

An das  
Bundesministerium für  
Landesverteidigung  
Per Mail:  
eleg@bmlvs.gv.at  
posteingang@bmlvs.gv.at

**Entwurf eines Bundesgesetzes, mit dem das Wehrgesetz 2001, das Heeresdisziplinalgesetz 2014, das Heeresgebührengesetz 2001, das Auslandseinsatzgesetz 2001, das Militärbefugnisgesetz, das Sperrgebietsgesetz 2002, das Munitionslagergesetz 2003, das Militärauszeichnungsgesetz 2002, das Verwundetenmedalliengesetz und das Truppenaufenthaltsgesetz geändert werden (Wehrrechtsänderungsgesetz 2019 –WRÄG 2019)**

Der Datenschutzrat hat in seiner **244. Sitzung am 21. Februar 2019 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

### **I. Allgemeines**

Laut den Erläuterungen sind im Hinblick auf das Militärbefugnisgesetz vereinzelte auf Grund der praktischen Erfahrungen (insbesondere durch den Rechtsschutzbeauftragten beim Bundesministerium für Landesverteidigung und Sport) sowie der neueren technischen Entwicklung notwendige Adaptierungen ins Auge gefasst. Dies betrifft insbesondere die Definition der „militärischen Rechtsgüter“ sowie die Voraussetzungen einer Datenübermittlung an inländische Behörden. Weiters sollen Anpassungen an die Novellen zum Sicherheitspolizeigesetz, BGBl. I Nr. 158/2005, 114/2007 und 13/2012, zur Strafprozessordnung (StPO), BGBl. I Nr. 19/2004, sowie an das Polizeiliche Staatsschutzgesetz (PStSG), BGBl. I Nr. 5/2016, durchgeführt werden.

### **II. Datenschutzrechtliche Bemerkungen**

**Zu Art. 5 (Änderung des Militärbefugnisgesetzes):**

#### **Zu Z 5 (§ 8 Abs. 2a):**

Der vorgeschlagene § 8 Abs. 2a ermächtigt militärische Organe im Wachdienst, „Personen [zu] kontrollieren, die einer öffentlichen Beleidigung des Bundesheeres oder einer selbständigen Abteilung des Bundesheeres verdächtig sind“. Da diese Befugnis zu einem Eingriff in Grundrechte (ua. in das Grundrecht auf Datenschutz gemäß § 1 DSG) ermächtigt, sollte geprüft werden, inwieweit die Regelung stärker determiniert bzw. eingegrenzt werden (oder gänzlich entfallen) kann: So könnte etwa – wie in § 8 Abs. 1 – normiert werden, dass Personenkontrollen nur in „engem zeitlichen Zusammenhang“ mit der mutmaßlichen Beleidigung durchgeführt werden dürfen. Auch sollte näher dargelegt werden, welche Handlungen das „Kontrollieren“ einer Person konkret umfasst.

In den Erläuterungen wird die Einführung der vorgeschlagenen Befugnis zur Personenkontrolle damit begründet, dass „oftmals [...] keine hierzu zuständigen Exekutivorgane vor Ort [sind]“. Es sollte geprüft werden, ob die Befugnis als subsidiäre Befugnis auszugestalten ist, die nur dann ausgeübt werden darf, wenn kein (zuständiges) Organ des öffentlichen Sicherheitsdienstes vor Ort ist, um rechtzeitig einzuschreiten.

#### **Zu Z 7 (§ 17 Z 2):**

Es wird angeregt, den Begriff „Computersystem“ und die Vorgaben für den Einsatz dieser Computersysteme zur Gefahrenabwehr präziser zu formulieren.

#### **Zu Z 8 (§ 22 Abs. 2a):**

Mit dem vorgeschlagenen § 22 Abs. 2a sollen die Auskunftsbefugnisse militärischer Organe und Dienststellen, die mit der nachrichtendienstlichen Aufklärung oder Abwehr betraut sind, erheblich erweitert werden. Angesichts der besonderen Grundrechtssensibilität (insbesondere mit Blick auf § 1 DSG und Art. 8 EMRK) dieser Befugnisse ist besonderes Augenmerk auf ihre verhältnismäßige Ausgestaltung zu legen: Dementsprechend ist sicherzustellen, dass die Regelungen einen ausreichenden Determinierungsgrad aufweisen und Grundrechtseingriffe auf das zur Zielerreichung unbedingt erforderliche Ausmaß begrenzt sind.

Der Datenschutzrat hat schon in seiner am 15. Februar 2013 einstimmig beschlossenen Stellungnahme zum Entwurf eines Verwaltungsgerichtsbarkeits-Begleitgesetzes-Wehrrecht – VwGBG-W (GZ BKA-817.339/0002-DSR/2013) Folgendes angemerkt:

*„Vorweg ist anzumerken, dass in § 22 Abs. 2a die Zwecke, für welche die Daten konkret benötigt werden, nicht ausreichend festgelegt sind. Überdies ist nicht klar ersichtlich, welcher Anwendungsbereich im Lichte der Zuständigkeitsverteilung gemäß § 2 Abs. 2 MBG, der den militärischen Eigenschutz und die Abgrenzung zur Sicherheitspolizei regelt, noch übrig bleiben. Für eine abschließende Beurteilung der Verhältnismäßigkeit des Eingriffes in das Grundrecht auf Datenschutz gemäß § 1 DSG 2000 ist jedoch eine konkrete Darlegung der Zwecke (und Aufgaben) für die Datenverwendung erforderlich.*

*Im Detail wird darauf hingewiesen, dass die pauschale Verwendung von Daten für (alle) den militärischen Organen und Dienststellen nach dem Militärbefugnisgesetz übertragenen*

*Aufgaben oder für den Fall, dass die Daten als wesentliche Voraussetzung zur Erfüllung der Aufgaben benötigt werden, hinsichtlich der in § 22 Abs. 2a Z 1 und 2 des Entwurfes genannten Daten nicht verhältnismäßig erscheint, weil aus den Bestimmungen nicht ausreichend konkret hervorgeht, um welche Aufgaben es sich hierbei jeweils handelt und wozu die Daten konkret benötigt werden.“*

In diesem Sinn wird zunächst vorgeschlagen, bezüglich der Begriffe „Betreibern öffentlicher Telekommunikationsdienste“ und „sonstigen Diensteanbietern“ – ebenso wie in § 53 Abs. 3a SPG – auf die Legaldefinitionen des § 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 und des § 3 Z 2 E-Commerce-Gesetz zu verweisen.

Überdies müssten die Zwecke, zu denen Auskünfte verlangt werden dürfen, genauer festgelegt werden: Während der geltende § 22 Abs. 2a eine Ermächtigung vorsieht, gewisse Auskünfte zu verlangen, die „als wesentliche Voraussetzung zur Erfüllung von Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr“ benötigt werden, stellt der vorgeschlagene § 22 Abs. 2a diesbezüglich lediglich auf die „Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben“ (Z 1) oder überhaupt bloß auf die „Erfüllung ihrer Aufgaben“ (Z 2 und 3) ab. Vor dem Hintergrund grundrechtlicher Vorgaben ist es erforderlich, die Auskunftsbefugnisse jeweils an die Erfüllung konkreter, genau abgegrenzter Aufgaben zu koppeln (vgl. dazu auch die gleichartige Befugnis gemäß § 53 Abs. 3a SPG) und auf das unbedingt notwendige Ausmaß zu beschränken.

Es stellt sich die Frage, in welchem Verhältnis der vorgeschlagene § 22 Abs. 2a Z 1 und der vorgeschlagene § 22 Abs. 2a Z 4 zu einander stehen. Insbesondere erscheint klärungsbedürftig, inwieweit sich diese beiden Befugnisse überschneiden. Dies sollte geprüft und in den Erläuterungen näher dargelegt werden.

Angesichts der Eingriffsintensität der Auskunftsbefugnisse nach dem vorgeschlagenen § 22 Abs. 2a wäre – ebenso wie bei den Befugnissen nach § 22 Abs. 3 bis 5 und 7 sowie dem vorgeschlagenen § 22 Abs. 2b – jedenfalls der Rechtsschutzbeauftragte nach § 22 Abs. 8 einzubinden.

Von den informierten Vertretern wurde zugesagt, dass in den Fällen des § 22a die generelle Einbindung des Rechtsschutzbeauftragten vorgesehen wird.

Es wird angemerkt, dass eine Änderung des § 99 Abs. 5 TKG 2003 erforderlich ist. Weiters sollte geprüft werden, ob die Durchlaufstelle nach TKG 2003 für Auskunftersuchen als sicherer Übertragungsweg genutzt werden kann.

Es wird angeregt, eine Klarstellung hinsichtlich der Speicherdauer und der Löschung der nach § 22 beauskunfteten Daten vorzunehmen.

#### **Zu Z 9 (§ 22 Abs. 2b):**

Im ersten Satz wäre klarzustellen, durch wen die Ermittlung personenbezogener Daten vorgenommen werden darf.

#### **Zu Z 12 (§ 25 Abs. 1 Z 2):**

Die vorgeschlagene Änderung des § 25 Abs. 1 Z 2 hätte eine deutliche Ausweitung der Ermächtigung zur Datenübermittlung an inländische Behörden zur Folge: So sollen militärische Organe und Dienststellen, die mit Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr betraut sind, pauschal ermächtigt werden, Daten an „inländische Behörden“ zu übermitteln, soweit die Übermittlung nur „der Wahrung eines wichtigen öffentlichen Interesses dient“.

Diese Befugnis zur Datenübermittlung erscheint mit Blick auf die Anforderungen des Grundrechts auf Datenschutz gemäß § 1 DSG nicht ausreichend determiniert: Zum einen erscheint es ganz generell problematisch, die Übermittlungsbefugnis pauschal von den (konkreten) Aufgaben der Empfängerbehörde loszulösen. Zum anderen führen auch die Erläuterungen aus, dass „[d]ie übermittelnde Dienststelle [...] ohne Kenntnis der Ermittlungsfälle bei der Empfängerbehörde (und deren Schwerpunkte) ein „wichtiges öffentliches Interesse“ eher nur vermuten als abwägen [kann].“ Insofern erscheint fraglich, ob sich die „Wahrung eines wichtigen öffentlichen Interesses“ als (bloße) Voraussetzung für eine derartige Übermittlungsbefugnis überhaupt eignet.

Angesichts des weiten Kreises potentieller Empfänger (alle „inländische[n] Behörden“) und in Ermangelung einer Beschränkung auf gewisse Kategorien von Daten ist es erforderlich, die zulässigen Fälle einer Übermittlung stärker zu konkretisieren und einzugrenzen (vgl. dazu die laut Erläuterungen „inhaltlich korrespondierende [...] Bestimmung“ des § 56 Abs. 1 Z 2 SPG). Zu § 25 Abs. 1 Z 1 bis 4 sollte klargestellt werden, dass eine Verpflichtung zum Vorgehen nach § 37 Abs. 8 und 9 DSG (nach dem Vorbild des § 56 Abs. 3 SPG) besteht.

22. Februar 2019  
Für den Datenschutzrat  
Der Vorsitzende:  
OFENAUER

***Elektronisch gefertigt***