



Kammer für Arbeiter und Angestellte für Tirol
Maximilianstraße 7, A-6020 Innsbruck
Tel: 0800/22 55 22, Fax: 0512/53 40-1749
konsument@ak-tirol.com, www.ak-tirol.com

Vorab per Fax:
01 50165 42765

Bundesarbeitskammer
Prinz-Eugen-Straße 20-22
1041 Wien

G.-Zl.: Kr-2015-9591/Dr.Ob/ia
Bei Antworten diese Geschäftszahl angeben.

Bei Rückfragen **Dr. Oberlechner**

Klappe **1800** Innsbruck, **24.04.2015**

Betrifft: Bundesgesetz, mit dem das Bundesgesetz über die Organisation, Aufgabe und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz-PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden

Bezug: Zuständiger Referent: Gerhard Penkner

Werte Kolleginnen und Kollegen!

Die Kammer für Arbeiter und Angestellte für Tirol nimmt zu dem im Betreff angeführten vorgelegten Entwurf eines polizeilichen Staatsschutzgesetzes (PStSG) wie folgt Stellung:

Grundsätzlich ist es zu begrüßen, dass Bestrebungen dahingehend erfolgen sollen, aufgrund diverser Bedrohungsszenarien in einer globalisierten Welt, die im Staatsgebiet lebenden Menschen, sowie die verfassungsmäßige Grundordnung verstärkt zu schützen. Insgesamt ist bei diesem Vorhaben jedoch immer darauf zu achten, dass eine gründliche Interessenabwägung zwischen Datenschutz (Schutz personenbezogener Daten) und Bürgerrechten bzw. möglichen Eingriffen in Grundrechte einerseits sowie notwendigen Maßnahmen einer (effektiven) Bekämpfung möglicher Bedrohungen andererseits erfolgt und der Grundsatz der Verhältnismäßigkeit gewahrt bleibt. Eine zulässige Datenverarbeitung muss immer notwendig! (im Sinne des gelindesten Mittels) und verhältnismäßig sein (Einzelfallprüfung). Jedenfalls ist eine (ausgeglichene) Balance zwischen Grundrechten beziehungsweise dem Schutz personenbezogener Daten und der inneren Sicherheit entsprechend sicher zu stellen. Diesbezüglich sind auch verfassungsrechtlich garantierte (Europäische Menschenrechtskonvention) und europarechtlich vorgegebene Grundrechte (EU-Grundrechte-Charta) entsprechend zu berücksichtigen. Mit Entscheidung des Europäischen Gerichtshofes vom

08.04.2014 wurde die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung (VDSBRL) zur Gänze aufgehoben. Dem folgend hat der österreichische Verfassungsgerichtshof (VfGH) auch die innerstaatliche Umsetzung der Richtlinie als verfassungswidrig erkannt und aufgehoben.

Zu den einzelnen, vorgeschlagenen Bestimmungen im polizeilichen Staatsschutzgesetz (PStSG) darf die Kammer für Arbeiter und Angestellte für Tirol Folgendes anführen:

Zu § 6 Abs. 1 Z 2 polizeiliches Staatsschutzgesetz-PStSG:

Die Formulierung „der vorbeugende Schutz vor „wahrscheinlichen“ verfassungsgefährdenden Angriffen durch eine Person“ ist auslegungsbedürftig, bietet einen zu großen Spielraum und ist auch zu wenig klar definiert. Was ist unter einem „wahrscheinlichen“ Angriff tatsächlich konkret zu verstehen? Hier müsste seitens des Gesetzgebers eine entsprechende Nachschärfung erfolgen.

Zu § 10 Abs. 5 polizeiliches Staatsschutzgesetz-PStSG:

