REPUBLIK ÖSTERREICH DATENSCHUTZRAT

An das
Bundesministerium für für Landwirtschaft,
Regionen und Tourismus
Sektion IV/1-2, Gruppe Telekom-Post

Per Mail:
tkp-begutachtung@bmlrt.gv.at

BMJ - StS DS (Stabsstelle Datenschutz)
Kompetenzstelle GDSR (Geschäftsstelle des Datenschutzrates)

dsr@bmj.gv.at
+43 1 52152 2918
Museumstraße 7, 1070 Wien

E-Mail-Antworten sind bitte
unter Anführung der Geschäftszahl an
dsr@bmj.gv.at zu richten.

Geschäftszahl: 2021-0.073.242

GZ des Begutachtungsentwurfes:
2020-0.482.482

Entwurf eines Bundesgesetzes, mit dem ein Telekommunikationsgesetz erlassen (Telekommunikationsgesetz 2020 – TKG 2020), das KommAustria-Gesetz (Komm-AustriaGesetz – KOG), die Strafprozeßordnung 1975 (StPO), das Polizeikooperationsgesetz (PolKG), das Polizeiliche Staatsschutzgesetz (PStSG) und das Sicherheitspolizeigesetz (SPG) geändert werden

Der Datenschutzrat hat in seiner 254. Sitzung am 29. Jänner 2021 einstimmig beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Allgemeines

1 Der Entwurf enthält **laut den Erläuterungen** folgende Hauptgesichtspunkte:

„Umsetzung der Richtlinie (EU) 2018/1972, ABl. L 321 vom 17.12.2018, S. 36-214, Neuordnung des TKG 2003.

Die Richtlinien 2002/19/EG, 2002/20/EG, 2002/21/EG und 2002/22/EG sowie die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates, auf denen das TKG 2003 aufbaute, wurden zum Teil erheblich geändert und in einer Richtlinie zusammengefasst. Die neue Struktur und die Vielzahl der Änderungen wurden daher zum Anlass genommen, die Richtlinie (EU) 2018/1972 in einem neuen TKG 2020 umzusetzen.

Mit dieser Richtlinie verfolgt der europäische Gesetzgeber das Ziel, ein kohärentes Binnenmarktkonzept für Frequenzpolitik und Frequenzverwaltung sowie geeignete Rahmenbedingungen für einen echten Binnenmarkt und leistungsfähige Netzbetreiber und Dienstanbieter zu schaffen. Ebenso sollen ein wirksamer Verbraucherschutz und möglichst gleiche Ausgangsbedingungen für die Marktteilnehmer garantiert werden. Aufgrund der stetig wachsenden Anforderungen an das Leistungsvermögen elektronischer Kommunikationsnetze ist außerdem die Schaffung von Anreizen für Investitionen in Hochgeschwindigkeitsbreitbandnetze („Netze mit sehr hoher Kapazität“) ein wesentlicher Punkt der Richtlinie. Um auch dem Grundsatz der Technologieneutralität Rechnung zu tragen und mit der technologischen Entwicklung Schritt halten, erfolgte zudem eine Anpassung der Begriffsbestimmungen.

Der Aufbau des Gesetzes folgt im Wesentlichen jenem der Richtlinie, jedoch unter Berücksichtigung der bewährten Struktur österreichischer Gesetze.

Die Richtlinie (EU) 2018/1972 folgt der Tendenz auf europäischer Ebene, auch Richtlinien immer präziser zu determinieren. Dementprechend ist der Handlungsspielraum für den nationalen Gesetzgeber weitgehend eingeschränkt. Die für die Regulierung notwendige Flexibilisierung hat in erster Linie durch die Vollziehung der Regulierungsbehörde zu erfolgen.

Mit dem vorliegenden Gesetz werden auch die notwendigen Anpassungen im KommAustria-Gesetz, in der Strafprozeßordnung 1975, im Polizeikooperationsgesetz (PolKG), im Polizeilichen Staatsschutzgesetz (PStSG) und im Sicherheitspolizeigesetz (SPG) vorgenommen.“

II. Datenschutzrechtliche Bemerkungen

A. Zu Art. 1 (Telekommunikationsgesetz 2020 – TKG 2020):

Grundsätzliches:

2 1. Aus datenschutzrechtlicher Sicht sollte die Neuerlassung des Telekommunikationsgesetzes zum Anlass genommen werden, die darin enthaltenen materienspezifischen Datenschutzregelungen (insbesondere im bisher 12., nunmehr 14. Abschnitt) vor dem Hintergrund des neuen unionsrechtlichen Datenschutzrechtsrahmens der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung; im Folgenden: DSGVO) einer umfassenden Prüfung zu unterziehen. So ist etwa das Verhältnis der Bestimmungen im TKG 2020

zu den Bestimmungen der DSGVO teilweise unklar (siehe dazu insbesondere die Anmerkung zu § 160).

3 Das komplexe Verhältnis zwischen materienspezifischen Datenschutzregelungen im TKG 2020 einerseits und in der DSGVO andererseits resultiert insbesondere daraus, dass die DSGVO in ihrem Art. 95 eine Ausnahme von ihren Verpflichtungen im Bereich elektronischer Kommunikationsdienste vorsieht. Diese Bereichsausnahme greift aber nur insoweit, als spezifische Verpflichtungen nach der Richtlinie 2002/58/EG (im Folgenden: ePrivacy-RL) bestehen, „die dasselbe Ziel verfolgen". Dementsprechend stellt sich in vielen Situationen die Frage, ob die Verpflichtungen der DSGVO gelten (weil die ePrivacy-RL hier keine Regelungen vorsieht oder diese nur einen Teilbereich der DSGVO abdecken oder andere Ziele verfolgen) oder nicht (weil materienspezifische Datenschutzregelungen bestehen und die DSGVO-Verpflichtungen „zusätzlich" auferlegt würden). Dies betrifft beispielsweise die Frage der Datensicherheitsmaßnahmen oder der Meldepflicht im Falle einer Verletzung des Schutzes personenbezogener Daten. Eine Klarstellung dieses Verhältnisses kann mangels Alternativen nur im Rahmen der materienspezifischen innerstaatlichen Umsetzung der ePrivacy-RL – dh. im Rahmen des TKG 2020 und den diesbezüglichen Erläuterungen – erfolgen.

4 2. Die Erläuterungen zum 14. Abschnitt erschöpfen sich weitgehend im Hinweis, dass die Bestimmungen im Wesentlichen der geltenden Rechtslage entsprechen. Eine solche Formalargumentation erscheint jedoch nicht geeignet, die Erforderlichkeit und Verhältnismäßigkeit der im TKG 2020 geregelten Datenverarbeitungen zu begründen. Zudem ist den Erläuterungen auch keine Gegenüberstellung der korrespondierenden Bestimmungen des TKG 2003 und des TKG 2020 zu entnehmen, sodass die Ermittlung der Materialien zu den jeweiligen Vorgängerbestimmungen für den Rechtsunterworfenen mit erheblichem Aufwand verbunden ist. Zudem wäre es nützlich, eine Textgegenüberstellung der geltenden mit der neuen Rechtslage zu erhalten.

5 Dementsprechend sollten datenschutzrechtliche Bestimmungen des TKG 2020 im Einzelnen erläutert oder, soweit es eine inhaltsgleiche Vorgängerbestimmung im TKG 2003 gibt und Ergänzungen oder Änderungen der Erläuterungen nicht erforderlich sind, zumindest auf diese verwiesen werden.

Zu § 31:

6 Abs. 2 sieht vor, dass Inhaber von Funkanlagen und Endeinrichtungen, soweit ihnen dies zumutbar ist, sowie unter Berücksichtigung des Grundrechtes auf Datenschutz im Sinne des

Datenschutzgesetzes und der DSGVO, geeignete Maßnahmen zu treffen haben, um eine missbräuchliche Verwendung auszuschließen.

