REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.339/0002-DSR/2013
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium
für Landesverteidigung und
Sport

Per E-Mail:

eleg@bmlvs.gv.at

Betrifft: Entwurf eines Verwaltungsgerichtsbarkeits-Begleitgesetzes-Wehrrecht – VwGBG-W

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **215. Sitzung am 15. Februar 2013 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Im gesamten Wehrrecht sind die einschlägigen legistischen Maßnahmen in Bezug auf die **Einführung einer Verwaltungsgerichtsbarkeit** umzusetzen. Die umfangreichsten Änderungen sind im Heeresdisziplinargesetz 2002 erforderlich. Weiters soll im **Wehrgesetz 2001** die wehrgesetzliche Bestimmung hinsichtlich der Verwendung von sensiblen Daten (§ 55a Abs. 1) stärker an jene des Datenschutzgesetzes 2000 (DSG 2000) unter Beachtung der Datenschutz-Richtlinie 95/46/EG angepasst werden. Im **Militärbefugnisgesetz (MBG)** soll zusätzlich zu der bereits seit 1. Oktober 2002 bestehenden Befugnis zum Verlangen von Auskünften betreffend die Teilnehmernummer bestimmter Telefonanschlüsse künftig auch auf vergleichbare Daten betreffend das „**Internet**“ Bedacht genommen werden. Eine vergleichbare Regelung besteht bereits seit 1. Jänner 2008 im § 53 Abs. 3a Sicherheitspolizeigesetz (SPG), der mit Wirkung vom 1. April 2012 inhaltlich

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

modifiziert wurde. Im Rahmen der mit 1. Jänner 2006 in Kraft getretenen SPG-Novelle 2006, BGBl. I Nr. 158/2005, wurde in den §§ 53 und 54 SPG ausdrücklich auf „**Bild- und Tonaufzeichnungsgeräte**“ bei der Wahrnehmung bestimmter sicherheitspolizeilicher Aufgaben Bedacht genommen. Weiters wurde die „Videoüberwachung“ im Rahmen der DSG-Novelle 2010, BGBl. I Nr. 133/2009 (§§ 50a ff DSG 2000), explizit geregelt, „sofern nicht durch andere Gesetze Besonderes bestimmt ist“. **Vor diesem Hintergrund soll nunmehr für den „militärischen Eigenschutz“ eine eigene diesbezügliche Bestimmung geschaffen werden.**

2) Datenschutzrechtlich relevante Regelungen

Artikel 1 (Änderung des Wehrgesetzes 2001)

Zu Z 34 (§ 55):

Nach § 55 Abs. 2 dürfen die mit der Vollziehung dieses Bundesgesetzes betrauten Behörden **zur Wahrnehmung der ihnen jeweils übertragenen Aufgaben** Daten verarbeiten.

Dazu ist anzumerken, dass eine **pauschale Ermächtigung zur Datenverwendung** – soweit es sich um die Verwendung **sensibler Daten** handelt (zB im Zusammenhang mit der Feststellung der Eignung zum Wehrdienst) – nicht ausreichend erscheint und hinsichtlich der Verwendung sensibler Datenarten und den jeweiligen Aufgaben präzisiert werden müsste. Für eine Verwendung von **nicht-sensiblen Daten** wäre die pauschale Ermächtigung hingegen **nicht erforderlich**, wenn sie gemäß § 8 Abs. 1 Z 4 iVm § 8 Abs. 3 Z 1 DSG 2000 für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist.

Zu Z 35 (§ 55a Abs. 1):

Nach § 55a Abs. 1 dürfen die einzelnen Ergebnisse der Untersuchungen zur Feststellung der Eignung der Personen zum Wehrdienst, soweit **zur Wahrung eines wichtigen öffentlichen Interesses** gesetzlich nicht anderes bestimmt ist, nur in den in den Z 1 und 2 genannten Gründen weitergegeben werden. Dazu wird angemerkt, dass ein Gesetz die Verwendung sensibler Daten durch eine staatliche Behörde aufgrund von § 1 Abs. 2 DSG 2000 ohnedies nur zur Wahrung wichtiger öffentlicher

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

Interessen vorsehen darf und gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen muss. **Sofern daher aufgrund dieser Bestimmung ausschließlich sensible Daten verwendet werden sollen, erscheint die Beifügung des wichtigen öffentlichen Interesses nicht erforderlich und sollte entfallen.**

Artikel 2 (Änderung des Heeresdisziplinargesetzes 2002)

Zu den Z 18 (§ 7 Abs. 1 und 2), 19 (§ 7 Abs. 4a) und 20 (§ 7 Abs. 5):

Nach § 7 Abs. 1 sind im militärischen Dienstbereich nach Eintritt der Rechtskraft **Disziplinarverfügungen und Disziplinarerkenntnisse, gerichtliche Verurteilungen und Strafverfügungen, verwaltungsbehördliche Straferkenntnisse und Strafverfügungen und Entscheidungen über Beschwerden gegen die Ausübung unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt wegen Rechtswidrigkeit zu verlautbaren**, sofern die Verlautbarung erforderlich ist, um der Begehung von Pflichtverletzungen entgegenzuwirken. Weitere Verlautbarungen für den jeweiligen Zuständigkeitsbereich sieht § 7 Abs. 2 für **Disziplinarverfügungen sowie für Disziplinarerkenntnisse, Urteile, Straferkenntnisse und Strafverfügungen** vor.

§ 7 Abs. 4a sieht zudem vor, dass der Bundesminister für Landesverteidigung und Sport Entscheidungen nach Abs. 1 Z 1 bis 3 verlautbaren kann, sofern er die Verlautbarung zur Aufrechterhaltung der Disziplin **in seinem gesamten Zuständigkeitsbereich** für angebracht hält.

Unklar ist, ob die Verlautbarungen nach § 7 in anonymer oder personenbezogener Form erfolgen. Zwar ordnet bereits die geltende Fassung des § 7 Abs. 5 des Heeresdisziplinargesetzes 2002 an, dass die Verlautbarung „**ohne Namensnennung**“ des Betroffenen zu erfolgen hat, ein **Personenbezug** kann sich jedoch auch aus anderen Umständen als dem Namen (zB dem Dienstort in Verbindung mit Dienstgrad und Tätigkeitsbereich) ergeben. Soweit die Verlautbarung jedoch in personenbezogener Form erfolgt, ist der Verhältnismäßigkeitsgrundsatz des § 1 Abs. 2 DSG 2000 zu beachten. Demgemäß dürfen personenbezogene Daten nur dann verwendet werden, wenn sie zur Zweckerreichung erforderlich sind und die Verwendung das gelindeste, zur Zielerreichung zur Verfügung stehende Mittel

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

darstellt. Insbesondere im Hinblick auf die Verlautbarung von **Entscheidungen im gesamten Zuständigkeitsbereich** des Bundesministers für Landesverteidigung und Sport (zB im Intranet) nach § 7 Abs. 4a zum Zweck der „Aufrechterhaltung der Disziplin“ erschiene eine personenbezogene Verlautbarung nicht verhältnismäßig. Es sollte daher festgelegt werden, dass eine Verlautbarung im gesamten Zuständigkeitsbereich in jedem Fall **nur anonymisiert** erfolgen darf.

Artikel 5 (Änderung des Militärbefugnisgesetzes)

Der Datenschutzrat begrüßt die durch den Vertreter des Bundesministeriums für Landesverteidigung und Sport überbrachte verbindliche Zusage des Bundesministers für Landesverteidigung und Sport, dass die in Artikel 5 des Entwurfes (Änderung des Militärbefugnisgesetzes) vorgesehenen Z 4 (§ 15 Abs. 2) und 5 (§ 22 Abs. 2a) ersatzlos gestrichen werden und daher in der Regierungsvorlage nicht enthalten sein werden.

Damit wird den nachstehend angeführten Bedenken des Datenschutzrates Rechnung getragen.

Zu Z 4 (§ 15 Abs. 2):

Nach § 15 Abs. 2 ist die **Datenermittlung mit Bildübertragungs- und Bildaufzeichnungsgeräten (Videoüberwachung)** zulässig, wenn dies für Zwecke des militärischen Eigenschutzes erforderlich ist.

Die Datenermittlung mit Bild- und Bildaufzeichnungsgeräten (Videoüberwachung) für **(alle) Zwecke des militärischen Eigenschutzes** erscheint im Hinblick auf die von § 1 Abs. 2 DSG 2000 geforderte Verhältnismäßigkeit zu weitgehend. Die vorgeschlagene Bestimmung würde wohl auch die Überwachung der gesamten Innenräumlichkeiten erfassen. Je nachdem, in welchen Bereichen die Überwachung eingesetzt wird, greift die Videoüberwachung jedoch unterschiedlich intensiv in das Geheimhaltungsrecht und das Recht auf Achtung des Privatlebens der Betroffenen ein: In Gemeinschaftsräumen, in denen das Verhalten der Betroffenen ohnehin auch von anderen Personen wahrgenommen wird, ist die Eingriffsintensität geringer zu bewerten als in Bereichen, in denen sich Personen ansonsten unbeobachtet und

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

alleine aufhalten. Am intensivsten stellen sich Eingriffe naturgemäß in Räumlichkeiten wie Sanitäranlagen dar, die der höchstpersönlichen Intimsphäre zuzurechnen sind. **Insbesondere muss daher im Gesetzestext klargestellt werden, dass mit einer Videoüberwachung nicht Ereignisse an Orten festgestellt werden dürfen, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen. Weiters hätte eine Abstufung zu erfolgen, wann – wenn überhaupt – nur das gelindere Mittel der Echtzeitüberwachung vorzusehen und wann Videoaufzeichnungen allenfalls ad hoc zu erlauben wären (vgl. in diesem Zusammenhang auch § 54 Abs. 4 Z 2 SPG). Zudem muss in den Erläuterungen der Zweck und der Ort der Videoüberwachungen sowie die Bedeutung im Zusammenhang mit dem militärischen Eigenschutz genauer dargelegt werden.**

Zu Z 5 (§ 22 Abs. 2a):

Der Datenschutzrat hat bereits mehrfach in seinen Stellungnahmen betont, dass die Frage der Verhältnismäßigkeit einer zwingenden Anordnung der flächendeckenden Speicherung von Verkehrsdaten für Zwecke der Strafverfolgung über jenen Zeitraum hinaus, in dem sie für die Übertragung der Nachricht oder für die Gebührenabrechnung und die Bezahlung von Zusammenschaltungen notwendig sind, in keiner Weise geklärt ist.

Zudem weist der Datenschutzrat darauf hin, dass der VfGH mit Beschluss G 47/12-11, G 59/12-10, G 62, 70, 71/12-11 vom 28. November 2012, grundsätzliche Bedenken zur Vorratsdatenspeicherung geäußert und ein Vorabentscheidungsverfahren beim EuGH beantragt hat. Im Lichte dieser vom VfGH gegen die Vorratsdatenspeicherung geäußerten Bedenken erscheint es nicht sinnvoll, den Zugriff auf solche Daten zu erweitern.

Zu dem in Begutachtung befindlichen Entwurf des § 22 Abs. 2a MBG wird Folgendes angemerkt:

Militärische Organe und Dienststellen nach § 22 Abs. 1 dürfen von den Betreibern öffentlicher Telekommunikationsdienste und sonstigen Diensteanbietern nach § 22 Abs. 2a **Auskünfte** verlangen über

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

1. **Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses**, wenn dies zur Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben erforderlich ist,
2. **Internetprotokolladresse zu einer bestimmten Nachricht** und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Erfüllung ihrer Aufgaben benötigen,
3. **Namen und Anschrift eines Benutzers, dem eine Internetprotokolladresse zu einem bestimmten Zeitpunkt zugewiesen war**, wenn sie diese Daten als wesentliche Voraussetzung zur Erfüllung ihrer Aufgaben benötigen, auch wenn hiefür die Verwendung von **Vorratsdaten** erforderlich ist,
4. **Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses** durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer, wenn dies für die Abwehr gegenwärtiger vorsätzlicher Angriffe gegen militärische Rechtsgüter unter Bedachtnahme auf die militärische Zuständigkeit nach § 2 Abs. 2 erforderlich ist.

Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

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**

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

Aufgaben es sich hierbei jeweils handelt und wozu die Daten konkret benötigt werden.

Weiters wird im Hinblick auf die Verwendung von **Vorratsdaten** nach § 22 Abs. 2a Z 3 auf § 102a Abs. 1 des Telekommunikationsgesetzes 2003 (TKG 2003), BGBl. I Nr. 70/2003, hingewiesen, wonach Anbieter von öffentlichen Kommunikationsdiensten über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 TKG 2003 hinaus nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern haben. **Die Speicherung erfolgt ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt.**

Auch nach § 53 Abs. 3a Z 3 des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991, kann dann Auskunft verlangt werden, wenn der Namen und die Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, **als wesentliche Voraussetzung zur Abwehr einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht, eines gefährlichen Angriffs oder einer kriminellen Verbindung benötigen wird.**

§ 22 Abs. 2a Z 3 des Entwurfes sieht jedoch **keine dem § 102a Abs. 1 TKG 2003 oder § 53 Abs. 3a Z 3 SPG vergleichbare Zweckbeschränkungen** vor. Das ist insofern äußerst problematisch, als die eingeschränkte Verwendung von Vorratsdaten im TKG 2003 auf der Erwägung beruht, dass schon die verdachtslose Speicherung von Verkehrsdaten einen erheblichen Grundrechtseingriff darstellt und daher die Nutzung dieser Daten nur unter besonderen Voraussetzungen verhältnismäßig ist. **Die vorgeschlagene Regelung entspricht daher nicht dem Verhältnismäßigkeitsgrundsatz nach § 1 Abs. 2 DSG 2000, da sie Auskünfte generell bereits dann als zulässig ansieht, wenn Vorratsdaten als wesentliche Voraussetzung zur Erfüllung der Aufgaben – sofern diese denkmöglich überhaupt vorliegen können – benötigt werden, wohingegen die Bestimmungen des TKG 2003 iVm jenen der StPO und des SPG deutlich**

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

höhere Schranken setzen und eine Auskunft nur in besonders schwerwiegenden Fällen erlauben.

Im Übrigen ist in § 22 Abs. 2a unklar, was unter einem „**sonstigen Diensteanbieter**“ zu verstehen ist.

Zu den Z 14 (§ 54) und 17 (§ 57 Abs. 6):

§ 54 Abs. 4 und § 57 Abs. 6 sehen jeweils eine (direkte) Inanspruchnahme des **Bundesverwaltungsgerichtes** vor. Diesbezüglich wird auf den vom Bundeskanzleramt-Verfassungsdienst am 24. Jänner 2013 ausgesendeten Entwurf eines Verwaltungsgerichtsbarkeits-Anpassungsgesetzes – Bundeskanzleramt, welcher im Wege einer Änderung des DSG 2000 die Einrichtung einer „**Datenschutzbehörde**“ zur Entscheidung in I. Instanz enthält, hingewiesen. Im Besonderen wird dabei auch auf Artikel 2 dieses Entwurfes hingewiesen, mit welchem im Rahmen einer lex fugitiva in anderen Bundesgesetzen der Begriff „Datenschutzkommission“ mit dem Begriff „Datenschutzbehörde“ ersetzt werden soll. **Demgemäß sollte für den Fall der Einrichtung einer „Datenschutzbehörde“ in § 54 Abs. 4 und § 57 Abs. 6 statt der Anrufung des Bundesverwaltungsgerichtes die „Datenschutzbehörde“ vorgesehen werden.**

4. März 2013
Für den Datenschutzrat
Der stv Vorsitzende:
BAUMGARTNER

Elektronisch gefertigt

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.