REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.290/0001-DSR/2014
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für
Inneres

Mit E-Mail:

bmi-III-1@bmi.gv.at

bmi-III-7@bmi.gv.at

Betrifft: Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz geändert wird (SPG-Novelle 2014)

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **219. Sitzung am 21. März 2014 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Laut den Erläuterungen enthält der Entwurf im Wesentlichen folgende Punkte:
1. Mit der Neuregelung der Bestimmung zur DNA-Untersuchung soll den Bedenken des VfGH Rechnung getragen werden, indem eine solche nur mehr bei gerichtlich strafbaren vorsätzlichen Handlungen, die mit mindestens einjähriger Freiheitsstrafe bedroht sind, gesetzlich zulässig sein soll. Damit in engem Zusammenhang steht die Bestimmung des § 65 Abs. 1, die derzeit vom VfGH einer Prüfung unterzogen wird. Auch hier sollen die vom VfGH im Prüfbeschluss geäußerten Bedenken einer gesetzlichen Klarstellung zugeführt werden.

2. Das BM.I hat in den letzten Jahren ein umfassendes Maßnahmenpaket zur Bekämpfung von Gewalt bei Sportgroßveranstaltungen erarbeitet, indem der Sicherheitsbehörde Befugnisse im Sicherheitspolizeigesetz eingeräumt wurden, die ein effektives Vorgehen bei gewalttätigen gefährlichen Angriffen ermöglichen. Damit ist es gelungen, die Zahl der Anzeigen wegen gerichtlich strafbarer Handlungen unter Anwendung von Gewalt bei Sportgroßveranstaltungen deutlich zu reduzieren.
In der nationalen sowie internationalen Entwicklung zeigt sich jedoch, dass der Fokus neben der Gewaltbereitschaft der Fans auch auf das Thema Rassismus bei Sportgroßveranstaltungen gerichtet sein muss. Erst im Mai 2013 hat sich die UEFA bei ihrem XXXVII. ordentlichen Kongress in London auf die IX. Resolution geeinigt, die unter dem Titel „Der europäische Fußball vereint gegen Rassismus“ steht.
Darin werden die Mitgliedsverbände aufgefordert, ihre Bemühungen, den Rassismus aus dem Fußball zu eliminieren, noch zu verstärken. Rassistisches Verhalten jedweder Art mit Bezug zum Fußball soll strenger bestraft werden und Fans, die rassistischen Verhaltens für schuldig befunden wurden, soll der weitere Besuch von Spielen von staatlicher Seite verboten werden. Ein erster Schritt in diese Richtung wurde bereits mit der SPG-Novelle 2011, BGBl I Nr. 13/2012 gesetzt, indem die Verwaltungsübertretungen nach Art. III Abs. 1 Z 4 des Einführungsgesetzes zu den Verwaltungsverfahrensgesetzen 2008 (EGVG) und § 3 des Abzeichengesetzes 1960 in den § 49b SPG (Gefährderansprache) aufgenommen wurden.
In einem weiteren Schritt sollen die für Sportgroßveranstaltungen relevanten Bestimmungen des Sicherheitspolizeigesetzes, wie etwa die Wegweisungsbefugnis (§ 49a Abs. 2) oder die Meldeauflage (§ 49c), um den Bereich des Rassismus erweitert werden.
3. Derzeit ist den Sicherheitsbehörden der vorbeugende Schutz von verfassungsmäßigen Einrichtungen und deren Handlungsfähigkeit (§ 22 Abs. 1 Z 2 SPG) übertragen. Die nunmehr vorgeschlagene Ergänzung soll den Sicherheitsbehörden vor dem Hintergrund der immer größer werdenden Abhängigkeit der Bevölkerung von funktionierenden Infrastrukturleistungen sowie möglichen Bedrohungsszenarien auch und vor allem im Bereich der Computerkriminalität die entsprechende Aufgabenerfüllung übertragen. Zudem verpflichtet die Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (RL zum Schutz kritischer

