschwerenden Ereignis erlangt hatte. Ein solch betroffenenfreundlicher Maßstab ist in Anbetracht des Ziels des Unionsgesetzgebers, betroffenen Personen einen einfachen und unentgeltlichen Rechtsschutzweg iZm den Schutz ihrer Daten zu gewährleisten (vgl. Punkt B.), auch geboten.

Aufgrund einer allgemeinen (und nicht individuellen) Benachrichtigung – etwa auf der Website der BG und auf www.123.at – kann aber nicht mit hoher Wahrscheinlichkeit der Rückschluss gezogen werden, dass eine Person individuell betroffen ist. Zudem stand zum damaligen Zeitpunkt – also im Mai 2020 – nur im Raum, dass es zu einem Datendiebstahl gekommen sein könnte (Konjunktiv) und war die konkret gestohlene Datenmenge unklar (siehe Sachverhaltsfeststellung C.4.).

Schließlich hat die BG in ihrer Stellungnahme vom 14. März 2023 im Hauptverfahren zur GZ: 123*** selbst ausgeführt, keine individuelle Benachrichtigung über den Vorfall durchführen zu können, da sie nicht wisse, wer konkret betroffen war. Wenn aber die BG – bis zum Zeitpunkt der Mitteilung durch die Datenschutzbehörde – selbst keine Kenntnis über die konkret betroffenen Personen hatte, kann nicht davon ausgegangen werden, dass die bP bereits vor einem Jahr (oder länger) eine solche Kenntnis hatte.

Als weiteres Zwischenergebnis ist daher festzuhalten, dass im vorliegenden Fall keine Präklusion des

Beschwerderechts iSd § 24 Abs. 4 DSG vorliegt.

D.3. Zur Rechtsverletzung im konkreten Fall

a) Anwendungsbereich von § 1 Abs. 1 DSG

Nach § 1 Abs. 1 DSG hat jedermann 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.

Die DSGVO und insbesondere auch die darin verankerten Grundsätze und Legaldefinitionen sind zur Auslegung des Rechts auf Geheimhaltung heranzuziehen (vgl. den Bescheid der DSB vom 31. Oktober 2018, GZ DSB-D123.076/0003-DSB/2018).

Im vorliegenden Fall ist ohne große Mühe erkennbar, dass im Datensatz zB. Vor- und Nachname oder die Adresse der bP enthalten sind (siehe Sachverhaltsfeststellung C.3). Der Datensatz der bP kann auch klar von den Datensätzen anderer betroffener Personen abgegrenzt werden. Es liegen somit personenbezogene Daten der bP iSd Art. 4 Z 1 DSGVO vor.

Als weiteres Zwischenergebnis ist daher festzuhalten, dass im vorliegenden Fall der Schutzbereich des § 1 Abs. 1 DSG und der sachliche Anwendungsbereich der DSGVO grundsätzlich eröffnet sind.

b) Datenschutzrechtliche Rolle der BG

Bevor die Rechtmäßigkeit der Datenverarbeitung überprüft wird, ist die datenschutzrechtliche Rolle der BG zu klären.

Die Rollenverteilung ist für das Beschwerdeverfahren nach Art. 77 Abs. 1 DSGVO iVm § 24 Abs. 1 DSG nämlich von entscheidender Bedeutung, da bestimmt wird, wer für die Einhaltung der jeweiligen Vorgaben verantwortlich ist und wie die betroffene Person ihre Rechte ausüben kann.

Nach Art. 4 Z 7 DSGVO ist jene natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle Verantwortlicher für eine Verarbeitung, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Dabei ist das wesentliche Kriterium die Entscheidungskomponente. Die Rolle des Verantwortlichen ergibt sich somit in erster Linie aus dem Faktum, dass eine bestimmte Stelle entschieden hat, personenbezogene Daten für ihre eigenen Zwecke zu verarbeiten. Der „Zweck“ beschreibt dabei ein erwartetes Ergebnis, während die „Mittel“ die Art und Weise festlegen, wie das erwartete Ergebnis erreicht werden soll (vgl. die Leitlinien 07/2020 des EDSA zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO V 2.0 Rz 15 ff).

