

Vorblatt

**Probleme und Ziele:**

Der vorliegende Entwurf bezweckt die Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten in die innerstaatliche Rechtsordnung.

**Inhalt:**

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.

Insbesondere werden

- die Begriffsbestimmungen an jene der Richtlinie 2006/24/EG angepasst,
- Anbieter zur Vorratsspeicherung von Daten für sechs Monate verpflichtet,
- die zu speichernden Daten taxativ aufgezählt,
- Anbieter zur Löschung der Daten nach Fristablauf verpflichtet,
- Anbieter zur Auskunftserteilung an Strafverfolgungsbehörden verpflichtet,
- Strafbestimmungen für den Fall der Nichteinhaltung der Verpflichtung zur Vorratsspeicherung bzw. der Auskunftserteilung aufgenommen.

**Alternativen:**

Keine.

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

Keine.

**Auswirkungen des Regelungsvorhabens**

**Finanzielle Auswirkungen:**

Mit dieser Novelle werden Anbieter dazu verpflichtet, Verkehrs- und Standortdaten, die beim Erbringen von Kommunikationsdiensten erzeugt oder verarbeitet werden, für Zwecke der Strafverfolgung zu speichern und in den gesetzlich geregelten Fällen Auskunft zu erteilen. Der Investitionsaufwand wird geschätzte 15 Millionen Euro betragen. Nähere Ausführungen zu dieser Kostenschätzung erfolgen nachstehend.

Erläuterung zur Kostenschätzung:

Anbieter von öffentlichen Kommunikationsdiensten haben künftig die in § 102a TKG aufgezählten Daten auch dann für sechs Monate zu speichern, wenn sie diese Daten für betriebliche Zwecke (Verrechnung, technische Wartung) nur für kürzere Zeiträume oder gar nicht benötigen. In diesen Fällen werden die Daten zu sogenannten „Vorratsdaten“ (§ 92 Abs. 3 Z 6b TKG) und dürfen vom Anbieter für eigene Zwecke nicht mehr verwendet werden. Zugriffe auf diese Daten für die in §§ 99 Abs. 5 bzw. 102b TKG normierten Zwecke müssen revisionssicher protokolliert werden und dürfen nur nach dem 4-Augen-Prinzip erfolgen. Die Speicherung der Daten muss physisch gesehen nicht getrennt von den Abrechnungssystemen erfolgen, denn diese Anforderung würde die Kosten enorm steigern und zugleich nur einen vergleichbar kleinen Zugewinn bei der Datensicherheit bedeuten, weil die Anbieter dann nicht einmal ihre bestehenden Data-Warehouse-Infrastrukturen nutzen dürften. Jedoch logisch (also in der Datenbankstruktur) müssen Vorratsdaten streng von sonstigen Daten getrennt sein, weil die Anbieter diese Daten für eigene Zwecke nicht nutzen dürfen. Das bedeutet, dass die Anbieter für diese Daten eigene Datenbank-Infrastrukturen aufbauen müssen (§ 102 c Abs. 1 TKG). Außerdem fällt eine im Vergleich zum Status Quo beträchtliche Datenmenge dabei an. Insbesondere die künftige zusätzliche Verfügbarkeit von Internet-Zugangs- und E-Mail- Daten (die bisher gar nicht gespeichert werden) erhöht den Bedarf an zusätzlichen Speichermedien enorm.

Auch wenn die Anbieter die gespeicherten Daten nicht für eigene Zwecke verwenden dürfen, so ist der Gegenstand der staatlichen Überwachungsaufgabe doch auf die von den Anbietern erbrachte Bereitstellung von Telekommunikationsdiensten zurückzuführen, die im wirtschaftlichen Interesse der Anbieter liegt.

Zum Zwecke der Kostenschätzung wurden zunächst Erhebungen bei vielen Anbietern angestellt, sowohl kleinere als auch sehr große Betriebe einschließlich der marktführenden Unternehmen wurden dabei befragt. Die befragten Anbieter haben dabei den Entwurf zur TKG-Novelle als Basis für ihre Schätzungen

angenommen, zu dem hinsichtlich der relevanten Bestimmungen schon Einigkeit unter den beteiligten Ministerien bestand. Nachfolgend werden Indikatoren zur möglichen Reduktion des Kostenaufwands benannt.

Es ist zu berücksichtigen, dass die Kostenrelation pro Anschluss umso höher ist, je kleiner der Anbieter ist, bei größeren Anbietern kann sie leicht darunter liegen: Während größere Anbieter am Markt in der Lage sind, Skaleneffekte zu erzielen, können für kleinere Anbieter im Vergleich die Investitionskosten pro Kunde weit höher liegen. Aus den Rückmeldungen der Anbieter lässt sich folgende (geschätzte) Kostenfunktion ableiten: Für einen fiktiven Anbieter A mit 100.000 Anschlüssen können Investitionskosten von 200.000 Euro angenommen werden (2 Euro pro Anschluss), für einen fiktiven Anbieter B mit 2,5 Mio. Anschlüssen Investitionskosten von 2,5 Mio. Euro (1 Euro pro Anschluss), für einen fiktiven Betreiber mit 5 Mio Anschlüssen 3,5 Mio. Euro (0,7 Euro pro Anschluss).

Aus dem Telekom Monitor 4/2010 der RTR ([http://www.rtr.at/de/komp/TKMonitor\\_4\\_2010/TM4-2010.pdf](http://www.rtr.at/de/komp/TKMonitor_4_2010/TM4-2010.pdf)) ist die Gesamtzahl der Anschlüsse in Österreich ersichtlich, wobei die zugrunde liegenden Daten aus dem 2. Quartal 2010 stammen:

Gesamtanzahl der Mobilfunknummern (S. 25/43):	12.192.000
- PrePaid:	3.772.000
- Vertragshandy:	8.420.000
Gesamtanzahl der Festnetzanschlüsse (S. 7):	2.674.000
- Privatkunden	2.047.000
- Geschäftskunden	627.000
Gesamtzahl der Endkundenbreitbandanschlüsse (S. 34):	3.395.100
- Mobile Breitbandanschlüsse	1.444.100
- DSL	1.035.900
- Koaxialkabel	577.700
- Entbündelte Leitungen (ANB)	340.600

Insgesamt bestehen 18.261.100 Anschlüsse. Zu berücksichtigen ist, dass jene Anbieter von der Speicherpflicht gemäß § 102a TKG ausgenommen sind, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 10 KommAustriaG unterliegen. Die angegebenen Anschlusszahlen bilden jedoch die Grundgesamtheit ab (zur Methode vgl. Seite 2 TK Monitor). Zahlenmäßig relevant ist die Ausnahme kleiner Anbieter im Bereich der Internet-Zugangsanbieter. Zur Berücksichtigung der Ausnahmen sowie zur einfacheren Schätzung wird daher von rund 18.000.000 Anschlüssen ausgegangen, für die eine Speicherpflicht im Sinne der Vorratsdatenspeicherung besteht.

Geht man davon aus, dass der österreichische Markt von einigen wenigen Marktteilnehmern mit sehr hohen Marktanteilen dominiert wird, liegen die durchschnittlichen Investitionskosten pro Anschluss jedenfalls unter 1 Euro, womit sich ein geschätzter Betrag von etwa 15.000.000 Euro für sämtliche Anschlüsse ergibt.

Kostenrelevante Indikatoren:

Ob die Kosten zum Aufbau der notwendigen Infrastruktur tatsächlich diesen Wert erreichen, hängt von einigen Indikatoren ab, die sich endgültig erst aus der „Technischen Richtlinie“ (Verordnung nach §§ 94 Abs. 4 und 102c TKG) zur Konkretisierung der Datensicherheits-Standards sowie der Bedingungen zur Übermittlung der Daten an auskunftsberechtigte Behörden ergeben werden. Hier sollen nur überblicksartig einige der wichtigsten benannt werden:

- Verfügbarkeit der Daten: Entsprechend den Anforderungen an die Geschwindigkeit einer Datenbankabfrage muss die Qualität der eingesetzten Speicherhardware angepasst werden. Wenn innerhalb weniger Minuten aus einer sehr großen Datenmenge Ergebnisse einer Datenbank-Abfrage gefordert sind, muss die Qualität der Speichermedien und damit der Preis anders beschaffen sein, als wenn die Abfrage z. B. eine ganze Nacht dauern darf.
- Datensicherheit (technisch): Für Backup Lösungen besteht eine beträchtliche Bandbreite an verfügbaren technologischen Standards mit unterschiedlichen Sicherheitsniveaus und daher entsprechender Preisunterschiede. Hier ist etwa unklar, ob und inwieweit die „Technische Richtlinie“ hierzu Standards oder Kriterien konkretisieren wird.

- System der Abfrage und Protokollierung: Sowohl die reversionssichere Protokollierung als auch das 4-Augen-Prinzip zum internen Zugriff des Anbieters auf Vorratsdaten sind Begriffe, die einer näheren Auslegung durch die „Technische Richtlinie“ bedürfen. Je nach dem, wie streng die Anforderungen hierzu sein werden, kann der Aufwand zur Implementierung sich verändern.
- System der Übermittlung der Daten bei Auskunftsbegehren: Die Übermittlung von Daten bei Auskunftsbegehren nach der StPO oder dem SPG hat „unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen“ und sind „unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als ‚Comma-Separated Value (CSV)‘ - Dateiformat zu übermitteln.“ (§ 94 Abs. 4 TKG) Die gesetzliche Vorgabe des CSV-Dateiformats wurde nicht zuletzt aus Gründen der Wirtschaftlichkeit gewählt und stellt die günstigste und einfachste Variante dar, weil keine Notwendigkeit für eine bestimmte Software oder Lizenzierung besteht. Die Frage der sicheren Authentifizierung der Anfrageberechtigten und die Architektur des Verschlüsselungssystems sind aber äußerst kostenrelevant. Wenn etwa zwischen jedem auskunftspflichtigen Anbieter und jeder auskunftsberechtigten Behörde (nach derzeitiger Rechtslage wären das theoretisch sämtliche Polizeidienststellen Österreichs, wengleich in der Praxis fast alle Verkehrsdaten-Auskünfte gemäß einem internen Erlass des BMI über 12 Stellen abgewickelt werden) eine sichere Kommunikation gewährleistet werden müsste („n x m - Problem“), sind die Kosten dafür ungleich höher, als wenn die Zahl der auskunftsberechtigten Stellen eingeschränkt ist und sichere Verbindungen nur zu beispielsweise 12 Stellen oder gar einer zentralen Drehscheibe zum Datenaustausch bestehen muss. Die „Technische Richtlinie“ wird ein System zum Datenaustausch klar definieren müssen, wobei die Grundsatzentscheidungen zur Determinierung dieses Systems noch ausstehen. Diesen Punkt wird das oben genannte Stakeholder-Treffen in KW 7 2011 zentral fokussieren.

#### Laufende Kosten:

Auf Auskünfte über Vorratsdaten ist gemäß § 94 Abs. 2 TKG die „Überwachungskostenverordnung“ (BGBl. II Nr. 322/2004) anwendbar. Diese enthält bestimmte Tarifsätze für Datenauskünfte je nach Art der begehrten Daten, wobei die derzeit gültige Verordnung nicht alle Datenkategorien enthält, die künftig aufgrund der Vorratsdatenspeicherung verfügbar sein werden (insbesondere bzgl. E-Mail-Daten). In einem Anschlussstück zur Novelle des Telekommunikationsgesetzes 2003 – TKG 2003 wird eine korrespondierende Novellierung von SPG bzw. StPO vorgenommen. Auf diesen Gesetzentwurf wird daher in diesem Zusammenhang hingewiesen.

Schätzungen des Bundesministeriums für Justiz ergeben folgendes: Durch die Schaffung der Möglichkeit der Auskunft über Vorratsdaten ist von einer nicht linearen Steigerung der Kosten für die Mitwirkung von Anbietern an Überwachungsmaßnahmen von 30% auszugehen. Bisher war den Strafverfolgungsbehörden der Zugriff auf historische Zugangsdaten bzw. E-Mail-Daten 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. Die Auferlegung der Verpflichtung erfolgt in Umsetzung von Gemeinschaftsrecht, sodass die diesbezüglichen Anordnungen nicht disponibel sind.

#### Finanzielle Bedeckung:

##### Investitionskosten:

Der initiale Investitionsaufwand zur Schaffung der für die Umsetzung der Vorratsdatenspeicherungsrichtlinie notwendigen Infrastruktur wird für die gesamte österreichische Telekommunikationsbranche geschätzte 15 Millionen Euro betragen.

Die Bedeckung dieser Kosten erfolgt wie folgt:

20 % durch die Anbieter,

80 % der tatsächlichen und nachweisbaren Investitionen werden durch den Bund getragen und den Anbietern ersetzt.

Der auf den Bund entfallende initiale Investitionsaufwand wird aus Budgetmitteln der Bundesministerien für Justiz, Inneres sowie Verkehr, Innovation und Technologie wie folgt bedeckt:

Bundesministerium für Verkehr, Innovation und Technologie: 63 %

Bundesministerium für Inneres: 34 %

Bundesministerium für Justiz: Fixbetrag in Höhe von 360.000,- Euro

#### Laufende Kosten

Die Bedeckung der laufenden Kosten erfolgt aus Budgetmitteln des Bundesministeriums für Justiz nach den Bestimmungen der Überwachungskostenverordnung und, soweit Standortdatenauskünfte nach Sicherheitspolizeigesetz betroffen sind, aus den Budgetmitteln des Bundesministeriums für Inneres gemäß den Bestimmungen der Überwachungskostenverordnung.

Der Anteil an den Investitionskosten, der vom Bund den Anbietern rückvergütet wird, wird ab dem Bundesfinanzjahr 2012 budgetwirksam. Dies gilt gleichfalls für die laufenden Kosten, die in diesem Zusammenhang erstmalig im Bundesfinanzjahr 2012 zu tragen sein werden.

#### **Wirtschaftspolitische Auswirkungen:**

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

Keine

##### **Auswirkungen auf die Verwaltungskosten für Bürger/innen und für Unternehmen:**

Für Bürger/innen fallen keine Kosten an.

Zu den laufenden Kosten für Unternehmen darf auf die Ausführungen im Vorblatt verwiesen werden. Hinsichtlich der Investitionskosten werden 80% der tatsächlichen und nachweisbaren Investitionen durch den Bund getragen. Ausgehend von einer 20% Kostentragung durch die Unternehmen und einer 5-jährigen Abnutzungsdauer belaufen sich die Investitionskosten für die Anbieter auf 600.000 € pro Jahr. Es darf auf das Formblatt in der Anlage verwiesen werden.

##### **Auswirkungen in umweltpolitischer Hinsicht, insbesondere Klimaverträglichkeit:**

Keine

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

Keine

##### **Geschlechtsspezifische Auswirkungen:**

Keine

##### **EU-Konformität:**

Gegeben. Der Entwurf dient der Umsetzung von Gemeinschaftsrecht.

##### **Besonderheiten des Normerzeugungsverfahrens:**

Keine.

## Erläuterungen

### Allgemeiner Teil

#### A. Zwischenstaatliche Verpflichtungen

##### 1. Rechtsakte der EU

##### a) Richtlinie 2006/24/EG vom 15. März 2006 über die Vorratsspeicherung von Daten

Die „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 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“ war von Österreich gemäß ihrem Art. 15 spätestens bis zum 15. September 2007 mit der Inkraftsetzung der erforderlichen Rechts- und Verwaltungsvorschriften umzusetzen. Österreich hat im Vorfeld auch eine Erklärung gemäß Art. 15 Abs. 3 der Richtlinie abgegeben, wonach deren Anwendung betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail bis 15. März 2009 zurückgestellt wurde. Mit Urteil vom 29. Juli 2010 hat der Europäische Gerichtshof entschieden, dass die Republik Österreich gegen die in Rede stehende Richtlinie verstoßen hat, indem sie nicht die zu deren Umsetzung erforderlichen Rechts- und Verwaltungsvorschriften erlassen hat.

Die Richtlinie 2006/24/EG verfügt in Art. 3, dass die Mitgliedstaaten durch entsprechende Maßnahmen dafür Sorge zu tragen haben, dass die in Art. 5 der Richtlinie genannten Datenkategorien, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen der vorliegenden Richtlinie auf Vorrat gespeichert werden. Im Sinne des Art. 1 Abs. 2 gilt diese Richtlinie für Verkehrs- und Standortdaten sowohl von juristischen als auch von natürlichen Personen sowie für alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind. Sie gilt gemäß Art. 5 Abs. 2 nicht für den Inhalt elektronischer Nachrichtenübermittlungen einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden. Art. 6 der Richtlinie bestimmt, dass die in Art. 5 angegebenen Datenkategorien für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden müssen. Gemäß Art. 8 haben die Mitgliedstaaten sicherzustellen, dass die in Art. 5 genannten Daten gemäß den Bestimmungen dieser Richtlinie so gespeichert werden, dass sie und alle sonstigen damit zusammenhängenden erforderlichen Informationen unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können. Mit dieser Richtlinie sollen gemäß deren Art. 1 Abs. 1 die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen.