Infrastrukturen), die Mitgliedstaaten zu entsprechenden rechtlichen Rahmenbedingungen zur Gewährleistung ihres Schutzes. Im Hinblick auf die Umsetzung der Richtlinie und vor dem Hintergrund, dass der Schutz kritischer Infrastrukturen und die Gewährleistung von Cyber-Sicherheit in diesem Bereich von besonderer Bedeutung für die Gesundheit, Sicherheit, das wirtschaftliche und soziale Wohl der Bevölkerung und das Funktionieren staatlicher Einrichtungen ist, erscheint es notwendig, bestimmte Einrichtungen und Systeme als sensibel zu erkennen und besonders zu schützen, weshalb eine eigenständige sicherheitspolizeiliche Aufgabe geschaffen werden soll.

2) Datenschutzrechtlich relevante Bestimmungen

Zu § 22 und § 55a Abs. 2 Z 3a:

Die Definition des Begriffs „kritische Infrastrukturen“ ist nach Ansicht des Datenschutzrates zu weit gefasst, da die Erweiterung sicherheitspolizeilicher Aufgaben auch eine Ausweitung der bestehenden Befugnisse nach sich zieht. Aufgrund dieser Regelung können ArbeitnehmerInnen, die in Bereichen tätig sind, wo kritische Infrastrukturen im Sinne des Entwurfes vorhanden sind, einer Sicherheitsüberprüfung im Auftrag des Arbeitgebers unterzogen werden, wobei nicht unterschieden wird, welche Funktionen diese Mitarbeiter im Unternehmen ausüben. Es sollte daher geprüft werden, ob die Sicherheitsüberprüfung nicht auf einzelne Bereiche kritischer Infrastrukturen eingeschränkt werden kann, zumal eine Sicherheitsüberprüfung voraussetzt, dass der Betroffene Zugang zu „vertraulichen Informationen“ hat, also zu Informationen, die unter strafrechtlichem Geheimhaltungsschutz (insb. nach dem 16. Abschnitt des StGB „Landesverrat“) stehen und deren Geheimhaltung im öffentlichen Interesse gelegen ist (§ 55 Abs. 3 Z 1 SPG). Sofern dies in einzelnen Bereichen kritischer Infrastrukturen von vornherein ausgeschlossen oder unwahrscheinlich ist, sollten diese Bereiche vom Anwendungsbereich der Sicherheitsüberprüfung von vornherein ausgenommen werden. **Nach Ansicht des Datenschutzrates sollte daher eine nähere gesetzliche Determinierung gemäß den oben genannten Kriterien erfolgen.**

Zu Z 12 (§ 56 Abs. 1 Z 3a):

Vorab wird darauf hingewiesen, dass diese Bestimmung **die Übermittlung von strafrechtsrelevanten Daten und allenfalls auch sensiblen Daten** (zB politische

Gesinnung) **an Private** vorsieht. Deshalb stellt sich die Frage nach besonderen Vorkehrungen im Hinblick auf das Risiko einer nicht zweckentsprechenden Weiterverwendung dieser Daten durch den Empfänger, um den Schutz des Geheimhaltungsrechts der Betroffenen sicherzustellen. **Insbesondere muss nach Ansicht des Datenschutzrates garantiert sein, dass die übermittelten Daten auch im Rahmen der Verwendung durch den Österreichischen Fußballbund und die Österreichische Fußball-Bundesliga einem ausreichenden Schutz in Bezug auf Speicherdauer, Datensicherheitsmaßnahmen usw. unterliegen, wobei gewährleistet werden muss, dass die gemäß § 56 Abs. 5 SPG eingeforderten Datensicherheitsmaßnahmen ausnahmslos eingehalten und vom BMI bzw. der unabhängigen Datenschutzbehörde überprüft werden.**

Wird dies nicht gewährleistet, ist auf die Gefahr hinzuweisen, dass durch die Übermittlung von polizeilichen Daten an den Österreichischen Fußballbund und die Österreichische Fußball-Bundesliga **„Schattendatenbanken" mit behördlichen Daten bei Privaten** existieren.

