BVwG
Bundesverwaltungsgericht
Republik Österreich

Postadresse:
Erdbergstraße 192 – 196
1030 Wien
[redacted]
E-Mail: einlaufstelle@bvwg.gv.at
www.bvwg.gv.at

Geschäftszahl (GZ):
W274 2248601-1/14E
(bitte bei allen Eingaben anführen)

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

Das Bundesverwaltungsgericht erkennt durch den Richter [redacted] als Vorsitzenden sowie die fachkundigen Laienrichter [redacted] und [redacted] als Beisitzer über die Beschwerde des [redacted], vertreten durch: [redacted], gegen den Bescheid der **Datenschutzbehörde**, Barichgasse 40-42 1030 Wien, vom 15.10.2021, GZ: D124.2635, Mitbeteiligte **A1 Telekom Austria Aktiengesellschaft**, Lassallestraße 9, 1020 Wien, vertreten durch [redacted] **wegen Verletzung im Recht auf Auskunft gemäß Art. 15 DSGVO**, in nichtöffentlicher Sitzung zu Recht:

Der Beschwerde wird **nicht Folge** gegeben.

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

E n t s c h e i d u n g s g r ü n d e :

1.1. Mit **Datenschutzbeschwerde vom 12.06.2020** beantragte [redacted] (im Folgenden: Beschwerdeführer, BF) zunächst vertreten durch noyb – Europäisches Zentrum für digitale Rechte, die Datenschutzbehörde (im Folgenden: belangte Behörde) wolle

1. untersuchen, ob die A1 Telekom Austria AG (im Folgenden: Mitbeteiligte, MB) den BF betreffend Verkehrsdaten, Standortdaten bzw. Standortkennungen im Sinne des TKG verarbeite sowie

2. diese anweisen, dem (näher durch den BF dargestellten) **Auskunftsbegehren** Folge zu leisten und wie folgt zu entscheiden:

Die MB sei gemäß Art. 15 Abs. 1 DSG schuldig,

- dem BF zu beauskunften, auf welche Dokumente sie sich in der Auskunft (Beilage ./C) beziehe, und diese Dokumente dem BF zugänglich zu machen;

- dem BF sämtliche Verarbeitungszwecke und Rechtsgrundlagen der jeweiligen Verarbeitungen differenziert zu beauskunften und hinsichtlich der auf Art. 6 Abs. 1 lit. a DSGVO geschützten Verarbeitungen nachzuweisen, dass der BF in die Verarbeitung seiner personenbezogenen Daten eingewilligt habe;

- dem BF sämtliche Empfänger (einschließlich Auftragsverarbeiter) der personenbezogenen Daten des BF, die Gegenstand der Verarbeitung seien, zu beauskunften, sofern diese bekannt seien. In allen anderen Fällen seien zumindest Empfängerkategorien zu beauskunften;

- dem BF aufgeschlüsselt nach verarbeiteten Datenkategorien zu beauskunften, wie lange personenbezogene Daten des BF, die Gegenstand der Verarbeitung seien, konkret gespeichert werden bzw. nach welchen Kriterien sich die Speicherdauer bestimme;

- dem BF alle verfügbaren Informationen über die Herkunft der personenbezogenen Daten des BF, die Gegenstand der Verarbeitung seien, zu beauskunften;

- dem BF eine Kopie der ihn betreffend Verkehrs-, Standortdaten sowie Standortkennungen im Sinne des TKG, die Gegenstand der Verarbeitung seien, zur Verfügung zu stellen.

Dazu brachte der BF vor, er sei Vertragsinhaber eines aufrechten Mobilfunkvertrages der Marke „Georg“ mit der MB. Dem BF seien die Kundennummer [redacted] und die Rufnummer [redacted] zugewiesen. Die Nummer der im Mobiltelefon eingelegten Simkarte laute [redacted]. Dieser Mobilfunkvertrag sei am 27.05.2019 aktiviert worden und werde seitdem ausschließlich vom BF privat genutzt. Der BF sei kinderlos und habe bis zum 03.01.2020 einen Einzelhaushalt geführt. Seit diesem Zeitpunkt teile er seinen Haushalt lediglich mit seiner Lebensgefährtin, die über einen eigenen Mobilfunkvertrag und über ein eigenes Mobiltelefon verfüge.

Der BF habe am 17.03.2020 per E-Mail ein Auskunftsbegehren gemäß Art. 15 DSGVO an die MB gerichtet, in dem er ausdrücklich die Beauskunftung von Verkehrsdaten gemäß § 92 Abs. 3 Z 4 TKG (2003 – Anmerkung des Gerichts) begehrt habe (Beilage. /D).

Nach Aufforderung, seinem Begehren eine Ausweiskopie beizulegen, habe der BF diesem eine digitale Signatur hinzugefügt und am 19.03.2020 per E-Mail eine Auskunft (Beilage ./C), eine Darstellung seiner Datenschutzeinstellungen (Beilage ./D) und eine Erklärung der in dieser Darstellung verwendeten Farbkategorien (Beilage ./E) erhalten.

Die Auskunft habe keine klare Aussage enthalten, ob die MB Verkehrs- und Standortdaten zum BF gespeichert habe, sondern lediglich Erklärungen, warum es sich bei diesen Daten jeweils handle sowie juristische Ausführungen, warum eine Kopie dieser Daten nicht übermittelt werden müsse.

Mit E-Mail vom 20.03.2020 habe der BF Klarstellung begehrt, ob die MB nun Verkehrs- und/oder Standortdaten zu seiner Person speichere und abermals um Übermittlung einer Kopie dieser Daten ersucht (Beilage ./F).

Mit E-Mail vom 01.04.2020 habe die MB ihre Antwort übermittelt, die abermals nur aus juristischen Ausführungen bestanden habe, jedoch keine klaren Aussagen zur tatsächlichen Speicherung von Verkehrs- und Standortdaten und keine Kopie dieser Daten enthalten habe (Beilage ./G).

Die MB ziehe insbesondere in Zweifel, dass ausschließlich der BF sein Mobiltelefon nutze und vermeine daher, dass es sich bei Standortdaten nicht um personenbezogene Daten, die den BF beträfen, handle. Zur Glaubhaftmachung der tatsächlichen ausschließlichen Nutzung seines Mobilfunkvertrages bzw. seines Mobiltelefons lege der BF daher eine eidesstattliche Erklärung (Beilage ./H) bei.

In weiterer Folge erstattete der BF Vorbringen betreffend weiterer Erkundigungen gegenüber der MB betreffend Datenschutzeinstellungen, auf deren Wiedergabe mangels Relevanz im Beschwerdeverfahren verzichtet wird.

Daran schließen sich umfangreiche rechtliche Ausführungen, die zusammengefasst wie folgt wiedergegeben werden.

Der BF wolle wissen, ob die MB Verkehrsdaten iSd § 92 Abs. 3 Z 4 TKG mit Personenbezug zum BF speichere oder nicht. Die MB gebe an, keine Auskunft über Standortdaten zu geben, weil

der BF als Nutzer der Rufnummer (SIM-Karte) nicht ausreichend nachweisen könne, dass ausschließlich er selbst die Rufnummer (SIM-Karte) nutze. Dabei stütze sich die MB auf eine Entscheidung der Datenschutzbehörde (DSB-D122.418/0002-DSB/2016). Die MB lasse dabei offen, ob sich diese Verweigerung nur auf Standortdaten iSd § 92 Abs. 3 Z 6 TKG 2003 beziehe, die auch als Verkehrsdaten iSd § 92 Abs. 3 Z 4 TKG 2003 zu qualifizieren seien, oder auch auf andere Standortdaten als Verkehrsdaten gemäß § 102 TKG 2003.

Sofern die MB Verkehrsdaten und Standortdaten zum BF verarbeite, seien diese jedenfalls zu beauskunften. Dies umfasse auch die Standortkennung iSd § 92 Abs. 3 Z 6a TKG 2003 (nunmehr § 160 Abs. 3 Z 10 TKG 2021), die sowohl als Verkehrs- als auch als Standortdatum zu qualifizieren sei.

Verkehrsdaten gemäß § 92 Abs. 3 Z 4 TKG (bzw. § 160 Abs. 3 Z 6 TKG 2021) seien ungeachtet des § 99 Abs. 5 TKG 2003 (§ 167 Abs. 5 TKG 2021) vollinhaltlich gemäß Art. 15 DSGVO zu beauskunften. Die Rechtsprechung der Datenschutzbehörde (DSB-D122.418/0002-DSB/2016, DSB-D122.616/0006-DSB/2016), wonach ein Telekommunikationsdiensteanbieter im Regelfall nicht feststellen könne, ob ein Auskunftswerber, dessen Standortdaten Gegenstand des Auskunftsverlangens seien, tatsächlich (zu jedem Zeitpunkt) Nutzer der einem Endgerät zugeordneten Rufnummer sei bzw. gewesen sei, und auch eine eidesstattliche Erklärung der ausschließlichen Benutzung daran nichts ändere, weil auch dadurch kein objektiver, d.h. für jedermann nachvollziehbarer, Nachweis erbracht werde, dass der Beschwerdeführer zu jedem Zeitpunkt des von ihm angegebenen Zeitraumes tatsächlicher Nutzer des Endgerätes gewesen sei, könne unter dem Regime der DSGVO ebenfalls nicht fortgeführt werden. Um Art. 15 DSGVO zur Wirksamkeit zu verhelfen, müsse der betroffenen Person daher ermöglicht werden, glaubhaft zu machen, dass sie „tatsächlicher Nutzer des Endgerätes war“, bzw. obliege es dem Verantwortlichen nachzuweisen, warum eine eindeutige Identifizierung einer betroffenen Person in Bezug auf Standortdaten nicht möglich sei.

Gemäß Art. 12 Abs. 2 DSGVO iVm Art. 11 Abs. 2 DSGVO obliege es im gegenständlichen Fall der MB, nachzuweisen, dass sie nicht imstande sei, den BF als betroffene Person hinsichtlich jener Standortdaten zu identifizieren, die von seinem Mobiltelefon erzeugt worden seien. Andernfalls würde auch das in Art. 5 Abs. 2 DSGVO normierte Rechenschaftsprinzip unterlaufen, da ein Verantwortlicher Standortdaten kaum jemals beauskunften müsste. Die Verarbeitung dieser Daten wäre der Kontrolle durch die betroffene Person und damit in weiten Teilen auch der Datenschutzbehörde entzogen, insbesondere wäre die Ausübung weiterer Betroffenenrechte gemäß Art. 16 bis Art. 22 DSGVO mangels Kenntnis über

gespeicherte Standortdaten faktisch nicht möglich. Die vor Gültigkeitsbeginn der DSGVO ergangene Rechtsprechung der Datenschutzbehörde, die eine Pflicht zum Nachweis der tatsächlichen ausschließlichen Nutzung bei der betroffenen Person verorte, könne insofern nicht aufrechterhalten werden. Bestünden Zweifel, dass die von einem Mobiltelefon erzeugten Standortdaten tatsächlich einen Auskunftswerber betreffen, sei diesem iSd Artikel 12 Abs. 2 DSGVO die Möglichkeit einzuräumen, darzulegen, dass die Standortdaten tatsächlich ihn beträfen. Für die Annahme von Zweifeln bedürfe es konkreter Anhaltspunkte.

Der BF sei Vertragsinhaber des gegenständlichen Mobilfunkvertrages und nutze diesen und sein Mobiltelefon ausschließlich selbst. Nach allgemeiner Lebenserfahrung handle es sich bei einem privaten Mobiltelefon um einen höchstpersönlichen Gegenstand. Aufgrund der persönlichen Lebensumstände des BF schieden andere Personen als (Mit)benutzer seines Mobiltelefons bzw. seines Mobilfunkvertrages aus. Falls der BF sein Mobiltelefon überhaupt jemals anderen Personen überlasse, geschehe dies ausschließlich in dessen unmittelbarer physischer Nähe, sodass allenfalls erzeugte Standortdaten sich jedenfalls auf den BF bezögen. Es sei nicht ersichtlich, warum Zweifel bestünden, dass der BF tatsächlich (zu jedem Zeitpunkt) Nutzer der einem Endgerät zugeordneten Rufnummer sei bzw. gewesen sei. Folgte man der Argumentation der MB und setzte die DSB ihre Rechtsprechung fort, hätte dies zur Folge, dass keinerlei personenbezogene Daten gemäß Art. 15 DSGVO zu beauskunften wären, die von einem mobilen Gerät übermittelt werden, das internet- oder GPS-fähig sei, denn für den Verantwortlichen bestünde niemals hundertprozentige Sicherheit über den Benutzer eines solchen Geräts.

Darüber hinaus sei das Mobiltelefon des BF durch eine nur ihm bekannte PIN sowie durch dessen Fingerabdruck geschützt, weshalb andere Personen, die seines Mobiltelefons habhaft werden, außerstande seien, es zu benutzen. Auch diesem Umstand zufolge sei daher davon auszugehen, dass es sich bei den gegenständlichen Standortdaten um den BF betreffende personenbezogene Daten handle.

Andernfalls müsste man bei sämtlichen passwortgeschützten Geräten und Diensten in Zweifel ziehen, dass die bei Benutzung dieser Geräte/Dienste generierten Daten personenbezogen seien bzw. lediglich eine Person beträfen, so neben Mobiltelefonen etwa bei Laptops, Smart-Watches, E-Mail- und Online-Banking-Accounts, Dating-Plattformen, Shopping-Portalen, Glücksspielanbietern usw. Schließlich sei nie mit Sicherheit auszuschließen, dass eine andere Person als der rechtmäßige Inhaber ein solches Gerät bzw. einen solchen Dienst nutze. Der Begriff der personenbezogenen Daten in Art. 4 Abs. 1 DSGVO folge jedoch einem

probabilistischen Ansatz: Nach allgemeiner Lebenserfahrung sei es mit hinreichender Wahrscheinlichkeit ausschließlich der rechtmäßige Inhaber eines Mobiltelefons (oder eines anderen persönlichen Geräts/Dienstes), der dieses benutze. Die im Zusammenhang mit der Benutzung des Mobiltelefons generierten Daten bezögen sich demnach auf eine eindeutig identifizierte bzw. identifizierbare Person. Dies gelte umso mehr für einen Telekommunikationsanbieter als Vertragspartner im Bezug auf einen Mobilfunkvertrag und zumeist auch als Verkäufer des Mobiltelefons. Aus Sicht der MB gäbe es keinen Grund daran zu zweifeln, dass die gegenständlichen Standortdaten ausschließlich den BF betreffen.

Im Übrigen gehe die MB an anderer Stelle offenkundig selbst von einer ausschließlichen Mobiltelefon-Nutzung durch den BF aus, denn in der Georg-Smartphone-App (www.georg.at/app) bestehe für Kunden der MB die Möglichkeit, persönliche Datenschutzeinstellungen zu ändern und Einwilligungen zu erteilen oder zu widerrufen. Bezweifle die MB ohne konkrete Anhaltspunkte, dass ausschließlich der BF sein Mobiltelefon benutze, müsse sie auch die Wirksamkeit sämtlicher Einwilligungen in Frage stellen, die über die App erteilt werden könnten. Schließlich wäre stets unklar, ob tatsächlich der Inhaber eines Vertrages samt zugehöriger SIM-Karte und Mobiltelefonnummer in der lokal auf seinem Mobiltelefon installierten App eine Einwilligung erteilt oder widerrufen habe oder ob eine Willenserklärung einer anderen Person vorliege.

Zusätzlich lege der BF zur Glaubhaftmachung der tatsächlichen und ausschließlichen Nutzung seines Mobilfunkvertrages bzw. seines Mobiltelefons eine eidesstattliche Erklärung bei. Bestünden weiterhin Zweifel, obliege es der MB, die tatsächliche Nutzung durch den BF zu überprüfen – etwa indem ihm im Zuge der Auskunftserteilung eine TAN zugesendet werde oder er über die Georg-Smartphone-App um Verifizierung seiner Identität ersucht werde.

Das Problem eines mangelnden Nachweises der tatsächlichen, ausschließlichen Nutzung seines Mobiltelefons durch die MB ergäbe sich auch bei dem gemäß § 100 TKG 2003 (nunmehr § 138 Abs. 6 TKG 2021) zu erstellenden Einzelgesprächsnachweis, da auch dort keine hundertprozentige Sicherheit bestehe, dass tatsächlich der BF – und nicht eine andere natürliche Person – einen Anruf getätigt oder entgegengenommen habe. Nichtsdestotrotz handle es sich bei den im Einzelgesprächsnachweis abgebildeten Daten ohne jeden Zweifel um personenbezogene Daten mit Bezug zum Inhaber des Mobilfunkvertrages.

Bezüglich anderer Standortdaten als Verkehrsdaten seien zudem Art. 9 e-Datenschutzrichtlinie und § 102 TKG 2003 (nunmehr § 169 TKG 2021) zu beachten. Gemäß § 102 Abs. 1 TKG 2003 (bzw. § 169 TKG 2021) dürften andere Standortdaten als Verkehrsdaten

unbeschadet des § 98 TKG 2003 (nunmehr § 123 TKG 2021) nur verarbeitet werden, wenn sie anonymisiert werden oder die Benutzer oder Teilnehmer eine jederzeit widerrufbare Einwilligung gegeben haben. Eine Einwilligung gemäß Art. 5 Abs. 1 lit. a iVm Art. 7 DSGVO könne sich jedoch nur auf personenbezogene Daten beziehen, die den jeweiligen Endnutzer betreffen. Insofern gehe auch das TKG 2003 (bzw. TKG 2021) selbst von einem eindeutigen Personenbezug anderer Standortdaten als Verkehrsdaten aus. Es sei nicht ersichtlich, warum es sich bei Standortdaten, die als Verkehrsdaten zu qualifizieren seien, anders verhalten sollte. Sämtliche Standortdaten seien daher gemäß Art. 15 DSGVO vollumfänglich zu beauskunften.

Dieser Beschwerde waren die Auskunftsanträge sowie die jeweiligen Antworten der MB angeschlossen.

1.2. Mit anwaltlicher **Stellungnahme vom 04.09.2020** beantragte die **MB,** die Beschwerde als unbegründet abzuweisen und führte zusammenfassend aus, sie habe durch die Übermittlung zusätzlicher Informationen an den BF einigen Beschwerdepunkten bzw. Anträgen im Sinne des § 24 Abs. 6 DSG nachträglich entsprochen. Sie habe die Rechtmäßigkeit der Nichtbeauskunftung von Verkehrs- und Standortdaten mit der vom Gesetzgeber getroffenen Abwägung zur Sicherstellung der Grundrechte aller an einer Kommunikation beteiligten Personen ausführlich dargelegt. Für eine Änderung der Rechtslage wäre der Gesetzgeber gefordert.

Dazu brachte sie im Einzelnen vor:

Das TKG und die einschlägigen Entscheidungen schützten nicht nur den Vertragsinhaber sondern auch die anderen Teilnehmer an einer Kommunikation, dazu gehörten die anrufenden Gesprächsteilnehmer bei eingehenden Anrufen, die das Recht hätten, die Anzeige ihrer Rufnummer zu unterdrücken, wenn sie dies wünschten, die Nutzer eines Anschlusses, die nicht Vertragsinhaber seien, aber auch die passiven Teilnehmer eines aktiven Calls (der Nutzer ruft jemanden an). Dazu bestehe nach den gesetzlichen Regelungen und Entscheidungen ein umfangreiches Schutzkonzept, an das sich die MB halte, andernfalls würde sie sich strafbar machen.

Nach ständiger Rechtsprechung der Datenschutzbehörde, sowohl vor als auch nach Inkrafttreten der DSGVO, sei der Anwendungsvorrang der Bestimmungen des TKG 2003 (bzw. TKG 2021) als lex specialis zur Befolgung eines Auskunftsanspruchs maßgeblich. Eine uneingeschränkte Übermittlung sämtlicher Verkehrsdaten im Zusammenhang mit einem Auskunftsverlangen des Betroffenen sehe das TKG 2003 nicht vor. Andernfalls wären die

umfangreichen Bestimmungen des TKG 2003 zur Verarbeitung von Verkehrsdaten ohne jegliche Wirkung. Nach der Rechtsprechung der Datenschutzbehörde präzisierten die datenschutzrechtlichen Bestimmungen (§ 26 Abs. 1 DSG) das verfassungsrechtlich gewährleistete Recht auf Auskunft auf die zu dieser Person verarbeiteten Daten, vorausgesetzt, dass die Identität in geeigneter Form nachgewiesen werde. Da die einschlägigen Bestimmungen des TKG 2003 (bzw. TKG 2021) bzw. der diesen zugrundeliegenden e-Datenschutzrichtlinie der DSGVO als lex specialis vorgingen, sei in Bezug auf diese Daten Art. 15 Abs. 3 DSGVO gewahrt, da die MB dem BF eine Kopie der zulässigerweise zu beauskunftenden personenbezogenen Daten zur Verfügung gestellt habe. Standortdaten seien nach herrschender Judikatur Verkehrsdaten im Sinne des § 92 Abs. 3 Z 4 TKG (§ 160 Abs. 3 Z 6 TKG 2021). Daher gelte zur Auskunftspflicht von Standortdaten dasselbe wie zu jener von Verkehrsdaten.

Oft sei es der Fall, dass Teilnehmer und Nutzer des mobilen Endgerätes auseinanderfallen (Familie, Verwandte, Freunde, Lebensgefährten, Mitarbeiter, etc). Ein Auftraggeber könne zu Recht die begehrte Auskunft über Standortdaten verweigern, solange nicht mit ausreichender Sicherheit feststehe und objektiv nachweisbar sei, dass ein Auskunftswerber auch tatsächlich Nutzer von einem einer Rufnummer zugeordneten Endgerätes sei oder gewesen sei. Ein solcher Nachweis könne nicht erbracht werden. Da die einschlägigen Bestimmungen des TKG 2003 und der zugrundeliegenden (gemeint) e-Datenschutz-Richtlinie der DSGVO als lex specialis vorgingen, sei Art. 11 DSGVO, der die Identifizierung der Betroffenen zur Ausübung seiner Betroffenenrechte regle, aus Sicht der MB nicht anwendbar. Doch selbst bei Anwendungsvorrang des Art. 11 DSGVO sei dieser in Verbindung mit Art. 12 DSGVO zu lesen. Art. 12 Abs. 2 DSGVO sehe vor, dass der Verantwortliche dem Betroffenen die Ausübung seiner Betroffenenrechte erleichtern soll, sich aber dann weigern könne, wenn er „glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren“. Im Unterschied zum Beweis erachte der Gesetzgeber die Glaubhaftmachung als ausreichend. Es sei dem Schutz der Betroffenen vor Ausübung ihrer Betroffenenrechte durch möglicherweise unberechtigte Personen damit ein sehr hoher Stellenwert eingeräumt. So könne ein Telekommunikationsdiensteanbieter zweifellos gemäß Art. 12 Abs. 2 DSGVO „glaubhaft machen“ oder schlüssig darlegen, dass er nicht in der Lage sei, die betroffene Person hinsichtlich jener Standortdaten zu identifizieren, die mit dem zugeordneten Endgerät erzeugt worden seien. Dem Betreiber sei nur sein Vertragspartner nachweislich bekannt, nicht jedoch der tatsächliche Nutzer. Der tatsächliche Nutzer zum Zeitpunkt der Entstehung eines Verkehrs- oder Standortdatums sei für den Telekommunikationsdiensteanbieter nicht ersichtlich. Ebenso wie der Nachweis der Nutzung sei dem Telekommunikationsdiensteanbieter auch

unmöglich, wie vom BF angeregt, konkrete Zweifel an der tatsächlichen Nutzung des zugeordneten Endgerätes durch eine bestimmte Person darzulegen bzw. zu entkräften. Dies treffe auch dann zu, wenn im vorliegenden Fall der BF behaupte, dass das Endgerät ausschließlich zur privaten Nutzung diene. Auch in diesem Fall sei es keinesfalls auszuschließen oder lebensfremd, dass Daten einer bestimmten Verbindung sich nicht auf den Teilnehmer, sondern auf etwaige Mitbenutzer des Anschlusses bezögen (vgl. § 100 Abs. 3 TKG 2003). Auch eine eidesstattliche Erklärung sei hierfür in Übereinstimmung mit der Judikatur der Datenschutzbehörde nicht ausreichend.

Das Spannungsverhältnis, bedingt durch den nachweislich bekannten Teilnehmer und die tatsächliche ausschließliche Nutzung durch denselben, sei auch dem Gesetzgeber bei der Legistik des TKG 2003 durchaus bewusst gewesen. Daher seien Bestimmungen geschaffen worden, die mögliche Gefahren für den Datenschutz von vom Teilnehmer verschiedene Nutzer ausgleichen sollen. Die diesbezügliche Abwägung zwischen der Möglichkeit der Nutzung durch mehrere Personen und dem Interesse an einem Detaillierungsgrad des Entgeltnachweises spiegle sich etwa im § 100 Abs. 3 TKG 2003 (§ 138 Abs. 6 TKG 2021) wieder, wonach bei der Erstellung eines Entgeltnachweises nur jene Daten verarbeitet werden dürften, die dafür unbedingt erforderlich seien. Die passiven Teilnehmernummern oder sonstigen Angaben zur Identifizierung eines Empfängers einer Nachricht dürften im Einzelentgeltnachweis nur in verkürzter Form ausgewiesen werden. Wünsche der Teilnehmer einen unverkürzten Entgeltnachweis, so sei er verpflichtet, eine Erklärung abzugeben, dass er alle bestehenden und künftigen Mitbenutzer eines Anschlusses davon informiere. Ohne eine vergleichbare Bestimmung für datenschutzrechtliche Beauskunftungen, die es nicht gäbe, wäre der Schutzzweck dieser Norm ausgehebelt. Eine derartige Absicht könne weder dem europäischen noch dem nationalen Gesetzgeber unterstellt werden.

§ 102 TKG (§ 169 TKG 2021) regle die Verarbeitung von „Anderen Standortdaten als Verkehrsdaten“. Auch hier habe der Gesetzgeber durch zusätzliche Maßnahmen den Schutz von Nutzern sichergestellt, indem die Verwendung von Standortinformationen bei jeder Verwendung untersagt werden könne. Der MB sei keine Anwendung bekannt, in der eine Einwilligung zur Nutzung anderer Standortdaten als Verkehrsdaten abgefragt werde, zumal seit der Verfügbarkeit von GPS-Empfängern in praktisch jedem Endgerät die Nutzung der deutlich unpräziseren Standortdaten aus einem Mobilfunknetz nicht mehr notwendig sei.

Der besondere Schutz von Verkehrsdaten verdeutliche sich auch in der Bestimmung des § 94 iVm § 102a ff TKG 2003, wonach die Übermittlung von Verkehrsdaten an Behörden

ausschließlich auf elektronischem Weg über die vom Bundesrechenzentrum betriebene Durchlaufstelle erfolgen dürfe. Das Gesetz sehe hier detailliert besondere Sicherheitsmaßnahmen, wie asymmetrische Verschlüsselung und umfassende weitere Maßnahmen, vor. Wenn eine solche Beauskunftung doch zulässig wäre, wäre wohl eine vergleichbare Übermittlungssicherheit beim Betroffenen auch vorgesehen worden.

Auch diesen Äußerungen waren Beilagen angeschlossen, darunter die Datenschutzerklärung und die Allgemeinen Geschäftsbedingungen der MB betreffend das Produkt „Ge org!“ (AGB Ge org!).

1.3. Nach Übermittlung dieser Stellungnahme zum Parteiengehör erfolgte eine weitere **Stellungnahme des BF vom 05.10.2020** mit nunmehr adaptierten Anträgen wie folgt:

Falls die belangte Behörde der Ansicht sei, dass die MB einzelne Rechtsverletzungen beseitigt habe und daher kein Leistungsauftrag zu erteilen sei, werde beantragt festzustellen, die MB habe das Auskunftsrecht des BF gemäß Art. 15 verletzt, indem sie

- innerhalb der Frist des Art. 12 Abs. 3 DSGVO dem BF entgegen Art. 15 Abs. 1 lit. a DSGVO keine vollständigen Informationen zu den Verarbeitungszwecken zur Verfügung gestellt habe;

- nicht sämtliche bekannte Empfänger (einschließlich Auftragsverarbeiter) der personenbezogenen Daten des BF, die Gegenstand der Verarbeitung seien, beauskunftet habe;

- keine vollständigen Informationen zur Speicherdauer innerhalb der Frist des Art. 12 Abs. 3 DSGVO zur Verfügung gestellt habe und

- nicht alle verfügbaren Informationen über die Herkunft der personenbezogenen Daten des BF zur Verfügung gestellt habe.

Zur „Kernfrage des gegenständlichen Verfahrens“, der Pflicht zur Bereitstellung einer Kopie von Verkehrs- und Standortdaten, seien sämtliche Rechtsverletzungen unverändert aufrecht.

Die MB habe diese Daten zusammengefasst aus folgenden Gründen zu beauskunften:

- § 99 Abs. 5 TKG 2003 stehe weder seinem Wortlaut noch seinem Zweck nach der Beauskunftung von Verkehrs- und Standortdaten entgegen.

- Selbst wenn die DSB einen Konflikt zwischen Art. 15 DSGVO und den Normen des TKG 2003 verorte, gehe Art. 15 DSGVO qua Anwendungsvorrang vor. § 99 Abs. 5 TKG 2003 sei keine lex specialis zur Art. 15 DSGVO.

  Die lex-specialis-Regel greife nur bei gleichrangigen Rechtsnormen. Der datenschutzrechtliche Auskunftsanspruch sei Anwendungsvorrang genießendes Unionsrecht, gemäß § 1 Abs. 3 DSG auf Verfassungsebene vorgesehen und somit höherrangiger als das TKG 2003.

  Eine Einschränkung des datenschutzrechtlichen Auskunftsanspruchs bezüglich Verkehrs- /Standortdaten sei auch nicht in der e-Datenschutz-Richtlinie vorgesehen. Auch über Art. 95 DSGVO ergäbe sich keine Derogation des datenschutzrechtlichen Auskunftsanspruchs, selbst wenn die DSB der Ansicht sei, dass das TKG 2003 derartige Einschränkungen vorsehe.

- Es obläge der MB nachzuweisen, dass auch andere natürliche Personen den Mobilfunkvertrag bzw. das Mobiltelefon des BF benutzten und vorhandene Standortdaten sich daher nicht auf den BF bezögen.

Dazu brachte der BF weiters vor wie folgt:

Es obliege der MB darzulegen, dass erzeugte Standortdaten nicht den BF sondern andere Personen beträfen. Gegenständlich fielen Teilnehmer und Nutzer des mobilen Endgerätes nicht auseinander und seien auch in der Vergangenheit nie auseinandergefallen. Sämtliche Standortdaten beträfen ausschließlich den BF. Es bleibe kein Raum für die Anwendung der lex-specialis-Regel. Art. 11 und Art. 12 DSGVO seien anwendbar. In Art. 12 Abs. 2 Satz 2 DSGVO sei die Frage der mangelnden Identifizierbarkeit des Antragstellers angesprochen. Der MB sei es bislang nicht gelungen, glaubhaft zu machen, dass sie nicht in der Lage sei, die betroffene Person hinsichtlich jener Standortdaten zu identifizieren, die mit dem zugeordneten Endgerät erzeugt worden seien. Der bloße Umstand, dass nicht mit Sicherheit ausgeschlossen werden könne, dass auch andere Personen den Mobilfunkvertrag bzw. das Mobiltelefon des BF benutzt haben könnten, sei noch keine Glaubhaftmachung iSd Art. 12 Abs. 2 Satz 2 DSGVO.

Es könne bei keinem internetfähigen bzw. GPS-fähigen Gerät bzw. bei keinem Online-Account jemals mit Sicherheit ausgeschlossen werden, dass dieses/dieser auch von anderen Personen als dem rechtmäßig dazu befugten Inhaber benutzt werde. Das habe aber nicht zur Folge, dass die erzeugten Daten sich nicht auf den rechtmäßigen Inhaber bezögen. Es gäbe für die MB keinen konkreten Grund daran zu zweifeln, dass die gegenständlichen Standortdaten

ausschließlich den BF betreffen. Insofern sei auch mit dem Verweis auf § 100 Abs. 3 TKG 2003 (§ 138 Abs 6 TKG 2021) bezüglich Schutz von Mitbenutzern nichts für die Position der MB gewonnen, da es gegenständlich keine Mitbenutzer des Mobilfunkvertrages bzw. des Mobiltelefons des BF gebe. Das Argument der MB, der Schutzzweck des § 100 Abs. 3 TKG 2003 (§ 138 Abs 6 TKG 2021) würde ausgehebelt, wenn eine Beauskunftung von Standortdaten gemäß Art. 15 DSGVO erfolge, gehe an der Sache vorbei, weil eine Datenkopie über Verkehrs- oder Standortdaten gemäß Art. 15 Abs. 3 DSGVO nicht dasselbe wie ein Einzelentgeltnachweis sei und es der MB offen stehe und diese auch gemäß Art. 15 Abs. 4 DSGVO verpflichtet sei, allfällige Informationen, deren Bereitstellung in die Datenschutzrechte anderer Personen eingriffen, entsprechend zu schwärzen bzw. sensible Passagen unkenntlich zu machen. Hierfür bedürfe es einer konkreten Kollisionslage, für die die MB als Verantwortliche die Beweislast trage. Dass nicht mit Sicherheit ausgeschlossen werden könne, dass der Mobilfunkvertrag bzw. das Mobiltelefon des BF auch von anderen Personen benutzt hätte werden können, berechtigte die MB nicht, die Beauskunftung von Standortdaten zu verweigern. Die Bezugnahme auf § 94 iVm §§ 102a ff TKG 2003 sei unzutreffend, weil die Übermittlung von personenbezogenen Daten an Behörden etwas vollkommen anderes sei, als die Bereitstellung einer Datenkopie an eine betroffene Person gemäß Art. 15 Abs. 3 DSGVO. Dass die MB auch bei der Bereitstellung einer Datenkopie gemäß Art. 15 Abs. 3 DSGVO angemessene Datensicherheitsmaßnahmen vorzusehen habe, ergäbe sich bereits aus Art. 5 Abs. 1 lit. f iVm Art. 32 DSGVO und habe nicht mit Datensicherheitsregeln im TKG 2003 zu tun. Verkehrs-/Standortdaten nicht gemäß Art. 15 Abs. 3 DSGVO zu beauskunften, weil der österreichische Gesetzgeber keine expliziten dem §§ 102a ff TKG 2003 entsprechenden Maßnahmen zur Sicherheit bei der Datenübermittlung vorgesehen habe, wäre eine Fehlinterpretation geltenden Rechts. Die MB übersehe, dass es sich bei Art. 15 DSGVO um ein subjektives Betroffenenrecht handle, welches in einer unter Anwendungsvorrang stehenden EU-Verordnung vorgesehen sei. Dieses könne nicht entfallen, weil ein nationaler Gesetzgeber keine spezielleren Vorschriften zur Sicherheit bei der Datenübermittlung erlassen habe.

1.4. Über Aufforderung vom 11.05.2021 der belangten Behörde, wonach nicht klar sei, ob sich der BF weiterhin in seinem Recht auf Auskunft betreffend Art. 15 Abs. 1 lit c verletzt erachte, erfolgte eine weitere **Stellungnahme vom 26.05.2021 des BF,** beinhaltend umfangreiches Vorbringen. Dieser führte insbesondere aus, dem BF sei nach wie vor unklar, an welchen Empfänger die MB seine personenbezogenen Daten tatsächlich übermittelt habe, insofern erachte er sich weiterhin in seinem Recht gemäß Art. 15 Abs. 1 lit c DSGVO verletzt. Die belangte Behörde möge die zur Klärung der tatsächlichen Situation notwendigen Sachverhaltselemente insbesondere durch Einschau in die Datenverarbeitungen in den

Geschäftsräumlichkeiten der MB untersuchen, den BF zu dieser Einschau laden, ihm sämtliche Ermittlungsergebnisse zukommen lassen und allenfalls einen Teilbescheid erlassen, der die Frage der Verletzung des Art. 15 Abs 1 lit c DSGVO ausklammere.

1.5.1 Mit dem bekämpften **Bescheid** gab die belangte Behörde der Beschwerde zu Spruchpunkt 1. teilweise statt und stellte fest, die MB habe den BF dadurch im Recht auf Auskunft verletzt, indem sie ihm keine Auskunft über die konkreten Datenempfänger erteilt habe, setzte zu Spruchpunkt 2. eine Frist zur Präzisierung, ob tatsächlich eine Datenübermittlung an die angeführten Empfänger erfolgt sei und wies zu Spruchpunkt 3. die Beschwerde „im Übrigen“ ab.

1.5.2. Die belangte Behörde traf dabei folgende Feststellungen:

A1 Telekom Austria AG
Lassallestraße 9
1020 Wien

Per E-Mail: service@georg.at

Antrag auf Auskunft gemäß Art 15 DSGVO

Sehr geehrte Damen und Herren,

Dies ist ein Antrag auf Auskunft gemäß Art 15 DSGVO. Ich ersuche um Zurverfügungstellung einer Kopie sämtlicher mich betreffender personenbezogener Daten und sämtlicher gemäß Art 15 Abs 1 DSGVO geforderten Informationen in Bezug auf:

[redacted]

Bitte beachten Sie, dass ich nicht gesetzlich dazu verpflichtet werden kann, ein internes Formular zur Ausübung meiner Rechte gemäß der DSGVO zu verwenden. Gerne können Sie mir zur Authentifizierung aber einen Bestätigungslink/-code per SMS zukommen lasssen.

Die Informationen, die ich anfordere, beinhalten:

Kopie meiner personenbezogenen Daten:

Alle über mich gewonnenen Daten, wie Meinungen, Rückschlüsse, Profile, Einstellungen und Vorlieben. Ich möchte eine Kopie aller meiner personenbezogenen Daten in elektronischer Form erhalten. Daten, die Ihnen in maschinenlesbarer Form zur Verfügung stehen, müssen mir in dieser Form zur Verfügung gestellt werden.

Insbesondere ersuche ich um Übermittlung sämtlicher zu meiner Person/Rufnummer gespeicherten Verkehrsdaten. Ich weise darauf hin, dass Art 15 DSGVO den Beschränkungen des § 99 TKG als unmittelbar anwendbare unionsrechtliche Bestimmung vorgeht und die Rechtsprechung der Datenschutzbehörde zur alten Rechtslage insofern ohne Relevanz ist. Zudem bezweckt § 99 TKG nicht eine Beschränkung des datenschutzrechtlichen Auskunftsanspruchs, sondern soll lediglich die Übermittlung an unbefugte Dritte verhindern.

Informationen zu Zwecken und Rechtsgrundlagen

Alle Verarbeitungszwecke und die gesetzliche Grundlage für diese Zwecke nach Kategorie der personenbezogenen Daten. Diese Liste muss nach Zweck, Rechtsgrundlage, die auf die Zwecke ausgerichtet ist, und nach Kategorien von Daten, die für diese Zwecke und auf Basis dieser Rechtsgrundlage(n) verarbeitet werden, aufgeschlüsselt sein. Separate Listen, in denen diese drei Faktoren nicht korrespondieren, sind nicht akzeptabel. Eine Tabelle kann der beste Weg sein, um diese Informationen anzuzeigen. Wenn Ihr Unternehmen sich auf berechtigte Interessen an der

[redacted]

Verarbeitung meiner personenbezogenen Daten stützt, bitte ich um eine Angabe der geltend gemachten berechtigten Interessen.

Informationen über die Verantwortlichen, die Auftragsverarbeiter, die Herkunft der Daten und deren Empfänger

- Die Identität aller (gemeinsamen) Verantwortlichen für meine personenbezogenen Daten.
- Alle Dritten, an die meine Daten weitergegeben wurden, einschließlich des Namens und der Kontaktdaten der Empfänger. Wenn Sie sich dafür entscheiden, Kategorien von Empfängern anstelle von konkreten Empfängern zu nennen, müssen Sie zumindest die Art des Empfängers, die Branche, den Sektor und den Teilsektor sowie den Standort der Empfänger angeben. Bitte beachten Sie, dass es bei übermittelten Daten, die auf der Grundlage meiner Einwilligung verarbeitet werden, keine Möglichkeit gibt, nur Kategorien von Empfängern zu nennen, ohne diese Rechtsgrundlage außer Kraft zu setzen.
- Wenn die Daten nicht bei selbst erhoben, beobachtet oder abgeleitet wurden, geben Sie bitte genaue Informationen über die Herkunft dieser Daten an, einschließlich des Namens und der Kontaktdaten der konkreten Datenquellen.

Informationen zur automatisierten Entscheidungsfindung

Bitte geben Sie an, ob Sie automatisierte Entscheidungen im Sinne von Artikel 22 DSGVO treffen oder nicht. Wenn die Antwort ja ist, geben Sie bitte aussagekräftige Informationen über die involvierte Logik, die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für mich, die Maßnahmen, die Sie zur Vermeidung von Fehlern, Verzerrungen und Diskriminierungen ergriffen haben, und wie ich meinen Standpunkt zum Ausdruck bringen und alle automatisierten Entscheidungen, die über mich getroffen wurden, in Frage stellen kann.

Informationen zur Speicherdauer

Bitte geben Sie an, wie lange personenbezogene Daten jeder Kategorie gespeichert werden oder nach welchen Kriterien die Entscheidung über die Speicherdauer getroffen wird. Bitte bestätigen Sie auch, wo meine personenbezogenen Daten physisch gespeichert sind (einschließlich Backups) und zumindest, ob sie zu irgendeinem Zeitpunkt die EU verlassen haben (wenn ja, geben Sie bitte auch die Rechtsgrundlagen und Sicherheitsvorkehrungen für solche Datenübertragungen außerhalb der EU an).

Bitte senden Sie Ihre Antwort auf gesichertem Wege per E-Mail an georg@contact.pasamail.net. Ich freue mich auf eine Antwort innerhalb eines Monats nach Eingang meines Antrags.

Mit freundlichen Grüßen

[redacted]

[redacted]

[redacted]

A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

Wien, 19.03.2020

Betreff: Auskunftsersuchen gemäß Artikel 15 Datenschutzgrundverordnung (DSGVO)

Sehr geehrter [redacted]

nachfolgend dürfen wir Sie über die Art der von uns zu verarbeitenden Daten und deren Behandlung unter Berücksichtigung der gesetzlichen Bestimmungen, insbesondere der Datenschutzgrundverordnung (DSGVO) in Verbindung mit unserer Datenschutzerklärung sowie des Telekommunikationsgesetzes (TKG 2003) in Verbindung mit unseren Allgemeinen Geschäftsbedingungen (AGB), informieren.

Stammdaten sind gemäß § 92 TKG 2003 alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter von Telekommunikationsdienstleistungen, oder soweit zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind.

Stammdaten sind Name, akademischer Grad, Anschrift, Teilnehmernummer und sonstige Kontaktinformationen für die Nachricht, Informationen über Art und Inhalt des Vertragsverhältnisses und Bonität.

