Republik Österreich
Datenschutzbehörde

A-1080 Wien, Wickenburggasse 8
Tel.: +43-1-52152 302581

E-Mail: dsb@dsb.gv.at
DVR: 0000027

GZ: DSB-D054.948/0001-DSB/2018

Sachbearbeiter: Michael Adelmann, LL.M.

Präsidium des Nationalrates

Dr. Karl Renner-Ring 3
1017 Wien

Stellungnahme der Datenschutzbehörde

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

Betrifft: Stellungnahme der Datenschutzbehörde zum Gesetzesentwurf eines „Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)“, GZ BKA-180.310/0234-I/6/2018

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

Zu § 9 Abs. 1:

Sollte diese Ermächtigung auf die Verarbeitung personenbezogener Daten abzielen, erscheint sie zu weitgehend. Es sollte klargestellt werden, dass nur solche Daten übermittelt werden dürfen, die der Bundesminister für Inneres zur Erfüllung seiner Aufgaben benötigt.

Zu § 10:

Gemessen an der ständigen Rechtsprechung des Verfassungsgerichtshofes zur Qualität einer Eingriffsnorm im Sinne des § 1 Abs. 2 DSG erscheint die pauschale Ermächtigung zur Datenverarbeitung in Abs. 1 als zu weitgehend (siehe dazu bspw. VfSlg. 18.146/2007). Es sollte vielmehr eine – wenn auch nur demonstrative – Aufzählung der einzelnen Datenkategorien im Normentext erfolgen; derzeit sind Datenkategorien nur in den Erläuterungen aufgezählt.

Zu Abs. 3 ist festzuhalten, dass fraglich ist, ob einem NIS-Büro überhaupt die Eigenschaft als Verantwortlicher iSd Art. 4 Z 7 DSGVO zukommt. Nach der Legaldefinition des § 3 Z 4 sind „NIS-Büros“ die „beim Bundeskanzler und Bundesminister für Inneres jeweils zur Erfüllung der diesen gemäß §§ 4 und 5

zugewiesenen Aufgaben eingerichteten Organisationseinheiten.“ Im Regelfall kommt einer Organisationseinheit innerhalb einer Behörde keine Verantwortlicheneigenschaft zu, da die (freie) Entscheidung zur Datenverarbeitung (welche einen Verantwortlichen kennzeichnet) mit der Weisungsgebundenheit gegenüber dem Behördenleiter kollidieren würde.

Zu Abs. 3 ist weiters festzuhalten, dass die Befugnis zur Einholung nicht näher spezifizierter Auskünfte sowie die korrespondiere Pflicht von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste Auskünfte zu erteilen, vor allem im Hinblick auf die darauf Bezug nehmende Strafbestimmung des § 23 Abs. 1 Z 1 zu unspezifisch erscheint. Vielmehr wäre eine Aufzählung der Datenkategorien zu befürworten.

Soweit Abs. 4 auf ein NIS-Büro Bezug nimmt, wird auf die Ausführungen zu Abs. 3 verwiesen. Darüber hinaus sollte eine Protokollierung so erfolgen, dass eine Zuordnung zu einer bestimmten Person (und nicht bloß zu einer bestimmten Organisationseinheit) möglich ist. Andernfalls könnte der Pflicht nach Art. 32 Abs. 1 lit. b DSGVO nicht ausreichend entsprochen werden.

Zu § 11:

Zu Abs. 1 und 2 ist festzuhalten, dass der Bestimmung die getrennten Verantwortlichkeitsbereiche im Rahmen der gemeinsamen Verantwortlichkeit (Art. 26 DSGVO) nicht hinreichend klar zu entnehmen sind. Es wäre in transparenter Weise darzulegen, für welchen Bereich welcher der genannten Verantwortlichen zuständig ist. Die Zuständigkeit wäre für einen Betroffenen sonst nur schwer zu ermitteln.

Beim geplanten „Informationsverbund“ stellt sich die Frage, ob hiefür nicht eine Datenschutz-Folgenabschätzung iSd Art. 35 DSGVO erforderlich wäre. Auf Art. 35 Abs. 10 DSGVO wird daher ausdrücklich hingewiesen.

In Bezug auf die Befugnis, die „erforderlichen Identifikations- und Erreichbarkeitsdaten sowie die erforderlichen Sachdaten etc.“ zu verarbeiten, wird auf die Ausführungen zu § 10 Abs. 1 verwiesen.

Abs. 2 fordert für die Geltendmachung von Betroffenenrechten den Nachweis der Identität. Dies ist gemäß Art. 12 Abs. 6 DSGVO nicht erforderlich. Vielmehr obliegt es dem Verantwortlichen bei Zweifeln an der Identität Schritte zu setzen, um diese festzustellen. Der in den Erläuterungen erwähnte ErwGr. 64 bezieht sich auf Art. 15 DSGVO (und nicht auf Art. 12).

Zu Abs. 3 ist auszuführen, dass ein gemeinsam Verantwortlicher iSd Art. 26 DSGVO nicht gleichzeitig Auftragsverarbeiter iSd Art. 4 Z 8 DSGVO sein kann (vgl. *Martini* in *Paal/Pauly*, Datenschutz-Grundverordnung [2017] Art. 26 Rn. 20). Es bedürfte hier einer klareren Abgrenzung, für welche Datenverarbeitung der Bundesminister für Inneres Auftragsverarbeiter ist.

Soweit auf Abs. 4 auf NIS-Büros Bezug nimmt, wird auf die Ausführungen zu § 10 Abs. 3 verwiesen.

Darüber hinaus erscheint hier unklar, weshalb eine Übermittlung an die Datenschutzbehörde für Zwecke des Art. 33 DSGVO normiert wird, zumal die Meldung einer Sicherheitsverletzung gemäß Art. 33 DSGVO ohnehin vom Verantwortlichen selbst an die Datenschutzbehörde zu erstatten ist.

Die Übermittlungsermächtigung „an sonstige in- und ausländische Behörden oder Stellen, soweit dies zur Aufgabenerfüllung erforderlich ist“ erscheint zu unbestimmt. Eine Aufzählung der in Frage kommenden Stellen wäre anzudenken.

Zu § 12 Abs. 7:

Auch hier ist unklar, ob den Computer-Notfallteams die Eigenschaft als Verantwortlicher iSd Art. 4 Z 7 DSGVO zukommt. Auf die Ausführungen zu § 10 Abs. 3 wird verwiesen.

Zu §§ 16 und 17:

Die Pflicht zur Meldung nach Art. 33 DSGVO an die Datenschutzbehörde ergibt sich zwar unmittelbar aus der DSGVO selbst. Um Unklarheiten zu vermeiden (insbesondere im Hinblick auf § 17), wird aber angeregt, (zumindest in den Erläuterungen) einen Hinweis aufzunehmen, wonach die Meldepflicht nach Art. 33 DSGVO davon unberührt bleibt. Die Erläuterungen sprechen hier nur von „sektorenspezifischen Rechtsvorschriften“, sodass unklar ist, ob Art. 33 DSGVO darunter fällt.

Zu § 23:

Nach Abs. 2 richtet sich die örtliche Zuständigkeit für Verwaltungsübertretungen nach der Hauptniederlassung des Betreibers wesentlicher Dienste oder des Anbieters digitaler Dienste. Der Begriff der Hauptniederlassung wird jedoch im Entwurf nicht definiert, in § 3 Z 10 wird er lediglich erwähnt. Um Unklarheiten in Bezug die Legaldefinition einer Hauptniederlassung in Art. 4 Z 16 DSGVO zu vermeiden, wird angeregt, den Begriff näher zu definieren. So führt bspw. Art. 18 Abs. 1 der Richtlinie (EU) 2016/1148 aus, dass ein Anbieter digitaler Dienste seine Hauptniederlassung in einem Mitgliedstaat hat, wenn er seinen Hauptsitz in diesem Mitgliedstaat hat.

24. Oktober 2018
Für die Leiterin der Datenschutzbehörde:
SCHMIDL