REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.430/0001-DSR/2012
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Inneres

Per E-Mail:
bmi-III-7@bmi.gv.at

Betrifft: Entwurf einer Anordnung der Bundesministerin für Inneres für die Handhabung von optischen oder akustischen Überwachungsmaßnahmen nach § 136 Abs. 1 Z 3 StPO und des automationsunterstützten Datenabgleichs nach § 141 StPO (Geheimschutzordnung – GSchO)

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner 211. Sitzung am 20. Jänner 2012 **einstimmig beschlossen**, zu der im Betreff angeführten Geheimschutzordnung folgende Stellungnahme abzugeben:

1) Allgemeines:

Die Bundesministerin für Inneres hat dem Datenschutzrat den Entwurf einer Geheimschutzordnung für die Handhabung von optischen oder akustischen Überwachungsmaßnahmen nach § 136 Abs. 1 Z 3 StPO und des automationsunterstützten Datenabgleichs nach § 141 StPO übermittelt.

Die Geheimschutzordnung ist als generelle Weisung der Bundesministerin für Inneres gemäß § 55c des Sicherheitspolizeigesetzes (SPG), BGBl. 1991/566, zuletzt geändert durch BGBl. I Nr. 33/2011, nach Anhörung des Datenschutzrates zu erlassen.

Die Bundesministerin für Inneres hat daher den Datenschutzrat ersucht, die Geheimschutzordnung in Behandlung zu nehmen.

2) Hintergrund:

Der Anwendungsbereich der vorgeschlagenen Regelung sind Daten, die bei der „besonderen Ermittlungsmaßnahme“ der optischen und akustischen Überwachung nach § 136 Abs. 1 Z 3 StPO (sog. „Großer Lauschangriff“) und bei der besonderen Ermittlungsmaßnahme des automationsunterstützten Datenabgleichs nach § 141 StPO (sog. „Rasterfahndung“) ermittelt werden.

Bei der vorgeschlagenen Maßnahme handelt es sich um eine allgemeine BMI-interne Weisung. Die Bundesministerin für Inneres ist aufgrund von § 55c Sicherheitspolizeigesetz (SPG) **verpflichtet,** eine solche Weisung zu erlassen und vor ihrer Erlassung den Datenschutzrat anzuhören.

3) Wesentliche datenschutzrechtliche Inhalte des Entwurfs:

Die **derzeit geltende** Geheimschutzordnung des BMI stammt aus dem Jahr 1997.

Gegenüber der derzeit geltenden Fassung der Geheimschutzordnung sieht der nunmehrige Entwurf **nur geringfügige** Änderungen vor.

Großteils handelt es sich um redaktionelle Formulierungsänderungen und eine Überarbeitung im Sinne geschlechtsneutraler Formulierungen sowie Anpassungen der Gesetzeszitate an die geänderte Rechtslage, so zB:

Anpassung der StPO Zitate,
Anpassung der SPG-Zitate,
Anpassung der DSG-Zitate
Anpassung der Zitate der neuen Geheimschutzordnung des Bundes,
und die dazu ergangenen Richtlinien des BMI.

Darüber hinaus sind folgende Änderungen der einzelnen Bestimmungen hervorzuheben, zu denen aus Sicht des Datenschutzrates datenschutzrechtliche Anmerkungen notwendig sind:

§ 1 Abs. 1

Änderung:

- Geltungsbereich wird erweitert auf „alle Bediensteten des BMI und der Sicherheitsbehörden, sowie der Polizeikommanden“ (früher: „Organwalter des BMI und der ihm nachgeordneten Sicherheitsbehörden sowie … Organe des öffentlichen Sicherheitsdienstes, die für die Sicherheitsbehörde Exekutivdienst leisten und für Bedienstete, die Schreibarbeiten, Dolmetscher- oder Übersetzungsdienste leisten“.