Die vorgesehene Ermächtigung des Bundesamtes beziehungsweise der Landesämter, personenbezogene (und auch sensible) Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten zu ermitteln und weiterzuverarbeiten, erscheint (auch verfassungsrechtlich) problematisch. Dies insbesondere deshalb, da die gewählte Formulierung als insgesamt zu wenig transparent beziehungsweise als zu wenig genau definiert erscheint. Den Behörden würde damit die Berechtigung eingeräumt, personenbezogene Daten unbeschränkt aus allen verfügbaren Quellen zu ermitteln und weiterzuverarbeiten. Hier erscheint es zweckmäßig, die „Quellen“, aus denen personenbezogene Daten ermittelt beziehungsweise weiterverarbeitet werden sollen, näher zu definieren. Ebenso ist die Kammer für Arbeiter und Angestellte für Tirol der Auffassung, dass die Formulierung „im Internet öffentlich zugängliche Daten“ konkreter zu definieren ist. Das Abstellen auf mögliche „zusätzliche Sicherungsschranken“ erscheint diesbezüglich als zu wenig. Insbesondere ist zu befürchten, dass in der Praxis Auslegungsschwierigkeiten hinsichtlich „öffentlich zugängliche Daten“ beziehungsweise „nicht öffentlich zugänglicher Daten“ ergeben würden. In diesem Zusammenhang bestehen auch verfassungsrechtliche wie auch europarechtliche Bedenken hinsichtlich einer möglichen Verletzung schutzwürdiger Interessen von Kommunikationsteilnehmern, dies auch bei rein passiv-rezeptiven Erhebungen von Daten. Zusammenfassend wäre daher jedenfalls eine exaktere Unterscheidung zwischen öffentlichen Daten und nicht öffentlichen Daten zu treffen.

Zu § 11 Abs. 1 Z1-4 polizeiliches Staatsschutzgesetz- PStSG:

Insbesondere bei der in § 11 Abs. 1 Z 3 geplanten Datenanwendung in Zusammenhang mit Kontakt- beziehungsweise Begleitpersonen erscheint die Analyse von Beruf und Qualifikation/Beschäftigung/Lebensverhältnissen und sachbezogene Daten zu Kommunikation- und Verkehrsmittel als zu überschießend. Diesbezüglich würde die Analyse von Daten gemäß § 11 Abs. 1 Z1 a-j ausreichen, sodass k und l bei Kontakt- und Begleitpersonen entfallen sollte. Des Weiteren erscheint in diesem Zusammenhang problematisch, dass von einer Kontakt- oder Begleitperson dann gesprochen wird, wenn diese „nicht nur zufällig“ mit Personen gemäß § 11 Abs. 1 Z1 oder Z2 (Betroffene beziehungsweise Verdächtige) in Kontakt

steht. Diesbezüglich ist in der Praxis zu befürchten, dass auch vollkommen unbescholtene Personen, die eben gerade „zufällig“ mit den in § 11 Abs. 1 Z 1 und Z2 genannten Personen in Kontakt stehen, einer erheblichen Datenanalyse unterzogen werden. Des Weiteren scheint eine unterschiedliche Behandlung zwischen Kontakt oder Begleitpersonen (§ 11 Abs. 1 Z3) sowie von Informanten (§11 Abs. 1 Z4) sachlich nicht gerechtfertigt. Die oben genannte Problematik verschärft sich insofern, dass aufgrund der geplanten ausdrücklichen Ermächtigung auch sensible Daten im Sinne des § 4 Z 2 DSGVO 2000 zu allen betroffenen Kreisen verwendet werden dürfen, sofern dies erforderlich ist und angemessene Vorkehrungen für die Geheimhaltung dieser Daten getroffen werden.

Die Formulierung im vorgesehenen Abs. 1 Z 4 hinsichtlich einer Verarbeitung von „tat- und fallbezogenen Informationen und Verwaltungsdaten“ erscheint vollkommen intransparent. Diese viel zu allgemein gehaltene Formulierung könnte dazu verwendet werden, allenfalls auch rechtlich unzulässige Datenanalysen bzw. Datenverarbeitungen ex post zu rechtfertigen. Entweder wären hier genaue Definitionen zu derartig erlangten Informationen erforderlich bzw. sollte dieser Passus allenfalls gänzlich weggelassen werden. Dies insbesondere auch deshalb, da auch besonders schutzwürdige Daten von der geplanten Analyse bzw. Verarbeitung betroffen sind.

Zu § 11 Abs. 3 polizeiliches Staatsschutzgesetz - PStSG:

Das Vorhaben, dass (nachweislich) unrichtige Daten nicht richtigzustellen beziehungsweise nicht zu löschen sind, falls die Weiterverarbeitung von falschen Informationen mit der Kennzeichnung *unrichtig* zur Erfüllung des Zwecks der Bewertung der Wahrscheinlichkeit einer Gefährdung sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse, erscheint sachlich nicht gerechtfertigt. Es stellt sich die Frage, in welchen Fällen derartige „falsche Informationen“ für eine verbesserte Einschätzung mögliche Gefährdungspotenziale tatsächlich dienlich sein sollten.

Zu § 11 Abs. 4 polizeiliches Staatsschutzgesetz - PStSG:

Die vorgesehene Aufbewahrungsfrist von Protokollaufzeichnungen sollte von 3 auf 5 Jahre ausgedehnt werden. Dies würde auch mit den § 11 Abs. 2 vorgesehenen Lösungsfrist (5 Jahre) korrelieren. Eine Verlängerung der Aufbewahrungsfrist für Protokollaufzeichnungen erscheint insbesondere deshalb sinnvoll, da gerade bei unrichtigen Daten auch nach 3 Jahren noch die Möglichkeit bestehen sollte, die Erhebungsart sowie den Grund, dass diese Daten nicht richtiggestellt beziehungsweise nicht gelöscht wurden, in Erfahrung zu bringen.

Zu § 12 polizeiliches Staatsschutzgesetz - PStSG:

Diesbezüglich handelt es sich um die gesetzlichen Voraussetzungen für besondere Ermittlungsmaßnahmen. Grundvoraussetzung für die jeweiligen Maßnahmen ist, dass vor ihrem Beginn die Ermächtigung des Rechtsschutzbeauftragten eingeholt und erteilt wird.

Die Notwendigkeit zur Einholung von Auskünften zu IP-Adressen (Z5) ist jedenfalls unter der Berücksichtigung von (europarechtlichen und verfassungsrechtlichen) Grundrechten beziehungsweise dem Schutz personenbezogener Daten der betroffenen Einzelpersonen durchzuführen, dies insbesondere hinsichtlich der Zulässigkeit zur Einholung einer Auskunft zu Standortdaten. Ebenso erscheint die

diesbezüglich geplante Mitumfassung von Kontakt-oder Begleitpersonen (§ 11 Abs. 1 Z3), die nicht nur „zufällig“ mit Personen gemäß § 11 Abs. 1 Z1 und Z2 (Betroffene beziehungsweise Verdächtige) in Kontakt stehen, besonders problematisch.

Zu § 14 polizeiliches Staatsschutzgesetz - PStSG:

Gemäß § 14 Abs.2 sollte im Einzelfall zulässig sein, Daten über das Ende der Ermächtigung hinaus zu speichern, auch wenn zu diesem Zeitpunkt keine aktuelle Gefährdungslage vorliegt. Dies erscheint insofern problematisch, da eine grundsätzlich erforderliche Ermächtigung eben gerade nicht vorhanden ist und auch nicht klar ist, in welchen konkreten Fällen „in Hinblick auf die Person oder Gruppierung“ aufgrund bestimmter Tatsachen erwartet werden kann, dass diese neuerlicher Anlass für eine erweiterte Gefahrenforschung und/oder Schutz vor verfassungsgefährdeten Angriffen geben bzw. gewährleisten könnten. Insbesondere erscheinen die vorgegebene Frist von 2 Jahren (nach Ablauf der Zeit, für die eine Ermächtigung erteilt wurde) sowie die absolute Frist von 6 Jahren für die Löschung als insgesamt zu lang, insbesondere dann, wenn eben gerade keine aktuelle Gefährdungslage vorliegt. Nach Ansicht der Kammer für Arbeiter und Angestellte für Tirol ist diesbezüglich die erforderliche Verhältnismäßigkeit nicht gegeben.

Zu § 17 polizeiliches Staatsschutzgesetz - PStSG:

Es ist zu begrüßen, dass der Gesetzgeber vorsieht, dass Betroffene deren personenbezogene Daten verarbeitet werden, umfassend informiert werden müssen. Dies erscheint auch deshalb notwendig, um die notwendige Verhältnismäßigkeit und Überprüfungsmöglichkeiten sicherstellen zu können sowie eine ausgeglichene Balance zwischen Grundrechten beziehungsweise dem Schutz personenbezogener Daten einerseits und der inneren Sicherheit andererseits herstellen zu können. Problematisch erscheint diesbezüglich jedoch die vorgesehene Ausnahme in § 17 Abs.3. Eine mögliche Aufschiebung der Information „solange durch sie die Aufgabenerfüllung gefährdet wäre“ ist zu wenig klar determiniert und könnte daher in der Praxis zur möglichen Auslegung zu Schwierigkeiten führen. Diesbezüglich sind auch mögliche verfassungsrechtliche und europarechtliche Bedenken anzusprechen. Die Überlegungen, dass die Verpflichtung zu Information des Betroffenen nach Ende der Ermächtigung solange aufgeschoben werden kann, als andernfalls der Zweck der bereits gegen den Betroffenen gesetzten Maßnahmen gefährdet wäre, um mögliche erneute Gefahren abzuwenden, ist nach Ansicht der Kammer für Arbeiter und Angestellte für Tirol keine ausreichende sachliche Rechtfertigung für die in § 17 Abs. 3 vorgesehene Ausnahme einer grundsätzlich verpflichtenden Information der Betroffenen.

Zu Artikel 2/geplante Änderung des Sicherheitspolizeigesetzes darf die Kammer für Arbeiter und Angestellte für Tirol Folgendes anführen:

Zu § 13 a Sicherheitspolizeigesetz:

Die – praktisch generelle (Befehls- und Zwangsgewalt) – Zulässigkeit zur Verwendung von erlangten Bild- und Tonaufzeichnungen erscheint insgesamt problematisch. Hier sollten exaktere Vorgaben vorgesehen werden, in welchen Fällen derartige Aufnahmen verwendet werden dürfen, auch wenn ein Einsatz nur „offen“ (dh. für die beteiligten erkennbar) und nicht verdeckt erfolgen muss.

Zu § 53 Abs. 3b Sicherheitspolizeigesetz:

Hier geht es um mögliche Zugriffe auf Telekommunikationsdaten (Mobiltelefone), die ausgeweitet werden soll. Künftig sollen derartige Rückgriffe bzw. Ortungen auch beim „Gefährder“, somit bei einem mutmaßlichen Verdächtigen möglich sein. Dies erscheint insofern problematisch, da derartige Zugriffe ohne richterliche Genehmigung/Kontrolle und auch ohne Genehmigungspflicht des Rechtsschutzbeauftragten erfolgen können.

Zu § 54 Abs. 3, 3a und 5 Sicherheitspolizeigesetz:

Bei dieser Bestimmung geht es um die Möglichkeit, auch Vertrauenspersonen für verdeckte Ermittlungen einzusetzen („...oder durch andere Personen im Auftrag der Sicherheitsbehörden“). Dies erscheint insofern problematisch, da bei „Vertrauenspersonen“ nicht gesichert ist, dass sie immer und zu jeder Zeit die Interessen der Sicherheitsbehörden (und nicht allenfalls eigene Interessen) verfolgen, noch dazu wo diese Personen, welche teilweise selbst zu einem „kriminellen Umfeld“ stammen, vielfach ihre Tätigkeit gegen Belohnung durchführen und des Weiteren auch verdeckte Ermittlungen mittels Bild- und Tonaufzeichnungsgeräten ermöglicht werden soll. Ob die diesbezüglich vorgesehenen Führungs-, Überwachungs- und Dokumentationspflichten zur effektiven Kontrolle der Tätigkeit von (dritten) Vertrauenspersonen ausreichen (§ 54 Abs. 3a), erscheint zumindest fragwürdig bzw. nicht gesichert.

Zusammenfassend erscheint der Gesetzesentwurf zumindest in einigen Bereichen als „zu überschießend“ und nicht verhältnismäßig in Bezug auf die notwendige Abwägung bzw. Balance zwischen möglichen Eingriffen in (verfassungsrechtliche und europarechtliche) Grundrechte und notwendigen Maßnahmen einer effektiven Bekämpfung diverser Bedrohungsszenarien. Daher wäre eine „Nachschärfung“ bzw. Überarbeitung in einigen Punkten erforderlich.

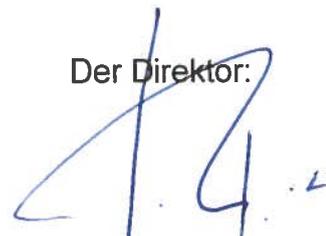
Mit kollegialen Grüßen!

Der Präsident:



(Erwin Zangerl)

Der Direktor:



(Mag. Gerhard Pirchner)