7 Die allgemeine Verpflichtung zur Ergreifung von Datensicherheitsmaßnahmen ergibt sich bereits aus dem unmittelbar anwendbaren Art. 32 DSGVO und unterliegt insoweit einem Transformationsverbot. Soweit § 31 Abs. 2 darüber hinausgehende oder konkret zu ergreifende Maßnahmen zur Verhinderung einer missbräuchlichen Verwendung erfasst, wäre dies im Gesetz näher festzulegen bzw. zu erläutern. Die – kaum verständlichen – Erläuterungen scheinen jedoch davon auszugehen, dass es sich lediglich um einen Hinweis auf den aufgrund des Grundrechts auf Datenschutz und der DSGVO ohnehin geltenden Mindeststandard handelt. Aus der Formulierung der Erläuterungen („weil durch die Zumutbarkeitsgrenze der Pflicht zur Setzung der Maßnahmen die Einhaltung der datenschutzrechtlichen Vorschriften jedenfalls einen Mindeststandard garantieren muss“) geht auch nicht hervor, ob die datenschutzrechtlich gebotenen Datensicherheitsmaßnahmen jedenfalls als zumutbar zu erachten sind.

Zu § 44:

8 In Abs. 1 werden Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus gefordert. Die Erläuterungen nehmen Bezug auf die beiden ENISA Leitlinien „Technical Guidelines on Security Measures“ und „Technical Guidelines on Incident Reporting“, die eine nähere Ausführung der Verpflichtungen darstellen. Es wäre hilfreich, zumindest in den Erläuterungen klarzustellen, welchen Status diese Maßnahmen haben (verpflichtend oder Leitlinien/Empfehlungen, Minimalanforderungen …).

Zu § 129:

9 Zum Verhältnis zwischen den in § 129 geregelten Informationspflichten für Verträge und den datenschutzrechtlichen Informationspflichten nach den Art. 13 und 14 DSGVO wird auf das zu § 160 Gesagte verwiesen.

Zu § 137:

10 Zu Abs. 3 wird darauf hingewiesen, dass mit dem neuen unionsrechtlichen Datenschutzrechtsrahmen der datenschutzrechtliche Terminus „Zustimmung“ durch den Terminus „Einwilligung“ ersetzt wurde. Für den Fall, dass diese Bestimmung auf eine Zustimmung im datenschutzrechtlichen Sinn abstellt, wäre daher auch hier der Begriff „Einwilligung“ zu verwenden.

Zu § 144:

11 Das Recht auf Weiterleitung von E-Mails bei Beendigung des Vertrags weist Überschneidungen mit dem Recht auf Datenübertragbarkeit nach Art. 20 DSGVO auf. Zum Verhältnis zwischen diesen Rechten wird auf das zu § 160 Gesagte verwiesen.

Zu § 160:

12 1. Gemäß Abs. 1 gelten die Bestimmungen des 14. Abschnitts für die Verarbeitung und Übermittlung von „personenbezogenen Daten". Der Begriff der personenbezogenen Daten gemäß Art. 4 Z 1 DSGVO umfasst ausschließlich auf natürliche Personen bezogene Daten. Die im 14. Abschnitt umgesetzte Richtlinie 2002/58/EG (ePrivacy-RL) knüpft – mit wenigen Ausnahmen – an die Begriffsbestimmungen der DSGVO an (s. Art. 2 erster Satz ePrivacyRL iVm Art. 94 Abs. 2 DSGVO).

13 Die Begriffsbestimmungen in Abs. 3 beziehen sich jedoch (teilweise explizit) auch auf juristische Personen (s. zB „Stammdaten" gemäß Abs. 3 Z 5), wodurch zwangsläufig der Eindruck entsteht, dass der Begriff „personenbezogene Daten" in Abs. 1 auch Daten zu juristischen Personen umfassen muss.

14 Zur Vermeidung unterschiedlicher Begrifflichkeiten sollte in Abs. 1 – in Anlehnung an die Begriffsbestimmung in Abs. 3 Z 16, in der bereits klar zwischen auf natürliche und auf juristische Personen bezogenen Daten differenziert wird – auf „die Verarbeitung und Übermittlung von personenbezogen Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person" Bezug genommen werden. Dies wäre auch in allen weiteren Bestimmungen des TKG 2020, die auf personenbezogene Daten Bezug nehmen, zu prüfen.