Zum Gläubigerschutz kann eine Bonitätsabfrage durchgeführt werden. Die diesbezüglichen Dienstleister sind in unseren AGB und der Datenschutzerklärung ausgewiesen. Diese sind: Bisnode Austria GmbH (vormals Wirtschaftsauskunftei Wisur GmbH), Jakov-Lind Straße 4/2, A-1020 Wien, CRIF GmbH (vormals Deltavista GmbH), Diefenbachgasse 35/3/8, A-1150 Wien, Lowell Inkasso Service GmbH, Regensburger Straße 3, A-4020 Linz (vormals IS Inkasso Service GmbH & Co KG, Südtirolerstraße 9, A-4020 Linz), Kreditschutzverband 1870, Wagenseilgasse 7, A-1120 Wien. Eine externe Bonitätsabfrage erfolgte nicht.

Stammdaten werden nach Beendigung der Rechtsbeziehung mit dem Teilnehmer gelöscht. Ausnahmen sind zulässig, wenn diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden (dreimonatige Einspruchsfrist) zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen, wie etwa gemäß Bundesabgabenordnung (BAO) oder Unternehmensgesetzbuch (UGB). Die Stammdaten werden aus Gründen der ordnungsgemäßen Buchführung und anhängigen Prüfungen durch die Finanzbehörde bis zu zehn Jahre (ab Vertragskündigung) aufbewahrt. Gesetzliche Grundlage dafür ist § 207 Abs. 2 BAO. Bücher und Aufzeichnungen sowie die zu den Büchern und Aufzeichnungen gehörigen Belege sind noch so lange aufzubewahren, als sie für die Abgabenerhebung betreffende anhängige Verfahren von Bedeutung sind. Dies kann bei Rechnungen (Stammdaten) der Fall sein. Zusätzlich wird der Zugriff auf die genannten Daten im Sinne des Artikel 32 DSGVO eingeschränkt.

A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

Verkehrsdaten sind gemäß § 92 TKG 2003 Daten, die zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorganges verarbeitet werden; diese sind etwa aktive und passive Teilnehmernummern, IP-Adressen, Logdaten, Zeitpunkt und Dauer der Verbindung, oder die übermittelte Datenmenge.

Gemäß § 99 TKG 2003 werden Verkehrsdaten, außer in den gesetzlich geregelten Fällen, grundsätzlich nicht gespeichert und werden von uns als Netzbetreiber unverzüglich gelöscht oder zu anonymisiert. Sofern dies für den Zweck der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungsleistungen, erforderlich ist, haben wir jedoch das Recht die Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Die Einspruchsfrist von drei Monaten beginnt je nach Kunde (Erhalt der Rechnung) unterschiedlich und ist diesbezüglich ein entsprechender Postlauf bzw. interner Prozess bei Aufnahme eines allfälligen Rechnungseinspruches zu berücksichtigen. Um die diesbezüglichen Rechte des Kunden zu wahren, sowie eine lückenlose Aufklärung allfälliger Rechnungseinsprüche zu gewährleisten, ergibt sich insgesamt eine bis zu sechsmonatige Speicherdauer für Verkehrsdaten. Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung nicht gelöscht werden.

Verkehrsdaten dürfen gemäß § 96 TKG 2003 in Verbindung mit unseren AGB und der Datenschutzerklärung mit Zustimmung des Teilnehmers zur Vermarktung für den Zweck der eigenen Telekommunikationsdienste verwendet werden.

Der Kunde kann gemäß unseren AGB iVm mit unserer Datenschutzerklärung seine jederzeit widerrufbare Zustimmung seiner Datenschutz-Einstellungen zur Verwendung der Stamm- und Verkehrsdaten erteilen, dies zur bedarfsgerechten Angebotslegung, Servicierung und zur Bereitstellung von Diensten mit Zusatznutzen, zur Unterbreitung persönlicher Handy- sowie Produkt- und Serviceangebote durch A1 Telekom Austria AG auch mittels SMS/MMS, E-Mail und Telefon, sowie an Wirtschaftsauskunfteien zum Zweck von Bonitätsabfragen. Die betreffenden Unternehmen sind in unseren AGB (Pkt. 26) bzw. in unserer Datenschutzerklärung konkret bezeichnet. Der Kunde kann auch weiteren in unserer Datenschutzerklärung genannten Verarbeitungszwecken zustimmen.

Eine Auswertung von Verkehrsdaten, Inhaltsdaten und Standortdaten stellt gemäß § 94 TKG 2003 in Verbindung mit §§ 134 Z. 2 und 135 Z. 2 Strafprozessordnung (StPO) eine Überwachung des Fernmeldeverkehrs dar. Im Rahmen eines Strafverfahrens werden nach vorliegender Anordnung nur der zuständigen Staatsanwaltschaft, entsprechend der gesetzlichen Bestimmungen, die notwendigen Daten, über einen besonders geschützten Übertragungsweg, zur Verfügung gestellt.

A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

Standortdaten, sind gemäß § 92 TKG 2003, Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationseinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben.
Gemäß § 102 TKG 2003 werden andere Standortdaten als Verkehrsdaten nur verarbeitet wenn sie anonymisiert oder die Benutzer bzw. Teilnehmer eine jederzeit widerrufbare Einwilligung gegeben haben.

Gestützt auf die Entscheidung der Datenschutzbehörde - DSB-D122.418/0002-DSB/2016 – erteilen wir keine Auskunft über Standortdaten, da der Nutzer der Rufnummer (SIM-Karte), nicht ausreichend nachweisen kann, dass nur er selbst die Rufnummer (SIM-Karte) ausschließlich nutzt.

Im Rahmen der gesetzlichen Mitwirkungspflicht (§ 94 TKG 2003) erteilen wir nur den Behörden gemäß § 98 TKG 2003, § 53/3b Sicherheitspolizeigesetz (SPG) sowie §§ 134-138 Sicherheitspolizeigesetz (StPO) Auskunft, zu Standortdaten.

Inhaltsdaten sind gemäß § 92 TKG 2003 die Inhalte übertragener Nachrichten, die gemäß § 101 TKG 2003 grundsätzlich nicht gespeichert werden. Sofern die Speicherung des Inhaltes Dienstmerkmal ist, werden die Daten unmittelbar nach der Erbringung des Dienstes gelöscht.

Gemäß § 96 TKG 2003 werden Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten nur für den Zweck der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet.

Gemäß unseren AGB (Pkt. 26) können wir auch sonstige personenbezogene Daten, die Sie oder Dritte uns bei der Vertragsanbahnung oder während des Vertragsverhältnisses zur Verfügung stellen: z.B. Geburtsdatum, Beruf, Ausweisdaten, oder Bankverbindung speichern. Unter den Begriff der sonstigen personenbezogenen Daten fallen keine sensiblen Daten iSd Datenschutzgesetzes.

Gemäß § 93 TKG 2003 unterliegen wir dem Kommunikationsgeheimnis, und achten wir sehr genau darauf, dass dieses eingehalten wird.

A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

Folgende Daten sind gespeichert:

Name	[redacted]
Geburtsdatum	
Ausweistyp	
Ausweisnummer	
Nationalität	
Angebotslegung	
Vertragsart	
Kundennummer	
Rufnummer	
SIM-Karten-Nummer	
Aktivierung	
Tarif	
Status	

A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

Herkunft der Daten

Die oben angeführten, gespeicherten Daten erhalten wir durch Bekanntgabe, durch den Vertragspartner, beziehungsweise sind diese zur Vertragserfüllung notwendig. Verkehrsdaten, Standortdaten und Inhaltsdaten entstehen bei der Inanspruchnahme unserer Kommunikationsdienste.

Zweck der Datenverwendung

Die ermittelten Daten werden von A1 Telekom Austria AG zum Zweck der Erbringung von Telekommunikationsdienstleistungen verarbeitet.

Rechtsgrundlagen

Die Rechtsgrundlagen für die Verarbeitung Ihrer Daten durch uns sind insbesondere das TKG 2003, das DSG und die DSGVO, sowie damit in Verbindung stehende Verordnungen.

A1 Telekom Austria AG besitzt unter anderem Gewerbeberechtigungen für:

- Handelsgewerbe, eingeschränkt auf den Einzelhandel (Freies Gewerbe)
- Uneingeschränktes Handelsgewerbe (Freies Gewerbe)
- Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik (Freies Gewerbe)
- Elektrotechnik/Errichtung von Alarmanlagen (§ 106 GewO 1994)
- Betrieb eines Callcenters (Freies Gewerbe)
- Internet, Einrichtung und Wartung von Netzdienste, einschließlich der Programmierung von elektronisch zu verteilenden Informationen - Content Providing (Freies Gewerbe)

DVR-Nummer (Verfahrensverzeichnis)

Unsere DVR-Nummer lautet: 0962635

Überlassung von Daten (Auftragsverarbeiter)

Insoweit A1 Telekom Austria AG Auftragsverarbeiter in Anspruch nimmt, werden diese Daten ausschließlich entsprechend des von uns erteilten Auftrags verarbeitet. Die Daten werden allein für das Erbringen der Auftragsverarbeitung überlassen. Unsere Auftragsverarbeiter sind nicht berechtigt, über die Verwendung von überlassenen Daten eigenverantwortlich zu entscheiden.

Löschung von Daten

Die Daten werden unter Berücksichtigung der gesetzlichen Bestimmungen, der DSGVO, des DSG, des TKG 2003, in Verbindung mit unseren AGB, unserer Datenschutzerklärung sowie der Bundesabgabenordnung (BAO) und des Unternehmensgesetzbuch (UGB), gelöscht. Steuer- bzw. abgabenrechtlich relevante Daten müssen daher auch nach Kündigung bis zum Ablauf der diesbezüglichen Fristen gespeichert werden.

A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

Vorratsdaten

Am 27. Juni 2014 hat der Verfassungsgerichtshof (G 47/2012) die gesetzlichen Regelungen zur Vorratsdatenspeicherung als verfassungswidrig aufgehoben. Seit wirksam werden des Verfassungsgerichtshoferkenntnis am 1. Juli 2014 speichert A1 Telekom Austria AG keine Vorratsdaten mehr. Alle bis zu diesem Zeitpunkt gespeicherten Vorratsdaten wurden gelöscht.

Datensicherheit

A1 besitzt ein eigenes Information Security Management System (ISMS), in dem alle unsere Sicherheitsprozesse geplant werden, ablaufen und regelmäßig überprüft werden. Im Rahmen von jährlichen Untersuchungsverfahren (Audits) wird mit dem weltweit anerkannten Sicherheitsstandard / Zertifikat - ISO 27001-Zertifizierung - die Qualität unseres ISMS bestätigt. Mehrstufige technische Schutzvorkehrungen gegen Schadprogramme (Malware), Firmware, Vorbeugemaßnahmen gegen Datenverlust etc. sind implementiert. Regelmäßig werden umfangreiche Überprüfungen der Sicherheit durch: Audits, Überprüfungen für Schadenpotenzial, Penetration-Tests etc. durchgeführt. Ein zertifiziertes Technik-Team überwacht ständig die Situation und ergreift bei Bedarf die notwendigen Gegenmaßnahmen.

Wir hoffen, Ihr Anliegen zur Zufriedenheit erledigt zu haben.

Freundliche Grüße

Ihr A1/Georg Datenschutzteam

Beilage: Datenschutz-Einstellungen
Farberklärung zu den Datenschutz-Einstellungen

Ihre Datenschutzeinstellungen können Sie entsprechend der Datenschutzgrundverordnung (DSVGO) jederzeit wie folgt ändern:

- Via georg! Kontomanager/APP
- Via Kundendienst 0681 840 610
- Via Mail an: service@georg.at
- Schriftlich an Georg, Postfach 0621, 1010 Wien

Bitte geben Sie immer Ihr Kundenkennwort an.
Bei schriftlicher Kontaktaufnahme zeichnen Sie Ihr Schreiben mit Unterschrift.

Weitere Informationen zum Datenschutz finden Sie unter www.yesss.at (www.a1.net).

Datenschutzeinstellung zur Rufnummer [redacted]

Datenschutzbestimmungen

Zusendung von Produktinformationen & Angeboten	[redacted]
E-Mail	
SMS	
Telefon	
Post	
Social Media	
Personalisierte Angebote & Weiterentwicklung unserer Services	
Personalisierte Angebote	
Nutzung unserer Services	
Big Data Analysen	
Weitergabe von Daten	
Telekom Austria Group Tochterunternehmen & Vodafone Global Enterprise Limited	
paybox	
Partnerunternehmen	

Datenschutz Einstellungen - Erklärung

	Status
Datenschutz bei A1	
Zusendung von Produktinformationen & Angeboten	
Telefonisch	
Per E-Mail	
Per SMS	
Per Post	
Über Social Media (z.B. Facebook, Instagram)	
Personalisierte Angebote & Weiterentwicklung unserer Services	
Personalisierte Angebote	
Nutzung unserer Services	
Big Data Analysen	
Weitergabe von Daten	
Telekom Austria Group Tochterunternehmen und Vodafone Global Enterprise Limited	
Paybox	

Statusanzeige zur Zustimmung der Punkte darunter:
Rot: Kunde hat nirgendwo zugestimmt
Gelb: Kunde hat unterschiedliche Aussage gemacht
Grün: Kunde hat überall zugestimmt

Statusanzeige zur Zustimmung der Punkte darunter:
Rot: Kunde hat nirgendwo zugestimmt
Gelb: Kunde hat unterschiedliche Aussage gemacht
Grün: Kunde hat überall zugestimmt

Statusanzeige zur Zustimmung:
Rot: Kunde hat nicht zugestimmt
Gelb: Kunde hat noch keine Aussage gemacht
Grün: Kunde hat zugestimmt

Statusanzeige zur Zustimmung:
Rot: Kunde hat nicht zugestimmt
Gelb: Kunde hat noch keine Aussage gemacht
Grün: Kunde hat zugestimmt

Statusanzeige zur Zustimmung:
Rot: Kunde hat nicht zugestimmt
Gelb: Kunde hat noch keine Aussage gemacht
Grün: Kunde hat zugestimmt

[redacted]

[redacted]

Sehr geehrter Herr [redacted]

wie bereits im der Art 15 Auskunft erörtert ist die Übermittlung von Verkehrs- und Standortdaten nur in dem im Telekommunikationsgesetz (TKG) vorgesehenen Umfang möglich. Verkehrsdaten werden daher gemäß § 100 TKG nur im Umfang eines Einzelentgeltnachweis (rückwirkend als verkürzter Einzelentgeltnachweis) zur Verfügung gestellt. Sie können ihre Einzelentgeltnachweise selbst im Kontomanager einsehen. Standortdaten können nur in gesetzlich geregelten Fällen (wie etwa gemäß § 98 TKG an Notrufträger) übermittelt werden.

[redacted]

Gerne übermittle ich Ihnen auch die Zusammenfassung der zitierten Entscheidung der Datenschutzbehörde, die diese im Datenschutzbericht 2016 veröffentlicht hat.

Bescheid vom 15.4.2016, DSB-D122.418/0002-DSB/2016 (Auskunftsrecht gegenüber einem Mobilfunkunternehmen, Standortdaten, Cell-ID):
Die Beschwerdeführerin verlangte von einer ein Mobilfunknetz betreibenden Kapitalgesellschaft (Beschwerdegegnerin) Auskunft über die gespeicherten Standortdaten von zwei ihr zuzuordnenden Mobilfunkanschlüssen in einem bestimmten Zeitraum. Dazu verwies sie auf die Pflicht der Beschwerdegegnerin gemäß § 90 Abs. 8 TKG 2003. Die Beschwerdegegnerin verweigerte diese Auskunft mit der Begründung, eine Verwendung solcher Verkehrsdaten sei nur in bescheinigten Notfällen für Notfalldienste oder in polizeilichen Ermittlungsverfahren bzw. auf richterliche Anordnung hin zulässig. Die Datenschutzbehörde hielt in ihrem Bescheid fest, dass keine Feststellung erfolgen konnte, dass die Beschwerdeführerin im Zeitraum, für den Auskunft verlangt wurde, stets die „tatsächliche Nutzerin" der den Anschlüssen zuzurechnenden Geräte war. In Großstädten sind die Funkzellen von Mobilfunknetzen klein (300 bis 500 m Durchmesser und ermöglichen allein durch das Einbuchen der mobilen Telekommunikationsendeinrichtung in die nächstgelegene Funkzelle auf Grund der verarbeiteten Cell-ID eine Standortbestimmung des jeweiligen Nutzers des Mobiltelefons. Der Teilnehmer (Vertragsinhaber) kann auf Grund häufiger Ausnahmen (z.B. Kinder, Unternehmensanschlüsse) nicht mit dem tatsächlichen Nutzer gleichgesetzt werden. Das Fernmelderecht räumt gemäß §§ 92 Abs. 1 iVm 100 Abs. 1 TKG 2003 dem Betroffenen nur ein auf den Erhalt eines Einzelentgeltnach-weises eingeschränktes Recht ein, über gespeicherte Verkehrsdaten Auskunft zu erhalten. Auch diese Beschränkung geht als Spezialvorschrift dem allgemeinen Auskunftsrecht gemäß § 26 DSG 2000 vor. Da die Beschwerdegegnerin die Auskunft begründet abgelehnt hatte, wurde die Beschwerde abgewiesen. Der Bescheid ist rechtskräftig.

Zur Verarbeitung von Verkehrsdaten in anonymisierter Form darf ich Sie wie folgt informieren:

A1 bietet gemeinsam mit Invenium, einem Spin Off der TU Graz, Bewegungsanalysen an, die aus vollständig anonymisierten Daten mittels Algorithmen errechnet werden. Mit diesen Daten ist es möglich, die Bewegungsströme von Menschengruppen zu visualisieren. Damit ist es beispielsweise möglich zu sehen, woher Touristen kommen die Sehenswürdigkeit A besichtigen, und welche Sehenswürdigkeit danach angesteuert wird. Die Lösung ist DSGVO-konform und TÜV-geprüft.

Derartige Technologien werden europaweit von einer Vielzahl an Unternehmen angeboten.

Das verwendete Anonymisierungsverfahren wurde nach aktuellem Stand der Technik entwickelt und vom TÜV Saarland zertifiziert. Wichtige Eckpunkte sind dabei:

- Es ist durch diese Analysen nicht möglich, auf einzelne Personen zu schließen, es können lediglich aggregierte Bewegungsströme von Gruppen analysiert werden (zb. kann nicht ausgesagt werden, dass 3 Personen von A nach B gehen. Es kann nur ausgesagt werden, dass sich „bis zu 20 Personen" bewegen. Ab 21 Personen „bis zu 40", usw.). Niemals wird eine Bewegungskette erstellt, die einer Person zuzuordnen ist. Die Analyse arbeitet mit hochspeziellen Rechenmodellen, die statistische Bewegungsmodelle berechnet.
- Die räumliche Komponente einer solchen Bewegungsstromanalyse ist ein Näherungs-/Mittelwert, basierend auf den Mobilfunkzellen in der Nähe. Dies ist mit punktgenauen GPS-Daten, wie sie etwa Navigations-Apps verwenden, in keiner Weise zu vergleichen. Die Genauigkeit entspricht einem errechneten Wert für ein größeres Gebiet. Die tatsächliche Lokation des Endgeräts kann auch außerhalb dieses Gebiets sein, es handelt sich um eine „Wahrscheinlichkeit". Abhängig von dem von einem Sender abgedeckten Bereich kann die Unschärfe auch mehrere Hundert Meter oder einige Kilometer betragen.
- Es handelt sich um keine Echtzeit-Analyse. Die Analyseergebnisse liegen immer erst nach Abschluss des 24-Stunden-Zyklus vor. „Live-Beobachtungen" sind daher nicht möglich.
- Der Analysezeitraum ist immer auf 24 Stunden begrenzt. Danach wird der Anonymisierungsschlüssel gelöscht und ein neuer Schlüssel generiert, sodass keine Analyseergebnisse über einen längeren Zeitraum verknüpft werden können.

Es werden lediglich die Analyseergebnisse (Bewegungsströme) Dritten zur Verfügung gestellt, niemals die der Analyse zugrunde liegenden, anonymisierten Rohdaten. Diese geben wir keinesfalls an Dritte weiter, so dass selbst der Versuch einer De-Anonymisierung unmöglich ist.

