

## Vorblatt

### **Problem:**

Der vorliegende Gesetzesentwurf stellt das Anschlussstück zur Novelle des Telekommunikationsgesetzes 2003 – TKG 2003 in Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. Nr. L 105 vom 13.4.2006 S. 54, dar.

### **Ziele und Grundzüge des Vorhabens:**

Der vorliegende Entwurf verfolgt das Ziel, die notwendigen Anpassungen der Strafprozessordnung und des Sicherheitspolizeigesetzes an die Änderungen des Telekommunikationsgesetzes vorzunehmen.

Ziel ist es, einerseits die Zulässigkeit von Ersuchen um Übermittlung von Stammdaten, einer Anordnung über die Auskunft von Stamm- und Zugangsdaten und der Auskunft über Vorratsdaten für Strafverfolgungsbehörden und andererseits von Anfragen an Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten oder öffentlichen Kommunikationsnetzen im Sicherheitspolizeigesetz sowie die weitere Verwendung der so ermittelten Daten an die Vorgaben des neuen § 99 Absatz 5 TKG zu normieren.

### **Alternativen der Problemlösungen:**

Keine.

### **Finanzielle Auswirkungen:**

Durch die Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten ist von einem nicht linearen Anstieg der Kosten zufolge Anordnungen und gerichtlichen Bewilligungen von Überwachungsmaßnahmen im Ausmaß von 30 % auszugehen. Bisher war den Strafverfolgungsbehörden der Zugriff auf historische Zugangsdaten bzw. E-Maildaten möglich, sofern die Daten zu Verrechnungszwecken noch gespeichert waren. Nun wird im Telekommunikationsgesetz eine davon unabhängige Speicherverpflichtung normiert. Es wird daher erwartet, dass die Anzahl der kostenersatzpflichtigen Mitwirkung von Anbietern an Überwachungsmaßnahmen entsprechend steigen wird.

Da der vorliegende Gesetzesentwurf jedoch ein Anschlussstück zur Novelle des Telekommunikationsgesetzes 2003 – TKG 2003 darstellt, ergeben sich finanzielle Auswirkungen insbesondere durch die Umsetzung und Vollziehung des Telekommunikationsgesetzes. Ergänzend wird daher auf die Ausführungen zu diesem Entwurf verwiesen.

Durch die Erweiterung des kommissarischen Rechtsschutzes auf die Fälle der Information Betroffener (§ 53 Abs. 3c) und den Einsatz technischer Mittel zur Lokalisierung einer Endeinrichtung (§ 53 Abs. 3b) sind geringfügige Mehrkosten zu erwarten.

### **Wirtschaftspolitische Auswirkungen:**

Keine.

### **Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:**

Keine.

### **Auswirkungen auf die Verwaltungslasten für Unternehmen:**

Keine.

### **Auswirkungen auf die Verwaltungslasten für Bürger:**

Keine.

### **Auswirkungen in umweltpolitischer, konsumentenschutzpolitischer sowie sozialer Hinsicht:**

Keine.

### **Geschlechtsspezifische Auswirkungen:**

Keine.

### **Verhältnis zu Rechtsvorschriften der Europäischen Union:**

Die Änderungen des TKG 2003 dienen der Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher

Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG. Um auch den Zugriff auf danach zu speichernde Vorratsdaten zur Verfolgung schwerer Straftaten zu regeln, sind die entsprechenden Rechtsgrundlagen in der StPO und im SPG zu schaffen.

**Kompetenzgrundlage:**

Die Kompetenz des Bundes zur Gesetzgebung stützt sich auf Art. 10 Abs. 1 Z 6 und 7 B-VG.

**Besonderheiten des Normerzeugungsverfahrens:**

Keine.

**Besonderheiten des Normerzeugungsverfahrens:**

Keine.

**Aspekte der Deregulierung:**

Keine.

## **Erläuterungen**

### **Allgemeiner Teil**

#### **Zu Artikel 1 Änderung der Strafprozessordnung 1975**

Die Änderungen der Strafprozessordnung sind Folge der geänderten Bestimmungen des Telekommunikationsgesetzes – TKG 2003. Sie zielen darauf ab, die Zulässigkeit von Ersuchen um Stammdatenübermittlung, der Anordnung über die Auskunft von Stamm- und Zugangsdaten, sowie die Auskunft über Vorratsdaten zu normieren.

#### **Zu Artikel 2 Änderung des Sicherheitspolizeigesetzes**

Ziel der Änderungen im Sicherheitspolizeigesetz ist es, die Zulässigkeit der Anfragen an Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten oder öffentlichen Kommunikationsnetzen auf Basis des Sicherheitspolizeirechtes sowie die weitere Verwendung der so ermittelten Daten zu regeln und an die Vorgaben der (neuen) Bestimmungen des Telekommunikationsgesetzes (TKG) anzupassen.

Für die Sicherheitsbehörden wird die Beauskunftung der Verkehrs- bzw. Zugangsdaten im Sinne des § 99 Abs. 5 TKG im adaptierten § 53 Abs. 3a und 3b SPG geregelt. Zugleich wird aber auch durch einen neuen § 53 Abs. 3c SPG die Verpflichtung der Sicherheitsbehörden zur nachweislichen Information Betroffener bei Standortbeauskunftungen und Beauskunftungen über Zuordnungen des Namens oder der Anschrift eines Betroffenen zu einer IP-Adresse, in beiden Fällen wenn hierfür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 oder 4 iVm § 102a TKG 2003 durch den Betreiber erforderlich war, eingeführt, deren Einhaltung der Prüfung durch den Rechtsschutzbeauftragten nach der ebenfalls ergänzten Bestimmung des § 91c SPG unterliegt. Ebenso ergänzt wird in § 91c Abs. 1 die Informationspflicht über den Einsatz technischer Mittel zur Lokalisierung einer Endeinrichtung (§ 53 Abs. 3b).

Im Rahmen dieser Anpassungen wird auch die Prüfpflicht des Rechtsschutzbeauftragten für Meldungen nach § 91c Abs.1 SPG und die Verpflichtung des Rechtsschutzbeauftragten zur Information Betroffener oder zur Erhebung einer Beschwerde an die Datenschutzkommission bei einer Rechtsverletzung durch die Verwendung personenbezogener Daten klargestellt.

## Besonderer Teil

### Zu Art. 1 (Änderungen der Strafprozessordnung 1975)

#### Zu Z 1 (§ 76a StPO):

Die vorgeschlagene Regelung soll die korrespondierende Bestimmung zu § 90 Abs. 7 TKG darstellen und die Erteilung einer Auskunft über Stammdaten auf Grund von Ersuchen der Gerichte, Staatsanwaltschaften und der Kriminalpolizei einer Rechtsgrundlage in der StPO zuführen und damit den unklaren Bedeutungsinhalt der bisherigen Bestimmung des § 103 Abs. 4 TKG klarstellen. Die Auskunft über die genannte Datenkategorie soll erteilt werden, wenn diese zur Aufklärung des konkreten Verdachts einer Straftat (siehe dazu auch die Definition des Beschuldigtenbegriffs in § 48 Abs. 1 Z 1 StPO) erforderlich ist (§ 90 Abs. 7 TKG und § 76a Abs. 1 StPO).

Die Regelung des Abs. 2 soll daran anknüpfen und solche Zugangsdaten erfassen, zu deren Auskunft der Betreiber Verkehrsdaten verarbeiten muss (§ 99 Abs. 5 Z 2 TKG; im Wesentlichen die Zuordnung einer bekannten dynamischen IP-Adresse). Von Bedeutung ist hierfür zum einen, dass die Strafverfolgungsbehörden durch eine solche Auskunft selbst keine Kenntnis der vorsorglich zu speichernden Daten erhalten. Die Staatsanwaltschaft ruft im Rahmen einer solchen Auskunftsanordnung nicht Verkehrsdaten selbst ab, sondern erhält lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses, der von den Anbietern unter Rückgriff auf diese Daten ermittelt wurde. Dabei bleibt die Aussagekraft dieser Daten eng begrenzt: Die Verwendung der vorsorglich gespeicherten Daten führt allein zu der Auskunft, welcher Anschlussinhaber unter einer bereits bekannten, etwa anderweitig ermittelten IP-Adresse im Internet angemeldet war. Im Unterschied zu der in § 135 Abs. 2 StPO geregelten Auskunft über Daten einer Nachrichtenübermittlung wird für solche Auskünfte nur ein von vornherein feststehender kleiner Ausschnitt der Daten verwendet. Den Anforderungen nach einer besonderen Beachtung des Verhältnismäßigkeitsgrundsatzes (§ 5 StPO) soll durch den Verweis auf die Bestimmung des § 102 StPO entsprochen werden; danach muss die Anordnung schriftlich ergehen und nicht nur die Verdachtslage sondern auch die Verhältnismäßigkeit begründen (siehe § 102 Abs. 2 Z 2 und 3 StPO).

Nach § 6 Abs. 2 StPO hat jede von der Ausübung von Zwangsmaßnahmen betroffene Person das Recht auf angemessenes rechtliches Gehör und auf Information über Anlass und Zweck der sie betreffenden Verfahrenshandlung sowie über ihre wesentlichen Rechte im Verfahren; die Einhaltung dieser Bestimmung ist sowohl von der Staatsanwaltschaft als auch von der Kriminalpolizei zu gewährleisten. Die Anordnung der Staatsanwaltschaft ist den Betroffenen zuzustellen, die sodann ihre Rechte auf Einsicht in die Ergebnisse und Löschung der gewonnenen Daten geltend machen können (§§ 138 Abs. 5, 139 StPO). Rechtsschutz ist dadurch gewährleistet, dass gegen solche Anordnungen der Staatsanwaltschaften der Einspruch wegen Rechtsverletzung nach § 106 Abs. 1 Z 2 StPO zusteht, über den das Gericht zu entscheiden hat. Der Umstand, dass nach dem Wortlaut des § 107 Abs. 1 StPO ein Einspruch nach Beendigung des Ermittlungsverfahren nicht mehr zusteht, schadet in diesem Zusammenhang deshalb nicht, weil nach der Rechtsprechung des Obersten Gerichtshofes nach Ausschöpfung des durch § 107 Abs 3 erster Satz StPO eröffneten Instanzenzugs bei ihm geltend gemacht werden könne, dass die Anerkennung und der allenfalls mögliche Ausgleich einer durch die Staatsanwaltschaft geschehenen Grundrechtsverletzung unterblieben ist (vgl. 14 Os 60/09v). Durch Anträge auf Erneuerung des Strafverfahrens (§ 363a StPO) können somit Betroffene Grundrechtsschutz beim Obersten Gerichtshof erlangen. Damit werden nicht nur Beschuldigte in ihren Grundrechten geschützt. Der Erneuerungsantrag dient auch dem Grundrechtsschutz Dritter (vgl. 13 Os 130/10g, 13 Os 136/10i). In diesem Sinn hat der Oberste Gerichtshof auch ausdrücklich festgehalten, dass ein Erneuerungsantrag des Beschuldigten auch in einem bereits eingestellten Ermittlungsverfahren zulässig ist (vgl. den Praxishinweis zu 14 Os 25/09x, EvBl-LS 2009/104, 618). Auch nach 13 Os 16/09s bringt schon die weite Umschreibung des möglichen Prüfungsgegenstands zum Ausdruck, dass diese Erneuerungskompetenz nicht auf in rechtskräftig abgeschlossenen Strafverfahren ergangene (End-)Entscheidungen beschränkt ist. Vielmehr sieht sich der OGH aufgerufen, als – nicht an völkerrechtliche Beschränkungen als Ausdruck staatlicher Souveränität gebundene – oberste Instanz in Strafrechtssachen (Art. 92 Abs. 1 B-VG) über die Einhaltung von Grundrechten in Strafverfahren zu wachen und dabei nicht bloß die Rechtsprechung des EGMR nachzuvollziehen, sondern erforderlichenfalls selbst Akzente ihrer Weiterbildung zu setzen.

Darüber hinaus hat die Bundesregierung im Verfahren vor dem VfGH, G 22/10 (siehe BGBl. I Nr 1/2011) die Möglichkeit einer verfassungskonforme Interpretation vorgestellt. Es fällt nämlich auf, dass die gegenüber der RV 25 BlgNR 22. GP im Justizausschuss vorgenommenen Änderungen ausschließlich wie folgt begründet wurden (siehe AB 406 BlgNR 22. GP, S. 16): „Im § 107 Abs. 1 soll klargestellt

*werden, dass Einsprüche wegen der Verweigerung von Verfahrensrechten (Akteneinsicht oder Beweisanträge) nicht mehr zu behandeln sind, wenn bereits das Hauptverfahren eröffnet wurde, in dem der Betroffene ohnehin seine Rechte neuerlich geltend machen kann. Einsprüche gegen die Anwendung unmittelbaren Zwangs sollen zur Vermeidung einer Vorbesatztheit und damit Befangenheit des Gerichts des Hauptverfahrens noch von dem Gericht entschieden werden, das im Ermittlungsverfahren zuständig wäre.“*

Das lässt den Schluss zu, dass der Gesetzgeber bloß vom Fall der Beendigung des Ermittlungsverfahrens durch Einbringen der Anklage ausging, hingegen für den Fall der Einstellung (nach den §§ 190 bis 192 StPO) eine planwidrige Lücke vorliegt, die jedenfalls für den Bereich der Rechtsverletzung (§ 106 Abs. 1 Z 2 StPO) – verfassungskonform – im Wege der Analogie zu schließen wäre. Die Staatsanwaltschaft bzw. das Gericht, das im Ermittlungsverfahren zuständig wäre, hätte daher auch über solche Einsprüche noch zu entscheiden (dafür spricht auch der Wortlaut des § 106 Abs. 4 StPO, der ja die Staatsanwaltschaft in jedem Fall verpflichtet zu prüfen, ob die behauptete Rechtsverletzung vorliegt, während sich § 107 Abs. 1 StPO seinem Wortlaut nach ausschließlich an das Gericht wendet). Damit im Einklang hat die Rechtsprechung des Obersten Gerichtshofs den Anwendungsbereich des § 106 Abs. 1 Z 2 StPO per analogiam erweitert (siehe 14 Os 108/08a; 13 Os 122/08b).

Im Zuge der auf Grund des Erkenntnisses des VfGH vom 16. Dezember 2010, G 259/09 u.a. (BGBl. I Nr. 1/2011), notwendigen Erneuerung des Rechtsschutzes im Ermittlungsverfahren wird auf diesem Gebiet auch eine ausdrückliche gesetzliche Klarstellung und Präzisierung in Aussicht genommen. Jedenfalls soll gesetzlich klargestellt werden, dass zur Sicherung sonst allenfalls nicht im Wege der §§ 106 f StPO gegebenen Rechtsschutzes Einsprüche wegen Rechtsverletzung im gegebenen Zusammenhang auch nach Beendigung eines Ermittlungsverfahrens durch Einstellung möglich sind.

**Zu Z 2 und 3 (Überschrift des 5. Abschnittes und § 134 StPO):**

In dieser Definition soll der Bedeutungsinhalt der „Auskunft über Vorratsdaten“ korrespondierend zur Bestimmung über die Speicherverpflichtung für die Anbieter nach § 102a Abs. 2 bis Abs. 4 TKG in der Fassung des Entwurfs aufgenommen und von den sonstigen Auskünften über Daten einer Nachrichtenübermittlung auch deutlich abgegrenzt werden. Daraus ergibt sich aber auch, dass eine Auskunft über Vorratsdaten nicht vorliegt, wenn auf solche Verkehrsdaten zugegriffen werden soll, die von den Anbietern zu Zwecken der Verrechnung gemäß § 99 Abs. 2 TKG gespeichert werden. Die sogenannten „Verrechnungsdaten“ unterliegen auch weiterhin der Auskunft über Daten einer Nachrichtenübermittlung nach § 134 Z 2 StPO.

Die vorgeschlagene Erweiterung der Definition „Ergebnis“ in § 134 Z 5 StPO ist Folge der Einführung der „Auskunft über Vorratsdaten“ in § 134 Z 2a StPO.

**Zu Z 4 (§ 135 StPO):**

§ 99 Abs. 5 Z 1 TKG in der Fassung des Entwurfs stellt klar, dass Strafverfolgungsbehörden wie bisher auf sogenannte „Verrechnungsdaten“ im Rahmen einer Auskunft über Daten einer Nachrichtenübermittlung (§ 135 Abs. 2 StPO) zugreifen können.

Entsprechend der höheren grundrechtlichen Eingriffsintensität der verdachtsunabhängigen Speicherung von Verkehrsdaten nach § 102a TKG soll die Auskunft über Vorratsdaten grundsätzlich nur unter den Bedingungen der Auskunft über Daten einer Nachrichtenübermittlung erteilt werden (§ 135 Abs. 2a StPO), wodurch auch das Erfordernis einer gerichtlichen Bewilligung hervorgehoben wird. Es erschiene schlechterdings unverständlich, wenn etwa im Fall des § 107a Abs. 2 Z 2 StGB („Cyber-Stalking“) selbst mit Einverständnis des Nutzers des Anschlusses nicht auf Vorratsdaten zurückgegriffen werden könnte. Ähnliches gilt für das Verschaffen einer kinderpornographischen Darstellung einer mündigen minderjährigen Person (§ 207a Abs. 3 erster Fall StGB).

Aus Anlass der gegenständlichen Novellierung soll auch die Zulässigkeit einer Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z 2 StPO) für den Fall klargestellt werden, dass der Aufenthalt einer flüchtigen oder abwesenden Person, die verdächtig ist, eine mit mehr als einjähriger Freiheitsstrafe bedrohte strafbare Handlung begangen zu haben, ermittelt werden kann (siehe so auch bei der Überwachung des Inhalts gemäß § 135 Abs. 3 Z 4 StPO).

**Zu Z 5 bis Z 9 (§§ 137, 138 Abs. 1, 2 und 5, 140 Abs. 1 Z 4, 144 Abs. 3 und 145 Abs. 3 StPO):**

Da es sich bei Vorratsdaten um historische Daten handelt soll klargestellt werden, dass die Auskunft über Vorratsdaten für einen vergangenen Zeitraum anzuordnen ist (§ 137 StPO). Darüber hinaus sollen in den erwähnten Bestimmungen die erforderlichen Zitatpassungen vorgenommen werden (jeweils Erweiterung um die Auskunft über Vorratsdaten gemäß § 135 Abs. 2a StPO).

**Zu Z 10 (§ 147 StPO):**

Die Regelung schlägt vor, dem Rechtsschutzbeauftragten die Kontrolle von Anordnungen und Bewilligungen und Durchführung von Auskünften über Vorratsdaten zu übertragen, wodurch ein zusätzliches Kontrollelement einbezogen wird, was auch die effektive Wahrnehmung des Schutzes von Berufsheimnisträgern (§ 157 Abs. 1 Z 2 bis 4) systemgerecht gewährleistet.

**Zu Z 11 (§ 381 Abs. 1 Z 5):**

Im Bereich des Kostenersatzes sollen auch die für eine Auskunft über Vorratsdaten aufgelaufenen Kosten zum Ersatz aufgetragen werden können, soweit das Ergebnis dieser Ermittlungsmaßnahme auch tatsächlich einen „Erfolg“ nach sich gezogen hat (erheblichen Beitrag zur Aufklärung der Tat).

**Zu Art. 2 (Änderungen des Sicherheitspolizeigesetzes)**

**Zu Z 1 (§ 53 Abs. 3a, 3b und 3c)**

Im Sinne einer transparenten Darstellung der unterschiedlichen Auskunftersuchen und der Voraussetzungen, unter denen die jeweilige Beauskunftung zulässig ist, wird § 53 Abs. 3a in vier Ziffern untergliedert. Dabei wird der Aufgabenbezug für jede Ziffer gesondert hergestellt und die bisherige Formulierung „wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen“ konkretisiert.

§ 53 Abs. 3a Z 1 regelt wie bisher die Stammdatenabfrage im Bereich der Telefonie. Diese Auskünfte sollen für jede Art der Aufgabenerfüllung nach dem SPG zulässig sein.

§ 53 Abs. 3a Z 2 und 3 sind aus der geltenden Rechtslage übernommen und beziehen sich auf IP-Adressen. Beide Beauskunftungen nehmen auf konkrete sicherheitspolizeiliche Aufgabenstellungen Bezug. Voraussetzung für die Zulässigkeit der Datenermittlung bei den Anbietern ist jeweils, dass eine „konkrete Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht vorliegt, oder die Sicherheitsbehörden das Datum „zur Abwehr allgemeiner Gefahren (§ 16) benötigen.

Eine allgemeine Gefahr besteht gemäß § 16 bei einem gefährlichen Angriff und bei einer kriminellen Verbindung. Für die Erfüllung dieser sicherheitspolizeilichen Kernaufgabe ist die Auskunftserteilung zu IP-Adressen jedenfalls erforderlich, weil eine Identifizierung von Benutzern oftmals anders nicht möglich ist.

§ 53 Abs. 3b wird an § 99 Abs. 5 Z 3 TKG angepasst und nimmt nunmehr Bezug auf die historischen Standortdaten, die als Vorratsdaten gespeichert werden. Die Verantwortung der rechtlichen Zulässigkeit von Auskunftsbegehren nach Abs. 3a und 3b obliegt den Sicherheitsbehörden. Dies umfasst auch eine entsprechende schriftliche Dokumentation, welche dem Betreiber im Falle des Abs. 3b unverzüglich, spätestens innerhalb von 24 Stunden nachzureichen ist.

Des Weiteren ist die Sicherheitsbehörde umgehend verpflichtet, den Betroffenen nachweislich und ehestmöglich unter Angabe von Rechtsgrundlage, Datum und Uhrzeit über eine erfolgte Standortdatenbeauskunftung und über eine Beauskunftung zu Name und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, wenn hierfür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 oder 4 iVm § 102a TKG 2003 durch den Betreiber erforderlich war, zu informieren. Die Verständigung kann dabei mündlich vor Ort (bei erfolgter Hilfeleistung), per SMS oder schriftlich erfolgen und ist entsprechend zu dokumentieren.

Die Information kann aufgeschoben werden, solange durch der Ermittlungszweck durch sie gefährdet wäre bzw. kann unterbleiben, wenn der Betroffene bereits nachweislich von der Auskunftserteilung Kenntnis erlangt hat. In den Fällen, wo eine Kenntnisnahme durch den Betroffenen auf Grund dessen Ablebens oder Abgängigkeit nachweislich nicht möglich ist, hat eine Verständigung durch die Sicherheitsbehörden zu unterbleiben.

Die Behörde ist verpflichtet, den Rechtsschutzbeauftragten über das Unterbleiben (auch im Ablebens- oder Abgängigkeitsfall des Betroffenen) bzw. einen allfälligen Aufschub der Information des Betroffenen und die dafür geltend gemachten Gründe ehestmöglich in Kenntnis zu setzen.

**Zu Z 2 (§ 53 Abs. 3d)**

Bisheriger Absatz 3c erhält die neue Absatzbezeichnung (3d).

**Zu Z 3 bis 5 (§ 91c Abs. 1 und 3 und § 91d Abs. 3)**

Zur Absicherung des Informationsrechts Betroffener nach § 53 Abs. 3c ist neben der Meldung der Standortbeauskunftung und Beauskunftungen über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn hierfür die Verwendung von Vorratsdaten

gemäß § 99 Abs. 5 Z 3 oder 4 iVm § 102a TKG 2003 erforderlich war, auch die erfolgte Verständigung des Betroffenen bzw. deren Unterbleiben oder deren Aufschiebung ehestmöglich an den Rechtsschutzbeauftragten zu melden. Dem Rechtsschutzbeauftragten obliegt somit die Überprüfung der Information, insbesondere der für das Unterbleiben oder den Aufschiebung geltend gemachten Gründe.

Über Anregung des Rechtsschutzbeauftragten wird eine Bestimmung aufgenommen, dass die Verwendung von technischen Mitteln zur Lokalisierung einer Endeinrichtung im Rahmen einer Standortbestimmung nach § 53 Abs. 3b in der Meldung nach § 91c gesondert auszuweisen ist.

Im Rahmen dieser Anpassungen wird sowohl die Prüfpflicht des Rechtsschutzbeauftragten für die Meldungen nach § 91c Abs. 1 SPG als auch die Informationspflicht oder Pflicht zur Erhebung einer Beschwerde bei der DSK im Falle einer wahrgenommenen Rechtsverletzung klargestellt (siehe dazu auch *Vogl, Der Rechtsschutzbeauftragte in Österreich, 2004*).

**Zu Z 6 (§ 94 Abs. 30)**

Es handelt sich um die Inkrafttretensbestimmung.