15 Da die Übermittlung einen Unterfall der Verarbeitung darstellt (vgl. Art. 4 Z 2 DSGVO), sollte es in Abs. 1 zudem „die Verarbeitung einschließlich der Übermittlung" lauten.

16 2. Unbeschadet der nachstehenden Ausführungen zur Anordnung der Anwendung unmittelbar geltenden Unionsrechts (Pkt. 3) wird darauf hingewiesen, dass die in Abs. 1 zweiter Satz enthaltene Anordnung der Anwendung der DSGVO „auf die in diesem Bundesgesetz geregelten Sachverhalte" – zumal der 14. Abschnitt offenbar auch die Verarbeitung von Daten zu juristische Personen regelt (siehe dazu Pkt. 1) – dahingehend verstanden werden kann, dass die DSGVO auch auf die Verarbeitung von auf juristische Personen bezogenen Daten anzuwenden ist, soweit das TKG 2020 nicht anderes bestimmt. Damit würde der An-

wendungsbereich der DSGVO erheblich erweitert. Um diesbezüglich ein Spannungsverhältnis zum Unionsrecht zu vermeiden (die Übereinstimmung des im Entwurf vorliegenden Bundesgesetzes mit dem Recht der Europäischen Union ist vornehmlich vom do. Bundesministerium zu beurteilen), wird zur Erwägung gestellt, die in Abs. 1 zweiter Satz enthaltene Anordnung der Anwendung der DSGVO jedenfalls auf die Verarbeitung personenbezogener Daten einzuschränken.

17 3. Ungeachtet dessen lässt die Anordnung der subsidiären Anwendbarkeit der DSGVO in Abs. 1 außer Acht, dass es sich dabei um unmittelbar anwendbares Unionsrecht handelt. Eine gesonderte Anordnung der Anwendbarkeit der DSGVO ist daher nicht erforderlich und sollte von vornherein unterbleiben.

18 Der Umstand, dass die DSGVO gemäß deren Art. 95 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 auferlegt, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen (siehe dazu die allgemeine Anmerkung), ändert nichts an der grundsätzlichen Anwendbarkeit der DSGVO. Die allgemeine Anordnung einer bloß subsidiären Anwendbarkeit der DSGVO entspricht daher nicht dem tatsächlichen Verhältnis zwischen unmittelbar anwendbarem Unionsrecht und hätte somit auch aus diesem Grund zu unterbleiben.

19 Der allgemeine Verweis auf die subsidiäre Anwendbarkeit der DSGVO in Abs. 1 sollte daher ersatzlos entfallen. Stattdessen sollte – im Sinne der Rechtsklarheit und Rechtssicherheit – bei den einzelnen Bestimmungen, die materienspezifische datenschutzrechtliche Sonderregelungen enthalten, das Verhältnis zu den entsprechenden Bestimmungen der DSGVO im Gesetzestext klargestellt bzw. zumindest in den Erläuterungen näher dargestellt werden.

20 Soweit in den Erläuterungen zum 14. Abschnitt (spezifische Erläuterungen zu § 160 sind nicht vorhanden) ausgeführt wird, dass dieser Abschnitt im Wesentlichen der geltenden Rechtslage entspricht, ist zu bemerken, dass eine Klärung des Verhältnisses zwischen der – unmittelbar anwendbaren – DSGVO und den telekommunikationsrechtlichen Sonderregelungen bereits anlässlich des Inkrafttretens der DSGVO geboten gewesen wäre. Anders als im Falle der früheren, umsetzungsbedürftigen (Datenschutz-)Richtlinie 95/46/EG stehen den materienspezifischen Regelungen im Telekommunikationsrecht nämlich seit dem Inkrafttreten der DSGVO keine gleichrangigen innerstaatlichen Regelungen (DSG 2000) mehr gegenüber, sondern unmittelbar anwendbares Unionsrecht.

21 4. In Abs. 1 sollte im Hinblick auf das Erstzitat in § 31 Abs. 2 die Fundstellenangabe der Stammfassung des DSG entfallen.

22 5. Zur Begriffsbestimmung in Abs. 3 Z 16 („Verletzung des Schutzes personenbezogener Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person“) ist zu bemerken, dass auch auf den „unbefugten Zugang zu personenbezogenen Daten oder nicht öffentlich zugänglichen Daten einer juristischen Person“ abgestellt werden sollte. Unbeschadet dessen wird auf die Anmerkung zu § 164 hingewiesen.

Zu § 161:

23 In Abs. 3 zweiter Satz sollte im Sinne des datenschutzrechtlichen Determinierungsgebots und des Grundsatzes der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) die Bezugnahme auf die Überwachung von Nachrichten und die Auskunft über Daten einer Nachrichtenübermittlung durch einen Verweis auf die einschlägigen Bestimmungen der StPO ergänzt werden (wie dies bei den Verweisen auf Bestimmungen des FinStrG und des PStSG bereits der Fall ist).

Zu § 162:

24 Die in Abs. 1, 2 und 3 enthaltenen Verweise auf die „Bestimmungen der StPO“ sollten durch konkrete Paragraphenbezeichnungen präzisiert werden (s. auch die Anmerkung zu § 161 Abs. 3 zweiter Satz).

Zu § 163:

25 Zum Verhältnis zwischen den in § 163 geregelten spezifischen Datenschutzmaßnahmen und der DSGVO wird auf das zu § 160 Gesagte verwiesen.

Zu § 164:

26 1. § 164 gilt dem Wortlaut nach nur für Verletzungen des Schutzes personenbezogener Daten und deckt somit nur den auf natürliche Personen bezogenen Teilbereich der in § 160 Abs. 3 Z 16 definierten Verletzungen ab (womit der auf juristische Personen bezogene Teilbereich in der genannten Definition überflüssig wird). Die genannte Begriffsbestimmung und § 164 sollten dementsprechend näher miteinander abgestimmt werden:

27 Entweder wäre in § 164 – in Anpassung an die Begriffsbestimmung in § 160 Abs. 3 Z 16 – jeweils auf eine „Verletzung des Schutzes personenbezogener Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person“ Bezug zu nehmen oder – für den Fall, dass § 164 tatsächlich nur für Verletzungen des Schutzes auf natürliche Personen personenbezogener Daten gelten soll – die Begriffsbestimmung in § 160 Abs. 3 Z 16 entsprechend einzuschränken.

28 2. Zum Verhältnis zwischen der in § 164 vorgesehenen Meldepflicht bei Sicherheitsverletzungen und der DSGVO wird auf das zu § 160 Gesagte verwiesen. Durch die Wendung „unbeschadet der Bestimmungen … der DSGVO“ in Abs. 1 entsteht der Eindruck, dass zusätzlich zu den Meldepflichten auch die (überschneidenden) Meldepflichten nach Art. 33 und 34 DSGVO einzuhalten sind. Aus dem Gesetzestext sollte – gegebenenfalls in Zusammenschau mit den Erläuterungen – klar hervorgehen, inwieweit § 164 den Art. 33 und 34 DSGVO derogiert.

Zu § 165:

29 Hinsichtlich des Verhältnisses der in Abs. 3 geregelten Informationspflicht zu den Informationspflichten nach den Art. 13 und 14 DSGVO wird auf das zu § 160 Gesagte verwiesen.

Zu § 171:

30 Abs. 4 Z 2 zweiter Satz sieht eine Ermächtigung zur Verarbeitung der Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang einer Endeinrichtung vor, wenn eine aktuelle Standortfeststellung nicht möglich ist. Unklar ist, ob es sich dabei um eine eigenständige Datenverarbeitungsgrundlage handelt bzw. eine solche anderweitig vorhanden ist. § 171 Abs. 4 regelt grundsätzlich nur bestimmte Modalitäten (konkret: eine Ausnahme von der Pflicht zur Verwendung eines bestimmten Dateiformats für Übermittlungen) für dem Grunde nach an anderer Stelle geregelte Datenübermittlungen.

31 Im Sinne der Rechtsklarheit sollte die Rechtsgrundlage für die Verarbeitung der Standortkennung zum letzten Kommunikationsvorgang an geeigneter Stelle – etwa in jener Regelung, die auch sonst dem Grunde nach die Auskunft über Standortdaten regelt – und nicht „versteckt“ in einer Vorschrift über technische Verarbeitungsmodalitäten verankert werden.