Da keine personenbezogenen Daten, sondern lediglich anonymisierte Daten verarbeitet werden, ist hierfür die Notwendigkeit einer Rechtsgrundlage gem. Art. 6 DSGVO, wie etwa einer Zustimmung, nicht gegeben. Wir informieren über die Verarbeitung zur Erstellung von Bewegungsstromanalysen

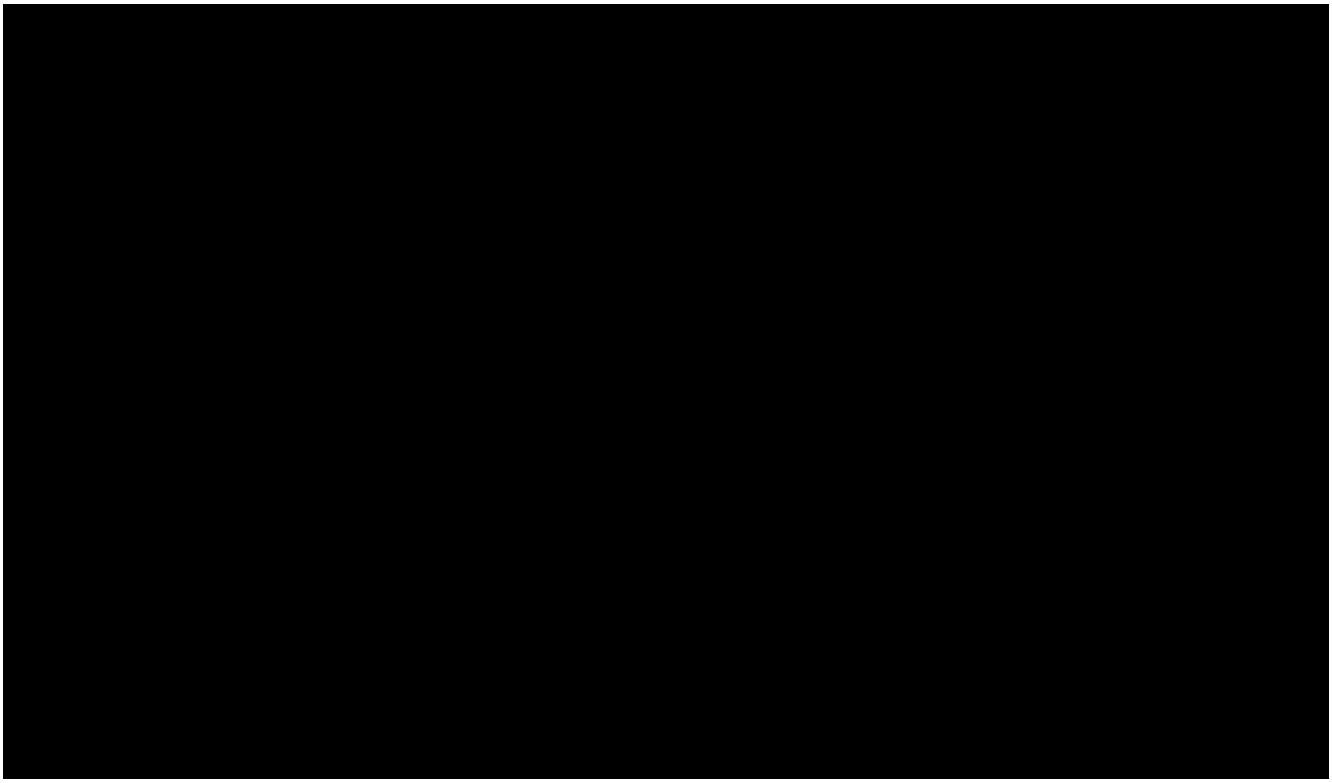
in unserer Datenschutzerklärung und auf unserer Webseite unter https://www.a1.net/datenschutz und bieten zudem freiwillig ein Opt-out Service für jene Kunden an, die eine solche anonymisierte Verwendung ihrer Daten nicht möchten.

Ich hoffe, Ihre Fragen mit meinen Ausführungen beantwortet zu haben.

Beste Grüße,

[redacted]

A1 Telekom Austria AG
Lassallestraße 9 1020 Wien



A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

[redacted]

[redacted]

Beilage ./2

Wien, 4.9.2020

Ergänzende Auskunft – Alan Dahi

Sehr geehrter Herr Dahi,

wir haben von der Datenschutzbehörde eine Aufforderung zur Stellungnahme wegen einer behaupteten Verletzung im Recht auf Auskunft erhalten.

Wir werden zu den einzelnen Beschwerdepunkten selbstverständlich im Verfahren ausführlich Stellung nehmen. Dennoch hoffen wir, einzelne Themenbereiche bereits vorab durch eine ergänzende Auskunft aufklären zu können. Wir werden dieses Schreiben natürlich auch der Datenschutzbehörde, gemeinsam mit unserer Stellungnahme, zur Kenntnis bringen.

1) Intransparente Verweise / fehlende Dokumente

Sie weisen darauf hin, dass in der übermittelten Auskunft zwar auf die Datenschutzerklärung und die Allgemeinen Geschäftsbedingungen (AGB) verwiesen werde, diese aber weder beigelegt wären, noch Links bereitgestellt würden.
Dies ist korrekt, die entsprechenden Dokumente sind aber aus unserer Sicht leicht auf der Produktwebseite www.georg.at auffindbar, und entsprechen daher auch dem Transparenzgebot. Es handelt sich hierbei um Ergänzungen zur umfassenden in der Auskunft gegebenen Information. Wir nehmen den Punkt dennoch gerne auf, und werden unser Standardschreiben auf entsprechende Verbesserungsmöglichkeiten überprüfen.
Die entsprechenden AGB und die Datenschutzerklärung übermitteln wir in der Anlage zu diesem Schreiben.

2) Rechtsgrundlagen

In der Datenschutzerklärung werden ausführlich die Datenverarbeitungen, die nur mit Einwilligung der Kunden durchgeführt werden, beschrieben. Wir nehmen ihren Kritikpunkt jedoch ernst und werden den Text der Artikel-15 Auskunft zukünftig anpassen, um alle Rechtsgrundlagen in einem Dokument zusammen zu fassen.

3) Empfänger der personenbezogenen Daten

In Entsprechung der in dem erst nach Auskunftserteilung an Sie am 2.6.2020 ergangenen Bescheid DSB D124.218 vertretenen Rechtsansicht der Datenschutzbehörde ergänzen wir unsere Auskunft durch die Nennung konkreter Empfänger, die für uns als Auftragsverarbeiter inhaltlich mit der Verarbeitung personenbezogener Daten befasst sind. Eine Gliederung nach Themenbereichen soll der besseren Übersichtlichkeit dienen.

- Logistik und Versand:

Unser Logistikpartner ist die mk Logistik GmbH, Dietersdorfer Straße 13, 2201 Hagenbrunn. Der Versand unserer Waren erfolgt über die österreichische Post AG. Bei Kunden-Direkt-Mailings unterstützt uns auch die Nullacht Sechzehn Printproduktion Gmbh, Türkenstrasse 15/2, 1090 Wien. Der elektronische Versand von Marketinginformationen an Kunden kann durch uns selbst oder durch die eyepin GmbH, Billrothstraße 52, 1190 Wien erfolgen.

- Service:

Wir stehen unseren Kunden für Anfragen über verschiedenste Kontaktmöglichkeiten gerne zur Verfügung. Unsere Service-Center betreiben wir zum Großteil selbst. Den Nachtdienst übernimmt für uns Customer Care Solutions Call & Assistance Center Betriebs GmbH, 1080 Wien, Skodagasse 28/5.
Die telefonische Kontaktierung von Kunden (Outbound Calls) kann auch über die Firma Herrgesell Elfriede– telepower, Haeckelstraße 23 a, 1230 Wien, oder die Telebiz GmbH, Zieglergasse 2/2, 1070 Wien erfolgen.
Die PAYBOX Service GmbH, Lassallestraße 9, 1020 Wien unterstützt uns bei der Identifizierung von Kunden (Sim-Karten-Registrierung).

- Vertriebspartner:

Der Abschluss von Verträgen und verschiedene andere Serviceleistungen in Zusammenhang mit unserem Produkt „Georg" können auch durch unsere ausgewählten Vertriebspartner erbracht werden. Dies sind die Media Markt TV-HiFi-Elektro Ges.m.b.H., und die Saturn Elektro-Handelsges.m.b.H., jeweils mit einer Vielzahl an Standorten in ganz Österreich.

- Rechnungslegung und Bezahlung:

Sofern Sie Ihre Rechnung per Post erhalten, erfolgt der Rechnungsdruck durch die D2D – direct to document GmbH, 1230 Wien, Halban-Kurz-Straße 11.
Bezahlen Sie Ihre Rechnung mittels SEPA-Lastschrift oder Kreditkarte, so arbeiten wir hierfür mit Banken, Kreditkartenunternehmen und anderen Zahlungsdiensteabwicklern zusammen. Bei Abwicklungen von Kreditkartenzahlungen arbeiten wir zudem mit der Wirecard Central Eastern Europe GmbH, Reininghausstraße 13a, 8020 Graz zusammen.

- Zahlen mit der Handyrechnung:

A1 ermöglicht Ihnen, Einkäufe bei dritten Diensteanbietern zu autorisieren und die Bezahlung über Ihre Handyrechnung abzuwickeln. Im Zuge der Zahlungsautorisierung ist es erforderlich, Ihre Rufnummer an den jeweiligen Diensteanbieter zu übermitteln, damit dieser Ihre Bestellung und Zahlung zuordnen kann. Detaillierte Informationen zu diesem Dienstleister können Sie vor einem solchen Einkauf im Zuge des Bestellprozesses abrufen.

4) Speicherdauer

Konkrete Informationen zur Aufbewahrung bestimmter Datenarten einschließlich zeitlicher Angaben finden sich in der Datenschutzerklärung (Seite 2 – Pkt.: „So lange bewahren wir Ihre Daten im Einzelnen auf").

5) Drittquellen

Hinsichtlich der Frage, ob konkret bei Ihren Daten Drittquellen herangezogen wurden, möchten wir Sie wie folgt informieren.

Da es sich bei Ihrem Vertragsverhältnis um ein Prepaid-Produkt handelt, wurde keine Bonitätsabfrage bei einer Auskunftei durchgeführt.

Gerne halten wir auch fest, dass keine Daten von anderen Drittquellen verwendet wurden.

A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

6) Sonstiges

In Hinblick auf die restlichen Beschwerdepunkte, und insbesondere die Frage der Beauskunftung von Verkehrs- und Standortdaten, möchten wir darauf hinweisen, dass unsere in der Art 15 Auskunft und der anschließenden Korrespondenz vertretene Rechtsmeinung in der am 2.6.2020 ergangenen Entscheidung DSB D124.218 der Datenschutzbehörde bestätigt wurde. Auch nach Inkrafttreten der DSGVO vertritt die Datenschutzbehörde die Rechtsansicht, dass die TKG Regelungen als lex specialis diesbezüglich dem Auskunftsrecht nach Art 15 DSGVO vorgehen. Es bedürfte demnach einer Änderung der gesetzlichen Bestimmungen, andernfalls würden wir uns bei einer Beauskunftung strafbar machen.

Beste Grüße,

[redacted]

1.5.3. Zum abweisenden Spruchpunkt 3. führte die belangte Behörde rechtlich aus wie folgt:

Die Datenschutzbehörde habe sich bereits vor In-Geltung-Treten der DSGVO im Bescheid vom 27. März 2017, GZ DSB-D122.616/0006-DSB/2016, mit der Frage beschäftigt, ob „Standortdaten“ iSd § 92 Abs. 3 Z 6 TKG 2003 (das seien Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzes eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Telekommunikationsendeinrichtungen, die Adresse der Einrichtung) im Rahmen einer datenschutzrechtlichen Auskunft zu beauskunften seien. Nichts anderes könne nach neuer Rechtslage gelten, zumal auch nach In-Geltung-Treten der DSGVO weiterhin die Bestimmungen des TKG 2003 hier maßgeblich seien, weil die datenschutzrechtlichen Bestimmungen der §§ 92 ff TKG 2003 auf den Vorgaben der Richtlinie 2002/58/EG (e-Privacy-Richtlinie) fußten und diese als lex specialis der DSGVO vorgingen (siehe dazu Art. 95 DSGVO). Art. 23 DSGVO sei diesfalls nicht einschlägig. Es sei daher bereits aufgrund dieser Erwägungen davon auszugehen, dass die MB zu Recht die Beantwortung des Auskunftsbegehrens verweigert habe, da eine Feststellung, ob es sich bei den verfahrensgegenständlichen Standortdaten (nur) um Daten des Auskunftswerbers handele, nicht möglich gewesen sei. Daran ändere auch die vom BF in Vorlage gebrachte eidesstattliche Erklärung nichts, weil auch dadurch kein objektiver, dh für jedermann nachvollziehbarer Nachweis erbracht werde, dass der BF zu jedem Zeitpunkt des von ihm angegebenen Zeitraumes tatsächlicher Nutzer des Endgerätes gewesen sei. Bei Verkehrsdaten handle es sich gemäß § 92 Abs. 3 Z 4 TKG 2003 um Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet würden. Die Speicherung bzw. Übermittlung dieser Daten richte sich gemäß § 99 Abs. 1 TKG 2003 nach den Bestimmungen dieses Gesetzes und sei nur eingeschränkt möglich. Wie bereits die Datenschutzkommission ausgesprochen habe, räume das Fernmelderecht gemäß §§ 92 Abs. 1 iVm 100 Abs. 1 TKG 2003 dem Betroffenen nur ein auf den Erhalt eines Einzelentgeltnachweises eingeschränktes Recht ein, über gespeicherte Verkehrsdaten Auskunft zu erhalten. Diese Beschränkung gehe als lex specialis dem allgemeinen Auskunftsrecht vor.

Die MB habe daher zu Recht die Auskunft der Verkehrsdaten verweigert. Ihm stellten sich zur Beauskunftung von Verkehrsdaten dieselben Fragen wie zur Beauskunftung von Standortdaten, weshalb auf die diesbezügliche Begründung verwiesen werde.

1.6. Allein gegen Spruchpunkt 3. richtet sich die **Beschwerde** des BF „soweit die Abweisung des Antrags auf Bereitstellung einer Kopie von Standort- und Verkehrsdaten (einschließlich Standortkennung) nach Art. 15 Abs. 3 DSGVO betroffen ist“ wegen unrichtiger rechtlicher Beurteilung mit den Anträgen, festzustellen, dass die MB gegen Art. 15 Abs. 3 DSGVO verstoßen habe, indem sie dem BF keine vollständige Kopie ihn betreffender Verkehrs-, Standortdaten und Standortkennungen iSd TKG zur Verfügung gestellt habe. Der MB sei aufzutragen, dem BF innerhalb einer Frist vollständige Kopien ihn betreffender derartiger Daten zur Verfügung zu stellen. Hilfsweise werde ein Aufhebungsantrag gestellt.

1.7. Die **belangte Behörde legte die Beschwerde samt dem elektronischen Verwaltungsakt dem Bundesverwaltungsgericht einlangend am 24.11.2021 vor**. Sie bestritt das Beschwerdevorbringen zur Gänze, beantragte, die Beschwerde abzuweisen und brachte im Wesentlichen vor:

Die Rechtsprechung der Datenschutzbehörde vor dem Inkrafttreten der DSGVO habe nach wie vor Bestand, da die zitierten einschlägigen telekommunikationsrechtlichen Vorgaben seither keine inhaltliche Änderung erfahren hätten. Europarechtliche Grundlage sei nach wie vor die Richtlinie 2002/58/EG, welche zunächst im TKG 2003 und nunmehr im TKG 2021 umgesetzt worden sei. Darüber hinaus weise bereits der Wortlaut des Art. 15 Abs. 1 Satz 1 DSGVO eine klare, diesbezügliche Einschränkung auf:
„Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, **ob sie betreffende personenbezogene Daten** verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten.“

In der englischen Version der DSGVO laute Art. 15 Abs. 1 Satz 1
„The data subject shall have the right to obtain from the controller confirmation as to whether or not **personal data concerning him or her** are being processed, and, where that ist the case, access to the personal data and the following information: (…)“

Eine ähnliche Formulierung finde sich in Erwägungsgrund 63, 1. Satz leg. cit:
„Eine betroffene Person sollte ein Auskunftsrecht hinsichtlich **der sie betreffenden** personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können.“

Wie die Datenschutzbehörde in ihrem Bescheid vom 18. April 2019, GZ D122.913/0001-DSB/2019 ausgesprochen habe, sei eine Auskunft gemäß Art. 15 DSGVO auf eigene Daten beschränkt, also auf Daten, die – nach dem Wortlaut des Art. 15 DSGVO – „sie – dh. die betroffene Person – betreffende personenbezogene Daten“ seien. Die belangte Behörde hege keinen Zweifel, dass der BF Vertragspartner der MB sei, doch könne allein daraus nicht mit der dafür erforderlichen Wahrscheinlichkeit und Sicherheit gefolgert werden, dass der BF sein Endgerät zu jedem Zeitpunkt auch physisch im Besitz gehabt bzw. selbst bedient habe. Dies lasse sich objektiv gesichert mit derzeit verfügbaren Methoden nicht feststellen. Darüber hinaus handle es sich bei den im Rahmen der Auskunft begehrten „Standortdaten“ um technische Betriebsdaten des Kommunikationsnetzbetreibers. Die Erfassung eines Endgerätes zu einem bestimmten Zeitpunkt in einem definierten Einzugsbereich eines Funkmasts (also die sogenannten Standortdaten) erfolge ausschließlich zu technischen Betriebszwecken, da die Erfassung der Standortdaten zur korrekten Weiterleitung eines Anrufes erforderlich sei. Dies bedeute konkret anhand eines Beispiels, dass das Mobiltelefon des BF im Mast XXX1 (bspw. Klagenfurt, St. Veiter Ring) am 19. November 2021 zwischen 12:42 und 15:00 Uhr deshalb erfasst werde, weil ein Anruf am Mobilfunkendgerät am 19.11.2021, um 13:00 Uhr, „technisch“ zum betreffenden Funkmasten XXX1 (Klagenfurt, St. Veiter Ring) durchgeleitet und adressiert werde, damit die Erreichbarkeit des Mobilfunktelefons gegeben sei. Dies sei einer der wesentlichen Unterschiede zu den vom BF angeführten Beispielen zu inhaltlichen Chat-Nachrichten, inhaltlichen Smart Watch Daten und der Viewing Historiy eines Streaming Accounts. Auch unter diesem Aspekt sei die Qualifikation von Standortdaten als den „Beschwerdeführer betreffende Daten“ im Sinne des Art. 15 Abs. 1, Satz 1 DSGVO zu verneinen. Standortdaten seien, vereinfacht ausgedrückt, Daten, die das mobile Endgerät produziert, ohne dass es darauf ankomme, wer der jeweilige Inhaber sei. Insofern würden einseitige Beteuerungen bzw. Aussagen des BF ins Leere gehen und keine objektiv gesicherte Methode darstellen, dass der BF auch tatsächlich im ständigen physischen Besitz des Endgerätes gewesen sei. Werde ein mobiles Endgerät – wenn auch nur für kurze Zeit – durch jemand anderen benutzt bzw. mit sich getragen (was dazu führe, dass Standort- und auch Verkehrsdaten durch das Einwählen in eine Funkzelle anfielen), lägen für diesen Zeitraum keine den BF betreffende Daten zu seiner Person vor. Dass mobile Endgeräte nicht stets durch den Vertragsinhaber als Auskunftswerber benützt werden, entspreche einer realistischen Lebensbetrachtung.

Es sei für das Anfallen von Standortdaten auch nicht erforderlich, dass eine Person allfällige Zugriffssperren zu einem mobilen Endgerät überwinde: Es reiche aus, dass ein mobiles Endgerät über eine gewisse Distanz bewegt werde und sich somit in unterschiedliche Funkzellen einwähle. Daher fielen Standortdaten auch an, wenn ein mobiles Endgerät bspw. in einem Auto vergessen werde. Es sei nach dem derzeitigen Stand der Technik daher nicht gesichert, dass der Vertragspartner eines Telekommunikationsunternehmens gesichert auch jene Person sei, zu der Standort- und Verkehrsdaten verarbeitet werden. Da nach gefestigter höchstgerichtlicher Rechtsprechung für einen Verantwortlichen aber mit nahezu absoluter Sicherheit feststehen müsse, dass die zu beauskunftenden Daten tatsächlich jene des Auskunftswerbers seien, erfolge die Abweisung durch die belangte Behörde zurecht (siehe zuletzt VwSlg. 19.411 A/2016).

1.8. Mit **Stellungnahme vom 12.08.2022** beschäftigte sich die **MB** ausführlich mit ihrer Behauptung, Verkehrsdaten bezögen sich nicht ausschließlich auf den BF und erstattete weiteres Vorbringen zu den Themen „TKG als lex specialis“ und Art. 11 und 12 DSGVO und regte an, das gegenständliche Verfahren mit jenem zu hg. W 256 2234027 zu verbinden.

Weiters werde die Einholung einer Vorabentscheidung des EuGH angeregt um dem EuGH folgende Fragen vorzulegen:

1. Stellt die e-Privacy-Richtlinie im Hinblick auf Verkehrs- und Standortdaten eine lex specialis zu den Regelungen des Art. 15 DSGVO dar, sodass diese der DSGVO vorgeht und eine Auskunft nur in dem in der e-Privacy-Richtlinie vorgesehenen Umfang (Einzelgesprächsnachweis) zu erfolgen hat?

2. Sofern Frage 1. mit „Nein“ beantwortet wird:

Kommt hinsichtlich Verkehrs- und Standortdaten Art. 11 DSGVO zur Anwendung, weil eine Identifizierung der betroffenen Person nicht erforderlich oder nicht möglich ist?

3. Sofern Frage 2. mit „Ja“ zu beantworten ist:

Welche Anforderungen müssen erfüllt sein, damit eine ausreichende Identifizierung des Teilnehmers gelingt?

Zu Punkt I. (Verkehrsdaten bezögen sich nicht ausschließlich auf den BF) führte die MB zusammengefasst aus, ausgehend von der herrschenden Auffassung, dass ausschließlich derjenige Träger des Auskunftsrechts sei, der auch betroffene Person sei, sei darauf zu

verweisen, dass derjenige, der eine Vertragsbeziehung zu einem Mobilfunkanbieter eingehe, oft gerade nicht derjenige sei, der das Mobiltelefon benutze. Branchenüblich seien Familien- oder Kombiangebote für mehrere Benutzer. Zu denken sei auch an Konstellationen, wonach ein Vertragsabschluss eines Mobilfunkvertrages von Eltern für ihre Kinder, von ArbeitgeberInnen für MitarbeiterInnen oder PartnerInnen für den/die anderen PartnerInnen vorliege. Die bloße eidesstättige Erklärung des BF, der ausschließliche Benutzer des Mobiltelefons zu sein, sei ein unbrauchbares Mittel, um die alleinige Nutzung des Mobilfunkvertrages darzulegen. Der MB läge keinerlei Möglichkeit zur Überprüfung dieser Behauptungen vor.

Zu 1 Ob 244/02t sei der OGH bei Mehrwertdiensten davon ausgegangen, dass auch ein Dritter Nutzer des Dienstes sein könne und man nicht davon ausgehen könne, dass der Nutzer der Teilnehmer (und umgekehrt der Teilnehmer der Nutzer) sei.

Gerade jemand, der ein großes und nicht legitimes Interesse an den Standort- und Verkehrsdaten einer dritten Person habe, die seinen Mobilfunkvertrag (mit)nutze, würde kaum davor zurückschrecken, wahrheitswidrig seine alleinige Nutzung zu beteuern.

Naheliegende Beispiele für eine solche mögliche missbräuchliche Verwendung von Verkehrs- und Standortdaten seien:

- Überwachung von ArbeitnehmerInnen durch ArbeitgeberInnen;
- Beziehungs- und Ehestreitigkeiten, Scheidungs- und Obsorgeverfahren;
- Überwachung oder gar Einschüchterung von LebensparterInnen und Kindern;
- Mobbing, Stalking etc.

Es könnten nicht nur durch die Verkehrsdaten angerufene/anrufende Personen herausgefunden werden, sondern durch die Standortdaten auch Bewegungsprofile erstellt werden. Gegenteilige Behauptungen seien selbst von Behörden oder Gerichten objektiv und in keiner Weise nachvollziehbar oder nachprüfbar. Umso weniger sei es für den Telekommunikationsanbieter möglich, im Fall von Verkehrs- und Standortdaten auch nur annähernd Gewissheit zu erlangen, dass es sich beim BF auch wirklich um den ausschließlichen Benutzer handle.

Auch der EU-Gesetzgeber habe das Problem, dass Teilnehmer (Vertragsinhaber) und (tatsächliche) NutzerInnen regelmäßig auseinanderfielen, schon bei der e-Privacy-Richtlinie vor Augen gehabt. Er habe im Zusammenhang mit der Beauskunftung und Ablehnung von Cookies erkannt, dass diese „besonders“ bedeutsam seien, wenn auch andere Nutzer Zugang

zu dem betreffenden Endgerät hätten und damit auch zu dort gespeicherten Daten, die sensible Informationen privater Natur beinhalten (ErwGrund 25 e-Privacy-Richtlinie). Keines der vom BF (in der Beschwerde S. 5 – Anmerkung des Gerichts) genannten Beispiele fiele in den Anwendungsbereich des TKG, weil sich die Beispiele nicht auf die Nutzung eines Kommunikationsnetztes bezögen. Der Benutzer – nicht der Vertragsinhaber (Teilnehmer) und nicht der Telekommunikationsanbieter – sei der einzige, der dem Kommunikationsgeheimnis unterliegende Daten weitergeben dürfe, und das auch nur dann, wenn er alle anderen beteiligten Benutzer gefragt und deren Einwilligung erhalten habe. Die vom BF genannten Beispiele, die Viewing-History eines Streamingaccounts, die Profile auf einer Socialmedia-Plattform, der Inhalt von Gesundheitsakten, seien nicht dem Kommunikationsgeheimnis unterliegende Daten. Bei der Nutzung von Streamingaccounts sei es die allgemeine Lebenserfahrung, dass neben dem Inhaber des Accounts auch andere Personen den Account nutzten.

Weiters erhob die MB in eventu (für den aus ihrer Sicht nicht vorliegenden Fall, dass eine Betroffenenstellung des BF angenommen werde) rechtliches Vorbringen zum Verhältnis der einschlägigen TKG-Regelungen zur DSGVO und weiters in eventu, wolle man das TKG nicht als lex specialis ansehen, zu Art. 11 und 12 DSGVO, nämlich Verarbeitungen, bei denen eine Identifizierung der betroffenen Person nicht erforderlich oder nicht möglich sei. Insbesondere werde auf Art. 11 Abs. 2 DSGVO verwiesen, wonach in diesen Fällen die Art. 15 bis 20 keine Anwendung fänden, es sei denn, die betroffene Person stelle zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichten. Die vom BF angebotene eidesstattliche Erklärung ermögliche dies gerade nicht.

1.9. Mit **ergänzender Stellungnahme vom 17.10.2022** führte die **MB** aus, die vollumfängliche Beauskunftung von Verkehrsdaten würde die Bestimmungen der e-Privacy-Richtlinie und des TKG zum Einzelgesprächsnachweis nutzlos machen. Dies gelte in gleicher Weise für die Regelungen zur Anzeige der Rufnummer des Anrufers beim Angerufenen (§ 139 TKG 2021) sowie zur Fangschaltung (§ 141 TKG 2021), weil mit den vollständigen Verkehrsdaten auch alle eingehenden Anrufe, einschließlich der Rufnummern aller Anrufer, offengelegt würden. Die e-Privacy-Richtlinie und das TKG 2021 schafften im Zusammenhang mit der Verarbeitung und Offenlegung von Verkehrsdaten einen wohlüberlegten Ausgleich in Hinblick auf die Interessen aller beteiligten Betroffenen (des Vertragsinhabers, der davon verschiedenen Nutzer, der Anrufer gegenüber dem Angerufenen und umgekehrt, der Behörden …). Dieser Ausgleich würde mit dem vom BF begehrten uneingeschränkten Auskunftsrecht zu Verkehrs- und Standortdaten zunichte gemacht und ausschließlich die Interessen des Auskunftswerbers zum Nachteil aller übrigen Betroffen vorangestellt.

Im Übrigen habe sich der Europäische Gerichtshof erst kürzlich in den verbundenen Rechtssachen C-339/20 und C-397/20 für die Stellung der e-Privacy-Richtlinie als Referenzrechtsakt und Maßstab im Bereich der Speicherung und allgemein der Verarbeitung personenbezogener Daten in der elektronischen Kommunikation ausgesprochen. Die e-Privacy-Richtlinie gehe sohin im Bereich der Speicherung und allgemein der Verarbeitung personenbezogener Daten in der elektronischen Kommunikation allen anderen Rechtsakten (sowohl EU Richtlinien als auch EU-Verordnungen) vor.

1.10. Der BF erhob in weiterer Folge am **30.11.2022**, nunmehr anwaltlich vertreten, einen **Fristsetzungsantrag**.

1.11. Mit verfahrensleitender Anordnung des VwGH vom 07.12.2022 wurde dem BVwG diesbezüglich eine Frist von drei Monaten gesetzt.

Die Beschwerde ist im Ergebnis nicht berechtigt:

2. Das Verwaltungsgericht legt die bereits von der belangten Behörde getroffenen unstrittigen - oben zu 5.2.1. wiedergegebenen - **Feststellungen** dem Erkenntnis zu Grunde und ergänzt diese wie folgt:

Die vom BF der MB vorgelegte „eidesstattliche Erklärung“ lautet wie folgt:

„Ich, [redacted] , erkläre hiermit als Vertragspartner des aufrechten Mobilfunkvertrages (Vertragsbeginn 27.05.2019) der Marke „Georg“ mit der A1 Telekom Austria AG, … , mit der Kundennnummer [redacted] der Rufnummer [redacted] und der SIM-Karten-Nummer [redacted] an Eides statt, dass

1. ich die genannte SIM-Karte seit Vertragsbeginn ausschließlich in ein einziges Endgerät, mein privates Mobiltelefon des Typs „iPhone 7“ eingelegt habe;

2. ich dieses Mobiltelefon seit Vertragsbeginn ausschließlich selbst benutze und es niemals an Dritte zur Benutzung überlassen habe;

3. sich dieses Mobiltelefon seit Vertragsbeginn stets in meiner unmittelbaren räumlichen Nähe befunden hat;

4. dieses Mobiltelefon seit Vertragsbeginn durch eine nur mir bekannte PIN und meinen Fingerabdruck geschützt ist, sodass unbefugte Dritte, die meines Mobiltelefons habhaft würden, außerstande wären, es zu benutzen.

Wien, 10.06.2020“

3. Die ergänzenden Feststellungen beruhen auf der vom BF bereits vor der DSB vorgelegten Beilage ./H, deren Inhalt durch die MB nicht bestritten wurde.

4. Daraus folgt rechtlich:

4.1. Gesetzliche Grundlagen:

Die gesetzlichen Grundlagen nach der DSGVO lauten auszugsweise wie folgt:

Art. 4 Z 1 DSGVO:

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 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 Personen sind, identifiziert werden kann;

Art. 11 DSGVO:

„Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

(1) Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

(2) Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

Erwägungsgrund 57 zu Art. 11 DSGVO:

Kann der Verantwortliche anhand der von ihm verarbeiteten personenbezogenen Daten eine natürliche Person nicht identifizieren, so sollte er nicht verpflichtet sein, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu identifizieren.

Allerdings sollte er sich nicht weigern, zusätzliche Informationen entgegenzunehmen, die von der betroffenen Person beigebracht werden, um ihre Rechte geltend zu machen. Die Identifizierung sollte die digitale Identifizierung einer betroffenen Person — beispielsweise durch Authentifizierungsverfahren etwa mit denselben Berechtigungsnachweisen, wie sie die betroffene Person verwendet, um sich bei dem von dem Verantwortlichen bereitgestellten Online-Dienst anzumelden — einschließen.

Art. 12 DSGVO:

„Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

(2) Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder

b) sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(6) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

(7) Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie maschinenlesbar sein.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.

Erwägungsgrund 58 zu Art. 12 DSGVO:

Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist. Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, wie etwa bei der Werbung im Internet. Wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.

Art. 15 DSGVO:

„Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Art. 23 DSGVO

„Beschränkungen

1. Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a, b, c, d, e und g genannten Zwecke verbunden sind;

i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) die Durchsetzung zivilrechtlicher Ansprüche.

2. Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf

a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,

b) die Kategorien personenbezogener Daten,

c) den Umfang der vorgenommenen Beschränkungen,

d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung;

e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen

f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,

g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und

h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.

Erwägungsgrund 73 zur Art. 23 DSGVO:

Im Recht der Union oder der Mitgliedstaaten können Beschränkungen hinsichtlich bestimmter Grundsätze und hinsichtlich des Rechts auf Unterrichtung, Auskunft zu und Berichtigung oder Löschung personenbezogener Daten, des Rechts auf Datenübertragbarkeit und Widerspruch, Entscheidungen, die auf der Erstellung von Profilen beruhen, sowie Mitteilungen über eine Verletzung des Schutzes personenbezogener Daten an eine betroffene Person und bestimmten damit zusammenhängenden Pflichten der Verantwortlichen vorgesehen werden, soweit dies in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um die öffentliche Sicherheit aufrechtzuerhalten, wozu unter anderem der Schutz von Menschenleben insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen, die Verhütung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung — was auch den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt — oder die Verhütung, Aufdeckung und Verfolgung von Verstößen gegen Berufsstandsregeln bei reglementierten Berufen, das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses sowie die Weiterverarbeitung von archivierten personenbezogenen Daten zur Bereitstellung spezifischer Informationen im Zusammenhang mit dem politischen Verhalten unter ehemaligen totalitären Regimen gehört, und zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, etwa wichtige wirtschaftliche oder finanzielle Interessen, oder die betroffene Person und die Rechte und Freiheiten anderer Personen, einschließlich in den Bereichen soziale Sicherheit, öffentliche Gesundheit und humanitäre Hilfe, zu schützen. Diese Beschränkungen sollten mit der Charta und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.

Art. 95 DSGVO

„Verhältnis zur Richtlinie 2002/58/EG

Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

Erwägungsgrund 173 zu Art. 95 DSGVO:

Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[1] bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten.

Die Richtlinie 2002/58/EG des europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation

iVm

der Richtlinie 2009/136/EG des europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz:

Artikel 6

„Verkehrsdaten

(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.

(2) Verkehrsdaten, die zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, dürfen verarbeitet werden. Diese Verarbeitung ist nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.

(3) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann die in Absatz 1 genannten Daten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu oder zur Vermarktung erforderlichen Zeitraums verarbeiten, sofern der Teilnehmer oder der Nutzer, auf den sich die Daten beziehen, seine Einwilligung gegeben hat. Der Nutzer oder der Teilnehmer hat die Möglichkeit, seine Einwilligung zur Verarbeitung der Verkehrsdaten jederzeit zurückzuziehen.

(4) Der Diensteanbieter muss dem Teilnehmer oder Nutzer mitteilen, welche Arten von Verkehrsdaten für die in Absatz 2 genannten Zwecke verarbeitet werden und wie lange das geschieht; bei einer Verarbeitung für die in Absatz 3 genannten Zwecke muss diese Mitteilung erfolgen, bevor um Einwilligung ersucht wird.

(5) Die Verarbeitung von Verkehrsdaten gemäß den Absätzen 1, 2, 3 und 4 darf nur durch Personen erfolgen, die auf Weisung der Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen oder Verkehrsabwicklung, Kundenanfragen, Betrugsermittlung, die Vermarktung der elektronischen Kommunikationsdienste oder für die Bereitstellung eines Dienstes mit Zusatznutzen zuständig sind; ferner ist sie auf das für diese Tätigkeiten erforderliche Maß zu beschränken.

(6) Die Absätze 1, 2, 3 und 5 gelten unbeschadet der Möglichkeit der zuständigen Gremien, in Einklang mit den geltenden Rechtsvorschriften für die Beilegung von Streitigkeiten, insbesondere Zusammenschaltungs- oder Abrechnungsstreitigkeiten, von Verkehrsdaten Kenntnis zu erhalten.“

Artikel 7

„Einzelgebührennachweis

(1) Die Teilnehmer haben das Recht, Rechnungen ohne Einzelgebührennachweis zu erhalten.

(2) Die Mitgliedstaaten wenden innerstaatliche Vorschriften an, um das Recht der Teilnehmer, Einzelgebührennachweise zu erhalten, und das Recht anrufender Nutzer und angerufener Teilnehmer auf Vertraulichkeit miteinander in Einklang zu bringen, indem sie beispielsweise sicherstellen, dass diesen Nutzern und Teilnehmern genügend andere, den Schutz der Privatsphäre fördernde Methoden für die Kommunikation oder Zahlungen zur Verfügung stehen.

Artikel 9

„Andere Standortdaten als Verkehrsdaten

(1) Können andere Standortdaten als Verkehrsdaten in Bezug

auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, sodürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung

ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. Die Nutzer oder Teilnehmer können ihre Einwilligung zur Verarbeitung anderer Standortdaten als Verkehrsdaten jederzeit zurückziehen.

(2) Haben die Nutzer oder Teilnehmer ihre Einwilligung zur Verarbeitung von anderen Standortdaten als Verkehrsdaten gegeben, dann müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und gebührenfrei zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Kommunikationsnetzes oder öffentlich zugänglichen Kommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.“

Artikel 15

„Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

(2) Die Bestimmungen des Kapitels III der Richtlinie 95/46/ EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

(3) Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt auch die in Artikel 30 jener Richtlinie festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr.

TKG 2021:

Der 14. Abschnitt des TKG 2021 entspricht im Wesentlichen der geltenden Rechtslage (EBRV 1043 BlgNR XXVII. GP 54)**.**

14. Abschnitt

Kommunikationsgeheimnis, Datenschutz

Allgemeines

§ 160. (1) Die Bestimmungen dieses Abschnitts gelten für die Verarbeitung einschließlich der Übermittlung von personenbezogenen Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen.

(2) Die Bestimmungen der Strafprozessordnung 1975 (StPO), BGBl. Nr. 631/1975, bleiben durch die Bestimmungen dieses Abschnittes unberührt.

(3) In diesem Abschnitt bezeichnet unbeschadet des § 4 der Begriff

1. “Anbieter” Betreiber von öffentlichen Kommunikationsdiensten;

2. “Benutzer” eine Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben;

3. „Nutzerkennung“ jene Kennung, welche die eindeutige Zuordnung eines Kommunikationsvorgangs zu einem Nutzer ermöglicht;

4. „E-Mail-Adresse“ die eindeutige Kennung, die einem elektronischen Postfach von einem Internet-E-Mail-Anbieter zugewiesen wird;

5. „Stammdaten“ alle Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Nutzerverzeichnissen erforderlich sind; dies sind:

a) Name (Familienname und Vorname bei natürlichen Personen, Name oder Bezeichnung bei juristischen Personen),

b) akademischer Grad bei natürlichen Personen,

c) Anschrift (Wohnadresse bei natürlichen Personen, Sitz oder Rechnungsadresse bei juristischen Personen),

d) Nutzernummer und sonstige Kontaktinformation für die Nachricht,

e) Information über Art und Inhalt des Vertragsverhältnisses,

f) Bonität;

g) Geburtsdatum

6. „Verkehrsdaten“ Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

7. „Zugangsdaten“ jene Verkehrsdaten, die beim Zugang eines Nutzers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Nutzer notwendig sind;

8. “Inhaltsdaten” die Inhalte übertragener Nachrichten (Z 11);

9. „Standortdaten“ Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Endeinrichtung eines Benutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Endeinrichtungen sind Standortdaten die Adresse der Einrichtung;

10. „Standortkennung“ die Kennung einer Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird (Cell-ID);

11. „Nachricht“ jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Empfänger in Verbindung gebracht werden können;

12. „Dienst mit Zusatznutzen“ jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;

13. „elektronische Post“ jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;

14. „E-Mail“ elektronische Post, die über das Internet auf Basis des „Simple Mail Transfer Protocol“ (SMTP) versendet wird;

15. „öffentliche IP-Adresse“ eine einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle (Regional Internet Registries) einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann. Öffentliche IP-Adressen sind Zugangsdaten im Sinne des § 160 Abs. 3 Z 7. Wenn eine konkrete öffentliche IP-Adresse einem Nutzer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 160 Abs. 3 Z 5;

16. „Verletzung des Schutzes personenbezogener Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person“ jede Verletzung der Sicherheit, die auf versehentliche oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Weitergabe von oder zum unbefugten Zugang zu personenbezogenen Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlicher Kommunikationsdienste in der Europäischen Union verarbeitet werden.

Kommunikationsgeheimnis

§ 161. (1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber oder Anbieter eines öffentlichen Kommunikationsnetzes oder -dienstes und alle Personen, die an der Tätigkeit des Betreibers oder Anbieters mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme und Abwicklung von Notrufen und die Fälle der Fangschaltung, der Überwachung von Nachrichten nach § 135 Abs. 3 StPO, der Auskunft über Daten einer Nachrichtenübermittlung nach §

135 Abs. 2 StPO, der Auskunft über Daten nach § 99 Abs. 3a des Bundesgesetzes vom 26. Juni 1958, betreffend das Finanzstrafrecht und das Finanzstrafverfahrensrecht (FinStrG), BGBl. Nr. 129/1958 idF BGBl. Nr. 21/1959 (DFB), der Auskunft über Daten nach § 11 Abs. 1 Z 7 des Bundesgesetzes über die Organisation, Aufgaben und Befugnisse des Verfassungsschutzes (SNG), BGBl. I Nr. 5/2016, und der Auskunft über Daten nach § 22 Abs. 2a und 2b des Militärbefugnisgesetzes (MBG), BGBl. I Nr. 86/2001, sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.

(4) Werden mittels einer Funkanlage, einer Endeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Endeinrichtung oder den Anwender der sonstigen Einrichtung nicht bestimmt sind, so dürfen der Inhalt der Nachrichten sowie die Tatsache ihres Empfanges weder aufgezeichnet noch Unbefugten mitgeteilt oder für irgendwelche Zwecke verwertet werden. Aufgezeichnete Nachrichten sind zu löschen oder auf andere Art zu vernichten.

(5) Das Redaktionsgeheimnis (§ 31 Mediengesetz) sowie sonstige, in anderen Bundesgesetzen normierte Geheimhaltungsverpflichtungen sind nach Maßgabe des Schutzes der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen sowie das Verbot deren Umgehung gemäß §§ 144 und 157 Abs. 2 StPO zu beachten. Den Anbieter trifft keine entsprechende Prüfpflicht.

Technische Einrichtungen

§ 162. (1) Der Anbieter ist nach Maßgabe der gemäß Abs. 3 und §§ 166 Abs. 2 und 171 Abs. 6 erlassenen Verordnungen verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung von Nachrichten nach § 135 Abs. 3 StPO und Auskunft über Daten einer Nachrichtenübermittlung nach § 135 Abs. 2 StPO, zur Auskunft über Daten nach § 11 Abs. 1 Z 7 SNG, zur Auskunft über Daten nach § 99 Abs. 3a FinStrG, zur Auskunft über Daten nach § 22 Abs. 2a und 2b MBG sowie zur Erfüllung der Verpflichtungen gemäß § 166 Abs. 2 erforderlich sind. Für die Bereitstellung sind dem Anbieter 80% der Kosten (Personal- und Sachaufwendungen), die er aufwenden musste, um die gemäß den Abs. 3 und §§ 166 Abs. 2 und 171 Abs. 6 erlassenen Verordnungen erforderlichen Funktionen in seinen Anlagen einzurichten, zu ersetzen. Die Bundesministerin für Landwirtschaft, Regionen und Tourismus hat im Einvernehmen mit der Bundesministerin für Justiz, der Bundesministerin für Landesverteidigung, dem Bundesminister für Inneres und dem Bundesminister für Finanzen durch Verordnung die Bemessungsgrundlage für diesen Prozentsatz sowie die Modalitäten für die Geltendmachung dieses Ersatzanspruches festzusetzen. Dabei ist insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, sowie auf die Einfachheit und Kostengünstigkeit des Verfahrens Bedacht zu nehmen.

(2) Der Anbieter ist verpflichtet, an der Überwachung von Nachrichten nach § 135 Abs. 3 StPO und der Auskunft über Daten einer Nachrichtenübermittlung nach § 135 Abs. 2 StPO, an der Auskunft über Daten nach § 11 Abs. 1 Z 7 SNG sowie an der Auskunft über Daten nach § 99 Abs. 3a FinStrG sowie an der Auskunft über Daten nach § 22 Abs. 2a und 2b MBG im erforderlichen Ausmaß mitzuwirken. Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, nach den Bestimmungen der StPO, des SPG, des FinStrG, des SNG sowie des MBG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Bundesministerin für Justiz hat im Einvernehmen mit der Bundesministerin für Landwirtschaft, Regionen und Tourismus und dem Bundesminister für Finanzen durch Verordnung einen angemessenen Kostenersatz vorzusehen. Dabei ist insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, sowie der öffentlichen Aufgabe der Rechtspflege Bedacht zu nehmen.

(3) Durch Verordnung kann die Bundesministerin für Landwirtschaft, Regionen und Tourismus im Einvernehmen mit dem Bundesminister für Inneres, der Bundesministerin für Justiz und der Bundesministerin für Landesverteidigung, dem jeweiligen Stand der Technik entsprechend, die näheren Bestimmungen für die Gestaltung der technischen Einrichtungen zur Gewährleistung der Überwachung von Nachrichten nach § 135 Abs. 3 StPO und der Auskunft über Daten einer Nachrichtenübermittlung nach § 135 Abs. 2 StPO und zum Schutz der zu übermittelnden Daten gegen die unbefugte Kenntnisnahme durch Dritte festsetzen. Nach Erlassung der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten.

Datensicherheitsmaßnahmen

§ 163. (1) Die Pflicht zur Erlassung von Datensicherheitsmaßnahmen im Sinne der Art. 24, 25 und 32 DSGVO im Zusammenhang mit der Erbringung eines öffentlichen Kommunikationsdienstes obliegt jedem Betreiber eines öffentlichen Kommunikationsdienstes jeweils für jeden von ihm erbrachten Dienst.

(2) Unbeschadet des Abs. 1 hat der Betreiber eines öffentlichen Kommunikationsdienstes in jenen Fällen, in denen ein besonderes Risiko der Verletzung der Vertraulichkeit besteht, die Nutzer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Betreiber zu treffenden Maßnahmen liegt – über mögliche Abhilfen einschließlich deren Kosten zu unterrichten.

(3) Betreiber eines öffentlichen Kommunikationsdienstes haben durch Datensicherheitsmaßnahmen jedenfalls Folgendes zu gewährleisten:

1. die Sicherstellung, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten;

2. den Schutz gespeicherter oder übermittelter personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe;

3. die Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten.

Die Regulierungsbehörde kann die von den Betreibern öffentlicher Kommunikationsdienste getroffenen Maßnahmen prüfen und Empfehlungen zum zu erreichenden Sicherheitsniveau abgeben.

Sicherheitsverletzungen

§ 164. (1) Im Fall einer Verletzung des Schutzes personenbezogener Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person hat unbeschadet des § 44 sowie unbeschadet der Bestimmungen des DSG und der DSGVO der Betreiber öffentlicher Kommunikationsdienste unverzüglich die Datenschutzbehörde von dieser Verletzung zu benachrichtigen. Ist anzunehmen, dass durch eine solche Verletzung Personen in ihrer Privatsphäre oder die personenbezogenen Daten selbst beeinträchtigt werden, hat der Betreiber auch die betroffenen Personen unverzüglich von dieser Verletzung zu benachrichtigen.

(2) Der Betreiber öffentlicher Kommunikationsdienste kann von einer Benachrichtigung der betroffenen Personen absehen, wenn der Datenschutzbehörde nachgewiesen wird, dass er geeignete technische Schutzmaßnahmen im Sinne der Verordnung (EU) 611/2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG (Data-Breach-Verordnung), ABl. Nr. L 173 vom 26.06.2013 S. 2, getroffen hat und dass diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet worden sind. Diese technischen Schutzmaßnahmen müssen jedenfalls sicherstellen, dass die Daten für unbefugte Personen nicht zugänglich sind.

(3) Unbeschadet der Verpflichtung des Betreibers nach Abs. 1 zweiter Satz kann die Datenschutzbehörde den Betreiber öffentlicher Kommunikationsdienste – nach Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung – auch auffordern, eine Benachrichtigung durchzuführen.

(4) Der Inhalt der Benachrichtigung der betroffenen Personen hat Art. 3 der Data-Breach-Verordnung zu entsprechen.

(5) Die Datenschutzbehörde kann im Einzelfall auch entsprechende Anordnungen treffen, um eine den Auswirkungen der Sicherheitsverletzung angemessene Benachrichtigung der betroffenen Personen sicherzustellen. Sie kann auch Leitlinien im Zusammenhang mit Sicherheitsverletzungen erstellen.

(6) Die Betreiber öffentlicher Kommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person zu führen. Es hat Angaben zu den Umständen der Verletzungen, zu deren Auswirkungen und zu den ergriffenen Abhilfemaßnahmen zu enthalten und muss geeignet sein, der Datenschutzbehörde die Prüfung der Einhaltung der Bestimmungen gemäß Abs. 1 bis 4 zu ermöglichen.

(7) Die Datenschutzbehörde hat die Regulierungsbehörde über jene Sicherheitsverletzungen zu informieren, die für die Erfüllung der der Regulierungsbehörde durch § 44 übertragenen Aufgaben notwendig sind.

Datenschutz-Allgemeines

§ 165. Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten dürfen nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden.

(2) Die Übermittlung von im Abs. 1 genannten Daten darf nur erfolgen, soweit das für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber eines öffentlichen Kommunikationsdienstes erforderlich ist. Die Verarbeitung der Daten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen sowie sonstige Übermittlungen dürfen nur auf Grund einer jederzeit widerrufbaren Einwilligung der Betroffenen erfolgen. Diese Verarbeitung ist auf das erforderliche Maß und den zur Vermarktung erforderlichen Zeitraum zu beschränken. Betreiber öffentlicher Kommunikationsdienste dürfen die Bereitstellung ihrer Dienste nicht von einer solchen Einwilligung abhängig machen.

(3) Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft im Sinne des § 3 Z 1 E-Commerce-Gesetz, BGBl. I Nr. 152/2001, sind verpflichtet, den Nutzer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er verarbeiten wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Eine Ermittlung dieser Daten ist nur zulässig, wenn der Nutzer oder Benutzer seine Einwilligung dazu aktiv und auf Grundlage von klaren und umfassenden Informationen erteilt hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder, wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Nutzer oder Benutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Der Nutzer ist auch über die Nutzungsmöglichkeiten auf Grund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen zu informieren. Diese

Information hat in geeigneter Form, insbesondere im Rahmen Allgemeiner Geschäftsbedingungen und spätestens bei Beginn der Rechtsbeziehungen zu erfolgen.

Stammdaten

§ 166. (1) Stammdaten dürfen unbeschadet der § 165 Abs. 1 und 2 sowie § 181 Abs. 8 und 9 von Anbietern nur für folgende Zwecke verarbeitet werden:

1. Abschluss, Durchführung, Änderung oder Beendigung des Vertrages mit dem Nutzer;

2. Verrechnung der Entgelte;

3. Erstellung von Nutzerverzeichnissen, gemäß § 126 und

4. Erteilung von Auskünften an Betreiber von Notdiensten, gemäß § 124.

(2) Vor Durchführung des Vertrages sowie vor der erstmaligen Wiederaufladung nach dem 1. September 2019 ist durch oder für den Anbieter die Identität des Nutzers zu erheben und sind die zur Identifizierung des Nutzers erforderlichen Stammdaten (§ 160 Abs. 3 Z 5 lit. a, b und g) anhand geeigneter Identifizierungsverfahren zu registrieren. Die Festlegung geeigneter Identifizierungsverfahren erfolgt durch Verordnung der Bundesministerin für Landwirtschaft, Regionen und Tourismus im Einvernehmen mit dem Bundesminister für Inneres. Die Abgeltung unbedingt erforderlicher Investitionen erfolgt nach den Regeln des § 162 Abs. 1.

(3) Stammdaten sind spätestens nach Beendigung der vertraglichen Beziehungen mit dem Nutzer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

Verkehrsdaten

§ 167. (1) Verkehrsdaten dürfen außer in den in diesem Gesetz ausdrücklich geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Die Zulässigkeit der weiteren Verarbeitung von Verkehrsdaten, die nach Abs. 5 übermittelt werden, richtet sich nach den Vorschriften der StPO, des FinStrG, des SPG, des SNG sowie des MBG.

(2) Sofern dies für Zwecke der Verrechnung von Endkunden- oder Vorleistungsentgelten erforderlich ist, hat der Betreiber eines öffentlichen Kommunikationsnetzes oder -dienstes Verkehrsdaten zu speichern. Die Verkehrsdaten sind zu löschen oder zu anonymisieren, sobald der Bezahlvorgang durchgeführt wurde und innerhalb einer Frist von drei Monaten die Entgelte nicht schriftlich beeinsprucht wurden. Die Daten sind jedoch nicht zu löschen, wenn

1. ein fristgerechter Einspruch erhoben wurde, bis zum Ablauf jener Frist, innerhalb derer die Abrechnung rechtlich angefochten werden kann.

2. die Rechnung nicht beglichen wurde, bis zum Ablauf jener Frist, bis zu der der Anspruch auf Zahlung geltend gemacht werden kann,

3. ein Verfahren über die Höhe der Entgelte eingeleitet wurde, bis zur endgültigen Entscheidung, oder

4. eine Anordnung nach § 135 Abs. 2b StPO erlassen wird, bis zum Ablauf der angeordneten Dauer oder auf Grund einer Anordnung der Staatsanwaltschaft (§ 138 Abs. 2 StPO).

Die Daten nach Z 1 bis 3 sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle (§ 205) unverkürzt zur Verfügung zu stellen. Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(3) Die Verarbeitung mit Ausnahme der Übermittlung von Verkehrsdaten darf nur durch solche Personen erfolgen, die für die Entgeltverrechnung oder Verkehrsabwicklung, Behebung von Störungen, Kundenanfragen, Betrugsermittlung oder Vermarktung der Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen zuständig sind oder die von diesen Personen beauftragt wurden. Der Umfang der verarbeiteten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(4) Dem Anbieter ist es außer in den in diesem Gesetz besonders geregelten Fällen untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Nutzernummer auszuwerten. Mit Zustimmung des Nutzers darf der Anbieter die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden.

(5) Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist zulässig zur Auskunft über

1. Daten einer Nachrichtenübermittlung gemäß § 134 Z 2 StPO;

2. Zugangsdaten an Gerichte und Staatsanwaltschaften nach Maßgabe des § 76a Abs. 2 StPO.

3. Verkehrsdaten und Stammdaten, wenn hiefür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a und 3b SPG, § 11 Abs. 1 Z 5 SNG sowie § 22 Abs. 2b MBG. Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung verarbeitet werden;

4. Zugangsdaten, wenn diese längstens drei Monate vor der Anfrage gespeichert wurden, an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 3 SPG, des § 11 Abs. 1 Z 5 SNG, des § 99 Abs. 3a FinStrG sowie des § 22 Abs. 2b MBG;

5. Verkehrsdaten, Zugangsdaten und Standortdaten nach Maßgabe des § 11 Abs. 1 Z 7 SNG sowie des § 22 Abs. 2b MBG.

Andere Standortdaten als Verkehrsdaten

§ 169. (1) Andere Standortdaten als Verkehrsdaten dürfen unbeschadet des § 124 nur verarbeitet werden, wenn sie

1. anonymisiert werden oder

2. die Benutzer oder Nutzer eine jederzeit widerrufbare Einwilligung gegeben haben.

(2) Selbst im Falle einer Einwilligung zur Verarbeitung von Daten gemäß Abs. 1 müssen die Benutzer oder Nutzer die Möglichkeit haben, diese Verarbeitung von Daten für jede Übertragung einfach und kostenlos zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß Abs. 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln. Unbeschadet des § 161 Abs. 3 ist die Ermittlung und Verwendung von Standortdaten, die nicht im Zusammenhang mit einem Kommunikationsvorgang stehen, zu Auskunftszwecken unzulässig.

Datensicherheit bei der Übermittlung von betriebsnotwendigen Verkehrs- und Standortdaten zu Auskunftszwecken an gesetzlich berechtigte Behörden

§ 170. (1) Die Übermittlung der Daten hat über eine zentrale Durchlaufstelle zu erfolgen, die die Bundesministerin für Landwirtschaft, Regionen und Tourismus bei der Bundesrechenzentrum GmbH einzurichten hat.

(2) Die technische Spezifikation zur Durchlaufstelle hat einen verschlüsselten Übertragungsweg vorzusehen (Transportverschlüsselung).

(3) Zusätzlich ist eine Verschlüsselung der Inhalte sowohl der Anfrage als auch der Beantwortung von Absender zu Empfänger durch asymmetrische Verschlüsselungsverfahren vorzusehen (Inhaltsverschlüsselung). Asymmetrische Verschlüsselungsverfahren können als hybride Verfahren implementiert werden.

(4) Über die Durchlaufstelle werden die Beteiligten des Datenaustausches über eine fortgeschrittene elektronische Signatur identifiziert und authentifiziert.

Durchlaufstelle – Grundstruktur

§ 171. (1) Die Durchlaufstelle hat ein elektronisches Postfachsystem zur sicheren Abwicklung von Anfragen und Auskünften im Sinne des Abs. 6 zu errichten. Alle Beteiligten sind dabei über einen verschlüsselten Übertragungskanal an die Durchlaufstelle anzubinden.

(2) Die Durchlaufstelle ist auf eine Weise einzurichten, dass für die Bundesrechenzentrum GmbH als Auftragsverarbeiter der Durchlaufstelle im Sinn des Art. 4 Z 8 DSGVO ein Zugang zu personenbezogenen Inhalten von Anfragen zu Datenauskünften sowie von deren Beantwortung nicht möglich ist.

(3) Über die Durchlaufstelle sind Auskünfte über Daten, die für den Anbieter für die in § 167 Abs. 2 und 3 erfassten Zwecke erforderlich sind, abzuwickeln. Über die Durchlaufstelle sind alle Auskunftsfälle revisionssicher statistisch zu erfassen.

(4) In der Spezifikation zur Durchlaufstelle ist eine Übertragungstechnologie vorzusehen, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als „Comma-Separated Value (CSV)“ – Dateiformat zu übermitteln. Ausgenommen davon ist

1. die Übermittlung von Daten in den Fällen des § 124;

2. bei Gefahr im Verzug die Übermittlung von Verkehrsdaten und Stammdaten, wenn hiefür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a und 3b SPG, § 11 Abs. 1 Z 5 SNG sowie § 22 Abs. 2b MBG. Ist eine aktuelle Standortfeststellung gemäß § 124 Abs. 1 nicht möglich, darf gemäß § 124 Abs. 4 die zuletzt verfügbare Standortkennung der Endeinrichtung verarbeitet werden;

3. bei Gefahr im Verzug die Übermittlung von Zugangsdaten, wenn diese längstens drei Monate vor der Anfrage gespeichert wurden, an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 3 SPG, § 11 Abs. 1 Z 5 SNG sowie § 22 Abs. 2b MBG;

4. die Übermittlung von Standortdaten in den Fällen der Feststellung des aktuellen Standortes gemäß §§ 134 ff StPO und

5. die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten.

(5) Für die Datenschutzbehörde sowie für die Rechtsschutzbeauftragten bei der Bundesministerin für Justiz, beim Bundesminister für Inneres und beim Bundesminister für Finanzen ist in der Spezifikation zur Durchlaufstelle jeweils ein Zugang vorzusehen, der entsprechend der jeweiligen Aufgabe dieser Stellen einen Zugang zu den Protokolldaten oder zur Statistik ermöglicht.

(6) Durch Verordnung kann die Bundesministerin für Landwirtschaft, Regionen und Tourismus im Einvernehmen mit dem Bundesminister für Inneres und der Bundesministerin für Justiz und dem Bundesminister für Finanzen die näheren Bestimmungen zur einheitlichen Definition der Syntax, der

Datenfelder und der Verschlüsselung, zur Speicherung und Übermittlung der Daten festsetzen. Insbesondere sind, unbeschadet der §§ 170, 171 und 172, näher auszuführen

1. Funktionen der Durchlaufstelle;

2. Auditierung der Durchlaufstellen-Funktionen;

3. Authentifizierung, Sicherheitsniveau der Anbindung, Verschlüsselung/Signatur;

4. Zugangsberechtigte Behörden;

5. Anbindung der Anbieter;

6. Postfächer und Zustellung;

7. Optionale Stammdatenauskünfte über die Durchlaufstelle;

8. Protokollierung des Datenverkehrs über die Durchlaufstelle;

9. Statistik aus den Protokolldaten.

Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten.

(7) Ein Betreiber, der nicht gemäß § 34 KOG zur Entrichtung eines Finanzierungsbeitrages verpflichtet wurde, ist nicht verpflichtet, seiner Auskunftspflicht über die Durchlaufstelle nachzukommen.

4.2. Daraus folgt:

4.2.1. Wie sich aus der Beschwerde an das Verwaltungsgericht (S 2) ergibt, wendet sich der BF im Beschwerdeverfahren nur mehr gegen die Abweisung seines Antrages auf Bereitstellung einer Kopie von Standort- und Verkehrsdaten (einschließlich Standortkennung), sodass über dieses Begehren hinausgehende von der belangten Behörde abgewiesene Anträge des BF (in Form der modifizierten Anträge seiner Datenschutzbeschwerde in der Stellungnahme vom 05.10.2020 (siehe oben S 10) nicht mehr entscheidungsgegenständlich sind.

4.2.2. Im Wesentlich geht es dem BF in dem offenbar als „Musterverfahren“ intendierten Verfahren darum, die MB zur Herausgabe von Kopien aller in ihrem Verfügungsbereich befindlichen Verkehrs- und Standortdaten zu verhalten, dies gegründet insbesondere auf eine nach Ansicht des BF gegenüber dem Entscheidungszeitpunkt des Bescheides der Datenschutzbehörde vom 27.03.2017 DSB-D122.616/0006-DSB/2016 aufgrund Inkrafttretens der DSGVO geänderte Rechtslage.

4.2.4. In Bezug auf die zu Spruchpunkt 3. erfolgte Abweisung der Beschwerde - soweit sie nicht das Auskunftsbegehren in Bezug auf konkrete Datenempfänger betrifft - bezog sich die belangte Behörde im Wesentlichen auf den genannten Bescheid vom 27.03.2017. Auch seit

Inkrafttreten der DSGVO seien weiterhin die Bestimmungen des TKG 2003 (nunmehr TKG 2021 - Anmerkung des Gerichts) maßgeblich, weil die Bestimmungen der §§ 92 ff TKG 2003 auf den Vorgaben der e-Datenschutz-Richtlinie fußten und als lex specialis der DSGVO vorgingen.

4.2.4. In dem genannten Verfahren vor der Datenschutzbehörde (DSB/D122.616) behauptete der dortige BF eine Verletzung im Recht auf Auskunft dadurch, dass die Beschwerdegegnerin eine Auskunft zu der auf ihn registrierten Telefonnummer betreffend Standortdaten in einem bestimmten Zeitraum im September 2016 verweigert habe.

Die DSB stellte fest, dass die Beschwerdegegnerin tatsächlich die Auskunft über die genannten Standortdaten verweigert habe und nicht festgestellt werden habe können, dass der BF tatsächlich Nutzer des Endgerätes im relevanten Zeitraum gewesen sei. Die letztgenannte Feststellung gründete die belangte Behörde auf die Überlegung, dass der tatsächliche Nutzer des Endgerätes im verfahrensgegenständlichen Zeitraum objektiv (für jedermann nachvollziehbar) nicht nachgewiesen habe werde können.

Rechtlich ging die belangte Behörde vom damals in Geltung stehenden § 26 Abs. 1 DSG 2000 als verfassungsgesetzlich gewährleistetes Recht auf Auskunft aus, das ausschließlich auf personenbezogene Daten des Auskunftswerbers als Betroffenen beschränkt, somit sein höchstpersönliches Recht sei. Der Telekommunikationsanbieter könne im Regelfall nicht feststellen, ob ein Auskunftswerber, dessen Standortdaten Gegenstand des Auskunftsverlangens seien, tatsächlich zu jedem Zeitpunkt Nutzer der einem Endgerät zugeordneten Rufnummer sei bzw. gewesen sei. Ein Auskunftsanspruch hätte zur Folge, dass der Auskunftswerber unter Umständen Auskunft zu Bewegungsdaten erhalte, die nicht seiner Person zuzuordnen seien. Auch unter Bezugnahme auf einen weiteren Bescheid (D122.418/0002-DSB/2016) führte die belangte Behörde sodann aus, solange nicht mit ausreichender Sicherheit feststehe und objektiv nachweisbar sei, dass ein Auskunftswerber auch tatsächlich Nutzer von einem einer Rufnummer zugeordneten Endgerät ist bzw. gewesen sei, könne ein Auftraggeber zu Recht die begehrte Auskunft über Standortdaten verweigern. Durch eine eidesstattliche Erklärung werde kein objektiver Nachweis einer ausschließlichen Nutzung erbracht. Weiters bezog sich die belangte Behörde auf ein Urteil des OGH zu 12 Os 93/14i vom 05.03.2019 zur Standortkennung, in dem der OGH eine nur sehr eingeschränkte Zulässigkeit der Verarbeitung von Daten zu Auskunftszwecken im Bereich Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG 2003) angenommen habe. Weiters bezog sie sich auf eine Entscheidung der Datenschutzkommission, wonach das Fernmelderecht gemäß § 92 Abs. 1 iVm § 100 Abs. 1 TKG 2003 den Betroffenen nur ein auf den Erhalt eines Einzelentgeltnachweises eingeschränktes Recht einräume, über gespeicherte Verkehrsdaten Auskunft zu erhalten.

Dieser Bescheid erwuchs ohne Befassung des Verwaltungsgerichts in Rechtskraft.