#### **Im Detail regelt die Richtlinie:**

##### i. Welche Daten sind auf Vorrat zu speichern?

Nach den Vorgaben der Richtlinie sind jene Daten (im Folgenden als Vorratsdaten bezeichnet, siehe dazu auch Art. 5 der Richtlinie) auf Vorrat zu speichern, die benötigt werden

- zur Rückverfolgung und Identifizierung der Quelle einer Nachricht (wie Rufnummer, Name und Anschrift des Teilnehmers, Benutzerkennung oder die zugewiesene IP-Adresse bei Internetnutzung),
- zur Identifizierung des Adressaten einer Nachricht (wie die angewählte Rufnummer, Name und Anschrift des Teilnehmers und die Benutzerkennung),
- zur Bestimmung von Datum, Uhrzeit und Dauer der Nachrichtenübermittlung,
- zur Bestimmung der Art der Nachrichtenübermittlung benötigter Daten (des in Anspruch genommenen Telefon- oder Internetdiensts),
- zur Bestimmung der Endeinrichtung von Benutzern benötigte Daten (wie IMSI und IMEI) und
- zur Bestimmung des Standorts mobiler Geräte.

Nicht erfasst werden soll hingegen der Inhalt der Kommunikation. In diesem Sinne normiert Art. 5 Abs. 2 der Richtlinie ausdrücklich, dass keinerlei Daten gespeichert werden dürfen, die Aufschluss über den Inhalt der Kommunikation geben. Jedoch besteht das Problem, dass häufig eine klare Trennung zwischen Verkehrsdaten (einschließlich Standortdaten) und jenen Daten, die Aufschluss über den Inhalt einer Kommunikation geben, nicht möglich ist.<sup>1</sup> Zwar ist die inhaltliche Aussagekraft von Verkehrsdaten keine einheitliche, sondern variiert je nach Datenkategorie, grundsätzlich können aber „bloße“ Verkehrsdaten über eine inhaltliche Aussagekraft verfügen, mitunter sogar Aufschluss über den Inhalt einer Kommunikation geben.<sup>2</sup>

ii. Wie sind die Daten zu speichern?

Die Richtlinie normiert, dass Vorratsdaten so zu speichern sind, dass

- sie von der gleichen Qualität sind und der gleichen Sicherheit und dem gleichen Schutz unterliegen wie die im Netz vorhandenen Daten (Art. 7 lit. a der Richtlinie);
- geeignete technische und organisatorische Maßnahmen getroffen werden, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verarbeitung zu schützen (Art. 7 lit. b der Richtlinie);
- geeignete technische und organisatorische Maßnahmen getroffen werden, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist (Art. 7 lit. c der Richtlinie);
- sie auf entsprechende Anfrage hin unverzüglich an die zuständige Behörde weitergeleitet werden können (Art. 8 der Richtlinie).

Die ersten drei dieser Bestimmungen finden sich in der Richtlinie unter der Überschrift „Datenschutz und Datensicherheit“. Wiewohl die Grenzen der Datensicherheit mit jenen des Datenschutzes in Teilbereichen verschwimmen,<sup>3</sup> stand bei der Abfassung dieser Bestimmung offenkundig mehr das Ziel der Datensicherheit und insbesondere der Datenrichtigkeit im Vordergrund als jenes des Datenschutzes. Dennoch weisen Teile dieser Bestimmungen des Art. 7 auch datenschutzrechtliche Teilaspekte auf. So muss der lit. b des Art. 7, der zu Folge der Zugang zu Vorratsdaten „ausschließlich besonders ermächtigten Personen“ vorzubehalten ist, (auch) ein datenschutzrechtlicher Charakter zugebilligt werden.<sup>4</sup>

1 So kann mitunter aus "bloßen" Verkehrsdaten durchaus auf den Inhalt der Kommunikation rückgeschlossen werden. Beispielsweise sei auf einen Anruf bei der Aidshilfe, Rat auf Draht oder einer ähnlichen Beratungseinrichtung verwiesen. Diese Anrufe werden in aller Regel eine entsprechende Beratung oder Hilfestellung und damit verbundene Inhalte zum Gegenstand haben. Ein Anruf bei einer Anwaltskanzlei wird in aller Regel eine anwaltliche Beratung zum Gegenstand haben, wie Telefonate eines Geistlichen regelmäßig einen seelsorgerischen Hintergrund haben. Nichts anderes gilt für andere Formen der Kommunikation. Insbesondere bei der Korrespondenz via Email tritt das (wahrscheinliche) Gesprächsthema und somit der (wahrscheinliche) Gesprächsinhalt regelmäßig noch unmittelbarer zu Tage als "bloß" bei einer Telefonnummer; dies, da das Tätigkeitsfeld des Emailadresseninhabers oftmals unmittelbar aus der Adresse hervorgeht.

2 Der allfällige Einwand, dass der aus den Verkehrsdaten via Rückschluss indizierte Inhalt des Gesprächs nicht zwingend den tatsächlichen Gegebenheiten entsprechen muss, geht insofern ins Leere, als der Richtlinienggeber in Art. 5 Abs. 2 nicht von Inhaltsdaten im engeren Sinn, sondern lediglich von Daten spricht, die "Aufschluss über den Inhalt der Kommunikation geben". Diese Formulierung weist zudem in auffallender Weise Parallelen zu Art. 8 Abs. 1 der Richtlinie 95/46/EG auf. Dieser Bestimmung zu Folge dürfen Daten, "aus denen die rassische und ethnische Herkunft, politische Meinungen (...) hervorgehen sowie (...) Daten über die Gesundheit oder Sexualleben" (so genannte "sensible personenbezogene Daten") grundsätzlich nicht verarbeitet werden. Für die "Sensibilität" eines Datums ist nun keinesfalls erforderlich, dass das sensible Faktum, also etwa die ethnische Herkunft oder die politische Meinung, selbst Gegenstand des Datums ist, sondern es genügt, wenn auf dieses Datum rückgeschlossen werden kann. Als Beispiel sei auf die Mitgliedschaft bei einer Vereinigung, der die Nähe zu einer bestimmten politischen Partei nachgesagt wird, verwiesen. Das Datum "Mitgliedschaft" bei dieser Vereinigung wäre ein sensibles, obgleich die "politische Meinung", also das die Sensibilität begründende Faktum, nicht selbst Gegenstand des Datums ist, sondern aus der Mitgliedschaft auf diese nur geschlossen werden kann. Ähnlich verhält es sich mit dem Datum "Besuch beim Lungenfacharzt". Dieses Datum wird als sensibles angesehen, obwohl es sich ja auch um einen Freundschaftsbesuch handeln könnte.

3 So dienen Maßnahmen, die die Daten vor unberechtigter und unrechtmäßiger Speicherung, Verarbeitung und Zugänglichmachung schützen, sowohl dem Ziel der Datensicherheit wie auch jenem des Datenschutzes.

4 Der datenschutzrechtliche Wert dieser Bedingung ist durch die weite und unbestimmte Textierung allerdings ein nur geringer. Denn "besonders ermächtigt" werden könnte auch ein sehr weit gefasster Personenkreis.

Obleich von den zuständigen Ausschüssen des EU-Parlaments zahlreiche Änderungsanträge mit datenschutzrechtlicher Schwerpunktsetzung ausgearbeitet und in den Ausschüssen fraktionsübergreifend bestätigt worden waren, finden sich in der Richtlinie keine weiteren, über die vorgenannten Regelungen hinausgehenden datenschutzrechtlichen Bestimmungen.

### iii. Zugang zu Daten

Hinsichtlich des Zugangs zu den Vorratsdaten sieht die Richtlinie (siehe Art. 4) lediglich vor, dass seitens der Mitgliedstaaten Maßnahmen zu erlassen sind, um sicherzustellen, dass die Daten „nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden“.

Ob es sich hierbei um Gerichte, Sicherheits- oder auch andere Behörden handelt, ist dem Text der Richtlinie mangels ausdrücklicher Regelung nicht unmittelbar zu entnehmen. Dass unter den „zuständigen Behörden“ im Sinne der Richtlinie freilich nicht jede nationale Behörde zu verstehen sein kann, ergibt sich schon durch die vom Richtliniengeber vorgenommene Zweckbestimmung der Vorratsspeicherung.

**Art. 1** der Richtlinie sieht ausdrücklich vor, dass mit der europaweiten Einführung der Vorratsspeicherung sichergestellt werden soll, „dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten (...) zur Verfügung stehen.“ Damit ist vorgegeben, dass die Daten nur jenen Behörden zur Verfügung zu stehen haben, die mit der Verfolgung dieser Zwecke betraut sind, also den Strafverfolgungsbehörden.

Soweit Art. 4 also normiert, dass die Vorratsdaten an die „zuständigen Behörden“ weiterzugeben sind, ist festzuhalten, dass die Autonomie des nationalen Gesetzgebers bei Bestimmung jener Behörden, die Zugriff auf die Vorratsdaten haben sollen, im vorgenannten Sinne eingeschränkt ist. Diese, schon durch eine systematische Interpretation gebotene Auslegung wird zudem auch durch einen Blick auf die Entstehungsgeschichte bestätigt.

Aus der eben dargelegten Zweckbestimmung, genauer aus der Festlegung des Zwecks der Vorratsspeicherung auf die Ermittlung, Feststellung und Verfolgung von „schweren Straftaten“ folgt eine weitere Einschränkung des Zugangs zu den auf Vorrat gespeicherten Daten. Der Entstehungsgeschichte der Richtlinie lassen sich Hinweise entnehmen, wonach der EU-Gesetzgeber ursprünglich an die Bekämpfung des Terrorismus und schwerer organisierter Kriminalität als Zweckbindung der Vorratsdatenspeicherung gedacht hat (siehe die Ausführungen unter Punkt 1/a). Auch in den Erwägungsgründen (7)-(9) der Richtlinie wird der Zusammenhang mit der Bekämpfung von Terrorismus und organisierter Kriminalität mehrfach deutlich. Da aber die Richtlinie zur Festlegung des Begriffs „schwere Straftaten“ auf das jeweilige nationale Recht verweist, dürfte deren Definition letztlich im – allerdings vor allem grundrechtlich begrenzten – Ermessen der Mitgliedstaaten liegen.

### iv. Speicherdauer

Im Hinblick auf die Speicherdauer normiert die Richtlinie, dass die Vorratsdaten für einen Zeitraum zwischen sechs Monaten und zwei Jahren zu speichern sind (siehe Art. 6).<sup>5</sup> Am Ende der Vorratsspeicherungsfrist sind die Vorratsdaten zu vernichten (mit Ausnahme jener Daten, die abgerufen und gesichtet worden sind).

### v. Haftung, Rechtsbehelfe und Sanktionen

Hinsichtlich dieser Themenbereiche wird in der Richtlinie festgehalten, dass die Mitgliedstaaten erforderliche Maßnahmen zu ergreifen haben, um sicherzustellen, dass die in der Datenschutzrichtlinie 95/46/EG normierte Haftung wie auch die dort vorgesehenen Rechtsbehelfe und Sanktionen auf Datenverarbeitungen nach der vorliegenden Richtlinie in vollem Umfang umgesetzt werden (siehe Art. 13).

### vi. Kontrollstelle

In jedem Mitgliedstaat ist eine oder sind mehrere unabhängige Kontrollstellen zu benennen, die für die Kontrolle der Anwendung der von den Mitgliedstaaten zur Umsetzung des Art. 7 über Datenschutz und Datensicherheit erlassenen Vorschriften zuständig sind (siehe Art. 9).<sup>6</sup>

<sup>5</sup> In diesem Zusammenhang sei auf Art. 12 hingewiesen, der die Möglichkeit einer über den Zeitraum von zwei Jahren hinausgehenden Höchstspeicherdauer eröffnet, sofern "besondere Umstände die Verlängerung der maximalen Speicherungsfrist" rechtfertigen.

<sup>6</sup> Dies dürfte eine der wenigen Bestimmungen sein, die tatsächlich auf eine Initiative des Europäischen Parlaments zurückgehen. Der LIBE-Ausschuss hatte in seinem dem Plenum vorgelegten Bericht zum Richtlinienentwurf den Änderungsantrag aufgenommen, dass jeder Mitgliedstaat "gemäß dem nationalen Recht die Datenschutzbehörde oder

#### vii. Statistik

Schließlich normiert die Richtlinie, dass die Mitgliedstaaten eine Statistik, die keine personenbezogenen Daten enthalten darf, zu führen und jährlich an die Kommission zu übermitteln hat (siehe Art. 10). Aus dieser hat insbesondere hervorzugehen,

- in welchen Fällen im Einklang mit dem innerstaatlichen Recht Daten an die zuständige Behörde weitergegeben wurden;
- wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefordert wurden, verging;
- in welchen Fällen die Anfragen nach Daten ergebnislos blieben.

Eine umfassende Evaluierung der Vorratsspeicherung ist offenbar nicht das Ziel dieser Statistik. Eine statistische Auswertung der Anwendung der zur Umsetzung der Richtlinie erlassenen Vorschriften wäre aber als Teil einer größer angelegten Evaluierung der Richtlinie zu begrüßen, insbesondere im Hinblick darauf, ob und inwieweit der vom Richtliniengeber vorgesehene Zweck der Vorratsspeicherung erreicht werden konnte. Eine statistische Erhebung, aus der hervorgeht, inwieweit verarbeitete Daten zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten beigetragen haben, ist aber gerade nicht Gegenstand der in Rede stehenden Bestimmung.

#### b) Weitere EU-Rechtsakte

Weiters sind noch folgende Richtlinien zu beachten, auf welche die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten auch ausdrücklich verweist, und zwar

- die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie) und
- die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

Während die Richtlinie 95/46/EG den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Gegenstand hat, dient die Richtlinie 2002/58/EG der Harmonisierung der Vorschriften der Mitgliedstaaten, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

#### 2. Rechtsakte außerhalb der EU

Neben der Richtlinie sind vom Gesetzgeber auch das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates vom 28.1.1981, BGBl. Nr. 317/1988, sowie das Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr vom 8. November 2001, BGBl. Nr. 91/2008, zu beachten.

#### **B. Stand der Umsetzung der Richtlinie in den EU-Mitgliedstaaten**

Nach derzeitigem Informationsstand haben neben Österreich weitere EU-Mitgliedstaaten die Richtlinie noch nicht oder noch nicht vollständig umgesetzt. Es sind dies: Griechenland, Irland und Schweden. Gegen diese Staaten laufen daher auch Vertragsverletzungsverfahren vor dem EuGH, die aufgrund von Klagen der Europäischen Kommission gemäß Art. 226 EGV eingeleitet wurden.

Im Hinblick auf die Dauer der Vorratsdatenspeicherung haben sich Deutschland, Rumänien und Tschechien für eine sechsmonatige Speicherung entschieden (geplant auch in Schweden), in England, Frankreich, Finnland und Italien beträgt die Speicherfrist zwölf Monate (geplant auch von Irland).

---

eine andere geeignete unabhängige Behörde beauftragt, die rechtmäßige Umsetzung dieser Richtlinie zu beaufsichtigen." Da weder der Rahmenbeschlusssentwurf des Jahres 2004 noch der Richtlinienentwurf der Kommission eine Kontrollstelle iSd Art. 9 vorsah, ist mit gutem Grund anzunehmen, dass der eben angesprochene Änderungsantrag in Art. 9 aufgenommen wurde.



### C. Der Begutachtungsentwurf 2007

Im Frühjahr wurde vom BMVIT bereits der Entwurf einer TKG-Novelle zur Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten in Begutachtung gegeben.<sup>7</sup> Der Gesetzentwurf sah die Erfüllung der Verpflichtung im Hinblick auf Daten betreffend Telefonfestnetz und Mobilfunk sowie jene Daten vor, die den Internetzugang, die Internet-Telefonie und Internet-E-Mail betreffen, die zur Identifizierung der Quelle einer Nachricht benötigt werden. Mit dem Entwurf wurden im Wesentlichen folgende Regelungen vorgeschlagen:

- Anpassung der Begriffsbestimmungen an jene der Richtlinie 2006/24/EG,
- Verpflichtung von Diensteanbietern und Netzbetreibern zur Vorratsspeicherung von Daten für sechs Monate,
- taxative Aufzählung der zu speichernden Daten,
- Verpflichtung zur Löschung der Daten nach Fristablauf,
- Verpflichtung von Diensteanbietern und Netzbetreibern zur Auskunftserteilung an Strafverfolgungsbehörden,
- Strafbestimmung für den Fall der Nichteinhaltung der Verpflichtung zur Vorratsspeicherung bzw. der Auskunftserteilung.

Da der Entwurf mehrfach von verschiedensten Seiten auf Kritik stieß und zeitnah eine Regierungsumbildung erfolgte, wurde er nicht mehr weiterverfolgt.

### D. Grundrechtskonforme Umsetzung der Richtlinie und Grundzüge des Entwurfes

#### 1. Grundrechtskonformität

Bei der Umsetzung der Richtlinie ist darauf zu achten, dass die gesetzlichen Bestimmungen den Anforderungen der Eingriffsvorbehalte des Art. 8 Abs. 2 EMRK insbesondere im Hinblick auf Datensicherheit und Datenschutz entsprechen. Dies steht auch mit Erwägungsgrund (17) der Richtlinie in Einklang, wonach die Mitgliedstaaten gesetzgeberische Maßnahmen zu ergreifen haben, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten „nur in Übereinstimmung mit den innerstaatlichen Rechtsvorschriften und unter vollständiger Achtung der Grundrechte der betroffenen Personen an die zuständigen nationalen Behörden weitergegeben werden“.<sup>8</sup> Keinesfalls dürfen gemäß Art. 5 der Richtlinie Daten auf Vorrat gespeichert werden, die Aufschluss über den Inhalt einer Kommunikation geben.<sup>9</sup>

Nach Erwägungsgrund (25) der Richtlinie berührt diese nicht das Recht der Mitgliedstaaten, Rechtsvorschriften über den Zugang zu und die Nutzung von Daten durch die von ihnen benannten nationalen Behörden zu erlassen. Dennoch sieht Art. 4 der Richtlinie vor, dass Mitgliedstaaten sicherstellen sollen, dass die gemäß dieser Richtlinie gespeicherten Vorratsdaten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden und im innerstaatlichen Recht unter Berücksichtigung insbesondere der EMRK in der Auslegung des EGMR das Verfahren und die Bedingungen festgelegt werden, die für den Zugang zu Vorratsdaten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind. Weiters verpflichtet Art. 13 Abs. 1 der Richtlinie die Mitgliedstaaten sicherzustellen, dass die einzelstaatlichen Maßnahmen zur Umsetzung der in Kapitel III der Richtlinie 95/46/EG<sup>10</sup> niedergelegten Bestimmungen über Rechtsbehelfe, Haftung und Sanktionen im Hinblick auf die Datenverarbeitung gemäß der vorliegenden Richtlinie in vollem Umfang umgesetzt werden.

In seiner jüngeren Rechtsprechung hat der EGMR für den Fall der Sammlung und Verwendung inhaltlicher Informationen, die im Zuge geheimer optischer und akustischer Überwachungsmaßnahmen gewonnen werden und von denen alle Einwohner eines Landes betroffen sein können, bestimmte Anforderungen und Voraussetzungen entwickelt, die sich an den Gesetzgeber richten.<sup>11</sup> Zwar ist die Ausgangslage dieses Falles nicht mit der hier gegenständlichen Vorratsdatenspeicherung vergleichbar, doch handelt es sich um eine Form geheimer Überwachung letztlich auch dann, wenn in konkreten Verdachtsmomenten auf Vorrat gespeicherte personenbezogene Daten – noch ohne Information der

<sup>7</sup> Ministerialentwurf 61/ME-XXIII. GP.

<sup>8</sup> Siehe auch die Verweise auf Art. 7 und 8 der EU-Grundrechtecharta in Erwägungsgrund (22).

<sup>9</sup> Jedoch dürfen bzw. müssen Verkehrsdaten gespeichert werden, selbst wenn aus ihnen gewisse Rückschlüsse auf Kommunikationsinhalte gezogen werden können, etwa zu E-Mail Kommunikationsvorgängen.

<sup>10</sup> Siehe Fn 8.

<sup>11</sup> Vor allem Urteil des EGMR im Fall Association for European Integration and Human Rights and Ekimdzhiiev gegen Bulgarien vom 28. Juni 2007, Z. 71 ff.

betroffenen Person – verwendet werden, um eine Straftat zu ermitteln, festzustellen oder zu verfolgen, weswegen die vom EGMR entwickelten Kriterien auch hier Berücksichtigung finden können. Ausdrücklich hält der EGMR fest, dass

- ein solches Gesetz hinreichend klar formuliert sein muss, um den Betroffenen adäquate Anhaltspunkte zu den Bedingungen und Umständen zu geben, unter denen Behörden ermächtigt sind, in das Recht auf Achtung des Privatlebens und der Korrespondenz im Sinne des Art. 8 EMRK einzugreifen;
- ein solches Gesetz im Hinblick auf die Missbrauchsgefahr, die einem System geheimer Überwachung immanent ist, besonders präzise formuliert sein muss;
- es essentiell ist, dass ein solches Gesetz klare, detaillierte Bestimmungen hinsichtlich des Gegenstandes enthalten muss, insbesondere im Hinblick darauf, dass die zur Verfügung stehende Technologie immer technisch ausgefeilter wird.

Um sicherzustellen, dass diese Grundsätze effektiv implementiert werden, verlangt der EGMR folgende Mindestsicherungsmaßnahmen, die in Gesetzesform und nicht etwa als Verordnung erlassen werden müssen:

- die Natur der Straftat, die Anlass für die Überwachung bietet;
- eine Definition jener Kategorien von Personen, die der Überwachung unterworfen werden können;
- eine zeitliche Beschränkung für derartige Überwachungsmaßnahmen;
- ein Verfahren, das bei der Prüfung, Verwendung und Speicherung der Daten einzuhalten ist;
- jene Schutzmaßnahmen, die einzuhalten sind, wenn die Daten an Dritte weitergegeben werden;
- die Umstände, unter denen die Daten zu löschen oder zu vernichten sind.

Zusätzlich muss das nationale Recht im Falle solcher Überwachungsmaßnahmen aufgrund der mangelnden öffentlichen Kontrolle und der Gefahr des Missbrauchs Schutz vor willkürlichen und unbegründeten Eingriffen bieten. Der EGMR betont, dass es im nationalen Recht adäquate und effektive Garantien gegen Missbrauch geben müsse.

## 2. Grundzüge des Entwurfs

Grundsätzlich verfolgt der Entwurf das Ziel, die Richtlinie so umzusetzen, dass zwar ihr Zweck, die harmonisierte Speicherung von Vorratsdaten zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten mittels auf Vorrat gespeicherter personenbezogener Daten, innerstaatlich erreicht wird, um den Strafverfolgungsbehörden die Verwendung zeitgemäßer technischer Mittel zu ermöglichen, zugleich aber über legitime Vorkehrungen sichergestellt ist, dass

- die mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe so gering wie möglich – und damit verhältnismäßig zum verfolgten Zweck – ausfallen,
- die Sicherheit der Daten sowohl bei den Telekommunikationsbetreibern als auch bei den zur Datenanwendung berechtigten Behörden bestmöglich gewährleistet ist,
- den datenschutzrechtlich erforderlichen Informationspflichten nachgekommen wird,
- alle notwendigen Rechtsmittel zur Verfolgung der datenschutzrechtlichen und grundrechtlichen Interessen Betroffener zur Verfügung stehen,
- darüber hinausgehende unabhängige datenschutzrechtliche Kontrollen vorgesehen werden, und
- die wirtschaftlichen Auswirkungen der Vorratsdatenspeicherung auf die zur Speicherung und Auskunft verpflichteten Telekommunikationsbetreiber grundrechtskonform zu gestalten.

Hinsichtlich der Speicherdauer<sup>12</sup> sieht der Entwurf aus folgenden Gründen einen Zeitrahmen von sechs Monaten vor (das ist die von der Richtlinie vorgegebene Mindestdauer): Einerseits stellt eine verdachtsunabhängige Speicherung personenbezogener Daten insbesondere im Hinblick auf die Missbrauchsgefahr einen erheblichen Grundrechtseingriff dar. Andererseits ist die Verwendung von Verkehrsdaten durch Strafverfolgungsbehörden in den meisten Fällen nur in einem Zeitraum von Nutzen, der nicht länger als drei Monate zurückliegt. In der Praxis wurden und werden in Österreich von den Betreibern die für die Verrechnung bzw. den technischen Betrieb erforderlichen Daten bis maximal sechs Monate gespeichert und den Strafverfolgungsbehörden auch zur Verfügung gestellt. Überwiegend wird

---

<sup>12</sup> Zur Speicherdauer siehe ausführlicher die Erläuterungen zum besonderen Teil zu § 102a Abs. 1.

ein Speicherzeitraum von sechs Monaten als wünschenswert erachtet. Die grundrechtlich gebotene Abwägung und Frage nach der Verhältnismäßigkeit der Maßnahme zeigt daher, dass kein die grundrechtlichen Interessen der Betroffenen überwiegendes (öffentliches) Interesse der Strafrechtspflege an einer längeren Speicherung der Daten vorliegen dürfte.

Der Entwurf sieht vor, dass über die schon bisher für Telekommunikationsbetreiber bestehende Berechtigung zur Speicherung und Verarbeitung von Daten für betriebsnotwendige-, insbesondere für Verrechnungszwecke (in der Regel für einen Zeitraum von drei Monaten) hinaus in Umsetzung der Vorgaben der Richtlinie bestimmte, näher umschriebene Daten (insbesondere IP-Adressen) ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern sind (vorgeschlagener § 102a TKG). Der Begriff „Vorratsdaten“ stellt keine neue Kategorie im Sinne von Verkehrsdaten, Standortdaten, Inhaltsdaten oder Stammdaten dar, sondern stellt vielmehr auf den Zweck ab, für den die Daten von den Telekommunikationsanbietern gesammelt werden müssen.

Nach dem Entwurf dürfen Verkehrsdaten außer in den im TKG geregelten Fällen weder gespeichert noch verwendet werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren (vorgeschlagener § 99 TKG). Mit dieser abschließenden Regelung soll insoweit Rechtssicherheit geschaffen werden, als damit aus anderen gesetzlichen Bestimmungen weder eine Berechtigung noch gar eine Verpflichtung zur Speicherung von Verkehrsdaten abgeleitet werden kann.

Von der Speicherpflicht nicht erfasst sind solche Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 10 KommAustriaG unterliegen. (vorgeschlagener § 102a Abs. 6 TKG). Die den Anbietern aus der Umsetzung der Vorratsdatenspeicherung entstehenden Kosten werden entsprechend vergütet (vorgeschlagener § 94 TKG).

Die auf Vorrat gespeicherten Daten dürfen abgesehen von den in § 99 Abs. 5 abschließend aufgezählten Ausnahmen ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt übermittelt werden .

So wie bisher haben die zuständigen Behörden nach der StPO zur Verfolgung „niederschwelliger“ Straftaten (also solcher, die keine „schweren Straftaten“ sind) das Recht auf Beauskunftung der bei den Telekommunikationsbetreibern für betriebsnotwendige Zwecke gespeicherten Verkehrsdaten (sogenannte „Billingdaten“ gemäß § 99 Abs. 2), wenn eine gerichtliche Bewilligung vorliegt (vorgeschlagener § 99 Abs. 5 Z 1 TKG).

Ebenso wie bisher sind die nach dem SPG zuständigen Sicherheitsbehörden für die Erfüllung ihrer im SPG geregelten präventiven Aufgaben berechtigt, Auskünfte über die bei den Telekommunikationsbetreibern für betriebsnotwendige Zwecke gespeicherten Daten nach Maßgabe des § 53 Abs. 3a und 3b einzuholen. (vorgeschlagener § 99 Abs. 5 Z 3 TKG).

Der Entwurf sieht eine Trennung zwischen für betriebsnotwendige Zwecke und auf Vorrat gespeicherte Daten vor, für deren Speicherung besondere Sicherungsmaßnahmen vorgesehen sind. Die Kontrolle wird der Datenschutzkommission übertragen (vorgeschlagener § 102c Abs. 1 TKG). Jeder Zugriff auf Vorratsdaten ist zudem revisionssicher zu protokollieren (vorgeschlagener § 102c Abs. 2 und 3 TKG). Die Beauskunftung von Daten einer Nachrichtenübermittlung nach den Bestimmungen der StPO wie auch die Beauskunftung solcher Daten an die Sicherheitsbehörden - unabhängig davon, ob es sich um Vorratsdaten oder nach § 99 Abs. 2 gespeicherte Daten handelt - hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, in technisch anspruchsvoll verschlüsselter Form zu erfolgen (vorgeschlagener § 94 Abs. 4 TKG).

Schließlich sieht der Entwurf entsprechende neue Verwaltungsstraftatbestände vor (vorgeschlagener § 109 TKG).

#### **E. Kompetenzgrundlage**

Die Kompetenz des Bundes zur Gesetzgebung gründet sich hinsichtlich des Datenschutzes auf die Verfassungsbestimmung des Art. 1 § 2 Abs. 1 DSG 2000 und hinsichtlich der einfachgesetzlichen Bestimmungen auf den Tatbestand „Post- und Fernmeldewesen“ in Art. 10 Abs. 1 Z 9 B-VG.

#### **F. Besonderheiten des Normerzeugungsverfahrens**

Keine.

## Besonderer Teil

### Zu § 1 Abs. 4:

Die Änderung enthält den Hinweis auf die 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. April 2006, S 54.

### Zu §§ 78 Abs. 2, 87 Abs. 2 und 92 Abs. 2:

An diesen Stellen sind Zitate anderer Gesetze zu korrigieren.

### Zu § 90 Abs. 6 und 7:

Die Ergänzung des Abs. 6 („soweit dies ohne Verarbeitung von Verkehrsdaten möglich ist“) stellt den Umfang von Stammdatenabfragen klar, indem jene Auskünfte ausgenommen sind, für deren Erfüllung eine Verarbeitung von Verkehrsdaten durch den Provider vorgenommen werden müsste. Damit wird ausgeschlossen, dass eine Verwaltungsbehörde materiell gesehen eine Verkehrsdatenauskunft als Stammdatenauskunft tarnt, indem sie den Kommunikationsvorgang im Auskunftsbegehren beispielsweise unter Angabe einer passiven Teilnehmernummer und des Zeitraums der Kommunikation beschreibt und hierzu die Auskunft über Name und Anschrift der aktiven Teilnehmer begehrt. Solche indirekten Auskünfte über Kommunikationsvorgänge und damit Verkehrsdaten, bei denen die Auswertung des Kommunikationsvorgangs gewissermaßen an den Anbieter ausgelagert wird, unterliegen dem Kommunikationsgeheimnis und sind nicht von den weitgehend Form- und Voraussetzungs-freien Stammdatenauskünften gedeckt.

Die Neueinführung des Abs. 7 zielt darauf ab, eine eindeutige und klare Rechtsgrundlage zur Auskunft über Stammdaten an die Strafverfolgungsbehörden nach den Bestimmungen der StPO zu schaffen. Sofern keine Verkehrsdaten, insbesondere IP-Adressen (Zugangsdaten) dafür ausgewertet werden müssen, wenn also eine Nachschau bei den Vertragsdaten genügt, bedarf es dafür keiner richterlichen Genehmigung. Bei Vorliegen einer schriftlichen und begründeten Anfrage können daher auch Anfragen der Staatsanwaltschaft, bzw. in deren Auftrag der Kriminalpolizei, beauskunftet werden. Die korrespondierende Befugnis der Strafverfolgungsbehörden findet sich im gleichzeitig neu eingeführten § 76a Abs. 1 StPO, wodurch in der Sache auch klargestellt wird, dass es sich nicht um eine Anordnung der Sicherstellung handelt. Ein darüber hinausgehender ausdrücklicher Verweis auf das Verfahren nach der StPO ist nicht erforderlich. „schriftliches Verlangen“ bedeutet die Angabe des Straftatbestandes, aufgrund dessen die Ermittlungen erfolgen, sowie die bestimmte Person, auf welche sich das Auskunftsbegehren bezieht, wobei hier keine über die StPO hinausgehenden Anforderungen normiert werden. Die Regelung des § 103 Abs. 4, welche im Zusammenhang mit den Teilnehmerverzeichnissen bisher die Rechtsgrundlage für solche Auskünfte war, kann dadurch entfallen. Wie bisher beziehen sich die Auskünfte auch auf Stammdaten, deren Eintragung ins Teilnehmerverzeichnis unterbleibt. Ob für die Auskunft eine - nach dieser Bestimmung nunmehr unzulässige - Auswertung von Verkehrsdaten notwendig ist, hängt nicht davon ab, ob eine Eintragung ins Teilnehmerverzeichnis vorliegt oder nicht.

Die Bestimmung muss im korrespondierenden Zusammenhang mit der klaren Definition zur IP-Adresse in § 92 Abs. 3 Z 16 gesehen werden. Dort wird klargestellt, dass eine IP-Adresse ein Zugangsdatum (Z 4a) und damit ein Verkehrsdatum (Z4) darstellt und nur dann zugleich auch ein Stammdatum (Z 3) ist, wenn dem Kunden im Vertrag ausdrücklich eine bestimmte IP-Adresse für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen wurde. Damit erfolgt die gesetzliche Klarstellung im Sinne der Entscheidung des OGH zu GZ 4 Ob 41/09x, wonach dynamische IP-Adressen jedenfalls als Verkehrsdaten zu behandeln sind (so im Ergebnis auch das VfGH-Erkenntnis G 31/08 vom 1. Juli 2009), mit der die sonst bestehende Judikaturdivergenz zur Entscheidung des 11. Senates (in Strafsachen) des OGH, GZ 11 Os 57/05z bereinigt wird.

Nicht als Auskunft über Stammdaten sind Fälle zu beurteilen, die eine Verarbeitung der IMEI (International Mobile Station Equipment Identity) auf Seiten der Betreiber erfordern. Dem in der Praxis vorkommenden Ersuchen, Auskunft über die Identität eines Teilnehmers zu geben, der mit einem durch eine IMEI-Nummer identifizierbaren Gerät telefoniert hat, konnte auch bisher nicht auf Grundlage des § 103 Abs. 4 entsprochen werden. Die IMEI ist nämlich nicht im Teilnehmerverzeichnis enthalten und beispielsweise bei gestohlenen Geräten auch nicht mit den sonstigen Daten eines Anbieters mit einem bestimmten Teilnehmer verknüpft. Da auch hier die Verarbeitung von Verkehrsdaten notwendig ist, um die begehrte Auskunft erteilen zu können, kann einem solchen Ersuchen nur durch eine Auskunft über Daten einer Nachrichtenübermittlung (früher: Rufdatenrückfassung) entsprochen werden (so bereits die

Erläuterungen zu § 103 Abs. 4). Eine Zuordnung der IMEI zu einem bestimmten Kommunikationsvorgang ist ohne Auswertung von Verkehrsdaten nicht möglich.

Unabhängig von der Zuordenbarkeit zu einem bestimmten Kommunikationsvorgang kann in manchen Fällen, etwa bei gleichzeitigem Kauf eines vertragsgebundenen Endgerätes, eine bestimmte IMEI teilweise im CRM (Customer Relationship Management) - System eines Betreibers vorhanden sein. Dennoch fällt die IMEI nicht unter die abschließende Definition der Stammdaten in § 92 Abs. 3 Z 3, da es sich weder um eine Teilnehmernummer noch um sonstige Kontaktinformationen für die Nachricht handelt, sondern vielmehr ein technisches Datum sui generis vorliegt, welches ausschließlich der Kennzeichnung des Endgerätes dient. Aus der Information im CRM-System kann der Betreiber auch nicht nachvollziehen, ob das durch die IMEI bezeichnete Gerät tatsächlich mit jener Teilnehmerkennung (MS-ISDN, Mobile Subscriber Integrated Services Digital Network Number) verwendet wird bzw. wurde, mit welcher bei Vertragsabschluss zunächst ein Zusammenhang bestand. Dieser Zusammenhang ist beispielsweise dann nicht mehr gegeben, wenn der Benutzer das Gerät mit einer anderen SIM-Karte verwendet oder die IMEI des Gerätes selbst verändert hat, was bei den meisten Endgeräten auch ohne tiefere technische Kenntnisse möglich ist.

Die IMSI (International Mobile Subscriber Identity), durch welche die SIM-Karte (Subscriber Identity Module) eindeutig identifiziert ist, stellt ihrer technischen Funktion nach jedenfalls ein Zugangsdatum im Sinne des § 92 Abs. 3 Z 4a und kein Stammdatum dar und ist als solches im Kommunikationssystem des Betreibers vorhanden. Für eine Zuordnung einer IMSI zu einem bestimmten Kommunikationsvorgang ist daher ebenfalls eine Auswertung von Zugangsdaten, somit entsprechend der Legaldefinition des § 92 Abs. 3 Z 4a von Verkehrsdaten notwendig.

Die Formulierung „nach Maßgabe des § 53 Abs. 3a Z 1 SPG“ im letzten Satz ist insbesondere so zu verstehen, dass an die Sicherheitsbehörden nicht automatisch sämtliche im TKG aufgezählten Stammdaten beauskunftet werden, sondern nur jene, die auch in der genannten Bestimmung aufgezählt sind. Sonstige Stammdatenauskünfte an Sicherheitsbehörden sind nach Maßgabe des § 90 Abs. 6 zulässig.

In dringenden Fällen, damit sind Fälle von Gefahr im Verzug gemeint, darf die schriftliche Dokumentation des Auskunftersuchens vorerst unterbleiben und die Anfrage mündlich gestellt werden. Diese ist dem Anbieter jedoch unverzüglich nachzureichen. Dies gilt sowohl für Anfragen im Anwendungsbereich der StPO wie auch des SPG.

Wie bei den bisherigen Auskünften nach § 103 Abs. 4 sind bei Auskünften nach dieser Bestimmung keine Kosten gemäß der Überwachungskostenverordnung zu ersetzen.

#### **Zu § 90 Abs. 8:**

Diese Bestimmung ist zur Umsetzung der Speicherpflicht gemäß Art. 5 Abs. 1 lit. f) Z 2 der RL 2006/24/EG notwendig. Die korrespondierende Bestimmung der Richtlinie zielt darauf ab, dass die Betreiber trotz sich ständig ändernder Standorte der Funkzellen bzw. Neubenennungen der Funkzellen in der Lage sein müssen, den geografischen Standort jener Funkzelle anzugeben, die zu Beginn jeder Verbindung gemäß § 102a Abs. 3 Z 6 lit. d zu speichern ist - auch wenn diese Funkzelle zwischenzeitlich nicht mehr existiert oder eine andere Bezeichnung hat. Dies bedingt eine Historisierung der Cell-ID und der entsprechenden geografischen Senderstandorte.

Die Verpflichtung zur Führung eines solchen historischen Registers ist bewusst an dieser Stelle – und nicht im Rahmen der Aufzählung der einzelnen „Vorratsdaten“ in § 102a – normiert, um auch in systematischer Hinsicht klarzustellen, dass durch die Einführung der Vorratsdatenspeicherung keine Erfassung von kommunikationsunabhängigen Bewegungsprofilen erlaubt wird.

#### **Zu § 92 Abs. 3 Z 2a:**

Obwohl die RL 2006/24/EG durchwegs den Begriff „Benutzerkennung“ anwendet, wird hier bewusst der Begriff „Teilnehmerkennung“ verwendet, da der zur Auskunft verpflichtete Anbieter nur Auskunft über den Teilnehmer, nicht aber zuverlässig über den tatsächlichen Benutzer geben kann. Diese Definition belässt überdies den Anbietern den Spielraum, selbst jene Kennung abhängig von der jeweils eigenen technischen Struktur zu speichern, welche zur eindeutigen Zuordnung des Kommunikationsvorgangs notwendig ist. Eine Speicherung der Kennung setzt nicht voraus, dass die Identität des Teilnehmers dem Anbieter tatsächlich bekannt ist (z. B. anonymer Prepaid-Dienst).

Teilnehmer und Benutzer sind streng voneinander zu unterscheiden. Teilnehmer ist der Vertragspartner des Diensteanbieters, Benutzer ist der tatsächliche Urheber einer Kommunikation. Der Zweck der Speicherung der Daten liegt letztlich darin, für die Strafverfolgungsbehörden jene natürliche Person zu identifizieren, die tatsächlich am Kommunikationsvorgang beteiligt war. Der tatsächliche Benutzer ist

somit immer eine natürliche Person. Wenn die Behörde Auskunft zu jener natürlichen oder juristischen Person braucht, welcher ein Anschluss zurechenbar ist, erhält sie diese über die Teilnehmerkennung.

**Zu § 92 Abs. 3 Z 2b:**

Unter E-Mail Adresse ist jene Zeichenfolge zu verstehen, die zur Adressierung von E-Mails verwendet wird und sich aus einem lokalen Teil („local part“), dem Trennzeichen „@“ sowie einem globalen Teil („domain part“) nach dem Muster Benutzer@Domain.at zusammensetzt.

Auch wenn es sich bei der E-Mail Adresse grundsätzlich im Zusammenhang mit § 102a Abs. 4 um ein Verkehrsdatum handelt, ist nicht auszuschließen, dass sie Aufschluss über den Inhalt einer Nachricht geben kann. Beispielfhaft angeführt sei an dieser Stelle etwa die Adressierung „hilfe@krebskrank.at“, die direkte, sehr wahrscheinlich zutreffende Rückschlüsse auf den Inhalt einer Nachricht, nämlich den Gesundheitszustand einer Person, zulässt. Insofern besteht ein qualitativer Unterschied zwischen dem Verkehrsdatum E-Mail-Adresse und z. B. dem Verkehrsdatum Telefonnummer, der in die Beurteilung der Zulässigkeit einer Datenverarbeitung bei der Abwägung der Verhältnismäßigkeit einfließt.

**Zu § 92 Abs. 3 Z 3:**

Die Änderungen in dieser Bestimmung dienen ausschließlich der begrifflichen Ausdehnung auf juristische Personen, die von der bisherigen Regelung formal nicht erfasst waren, deren Daten jedoch schon bisher im obigen Sinne gehandhabt wurden.

**Zu § 92 Abs. 3 Z 6a:**

Soweit Daten erzeugt und verarbeitet werden, sind diese Daten bei aktiven und passiven Verbindungsherstellungen vorhanden.

Die Angabe der Standortkennung erfolgt bei der Auskunft unter Angabe von Geo-Koordinaten des Standortes der Funkzelle. Siehe dazu die Erläuterungen zu § 90 Abs. 8.

**Zu § 92 Abs. 3 Z 6b:**

Bei Vorratsdaten handelt es sich nicht um eine neue Kategorie von Daten im Sinne der im TKG bestehenden Unterteilung in Verkehrsdaten, Standortdaten, Inhaltsdaten und Stammdaten, die primär durch ihre faktische Funktion im Rahmen der Kommunikation (Nachrichtenübermittlung, Vertragsabwicklung etc.) abgegrenzt werden. Bei der Beurteilung, ob es sich bei einem Datum um ein Vorratsdatum handelt, ist vielmehr darauf abzustellen, ob es von Anbietern der in § 102a genannten Dienste ausschließlich aufgrund der Speicherverpflichtung des § 102a gesammelt bzw. gespeichert wird. Dabei ist zu beachten, dass auch beim Anbieter zunächst zu anderen Zwecken vorhandene Daten zu Vorratsdaten werden können, wenn alle anderen zulässigen Speicherzwecke (insbesondere die Betriebsnotwendigkeit der Speicherung) wegfallen. Die Einordnung von Daten als Vorratsdaten ist also durch den Zweck determiniert, zu dem die Daten gespeichert werden (dürfen).

Vorratsdaten umfassen bestimmte Standort- und Verkehrsdaten sowie mit den jeweiligen Kommunikationsvorgängen verbundenen Stammdaten, nicht aber Inhaltsdaten. Der Begriff „Vorratsdaten“ verdeutlicht explizit, dass die Speicherung der Daten für die in §102a Abs. 1 festgelegte Dauer ab ihrer Entstehung deshalb flächendeckend und vorrätig erfolgt, damit sie später den Strafverfolgungsbehörden zur Verfügung stehen, falls die Auskunft zu bestimmten Daten einer Nachrichtenübermittlung in einem bestimmten Verfahren zur Ermittlung, Feststellung und Verfolgung einer bestimmten Straftat, deren Schwere eine Auskunft nach § 135 Abs. 2a StPO rechtfertigt, notwendig ist. Die vorrätige Datensammlung selbst erfolgt also zunächst unabhängig von einem konkreten Verdacht gegen bestimmte Personen oder wegen bestimmter strafbarer Handlungen; alle auf solcherart gespeicherten Daten sind zunächst von potentiell gleichem Nutzen und müssen daher vorrätig gehalten werden, da eine allfällige spätere Verwendung noch nicht absehbar ist, zugleich aber sichergestellt werden muss, dass für den Fall einer zulässigen strafgerichtlichen Anfrage die benötigten Daten vorhanden sind.

Entsprechend dem Grundsatz des § 96, wonach Stammdaten, Verkehrsdaten und Standortdaten nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden dürfen, enthält das TKG durch die TKG-Novelle 2010 eine abschließende Aufzählung der zulässigen Zwecke, für die Daten im Zusammenhang mit Kommunikationsdiensten gespeichert und verwendet werden dürfen (siehe dazu auch die Erläuterungen zu § 99).

**Zu § 92 Abs. 3 Z 8:**

Die vorgeschlagene Änderung berücksichtigt die technische Möglichkeit von Konferenzschaltungen und passt die Bestimmung an die Legaldefinition des § 3 Z 16 an, bringt darüber hinaus aber keine Änderung des Begriffes.

**Zu § 92 Abs. 3 Z 8a:**

Die Definition wurde wortlautgetreu aus der RL 2006/24/EG übernommen und ist notwendig, weil sich die Speicherpflichten gem. § 102a auch auf die genannten erfolglosen Anrufversuche beziehen. Hierzu ist festzuhalten, dass das Kommunikationsgeheimnis des § 93 TKG ausdrücklich auch die dabei entstehenden Daten erfasst und der Gesetzgeber den Schutz damit ganz bewusst ausgeweitet hat, obwohl gar kein Kommunikationsvorgang im engen Sinn vorliegt, sondern nur Verkehrsdaten selbst den Inhalt der Kommunikation darstellen. So erhält beispielsweise ein Teilnehmer auf seinem Mobiltelefon die Information „Vermisste Anrufe, Datum, Uhrzeit ...“. Auch diese Information ist bereits eine Art der Nachrichtenübermittlung.

**Zu § 92 Abs. 3 Z 10:**

Die Änderung beinhaltet nur die Ersetzung des Punktes durch einen Strichpunkt am Ende, weil die Aufzählung mit neuen Begriffsdefinitionen fortgesetzt wird. Zur besseren Lesbarkeit wird der Text jedoch wiedergegeben.

**Zu § 92 Abs. 3 Z 11:**

Die Einteilung des Ablagesystems in verschiedene Unterordner (z. B. Aufteilung in Posteingang, gesendete Objekte, Entwürfe etc.) ist davon nicht umfasst.

**Zu § 92 Abs. 3 Z 12:**

Die Definition erfasst sowohl „klassisches“ E-Mail als auch Webmail, soweit dabei Übermittlungen auf Basis des „Simple Mail Transfer Protocol“ (SMTP) stattfinden. Die Übertragung ist im Standard RFC 821 (SMTP-Definition) und darauf aufbauenden RFCs definiert.

**Zu § 92 Abs. 3 Z 13:**

Diese Bestimmung enthält eine Klarstellung im Sinne der Rechtssicherheit. Ein Internet-Telefondienst ist als Unterfall des technologieneutralen Begriffs des „öffentlichen Telefondienstes“ iSd § 3 Z 16 zu verstehen. Im Sinne der Richtlinien für Anbieter von Voice over IP (VoIP) Diensten der RTR ist Internet-Telefondienst als Voice over IP (VoIP) Klasse A zu verstehen. Soweit die Verbindung mit denselben Vermittlungsmöglichkeiten wie das leitungsvermittelte Telefonsystem auch paketvermittelt bereitgestellt wird, fällt auch ein solches System unter diese Definition (Stratil, Kommentar 2004 zu § 3 TKG). Der Internet-Telefondienst erfasst damit all jene Voice over IP (VoIP) Dienste, die bereits jetzt dem TKG unterliegen. Die Definition dieses Begriffes ist geboten, weil sich die Speicherpflichten nach § 102a Abs. 3 auch auf Internet-Telefondienste beziehen.

Die Zusammenfassung von Voice over IP (VoIP) mit herkömmlicher Telefonie wird auch von der ERG empfohlen (Technologieneutralität, ERG (07) 56rev2). Eine neue Definition „Telefondienst“ ist zur Umsetzung der RL 2006/24/EG darüber hinaus nicht notwendig, da keine Abweichung vom Begriff „öffentlicher Telefondienst“ in § 3 Z 16 TKG vorliegt (siehe die Erläuterungen zu § 3 Z 16, der die erweiterte Definition nach der UniversaldienstRL 2002/22/EG, Art. 2 c mit einschließt).

**Zu § 92 Abs. 3 Z 16:**

Öffentliche IP-Adressen sind nur solche, die aus einem Adressblock aus dem sog. Provider Aggregatable Address Space (PA-Space) einem ISP zugewiesen und von diesem an seine Kunden weitergegeben wurden. Der Begriff „Rechner“ ist in diesem Zusammenhang weit zu verstehen und bezeichnet jedes Gerät, welches zur selbständigen Kommunikation über ein IP-Netzwerk auf der Ebene des Internet-Protokolls fähig ist, wie beispielsweise ein Router.

IP-Adressen, unabhängig davon, ob sie dynamisch oder statisch vergeben werden, sind erforderlich für den Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen. Aus der Sicht des technischen Kommunikationsprozesses sind IP-Adressen daher jedenfalls immer Zugangsdaten im Sinne des § 92 Abs. 3 Z 4a TKG. Zugleich kann es aber auch sein, dass IP-Adressen für die Begründung und die Abwicklung sowie die Änderung und Beendigung der Rechtsbeziehung zwischen dem Teilnehmer und dem Anbieter relevant sind. Das ist dann der Fall, wenn sog. statische IP-Adressen vertraglich einem Teilnehmer zur ausschließlichen Nutzung individuell dauerhaft zugewiesen werden. Nur in diesem Fall handelt es sich bei der IP-Adresse auch um ein Stammdatum. Ihre Verknüpfung mit anderen Stammdatums ist ohne Auswertung von Verkehrsdaten möglich.

Auch wenn die IP-Adresse – insbesondere im Hinblick auf Internet-Telefonie – ähnliche Funktionen erfüllen kann, handelt es sich dabei nicht um eine mit einer Telefonnummer gleichzusetzende Teilnehmernummer. Insbesondere ist nicht verifizierbar, ob ein Datenpaket tatsächlich von der vorgeblichen IP-Adresse stammt. So kann beispielsweise beim Versenden von Datenpaketen

vorgetauscht werden, mit der IP-Adresse eines anderen Kunden den Datenverkehr zu verursachen. Außerdem hat bei dynamischen IP-Adressen der Teilnehmer im Gegensatz zur Telefonnummer keine Kontrolle darüber, welche IP-Adresse ihm für die jeweilige Zugangsverbindung zugeteilt wird. Nur mit tiefer gehenden technischen Kenntnissen kann er sich diese Information jeweils am eigenen Rechner beschaffen. Schließlich besteht im Gegensatz zur Telefonnummer keine Möglichkeit, die Sichtbarkeit der IP-Adresse nach außen bei einem Kommunikationsvorgang zu unterdrücken. Die Vergleichbarkeit mit Telefonnummern ist also wirklich nur in jenen Ausnahmefällen gegeben, in denen eine bestimmte IP-Adresse unmittelbar im Vertrag einem bestimmten Teilnehmer zugewiesen wird. Dann ist eine Beauskunftung allein aufgrund einer Einsichtnahme in die Stammdaten möglich, ohne hierzu Zugangsdaten-Logfiles auswerten zu müssen. Damit sind IP-Adressen nicht automatisch zugleich Stammdaten, auch wenn sie rein technisch statische IP-Adressen sind, also nicht ständig neu (dynamisch) zugewiesen werden. Kriterium ist lediglich, ob sie ausdrücklich Bestandteil des Vertrages geworden sind. Vertragsbestandteil muss dabei eine bereits konkrete IP-Adresse sein. Vertragskonstruktionen, die einem Kunden zwar die technische Zuordnung einer statischen IP-Adresse zusichern, dabei aber nicht festlegen, welche IP-Adresse zugeordnet wird, begründen keine Stammdateneigenschaft einer sodann vergebenen IP-Adresse. Der Unterschied liegt vor allem darin begründet, dass solche Konstruktionen lediglich darauf abzielen, das Protokoll der technischen Zuordnung zu fixieren, aber keinen ausschließlichen Nutzungsanspruch für die Vertragsdauer an einer bestimmten IP-Adresse begründen und diese damit nicht für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Teilnehmer und dem Anbieter notwendig ist. Der Anbieter darf also bei Vorliegen sachlicher Gründe - etwa einer Reorganisation seiner Adressbereiche - und unter rechtzeitiger Ankündigung auch während der laufenden Vertragsdauer durchaus eine andere IP-Adresse zuweisen, solange die Zuweisung technisch weiterhin statisch bleibt. In den Fällen der vertraglichen Zuweisung einer bestimmten IP-Adresse ist eine solche Vorgehensweise zivilrechtlich nur mit Zustimmung des Kunden zulässig.

**Zu § 93 Abs. 3:**

Diese Änderung stellt ausdrücklich klar, dass die Kommunikationsüberwachung nach der StPO eine zulässige Durchbrechung des Kommunikationsgeheimnisses darstellt. Der Begriff „Fangschaltung“ bleibt neben der ausdrücklichen Erwähnung der „Überwachung von Nachrichten“ enthalten, weil er in §106 enthalten ist und für die Anbieter klarstellt, dass jeweils nach Implementierung der Fangschaltung eine Auswertung von Verkehrsdaten zulässig ist, um die Identität des Anrufers gegen dessen Willen festzustellen. Für die Fälle einer zulässigerweise eingerichteten Fangschaltung bleibt die damit verbundene Aufzeichnung von Verkehrsdaten eine zulässige Durchbrechung des Kommunikationsgeheimnisses. Ebenso bleibt eine die Überwachung von Nachrichten begleitende Feststellung von Standortdaten weiterhin zulässig.

**Zu § 93 Abs. 5:**

Diese Bestimmung stellt eine Schutznorm in Ergänzung des Kommunikationsgeheimnisses dar und trägt den massiven und mehrfach öffentlich geäußerten Bedenken sämtlicher Berufsgruppen mit gesetzlichen Verschwiegenheitsverpflichtungen und besonderen Vertrauensverhältnissen Rechnung. Gleichzeitig ist dieses Umgehungsverbot auch durch Bestimmungen in der StPO (insbesondere §§ 144 und 157) abgesichert, was aber, wie Diskussionen mit den betroffenen Gruppen im Entstehungsprozess der Novelle verdeutlichen, im Bewusstsein der genannten Berufsgruppen zum Teil wenig verankert ist. Es wird daher klargestellt, dass es nicht den Anbietern obliegt, zu beurteilen, ob eine solche Umgehung vorliegt. Vielmehr muss stets das Gericht bzw. der Rechtsschutzbeauftragte die letzte Entscheidung treffen, zumal eine berufliche Verschwiegenheitspflicht die Ermittlungsmaßnahme nicht verhindert, wenn der Träger dieser Pflicht selbst einer entsprechenden Straftat dringend verdächtig ist. Diese Regelung steht auch im Einklang mit der ständigen Rechtsprechung des EGMR (zB. EGMR RS Kopp gg Schweiz, Urteil vom 25.3.1998, Recueil des arrêts et décisions 1998-II, deutsch in ÖJZ 1999, 115; eine systematische Aufarbeitung dieser Rechtsprechung ist zu finden bei: Dean Spielmann, Das anwaltliche Berufsgeheimnis in der Rechtsprechung des EGMR, Österreichisches Anwaltsblatt 2010/07-08, 346ff; der Autor ist seit 2004 Richter am EGMR).

Von einer Ausnahme von der Auskunft über Verkehrsdaten betreffend solche besonders geschützten Gruppen, wie sie im Begutachtungsverfahren gefordert wurde und auch im Urteil des deutschen Bundesverfassungsgerichts zu BVerfG, 1 BvR 256/08 vom 2.3.2010 zur dortigen Umsetzung der Vorratsdatenspeicherungsrichtlinie ohne tiefere Auseinandersetzung mit der hier dargestellten Problematik gefordert wurde, wird daher bewusst abgesehen. Denn selbst wenn die Ausnahme zunächst die Datenauskunft verhindern würde, würde aus den genannten Gründen stets dem Gericht die letzte Entscheidung obliegen, solche Daten dennoch anzufordern, selbst wenn ein Berufsgeheimnis einer solchen Auskunft prima vista entgegenstünde. Der einzige Vorteil eines grundsätzlichen Übermittlungsverbotes würde darin liegen, die Aufmerksamkeit des Gerichts auf die Tatsache einer



bestehenden beruflichen Verschwiegenheitspflicht zu konzentrieren, was aber im Gerichtsverfahren auch durch die Betroffenen selbst spätestens im Rechtsmittelverfahren wahrgenommen werden kann. Diesem möglichen Mehrwert von Ausnahmen zur Auskunft stünde aber ein gewichtiger Datenschutzrechtlicher Nachteil gegenüber. Denn die Umsetzung eines Übermittlungsverbotes würde eine Liste bedingen, die als eine Art „Whitelist“ alle Mitglieder solcher Gruppen (Ärzte, Seelsorger, Journalisten, Psychosoziale Beratungsdienste, Anwälte, Bewährungshelfer,...) zentral und behördlich mit Namen, Anschrift und allen Teilnehmernummern erfassen müsste und den Anbietern zur Verfügung zu stellen wäre. Abgesehen von den Schwierigkeiten, diese Liste überhaupt zu erstellen und aktuell zu halten, wäre diese Liste aus der Perspektive des Datenschutzes für sich eine weitere nicht zu unterschätzende Risikoquelle. Im Übrigen ist diese Problematik nicht neu sie besteht vielmehr, seit es die Auskunftspflicht über Verkehrsdaten an Gerichte gibt. Durch die Vorratsdatenspeicherung wird das Problem allenfalls verstärkt.

**Zu § 94 Abs. 1:**

Diese Änderung ist als Anpassung an die aktuellen Bestimmungen des neuen TKG, der neuen StPO sowie des SPG erforderlich, da in den jeweils alten Fassungen unter „Überwachung einer Telekommunikation“ sowohl die Inhaltsüberwachung als auch die „Auskunft über Daten einer Nachrichtenübermittlung“, somit also die Verkehrs- und Standortdatenauskunft, subsumiert wurde. Durch die ausdrückliche Nennung der „Auskunft über Vorratsdaten“ wird klargestellt, dass die Bereitstellungspflicht sowie der Kostenersatz auch für jene Einrichtungen gilt, die bisher nicht gespeicherte Daten, die nunmehr aufgrund der Umsetzung der RL 2006/24/EG speicherungspflichtig sind, betreffen. In diesem Zusammenhang wird auf die Erläuterungen zu § 92 Abs. 3 Z 6b verwiesen, wonach Vorratsdaten keine eigene Kategorie von Daten darstellen, sondern lediglich auf die Rechtsgrundlage der Speicherung abzustellen ist.

Bei den Regelungen zum Kostenersatz wird den Vorgaben des VfGH-Erkenntnisses vom 27.02.2003 zu GZ 37/02 ua (VfSlg 16.808) Beachtung geschenkt. Der VfGH hat mit diesem Erkenntnis die Überwälzung aller Kosten für die Bereitstellung von Überwachungseinrichtungen durch den Ausschluss eines Kostenersatzes an die Telekommunikationsbetreiber für verfassungswidrig erklärt.

**Zu § 94 Abs. 2:**

Die Ergänzung der Bestimmung um die „Auskunft über Vorratsdaten“ stellt klar, dass auch für derartige Auskünfte eine Mitwirkungspflicht besteht sowie Kostenersatz zu leisten ist. Da es sich bei Vorratsdaten grundsätzlich um Verkehrs-, Standort- und Stammdaten handelt (siehe dazu die Erläuterungen zu § 92 Abs. 3 Z 6b), gilt wie bisher die bereits aufgrund dieser Vorschrift erlassene Überwachungskostenverordnung, unabhängig davon, ob die übermittelten Datensätze Vorratsdaten beinhalten oder nicht.

**Zu § 94 Abs. 3:**

Die Änderung in diesem Absatz beschränkt sich auf die notwendige Anpassung an die differenzierte Terminologie der neuen StPO und ersetzt daher „Überwachung einer Telekommunikation“ durch „Überwachung von Nachrichten“. Die Regelung zur „Auskunft über Daten einer Nachrichtenübermittlung“ einschließlich Vorratsdaten erfolgt differenziert im neuen Abs. 4.

**Zu § 94 Abs. 4:**

Die Bestimmung identifiziert die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten. Die Übertragungstechnologie, welche durch eine Verordnung („Technische Richtlinie“) nach dieser Bestimmung zu konkretisieren ist, soll durch sichere „Identifikation und Authentifizierung von Sender Empfänger“ sicherstellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht. Dabei muss auf technischer Ebene die Datenintegrität gewahrt sein, das bedeutet, dass jede allfällige Veränderung der übermittelten Daten auf dem Übertragungsweg für den Empfänger sofort identifizierbar wäre und dieser sich damit auf die Richtigkeit der Daten nicht mehr verlassen darf. Die Formulierung „unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie“ (im Gegensatz zur Fassung im ursprünglichen Begutachtungsentwurf vom Dezember 2009 „Übertragung per E-Mail“) ist eine Ergänzung zur Erfüllung anspruchsvoller Datensicherheitsstandards, wie sie insbesondere im Urteil des deutschen Bundesverfassungsgerichts zu BVerfG, 1 BvR 256/08 vom 2.3.2010 beschrieben werden. Die Formulierung lässt genügend Spielraum, die nähere technische Ausgestaltung durch Verordnung zu regeln und stellt gleichzeitig einen Auftrag an den Ordnungsgeber dar. Die gesetzlich vorgezeichneten Indikatoren sind dabei technologieneutral formuliert. Wesentlich ist, dass die eingesetzte Technologie den Zielvorgaben entspricht. Ob dafür symmetrische oder asymmetrische Verschlüsselungsverfahren zum Einsatz kommen hängt letztlich von der gesamten Sicherheitsarchitektur ab und bleibt Gestaltungsspielraum des Ordnungsgebers. Als

Minimalvariante möglich wäre beispielsweise eine verschlüsselte Übertragung per E-Mail unter Verwendung des Standards 'Secure/Multipurpose Internet Mail Extensions (S/MIME)'. S/MIME ist ein Standard für die Verschlüsselung und Signatur von MIME-gekapselten E-Mails durch ein asymmetrisches Kryptosystem. S/MIME definiert zwei Content-Types für MIME: das Multipart/Signed-Format zur Signierung einer E-Mail und das Multipart/Encrypted-Format zu deren Verschlüsselung. S/MIME wird von den meisten modernen Mailclients unterstützt und erfordert X.509-basierte Zertifikate für den Betrieb.

Das Dateiformat CSV beschreibt den Aufbau einer Textdatei zur Speicherung oder zum Austausch einfach strukturierter Daten. Die Dateiergung CSV ist eine Abkürzung für „Comma-Separated Values“. Das Dateiformat CSV wird im RFC 4180 grundlegend beschrieben. Die Normierung dieses Dateiformats bei gleichzeitig eindeutiger Definition der Datenfelder in der technischen Richtlinie hat den großen Vorteil völliger Technikneutralität, das heißt, dass weder die Anbieter noch die staatlichen Stellen, an welche die Daten übermittelt werden, an besondere technische Voraussetzungen gebunden sind. CSV-Dateien können von allen gängigen Datenbanksystemen verwendet werden. Diese Lösung stellt daher überdies die geringste Kostenbelastung dar.

Ausdrücklich gesetzlich gefordert ist eine Verschlüsselung bei der Übermittlung. Davon ausgenommen sein soll die Übermittlung von Daten in Notfällen. In diesen Fällen soll daher die bisher praktizierte Übermittlungsform beibehalten werden, also Auskünfte per Telefon oder Fax. Die weiteren Ausnahmen vom Grundsatz der Übermittlung in einem CSV File berücksichtigen die in der Praxis wichtigen Fälle, in denen aufgrund der besonderen Dringlichkeit (insbesondere bei Standortdatenauskünften, etwa zur Lebensrettung oder bei zeitkritischen Observationen) dieses Verfahren nicht zweckmäßig wäre. Außerdem sind die sogenannten „S-Records“ (das sind die begleitenden Verkehrsdaten bei einer Inhaltsüberwachung von Telefongesprächen) berücksichtigt, welche über eine besondere technische Schnittstelle gemeinsam mit der Inhaltsüberwachung abgewickelt werden.

Der Spielraum für eine nach dieser Bestimmung zu erlassenden Verordnung ist eng determiniert. Die technische Richtlinie soll für alle Anbieter einheitlich definieren, welche der zu beauskunftenden Werte an welcher Stelle innerhalb der CSV-Datei zu stehen haben und welche Zeichensätze dabei zu verwenden sind. Klar festgelegt ist auch, dass eine Übermittlung der Daten unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie zu erfolgen hat. Zur weiteren Verbesserung des Sicherheitsstandards kann eine asymmetrische Verschlüsselung vorgeschrieben werden. Hier sind allenfalls die näheren technischen Details zur Public Key Infrastructure zu definieren. Kein Platz besteht für Vorschriften, bestimmte Programme zu verwenden oder gar eine komplexe Schnittstelle wie beispielsweise den ETSI-Standard zur Vorratsdatenspeicherung vollständig zu normieren.

Die Verwendung des Begriffs „Übermittlung“ von Auskünften legt fest, dass solche Auskünfte in jedem Fall durch aktives Handeln des Anbieters an die Behörden weitergegeben werden und kein System geschaffen wird, mit dem Zugriffe auf die Daten ohne Mitwirkung des Anbieters im Einzelfall ermöglicht werden. Die Konzeptionierung der Datenauskünfte als „push“ und nicht als „pull“ System ist dabei verfassungsrechtlich geboten. Da nämlich das auf die gegenständlichen personenbezogenen Daten anwendbare Grundrecht auf Datenschutz in § 1 Abs. 5 DSGVO eine sog. unmittelbare Drittwirkung normiert, steht die rechtliche Verantwortung, welche die Anbieter gegenüber ihren Kunden haben, dem einfachen Gesetzgeber nicht beliebig zur Disposition. Ein System, durch welches die Anbieter als datenschutzrechtliche Auftraggeber überhaupt keine Kontrolle mehr über die Verwendung der Daten ihrer Kunden haben, steht dieser im Verfassungsrang verankerten Verantwortung entgegen. Aus diesem Grund kommt auch eine einfachgesetzliche Normierung einer zentralen Speicherung sämtlicher Vorratsdaten aller Anbieter auf einem staatlichen Datenbanksystem nicht in Frage. Eine solche zentrale Speicherung aller Vorratsdaten würde zugleich bedeuten, dass sämtliche Daten aller Kunden verdachtsunabhängig stets zur Verfügung stünden und nicht nur für den Fall eines tatsächlichen Verdachts im Zusammenhang mit der Verfolgung einer Straftat, deren Schwere eine Auskunft nach § 135 Abs. 2a StPO rechtfertigt, im Einzelfall. Daten durch sogenanntes „Data-Mining“<sup>13</sup> mit anderen Informationen automatisiert zu verknüpfen ist nach dem strengen datenschutzrechtlichen Zweckbindungsgrundsatz (Art. 6 Abs. 1 lit. b DSGVO) unzulässig. Eine dezentrale Speicherung der Vorratsdaten bei den Anbietern bietet insofern einen effektiven Schutz vor einer extensiven Verwendung der vorrätig gesammelten Datenmengen. Dass die Daten über verschiedene Anbieter „verstreut“ sind und nur mit deren Mitwirkung zur Verfügung stehen, bedeutet eine nicht unwesentliche Hemmschwelle.

<sup>13</sup> Dazu ausführlich Nathan Eagle, Alex Pentland, David Lazer, Inferring Social Network Structure using Mobile Phone Data, Proceedings of the National Academy of Sciences 2007.

Die Bestimmungen zur Datensicherheit und zur Übermittlung nach diesem Absatz sind sowohl für den Ersatz der Investitionskosten nach § 94 Abs. 1 als auch für den Ersatz der laufenden Kosten für Datenauskünfte nach § 94 Abs. 2 relevant. Das tatsächliche Ausmaß sowohl für die Investitionskosten als auch die laufenden Kosten hängt aber wesentlich davon ab, wie die konkrete Ausgestaltung durch die Verordnung nach diesem Absatz beschaffen ist.

**Zu § 97 Abs. 1:**

Die Ergänzungen nehmen auf die Änderungen in den §§ 90 und 96 Bedacht.

**Zu § 98 Abs. 1:**

Die Änderung beschränkt sich auf die Neubezeichnung des bestehenden § 98 als § 98 Abs. 1.

**Zu § 98 Abs. 2:**

Die aktuelle Standortfeststellung des Endgeräts erfolgt regelmäßig durch eine sog. „stille SMS“ und daher grundsätzlich ohne Verarbeitung von gespeicherten Verkehrsdaten. Nur wenn eine Feststellung des aktuellen Standorts nicht möglich ist, etwa weil die Endeinrichtung zum Zeitpunkt der versuchten Standortfeststellung nicht (mehr) in Betrieb ist, ist eine Auswertung des letzten bekannten Standorts der Endeinrichtung notwendig. Allein aus diesem Grund ist der Rückgriff auf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang dieser Endeinrichtung zulässig, dann aber auch notwendig und verhältnismäßig. Weil Standortdaten für Betriebszwecke des Anbieters regelmäßig keine Funktion erfüllen und daher ab ihrer Speicherung künftig als Vorratsdaten gemäß § 102a Abs. 3 Z 6 lit. d vorhanden sind, wird hier wie auch in § 99 Abs. 5 Z 3 eine auf den letzten Kommunikationsvorgang eingeschränkte und damit eng gefasste Ausnahme von der grundsätzlich strengen Zweckbindung des § 102a Abs. 1 normiert. Aus Sicht der Praxis wird in diesen Fällen regelmäßig nicht zwingend der Notruf selbst der letzte Kommunikationsvorgang sein.

Schließlich wird normiert, dass der Anbieter den Teilnehmer über die Erteilung einer Auskunft an Notrufträger zu informieren hat. Diese Bestimmung wird weiter ausgestaltet durch Regelungen über den Zeitraum, in welchem die Information stattzufinden hat, sowie über Form und Inhalt der Information.

**Zu § 99 Abs. 1:**

Aus der Sicht der Anbieter als die primären Adressaten des TKG müssen im Sinne des Datenschutzrechtlichen Transparenzgrundsatzes die Fälle der Datenverwendung im TKG geregelt sein. Eine Nachschau im TKG muss dem Anbieter Rechtsklarheit bieten, welche Datenverwendungen zulässig sind. Davon bleibt unberührt, wie Verkehrsdaten durch die Strafverfolgungsbehörden weiter verwendet werden, nachdem sie nach § 99 Abs. 5 TKG zulässigerweise beauskunftet wurden. Durch Ersetzung des Wortes „gesetzlich“ durch die Wortfolge „in diesem Gesetz“ wird klargestellt, dass die rechtliche Zulässigkeit und damit auch die Zwecke der Speicherung von Verkehrsdaten im TKG abschließend geregelt werden sollen. Insbesondere soll dadurch die Rechtssicherheit geschaffen werden, dass aus materiellen Auskunftsansprüchen in anderen Materiengesetzen keine implizite Berechtigung oder gar Verpflichtung zur Speicherung von Verkehrsdaten abgeleitet werden kann. Die Bestimmung folgt damit den klaren Vorgaben des Beschlusses des VfGH vom 1.7.2009, GZ G 147,148/08-14 sowie auch der Entscheidung des OGH vom 14.7.2009, GZ 4 Ob 41/09x.

Diese Entscheidungen heben zentral den datenschutzrechtlichen Grundsatz hervor, dass die Speicherung von personenbezogenen Daten einer ausdrücklichen und klaren gesetzlichen Bestimmung bedarf, die auch eindeutige Zwecke erkennen lässt. Dass eine bestehende materielle Auskunftspflicht eine Berechtigung bzw. Verpflichtung zur Speicherung bloß impliziert, genügt diesem Bestimmtheitsgebot nicht. Deshalb werden nunmehr im TKG die gesetzlichen Grundlagen für die Speicherung von Daten geschaffen, mit denen Bestimmungen zur Auskunft oder sonstigen Verwendung korrespondieren sollen.

**Zu § 99 Abs. 5:**

§ 99 Abs. 5 erfüllt im Zuge der Umsetzung der Vorratsdatenspeicherung zwei wesentliche Funktionen: Einerseits soll damit aufgrund der Aufzählung der zulässigen Fälle einer Übermittlung von Verkehrsdaten zu Auskunftszwecken im TKG sichergestellt werden, dass Auskünfte über gemäß § 99 Abs. 2 gespeicherte Daten (sogenannte „Billingdaten“) wie bisher an die Strafverfolgungsbehörden nach der StPO bzw. an die Sicherheitsbehörden nach dem SPG beauskunftet werden können. Andererseits wird damit die von Art. 11 der Vorratsdatenspeicherungsrichtlinie 2006/24/EG durch Ergänzung des Art. 15 der E-Privacy Richtlinie 2002/58/EG eröffnete Möglichkeit genutzt, die Verwendung von Vorratsdaten in eingeschränktem Ausmaß unter Wahrung der Verhältnismäßigkeit über den Zweck der „Ermittlung, Feststellung und Verfolgung schwerer Straftaten“ (Art. 1 RL 2006/24/EG) hinaus vorzusehen.

**Zu § 99 Abs. 5 Z 1:**

Diese Bestimmung stellt sicher, dass gemäß § 99 Abs. 2 gespeicherte Daten (sogenannte „Billingdaten“) wie bisher im Rahmen der „Auskunft über Daten einer Nachrichtenübermittlung“ gemäß § 134 Z 2 StPO an die nach der StPO zuständigen Organe bei Vorliegen der entsprechenden formellen Voraussetzungen übermittelt werden.

**Zu § 99 Abs. 5 Z 2:**

Die Bestimmung regelt die Auskunft über Zugangsdaten, namentlich IP-Adressen (§ 102a Abs. 2 Z 1), IMSI und IMEI (§ 102a Abs. 3 Z 6 lit. a und b) sowie Email Adressen (§ 102a Abs. 4 Z 1, 2, 3 und 5). Auskünfte über E-Mail Adressen nach dieser Ziffer sind auf § 102a Abs. 4 Z 1, 2, 3 und 5 eingeschränkt. Das bedeutet, dass die Ermittlungsbehörden nach dieser Ziffer feststellen können, welchem Teilnehmer eine E-Mail Adresse zu einem bestimmten, nicht länger als sechs Monate zurückliegenden Zeitpunkt zugewiesen war. Diese Information ist dann nötig, wenn der ermittlungsrelevante E-Mail Verkehr selbst schon bekannt ist, etwa wenn ein E-Mail mit Drohungen Anlass für die Ermittlungen gibt. Wenn den Ermittlungsbehörden ein solches E-Mail in elektronischer Form vorliegt, kann der Anbieter die benötigte Information durch Auswertung der Daten nach § 102a Abs. 4 Z 1 und 2 ermitteln, liegt das E-Mail hingegen nur z.B. als Ausdruck auf Papier vor, werden zusätzlich die Daten nach Z 3 leg. cit. benötigt. Die Daten nach Z 5 leg. cit. sind schließlich dann nötig, wenn sich eine Anfrage im genannten Sinn auf die Nutzung eines Webmail Service bezieht. Die Ausforschung eines noch nicht bekannten E-Mail Verkehrs, wofür sämtliche Daten nach § 102a Abs. 4 Z 1 bis 5 notwendig sind, ist für den „niederschweligen Bereich“, also unterhalb einer Straftat deren Schwere eine Auskunft nach § 135 Abs 2a StPO rechtfertigt, unzulässig. Dies wäre eine „Auskunft über Daten einer Nachrichtenübermittlung“ und fällt damit - weil E-Mail Daten immer Vorratsdaten sind - unter die neue Bestimmung des § 134 Z 2a StPO. Aus diesem Grund sind die für diesen Zweck zulässig verfügbaren Daten auch auf das unbedingt erforderliche Ausmaß eingeschränkt.

Auskünfte über Name und Anschrift eines Teilnehmers, dem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, werden aus Sicht der Ermittlungen überhaupt nur dann begehrt, wenn das Ermittlungsinteresse darin besteht, einen bereits bekannten Kommunikationsvorgang (etwa das Verfassen oder Abrufen eines bestimmten Inhalts, die Nutzung eines bestimmten Dienstes etc.) einem bestimmten Teilnehmer zuzuordnen. Mit anderen Worten ist der Inhalt aufgrund vorhergehender Ermittlungsschritte bereits bekannt und soll letztlich einer Person zugeordnet werden. Wenngleich die Auswertung der Zugangsdaten (der IP-Adressen Logfiles) beim Provider erfolgt und das Ergebnis der Auskunft in der Übermittlung von Name und Anschrift besteht, steht die Ermittlungsmaßnahme damit einer Verkehrsdaten- bzw. Inhaltsüberwachung näher als einer bloßen Stammdatenauskunft. Es gilt das Formerfordernis des § 76 a iVm § 102 StPO.

**Zu § 99 Abs. 5 Z 3:**

Diese Bestimmung beinhaltet das ausnahmsweise Abgehen vom Grundsatz, dass Verkehrsdaten (egal, ob es sich dabei um Vorratsdaten oder solche Daten handelt, die nach § 99 Abs. 2 auch für Betriebszwecke gespeichert sein dürfen) nur bei Vorliegen einer richterlichen Bewilligung beauskunftet werden dürfen.

Der erste europäische Entwurf zur Vorratsdatenspeicherung sah neben der Verwendung zu repressiven Zwecken auch die Verwendung für präventive Zwecke vor. Der präventive Bereich, in Österreich also Datenauskünfte nach dem SPG, wurde für die geltende Fassung der RL 2006/24/EG gestrichen, nachdem das EU-Parlament massive Bedenken geäußert hatte, dass in diesem Bereich die Gefahren von Missbrauch erheblich größer seien als im Zuständigkeitsbereich der Gerichte. Durch die hier vorgeschlagene Regelung erhält die Sicherheitspolizei im Anwendungsbereich des SPG Zugriff auf die kurz oft als „Billingdaten“ bezeichneten, also betriebsnotwendigen Daten und damit auf all jene Daten, die schon bisher zulässigerweise gespeichert wurden. Sobald die Anbieter diese Daten selbst nicht mehr benötigen, sind sie nur noch als Vorratsdaten vorhanden und dürfen dann für keine anderen Zwecke als nach § 102a verwendet werden, also auch nicht mehr für eigene Zwecke. Für die Sicherheitspolizei bleibt der Zugriff auf alle Daten, die schon bisher zulässigerweise bei den Anbietern vorhanden waren, nach Maßgabe des § 53 Abs. 3a und 3b SPG. Damit korrespondiert die Regelung des § 102c Abs. 1, wonach die Speicherung der Vorratsdaten so zu erfolgen hat, dass eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist.

In jenen Fällen, in denen eine Verarbeitung von Verkehrsdaten zur Auskunft über Stammdaten zum Zweck der Abwehr einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen notwendig ist, handelt es sich regelmäßig um Fälle der ersten allgemeinen Hilfeleistungspflicht oder der akuten Verhinderung von Straftaten im Sinne des § 53 Abs 3a SPG. In solchen Zusammenhängen werden üblicherweise ohnehin Daten aus den „live-Systemen“ der Anbieter benötigt,

um auf eine gegenwärtige Gefahr reagieren zu können. Auskünfte über ältere Daten fallen zumeist in den Anwendungsbereich der Kriminalpolizei und haben daher nach den Regeln der StPO zu erfolgen.

Einen Sonderfall stellt die Auskunft über Standortdaten dar. Schon nach der bisherigen Bestimmung des § 53 Abs. 3b SPG dürfen die Sicherheitsbehörden nur die Standortdaten der gefährdeten Person selbst, nicht aber etwa jene des Verdächtigen, von dem die Gefahr möglicherweise ausgeht (z. B. eines mutmaßlichen Entführers) anfordern. Paradebeispiel ist – abgesehen vom Entführungsfall – der verunglückte Tourengänger. Die aktuelle Standortfeststellung des Endgeräts erfolgt regelmäßig – wie bereits zu § 98 Abs. 2 ausgeführt – durch eine sog. „stille SMS“ und daher grundsätzlich ohne Verarbeitung von gespeicherten Verkehrsdaten. Nur wenn eine Feststellung des aktuellen Standorts nicht möglich ist, etwa weil die Endeinrichtung zum Zeitpunkt der versuchten Standortfeststellung nicht (mehr) in Betrieb ist, ist eine Auswertung des letzten bekannten Standorts der Endeinrichtung notwendig. Allein aus diesem Grund ist der Rückgriff auf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang dieser Endeinrichtung zulässig. Weil Standortdaten für Betriebszwecke des Anbieters regelmäßig keine Funktion erfüllen und daher ab ihrer Speicherung nur als Vorratsdaten gemäß § 102a Abs. 3 Z 6 lit. d vorhanden sind, wird hier wie auch in § 98 eine auf den letzten Kommunikationsvorgang eingeschränkte und damit eng gefasste Ausnahme von der grundsätzlich strengen Zweckbindung des § 102a Abs. 1 normiert. Betreffend Standortdaten ist diese Bestimmung einerseits komplementär zur Auskunft an Notrufträger zu sehen, nämlich für jene Fälle, in denen gerade kein Notruf abgesetzt wurde (aber möglicherweise eine Verständigung durch Angehörige o.Ä. stattgefunden hat).