Zu § 182:

32 Abs. 1 sieht eine Veröffentlichung von Entscheidungen von grundsätzlicher Bedeutung „unter Berücksichtigung des Datenschutzes“ durch die Regulierungsbehörde vor. Vor dem Hintergrund der Erläuterungen zu dieser Bestimmung wird empfohlen, konkrete Mindestparameter für die Depersonalisierung der veröffentlichten Entscheidung bereits im Gesetzestext zu verankern.

33 Soweit die Erläuterungen im vorliegenden Zusammenhang den Begriff „Anonymisierung“ verwenden, wird darauf hingewiesen, dass die Entfernung von einzelnen Personenbezügen (insb. Name) keine Anonymisierung im datenschutzrechtlichen Sinn darstellt, da die betroffene Person – insbesondere anhand der üblicherweise veröffentlichten Geschäftszahl – weiterhin identifizierbar bleibt (wenngleich für einen eingeschränkten Personenkreis). Der Begriff „Anonymisierung“ sollte daher vermieden werden, zumal dieser Begriff derzeit nicht ausreichend definiert ist und im vorliegenden Fall ohnedies eine Pseudonymisierung vorliegen dürfte.

Zu § 188:

34 § 188 sieht Verwaltungsstrafen für das Zuwiderhandeln gegen zahlreiche näher bezeichnete Verpflichtungen des TKG 2020 vor. Im Hinblick auf die obenstehenden Anmerkungen zu einzelnen Verpflichtungen des TKG 2020, die in unklarer Weise auf datenschutzrechtliche Verpflichtungen nach der DSGVO Bezug nehmen (siehe etwa die Anmerkungen zu § 31 Abs. 2 und § 164), wird darauf hingewiesen, dass eine klare Determinierung der Verpflichtungen auch mit Blick auf die daran anknüpfenden Verwaltungsstraftatbestände unerlässlich ist.

Zu § 209:

35 Abs. 1 ermächtigt näher bezeichnete Behörden, untereinander Informationen, „nicht aber personenbezogene Daten ohne ausdrückliche gesetzliche Grundlage“, auszutauschen, die für die Vollziehung des TKG 2020 notwendig sind. Diesbezüglich wird angeregt, einschlägige Rechtsgrundlagen für den Austausch personenbezogener Daten in den Erläuterungen anzuführen.

B. Zu Art. 6 (Änderung des Sicherheitspolizeigesetzes):

Zu Z 3 (§ 53 Abs. 3c):

36 In den Erläuterungen zu Art. 6 Z 1 bis 5 wird pauschal auf erforderliche Anpassungen an das Telekommunikationsgesetz 2020 ohne inhaltliche Änderungen hingewiesen. Auf den Entfall des § 53 Abs. 3c vierter bis letzter Satz dürfte dies allerdings nicht zutreffen; es scheint sich vielmehr um eine Rechtsbereinigung vor dem Hintergrund der Aufhebung der Regelungen über die Vorratsdatenspeicherung durch den Verfassungsgerichtshof (VfSlg. 19.892/2014) handeln. Die Erläuterungen sollten diesbezüglich nochmals geprüft werden.

C. Zur Wirkungsorientierten Folgenabschätzung:

37 Im Vorblatt wird zur Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO nichts Inhaltliches ausgeführt. Aus der Angabe „Keine“ ist nicht ersichtlich, ob und gegebenenfalls von wem eine Datenschutz-Folgenabschätzung vorzunehmen ist.

38 Nachdem der Entwurf unzweifelhaft die Verarbeitung zahlreicher personenbezogener Daten regelt, wäre auch im Rahmen der vereinfachten wirkungsorientierten Folgenabschätzung zumindest darzulegen, ob für Datenverarbeitungen insbesondere im Rahmen des TKG 2020 eine Datenschutz-Folgenschätzung gemäß Art. 35 DSGVO erforderlich ist oder nicht.

Für den Datenschutzrat
Der Vorsitzende:
OFENAUER
3. Februar 2021

Elektronisch gefertigt