Fallgegenständlich ist dazu auszuführen:

4.2.4. Der BF stützt sein Auskunftsbegehren auf den auch im gegenständlichen Fall seiner Ansicht nach uneingeschränkt anwendbaren Art 15 DSGVO. Ungeachtet der Frage von dessen tatsächlicher Anwendbarkeit im Spannungsverhältnis zu allfälligen lex-specialis-Regelungen knüpft die Bestimmung des Art. 15 DSGVO an die Verarbeitung von den Auskunftswerber betreffenden personenbezogenen Daten an (Art. 15 Abs. 1 DSGVO). Nur wenn der Verantwortliche personenbezogene Daten der betroffenen Person verarbeitet, kommt eine Auskunftspflicht nach der DSGVO überhaupt in Betracht.

4.2.5.1. Zur Rechtsnatur von Verkehrs- bzw. Standortdaten kann zunächst auf die oben wiedergegebenen gesetzlichen Definitionen des TKG 2021 (§ 160 Abs. 3 Z 6, Z 9 und Z 10), sich wiederum beziehend auf die e-Datenschutz-Richtlinie (Begriffsbestimmungen des Art. 2), zurückgegriffen werden, wonach Verkehrsdaten solche sind, die zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet werden, und Standortdaten solche sind, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geographischen Standort der Endeinrichtung eines Benutzers eines öffentlichen Kommunikationsdienstes angeben.

4.2.5.2. Verkehrsdaten können alle Formen einschließen, in die in Nachrichten enthaltene Informationen über Name, Nummern und Adressen durch das Netz, über das die Nachricht übermittelt wird, für Zwecke der Übermittlung umgewandelt werden. Verkehrsdaten umfassen daher 2 Datenkategorien: Solche, die für die Weiterleitung der Nachricht an das elektronische Kommunikationsnetz benötigt werden und solche, die für die Verrechnung erforderlich sind (Billingdaten). Unter diesem Begriff ist die gesamte Weiterleitung der Information über das elektronische Kommunikationsnetz umfasst. Sie sind heikler als Stammdaten, was sich aus der Tatsache ableiten lässt, dass sie dem Kommunikationsgeheimnis unterliegen. Aus ihnen lassen sich Rückschlüsse auf die Nutzung eines Anschlusses, nicht aber auf den Teilnehmer selbst ziehen (Riesz in Riesz/Schilchegger TKG 2016, § 99 Rz 4).

4.2.5.3. Zu den Daten für die Weiterleitung an das Kommunikationsnetz zählen Informationen wie die aktive und passive Rufnummer (des anrufenden und des angerufenen Anschlusses), wobei letztere auch Stammdaten, somit doppelfunktional sind. Weiters zählen dazu Beginn, Ende und Dauer einer Verbindung, Informationen über die Art des Endgerätes oder die Funkzelle, zu der das mobile Endgerät die Verbindung hält; weiters die Leitwege sowie die zum

Aufbau und zur Aufrechterhaltung der Verbindung erforderlichen Daten. Ferner zählen dazu Daten, die bei paketvermittelten Diensten zur Übertragung im Internet erzeugt werden, wie die IP-Adressen, Daten über das verwendete Protokoll, das Format, in dem die Nachricht über das Netz weitergeleitet wird sowie Dauer, Zeitpunkt und Datenmenge einer Nachricht (wie oben, Rz 5).

4.2.5.4. Zur Definition von Standortdaten bedarf es zunächst der Klärung des Begriffs Endgerät. Ein solches ist jener Apparat, der an einen Netzabschluss eines Kommunikationsnetzes angeschlossen ist, somit das Festnetz- und das Mobiltelefon. Standortdaten können sich auf den Standort des Endgerätes des Nutzers nach geografischer Länge, Breite und Höhe, die Übertragungseinrichtung, den Grad der Genauigkeit der Standortinformationen, die Identifizierung des Netzpunktes, an dem sich das Endgerät zu einem bestimmten Zeitpunkt befindet, sowie den Zeitpunkt, zu dem die Standortinformationen erfasst wurden, beziehen. Es ist dazu nicht erforderlich, dass eine Kommunikation geführt wird, da auch wenn das Endgerät nur eingeschaltet ist und sich in das jeweilige Kommunikationsnetz einbucht, um insbesondere für eingehende Anrufe empfangsbereit zu sein, Daten im Kommunikationsnetz verarbeitet werden. Standortdaten, die insbesondere von digitalen Mobilfunknetzen verarbeitet werden, haben hohe datenschutzrechtliche Bedeutung. Mit ihnen kann die geografische Position des Teilnehmers oder Nutzers bzw dessen Endgeräts jederzeit festgestellt werden und damit zu Bewegungsprofilen zusammengeführt werden (Riesz in Riesz/Schilchegger TKG 2016, § 102 Rz 4).

4.2.5.5. Jene Standortdaten, die zur Nachrichtenübermittlung erforderlich sind bzw diese ermöglichen, sind (zugleich) Verkehrsdaten und stellen eine Untergruppe bzw einen Teil dieser dar. Davon sind jene Standortdaten zu unterscheiden, die genauer sind und für die Übertragung der Nachricht im Kommunikationsnetz oder zur Fakturierung dieses Vorgangs nicht erforderlich sind (wie oben, Rz 6).

Wie schon die DSB zu D122.616/2016 zutreffend ausführte, handelt es sich bei den Standortdaten um betriebstechnisch notwendige Daten zum „Routing“, somit zur Verbindungsherstellung mittels mobilen Endgeräts in einem Telekommunikationsnetz.

4.2.6.1. Da die Anwendung der DSGVO ganz generell das Vorliegen personenbezogener Daten voraussetzt, ist kurz auf die Frage einzugehen, ob es sich bei den hier gegenständlichen Verkehrs- und Standortdaten um personenbezogene Daten im Sinne des Art. 4 Z 1 DSGVO handelt.

Demnach sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen, wobei als identifizierbar eine natürliche Person dann angesehen wird, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung und zu einem oder mehreren besonderen Merkmalen identifiziert werden kann.

4.2.6.2. Gerade aufgrund des Umstandes, dass sich die MB darauf stützt, sie könne glaubhaft machen, dass sie nicht in der Lage sei, den BF als betroffenen Auskunftswerber (als ausschließlichen Nutzer) zu identifizieren (unter anderem Stellungnahme vom 04.09.2020, S 8), ist zunächst auf die Frage einzugehen, ob der BF aus Sicht der MB eine identifizierte oder identifizierbare natürliche Person ist. Keine Rolle spielt im Zusammenhang dieses Verfahrens die Frage, ob an der Identität des BF als jener natürlichen Person zu zweifeln ist, die den Antrag gem. den Art. 15 bis 21 stellt (siehe Jahnel, Kommentar zur Datenschutzgrundverordnung Art. 15 DSGVO, Rz 12, Stand 01.12.2020, rdb).

4.2.6.3. Keine Zweifel bestehen auch daran, dass der BF Vertragspartner eines Mobilfunkvertrages der MB für das Produkt „Ge org!“ ist, dessen Wesen es ist, dass vom einem Endgerät aus standort- ungebunden telefoniert werden kann und darüber hinausgehend zahlreiche weitere elektronische Dienste (Messengerdienste etc). in Anspruch genommen werden können. Dass es dem BF als Vertragspartner der MB gemäß den Vertragsbedingungen (AGB) nicht gestattet wäre, das Endgerät an weitere Benutzer in jeglicher Form weiterzugeben, wurde weder behauptet noch sind hiefür Anhaltspunkte ersichtlich.

4.2.6.4. Geht man im Sinne des Vorbringens der MB davon aus, dass Vertragspartner eines Mobilfunkvertrages durch (partielle) Weitergabe des Endgerätes daher auch „Datenspuren“ begründen können, die nicht von ihnen persönlich ausgelöst werden (z.B. durch das Bewegen eines Endgerätes durch eine vom Vertragspartner verschiedene Person), ist im Sinne des Art. 4 Z 1 DSGVO die Frage zu stellen, ob diesbezüglich noch personenbezogene Daten vorliegen.

4.2.6.5. Nach dem dargestellten Normtext des Art. 4 Z 1 ist es ausreichend, dass sich Informationen auf eine identifizierbare natürliche Person beziehen, um personenbezogene Daten zu begründen. Ausdrücklich spricht die DSGVO in diesem Zusammenhang in Art. 4 Z 5 von Pseudonymisierung, wenn personenbezogene Daten in einer Weise verarbeitet werden, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Identifizierbar ist eine Person, wenn die Information zwar für sich genommen nicht ausreicht, um sie einer Person zuzuordnen, dies aber gelingt, sobald die Information mit weiteren Informationen verknüpft wird. Bei

pseudonymisierten Daten ist der Personenbezug herstellbar. Entscheidend ist, dass rechtlich zulässige, vernünftigerweise einsetzbare Mittel zur Verfügung stehen, womit ein zumutbarer bzw. nicht ungewöhnlicher Ermittlungsaufwand gemeint ist (Hödl in Knyrim, DatKomm Art. 4 DSGVO, Rz 12 und 13, Stand 01.12.2018, rdb).

4.2.6.6. Kommt es bei der Herstellung des Personenbezugs auf den jeweils Verantwortlichen an, spricht man von relativem Personenbezug, vertritt man die Ansicht, dass es ausreicht, dass irgendein beliebiger Dritter den Personenbezug herstellen kann, spricht man von absolutem Personenbezug. Um festzustellen, ob eine Person identifizierbar ist, sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich zur Identifizierung einer natürlichen Person genutzt werden. Die Nutzung der Mittel durch den Dritten muss aber nach allgemeinem Ermessen wahrscheinlich sein. Es erscheint diesbezüglich die Schlussfolgerung zulässig, dass es nicht ausreichend ist, dass irgendeine beliebige Person irgendwo auf der Welt den Personenbezug herstellen könnte (wie oben, Rz 14).

4.2.6.7. Laut Hödl in Knyrim (siehe oben) ist ungeklärt, wie die Situation für ein offenes WLAN, das von mehreren Nutzern genutzt wird, einzustufen ist, da der Bezug zu einer natürlichen Person fraglich sein kann (wie oben, Rz 15).

Mit der Frage, ob im Falle problematischer Identifizierbarkeit personenbezogene Daten vorliegen, befassen sich (jedenfalls indirekt) auch die Art. 11 und 12 DSGVO:

4.2.6.8. Gemäß Art. 11 Abs. 1 ist der Verantwortliche nicht verpflichtet, zur bloßen Einhaltung der DSGVO zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren, wenn für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich ist.

Gemäß Abs. 2 finden die Art. 15 bis 20 keine Anwendung, wenn der Verantwortliche in Fällen gemäß Abs. 1 nachweisen kann, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, es sei denn, die betroffene Person stellt zur Ausübung ihrer genannten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

4.2.6.9. Art. 11 greift in Fällen, in denen die Daten keinen unmittelbaren Personenbezug aufweisen, weil dieser für den jeweiligen Verarbeitungszweck nicht (mehr) erforderlich ist, zulässigerweise aber mittelbarer Personenbezug besteht, der Betroffene also grundsätzlich identifizierbar ist (Hötzendorfer in Knyrim, DatKomm Art. 11, Rz 8; Stand 07.05.2020, rdb.at).

Ein wesentlicher Anwendungsfall von Art. 11 sind pseudonymisierte Daten, weiters Onlinebenutzerkonten (wie oben, Rz 19 und 20).

4.2.6.10. Gemäß Art. 12 Abs. 2 DSGVO darf der Verantwortliche sich in den in Art. 11 Abs. 2 genannten Fällen nur weigern, aufgrund des Antrags auf Wahrnehmung ihrer Rechte gemäß Art. 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

4.2.6.11. Aus allen dargestellten Erwägungen ist abzuleiten, dass allein der Umstand, dass ein Verantwortlicher die betroffene Person nicht identifizieren kann, das Vorliegen personenbezogener Daten iSd Art. 4 Z 1 DSGVO und somit die grundsätzliche Anwendbarkeit der DSGVO an sich und somit des Art. 15 (Auskunftspflicht) nicht ausschließt. Die Abgrenzung, ob im Falle von Verkehrs- und Standortdaten die Identifizierbarkeit des Betroffenen (jener Person, die durch das Mitsichführen bzw. das Verwenden der Endgeräte solche Daten erzeugt) (überhaupt) noch gegeben ist, kann im Einzelfall schwierig sein (siehe dazu auch Riesz in Riesz/Schilchegger TKG 2016, § 99 Rz 4 letzter Absatz). Ginge man im Einzelfall davon aus, dass eine Identifizierbarkeit absolut oder auch nur relativ (nach allgemeinem Ermessen unwahrscheinlich) ausgeschlossen wäre, wäre hieraus für den BF allerdings nichts gewonnen, weil in diesem Falle infolge Nichtvorliegens personenbezogener Daten ein Auskunftsrecht nach der DSGVO generell nicht bestehen würde.

4.2.7.1. Aufgrund des Zwischenergebnisses, dass grundsätzlich personenbezogene Daten durch im Vertragsbereich des BF entstandene Verkehrs- und Standortdaten vorliegen, ist im Hinblick auf Art. 15 Abs. 1 DSGVO zu prüfen, ob die MB in Bezug auf das Auskunftsbegehren des BF „diesen betreffende“ personenbezogenen Verkehrs- und Standortdaten verarbeitet.

4.2.7.2. Dies wird zwar zweifellos im Regelfall der Fall sein, allerdings ist es selbst nach den Vertragsbedingungen dem Vertragspartner eines Mobilfunkvertrages keineswegs verboten, Endgeräte in jeder Weise - auch durch gänzliche oder partielle Weitergabe bzw. gelegentliche Benutzung durch andere, Mitnutzung der elektronischen Funktionen etc. - zu verwenden. Ein Rückgriff auf die von der MB in der Stellungnahme vom 12.08.2022 aufgezeigten Möglichkeiten vorsätzlicher oder böswilliger Weitergabe der Einholung von Standortinformationen im Sinne eines „verdeckten Trackings“ ist dabei gar nicht erforderlich.

4.2.7.3. Der besonderen Schutzwürdigkeit der dem Telekommunikationsgesetz unterliegenden Daten, darunter auch der Verkehrs- und Standortdaten, tragen einerseits das Kommunikationsgeheimnis (§ 161 TKG 2021), andererseits auch die damit im Zusammenhang stehende Strafbestimmung des § 187, denen jedenfalls die MB unterliegt, Rechnung.

4.2.7.4.Die Thematik der Einschränkung des Auskunftsrechts gemäß Art. 15 DSGVO auf „die betroffene Person betreffende“ personenbezogene Daten wurde – soweit ersichtlich – im Rahmen der in Österreich verfügbaren Kommentierungen zur DSGVO noch wenig ausführlich dargestellt (siehe Haidinger in Knyrim, DatKomm Art. 15 DSGVO, Rz 12 unter Verweis auf Illibauer in Knyrim, DatKomm Art. 12 DSGVO, Rz 74 ff). Dort wurde im Wesentlichen die Frage abgehandelt, ob eine anfragende Person gleichzeitig auch die berechtigte Person ist.

4.2.7.4. Im Grunde genommen liegt auch hier diese Frage zur Beurteilung vor, allerdings ist diese differenzierter zu stellen, nämlich dahingehend, ob die anfragende Person die betreffend aller sich auf einen bestimmten Vertrag beziehenden Verkehrs- und Standortdaten die berechtigte Person ist und, falls dies nicht der Fall ist, ob die MB aufgrund dessen berechtigt bzw. verpflichtet ist, die gesamte Auskunft zu verweigern, weil diesfalls die einzige denkbare Rechtsgrundlage des Art 15 DSGVO (bzw § 1 Abs 3 DSG) nicht zur Verfügung steht.

4.2.7.5. Nach Jahnel (Kommentar zur Datenschutzgrundverordnung, Art. 15 DSGVO, Rz 17; Stand 01.12.2020, rdb.at) bezieht sich der Bestätigungsanspruch ebenso wie der Auskunftsanspruch nur auf „die eigenen personenbezogenen Daten der betroffenen Person“, nicht aber auf die Daten anderer. Gemäß Art. 15 Abs. 4 iVm Erwägungsgrund 63 darf das Auskunftsrecht die Freiheiten anderer Personen nicht beeinträchtigen.

4.2.7.6. Wie dargestellt, darf sich der Verantwortliche nur dann weigern, aufgrund des Antrages der betroffenen Person auf Wahrnehmung ihrer Rechte (gemäß den Artikeln 15 bis 22) tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

4.2.7.8. Eine derartige Einschätzung wird im Einzelfall durchgeführt werden müssen. Begründete Zweifel können beispielsweise bei telefonischen Anfragen vorliegen, da hier nicht direkt nachvollziehbar ist, wer spricht oder bei elektronischen Anfragen mit Absender – E-Mail-Adressen ohne Klarnamen. Nach den Erwägungsgründen hat der Verantwortliche alle vertretbaren Mittel in Anspruch zu nehmen, um die Identität einer betroffenen Person überprüfen zu können (Illibauer in Knyrim, wie oben, Rz 77).

4.2.7.8. Obwohl die diesbezüglichen Ausführungen erkennbar in Bezug auf die Frage erfolgten, ob die anfragende Person auch gleichzeitig die berechtigte Person ist, haben diese auch in der konkreten Konstellation Gültigkeit: Es ist zu prüfen, ob die MB in Bezug auf die festgestellten Anfragen des BF, die darin erfolgten Angaben und die eidesstattliche Erklärung alle vertretbaren Mittel in Anspruch genommen hat, die Identität des BF in Bezug auf die gesamten angefragten Verkehrs- und Standortdaten festzustellen.

4.2.7.9. Vor Erteilung einer Auskunft betreffend Verkehrs- und Standortdaten, die in Bezug auf den BF als Vertragspartner der MB generiert wurden, müsste - soweit diese nicht ohnehin aufgrund der gesetzlichen Bestimmungen des TKG bereits gelöscht sind - jedenfalls sichergestellt sein, dass lediglich durch den BF persönlich erzeugte (ihn betreffende) Verkehrs- und Standortdaten beauskunftet werden.

4.2.7.10. Nach Einschätzung des erkennendes Senates ist es, unter Berücksichtigung der besonderen Rechtsnatur von Verkehrs- und Standortdaten und deren Eignung, Benutzerprofile zu erstellen (siehe oben 4.2.6.), und deren Unterstellung unter ein strafbewährtes Kommunikationsgeheimnis, nicht zu beanstanden, dass die MB aufgrund deren festgestellten Wissenstandes betreffend die Urheber dieser Daten die Auskunft verweigert hat bzw. keine weiteren Mittel in Anspruch genommen hat, die Identität des BF als Auskunftswerber in Bezug auf seine persönliche Berechtigung betreffend der angefragten Daten zu prüfen.

4.2.7.11. Der MB ist dabei zuzubilligen, dass ihr aus ihrem Vertrag mit dem BF keinerlei Kenntnis über die persönliche Verwendung bzw. den Einsatz des Endgerätes zukommt und sie aufgrund des Vertrages auch keinerlei Berechtigung hat, diese Verwendung einer näheren Überprüfung zu unterziehen.

4.2.7.12. Der MB ist auch zuzugestehen, dass im Einzelfall die der belangten Behörde vorgelegte eidesstattliche Erklärung Beilage ./H keine hinreichende Absicherung für die MB bedeutet, dem BF alle sich auf den BF als Vertragspartner beziehenden Verkehrs- und Standortdaten, soweit diese noch (zulässigerweise) gespeichert werden, zu übermitteln.

„Eidesstattliche Erklärungen“ sind als ausdrückliches Rechtsinstrument in Österreich nicht geregelt. In einigen Verwaltungsvorschriften wird auf solche Erklärungen Bezug genommen. Strafrechtlich sind sie weitgehend bedeutungslos:

Bloße eidesstattliche Erklärungen sind kein Eid; die Abgabe solcher Erklärungen mit Täuschungs- und Bereicherungsvorsatz kann Betrug sein (Fabrizy/Michel-Kwapinski/Oshidari, StGB § 288 Rz 11, Stand 10.03.2022, rdb.at). Eine falsche Beweisaussage vor einer Verwaltungsbehörde (§ 289) wird nur dann von § 64 erfasst, wenn die Aussage unter Eid abgelegt oder bekräftigt wurde. Falsche eidesstattliche Erklärungen bzw Vermögensverzeichnisse werden nicht erfasst (Tipold in Leukauf/Steininger, StGB Update 2020, § 64 Stand 1.2.2020; rdb.at).

Auch zivilrechtlich spielen eidesstattliche Erklärungen nur eine untergeordnete Rolle:

In der Verwertung eidesstattlicher Erklärungen zur Begründung tragender Feststellungen liegt ein wesentlicher Verfahrensmangel (Lovrek in Fasching/Konecny Zivilprozessgesetze³, IV/1, § 503 Rz 58, Stand 1.9.2019, rdb.at).

Der BF konnte daher nicht darlegen, dass er sich betreffend aller Verkehrs- und Standortdaten im Bezug auf seinen Vertrag durch die festgestellte „eidesstattliche“ Erklärung“ gegenüber der MB hinreichend identifiziert hat.

4.2.8. Somit teilt der erkennende Senat im Ergebnis den im Verfahren eingenommenen Standpunkt der MB, dass Verkehrs- und Standortdaten aus dem Vertragsverhältnis zum BF nicht zu beauskunften waren, weil betreffend keiner Bestandteile dieser Verkehrsdaten eine hinreichende Identifizierung dahingehend vorliegt, dass es sich dabei tatsächlich und ausschließlich um den BF betreffende Daten handelt.

4.2.9. Zu diesem Ergebnis gelangte das BVwG auch im rezenten Erkenntnis vom 27.02.2023 zu W256 2234027 mit über den Einzelfall, welche Mittel der Betroffene zur Identifizierung nützt, hinausgehender Begründung:

Das bloße Vertrauen der mitbeteiligten Partei auf die Richtigkeit von Angaben des Beschwerdeführers als Auskunftswerber kann nicht als ausreichende Maßnahme zur Verhinderung eines allfällig möglichen Datenmissbrauchs angesehen werden.

Daran ändert auch nichts, dass der Beschwerdeführer weitere Benutzer genannt und deren (eidesstattliche) Einverständniserklärung zur gegenständlichen Datenauskunft sowie eine Meldeauskunft vorgelegt hat, weil dadurch keine Aussage über weitere allfällige (vom Auskunftswerber eben nicht genannter) Benutzer des Anschlusses getroffen wird. Eine hinreichende Möglichkeit zur Überprüfung der Richtigkeit der Angaben eines Auskunftswerbers und der von ihm angebotenen Zeugen besteht für die mitbeteiligte Partei jedenfalls nicht.

Dabei darf nicht übersehen werden, dass die Identitätsprüfung nach der DSGVO allein durch die mitbeteiligte Partei als verantwortliche Stelle zu erfolgen hat. Diese muss in der Lage sein, anhand der ihr zur Verfügung stehenden bzw. vom Auskunftswerber angebotenen Mittel, eine Zuordnung zum Betroffenen vorzunehmen. Die Durchführung eines gerichtlichen Verfahrens zur Klärung dieser Frage wird der verantwortlichen Stelle in der DSGVO nicht eingeräumt. Vielmehr muss diese – nach intern erfolgter Identitätsprüfung – eigenständig beurteilen können, ob eine ausreichende Identifizierung vorliegt oder nicht.

Gegenstand des Verfahrens ist daher allein die Frage, ob die mitbeteiligte Partei anhand der ihr zur Verfügung stehenden Mittel zur Identifikation in der Lage und insofern eine Auskunftserteilung allenfalls geboten gewesen wäre. Eine Identitätsprüfung durch das Bundesverwaltungsgericht – wie vom Beschwerdeführer angedacht – ist im Zuge eines solchen Verfahrens jedoch nicht vorgesehen. …

Schon angesichts der enormen Tragweite und des Umfanges der begehrten Datenschutzauskunft durfte sich die mitbeteiligte Partei daher mit den bloßen und für sie nicht näher überprüfbaren Angaben des Beschwerdeführers zu Recht nicht begnügen (vgl. Dix in Simitis|Hornung|Spiecker [Hrsg.], Datenschutzrecht, DSGVO mit BDSG, Art. 12 Rz 37, wonach demgegenüber das Erfordernis zusätzlicher Identifikationsmerkmale in Fällen, in denen nur allgemeine Informationen über den Zweck der Datenverarbeitung oder die Kategorien der verarbeiteten Daten abnimmt).

Dass der Gesetzgeber in § 138 TKG 2021 iVm § 6 Einzelentgeltnachweisverordnung 2011 (EEN-V 2011) dem Anbieter erlaubt, u.a. aufgrund einer schriftlichen Erklärung des Nutzers, dass er alle bestehenden bzw. zukünftigen Mitbenutzer des Anschlusses über eine unverkürzte Darstellung von passiven Nutzernummern informiert hat bzw. informieren wird, für zukünftige Abrechnungszeiträume passive Teilnehmernummern im Einzelentgeltnachweis vollständig anzugeben, kann damit nicht in Widerspruch gebracht werden. Durch diese Bestimmung soll vielmehr in Umsetzung des Art 7 der RL 2002/58/EG ein gerechter Ausgleich zwischen dem Interesse des Nutzers die Richtigkeit der vom Anbieter erhobenen Entgelte überprüfen zu können, und dem Interesse des (auch unbeteiligten) Benutzers auf Schutz seiner Privatsphäre geschaffen werden (EG 33). Dabei wird das Recht des Benutzers auf Schutz seiner Privatsphäre aufgrund der Information im Vorfeld und dem Umstand, dass lediglich bestimmte und zwar nach § 138 Abs. 1 Satz 1 TKG 2021 auf das unbedingt erforderliche Ausmaß beschränkte (zukünftig anfallende) Teilnehmerdaten betroffen sind, gegenüber dem Recht des Nutzers auf Überprüfung seiner Gebührenverrechnung zurückgedrängt. Lediglich in diesem zum Zweck der Überprüfung der Entgelte gesetzlich geregelten Fall lässt der Gesetzgeber eine Erklärung des Nutzers gelten. Der vorliegende Fall, der auf ein (unbeschränktes) Zugangsrecht zu in der Vergangenheit verarbeiteten Verkehrsdaten zu Auskunftszwecken abstellt, ist damit jedoch in keiner Weise vergleichbar.

Gleiches gilt für § 167 Abs. 4 TKG 2021, wonach der Anbieter mit Zustimmung des Nutzers Verkehrsdaten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die

Bereitstellung von Diensten mit Zusatznutzen verwenden kann. Da der Anbieter diese Daten gerade nicht mit sonstigen Benutzern in Verbindung bringen kann, soll die Gefahr eines Datenmissbrauchs und damit das Interesse dieser Personen am Schutz ihrer Privatsphäre nach hinten gerückt werden.

Vor diesem (rechtlichen) Hintergrund bestehen daher im vorliegenden Fall insgesamt keine Bedenken daran, dass sich die mitbeteiligte Partei aufgrund der ihr zur Verfügung stehenden und vom Beschwerdeführer angebotenen Mittel außer Stande sah, die zum Vertrag des Beschwerdeführers verarbeiteten Verkehrsdaten einer bestimmten Person und damit auch dem Beschwerdeführer zweifelsfrei zuzuordnen.

Dieser – teilweise erweiterten – Begründung schließt sich auch der hier erkennende Senat an.

4.3.1. Eine eingehende Auseinandersetzung mit der im Verfahren weitwendig diskutierten Frage, ob durch das TKG auch im Bezug auf die e-Datenschutz-Richtlinie lex-specialis Regeln vorliegen, die dem allgemeinen Auskunftsrecht der DSGVO vorgehen, konnte schon deshalb unterbleiben, weil aus den dargelegten Gründen die einzige in Frage kommende Anspruchsgrundlage für den BF, ein Auskunftsrecht nach Art. 15 DSGVO, jedenfalls nicht zur Verfügung steht, weil die MB glaubhaft machen konnte, die Identität des BF betreffend die Verkehrs- und Standortdaten nicht überprüfen zu können.

Zu dieser Problematik kann aber ausgeführt werden:

4.3.2. Zum Verhältnis der e-Datenschutz-Richtlinie zur DSRL:

Die e-Datenschutz-Richtlinie ist jünger als die DSRL und bereits Art. 1 Abs. 2 e-Datenschutz-Richtlinie sah vor, dass deren Vorschriften eine Detaillierung und Ergänzung der DSRL darstellen und gegenüber dieser als telekommunikationsspezifische Regelung spezieller sind (siehe EG 4 e-Datenschutz-Richtlinie). Nach Erwägungsgrund 12 e-Datenschutz-Richtlinie zielte diese auf die Ergänzung der Vorgaben der DSRL, nicht aber auf eine zusätzliche Erweiterung der bereits zur Umsetzung dieser Richtlinie erlassenen nationalen Vorschriften ab.

4.3.3. Zum Verhältnis der e-Datenschutz-Richtlinie zur DSGVO:

1. Die e-Datenschutz-Richtlinie kann mit Art. 95 eine fortgesetzte Geltung unter der DSGVO beanspruchen. Die sie umsetzenden nationalen Vorschriften werden ebenfalls erfasst und

sind als speziellere Vorschriften auf nationaler Ebene für Diensteanbieter verbindlich (Karg in Simits/Hornung/Spiecker, Art. 95, Rz 20).

2. Art. 95 DSGVO regelt das Verhältnis der DSGVO zur e-Datenschutz-Richtlinie. Dem Wortlaut nach soll die DSGVO natürlichen oder juristischen Personen „in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen“ keine zusätzlichen Pflichten auferlegen. Speziell datenschutzrechtliche Pflichten der e-Datenschutz-Richtlinie (genauer: Pflichten aus den nationalen Regelungen, die in Umsetzung der Vorgaben dieser Richtlinie geschaffen wurden) würden damit grundsätzlich jenen der DSGVO vorgehen. Es sollen, dem Wortlaut nach keine über die in der e-Datenschutz-Richtlinie bestehenden Vorgaben gemacht werden (Piltz in Gola, Art. 95, RZ 4). Die bereichsspezifischen Vorgaben Datenvorgaben der e-Datenschutz-Richtlinie sollten durch die Vorgaben der DSGVO nicht modifiziert oder aufgehoben werden (Karg in Simits/Hornung/Spiecker, Art. 95, Rz 16)

Mit Blick auf den Zweck der Vorschrift und die Vorgaben des europäischen Gesetzgebers sowohl in Art. 95 als auch Erwägungsgrund 173, geht die RL 2002/58/EG als Spezialregelung (lex specialis) den Pflichten der DSGVO unter zwei Vorrausetzungen vor: Zum einen muss es sich um Datenverarbeitungen handeln, die in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste stehen. Bezieht man in diese Überlegungen noch Erwägungsgrund 173 mit ein, der den Anwendungsbereich, anders als Art. 95, nicht auf Datenverarbeitungen in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste beschränkt, so dürfte die Spezialität der e-Datenschutz-Richtlinie auch für solche Datenverarbeitungen gelten, die nicht in diesem beschränkten Anwendungsbereich durchgeführt werden (wie insbesondere bei Art. 5 Abs. 3 e-Datenschutz-Richtlinie), sondern für alle der e-Datenschutz-Richtlinie entstammenden Rechte und Pflichten der Betroffenen gelten. Zum anderen müssen sich eventuell überschneidende Pflichten vom Ziel her decken. Nur wenn diese Voraussetzungen erfüllt sind, erlegt die DSGVO den Verantwortlichen keine zusätzlichen Pflichten auf (Piltz in Gola, Art. 95 DSGVO, Rz 10). Die DSGVO hat damit keinen direkten Einfluss auf die Vorgaben der e-Datenschutz-Richtlinie, nimmt an dieser keine inhaltlichen Änderungen vor oder verdrängt diese in ihrem Anwendungsbereich auch nicht (Piltz in Gola, Art. 95 DSGVO, Rz 11).

Gemäß Art. 1 Abs. 2 Satz 1 e-Datenschutz-Richtlinie stellen deren Bestimmungen „eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz 1 genannten Zwecke dar“. Der Begriff der Detaillierung spricht dafür, dass die RL 2002/58/EG lex specialis zur DSGVO ist und der Begriff der Ergänzung dafür, dass die datenschutzrechtlichen Pflichten der DSGVO weiterhin, also parallel zu jenen der RL 2002/58/EG gelten (Piltz in Gola, Art. 95 DSGVO, Rz 12). Nur wenn die zwei Voraussetzungen des Art. 95 erfüllt sind, treten die Pflichten des DSGVO, soweit sie sich in ihrer Zielvorgabe decken, hinter jenen der RL 2002/58/EG zurück (Piltz in Gola, Art. 95 DSGVO, RZ 12).

Nach Erwägungsgrund 10 der e-Datenschutz-Richtlinie gilt im Bereich der elektronischen Kommunikation die RL 95/46/EG vor allem für alle Fragen des Schutzes der Grundrechte und Grundfreiheiten, die von der e-Datenschutz-Richtlinie nicht spezifisch erfasst werden, einschließlich der Pflichten des Verantwortlichen und der Rechte des Einzelnen. Auch daraus lässt sich der Schluss ziehen, dass die Anwendungsbereiche der DSGVO und der e-Datenschutz-Richtlinie teilweise deckungsgleich sind und in diesem Fall die e-Datenschutz-Richtlinie vorgeht, soweit es sich um solche Pflichten handelt, die dieselben Ziele wie jene der DSVGVO verfolgen. Sind datenschutzrechtliche Pflichten und insbesondere Grundprinzipien zum Umgang mit personenbezogenen Daten (wie etwa Art. 5) in der e-Datenschutz-Richtlinie jedoch nicht adressiert, gelten die Vorgaben der DSGVO (Piltz in Gola, Art. 95 DSGVO, Rz 14).

4.3.4. Auch ohne das dargestellte Verhältnis fallbezogen einer abschließenden Beurteilung unterziehen zu müssen (siehe oben 4.2.) kann hier festgehalten werden, dass die spezifischen Regelungen des auf der e-Datenschutz-Richtlinie beruhenden TKG in beiden Fassungen sehr restriktive Bestimmungen enthalten, unter denen u.a. die hier gegenständlichen Verkehrs- und Standortdaten ermittelt oder verarbeitet werden dürfen, darüber hinaus Anordnungen zu unverzüglicher Löschung bzw Anonymisierung von Verkehrsdaten (mit Ausnahmen von für Verrechnungszwecke notwendigen Daten), weiters Verarbeitungsregeln für andere Standortdaten als Verkehrsdaten (§ 165, 167, 169 TKG 2021). In § 99 Abs 1 Satz 1 TKG 2003 („in diesem Gesetz“, somit auch geltend für die im Wesentlichen gleichlautende Bestimmung des § 167 TKG 2021) sollte die rechtliche Zulässigkeit und damit der Zweck der Speicherung von Verkehrsdaten im TKG abschließend geregelt werden. Insbesondere soll dadurch Rechtssicherheit dahingehend geschaffen, dass aus materiellen Auskunftsansprüchen in

anderen Materiengesetzen keine implizite Berechtigung oder gar Verpflichtung zur Speicherung von Verkehrsdaten abgeleitet werden kann (EBRV 1074 BlgNR XXIV. GP 19).

4.3.5. Im Ergebnis entspricht dies für die begehrte und hier noch gegenständliche Herausgabe von Kopien der Verkehrs- und Standortdaten der Verneinung des Auskunftsanpruchs mangels Identifizierbarkeit, wie oben ausführlich dargetan

4.4. Zu weiteren Ausführungen des BF in der Beschwerde:

4.4.1. Wenn der BF den Bescheid insbesondere im Hinblick darauf in Kritik zieht, dass die belangte Behörde ihre Entscheidung primär auf Entscheidungen gestützt hat, die vor Inkrafttreten der DSGVO gefällt wurden, so wird hiedurch eine unrichtige Rechtsanwendung nicht aufgezeigt, zumal das Hauptargument des Bescheides vom 27.03.2017 war, solange nicht mit ausreichender Sicherheit feststehe und objektiv nachweisbar sei, dass ein Auskunftswerber auch tatsächlich Nutzer von einem Endgerät sei, könne ein Auftraggeber zu recht die begehrte Auskunft über die Standortdaten verweigern. Gerade dieser Umstand ist letztendlich auch für die tatbestandliche Beurteilung des Art. 15 Abs. 1 DSGVO wesentlich.

4.4.2. Es mag aus Sicht des BF eine „abstrakte Spekulation“ sein, dass auch vom BF verschiedene Personen Benutzer des Endgerätes seien konnten. Wie dargelegt, war schon aus vertraglichen Gründen eine ausschließliche Nutzung durch den Vertragsinhaber keineswegs geboten. Aus Sicht des Telekommunikationsdiensteanbieters ist es sowohl aufgrund der Vertragsbeziehung als auch aufgrund technischer Möglichkeiten nicht möglich festzustellen, wer (jeweils) der Benutzer des Endgerätes ist, woraus sich zwingend ergibt, dass er Verkehrs- und Standortdaten zu beurteilen hat, betreffend derer ihm die tatsächliche Urheberschaft (Bewegung des Geräts durch eine Person) nicht bekannt ist.

4.4.3. Nicht erforderlich ist es zur Beurteilung des gegenständlichen Falles, technische Umstände der vom BF ins Treffen geführten Beispiele des Nutzers einer Smartwatch, eines Streamingaccounts, von Chatnachrichten auf einer Social-Media-Plattform sowie einer IP-Adresse zur erörtern. Ganz allgemein ist davon auszugehen, dass sich aufgrund des möglichen Auseinanderfallens der Person des Vertragspartners und allfälliger tatsächlicher Benutzer dann besondere datenschutzrechtliche Probleme stellen können, wenn der grundsätzlich Auskunftsverpflichtete begründete Zweifel hat, dass Daten zu beauskunften wären, die nicht dem Auskunftswerber zuzuordnen sind. Die Argumente, weshalb im vorliegenden Fall glaubhaft war, dass die MB den BF nicht identifizieren konnte, wurden oben ausführlich dargelegt.

4.4.4. Ob ein privates Mobiltelefon bestimmungsgemäß ein „höchstpersönlicher Gegenstand“ ist, kann ebenso dahingestellt werden, zumal evident die Weitergabe eines Mobiltelefons zur Benutzung durch andere möglich und selbst vertraglich zulässig ist.

4.4.5. Es mag aus Sicht des BF, sollte er tatsächlich der ausschließliche Nutzer des Mobiltelefons gewesen sein, unbefriedigend sein, der hier erfolgten Auskunftsverweigerung gegenüber zu stehen. So wie aus seiner Sicht allenfalls kein Beweisergebnis oder Indiz dafür spricht, dass er nicht der alleinige Nutzer wäre, bestehen auch strukturell für den Telekommunikationsdiensteanbieter keine Anhaltspunkte dafür, dass der Vertragspartner der ausschließliche Nutzer ist.

4.4.6. Eine abschließende Stellungnahme zu den in Punkt 4.3. der Beschwerde erfolgten Argumenten betreffend „lex-specialis-Derogation“, Normenkonflikt und Art. 95 DSGVO können dahinstehen, weil – wie mehrfach dargelegt - der erkennende Senat ohnehin die Erfüllung des Tatbestandes des Art 15 DSGVO durch den BF geprüft – und verneint hat.

4.4.7. Zuletzt ist zum Einwand des BF, die Datenschutzbehörde habe zu dem mit Eingabe vom 27.04.2022 vorgelegten Teilbescheid (Geschäftszahl geschwärzt) vom 22.04.2022 eine Gegenansicht zur Frage vertreten, ob die von einem bestimmten Endgerät erzeugten Daten personenbezogene Daten des dortigen Beschwerdeführers seien, auszuführen:

Die auf Seite 32 dieses Bescheides getroffenen Ausführungen könnten im Sinne des diesbezüglichen Vorbringens des BF verstanden werden, beziehen sich letztlich aber lediglich auf die Frage, ob personenbezogene Daten iSd Art. 4 Z 1 DSGVO im dortigen Zusammenhang vorlagen. Diese Frage wurde – grundsätzlich im Sinne der Rechtsansicht des BF – auch im gegenständlichen Zusammenhang bejaht, wobei - wie dargelegt - eine Identifizierbarkeit im Sinne einer Bejahung des Vorliegens personenbezogener Daten nicht zwingend gleichbedeutend mit einer Identifizierbarkeit iSd Art. 15 Abs. 1 DSGVO, einer Datenauskunftsanfrage im Bezug auf Daten des Betroffenen, ist.

5. Eine Verhandlung wurde nicht beantragt und war auch nicht erforderlich, zumal allein Rechtfragen zu lösen waren.

6. Der **Ausspruch der Zulässigkeit der Revision** gründet auf dem Umstand, dass – soweit ersichtlich – die Frage des Umfangs der Beauskunftungspflicht von Telekommunikationsanbietern gegenüber deren Vertragspartnern im Bezug auf Verkehrs- und Standortdaten höchstgerichtlich nicht geklärt ist. Gleiches gilt für die – aufgrund der hier getroffenen Lösung allerdings nicht präjudizielle – Frage des Verhältnisses der Bestimmungen

des TKG 2021, die keine ausdrücklichen Bestimmungen zum Auskunftsrecht enthalten, gegenüber der DSGVO.

Rechtsmittelbelehrung:

Gegen diese Entscheidung kann innerhalb von sechs Wochen ab Zustellung eine Beschwerde an den Verfassungsgerichtshof und/oder eine ordentliche bzw. außerordentliche Revision an den Verwaltungsgerichtshof erhoben werden. Für die Abfassung und Einbringung einer Beschwerde bzw. einer Revision gilt Anwaltspflicht.

Zur Erhebung einer Beschwerde an den Verfassungsgerichtshof ist berechtigt, wer sich durch die Entscheidung in einem verfassungsgesetzlich gewährleisteten Recht oder wegen Anwendung einer rechtswidrigen generellen Norm in Rechten verletzt erachtet. Eine Revision ist zulässig, wenn die Entscheidung von der Lösung einer Rechtsfrage grundsätzlicher Bedeutung abhängt.

Eine Beschwerde ist beim Verfassungsgerichtshof einzubringen. Eine Revision ist beim Bundesverwaltungsgericht einzubringen. Soweit gesetzlich nicht anderes bestimmt ist, ist eine Eingabengebühr von € 240,-- zu entrichten.

Eine Beschwerde an den Verfassungsgerichtshof und/oder eine Revision an den Verwaltungsgerichtshof sind nicht mehr zulässig, wenn nach Verkündung oder Zustellung des Erkenntnisses oder Beschlusses ausdrücklich darauf verzichtet wurde. Der Verzicht auf die Beschwerde an den Verfassungsgerichtshof ist bis zur Zustellung der Ausfertigung des Erkenntnisses oder Beschlusses dem Bundesverwaltungsgericht, nach Zustellung der Ausfertigung des Erkenntnisses oder Beschlusses dem Verfassungsgerichtshof schriftlich bekanntzugeben oder zu Protokoll zu erklären. Der Verzicht auf die Revision ist dem Bundesverwaltungsgericht schriftlich bekanntzugeben oder zu Protokoll zu erklären. Wurde der Verzicht nicht von einem berufsmäßigen Parteienvertreter oder im Beisein eines solchen abgegeben, so kann er binnen drei Tagen schriftlich oder zur Niederschrift widerrufen werden.

BUNDESVERWALTUNGSGERICHT

Gerichtsabteilung W274, am 03.03.2023

[redacted]

(Richter)

BVwG Bundesverwaltungsgericht	Unterzeichner	Bundesverwaltungsgericht
	Datum/Zeit	2023-03-03T13:41:36+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1054911121
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signatur.rtr.at/de/vd/Pruefung.html Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bvwg.gv.at/service/amtssignatur	