REPUBLIK ÖSTERREICH DATENSCHUTZRAT

An das
Bundeskanzleramt
Ballhausplatz 2
1010 Wien

Mit E-Mail:
technologiemanagement@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: 2024-0.326.395

GZ des Begutachtungsentwurfes:
2024-0.221.515

Entwurf eines Bundesgesetzes zur Einrichtung einer nationalen Behörde für die Cybersicherheitszertifizierung (Cybersicherheitszertifizierungs-Gesetz – CSZG);
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 Materialien zum Entwurf wird mit der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zu Cybersicherheit), die am 27. Juni 2019 in Kraft getreten sei, ein unionsweiter Rahmen zur Zertifizierung von IKT-Produkten, -Diensten und -Prozessen betreffend die Cybersicherheit geschaffen.

2 Jeder Mitgliedstaat habe in diesem Zusammenhang eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung in seinem Hoheitsgebiet zu benennen. Den nationalen Behörden obliege die Überwachung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse mit den europäischen Cybersicherheitszertifikaten, die Überwachung der Verpflichtungen der Hersteller oder Anbieter von IKT-Produkten, -

Diensten und -Prozessen, die eine Selbstbewertung der Konformität vornehmen und die Überwachung der Konformitätsbewertungsstellen sowie Angemessenheit des Fachwissens des Personals der Einrichtungen, die Zertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen.

3 Mit dem vorliegenden Gesetzesvorhaben werden laut den Materialien zum Entwurf die innerstaatlichen Maßnahmen zur Errichtung der nationalen Behörde für die Cybersicherheitszertifizierung in Österreich und damit einhergehend zur digitalen Sicherheit von Informations- und Kommunikationstechnik erlassen. Gleichzeitig werde mit dem Gesetzesvorhaben der Zielsetzung des Regierungsprogramms zur Förderung der strategischen Koordinierungsfunktion des Bundeskanzleramtes im Cyber-Bereich, Ziel 12 der Österreichischen Strategie für Cybersicherheit 2021 sowie den Punkten 1.5 und 4.4 des Digital Austria Acts entsprochen.

II. Inhaltliche Bemerkungen

A. Grundsätzliches

4 Der vorliegende Entwurf regelt die nationale Durchführung bestimmter Aspekte der durch die Verordnung 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (IKT) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit bzw. „Cybersecurity Act“ – CSA) normierten unionsrechtlichen Vorgaben (Öffnungsklauseln). Die übrigen materiellrechtlichen Vorgaben des CSA gelten unmittelbar und lassen somit dem nationalen Gesetzgeber keinen Spielraum, dies gilt auch grundsätzlich für datenschutzrechtliche Aspekte bei der Durchführung des CSA. Unter dieser Prämisse sind auch die nachfolgenden Anmerkungen zu lesen.

B. Zum Entwurf

Allgemeines:

5 Zur Abgrenzung sei festgehalten, dass der primäre Gegenstand des vorliegenden Entwurfs die Durchführung des CSA in Bezug auf die Benennung nationaler Stellen zum Zweck der Cyber- und digitalen Sicherheitszertifizierung ist, und somit inhaltlich von der datenschutzrechtlichen Zertifizierung im Sinne von Art. 42 DSGVO zu unterscheiden ist, welcher ein datenschutzspezifisches Zertifizierungsverfahren zum Nachweis der Einhaltung der DSGVO-Vorschriften zum Inhalt hat.

6 Datenschutzrechtlich relevante Bestimmungen finden sich in Abschnitt 3 („Befugnisse und Datenverarbeitung“) des Entwurfs, wobei nur in § 5 zur „Datenverarbeitung“ materielle datenschutzrechtliche Bestimmungen enthalten sind.

Zu § 5:

7 Zusätzlich zu der Ermächtigung des Bundeskanzlers zur Datenverarbeitung mit dem Zweck der Erfüllung der Aufgaben gemäß CSA in Abs. 1 wäre auch noch seine konkrete datenschutzrechtliche Rolle als Verantwortlicher im Sinne von Art. 4 Z 7 DSGVO zu definieren.

8 Weiters ist mit Bezug auf die in Abs. 2 angeführten personenbezogenen Datenarten wie folgt festzuhalten:

9 Aus der einschlägigen Rechtsprechung des Verfassungsgerichtshofs zur Frage der Anforderungen an den Grad der Bestimmtheit gesetzlicher Eingriffe in das Grundrecht auf Datenschutz im Hinblick auf § 1 Abs. 2 DSG iVm Art. 18 B-VG ist abzuleiten, dass eine Ermächtigungsnorm iSd § 1 Abs. 2 DSG ausreichend präzise, also für jedermann vorhersehbar, bezeichnen muss, unter welchen Voraussetzungen die Ermittlung bzw. 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).

10 § 5 Abs. 2 bezieht sich in den Z 1 – 3 auf bestimmte, mit der Durchführung des CSA im Zusammenhang stehende Daten, lässt aber offen, welche konkreten weiteren Daten von der allgemeinen Ermächtigung zur Verarbeitung im Sinne von Abs. 1 zusätzlich erfasst sind.

11 Daher reicht unter diesem Blickwinkel bzw. dem hohen Anforderungsniveau zum Detailgrad der Eingriffsnorm eine lediglich demonstrative Aufzählung der Datenarten [„insbesondere“] nicht aus.

12 Aus diesen Überlegungen wird eine Präzisierung im Sinne einer taxativen Aufzählung der Datenarten in Abs. 2 dringend angeregt.

Für den Datenschutzrat:
Der Vorsitzende
OFENAUER
03. Mai 2024

Elektronisch gefertigt