REPUBLIK ÖSTERREICH DATENSCHUTZRAT

Museumstraße 7, A-1070 WIEN
BMVRDJ-818.020/0002-DSR/2018
TELEFON ● +43 1 52152 2906
E-MAIL ● DSR@BMVRDJ.GV.AT
Ihr Zeichen: BKA-180.310/0234-I/6/2018

An das
Bundeskanzleramt

Per Mail:
recht@bka.gv.at
nis@bka.gv.at

Entwurf eines Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)

Der Datenschutzrat hat in seiner **241. Sitzung am 22. Oktober 2018 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Allgemeines

Laut den Erläuterungen soll mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (im Folgenden: NIS-RL), die am 8. August 2016 in Kraft getreten ist, unionsweit ein hohes Sicherheitsniveau der Netz- und Informationssysteme erreicht werden. Vor diesem Hintergrund soll(en) unter anderem die Zusammenarbeit zwischen den Mitgliedstaaten in strategischer und operationeller Hinsicht gestärkt werden, Mitgliedstaaten eine nationale NIS-Strategie erarbeiten, die strategische Ziele, Prioritäten und Maßnahmen enthalten soll, um in den einzelnen Mitgliedstaaten ein hohes Sicherheitslevel der Netz- und Informationssysteme zu erreichen, nationale Behörden und Computer-Notfallteams benannt werden und bestimmte, für das Gemeinwohl wichtige private und öffentliche Anbieter (Betreiber wesentlicher Dienste und digitale Diensteanbieter) zu angemessenen Sicherheitsmaßnahmen und zur Meldung erheblicher Störfälle verpflichtet werden.

Betreiber eines wesentlichen Dienstes stellen einen Dienst der in Anhang II der NIS-RL genannten und im Folgenden aufgelisteten Sektoren zur Verfügung: Energie (Elektrizität, Erdöl,

Erdgas), Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr), Bankwesen (Kreditinstitute), Finanzmarktinfrastrukturen (Betreiber von Handelsplätzen, zentrale Gegenparteien), Gesundheitswesen (Einrichtungen der medizinischen Versorgung, einschließlich Krankenhäuser und Privatkliniken), Trinkwasserlieferung und -versorgung, Digitale Infrastruktur (Internet Exchange Points, DNS-Diensteanbieter, TLD-Name-Registries). Ferner sollen (ohne entsprechende RL-Vorgabe) bestimmte Einrichtungen des Bundes im Rahmen der österreichischen Umsetzung berücksichtigt werden.

Digitale Diensteanbieter sind – ab einer gewissen Größe – sämtliche Anbieter eines Online-Marktplatzes, einer Online-Suchmaschine oder eines Cloud-Computing-Dienstes.

In Österreich soll die NIS-RL mit dem vorliegenden Bundesgesetz (Netz- und Informationssystemsicherheitsgesetz – NISG) umgesetzt werden. Dabei sollen Aufgaben, die sich aus der NIS-RL ergeben, auf bereits bestehende Strukturen übertragen werden.

Der Bundeskanzler wird die strategischen Aufgaben wahrnehmen und somit als „strategisches NIS-Büro“ fungieren, der Bundesminister für Inneres wird die operativen Aufgaben wahrnehmen und somit als „operatives NIS-Büro“ fungieren.

Die Hauptgesichtspunkte sind im Einzelnen:

- die Festlegung von Aufgaben und Behördenzuständigkeiten sowie Befugnissen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen;
- die Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;
- die Ermittlung der vom Anwendungsbereich konkret erfassten Betreiber wesentlicher Dienste anhand der in einer Verordnung noch näher zu definierenden Teilsektoren und Faktoren;
- die Regelung zweier Arten von Verpflichtungen für die ermittelten Betreiber wesentlicher Dienste, die digitalen Diensteanbieter und Einrichtungen des Bundes: Diese haben a) angemessene Sicherheitsvorkehrungen für ihre Netz- und Informationssysteme vorzusehen und b) Sicherheitsvorfälle an die zuständigen Stellen zu melden;

- die Überprüfung der Einführung geeigneter Sicherheitsvorkehrungen und Einhaltung der Meldepflicht. Während bei Betreibern wesentlicher Dienste diese Überprüfungen jederzeit – zumindest aber alle drei Jahre – durchgeführt werden können, ist dies bei digitalen Diensteanbietern nur im Anlassfall zulässig;
- die Einrichtung von Computer-Notfallteams und Festlegung der Aufgaben, die diesen zukommen sollen;
- die Regelung von Strukturen, Aufgaben und Befugnissen im Falle der Cyberkrise;
- die Festlegung von Sanktionen bei Nichteinhaltung der nach diesem Bundesgesetz einzuhaltenden Pflichten.

II. Datenschutzrechtliche Bemerkungen

Datenschutzrechtliche Vorbemerkungen:

Es wird 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. In diesem Sinne sollte hinsichtlich jener (auch behördeninterner) Datenverarbeitungen, die über die unionsrechtlichen Vorgaben hinausgehen, näher erläutert werden, weshalb diese notwendig sind. Insbesondere wären die verarbeiteten personenbezogenen Daten auch im Gesetzestext zu nennen (§§ 9, 10, 11 und 12 des Entwurfes).

Nach einem noch näher zu definierenden Zeitraum sollte eine Evaluierung vorgesehen werden.

Es wäre angesichts der Kompetenzdeckungsklausel zu prüfen, ob auch der Vollzugsbereich anderer Gebietskörperschaften miteinbezogen werden sollte.

Der Datenschutzrat geht nach den Ausführungen der informierten Vertreter davon aus, dass Art. 33 und 34 DSGVO unberührt bleiben.

Zu § 3 Z 4:

Es wäre klarzustellen, ob die „NIS-Büros“ (eigenständige) Verantwortliche im Sinne des Art. 4 Z 7 DSGVO sind.

Zu § 11:

In § 11 Abs. 1 wäre zu präzisieren, welche personenbezogenen Daten verarbeitet werden. Die Formulierung in den Erläuterungen (S 12), wonach im Rahmen der gemeinsamen Verarbeitung „gleichzeitig aber auch alle anderen Daten zu verarbeiten sind, die notwendig sind, um einen Sicherheitsfall oder eine sonstige Störung eines betroffenen Dienstes beurteilen und bewerten zu können“ ist jedenfalls zu weitreichend und wäre entsprechend den datenschutzrechtlichen Vorgaben zu präzisieren.

In § 11 Abs. 2 wird angeordnet, dass der Betroffene seine datenschutzrechtlichen Ansprüche nur gegenüber einem bestimmten (gemeinsamen) Verantwortlichen wahrnehmen kann. Nimmt eine betroffene Person ein Recht nach der DSGVO gegenüber einem „unzuständigen“ Verantwortlichen wahr, ist sie an den zuständigen Verantwortlichen zu verweisen. Es erscheint fraglich, inwieweit diese Form einer (außenwirksamen) Zuständigkeitsverteilung zwischen mehreren gemeinsam für die Verarbeitung Verantwortlichen unionsrechtlich zulässig ist. Insbesondere im Anwendungsbereich der DSGVO sollte dies nochmals geprüft werden.

§ 11 Abs. 3 normiert, dass der Bundesminister für Inneres die Funktion des Auftragsverarbeiters gemäß Art. 4 Z 8 iVm Art. 28 Abs. 1 DSGVO ausübt. Es ist fraglich, inwieweit es im Hinblick auf die Regelungen in §§ 10 und 11 des Entwurfes zulässig ist, einem obersten Organ die Rolle eines Auftragsverarbeiters zuzuweisen und als Verantwortliche andere (oberste) Organe (Bundesminister für Landesverteidigung und Bundeskanzler) vorzusehen. Nachdem der Auftragsverarbeiter hinsichtlich der Datenverarbeitung gemäß Art. 28 Abs. 3 lit. a und Art. 29 DSGVO den (datenschutzrechtlichen) Weisungen des Verantwortlichen unterliegt, könnte ein Spannungsverhältnis zwischen der Rollenverteilung und der Befugnis zwischen Verantwortlichem und Auftragsverarbeiter und der Stellung als oberstes Organ im Sinne des B-VG bestehen. Lehre und Rechtsprechung gehen davon aus, dass die in Art. 19 Abs. 1 B-VG genannten obersten Organe „nicht der Leitung, insb der Aufsicht und den Weisungen (und sonstigen Anordnungen) anderer Organe unterworfen sind, soweit nicht verfassungsrechtlich anderes bestimmt ist“ (s. *Raschauer*, Art. 19 Abs. 1 B-VG in Korinek/Holoubek, Österreichisches Bundesverfassungsrecht Rz 52).

§ 11 Abs. 4 sieht eine Ermächtigung zur Datenverarbeitung durch die NIS-Büros vor. Hinsichtlich der damit zusammenhängenden Frage der datenschutzrechtlichen Rollenverteilung wird auf die Anmerkungen zu § 3 Z 4 des Entwurfes verwiesen.

Die vorgeschlagene Bestimmung ermächtigt die NIS-Büros und den Bundesminister für Landesverteidigung zur Datenübermittlung auch an „sonstige in- und ausländische Behörden oder Stellen […], soweit dies zur Aufgabenerfüllung erforderlich ist“. Es ist unklar, welche sonstigen in- und ausländischen Behörden oder Stellen dies sein sollen, welche Aufgaben davon umfasst sind und welche Datenarten zur Erfüllung dieser Aufgaben verarbeitet werden sollen. Die in der derzeitigen Formulierung weitgehend schrankenlose Ermächtigung wäre iSd § 1 Abs. 2 DSG und Art. 18 B-VG zu präzisieren. Allfällige Datenübermittlungen ins Ausland dürfen im Übrigen nur vorgenommen werden, wenn sie den Vorgaben des Kapitels V der DSGVO entsprechen.

Zu § 12:

Die Ermächtigung zur Datenverarbeitung im vorgeschlagenen § 12 Abs. 2 wäre – zumal im vorliegenden Entwurf nur Aufgaben geregelt werden – zu präzisieren (s. die Anmerkungen zu § 11 Abs. 1 und 4). Ebenso wäre darzulegen, ob die Computer-Notfallteams (eigenständige) Verantwortliche im Sinne des Art. 4 Z 7 DSGVO sind.

In § 12 Abs. 5 sollte vor „erforderlich“ die Wortfolge „nach diesem Bundesgesetz“ zur Konkretisierung eingefügt werden.

Zu § 15:

Einschaumöglichkeiten für das BMI in Netz- und Informationssysteme und Unterlagen der qualifizierten Stellen sollten in den Erläuterungen zu § 15 Abs. 3 präzisiert werden.

24. Oktober 2018
Für den Datenschutzrat
Der Vorsitzende:
OFENAUER

Elektronisch gefertigt