REPUBLIK ÖSTERREICH DATENSCHUTZRAT

An das
Bundeskanzleramt
Ballhausplatz 2
1010 Wien

Mit E-Mail:
nis@bka.gv.at

BMJ - 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: 2024-0.326.376

GZ des Begutachtungsentwurfes:
2024-0.220.735

Entwurf eines Bundesgesetzes, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden;
Stellungnahme des Datenschutzrates

Der Datenschutzrat hat in seiner 277. Sitzung am 2. Mai 2024 einstimmig beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Materialien zum Entwurf

1 Laut den Erläuterungen bietet die zunehmende Durchdringung nahezu aller Bereiche der Gesellschaft und des täglichen Lebens mit digitaler Technologie erhebliche Chancen und Möglichkeiten. Gleichzeitig würde die Gesellschaft dadurch aber auch angreifbarer und abhängiger von der Vertraulichkeit, Verfügbarkeit und Integrität von digital verarbeiteten und gespeicherten Informationen, mit anderen Worten: von der Sicherheit im Cyberraum. Staaten, Gruppierungen, aber auch kriminellen Akteuren würden sich immer neue Wege eröffnen, die digitale Vernetzung für Spionage, Sabotage oder andere kriminelle Aktivitäten nutzbar zu machen. Dabei könnten schon die Fähigkeiten einzelner krimineller Individuen genügen, um Cyberangriffe mit im Vorfeld nicht abschätzbaren Folgen für die

Sicherheit Österreichs durchzuführen. Immer mehr österreichische Unternehmen wären in den vergangenen Jahren Opfer von Cyberattacken geworden, wie insbesondere von Datenverschlüsselungsangriffen (Ransomware-Attacken) und Angriffen auf die Verfügbarkeit ihrer IT-Systeme (DDoS-Attacken). Im Lichte dieser Entwicklungen würde deutlich, dass moderne Demokratien ein entsprechendes organisatorisches, personelles und finanzielles Fundament benötigen, um die wachsende Bedeutung von Cybersicherheit gesamtstaatlich abbilden zu können.

2 Aufgrund der seit Jahren rapide zunehmenden Bedeutung von Cybersicherheit habe die Europäische Union (EU) laut den Erläuterungen mehrere Rechtsakte erlassen, die der unionsweiten Erhöhung der Cybersicherheit dienen würden. Mit der Verordnung (EU) 2021/887 vom 20. Mai 2021 wurde das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit eingerichtet und in diesem Zusammenhang die Benennung von nationalen Koordinierungszentren durch die Mitgliedstaaten vorgesehen. Mit der Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), welche am 16. Jänner 2023 in Kraft getreten sei, würde unter anderem eine erhebliche Steigerung der zu beaufsichtigenden Einrichtungen sowie eine erhebliche Ausweitung des Aufgabenspektrums der NIS-Behörden vorgesehen.

3 Das NISG 2024 würde das nationale Koordinierungszentrum für Cybersicherheit gemäß der Verordnung (EU) 2021/887 errichten und die NIS-2-Richtlinie umsetzen.

II. Inhaltliche Bemerkungen

A. Grundsätzliches

4 a. Der vorliegende Entwurf regelt zahlreiche Datenverarbeitungen und legt im Detail Datensicherheitsmaßnahmen fest.

5 Der Datenschutzrat hat in seiner Stellungnahme zum Begutachtungsentwurf des Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) vom 24. Oktober 2018, GZ BMVRDJ-818.020/0002-DSR/2018, im Rahmen der Vorbemerkungen auf die Grundsätze der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) und Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) sowie auf den Verhältnismäßigkeitsgrundsatz (§ 1 Abs. 2 DSG)

hingewiesen. Zudem sollte hinsichtlich jener Datenverarbeitungen, die über die unionsrechtlichen Vorgaben hinausgehen, näher erläutert werden, weshalb diese notwendig sind. Insbesondere wären – laut der zit. Stellungnahme des Datenschutzrates – die verarbeiteten personenbezogenen Daten auch im Gesetzestext zu nennen.

6 Diese datenschutzrechtlichen Fragestellungen betreffen grundsätzlich auch den vorliegenden Entwurf des NISG 2024.

7 Zu berücksichtigen ist insbesondere die Rechtsprechung des Verfassungsgerichtshofes. Im Hinblick auf § 1 Abs. 2 DSG iVm Art. 18 B-VG und die Anforderungen an den Grad der Bestimmtheit gesetzlicher Eingriffe in das Grundrecht auf Datenschutz hat der Verfassungsgerichtshof festgehalten, dass eine Ermächtigungsnorm iSd § 1 Abs. 2 DSG ausreichend präzise, also für jedermann vorhersehbar, bezeichnen muss, unter welchen Voraussetzungen die Ermittlung bzw. die Verarbeitung der Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist (VfSlg. 18.146/2007; 16.369/2001; zuletzt Erkenntnis vom 11.12.2019, G 72-74/2019 ua., Rz 64 ff ua.).

8 Es sollte daher allgemein im gesamten Entwurf präzisiert werden, welche personenbezogenen Daten (insbesondere auch, ob besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 und personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO) verarbeitet werden. Diese Fragen stellen sich insbesondere auch iZm den im Entwurf mehrfach geregelten Übermittlungen von Daten, der Zusammenarbeit von diversen Behörden und Stellen (zB gemäß § 20 Abs. 2) bzw. dem Austausch von Daten. Die pauschale Anordnung, dass die „erforderlichen“ personenbezogenen Daten verarbeitet werden dürfen (zB gemäß § 42 Abs. 1), erscheint jedenfalls nicht ausreichend.

9 Zudem sollte auch zumindest erläutert werden, wer jeweils der Verantwortliche (Art. 4 Z 7 DSGVO) der Datenverarbeitungen ist (dies ist derzeit nur zT aus dem Entwurf ersichtlich), so etwa im Hinblick auf die Operative Koordinierungsstruktur („OpKoord“) gemäß § 14).

10 Im Übrigen sollte hinsichtlich jener Datenverarbeitungen, die allenfalls auch über die unionsrechtlichen Vorgaben hinausgehen, näher erläutert werden, weshalb diese erforderlich sind.

11 b. Mehrfach wird im Entwurf auf die sinngemäße Anwendung von Rechtsvorschriften verwiesen (zB in § 37 Abs. 3).

12 Diesbezüglich wird darauf hingewiesen, dass eine „sinngemäße“ (oder „entsprechende“) Anwendung anderer Rechtsvorschriften nicht angeordnet werden darf. Es ist entweder uneingeschränkt auf die anderen Rechtsvorschriften in ihrer bestehenden Fassung zu verweisen oder aber anzugeben, mit welcher Maßgabe sie angewendet werden sollen.

13 Dies gilt vor dem Hintergrund des datenschutzrechtlichen Determinierungsgebots umso mehr, wenn es um Regelungen geht, die eine Verarbeitung personenbezogener Daten umfassen.

14 Diese Vorgaben wären im Entwurf entsprechend zu berücksichtigen.

B. Zum Entwurf

1. Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024)

Allgemeines:

15 Angemerkt wird, dass nach der Promulgationsklausel offenbar die Festlegung des NISG 2024 als Artikel 1 der Sammelnovelle fehlt. Es wird davon ausgegangen, dass es sich bei den gegenständlichen Regelungen (§§ 1 bis 51) um die Erlassung des NISG 2024 handelt.

Zu § 8:

16 Gemäß § 8 Abs. 11 könnten Computer-Notfallteams (CSIRTs) die Aufgaben gemäß § 8 Abs. 1 Z 2 bis 4 auch gegenüber sonstigen Einrichtungen oder Personen wahrnehmen, sofern diese von einem Risiko oder einem Cybersicherheitsvorfall betroffen sind.

17 Es sollte in § 8 Abs. 11 konkretisiert werden, welche sonstigen Einrichtungen oder Personen von dieser Regelung betroffen sein können. Gleiches ist zu § 43 Abs. 4 anzumerken, welcher auf § 8 Abs. 11 verweist.

Zu § 10:

18 Das in § 10 Abs. 2 normierte Weisungsrecht sollte dahingehend konkretisiert werden, dass es nur der Vollziehung der Gesetze im Kontext mit der Cybersicherheit dient.

Zu § 14:

19 Gemäß § 14 Abs. 5 dürfen die an der OpKoord teilnehmenden Einrichtungen die zum Zweck der Organisation der OpKoord und die zur Wahrnehmung der Aufgaben gemäß § 14 Abs. 1 erforderlichen personenbezogenen Daten gemäß § 42 Abs. 2 verarbeiten.

20 Unklar erscheint, welche personenbezogenen Daten in dieser Hinsicht erforderlich sind, dies vor allem auch vor dem Hintergrund, dass § 42 Abs. 2 die Datenarten nur demonstrativ aufzählt.

21 Vor diesem Hintergrund müsste die Regelung konkretisiert werden. Diesbezüglich wird auf die Anmerkungen unter Pkt. II.A. hingewiesen.

Zu § 17:

22 § 17 Abs. 2 legt fest, dass wesentliche und wichtige Einrichtungen an den vom Bundesminister für Inneres betriebenen IKT-Lösungen teilnehmen und festlegen können, welche Daten an den Bundesminister für Inneres übermittelt werden.

23 Unklar erscheint, um welche (allenfalls personenbezogenen) Daten es sich handelt. Auch diesbezüglich wird auf die Anmerkungen unter Pkt. II.A. hingewiesen.

24 Gleiches ist zu den „personenbezogenen technischen Daten“ gemäß § 17 Abs. 3 anzumerken.

Zu § 20:

25 a. Gemäß § 20 Abs. 2 hat die Cybersicherheitsbehörde für die Erfüllung ihrer gesetzlichen Aufgaben und Pflichten insbesondere mit den in den Z 1 bis 6 genannten Behörden und Einrichtungen zusammenzuarbeiten.

26 Es sollte abschließend geregelt werden, mit welchen Behörden und Einrichtungen die Cybersicherheitsbehörde zusammenzuarbeiten hat, zumal in diesem Zusammenhang auch Informationen über relevante Umstände ausgetauscht werden können. Auf die unter Pkt. II.A. zit. Rechtsprechung des Verfassungsgerichtshofes wird idZ hingewiesen.

27 b. Weiter sollte in § 20 Abs. 7 klargestellt werden, ob bzw. welche personenbezogenen Daten vom Informationsaustausch mit der Aufsichtsstelle umfasst sein können.

Zu § 21:

28 a. Die Cybersicherheitsbehörde und die Datenschutzbehörde arbeiten gemäß § 21 Abs. 1, unbeschadet ihrer Zuständigkeiten und Aufgaben nach der DSGVO und dem DSG, bei der Bearbeitung und der Anordnung von Abwehr- und Abhilfemaßnahmen von Cybersicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten iSd Art. 4 Z 12 DSGVO und § 36 Abs. 2 Z 1 DSG führen, eng zusammen und tauschen relevante Informationen aus. Der Bundesminister für Inneres gewährt der Datenschutzbehörde zu diesem Zweck Zugang zum Register gemäß § 29.

29 Es sollte näher erläutert werden, wie die Zusammenarbeit dieser Behörden „unbeschadet ihrer Zuständigkeiten und Aufgaben nach der DSGVO und dem DSG“ vorgenommen wird bzw. was unter dieser Wendung zu verstehen ist. Unklar ist auch, was unter einer „engen“ Zusammenarbeit zu verstehen ist und welche Informationen „relevant“ sind.

30 Weiters stellt sich die Frage, wie die von Art. 52 DSGVO vorgesehene völlige Unabhängigkeit der Aufsichtsbehörde (Datenschutzbehörde) bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse gewährleistet wird. Hingewiesen wird idZ auch auf Art. 58 Abs. 6 DSGVO, wonach jeder Mitgliedstaat durch Rechtsvorschriften vorsehen kann, dass seine Aufsichtsbehörde neben den in den Art. 58 Abs. 1, 2 und 3 DSGVO aufgeführten Befugnissen über zusätzliche Befugnisse verfügt. Die Ausübung dieser Befugnisse darf nicht die effektive Durchführung des Kapitels VII beeinträchtigen. Auch diesbezüglich sollten entsprechende Erläuterungen aufgenommen werden.

31 b. Besteht Grund zur Annahme, dass ein Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den §§ 32 und 34 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten zur Folge hat, die gemäß Art. 33 DSGVO zu melden ist, hat die Cybersicherheitsbehörde gemäß § 21 Abs. 2 unverzüglich, möglichst innerhalb von 72 Stunden, die Datenschutzbehörde zu unterrichten. Betrifft die Verletzung des Schutzes personenbezogener Daten Betroffene in einem anderen Mitgliedstaat der Europäischen Union, hat die Cybersicherheitsbehörde ebenfalls die Datenschutzbehörde zu unterrichten.

32 Es sollte erläutert werden, in welchem Verhältnis die Regelung des § 21 Abs. 2 zu Art. 33 DSGVO (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde) steht. Dies betrifft insbesondere eine mögliche parallele Meldung desselben Vorfalles durch die Cybersicherheitsbehörde und die betroffene Einrichtung.

Zu § 24:

33 Es wird angeregt, eine Möglichkeit vorzusehen, auf Antrag potentiell betroffener wesentlicher und wichtiger Einrichtungen mit Bescheid festzustellen, ob sie in den Anwendungsbereich dieses Gesetzes fallen.

Zu § 27:

34 Unter den in § 27 Abs. 1 geregelten Voraussetzungen gelten Bestimmungen von sektorspezifischen Rechtsakten anstelle der im NISG 2024 geregelten Bestimmungen, wenn ua. der Bundesminister für Inneres diese Bestimmungen und deren Gleichwertigkeit durch Verordnung festgestellt hat.

35 Angemerkt wird vorweg, dass nicht klar erkennbar ist, welche sektorspezifischen unionsrechtlichen Rechtsakte und Bestimmungen gemeint sind. Dies sollte zumindest noch näher erläutert werden.

36 Hinsichtlich der Verordnungsermächtigung wird zudem angemerkt, dass eine Verarbeitung von personenbezogenen Daten bereits aus dem Gesetz „vorhersehbar" sein muss, um in einer Verordnung angeordnet werden zu können. Es sollte geprüft werden, ob die in § 27 Abs. 1 vorgesehene (nur allgemein geregelte) Verordnungsermächtigung der unter Pkt. II.A. zit. Rechtsprechung des Verfassungsgerichtshofes – insbesondere hinsichtlich der Vorhersehbarkeit der Datenverarbeitung – tatsächlich entspricht.

37 IdZ sollten auch die sonstigen im Entwurf geregelten Verordnungsermächtigungen (zB in § 29 Abs. 5 hinsichtlich der Anforderungen an Angaben, in § 33 Abs. 6 hinsichtlich der „notwendigen Inhalte" oder in § 35 Abs. 3 hinsichtlich der „weitere[n] Kriterien und nähere[n] Regelungen") nochmals geprüft werden.

Zu § 34:

38 Die Cybersicherheitsbehörde kann gemäß § 34 Abs. 6 personenbezogene Daten gemäß §§ 42 und 43 nach erfolgter Interessenabwägung bezüglich der Auswirkungen auf die Betroffenen veröffentlichen, um die Öffentlichkeit über Cybersicherheitsvorfälle zu unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von Cybersicherheitsvorfällen erforderlich ist oder die Offenlegung des Cybersicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.

39 Die Regelung erscheint zu unbestimmt. Die Ausführungen in den Erläuterungen, dass bei der Abwägung auf den Verhältnismäßigkeitsgrundsatz gemäß § 1 Abs. 2 DSG und den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO Bedacht zu nehmen ist,

sind zwar inhaltlich richtig, können entsprechende detaillierte Erläuterungen zur Interessenabwägung aber nicht ersetzen. Vor allem sollte konkreter (etwa auch anhand von Beispielen) erläutert werden, nach welchen Gesichtspunkten die Interessenabwägung vorgenommen wird.

40 Fraglich ist überdies, was „auf sonstige Weise im öffentlichen Interesse“ liegt. Auch dies sollte näher dargelegt werden.

41 Hinsichtlich der in §§ 42 und 43 geregelten Datenarten wird angemerkt, dass die Datenarten in diesen Regelungen zT nur demonstrativ genannt sind und damit nicht klar erkennbar ist, welche Datenarten veröffentlicht werden können.

Zu § 36:

42 Gemäß § 36 Abs. 2 hat der Informationsaustausch zwischen den wesentlichen und wichtigen Einrichtungen und gegebenenfalls ihrer Lieferanten oder Dienstleister im Wege von Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit unter Beachtung des potentiell sensiblen Charakters der ausgetauschten Informationen zu erfolgen. In diesen Vereinbarungen können operative Elemente, einschließlich der Nutzung spezieller IKT-Plattformen und Automatisierungsinstrumente, der Inhalt und die Bedingungen der Vereinbarungen über den Informationsaustausch bestimmt werden.

43 Fraglich erscheint, ob im Wege von Vereinbarung auch personenbezogene Daten aus der Hoheitsverwaltung übermittelt werden. Unklar ist überdies, was die Wendung „unter Beachtung des potentiell sensiblen Charakters der ausgetauschten Informationen“ bedeutet bzw. was ein „potentiell sensibler Charakter“ ist.

Zu § 37:

44 § 37 Abs. 3 sieht vor, dass eine freiwillige Meldung weder die Identität der Einrichtung noch Informationen, die auf diese schließen lassen, beinhalten muss. Die Meldung kann personenbezogene Daten gemäß § 42 Abs. 2 enthalten. § 34 Abs. 2 gilt sinngemäß.

45 Aus der Regelung ist nicht klar nachvollziehbar, in welchen Fällen die Meldung personenbezogene Daten enthalten darf. Zudem ist auch diesbezüglich fraglich, welche personenbezogenen Daten gemäß § 42 Abs. 2 übermittelt werden dürfen, zumal die Aufzählung der Datenarten in dieser Regelung nur demonstrativ ist.

46 Hinsichtlich der „sinngemäßen“ Geltung des § 34 Abs. 2 wird auf die Ausführungen unter Pkt. II.A. hingewiesen.

Zu § 39:

47 Die Cybersicherheitsbehörde ist gemäß § 39 Abs. 3 Z 1 lit. b befugt, anzuordnen, einzelne Aspekte seitens der Cybersicherheitsbehörde aufgezeigter, nicht eingehaltener sich aus dem NISG 2024 ergebenden Verpflichtungen öffentlich bekannt zu machen, sofern dies erforderlich ist, um das damit verbundene Risiko auf ein vertretbares Ausmaß zu reduzieren.

48 Es sollte klargestellt werden, ob davon auch personenbezogene Daten umfasst sind bzw. personenbezogene Daten veröffentlicht werden. Zudem erscheint unklar, in welchen Fällen und zu welchem konkreten Zweck die Veröffentlichung vorzunehmen ist. Fraglich ist auch, welche „Aspekte" der Verstöße gemeint sind.

Zu § 42:

49 a. § 42 Abs. 1 regelt die datenschutzrechtliche Rollenverteilung sowie die Ermächtigung zur Datenverarbeitung.

50 Die Datenverarbeitung wird jedoch nur sehr allgemein und äußert weit geregelt. Klargestellt werden sollte, zur Wahrnehmung welcher Aufgaben welche Datenarten tatsächlich erforderlich sind.

51 b. § 42 Abs. 2 regelt zwar die betreffenden Datenarten, die Aufzählung ist jedoch in mehrfacher Hinsicht nur demonstrativ („insbesondere", „wie etwa"). Unklar ist damit, welche weiteren Datenarten allenfalls aufgrund dieser Regelung verarbeitet werden können.

52 Zudem ist aus § 42 Abs. 2 nicht erkennbar, ob alle in der Regelung genannten Datenarten auch für alle Aufgaben gemäß Abs. 1 unbedingt benötigt werden. Es sollte dargelegt werden, inwieweit die Befugnis der Datenverarbeitung „zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit" erforderlich ist.

53 In diesem Sinne wird auch auf die unter Pkt. II.A. zit. Rechtsprechung des Verfassungsgerichtshofes zum Detailgrad einer Eingriffsnorm hingewiesen. § 42 Abs. 2 müsste daher präzisiert werden. Insbesondere sollten die betreffenden Datenarten taxativ genannt werden.

54 c. § 42 Abs. 5 regelt die Beschränkung bestimmter Rechte der betroffenen Person.

55 Bei der gesetzlichen Ausgestaltung einer Beschränkung der Rechte der betroffenen Person müssen die in Art. 23 Abs. 2 DSGVO genannten legistischen Vorgaben in der Gesetzgebungsmaßnahme jedenfalls umgesetzt werden.

56 Zudem sollte geprüft werden, in welchem Ausmaß und für welchen Zeitraum die Beschränkung zur Zweckerreichung unbedingt erforderlich ist und diese dementsprechend eingeschränkt und befristet werden kann.

Zu § 43:

57 Hinsichtlich der in § 43 geregelten Datenübermittlungen sollte im Gesetz konkret geregelt werden, welche personenbezogenen Daten an welche Stelle jeweils übermittelt werden, zumal aufgrund des Verhältnismäßigkeitsgrundsatzes gemäß § 1 Abs. 2 nur die Übermittlung jener Daten angeordnet werden darf, die zur Zweckerreichung erforderlich sind. Zudem darf der Eingriff in das Grundrecht auf Datenschutz jeweils nur in der gelindesten Art erfolgen.

58 Die Befugnisse des BMI nach § 43 Abs. 2 zur Übermittlung personenbezogener Daten an ausländische Stellen sollte auf die Erforderlichkeit zur Wahrnehmung von Aufgaben nach diesem Bundesgesetz beschränkt werden.

59 Unklar erscheint zudem, an welche „Dritte“ und „sonstige Einrichtungen“ gemäß § 43 Abs. 3 Daten übermittelt werden. Klargestellt werden sollte auch, an welche „inländische[n] Behörden“ gemäß § 43 Abs. 4 Daten übermittelt werden und was „gleichwertige Stellen“ sind.

Zu § 46:

60 § 46 Abs. 2 sieht vor, dass unter den in dieser Bestimmung genannten Voraussetzungen die Bezirksverwaltungsbehörde nach Rechtskraft des Bescheides die Nichteinhaltung der Verpflichtungen in einer allgemeinen Weise zu veröffentlichen hat, die geeignet scheint, einen möglichst weiten Personenkreis zu erreichen. Diese Veröffentlichung darf nur insoweit erfolgen, als diese keine Gefahr für die öffentliche Ordnung oder Sicherheit darstellt.

61 Es sollte konkretisiert werden, ob bzw. welche personenbezogenen Daten von dieser Veröffentlichung umfasst sein können.

2. Artikel 2 – Änderung des Telekommunikationsgesetzes 2021

Zu Z 1 (§ 44):

62 Betreiber und Anbieter haben gemäß § 44 Abs. 1 nach Maßgabe anderer Rechtsvorschriften Maßnahmen für Cybersicherheit zu ergreifen. Für den Fall, dass diese Rechtsvorschriften nicht ausreichen, das in § 1 Abs. 2 Z 4 genannte Ziel der Aufrechterhaltung der Sicherheit der Netze und Dienste zu gewährleisten, ist die Regulierungsbehörde ermächtigt, im Einvernehmen mit dem Bundeskanzler, dem Bundesminister für Finanzen und dem Bundesminister für Inneres unter Bedachtnahme auf relevante internationale Vorschriften, die nationale Cybersicherheitsstrategie, die Art des Netzes oder des Dienstes, die technischen Möglichkeiten, den Schutz personenbezogener Daten und sonstige schutzwürdige Interessen von Nutzern mit Verordnung nähere Bestimmungen über technische und organisatorische Sicherheitsmaßnahmen festzulegen.

63 Unklar ist, wie die „Bedachtnahme“ auf den Schutz personenbezogener Daten und sonstige schutzwürdige Interessen erfolgt und ob auch Datenverarbeitungen in der Verordnung geregelt werden sollen. Hinsichtlich der Verordnungsermächtigung wird auf die Anmerkungen zum vorgeschlagenen § 27 NISG 2024 sowie auf die Ausführungen unter Pkt. II.A. hingewiesen.

3. Artikel 3 – Änderung des Gesundheitstelematikgesetzes 2012

Zu Z 2 (§ 8a):

64 Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin hat zur Gewährleistung der Sicherheit von Netz- und Informationssystemen im Gesundheitswesen gemäß § 8a Abs. 1 ein sektorspezifisches Computer-Notfallteam („Austrian Health CSIRT“) gemäß § 8 NISG 2024 für den Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2024 einzurichten und zu betreiben.

65 Es sollte erläutert werden, wer der Verantwortliche (Art. 4 Z 7 DSGVO) für Datenverarbeitungen iZm dem „Austrian Health CSIRT“ ist (das „Austrian Health CSIRT“ oder allenfalls der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin).

66 Weiters ist fraglich, ob auch besondere Kategorien personenbezogener Daten (zB Gesundheitsdaten von Patienten) gemäß Art. 9 Abs. 1 DSGVO verarbeitet werden.

III. Zu den Materialien

Zur Datenschutz-Folgenabschätzung:

67 Die Erläuterungen enthalten Ausführungen zur Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO.

68 Inwiefern diese Ausführungen den Vorgaben für eine Vorwegnahme der Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 10 iVm Abs. 7 DSGVO entsprechen, wäre mit der Datenschutzbehörde zu klären.

Für den Datenschutzrat:
Der Vorsitzende
OFENAUER
03. Mai 2024

Elektronisch gefertigt