REPUBLIK ÖSTERREICH DATENSCHUTZRAT

An das
Bundesministerium für Justiz

Per Mail:
team.s@bmj.gv.at

BMJ - StS DS (Stabsstelle Datenschutz)
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: 2021-0.073.233

GZ des Begutachtungsentwurfes:
2020-0.834.703

Entwurf eines Bundesgesetzes, mit dem das Strafgesetzbuch, die Strafprozeßordnung 1975, das Strafvollzugsgesetz und das Gerichtsorganisationsgesetz zur Bekämpfung von Terror geändert werden (Terror-Bekämpfungs-Gesetz – TeBG)

Der Datenschutzrat hat in seiner 254. Sitzung am 29. Jänner 2021 einstimmig beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Allgemeines

1 Laut den Erläuterungen zum gegenständlichen Gesetzesentwurf hat die Bundesregierung sich im Ministerratsvortrag vom 11. November 2020 zu einer Reihe von Maßnahmen zur verbesserten Prävention und Bekämpfung des Terrorismus bekannt und angekündigt, Anfang Dezember ein erstes Gesetzespaket zur Begutachtung zu versenden. Mit Ministerratsvortrag vom 16. Dezember 2020 hat die Bundesregierung die Vorlage eines ersten Gesetzespakets und dessen Versendung zur allgemeinen Begutachtung beschlossen.

2 Im Bereich der Justiz konzentriere sich dieser Entwurf insbesondere darauf, die Überwachung des Verhaltens terroristischer Straftäter während des Vollzugs und nach bedingter Entlassung zu intensivieren und Deradikalisierungsmaßnahmen zu verbessern. Das sei auch deshalb binnen kurzem notwendig, weil künftig terroristische Straftäter nur bei gesichertem Wissen über ihr Gefährdungspotenzial bedingt entlassen werden sollten.

3 Darüber hinaus solle durch eine Verschärfung der Bestimmung über den erweiterten Verfall Geldwäsche und Terrorismusfinanzierung effizienter bekämpft werden können.

4 Schließlich solle religiös motivierter Extremismus mit einer auf diesen Bereich fokussierten Strafbestimmung bekämpft werden können.

II. Datenschutzrechtliche Bemerkungen

Artikel 1 – Änderung des Strafgesetzbuches

Zu Art. 1 Z 5 (§ 52b StGB):

5 1. Abs. 3 sieht im Rahmen der nach dieser Bestimmung abzuhaltenden Sozialnetzkonferenz (§ 29e BewHG) eine Einbindung der zuständigen Organisationseinheit des polizeilichen Staatsschutzes und der Koordinationsstelle für Extremismusprävention und Deradikalisierung im Straf- und Maßnahmenvollzug vor. Da den Erläuterungen keine Anhaltspunkte dafür zu entnehmen sind, dass mit dieser Regelung den genannten Stellen zusätzliche Aufgaben übertragen werden sollen, wird angeregt, hier auf eine Mitwirkung „im Rahmen ihrer jeweiligen gesetzlichen Aufgaben“ abzustellen (vgl. auch § 17a Abs. 1 und § 35a Abs. 2 Jugendgerichtsgesetz 1988). Dies gilt ebenso für die gleichartige Regelung in § 144a Abs. 1 StVG (Art. 3 Z 1 des Entwurfs).

6 Im Hinblick auf den Austausch personenbezogener Daten unter den Teilnehmern der Sozialnetzkonferenz wäre zu prüfen, ob diesbezüglich eine ausreichende gesetzliche Grundlage sowie Vorkehrungen zum Schutz der Rechte der betroffenen Personen bestehen. Dies gilt auch hinsichtlich einer allfälligen weiteren Verarbeitung zu anderen Zwecken, insbesondere durch die zuständigen Organisationseinheiten des polizeilichen Staatsschutzes zu Zwecken des PStSG.