Wie festgestellt (siehe Sachverhaltsfeststellung C.1.) und wie von der BG im Rahmen der mündlichen Einvernahme vom 25. Mai 2023 im Hauptverfahren zur GZ: 123*** auch vorgebracht (vgl. S. 5 ff der

Niederschrift), hat sich die BG im Rahmen der Einführung eines sog. Customer-Relationship-Management-Systems (CRM-Systems) eines IT-Unternehmens bedient und betraf der gegenständliche Vorfall einen Teilschritt des Projekts. Konkret war dieses IT-Unternehmen seitens der BG mit der Entwicklung und Implementierung des Projekts, inklusive Durchführung von Tests, beauftragt.

Weder aufgrund der Befragung der BG, noch aufgrund der Befragung des beauftragten IT-Unternehmens vom 25. August 2023 im Hauptverfahren zur GZ: 123*** (siehe Punkt A.9.) ist erkennbar, dass das beauftragte IT-Unternehmen die personenbezogenen Daten, die die BG zur Verfügung gestellt hat, zu eigenen Zwecken verarbeitet hätte. Gegenstand der Datenverarbeitung war stets die Einführung eines CRM-Systems. Es sind keine Anhaltspunkte vorhanden, dass das IT-Unternehmen eigenständig über die wesentlichen Mittel der gegenständlichen Datenverarbeitung entschieden hätte (wobei Auftragsverarbeitern bei der Wahl der Mittel ohnedies ein gewisser Spielraum zukommt; vgl. die bereits angeführten Leitlinien 07/2020 Rz 39 ff).

Schließlich hat die BG im Rahmen der mündlichen Einvernahme vom 25. Mai 2023 im Hauptverfahren zur GZ: 123*** (S. 6) angegeben, dass mit dem beauftragten IT-Unternehmen eine Vereinbarung gemäß Art. 28 Abs. 3 DSGVO abgeschlossen wurde. Der (bloße) Verstoß des Auftragsverarbeiters gegen die vertraglichen Vorgaben gegen die Sicherheit der Verarbeitung nach Art. 28 Abs. 3 lit. c DSGVO – worauf noch später einzugehen ist – führt jedenfalls nicht zu seiner Verantwortlichkeit, wenn der Auftragsverarbeiter nicht auch über Zwecke und Mittel dieser Verarbeitung bestimmt. Hiervon ist aus den dargelegten Gründen aber nicht auszugehen.

Als weiteres Zwischenergebnis ist daher festzuhalten, dass die BG als datenschutzrechtliche Verantwortliche gemäß Art. 4 Z 7 DSGVO für die Durchführung des Projekts sowie der Tests und die damit verbundene Datenverarbeitung zu qualifizieren ist. Das seitens der BG beauftragte IT-Unternehmen ist hingegen als Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO zu qualifizieren.

c) Verhältnis zwischen BG und Auftragsverarbeiter

Nach Art. 4 Z 8 DSGVO verarbeitet ein Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Aus ErwGr 81 der Verordnung ergibt sich, dass ein Auftragsverarbeiter die Datenverarbeitung im Namen des Verantwortlichen durchführt, dieser also der „verlängerte Arm“ des Verantwortlichen ist.

Ausgehend von den genannten Bestimmungen hat das BVwG bereits ausgesprochen, dass die Auftragsverarbeitung als Teil der Verarbeitung durch den Verantwortlichen selbst zu sehen ist (vgl. das Erkenntnis des BVwG vom 20. Oktober 2021, Zl. W211 2231475-1; vgl. auch die die bereits angeführten Leitlinien 07/2020 Rz 80, wonach sich die Rechtmäßigkeit der Datenverarbeitung durch den Auftragsverarbeiter von der Tätigkeit des Verantwortlichen ableitet).

Als weiteres Zwischenergebnis ist daher festzuhalten, dass für das Beschwerdeverfahren – aus datenschutzrechtlicher Sicht – die Verarbeitung durch den Auftragsverarbeiter so zu qualifizieren ist,

als hätte sie die BG selbst durchgeführt.

d) Zum Verstoß gegen die Vorgaben für die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO

Nach gefestigter Judikatur der Datenschutzbehörde ist von einem Verstoß gegen § 1 Abs. 1 DSG auszugehen, wenn personenbezogene Daten – als Folge mangelnder technischer und organisatorischer Maßnahmen – einem unbefugten Dritten zugänglich gemacht werden (vgl. den Bescheid der DSB vom 9. Oktober 2019, GZ: DSB-D130.073/0008-DSB/2019 und die dort angeführten weiteren Nachweise).

Auch aus der Judikatur des BVwG lässt sich ableiten, dass eine Verletzung von § 1 Abs. 1 DSG denkbar ist, sofern die Verletzung eine Folge „ungenügender Datensicherheitsmaßnahmen“ ist (vgl. Punkt 3.2.2.2.1. des Erkenntnisses vom 18. Oktober 2023, GZ: W108 2263948-1).

Diese Überlegungen können auf den gegenständlichen Fall übertragen werden:

Wie festgestellt, hat der Auftragsverarbeiter der BG die von dieser zur Verfügung gestellten Meldedaten – darunter auch die Daten der bP – auf eine Testumgebung geladen. Der Auftragsverarbeiter der BG hat in Folge im Rahmen von Entwicklungs- bzw. Testtätigkeiten eine Re-Konfiguration am Server der Testumgebung vorgenommen und einen Zugangs-Port zum Server geöffnet und offengelassen. Dieser offene Port wurde seitens einer dritten Person genutzt, um die gegenständlichen Daten zu erhalten. Der Zugriff auf diese Daten war ohne große Mühe seitens der dritten Person möglich. Andere Sicherheitsvorkehrungen, um unautorisierte Zugriffe auf die Datenbank zu verhindern (wie zB. eine zusätzliche Zugangsbeschränkung durch Authentifizierung mittels Nutzername und Passwort), waren gegenständlich bei der Konfiguration nicht getroffen worden (siehe Sachverhaltsfeststellung C.2.).

Allein schon aufgrund des Umfangs der betroffenen Datenmenge – personenbezogene Daten von mehreren Millionen Menschen – ist von einem hohen Maßstab an die gemäß Art. 32 DSGVO geforderten technischen und organisatorischen Maßnahmen auszugehen. Zudem ist die Art der Daten zu berücksichtigen. So können Meldedaten (zB. Vor- und Nachname, Adresse und Geburtsdatum) etwa für Identitätsdiebstahl missbraucht werden (vgl. ErwGr 75 DSGVO).

Ein derart ungeschützter Zugang zu den Meldedaten von Millionen betroffener Personen – inklusive jener der bP – ist jedenfalls nicht mit den Vorgaben von Art. 32 DSGVO für die Sicherheit der Verarbeitung vereinbar:

Die Möglichkeit, über spezielle Suchmaschinen, nach mit dem Internet verbundenen Anwendungen zu suchen, ist im Bereich der IT-Sicherheit nämlich hinreichend bekannt und sogar unverzichtbar, um die Angriffsoberfläche des eigenen Netzwerkes zu überprüfen. So verwundert es nicht, dass sich auch Kriminelle diese einfachen Suchmöglichkeiten zu Nutze machen, um neue und leicht angreifbare Opfer aufzuspüren. Daher werden bei einer IT-Schwachstellenanalyse („Penetrationstest“) auch regelmäßig solche Suchmaschinen eingesetzt.

Sobald IT-Anwendungen mit dem Internet verbunden sind, ist es somit essenziell, diese durch

Sicherheitsmaßnahmen, wie etwa die Authentifizierung mit Nutzernamen und Passwort, abzusichern. Auch das österreichische Informationssicherheitshandbuch betont, dass die Wahl eines geeigneten Authentifizierungsverfahren von entscheidender Bedeutung für die Sicherheit des Gesamtsystems ist (vgl. Punkt 9.6.1, „Wahl geeigneter Mittel zur Authentisierung“, abrufbar unter https://sicherheitshandbuch.gv.at/#1060).

Eine IP-Adresse zu einem Datenbankserver geheim zu halten, kann daher alleine niemals ausreichen, um den Vorgaben von Art. 32 DSGVO für die Sicherheit der Verarbeitung zu entsprechen. Ein Zugang muss auch entsprechend – etwa durch Authentifizierung – abgesichert werden. Dem wären im vorliegenden Fall auch keine hohen Implementierungskosten entgegengestanden.

Zudem hat die BG – trotz eingeräumter Möglichkeiten, u.a. im Rahmen der Einvernahme vom 25. Mai 2023 im Hauptverfahren zur GZ: 123*** und Nachfrage seitens der Datenschutzbehörde zu den offen gelassenen Ports – die Einhaltung der Vorgaben für die Sicherheit der Verarbeitung im Zusammenhang mit dem gegenständlichen Vorfall nicht nachgewiesen. Für den Nachweis der Einhaltung von Art. 5 Abs. 1 lit. f iVm Art. 32 DSGVO trägt die BG nach gefestigter Judikatur des EuGH die Beweislast (vgl. das Urteil vom 4. Juli 2023, C-252/21 Rz 95).

Somit ist beim gegenständlichen Datenverlust davon auszugehen, dass dieser eine unmittelbare Folge einer Verletzung von Art. 32 DSGVO durch den Auftragsverarbeiter und somit auch durch die BG als Verantwortliche war, welcher das Verhalten des Auftragsverarbeiters – wie oben dargelegt – aus datenschutzrechtlicher Sicht zuzurechnen ist.

Ein Datenverlust als Folge einer Verletzung von Art. 32 DSGVO – also ein, wenngleich ungewolltes, Zugänglichmachen – ist zudem als Vorgang gemäß Art. 4 Z 2 DSGVO zu qualifizieren (vgl. zur sehr weiten Auslegung des sachlichen Anwendungsbereichs der DSGVO die Urteile des EuGH vom 22. Juni 2021, C-439/19, Rz 61; zur insofern vergleichbaren Rechtslage die Urteile vom 20. Dezember 2017, C-434/16, Rz 33, sowie vom 7. Mai 2009, C-553/07, Rz 59).

e) Rechtmäßigkeit der Datenverarbeitung

Im Hinblick auf die Rechtmäßigkeit war die gegenständliche Verarbeitung, konkret das – wenngleich ungewollte – Zugänglichmachen der Daten der bP (an einen unbefugten Dritten) – im Übrigen offenkundig durch keine Rechtsgrundlage gemäß § 1 Abs. 2 DSG oder Art. 6 Abs. 1 DSGVO gerechtfertigt. Eine nähere Prüfung der einzelnen Rechtsgrundlagen – also etwa, ob eine Einwilligung oder „berechtigte Interessen“ vorliegen – erübrigt sich demnach.

Eine solche Rechtsgrundlage wurde seitens der BG im Übrigen auch nicht ins Treffen geführt, wobei diese für den Nachweis der Rechtmäßigkeit der Verarbeitung nach gefestigter Judikatur des EuGH die Beweislast trägt (vgl. das Urteil des EuGH vom 4. Juli 2023, C-252/21 Rz 95 und die dort angeführten weiteren Nachweise).

Ein allfälliges Verschulden seitens des Auftragsverarbeiters oder der BG ist in einem Beschwerdeverfahren nach Art. 77 Abs. 1 DSGVO iVm § 24 Abs. 1 DSG keine Voraussetzung für den

Beschwerdeerfolg, weshalb ein solches nicht geprüft wurde.

D.4. Ergebnis

Ausgehend von all diesen Überlegungen ist im Ergebnis festzuhalten, dass eine Verletzung von § 1 Abs. 1 DSG (Recht auf Geheimhaltung) und Art. 6 Abs. 1 DSGVO (Rechtmäßigkeit der Datenverarbeitung) als Folge einer Verletzung von Art. 32 DSGVO vorliegt.

Es war daher spruchgemäß zu entscheiden.