Im Lichte des Zwecks der Geheimschutzordnung wäre nach Ansicht des Datenschutzrates der personelle Anwendungsbereich weiter zu fassen:

Die Reichweite der Geheimhaltungspflichten sollte nicht davon abhängig sein, ob eine im Bereich von besonderen Ermittlungsverfahren tätige Person „Bediensteter“ im engeren Sinn ist (man denke an Dolmetscher, die auf Werkvertragsbasis herangezogen werden und nicht „Bedienstete“ sind). Es sollten daher möglichst alle Personen einbezogen werden, die mit der Erfüllung von Aufgaben im Zusammenhang mit optischen Überwachungsmaßnahmen nach § 136 Abs. 1 Z 3 StPO und des automationsunterstützten Datenabgleichs nach § 141 StPO befasst sind.

Weiters wäre festzulegen, dass Personen, die keine Bediensteten sind, sondern auf Auftragsbasis tätig werden, vertraglich zur Einhaltung der Geheimschutzordnung und zur Befolgung entsprechender Weisungen zu verpflichten sind, wobei auch entsprechende Sanktionen zu vereinbaren wären.

§ 3

Änderung:

- Ausweitung des Umfangs der geschützten Informationen auf „Daten“ (somit auch nicht-personenbezogene Daten).
- Anpassung der Gesetzeszitate und Anpassung an die Begrifflichkeit der StPO („besondere Ermittlungsmaßnahmen“ statt dem veralteten Begriff „Überwachungsmaßnahmen“),

Aus Sicht des Datenschutzrates sind diese Änderungen datenschutzrechtlich unbedenklich.

§§ 4, 5

Änderung:

- Anpassung der Verweisungen an die neue Geheimschutzordnung des Bundes

Es ist unklar, in welcher Klassifizierungsstufe die Informationen zu behandeln sind.

Die Geheimschutzordnung des Bundes sieht nämlich 4 Klassifizierungsstufen vor (Eingeschränkt / Vertraulich / Geheim / Streng Geheim). Je nachdem, in welche Klassifizierungsstufe eine Information eingereiht wird, gelten unterschiedlich strenge Regeln hinsichtlich der Garantien, die der eingebundene Personenkreis erfüllen muss.

Der Entwurf sollte daher nach Ansicht des Datenschutzrates dahingehend überarbeitet werden, dass klargestellt wird, mit welcher/welchen Klassifizierungsstufe/n vorgegangen werden soll und welche Anforderungen an die Personen gestellt werden, die Zugang zu den Daten haben.

Darüber hinaus wird darauf hingewiesen, dass auch die Klassifizierung als „vertraulich“, „geheim“ oder „streng geheim“ nach den Regelungen der Geheimschutzordnung des Bundes nicht ausnahmslos zur Folge hat, dass nur sicherheitsüberprüfte Personen Zugang zu den Daten haben, weil die Geheimschutzordnung des Bundes diesbezüglich Ausnahmen erlaubt (§ 6 Abs. 2 der Geheimschutzordnung des Bundes).

Es sollte daher überlegt werden, ob solche Ausnahmen auch im Bereich der Geheimschutzordnung des BMI zulässig sein sollen und gegebenenfalls geregelt werden, auf welche Weise in diesem Fall überprüft wird, ob eine Person vertrauenswürdig ist.

§ 6

Änderung:

- Anpassung der Gesetzeszitate und Anpassung an die Begrifflichkeiten der StPO („besondere Ermittlungsmaßnahmen“ statt dem veralteten Begriff „Überwachungsmaßnahmen“).

Aus Sicht des Datenschutzrates ist diese Änderung datenschutzrechtlich unbedenklich.

§ 7

Änderung:

- Verwendung des Begriffs „Zugriffsberechtigung“ statt „Zugriffsermächtigung“,
- Entfall der Aufzählung jener Organe, denen eine Zugriffsberechtigung erteilt werden kann; stattdessen Regelung der Erteilung einer Berechtigung an „Bedienstete gemäß § 1 Abs. 1 sowie vom zuständigen Gericht zur technischen Durchführung … bestellten Dolmetschern oder Sachverständigen“.
- Ergänzung durch eine Regelung, wonach (auch) der Rechtsschutzbeauftragte gemäß § 47a StPO zur Einsicht berechtigt ist.

§ 7 möchte sicherstellen, dass nur ein eingeschränkter, im Vorhinein definierter und feststehender Personenkreis Zugang zu den im Rahmen besonderer Ermittlungsmaßnahmen ermittelten Daten hat.

Die Regelung ist vor dem Hintergrund zu sehen, dass Personen, die Zugang zu Daten haben sollen, die im Rahmen eines sog. „großen Lauschangriffs“ ermittelt werden („Überwachungsmaßnahmen nach § 136 Abs. 1 Z 3 StPO“), gemäß § 55a SPG einer „Sicherheitsüberprüfung“ unterzogen werden müssen. Dadurch will der Gesetzgeber gewährleisten, dass solche Personen hinreichend vertrauenswürdig sind).

Allerdings sieht hinsichtlich der Personen, die „nur“ mit automationsunterstützten Datenabgleichen befasst sind (sog. „Rasterfahndung“, § 141 StPO) das SPG keine verpflichtende

Sicherheitsüberprüfung vor.

Die vorgeschlagene Regelung ist daher hinsichtlich des automationsunterstützten Datenabgleichs lückenhaft, weil keine gesetzliche Pflicht zur Sicherheitsüberprüfung besteht.

Es ist daher nach Ansicht des Datenschutzrates in dieser Geheimschutzordnung – unabhängig von einer allfälligen Novellierung des SPG – klarzustellen, wie die Vertrauenswürdigkeit aller Zugangsberechtigten kontrolliert bzw. gewährleistet wird.

Weiters wäre es sinnvoll, eine Regelung darüber aufzunehmen, dass/wie **durch technische Mittel** (Schlüssel, Geräte, verschlossene Räume) sicherzustellen ist, dass nur die Zugriffsberechtigten faktischen Zugang zu den im Rahmen besonderer Ermittlungsmaßnahmen ermittelten Informationen/Akten erhalten.

Weiters wäre festzulegen, **zu welchem Zweck** die Dokumentation der Zugriffsberechtigungen erfolgt und wer in diese Dokumentation Einsicht nehmen darf.

§ 8
Änderung:
Ersatz des Begriffs „Belehrung“ durch das Wort „Information“.

Der Entfall des in der aktuellen Fassung der Geheimschutzordnung verwendeten Wortes „Belehrung“ mag aus Sicht des Ressorts bestimmte Gründe haben. Dennoch ist fraglich, ob es zweckmäßig ist, diesen Begriff durch den Begriff „Information“ zu ersetzen. **Es wäre nämlich anzustreben, dass in der Regelung nicht nur der bloße Informationscharakter zum Ausdruck kommt, sondern auch, dass es sich um eine Unterweisung handelt, dass dem Betroffenen also gleichzeitig mit der Information – hinreichend eindringlich – die Pflicht zur Befolgung der in den Geheimhaltungsvorschriften aufgestellten Regeln verdeutlicht wird.**

Der Datenschutzrat regt daher an, den Begriff „Belehrung“ beizubehalten.

§ 9

Keine inhaltliche Änderung.

§ 10

Änderung:

- (Abs. 1 und 2): Ersatz der Begriffe „Protokollierung/Verschlussprotokoll“ mit dem Begriff „Registrierung“.
- Bloße Anpassung der Verweisung auf die Geheimschutzordnung des Bundes.

Aus Sicht des Datenschutzrates ist diese Änderung zwar datenschutzrechtlich unbedenklich, entspricht jedoch nicht der datenschutzrechtlichen Terminologie des Datenschutzgesetzes (Ersatz der Formulierung „Protokollierung“ durch „Registrierung“).

Aus Sicht des Datenschutzrates ist es **im Sinne der Einheitlichkeit der Rechtsordnung** und im Sinne der Verständlichkeit von Rechtsvorschriften **vorzuziehen**, wenn der Entwurf den Begriff der **„Protokollierung“ beibehalten würde**. Dieser Begriff ist nämlich auch jener, den das Datenschutzgesetz (§ 14 Abs. 2 Z 7 DSG 2000) verwendet.

Weiters ist unklar, **was** im Zusammenhang mit den einzelnen Datenverwendungsschritten zu protokollieren ist: Es ist nicht ausreichend, wenn die Ermittlung, Vervielfältigung, Überlassung, etc. als solche protokolliert wird, sondern es muss auch festgehalten sein, welche **Person**, zu welcher **Zeit** welchen **Vorgang** gesetzt hat. Aus der Geheimschutzordnung des Bundes, auf die in § 10 Abs. 2 verwiesen wird, ergeben sich derartige Dokumentationspflichten nämlich nur zum Teil, beziehungsweise abhängig von der jeweiligen Klassifizierungsstufe.

Der Datenschutzrat empfiehlt daher, die Geheimschutzordnung des BMI in diesem Punkt präziser und umfassender auszugestalten.

Schließlich ist noch festzulegen, **zu welchem Zweck** die Protokollierung erfolgt und wer in die protokollierten Daten Einsicht nehmen darf.

§ 11

Änderung:

- Bloße Anpassung der Verweisung auf die Geheimschutzordnung des Bundes.

Aus Sicht des Datenschutzrates ist diese Änderung datenschutzrechtlich unbedenklich.

§ 12

Änderung:

- Abs. 1 Keine inhaltliche Änderung
- Abs. 2 Keine inhaltliche Änderung
- Abs. 3 Verwendung von „registrieren“ statt „protokollieren“
- Abs. 4 Keine inhaltliche Änderung

Zu den vorgeschlagenen Änderungen ist ein grundsätzliches Problem aufzuzeigen, das schon in der geltenden Geheimschutzordnung bestand:

In Abs. 3 ist angeordnet, dass die Vervielfältigung in einer speziellen Weise zu vermerken ist. **Diese Regelung lässt sich aber auf Datenträger nicht ohne weiteres anwenden. Eine besondere Regelung für elektronische Datenträger ist nach Ansicht des Datenschutzrates erforderlich, damit das gleiche Schutzniveau und der gleiche Dokumentationseffekt auch für elektronische Medien sichergestellt wird.**

§ 13

Änderung:

- Verwendung des Begriffs „Transport“ statt „Beförderung“.
- Verwendung der Formulierung „Datenträger, auf dem Informationen **festgehalten sind**…“ statt „… gespeichert sind“.
- Anpassung der Verweisung (auf Geheimschutzordnung des Bundes). Allerdings **Entfall der Festlegung auf eine bestimmte Klassifizierungsstufe**.

Die vorgeschlagene Regelung verweist hinsichtlich der beim „Transport“ von

Informationen zu beachtenden Maßnahmen generell auf die Geheimschutzordnung des Bundes. **Durch den vorgeschlagenen Entfall der Festlegung auf eine bestimmte Klassifizierungsstufe ist es vollkommen unklar, welche Regelungen der Geheimschutzordnung des Bundes nunmehr zur Anwendung kommen sollen.**

Gerade vor dem Hintergrund, dass die vorgeschlagene Regelung für einen ganz spezifischen Bereich gelten soll (nämlich Observationsmaßnahmen und automatisierter Datenabgleich im Rahmen der Kriminalpolizei) wäre es notwendig, die einzuhaltenden Prozesse **maßgeschneidert und genau** festzulegen und nicht bloß allgemein auf die generelle Geheimschutzordnung des Bundes zu verweisen. So sollte aus Sicht des Datenschutzrates festgehalten werden, welche Dokumentationspflichten bestehen (Empfangsbestätigungen?), welche Übermittlungsmodalitäten zu wählen sind (Post? Boten? Persönliche Übergabe?)und auf welche Weise sich der Übermittelnde von der Identität und Vertrauenswürdigkeit der Empfängers im Vorhinein zu überzeugen hat, etc.

§ 14

Änderung:

- Verwendung des Begriffs „Datenweitergabe“ statt „Übermittlung“
- Legistische Umstellung der Systematik: Entfall des Abs. 1 (Vorschrift, dass „Übermittlungen“ von Informationen nur dann stattfinden dürfen, wenn „dies gesetzlich vorgesehen ist“) und Aufnahme der diesbezüglichen Vorschrift in den ersten Satz des Abs. 2.
- Entfall der in Abs. 2 enthaltenen Protokollierungspflichten (offenbar im Hinblick darauf, dass sich die entsprechende Verpflichtung generell zwingend aus § 10 ergeben soll).

Dazu ist aus Sicht des Datenschutzrates anzumerken, dass durch die vorgeschlagene Änderung der Mehrwert der bisherigen Regelung verloren ginge (nämlich, dass auch Übermittlungsempfänger, Zweck, Datum, Art, Genehmigung und Übermittler zu dokumentieren sind).

Die Regelung ist in diesem Sinne zu überdenken, wobei diese Überarbeitung auch

generell im Rahmen einer genaueren Festlegung der Dokumentationspflichten im Rahmen des § 10 (siehe die diesbezüglichen Anmerkungen oben) erfolgen könnte.

§ 14 Abs. 2 ordnet an, dass „Datenübermittlungen“ nur nach Maßgabe des Gesetzes und über Anordnung der zuständigen Staatsanwaltschaft zulässig sind. In diesem Zusammenhang wäre ausdrücklich klarzustellen, dass diese Beschränkung nicht nur für die Übermittlung der Daten an Außenstehende, sondern auch dann gilt, wenn die Daten innerhalb der Sicherheitsbehörde und durch **Änderung des Zwecks der Verwendung der Daten** (anderes Aufgabengebiet des Auftraggebers vgl. § 4 Z 12 DSG 2000), stattfinden soll: **Auch die Zweckänderung** darf nur unter der Voraussetzung stattfinden, **dass diese gesetzlich vorgesehen ist und von der Staatsanwaltschaft genehmigt wurde.**

§ 15

Abs 1 keine Änderung

Abs 2 „Menschen“ statt „Personen“, geschlechtsneutrale Bezeichungen

Abs. 3-5 keine Änderungen

Aus Sicht des Datenschutzrates sind diese Änderungen datenschutzrechtlich unbedenklich.

§ 16

Änderung:

Abs. 1 und 3 keine inhaltliche Änderung, außer der Umstellung vom Wort „protokollieren“ auf „registrieren“.

Abs. 2 Umstellung der Formulierung: Entfall der Verpflichtung zur Löschung/Vernichtung der Daten „**sobald sie für die Erfüllung der Aufgabe nicht mehr benötigt werden**“, stattdessen Regelung, wonach die Vernichtung zu erfolgen hat, wenn dies „die StA oder das Gericht anordnet“, es sei denn, für die Weiterverwendung bestehen besondere gesetzliche Regelungen.

Hinsichtlich der Begriffsauslegung wird auf die Ausführungen zu § 10 des Entwurfes verwiesen. Nach Ansicht des Datenschutzrates darf bei der Löschung/Vernichtung der Daten nicht solange zugewartet werden, bis die

Staatsanwaltschaft/das Gericht aktiv eine dahingehende Anordnung trifft. Es sollte auch eine Löschungspflicht für den Fall geben, dass die Staatsanwaltschaft (das Gericht) in dieser Hinsicht passiv bleibt. Eine Löschungsverpflichtung der Daten sollte jedenfalls nach Ablauf der Verjährungsfrist vorgesehen werden.

§ 17 (Regelung zum Geheimschutzbeauftragten)

Die Aufgaben des/der Geheimschutzbeauftragten sind im Wesentlichen unverändert geblieben.

Im Sinne der Effektivität des Rechtsschutzes der in ihren Rechten allenfalls betroffenen Personen wäre es empfehlenswert, wenn der/die Geheimschutzbeauftragte nicht nur Veranlassungen im Sinne von § 15 Abs. 4 zu treffen hat, sondern auch verpflichtet wird, das Auftauchen allfälliger Datensicherheitsrisiken oder das Bekanntwerden von Umständen, die auf einen allfälligen Bruch von Datensicherheitsvorschriften hinweisen, anlassbezogen dem Rechtsschutzbeauftragten (im Sinne der StPO) mitzuteilen, da nur so gewährleistet werden kann, dass die Rechte der in ihrem Grundrecht auf Datenschutz betroffenen Personen in effektiver Weise wahrgenommen werden können.

Unklar ist nach Ansicht des Datenschutzrates weiterhin, welche Untersuchungs-, Sanktions- und Reaktionsmöglichkeiten der Geheimschutzbeauftragte besitzt. Dies wäre aber konkret gesetzlich zu regeln.

25. Jänner 2012
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt