BUNDESARBEITSKAMMER
PRINZ EUGEN STRASSE 20-22
1040 WIEN
T 01 501 65
www.arbeiterkammer.at
DVR 1048384

Bundeskanzleramt
Büro für strategische Netz-
und Informationssystemsicherheit
Ballhausplatz 2
1010 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65** Fax **501 65**	Datum
BKA-180.310/0234-I/6/2018	BAK/KS-GSt/DZ/Ho	Daniela Zimmer	DW 12722 DW 12693	29.10.2018

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (NISG)

Die Bundesarbeitskammer (BAK) bedankt sich für die Übermittlung des im Betreff genannten Entwurfs und nimmt dazu wie folgt Stellung:

Zweck des Vorhabens

Mit dem vorliegenden Entwurf wird die EU-Richtlinie 2016/1148 (NIS-RL) umgesetzt.

Mit Blick auf das wachsende Risiko von Cyberangriffen auf strategisch wichtige Ziele (bspw Energieversorgung, Verkehrsträger, Gesundheits- und Bankwesen, Trinkwasserversorgung oder digitale Infrastruktur) sieht die Richtlinie eine stärkere Zusammenarbeit der Mitgliedstaaten zur EU-weiten Absicherung der Sicherheit von Netzen und Informationssystemen, die Erarbeitung einer entsprechenden nationalen Sicherheitsstrategie für Netzwerke und die Benennung zuständiger Behörden und Computer-Notfallsteams für den Störfall vor.

Zusammenfassende Bewertung

- Bei der Umsetzung der Richtlinie sollte auf die Grundsätze der Datenschutz-Grundverordnung (DSGVO) wie bspw Zweckbindung, Datenminimierung, Verhältnismäßigkeit stärker Bedacht genommen werden. Diesbezüglich hält die BAK den Entwurf in zweierlei Hinsicht für verbesserungsbedürftig: Datenverarbeitungen, die über die Vorgaben der NIS-Richtlinie hinausgehen, bedürfen einer eingehenden Begründung, weshalb sie zwingend erforderlich sind. Vor allem aber sind in den §§ 9, 10, 11 und 12 jene Datenarten, die verarbeitet

werden dürfen, auch konkret zu benennen. Beispielhafte Aufzählungen in den Erläuterungen sind nicht ausreichend, um den Präzisierungsanforderungen für Rechtsgrundlagen nach Art 6 Abs 3 der DSGVO zu entsprechen.

- Die behördliche Informationspflicht über Sicherheitsvorfälle gegenüber der Bevölkerung ist so verbindlich zu gestalten, dass möglichst wenig Auslegungsspielraum verbleibt, ob eine Verständigung der Öffentlichkeit im Anlassfall zu erfolgen hat oder unterbleiben kann. Zumindest sollte die „kann"- durch eine „hat"-Bestimmung ersetzt werden.

- Betroffene, die ihre datenschutzrechtlichen Rechte (Auskunft, Löschung, usw) gegenüber dem Bundeskanzler, Innen- und Verteidigungsminister als gemeinsame Datenverantwortliche ausüben wollen, sollten nicht bloß an den Verantwortlichen nach der internen Zuständigkeitsverteilung verwiesen werden. Jedes Ressort sollte die Gesamtverantwortung – mit Blick auf Bürgernähe und zweifelsfreie DSGVO-Konformität – auch im Außenverhältnis zu den Betroffenen wahrnehmen.

- Eine praxisgerecht klare Zuordnung der Zuständigkeiten zwischen Bundeskanzleramt und Innenressort wäre zweckmäßig.

Aufgaben des Bundeskanzlers und des Innenministers (§§ 4, 5):

Nach den Erläuterungen erfolgte die Aufgabenzuordnung zu den beiden genannten Ressorts entsprechend folgender Maxime: Die Aufgaben des Bundeskanzlers sollten „hauptsächlich strategischer Natur" sein, jene des Innenministers „vorrangig operativ". So soll sich das Aufgabenspektrum im Innenressort auf „koordinierende, kommunikative, analysierende und kontrollierende Aufgaben erstrecken". Der Bundeskanzler soll demgegenüber ua die Abwehrstrategien koordinieren und als „zentrale Schnittstelle des Staates zu Gesellschaft, Wirtschaft und Wissenschaft" fungieren.

Bereits die allgemeine Beschreibung der Ressortagenden in den Erläuterungen liefert Hinweise auf mögliche Überschneidungen und damit einhergehende Abgrenzungsprobleme. Dies sei nur anhand eines Beispiels illustriert: Die Vertretung Österreichs „in anderen EU-weiten und internationalen Gremien für Netz- und Informationssystemsicherheit" obliegt dem Bundeskanzler, allerdings nur insoweit als ihnen „strategische Aufgaben" zugewiesen sind. Aufgabe des Innenministers ist es wiederum, eine „zentrale Anlaufstelle" zu betreiben, die als „Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit" fungieren soll.

Aus BAK-Sicht bestehen Zweifel, ob sich die Aufgabengebiete in der Praxis ohne (positive bzw negative) Kompetenzkonflikte zuordnen lassen. Vor diesem Hintergrund regt die BAK an, zumindest jene Aufgaben, die Unklarheiten in Bezug auf die Zuständigkeit induzieren, dem Bundeskanzleramt zuzuweisen.

Befugnisse und Datenverarbeitung (§9)

Der Innenminister darf nach Abs 1 eigene technische Einrichtungen betreiben, die Unregelmäßigkeiten oder Störungen in Netzen oder Informationssystemen frühzeitig erkennen. Betreiber sensibler Infrastrukturen können an diesen Einrichtungen freiwillig „teilnehmen“ und festlegen, welche personenbezogenen Daten (etwa IP-Adressen und andere Verbindungsdaten) dem Innenminister übermittelt werden.

Der Umfang der übermittelten Daten kann nicht der Privatautonomie der Vertragspartner überantwortet werden. Die Datenarten sind im Gesetz selbst unbedingt konkret zu benennen und dabei taxativ aufzuzählen.

Zudem darf der Innenminister gemäß Abs 2 technische Einrichtungen betreiben oder auch nur „nutzen“, um Angriffsmuster zu studieren.

Wiederum fehlt eine gesetzliche Beschränkung der dabei verarbeiteten personenbezogenen Daten, aber auch eine Festlegung, wessen Einrichtungen das Innenressort abseits des Eigenbetriebes noch „nutzen“ darf. Bei der Nutzung fremder Systeme ist zudem unklar, wer für die Datenverarbeitung verantwortlich zeichnet.

Gemeinsame Verarbeitung (§11)

Bundeskanzler, Innen- und Verteidigungsminister dürfen zur Risikobewertung und Erstellung eines Lagebilds gemeinsam personenbezogene Daten verarbeiten. Wie schon mehrfach beanstandet, fehlt im Sinne der Datensparsamkeit und Verhältnismäßigkeit im Gesetzestext eine Auflistung der personenbezogenen Daten, die zulässigerweise verwendet werden dürfen. Die Erläuterungen zählen beispielhaft eine Vielzahl an potentiell nutzbaren Datenarten auf (darunter Telefonnummern, IP- und Mailadressen, Domains, Usernamen). Entsprechend den Anforderungen des Art 6 Abs 3 DSGVO an Rechtsgrundlagen sind die Datenarten möglichst konkret und abschließend in der Erlaubnisnorm zu bezeichnen.

Nach Abs 2 können Betroffene, die ihre datenschutzrechtlichen Ansprüche (Auskunft, Löschung, usw) gegenüber den gemeinsamen Datenverantwortlichen ausüben wollen, nach der Zuständigkeitsverteilung im Innenverhältnis an den zuständigen Verantwortlichen verwiesen werden. Eine derartige Vorgangsweise könnte bei gemeinsamer Verantwortlichkeit nach der DSGVO nicht verordnungskonform sein. Vor diesem Hintergrund sollte jeder angesprochene Verantwortliche die Gesamtverantwortung auch im Außenverhältnis zu Betroffenen wahrnehmen.

Meldepflicht Sicherheitsvorfälle (§16)

Nach Abs 6 „kann“ der Bundeskanzler bzw Innenminister die Öffentlichkeit über Sicherheitsvorfälle informieren, sofern die Sensibilisierung der Öffentlichkeit zur Bewältigung oder Verhütung von Sicherheitsvorfällen erforderlich ist oder „auf sonstige Weise“ ein öffentliches Interesse daran besteht.

Im Falle des Vorliegens der genannten Voraussetzungen sollten die zuständigen Behörden ihrer Informationspflicht jedenfalls nachkommen müssen. Vor diesem Hintergrund sollte der Terminus „kann“ zumindest durch ein „hat“ ersetzt werden. Im Dienste der Transparenz gegenüber der betroffenen Bevölkerung sollten auch die Voraussetzungen für die behördliche Informationspflicht so unmissverständlich gestaltet sein, dass möglichst wenig Auslegungsspielraum darüber verbleibt, ob eine Verständigung der Öffentlichkeit im Anlassfall erfolgen muss oder unterbleiben kann.

Renate Anderl
Präsidentin
F.d.R.d.A.

Melitta Aschauer-Nagl
iV des Direktors
F.d.R.d.A.