7 2. Abs. 4 ermöglicht im Rahmen der gerichtlichen Aufsicht die Erteilung einer Weisung, geeignete technische Mittel für die elektronische Überwachung der Befolgung von Weisungen nach Abs. 1 ständig – mit Ausnahme der Dauer des Aufenthalts in der eigenen Wohnung – mitzuführen. Aufgrund des Verhältnismäßigkeitsgrundsatzes (§ 1 Abs. 2 DSG) dürfen personenbezogene Daten nur verarbeitet (bzw. übermittelt) werden, wenn dies für die Erreichung des Zwecks unbedingt erforderlich ist und der Eingriff in das Grundrecht jeweils nur in der gelindesten zum Ziel führenden Art vorgenommen wird. Im Hinblick auf die besondere Eingriffsintensität dieser vorgesehenen Maßnahme wird angeregt, von allen zur

Verfügung stehenden Möglichkeiten zur Abmilderung des Grundrechtseingriffs Gebrauch zu machen.

8 2.1. Der Umstand, dass eine Weisung nach Abs. 4 nur mit Zustimmung des betroffenen Rechtsbrechers erteilt werden kann, erscheint aus Sicht des Datenschutzrates in der vorgeschlagenen Form nicht zwingend zur Abmilderung des Grundrechtseingriffs geeignet. Den Erläuterungen ist nämlich zu entnehmen, dass, wenn der Verurteilte der Überwachung nicht zustimmt, eine bedingte Entlassung mangels Vorliegens der Voraussetzungen nach § 46 Abs. 1 auch nach Verbüßung von zwei Drittel der Freiheitsstrafe nicht auszusprechen sein wird. Damit erscheint das Element der Freiwilligkeit bei einer solchen Zustimmung fraglich.

9 2.2. Aufgrund der Eingriffsintensität der Maßnahme wird angeregt, die zulässige Höchstdauer einer solchen Weisung im Einzelnen (also in Bezug auf die jeweilige Anordnung) sowie im Gesamten zu beschränken. Die Probezeit bei der bedingten Entlassung beträgt in bestimmten Fällen fünf oder zehn Jahre (vgl. § 48 Abs. 1 und 2). Im Hinblick auf die besondere Eingriffsintensität der elektronischen Überwachung erscheint deren Anordnung für einen so langen Zeitraum unverhältnismäßig. Eine Beschränkung der Weisung auf einen kürzeren Zeitraum mit der Möglichkeit einer (ggf. mehrfachen) Verlängerung würde eine regelmäßige Überprüfung der Erforderlichkeit und Verhältnismäßigkeit der elektronischen Überwachung sicherstellen (vgl. idZ auch § 137 Abs. 3 StPO hinsichtlich strafprozessualer Überwachungsmaßnahmen). Überdies sollte die Festlegung einer Gesamthöchstdauer für Wiesungen gemäß Abs. 4 geprüft werden.

10 2.3. Der Gesetzestext lässt offen, mit welcher Art von Geräten die Überwachung durchgeführt werden soll. Gemäß Abs. 8 ist die Bundesministerin ermächtigt, durch Verordnung im Einvernehmen mit dem Bundesminister für Inneres Richtlinien über die Art und Durchführung der elektronischen Überwachung zu erlassen. Den Erläuterungen ist zwar zu entnehmen, dass es sich um mit einer „elektronischen Fußfessel“ vergleichbare Geräte handeln soll. Im Gesetzestext ist eine derartige Vorgabe jedoch nicht verankert, sodass – wenn dies nicht durch Verordnung gemäß Abs. 8 ausgeschlossen wird – auch die Anordnung einer elektronischen Überwachung unter Nutzung von Alltagsgeräten (zB Smartphone mit GPS-Funktion) in Betracht käme. Im Hinblick darauf, dass ein Einsatz von ausschließlich zum Zweck der Überwachung eingesetzten Geräten (zB Token) wohl ein gelinderes Mittel darstellen würde (keine Freigabe der Ortungsdienste am Smartphone erforderlich; kein Mitführen innerhalb der eigenen Wohnung in der Praxis), wird angeregt, diesbezügliche Anforderungen an das Gerät soweit möglich bereits im Gesetzestext zu verankern.

11 2.4. In Abs. 5 werden die zulässigen Verwendungszwecke für im Rahmen einer elektronischen Überwachung erhobene Daten abschließend geregelt. Den Erläuterungen zufolge ergebe sich aus dieser abschließenden Regelung, dass nur anlassbezogene (etwa bei Hinweisen auf einen Verstoß), nicht jedoch stichprobenartige Zugriffe auf die Aufenthaltsdaten ermöglicht werden.

12 Aus Sicht des Datenschutzrates ist dem Gesetzestext eine solche – aus Verhältnismäßigkeitsgründen zu befürwortende und offenbar auch intendierte – Anlassbezogenheit als Voraussetzung für die Zulässigkeit des Zugriffs auf die gespeicherten Daten jedoch nicht zu entnehmen. Insbesondere können nämlich auch stichprobenartige Überprüfungen der Feststellung von Verstößen gegen Weisungen dienen. Die Anlassbezogenheit im Hinblick auf die Feststellung von Verstößen gegen Weisungen im Rahmen der Z 1 sollte daher im Gesetzestext klar verankert werden.

13 In Bezug auf die in den Z 2 bis 4 geregelten Fälle dürfte sich die Anlassbezogenheit hingegen implizit bereits aus dem jeweiligen Zweck ergeben, zumal Z 2 einen Verstoß gegen eine Weisung, Z 3 eine erhebliche gegenwärtige Gefahr und Z 4 eine mit Strafe bedrohte Handlung voraussetzt.

14 2.5. Abs. 6 erster Satz sieht zur Einhaltung der Zweckbindung eine „automatisierte" Verarbeitung der Daten zur Feststellung von Verstößen nach Abs. 5 Z 1 vor. Unklar ist, ob damit im vorliegenden Zusammenhang eine rein automatisierte Verarbeitung (dh. ohne menschliches Zutun; in Abs. 5 erster Satz scheint der Begriff „automatisiert" – dort im Zusammenhang mit der Erhebung und Speicherung – in diesem Sinn verwendet zu werden) oder eine automationsunterstützte Verarbeitung durch ein zuständiges Organ gemeint ist.

15 Für den Fall, dass in Abs. 6 erster Satz eine automationsunterstützte Verarbeitung durch ein zuständiges Organ (und nicht ein rein automatisierter Abgleich) gemeint ist, sollte im Gesetzestext der Begriff „automationsunterstützt" verwendet werden.

16 Falls hingegen tatsächlich ein rein automatisierter Abgleich zur Feststellung von Verstößen (zB gegen die Weisung, einen bestimmten Ort zu betreten) intendiert sein sollte, wird darauf hingewiesen, dass gemäß § 41 DSG ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidungen einschließlich Profiling, die für die betroffene Personen nachteilige Rechtsfolgen haben oder sie erheblich beeinträchtigen können (was vorliegend bei Feststellung eines Verstoßes gegen eine Weisung zweifellos der Fall wäre), nur zulässig sind, soweit sie gesetzlich ausdrücklich vorgesehen sind. Eine solche gesetzliche Regelung muss nach den Vorgaben des Art. 11 Abs. 1 der Richtlinie (EU) 2016/680 (DSRL-PJ) jedenfalls

geeignete Garantien für die Rechte und Freiheiten der betroffenen Person, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen, vorsehen.

17 Um den – wohl nicht intendierten – Eindruck zu vermeiden, dass sämtliche in Abs. 6 geregelten Verpflichtungen nur in Bezug auf zum Zweck des Abs. 5 Z 1 verarbeiteten Daten gelten, wird angeregt, die auf Abs. 5 Z 1 beschränkte Verpflichtung zur automatisierten Verarbeitung in einem eigenen Satz zu regeln.

Für den Datenschutzrat
Der Vorsitzende:
OFENAUER
2. Februar 2021

Elektronisch gefertigt