Die im Entwurf vorgesehene **„Übermittlung vorhandener Beweismittel" ist jedenfalls zu weit gefasst und könnte dem Wortlaut nach etwa auch Kommunikationsdaten oder DNA-Daten beinhalten**. Eine Einschränkung auf konkrete Beweismittel, etwa auf die in den Erläuterungen genannten Lichtbilder und Vernehmungsprotokolle, wäre in diesem Zusammenhang jedenfalls einer pauschalen Formulierung vorzuziehen. Dabei ist zu berücksichtigen, dass diese Beweismittel auch Daten weiterer Betroffener enthalten können (zB Nennung von Namen im Vernehmungsprotokoll). **Zudem ist sicherzustellen, dass die Übermittlung von Daten in jedem Einzelfall auf ihre Erforderlichkeit und Verhältnismäßigkeit hin geprüft wird; im Falle einer rechtskräftigen Verurteilung würde etwa die Mitteilung über den Ausgang des Strafverfahrens ausreichen, womit eine Übermittlung von Beweismitteln nicht mehr erforderlich wäre.**

Der Datenschutzrat hält fest, dass im Gesetz entsprechende Vorkehrungen zB dafür getroffen werden sollten, dass übermittelte Beweismittel nach Erfüllung ihres Zwecks (hier: Prüfung und Veranlassung eines Sportstättenbetretungsverbotes) zwingend an die Behörde zurückzustellen sind und eine weitere lokale Speicherung sowie die Weiterübermittlung oder Verarbeitung zu anderen Zwecken unzulässig ist.

Wobei allerdings angemerkt wird, dass eine weitere Übermittlung personenbezogener Informationen über die Verhängung eines Sportstättenbetretungsverbotes vom Österreichischen Fußballbund oder der Österreichischen Fußball-Bundesliga an die einzelnen Fußballspiel-Veranstalter, die

das Sportstättenbetretungsverbotes auch vollziehen müssten, derzeit gesetzlich nicht vorgesehen ist.

Zu Z 15 (§ 65 Abs. 1 und 5):

Die explizite Einschränkung der Zulässigkeit einer erkennungsdienstlichen Behandlung auf Menschen, die im Verdacht stehen, eine mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, ist grundsätzlich positiv zu bewerten. Allerdings ist darauf hinzuweisen, dass der Verfassungsgerichtshof in seinem Prüfungsbeschluss vom 1. Oktober 2013, B 1156/2013 (Gesetzesprüfungsverfahren G 90/2013), hinsichtlich § 65 Abs. 1 das Bedenken formuliert hat, dass „der Verdacht der Begehung jedweder Straftat – selbst einer Verwaltungsstraftat sowie gerichtlich strafbarer Fahrlässigkeitsdelikte oder gerichtlich strafbarer Vorsatzdelikte mit geringem Unwertgehalt („Bagatelldelikte“) – Anlass für eine erkennungsdienstliche Behandlung geben“ kann. **Mit der vorgeschlagenen Formulierung wird dieses Bedenken zwar im Hinblick auf Verwaltungsstraftaten und Fahrlässigkeitsdelikte entkräftet, nicht jedoch im Hinblick auf gerichtlich strafbare Vorsatzdelikte mit vergleichsweise geringem Unwertgehalt.**

Zu Z 16 (§ 67 Abs. 1):

Die neu eingezogene Schwelle der mit mindestens einjähriger Freiheitsstrafe bedrohten gerichtlich strafbaren Handlung ist grundsätzlich positiv zu bewerten.

Im Hinblick auf die vom Verfassungsgerichtshof in seinem Erkenntnis vom 12. März 2013, G 76/2013, angesprochene „besondere Sensibilität eines DNA-Profiles …, dessen künftige Verwendbarkeit bzw. Aussagekraft heute noch gar nicht absehbar ist …, sowie die Möglichkeit einer zweckentfremdeten Nutzbarmachung“ wäre ergänzend zu einer Differenzierung nach der Strafdrohung jedoch eine Differenzierung nach Deliktstypen zu prüfen. Soweit in den Erläuterungen darauf hingewiesen wird, dass die Abgrenzung jener des Europäischen Haftbefehles sowie jener für den Zugriff auf DNA-Daten im Rahmen des Prümer Datenverbundes entspricht, ist zu bemerken, dass die Verhältnismäßigkeit der Übermittlung vorhandener (zulässigerweise ermittelter) DNA-Daten unter anderen Gesichtspunkten zu beurteilen ist, als deren Ermittlung.

Der Verfassungsgerichtshof hat in diesem Zusammenhang ausgesprochen, dass § 67 Abs. 1 erster Satz SPG keine hinreichenden Kriterien enthält, welche die im Einzelfall vorzunehmende Prognoseentscheidung entsprechend determinieren

würden (Erkenntnis des VfGH vom 12. März 2013, G 76/2013, Rz 29). Dies wäre jedenfalls im Sinne einer ausreichenden Determinierung zu berücksichtigen.

Zu Z 17 (§ 73):

Wenngleich § 73 Abs. 1 nach dem Erkenntnis des Verfassungsgerichtshofes vom 12. März 2013, G 76/12, bei einer verfassungskonformen Interpretation eine angemessene Abwägung und Gewichtung des Interesses des Betroffenen an der Geheimhaltung bzw. Löschung seiner personenbezogenen Daten und dem Interesse des Staates am Fortbestehen des Eingriffes durch Fortsetzung der Speicherung nach den allgemeinen Grundsätzen über die Verwendung von Daten im Einzelfall erlaubt, wird empfohlen, eine dementsprechende gesetzliche Regelung aufzunehmen.

Die im Falle einer Verurteilung anzuwendende Bestimmung der Z 1 (eine Anwendung der Z 4 kommt diesfalls nicht in Betracht) legt eine sehr umfangreiche Maximalspeicherdauer für Daten aus einer erkennungsdienstlichen Behandlung (Vollendung des 80. Lebensjahres und seit der letzten erkennungsdienstlichen Behandlung mindestens fünf Jahre verstrichen) fest.

Da in der Praxis eine regelmäßige amtswegige Prüfung sämtlicher Datensätze dahingehend, ob die fortdauernde Speicherung nach den allgemeinen Grundsätzen des Datenschutzes nach wie vor zulässig ist, kaum umsetzbar ist, wird angeregt, zu prüfen, ob in § 73 Abs. 1 (insbesondere auch für den Fall einer gerichtlichen Verurteilung) generell die amtswegige Löschung der Daten aus einer erkennungsdienstlichen Behandlung nach einem bestimmten Zeitraum angeordnet werden kann und eine weitere Verarbeitung im Einzelfall davon abhängig gemacht werden kann, dass dies erforderlich ist, weil auf Grund konkreter Umstände zu erwarten sei, der Betroffene werde gefährliche Angriffe begehen.

Anregung zu § 74:

§ 74 Abs. 3 SPG bestimmt, dass erkennungsdienstliche Daten, die gemäß § 68 Abs. 1, 3 oder 4 ermittelt wurden, auf Antrag des Betroffenen zu löschen sind. Wenngleich nach Aufhebung des § 74 Abs. 1 und 2 betreffend die Löschung erkennungsdienstlicher Daten auf Antrag des Betroffenen die allgemeinen Regelungen des Datenschutzgesetzes 2000 Anwendung finden, sollte der Wegfall dieser verfassungswidrigen Bestimmungen nicht dazu führen, dass das SPG gar keine Regelung darüber enthält, unter welchen Voraussetzungen eine Löschung erkennungsdienstlicher Daten auf Antrag des Betroffenen zu erfolgen hat. **Insbesondere auch im Hinblick auf erkennungsdienstliche Daten aus einer**

DNA-Untersuchung wäre eine klare Regelung, in welchen Fällen diese Daten auf Antrag zu löschen sind, jedenfalls erforderlich.

26. März 2014
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt