Republik Österreich
Datenschutzbehörde

Barichgasse 40-42
A-1030 Wien
Tel.: +43-1-52152 302579

E-Mail: dsb@dsb.gv.at

GZ: D055.518

2021-0.474.423

Sachbearbeiterin: Mag. Katharina MAYRHOFER
Dr. Matthias SCHMIDL

Präsidium des Nationalrates

Stellungnahme der Datenschutzbehörde

per E-Mail: begutachtungsverfahren@parlament.gv.at

Betrifft: Stellungnahme der Datenschutzbehörde zum Entwurf des Bundesgesetzes, mit dem das Bundesstatistikgesetz 2000 und das Forschungsorganisationsgesetz geändert werden

Die Datenschutzbehörde nimmt in o.a. Angelegenheit aus Sicht ihres Wirkungsbereiches wie folgt Stellung:

Zu Art. 1 (Änderung des Bundesstatistikgesetzes 2000)

Allgemeines

Aus legistischer Sicht wird zunächst angemerkt, dass der Entwurf – ohne erkennbaren Grund – die Begriffe „DSGVO“ und „Datenschutz-Grundverordnung“ nebeneinander verwendet. Es wird daher angeregt, durchgehend denselben Begriff zu verwenden.

Der vorliegende Entwurf zeigt exemplarisch das Spannungsverhältnis zwischen der Datenverarbeitung für statistische Zwecke und dem Schutz personenbezogener Daten auf.

Sowohl die Verordnung (EG) Nr. 223/2009 („Statistik-Verordnung“) als auch die DSGVO schließen einander nicht aus, gelten für den jeweiligen Bereich und sind folglich für den jeweils anderen Bereich beachtlich.

Gemäß ErwGr. 22 der Verordnung (EG) Nr. 223/2009 führt diese Verordnung die Bestimmungen der Richtlinie 95/46/EG (nunmehr: DSGVO; siehe Art. 94 Abs. 2 DSGVO) im Hinblick auf europäische Statistiken näher aus.

Gleichzeitig nimmt die DSGVO an verschiedenen Stellen (ErwGr. 50, 156, 162 und 163, Art. 5 Abs. 1 lit. e, Art. 89) ausdrücklich auf Datenverarbeitungen für statistische Zwecke Bezug. ErwGr. 162 stellt darüber hinaus klar, dass die DSGVO „auch für Verarbeitung personenbezogener Daten zu statistischen Zwecken gelten" sollte.

Daraus folgt, dass der europäische Gesetzgeber mit den genannten Rechtsakten zwei legitime Ziele (Datenverarbeitung für statistische Zwecke und den Schutz personenbezogener Daten) verfolgt, die aber in keinem hierarchischen oder einander ausschließenden Verhältnis, sondern parallel zueinander stehen.

Auch der Verfassungsgerichtshof hat in VfSlg. 12.228/1990 ausgesprochen, dass datenschutzrechtliche Vorgaben bei statistischen Erhebungen und Veröffentlichungen zu berücksichtigen sind.

Die Kernaussage des genannten Erkenntnisses lautet dabei wie folgt:

Es kann in diesem Verfahren unerörtert bleiben, ob nicht auch bei aggregierten Daten einer Klasse dieser Größenordnung mit Hilfe von statistikexternen Informationen Rückschlüsse auf die Daten eines bestimmten Wirtschaftsunternehmens möglich sind, sodaß etwa Insider bei Branchen mit nur wenigen Unternehmern durch Verknüpfung mit ihnen bekannten Wirtschaftsdaten Rückschlüsse auf Daten anderer Unternehmungen ziehen können. Es muß nämlich durch den Gesetzgeber selbst (und nicht etwa nur im Wege einer Verordnung) sichergestellt werden, daß auf Grund der Veröffentlichung keine derartigen Rückschlüsse auf (schutzwürdige und durch das Grundrecht auf Datenschutz auch geschützte) Daten gezogen werden können.

Nach der ständigen Rechtsprechung der Datenschutzkommission bzw. der Datenschutzbehörde hat daher eine statistische Auswertung und Zurverfügungstellung dergestalt zu erfolgen, dass Rückschlüsse auf einzelne Personen mit vertretbarem Aufwand nicht möglich sind (siehe dazu insbesondere die Empfehlungen vom 22. Mai 2013, GZ K213.180/0021-DSK/2013, sowie vom 30. März 2015, GZ DSB-D215.611/0003-DSB/2014).

Ein Überschneidungsbereich zwischen der DSGVO und statistischen Daten ist folglich immer dann gegeben, wenn es möglich ist, Rückschlüsse auf einzelne Personen zu ziehen.

Nach der ständigen Rechtsprechung des Verfassungsgerichtshofes (siehe insbes. VfSlg. 18.146/2007) zur Qualität einer Eingriffsnorm iSd § 1 Abs. 2 DSG muss eine solche Norm „*ausreichend präzise, also für jedermann vorhersehbar, bezeichnen, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung der Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist. Der jeweilige Gesetzgeber muss somit iSd § 1 Abs. 2 DSG 2000 eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden. […] Auch der Europäische Gerichtshof für Menschenrechte (im Folgenden: EGMR) geht davon aus, dass ein Gesetz, das einen Eingriff in die durch Art. 8 EMRK gewährleisteten Rechte gesetzlich vorsieht, mit ausreichender Genauigkeit die Umstände festlegen muss, unter denen ein*

solcher Eingriff zulässig ist. Insbesondere müssen mit hinreichender Klarheit das Ausmaß und die Art des behördlichen Ermessens aus der gesetzlichen Regelung erkennbar sein (vgl. zB EGMR 25.3.1998, Kopp gg. die Schweiz, ÖJZ 1999, 115; EGMR 16.2.2000, Amann gg. die Schweiz, ÖJZ 2001, 71; EGMR 4.5.2000, Rotaru gg. Rumänien, ÖJZ 2001, 74).“

Auch die Rechtsprechung des EuGH geht in diese Richtung (siehe bspw. das Urteil vom 6. Oktober 2020, C-511/18, Rz 132):

Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine Regelung klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisiert verarbeitet werden, vor allem wenn eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht. Diese Erwägungen gelten in besonderem Maß, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht.

Zu berücksichtigen ist dabei, dass zwar die DSGVO selbst juristische Personen nur eingeschränkt schützt (siehe dazu insbesondere das Urteil des EuGH vom 9. November 2010, C-92/09 und C-93/09, Rz 53), die Verfassungsbestimmung des § 1 DSG hingegen auch juristischen Personen einen umfassenden Schutz gewährt (siehe dazu im Detail den Bescheid der Datenschutzbehörde vom 25. Mai 2020, GZ 2020-0.191.240, RIS).

Im Hinblick auf statische Daten macht es folglich keinen Unterschied, ob Rückschlüsse auf einzelne natürliche oder juristische Personen gezogen werden können.

Für das vorliegende Gesetzesvorhaben ergibt daraus Folgendes:

Zu § 6 und zu § 9

§ 6 Abs. 1 normiert, dass statistische Erhebungen - unter gewissen Voraussetzungen - durch Verordnung entsprechend der in Z 1 bis Z 9 vorgesehenen Rangordnung angeordnet werden können.

Gemäß § 9 Z 3 sind die Inhaber oder Verfügungsberechtigten über Daten gemäß § 6 Abs. 1 Z 5 bis 8 verpflichtet, entsprechend einer Anordnung gemäß § 4 Abs. 1 Z 1 oder 2 entweder einen Online-Zugang oder einen Fernzugriff (Remote Access) zu diesen Daten einzuräumen. Sollte dies technisch nicht möglich sein, so hat die Datenübermittlung in sonstiger elektronischer Form zu erfolgen.

Diese Bestimmungen postulieren ein weitgehendes Zugriffsrecht auf (externe) Datenbestände für statistische Zwecke, wobei die Inhaber oder Verfügungsberechtigen eine Verpflichtung zur Offenlegung trifft.

Die Datenschutzbehörde stellt nicht in Zweifel, dass eine derartige Zugriffsberechtigung – kombiniert mit einer Mitwirkungspflicht – im Ergebnis geeignet ist, statistischen Zwecken zu dienen.

Die Datenschutzbehörde vertritt jedoch die Ansicht, dass eine derart weitgehende Ermächtigung zum elektronischen Zugriff auf externe Datenbestände nicht bloß durch eine Verordnungsermächtigung gedeckt sein sollte, weil es diesbezüglich nämlich in der alleinigen Disposition des Verordnungsgebers stünde, den Zugriff auf externe Daten anzuordnen, wobei den Verfügungsberechtigten bzw. Inhabern keine Möglichkeit eingeräumt wird, den Zugriff prüfen zu lassen, wenn sie die Ansicht vertreten, dass dieser gegen datenschutzrechtliche Bestimmungen verstoßen könnte.

Vielmehr muss, um den Vorgaben des § 1 Abs. 2 DSG bzw. der DSGVO (Art. 6 Abs. 2 und 3 iVm ErwGr. 41 und 45) zu entsprechen, bereits die gesetzliche Grundlage ausreichend präzise festlegen, unter welchen Voraussetzungen personenbezogene Daten überhaupt verarbeitet werden dürfen, wobei auch geeignete Garantien zum Schutz personenbezogener Daten vorzusehen wären.

Auch Art. 89 Abs. 1 DSGVO verlangt, dass die Verarbeitung zu im öffentlichen Interesse liegenden statistischen Zwecken geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen gemäß der DSGVO unterliegt.

Eine weitgehend pauschale Verordnungsermächtigung, gepaart mit nicht vorhandenen Einschränkungen zugunsten des Schutzes personenbezogener Daten, erfüllt nach Ansicht der Datenschutzbehörde die genannten Anforderungen nicht (siehe dazu nochmals das Urteil des EuGH vom 6. Oktober 2020).

Soweit es den elektronischen Zugriff betrifft, wird auf die Ausführungen zu § 10 verwiesen.

Es wird daher angeregt, § 6 näher zu präzisieren.

Zu § 10 Abs. 5

Soweit es eine Datenübermittlung über eine „Schnittstelle für den elektronischen Datenaustausch“ betrifft, fehlen nach Ansicht der Datenschutzbehörde jegliche Anforderungen an eine derartige Schnittstelle (Art. 32 DSGVO).

In diesem Kontext ist zu bedenken, dass jede Schnittstelle potentiell geeignet ist, von Externen kompromittiert zu werden und damit gleichsam als „Einfallstor“ genutzt werden kann, um Zugriff auf interne Datenbestände zu erlangen. Der Datenschutzbehörde ist aus ihrer Vollzugspraxis bekannt, dass diese Möglichkeit nicht nur eine theoretische, sondern eine praktisch relevante ist und dass die „(Un-)Bekanntheit“ einer Einrichtung kein Maßstab dafür ist, ob Angriffe erfolgen. Im Gegenteil: Auch „unbekannte“ Einrichtungen können Ziele externer Angriffe sein. Sind Einrichtungen untereinander vernetzt, so haben mangelnde Datensicherheitsmaßnahmen einer Einrichtung sofort Auswirkungen auf alle mit ihr verbundenen Einrichtungen.

Es sollten daher, bspw. mittels Verordnung (siehe bspw. die IMA-VO, BGBl. II Nr. 339/2011), nähere Vorgaben zur Qualität einer derartigen Schnittstelle festgelegt werden, um einerseits diese Schnittstellen einheitlich zu definieren und andererseits um sicherzustellen, dass sie dem jeweiligen Stand der Technik entsprechen. Dabei könnte auf einschlägige Normen (ÖNORM, ISO-Norm) abgestellt werden.

Zu § 16 Abs. 3

§ 16 Abs. 3 spricht von *„personenbezogenen und unternehmensbezogenen Daten“.* Den Erläuterungen zu dieser Bestimmung ist zu entnehmen, dass diese Begriffe gewählt wurden, zumal die DSGVO sich ausschließlich auf natürliche Personen bezieht und die für die Statistik maßgebliche Verordnung (Verordnung (EG) Nr. 223/2009) von „*vertraulichen Daten von statistischen Einheiten*“ spricht.

Wie bereits im Einleitungsteil ausgeführt, sind Daten juristischer Personen jedenfalls vom Schutzbereich des § 1 DSG erfasst und können sohin auch „*unternehmensbezogene Daten*“ personenbezogene Daten im Sinne ebendieser Bestimmung sein (vgl. dazu nochmals VfSlg. 12.228/1990, wo auf „unternehmensbezogene Daten“ ausdrücklich Bezug genommen wird).

Zu § 19 Abs. 2

§ 19 regelt die Veröffentlichung von Statistiken.

Dazu wird nochmals ausdrücklich auf VfSlg. 12.228/1990 verwiesen.

§ 19 Abs. 2 sieht vor, dass eine Veröffentlichung bei Möglichkeit eines Rückschlusses auf einen bestimmten oder bestimmbaren Betroffenen erfolgen kann, wenn der Betroffene an der Geheimhaltung der Angaben kein schutzwürdiges Interesse hat.

Die Datenschutzbehörde merkt dazu an, dass die unionsrechtlichen Vorgaben zum Schutz personenbezogener Daten (Art. 1 und 2 DSGVO und insbesondere Art. 8 EU-GRC) das in § 1 Abs. 1 DSG vorgesehene „Privileg“ zugunsten eines mangelnden schutzwürdigen Interesses nicht kennen, weshalb eine unionsrechtkonforme – restriktive – Auslegung zu erfolgen hat.

Abgesehen davon geht aus dieser Bestimmung auch nicht hervor, wann und unter welchen Voraussetzungen kein schutzwürdiges Interesse vorliegt.

Nach Ansicht der Datenschutzbehörde wäre vom Gesetzgeber eine klare Gewichtung vorzunehmen, wann eine Veröffentlichung mit Personenbezug zu erfolgen und wann diese zu unterbleiben hat. So hat der EuGH in einer rezenten Entscheidung ausgesprochen, dass die DSGVO der gesetzlichen Anordnung einer Veröffentlichung mit Personenbezug nicht entgegensteht, sofern bestimmte Voraussetzungen erfüllt sind (Urteil vom 22. Juni 2021, C-439/19, Rz 104):

Auch wenn Art. 5 Abs. 1 Buchst. c der DSGVO die Verarbeitung personenbezogener Daten von der Einhaltung des Grundsatzes der „Datenminimierung“ abhängig macht, geht aus dem Wortlaut dieser Bestimmung nämlich klar hervor, dass mit ihr kein solches allgemeines und absolutes Verbot eingeführt werden soll und dass sie insbesondere der Übermittlung personenbezogener Daten an die Öffentlichkeit nicht entgegensteht, wenn diese Übermittlung im Sinne von Abs. 6 Abs. 1 Buchst. e der DSGVO für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichem Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Dies gilt auch dann, wenn die fraglichen Daten unter Art. 10 DSGVO fallen, sofern die Regelung, die diese Übermittlung gestattet, geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht.

Andererseits gestaltet sich die *„vorherige ausdrückliche schriftliche und rechtmäßige Zustimmung des Betroffenen*“ des § 19 Abs. 2 problematisch. Dabei stellt sich die Frage, ob die Zustimmung mit einer Einwilligung entsprechend Art. 4 Z 11 DSGVO gleichzusetzen ist und wäre es aus Sicht der Datenschutzbehörde wünschenswert, dies klarzustellen. Zu beachten wäre weiters, dass eine Einwilligung von einer betroffenen Person jederzeit und ohne Gründe widerrufen werden kann. Im Falle eines Widerrufs wären die Daten vom Verantwortlichen in Entsprechung von Art. 17 Abs. 1 lit. b DSGVO unverzüglich zu löschen.

Eine Überprüfung dieser Bestimmung wird angeregt.

Zu § 23 Abs. 2

Es wird angeregt, eine Definition von *„ähnlichen Leistungen“* in den Erläuterungen zu ergänzen.

Zu § 24 Abs. 7

Die in § 24 Abs. 7 vorgesehene „*Wahrung der Grundrechte des Datenschutzes*“ sollte näher dargelegt werden; allenfalls durch Verweis auf gesetzliche Bestimmungen (bspw. Art. 5 DSGVO).

Zu § 26

Es erscheint fraglich, ob „*nach Beseitigung der Identitätsdaten*“ eine Rückführbarkeit auf eine betroffene Person bereits ausgeschlossen werden kann.

Betreffend die Begrifflichkeit der „*unternehmensbezogenen Daten*“ wird auf die Ausführungen zu § 16 Abs. 3 verwiesen.

Überdies erscheint es aus Sicht der Datenschutzbehörde erforderlich, maximale Speicherfristen im Gesetz vorzusehen.

Zu § 31 Abs. 3 bis 14

Eingangs wird angemerkt, dass der Zugang „der Wissenschaft“ zu statistischen Daten von der DSGVO anerkannt wird (ErwGr. 157). Dennoch sind auch in diesem Fall die materiellen Vorgaben der DSGVO zur Gänze zu beachten.

In Bezug auf die erforderlichen Maßnahmen bei Fernzugriffen wird auf die Ausführungen zu § 10 verwiesen.

Es stellt sich die Frage, wann ein Einzelfall iSd Abs. 3 vorliegt, der die Zurverfügungstellung über Fernzugriff erforderlich erscheinen lässt. Dies sollte näher in den Erläuterungen dargelegt werden.

Abs. 4 sieht vor, dass Registerdaten für den Fernzugriff so aufzubereiten sind, dass „*keine Identifizierung der betroffenen Person und Unternehmen durch Name, Anschrift, oder anhand öffentlich zugänglichen Identifikationsnummern möglich ist*“. Entsprechend dem Wortlaut wird sohin eine „*direkte Identifikation*“ – iSd der Verordnung (EG) Nr. 223/2009 über europäische Statistiken – unmöglich gemacht; ein Rückschluss auf die betroffene Person über andere Merkmale- sohin eine „*indirekte Identifikation*“ - ist allerdings weiterhin möglich.

Dazu wird abermals auf VfSlg. 12.228/1990 sowie die zitierte Rechtsprechung der Datenschutzbehörde verwiesen.

Es erscheint fraglich, wie das Vorhandensein der „*gesicherten Umgebung*“ iSd § 31 Abs. 4 im konkreten Anlassfall dargelegt wird und wie die „*Unmöglichkeit der Abspeicherung von vertraulichen Daten*“ in der Praxis gewährleistet werden kann. Insbesondere das Risiko des Anfertigens einer Bildschirmkopie durch Fotografieren etc. durch Mitarbeiter wird wohl in der Praxis nie gänzlich ausgeschlossen werden können.

Folglich erscheint es aus Sicht der Datenschutzbehörde wünschenswert, in Abs. 6 eine ausdrückliche Zusicherung der Einhaltung der Vorgaben nach Abs. 4 aufzunehmen.

Die Datenschutzbehörde erachtet es überdies als erforderlich, dass die Rechtmäßigkeit der Zugriffe überprüfbar ist (bspw. durch Zugriffsprotokollierungen).

Im Hinblick auf den Verweis in Abs. 12, wonach Art. 83 DSGVO neben einer Verletzung des Statistikgeheimnisses unberührt bleibt, ist fraglich, ob diese Form der Anordnung überhaupt zulässig ist. Art. 83 DSGVO ist unmittelbar anwendbar und kann durch innerstaatliche Normen weder begrenzt noch ausgeschlossen werden. Eine allfällige Nichtanwendbarkeit stellt sich am ehesten im Lichte des Grundsatzes „*ne bis in idem*“, was jedoch nur im Rahmen einer Einzelfallbeurteilung erfolgen kann.

Weiters sollte die konkrete Ausgestaltung eines Ausschlusses näher in den Erläuterungen dargelegt werden (bspw. die Dauer des Ausschlusses etc.).

Zu § 31a

Soweit in § 31a auf § 31 Bezug genommen wird, wird auf die obigen Ausführungen verwiesen.

Ganz allgemein wird angemerkt, dass die Verantwortung für die Einhaltung der Vorgaben der DSGVO auch im Falle der Beauftragung der Statistik Österreich den jeweiligen datenschutzrechtlichen Verantwortlichen (hier wohl § 2d Abs. 2 Z 3 FOG) trifft und eine „Auslagerung“ dieser Verantwortung in der DSGVO nicht vorgesehen ist.

Daher ist bspw. zu Abs. 1 Z 2 anzumerken, dass die Einhaltung von Datensicherheitsmaßnahmen (Art. 32 DSGVO) Sache des Verantwortlichen und nicht des Auftragsverarbeiters ist.

§ 31a Abs. 2 ist nicht zweifelsfrei zu entnehmen, ob die registerführenden Stellen oder die jeweiligen Bundesminister als datenschutzrechtliche Verantwortliche anzusehen sind. Dies wäre ergänzend auszuführen.

Zu § 31b

Auch bei Verknüpfungen wäre sicherzustellen, dass nach einer erfolgten Auswertung kein Personenbezug möglich ist bzw. eine Verknüpfung *a priori* überhaupt nur dann erfolgen darf, wenn ein Personenbezug (weitgehend) ausgeschlossen werden kann.

Zu § 31d Abs. 6

Es wird auf die Ausführungen zu § 31a Abs. 2 verwiesen.

Zu Art. 2 (Änderung des Forschungsorganisationsgesetzes)

Zu § 2d

Abs. 1 Z 1 sieht vor, dass Zugriffsprotokollierungen nunmehr lediglich „*im notwendigen Ausmaß*“ erfolgen sollen – dahingegen normiert die geltende Fassung eine lückenlose Protokollierung. Es wird in den Erläuterungen nicht näher dargelegt, weshalb die aktuelle Praxis überschießend sein soll und erschließt sich der Datenschutzbehörde daher nicht, aus welchem Grund von der lückenlosen Protokollierung abgegangen werden soll und.

Es wird dazu angemerkt, dass im Falle eines Verfahrens vor der Datenschutzbehörde (oder den Gerichten; siehe dazu insbesondere Art. 82 DSGVO und die in Abs. 3 normierte Beweislastumkehr!) den jeweiligen Verantwortlichen die Pflicht trifft, die Einhaltung der Grundsätze der DSGVO – hier: Art. 5 Abs. 1 lit. a, b und f – nachweisen zu können (Art. 5 Abs. 2 DSGVO). Insofern ist die derzeitige Pflicht zur lückenlosen Protokollierung jedenfalls als Schutzfunktion zu werten, die es dem Verantwortlichem ermöglicht, seiner Rechenschaftspflicht nachzukommen. Eine lediglich lückenhafte Protokollierung wäre demnach eindeutig zum Nachteil des Verantwortlichen aber auch der betroffenen Personen.

Es wird daher angeregt, die geltende Fassung beizubehalten.

Zu Abs. 2 Z 3 ist anzumerken, dass nicht ersichtlich ist, weshalb in diesem Zusammenhang auf die in Art. 12 Abs. 3 DSGVO vorgesehene Frist verweisen wird. Dies möge gegebenenfalls in den Erläuterungen dargelegt werden.

Sofern Abs. 2a vorsieht, dass die Stammzahlenregisterbehörde die in Z 1 und Z 2 leg. cit. vorgesehenen Daten „*auf jede beliebige Art*“ verarbeiten darf, ist auszuführen, dass diese Bestimmung wohl nicht als ausreichend determiniert iSd obigen Ausführungen anzusehen ist und bei dieser Bestimmung auch nicht von einem verhältnismäßigen Eingriff in das Grundrecht auf Datenschutz ausgegangen werden könnte.

Die Datenschutzbehörde regt an, diese Bestimmung unter Bedachtnahme auf die obigen Ausführungen zu überarbeiten.

Zu den jeweiligen Vorblättern

Es ist den jeweiligen Vorblättern nicht zu entnehmen, ob es für erforderlich erachtet wird, eine Datenschutz-Folgenabschätzung (DSFA) entsprechend Art. 35 Abs. 10 DSGVO im Zusammenhang mit den gegenständlichen Gesetzesvorhaben durchzuführen. Die Durchführung einer solchen legt § 2 Abs. 2 Z 5 bzw. Abs. 3 Z 1 und 5 DSFA-V, BGBl. II Nr. 278/2018, zumindest nahe.

Dies wäre zu ergänzen.

Die Datenschutzbehörde steht für allfällige weitergehende Gespräche gemäß Art. 57 Abs. 1 lit. c DSGVO iVm § 21 Abs. 1 DSG zur Verfügung.

3. August 2021
Für die Leiterin der Datenschutzbehörde:
SCHMIDL

REPUBLIK ÖSTERREICH DATENSCHUTZBEHÖRDE @ AMTSSIGNATUR	Unterzeichner	serialNumber=1831845058,CN=Datenschutzbehörde,C=AT
	Datum/Zeit	2021-08-03T13:22:30+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.dsb.gv.at/-/amtssignatur
	Hinweis	Dieses Dokument wurde amtssigniert.