Wenn eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht, sind die Sicherheitsbehörden berechtigt, zur Hilfeleistung oder Abwehr dieser Gefahr von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) einer von der gefährdeten Person mitgeführten Endeinrichtung zu verlangen. Zugleich wird durch einen neuen § 53 Abs. 3c SPG die Pflicht der Sicherheitsbehörde zur nachweislichen Information der Betroffenen bei Standortdatenerfassung nach § 53 Abs. 3b SPG eingeführt, deren Einhaltung dem Rechtsschutzbeauftragten nach der ebenfalls neugefassten Bestimmung des § 91c SPG obliegt.

#### **Zu § 99 Abs. 5 Z 4:**

Die Ausführungen zu Abs. 5 Z 2 gelten sinngemäß.

#### **Zu § 102 Abs. 3:**

Neben der systematischen Klarstellung im neuen § 90 Abs. 8 wird hier das ausdrückliche Verbot normiert, kommunikationsunabhängige Bewegungsprofile zu ermitteln und zu speichern. Die Regelung ist insbesondere zur Klärung notwendig, dass auch die Umsetzung der RL 2006/24/EG die Erfassung solcher Standortdaten nicht erlaubt.

#### **Zu § 102a Abs. 1:**

Die Formulierung „nach Maßgabe der Abs. 2 - 4“ schließt „andere“ Anbieter als die von der RL 2006/24/EG anvisierten und in den Abs. 2 - 4 konkretisierten aus.

Obwohl die Richtlinie ausdrücklich auch Betreiber öffentlicher Kommunikationsnetze nennt, ist die Normierung der Speicherpflicht im Hinblick auf die Anbieter öffentlicher Kommunikationsdienste hinreichend. Es gibt nämlich hinsichtlich der zu speichernden Datenkategorien der Abs. 2 - 4 keine Fälle, in denen die Daten ausschließlich beim Netzbetreiber anfallen. Auch bei Wholesale-Kooperationen verfügt der Diensteanbieter über alle Daten, deren Speicherung vorgeschrieben ist. Diese Ausklammerung der Netzanbieter ist darüber hinaus auch aus ökonomischen Gründen sinnvoll, weil dadurch die Gefahr einer nach dem Erwägungsgrund 13 der RL 2006/24/EG zu vermeidenden Doppelspeicherung begrenzt wird.

Hinsichtlich der Speicherdauer für Vorratsdaten sieht die RL 2006/24/EG einen Zeitrahmen von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt des Kommunikationsvorganges vor.

Da bereits durch die Verpflichtung zur vorrätigen Speicherung der Daten in verfassungsgesetzlich gewährleistete Rechte der speicherpflichtigen Anbieter (siehe dazu die Erläuterungen zu § 91 Abs. 1) wie auch in weiterer Folge (durch die Speicherung) in jene der Benutzer dieser Dienste eingegriffen wird, ist bei der Normierung der Speicherdauer auf die Verhältnismäßigkeit der Maßnahme Bedacht zu nehmen.

In Anbetracht der Tatsache, dass es sich um eine verdachtsunabhängige Speicherung handelt und der Grundrechtseingriff für die Betroffenen daher besonders schwer wiegt, müsste ein überwiegendes öffentliches Interesse an einer längeren Speicherdauer bestehen, etwa ein belegbarer, nicht unwesentlicher

zusätzlicher Nutzen einer über die sechsmonatige Untergrenze hinausgehenden Speicherdauer. Im Hinblick auf den Nutzen von Verkehrsdaten hat schon zum Zeitpunkt der Entstehung der RL 2006/24/EG eine von der Wik Consult durchgeführte Studie<sup>14</sup> ergeben, dass sich zwischen 80 und 85% der Anfragen zu Verkehrsdaten durch Strafverfolgungsbehörden auf einen Zeitraum beziehen, der nicht länger als drei Monate zurückliegt. Eine 2005 im Auftrag des deutschen Bundeskriminalamtes durchgeführte Befragung innerhalb der Polizei zur Erhebung von Rechtsdefiziten im Bereich der Verkehrsdatenspeicherung<sup>15</sup> ergab zudem, dass unter Berücksichtigung der Notwendigkeit und Relevanz von Verkehrsdaten in verschiedenen Deliktsbereichen die gewünschte Speicherdauer sechs Monate beträgt.

Auch eine Erhebung der Europäischen Kommission<sup>16</sup> aus 2008 in Mitgliedsstaaten, die die RL 2006/24/ERG bereits umgesetzt hatten, ergibt, dass der weitaus größte Anteil an angefragten Vorratsdaten nicht älter als drei Monate ist. Gleichzeitig konnten Statistiken zum Beleg der Notwendigkeit der in der RL 2006/24/EG normierten Speicherdauer von mindestens sechs Monaten bislang nicht vorgewiesen werden.

Ganz im Gegenteil zeigt ein aktueller, sehr umfassender Forschungsbericht des Max-Planck-Instituts für ausländisches und internationales Strafrecht<sup>17</sup>, dass sich der überwiegende Anteil der Verkehrsdatenabfragen entweder auf einen Erhebungszeitraum von einem Tag oder von drei Monaten bezieht;<sup>18</sup> Dieser beginnt durchschnittlich 26 Tage vor dem Zeitpunkt der Anfrage, wobei etwa die Hälfte der Abfragen einen Zeitraum von lediglich vier Tagen oder weniger vor dem Anfragezeitraum betrifft<sup>19</sup>.

In der bisherigen österreichischen Praxis wurden von den Betreibern von Kommunikationsdiensten betriebsnotwendige Daten weitgehend für eine Dauer von sechs Monaten gespeichert und im Falle einer zulässigen Anfrage einer Strafverfolgungsbehörde beauskunftet. Dies ist insofern zu berücksichtigen, als eine Verlängerung der Speicherdauer gegenüber der bisherigen Speicherpraxis zu entsprechend höheren Kosten auf Seiten der speicherpflichtigen Anbieter führen würde<sup>20</sup>.

Im Hinblick auf die Intensität des Grundrechtseingriffs durch die Vorratsdatenspeicherung besteht kein überwiegendes Interesse an einer Verlängerung des bisherigen Speicherzeitraumes. Die Dauer der Speicherpflicht erfüllt mit sechs Monaten die Vorgaben der RL 2006/24/EG und ist im Hinblick auf sämtliche bisher vorliegende Statistiken ausreichend, um die angestrebten Zwecke der Strafverfolgung zu erfüllen. Da auch die Europäische Kommission aus den Erhebungen in den Mitgliedsstaaten, die die RL 2006/24/EG bereits umgesetzt haben, bislang keine fundierten Nachweise für die Effizienz der Richtlinie vorlegen konnte und sich nach bisherigen Statistiken der weit überwiegende Anteil der polizeilichen Anfragen auf Daten bezieht, die jünger als sechs Monate sind und damit außerhalb des von der Richtlinie vorgegebenen Speicherzeitraumes liegen, wäre die Normierung einer längeren Speicherdauer im Hinblick auf den tatsächlichen Nutzen unverhältnismäßig.

#### **Zu § 102a Abs. 2 Z 1:**

Eine Speicherpflicht bezüglich IP-Adressen trifft jenen öffentlichen Internet-Zugangsdiensteanbieter (Access-Provider), dem die Verwaltung der jeweiligen öffentlichen IP-Adressen von der zuständigen IP-

14 Franz Büllingen, Aurélie Gillet, Christin-Isabel Gries, Annette Hillebrand, Peter Stamm, Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich. Studie für die BITKOM Servicegesellschaft mbH, Bad Honnef, Februar 2005 (erhältlich unter <http://www.wik.org>).

15 Eva Mahnken, Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten. Rechtsstatsachen zum Beleg der defizitären Rechtslage, Bundeskriminalamt, Wiesbaden, November 2008 (erhältlich unter [http://www.vorratsdatenspeicherung.de/images/bka\\_vorratsdatenspeicherung.pdf](http://www.vorratsdatenspeicherung.de/images/bka_vorratsdatenspeicherung.pdf)).

16 Data retention statistics 2008 aggregated on the basis of statistics of CZ, DA, EE, IE, LT, MT, CY, Mai 2008 (erhältlich unter <http://www.dataretention2009.eu/all-doc.jsp>).

17 Hans J. Albrecht, Adina Grafe, Michael Kilchling, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Forschungsbericht im Auftrag des Bundesministeriums der Justiz, Duncker & Humblot, Februar 2008.

18 A.a.O. S. 222 ff. "In 88 % der Beschlüsse betrug die Antragsdauer bis zu drei Monaten. Bei den übrigen 12 % handelte es sich fast ausschließlich um sowohl in die Zukunft als auch in die Vergangenheit gerichtete Verkehrsdatenabfragen. Lediglich in 5 Fällen konnte festgestellt werden, dass eine Verkehrsdatenabfrage von zukünftigen Daten beantragt wurde, die die zulässige Höchstdauer von 3 Monaten (§§ 100 h I 3 iVm 100b II 4 StPO) überschritt. Diese Abfragen waren auf 100 Tage ausgerichtet. Den 12 % der Beschlüsse, mit denen über einen längeren Zeitraum als 90 Tage Daten abgefragt wurden, lagen v.a. Betäubungsmitteldelikte (42 %), Schleusungen (30 %) und (schwere) Bandendiebstähle (22 %) zugrunde." (S. 223).

19 A.a.O. S. 114.

20 Vgl. die Ausführungen in G. Stampfel, W. Gansterer, M. Ilger, K. Stark, The EU Data Retention Directive 2006/24/EC from a Technical Perspective, Universität Wien, Wien, Oktober 2007.

Adress-Verwaltungsinstitution (für Europa derzeit RIPE NCC) nach den Regeln der IANA (Internet Assigned Numbers Authority) zugewiesen ist. Dies gilt auch für die vertragliche und uU längerfristige Vergabe von IP-Adressen, unabhängig davon, ob diese statisch oder dynamisch vergeben werden. Auskunft wird darüber erteilt, wem die IP-Adresse überlassen wurde. Bezüglich des Internetzugangs werden mit dieser Bestimmung Art. 5 Z 2 lit. a i und ii der RL 2006/24/EG zusammengefasst.

Die Speicherverpflichtung im Sinne der Richtlinie bezieht sich ausschließlich auf zugewiesene öffentliche IP-Adressen; interne Adressen (z. B. gemäß RFC 1918) und IP-Ports (z. B. entstanden durch NAT gemäß RFC 1631, RFC 2663, RFC 3022) sind nicht umfasst. Der Zusammenhang zwischen dem zu beauskunftenden Kommunikationsvorgang und der IP-Adresse bzw. Teilnehmerkennung ergibt sich über den Zeitpunkt der Nachricht und der zeitlich korrespondierenden Vergabe der IP-Adresse.

**Zu § 102a Abs. 2 Z 2:**

In der Regel existiert kein zur Anmeldung äquivalentes Abmeldungsverfahren. Die An- bzw. Abmeldung entspricht beim Internetzugang der Zuteilung bzw. dem Entzug einer öffentlichen IP-Adresse und gibt damit lediglich Auskunft über die Möglichkeit einer Internetkommunikation für einen bestimmten Teilnehmer. Technisch erfolgt der Entzug einer IP-Adresse in der Regel durch die Neuzuteilung an denselben oder einen anderen Teilnehmer. Nicht notwendig ist die Protokollierung des Entzugs einer IP-Adresse, wenn dieser etwa wegen Verbindungsabbruch oder timeout verursacht ist. Da die öffentliche IP-Adresse zu jedem Zeitpunkt nur einmalig vergeben sein kann und jede Neuzuteilung gespeichert wird, bleibt jede Nachricht auch bei sog. „always on - Diensten“ dem Teilnehmer zeitlich zuordenbar.

**Zu § 102a Abs. 2 Z 3:**

Damit sind Dial-up-Zugänge zum Internet erfasst, die mittels Modem auf dem Sprachtelefonie-Frequenzband über POTS, ISDN (Festnetz) oder CSD (Mobilfunknetz) hergestellt werden.

**Zu § 102a Abs. 2 Z 4:**

Die eindeutige Kennung ist bei DSL-Anschlüssen, die an einen Festnetz-Anschluss gekoppelt sind, die Telefonnummer des Teilnehmers. Bei DSL-Providern, die lediglich den Zugang anbieten und somit keine Telefonnummern vergeben, ist als eindeutige Kennung die dem Kunden vergebene Zugangskennung (z. B. Benutzername) zu speichern. Die eindeutige Kennung beim Internet-Zugang über eine Mobilfunkverbindung ist die IMSI bzw. MS-ISDN (Rufnummer = Teilnehmernummer) Gegenstand der Speicherpflicht nach § 102a Abs. 3 Z 1 (Teilnehmernummer) bzw. Z 6 (IMSI).

**Zu § 102a Abs. 3 Z 1:**

Unter „andere Kennung“ ist im Sinne der gesetzlich geforderten Technologieneutralität (siehe auch Art. 8 Rahmen-RL 2002/21/EG) bei Internet-Telefondiensten (VoIP) z. B. die dem Teilnehmer zugeordnete IP-Adresse oder SIP-Adresse zu verstehen. Ein Internet-Telefondienst ist als Unterfall der „öffentlichen Telefondienste“ iSd § 3 Z 16 TKG zu verstehen. Im Sinne dieser Bestimmung ist VoIP Klasse A iSd Richtlinien für Anbieter von VoIP Diensten der RTR zu verstehen. Siehe dazu auch die Ausführungen zu § 92 Abs. 3 Z 13. Eine zusätzliche Speicherpflicht bei Internet-Telefondiensten im Vergleich zu „herkömmlichen“ Telefondiensten bezieht sich daher auf die IP-Adresse oder die SIP-Adresse.

**Zu § 102a Abs. 3 Z 2 und 3:**

Auch für VoIP-Telefonie ist der Teilnehmer eindeutig definiert.

**Zu § 102a Abs. 3 Z 4:**

Beginn und Dauer entsprechen dem Regelfall der heutigen Aufzeichnungspraxis.

**Zu § 102a Abs. 3 Z 5:**

„Anrufe“ schließt Sprachtelefonie, Sprachspeicherdienst, Konferenzschaltungen und Datenabrufungen ein; „Zusatzdienste“ schließt Rufweiterleitung und Rufumleitung ein; „Mitteilungsdienste und Multimediadienste“ schließt Kurznachrichtendienste (SMS), erweiterte Nachrichtendienste (EMS) und Multimediadienste (MMS) ein. Der Anbieter obiger Dienste und Anrufarten ist nicht notwendigerweise ident mit dem Netzbetreiber.

**Zu § 102a Abs. 3 Z 6:**

Der Begriff „Mobilfunknetz“ ist im TKG bislang nicht definiert (ebensowenig Mobilfunkdienst), er wird jedoch in § 3 Z 23 verwendet und damit offenbar vorausgesetzt, ebenso in § 23 Abs. 3 sowie in § 41 Abs. 2 Z 7 TKG. Eine ausdrückliche Definition ist daher rechtlich nicht zwingend geboten.

**Zu § 102a Abs. 3 Z 6a und b:**

Die IMEI ist - abhängig vom Netzbetreiber - nicht notwendigerweise ein erzeugtes oder verarbeitetes Datum. Zum Teil werden diese Daten nur dann erzeugt oder verarbeitet, wenn es sich um Teilnehmer im „eigenen“ Netz des Anbieters handelt; die Daten sind, sofern sie im eigenen Netz anfallen, zu speichern.

Ein Problem besteht hier in der Praxis, wenn sich die gerichtliche Anordnung pauschal auf alle weiteren Teilnehmernummern bezieht, mit denen die zunächst bestimmte Teilnehmernummer im angefragten Zeitraum kommuniziert hat. In diesem Fall können IMEI, IMSI und Standortkennung (Cell-ID) nur für jene weiteren Teilnehmer beauskunftet werden, die zum Netz des Anbieters gehören, an den die ursprüngliche Anordnung gerichtet ist. Für die Teilnehmer anderer Anbieter werden diese Daten nicht verarbeitet und daher auch nur beim jeweiligen anderen Anbieter gespeichert.

**Zu § 102a Abs. 3 Z 6c:**

Der Wortlaut dieser Bestimmung stammt aus Art. 5 Abs. 1 lit. e Z 2 vi) der RL 2006/24/EG. Festzuhalten ist, dass die Standortkennung (Cell-ID) bei der Erstaktivierung von Prepaid Kunden kein Stammdatum ist, sondern als Verkehrsdatum gespeichert wird und damit ausschließlich als Vorratsdatum zur Verfügung steht.

**Zu § 102a Abs. 3 Z 6d:**

Auch durch die Einführung der Vorratsdatenspeicherung wird nicht zulässig, dass den Strafverfolgungs- oder den Sicherheitsbehörden kommunikationsunabhängige Standortdaten beauskunftet werden.

**Zu § 102a Abs. 4 Z 1 und 2:**

Dies erfordert entweder eine derzeit bei österreichischen E-Mail Dienstanbietern nicht verfügbare Funktionalität der Historisierung von E-Mail Adresszuordnungen (z. B. bei frei durch den Teilnehmer änder- oder ergänzbaren E-Mail Alias Adressen) zu Teilnehmerkennungen oder eine bei jeder Zustellung einer E-Mail in ein elektronisches Postfach erfolgende dynamische Zuordnung und Speicherung von E-Mail Adresse und Teilnehmerkennung. E-Mail Alias Adressen können in diesem Sinne nur verarbeitet werden, wenn sie im angegebenen Zeitraum auch verwendet werden (d.h. eine E-Mail wird gesendet oder empfangen). In Bezug auf E-Mail Alias Adressen (damit aus Benutzersicht „dynamische“ E-Mail Adressen) liegt damit hinsichtlich der historischen Zuordnung solcher Adressen zu bestimmten Teilnehmern derzeit systembedingt bei allen österreichischen Anbietern der Fall vor, dass solche Daten weder erzeugt noch verarbeitet werden und daher gemäß § 102a Abs. 5 auch nicht gespeichert werden müssen.

Diese Daten sind außerdem nur dann zu speichern, soweit sie nach der Gestaltung des Dienstes bei Abschluss des Vertrages überhaupt erhoben werden, weil sie ansonsten weder erzeugt noch verarbeitet werden und damit nach Abs. 5 auch keiner Speicherpflicht unterliegen. Das bedeutet, dass bei so genannten Freemail-Diensten, die anonyme Email Accounts anbieten, Name und Anschrift des Teilnehmers nicht verfügbar sind und auch künftig nicht erhoben werden müssen.

**Zu § 102a Abs. 4 Z 3:**

Die E-Mail Adressdaten des Absenders und der Empfänger stammen vom „MAIL“ und „RCPT“ command der E-Mail iSd RFC 821. Absender ist die letztübermittelnde Kommunikationseinrichtung mit einer zugeordneten öffentlichen IP-Adresse, die nicht notwendigerweise mit der IP-Adresse des Absenders der E-Mail übereinstimmt, und, - z. B. bei Webmail - auch mit der IP-Adresse des versendenden Mailservers ident sein kann. Die Absender E-Mail Adresse ist nicht notwendigerweise einem bestimmten Teilnehmer zuordenbar, da im E-Mail Protokoll die dynamische Erzeugung einer Absender-Adresse durch den Endbenutzer ohne Mitwirkung des Betreibers möglich ist.

**Zu § 102a Abs. 4 Z 4:**

Die Daten stammen vom „MAIL“ und „RCPT“ command der E-Mail iSd RFC 821. Daten vorangehender Kommunikationsübermittlungseinrichtungen werden vom Empfänger weder erzeugt noch verarbeitet und sind daher nicht verfügbar. Zwar sind unter „Kommunikationsübermittlungseinrichtungen“ grundsätzlich „zugehörige Einrichtungen“ im Sinne des § 3 Z 24 zu verstehen, doch sind diese Einrichtungen gerade nicht Bestandteil des Kommunikationsdienstes, den der Anbieter gemäß Abs. 4 betreibt. Vielmehr handelt es sich um einen beliebigen Netzknoten im Internet, über den die Nachrichtenübermittlung auf der Ebene des IP-Protokolls vor der Zustellung an den Posteingangsserver des Dienstanbieters zuletzt geroutet wurde. Nur dessen IP-Adresse wird vom E-Mail Anbieter selbst verarbeitet.

**Zu § 102a Abs. 4 Z 5:**

Unter Anmeldung bei einem E-Mail Dienst ist zu verstehen: 1) das Login bei einem Webmaildienst, 2) die Benutzerauthentifizierung beim Zugriff auf das Postfach mittels IMAP (gemäß RFC 1730 und darauf



aufbauenden RFCs, Quelle: <http://www.rfc-editor.org/rfcxx00.html>) oder POP (gemäß RFC 1939). Ein Datum der Abmeldung wird nur dann erzeugt oder verarbeitet, wenn von der Anwendung eine Abmeldemöglichkeit vorgesehen ist und diese vom Teilnehmer benutzt wurde (z. B. Logout bei Webmail). Technisch gesehen kennt das POP3 Protokoll ein „QUIT“ command, das IMAP Protokoll ein „LOGOUT“ command. In beiden Fällen hängt das Vorhandensein eines entsprechenden Abmeldedatums jedoch von einer tatsächlichen Abmeldung durch den Teilnehmer ab, die in der Regel kaum erfolgt. Die tatsächliche Verwendung des E-Mail Dienstes ist durch die üblicherweise nicht konsistent verwendete Abmeldung durch den Teilnehmer in der Regel nicht zeitlich einschränkbar.

#### **Zu § 102a Abs. 5:**

Die Aufzählung der Daten „gemäß Abs. 2 bis 4“ ist taxativ. Die Formulierung „der betreffenden Kommunikationsdienste“ ist so zu verstehen, dass die Speicherpflicht richtlinienkonform nur bezüglich jener Daten besteht, welche vom jeweiligen Betreiber für die Erbringung seiner eigenen Dienste erzeugt oder verarbeitet werden, wodurch Doppelspeicherungen im Sinne des Erwägungsgrundes 13 der RL 2006/24/EG vermieden werden.

Da Art. 2 Abs. 1 der RL 2006/24/EG ausdrücklich auf die Begriffsbestimmungen der RL 95/46/EG (DatenschutzRL) verweist, ist grundsätzlich der Verarbeitungsbegriff aus Art. 2 lit. b) dieser Richtlinie maßgeblich. Die Verarbeitung umfasst demzufolge jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, insbesondere die in Art. 2 lit. b) demonstrativ aufgezählten Vorgänge.

Aufgrund der unterschiedlichen Ziele der beiden Richtlinien ist bei der Auslegung des Begriffs „verarbeiten“ dennoch zu differenzieren: Während die DatenschutzRL auf einen möglichst umfassenden Grundrechtsschutz abzielt (vgl. Erwägungsgründe 10 und 12) und daher der Verarbeitungsbegriff sehr weit auszulegen ist, sollen im Rahmen der Vorratsdatenspeicherung die Pflichten, die den Providern von der RL 2006/24/EG auferlegt werden, verhältnismäßig sein und nur jene Daten gespeichert werden, die im Zuge der Bereitstellung von Kommunikationsdiensten erzeugt oder verarbeitet werden (Erwägungsgrund 23 der Richtlinie).

Auch aus dem Entstehungsprozess der RL 2006/24/EG ergibt sich, dass es sich bei den auf Vorrat zu speichernden Daten ausschließlich um solche handelt, die bei den Betreibern von Kommunikationsdiensten bereits in irgendeiner Form vorhanden sind (Erläuternder Vermerk zum vorgeschlagenen Rahmenbeschluss über die Vorratspeicherung von Kommunikationsdaten, Dok. 8958/04).

Auf diese unterschiedlichen Ziele sowie die konkreten Entstehungsgeschichten dieser beiden Richtlinien ist bei der Beurteilung, ob ein Datum auf Vorrat zu speichern ist, insbesondere in Grenzfällen Bedacht zu nehmen. „Erzeugen oder verarbeiten“ im Sinne der RL 2006/24/EG bedingt, dass es auch eine technische Komponente gibt, die auf irgendeiner Ebene dieses Datum interpretiert. Der reine Durchlauf eines Datums beim Transport ist kein Erzeugen oder Verarbeiten im Sinne der RL 2006/24/EG (z. B. MPLS Netzbetreiber). Beispielhaft sei an dieser Stelle auch die IMEI angeführt, die zwar als Verkehrsdatensatz zunächst vorhanden ist, abhängig vom System des Betreibers jedoch möglicherweise gar nicht „angenommen“ und weiterverarbeitet werden kann. In einem derartigen Fall besteht keine Verpflichtung zur Speicherung dieses Datums.

Keine Speicherverpflichtung nach Z 3 und 4 besteht für die Kommunikationsdaten von Spam E-Mails, sofern diese bereits vor dem Versand bzw. der Zustellung in ein elektronisches Postfach vom Anbieter des E-Mail Dienstes herausgefiltert werden, da in diesem Fall gar kein vollständiger Kommunikationsvorgang stattfindet. Wird eine Spam E-Mail dagegen in das elektronische Postfach des Empfängers zugestellt (wenn auch möglicherweise als „Spam“ oder „Junk“ markiert) oder dem Empfänger in irgend einer anderen Weise ermöglicht, auf die Spam E-Mail zuzugreifen (beispielsweise durch Ablage in einem für den Benutzer zugänglichen Ordner und/oder Benachrichtigung über den Eingang der Spam E-Mail), besteht die Speicherpflicht in vollem Umfang. Im Hinblick auf die Tatsache, dass der weitaus überwiegende Anteil (über 80%) der gesamten E-Mail Kommunikation Spam ist, wird so sichergestellt, dass ausschließlich für Zwecke der Strafverfolgung potentiell nützliche Daten gespeichert werden und zudem den Anbietern von E-Mail Diensten keine unzumutbaren Verpflichtungen auferlegt werden. Eine entsprechende Vorgangsweise bei der Umsetzung der RL 2006/24/EG wird zudem von der von der Europäischen Kommission mit dem Beschluss 2008/324/EG eingesetzten Expertengruppe („the platform for electronic data retention for the investigation, detection and prosecution of serious crime“) ausdrücklich empfohlen.

**Zu § 102a Abs. 6:**

Die Wahrung des Verhältnismäßigkeitsgrundsatzes gebietet, kleine Unternehmen von der Speicherverpflichtung auszunehmen: Einerseits würden solche Unternehmen durch die notwendigen Investitionen und Erhaltungskosten unverhältnismäßig stark belastet, andererseits wären diese kleinen Unternehmen in der Praxis nur äußerst selten tatsächlich von Auskunftersuchen betroffen. Es ist zu berücksichtigen, dass die Instandhaltung der für die Speicherung erforderlichen Datenbanksysteme unabhängig von der tatsächlichen Zahl der gespeicherten Datensätze auch für kleine Anbieter einen Aufwand bedeuten würde, der sich grundsätzlich nicht wesentlich von einer Datenbankhaltung für große Kundenzahlen unterscheidet. Der Nutzen stünde also in keinem Verhältnis zu den jedenfalls anfallenden Kosten, zumal Auskünfte über Verkehrsdaten gemäß § 99 Abs. 5 unbenommen bleiben.

Die Grenzziehung, auf welche sich die Ausnahme kleiner Anbieter bezieht, orientiert sich an § 10 KommAustriaG, auf Grund dessen kleinere Unternehmen bereits im Zug des Verfahrens zur Einhebung der Finanzierungsbeiträge durch die RTR ausgefiltert werden. Die Koppelung an diesen Vorgang dient der Vermeidung überflüssigen Verwaltungsaufwandes.

**Zu § 102a Abs. 7:**

Diese Bestimmung ist eine notwendige Ergänzung zum Telekommunikationsgeheimnis des § 93. Damit soll kein Zweifel offen bleiben, dass auch die Umsetzung der Vorratsdatenspeicherungsrichtlinie 2006/24/EG nicht dazu führt, dass Inhaltsdaten erfasst werden. Nur demonstrativ wird dabei der wichtigste Fall angeführt, nämlich die aufgerufenen Web-Seiten (so genannte URL, Uniform Resource Locator). Erfasst sind aber alle Formen von Kommunikationsinhalten, etwa die Betreffzeile einer E-Mail, Informationen zu Newsgroup-Diensten oder zu Chaträumen wie IRC-Channels.

**Zu § 102a Abs. 8:**

Durch die einmonatige Frist für die Löschung der Vorratsdaten ab dem Ende der Speicherpflicht wird verhindert, dass die Anbieter eine tägliche Löschung der Vorratsdaten durchführen müssen. Die Lösungsverpflichtung wird an die gängige Praxis in der Branche angepasst, Daten periodisch, d.h. zu bestimmten Teilnehmern immer an einem bestimmten Tag, zu löschen, womit eine angemessen geringe Belastung der Dienstanbieter durch die Lösungsverpflichtung erreicht wird. Nach Ende der Speicherfrist dürfen die Daten jedoch nicht mehr beauskunftet werden.

**Zu § 102a Abs. 9:**

Die im ursprünglichen Begutachtungsentwurf vom Dezember 2009 enthaltene Bestimmung im ersten Satz: „Im Hinblick auf Vorratsdaten gilt jener Anbieter, der die Daten den vorstehenden Absätzen entsprechend zu speichern hat, als Auftraggeber des öffentlichen Bereichs gemäß § 4 Z 4 in Verbindung mit § 5 Abs. 2 Z 2 DSG 2000.“ entfällt, da sich Verfassungsdienst und Datenschutzkommission ausdrücklich gegen diese Konstruktion ausgesprochen haben. Als Konsequenz bleibt der Rechtsschutzweg im Falle von Datenschutzverletzungen wie üblicherweise gegen private Rechtsträger in der Zuständigkeit der Zivilgerichte. Die Datenschutzkommission ist damit im Hinblick auf Vorratsdaten nur für Auskunftsbegehren gem. § 26 DSG zuständig, soweit diese Zuständigkeit nicht durch die besonderen Bestimmungen der StPO verdrängt wird. Bezüglich Vorratsdaten verbleibt damit eine Zuständigkeit der DSK gemäß § 26 DSG nur in Bezug auf die Bestimmungen des § 99 Abs. 5 Z 3 und 4, wonach Vorratsdaten in eingeschränktem Umfang ausnahmsweise an Sicherheitsbehörden nach dem SPG für Auskunftsziele übermittelt werden dürfen. Im Hinblick auf Daten, die noch bzw. auch für betriebliche Zwecke des Anbieters nach § 99 vorhanden sind, gelten diese entsprechend § 5 Abs. 3 DSG 2000 als Auftraggeber des privaten Bereichs.

Hinsichtlich des Rechts auf Information (§ 24 DSG 2000) bzw. des Rechts auf Auskunft (§ 26 DSG 2000) bestünde im Bereich der Strafverfahren das Problem, dass die Anbieter praktisch nicht beurteilen können, wann eine Information/Auskunft die Ermittlungen gefährden würde und damit eine Ausnahme von der Informationspflicht gemäß § 24 Abs. 4 iVm § 17 Abs. 3 Z 5 DSG 2000 vorliegt, weil dies „zur Verwirklichung des Zweckes der Datenanwendung notwendig ist“. Aus diesem Grund stellt der Verweis auf die Auskunft bzw. Information nach der StPO (gegenwärtig § 139) als *lex specialis* die entsprechende Rechtssicherheit für die Anbieter her.

**Zu § 102b Abs. 1:**

In dieser Bestimmung wird die in Art. 1 der umzusetzenden Richtlinie festgesetzte Zweckbindung der Datenspeicherung zur „Ermittlung, Feststellung und Verfolgung von schweren Straftaten“ aufgegriffen und hinsichtlich der Schwere des Delikts eine Orientierung an § 135 Abs. 2a StPO festgelegt.

**Zu § 102b Abs. 2:**

Die Wendung „unverzüglich“ impliziert keinesfalls, dass Anbieter zur Einrichtung eines Journaldienstes zur Erteilung von Auskünften über Vorratsdaten verpflichtet sind. Eine Verpflichtung zur Beauskunftung außerhalb der Bürozeiten besteht daher nicht.

Eine Auskunft über Stammdaten, für die eine Auswertung von Verkehrsdaten notwendig ist, gilt als Auskunft über Daten einer Nachrichtenübermittlung im Sinne des § 134 Z 2 StPO. Damit wird die „Interpretationslücke“ in Bezug auf § 134 Z 2 StPO geschlossen, die zur Judikaturdivergenz zwischen dem 11. (Straf-)Senat des OGH, GZ 11 Os 57/05z einerseits und dem Bescheid der Datenschutzkommission vom 3.10.2007, K121.279/0017-DSK/2007, dem diese Entscheidung der DSK bestätigenden VwGH-Erkenntnis vom 27.5.2009, GZ 2007/05/0280 sowie jüngst dem 4. (Zivil-)Senat des OGH vom 14.7.2009, GZ 4 Ob 41/09x andererseits zuletzt besteht. Weil nach dem Standpunkt des 11. (Straf-)Senats des OGH eine „Auskunft über Daten einer Nachrichtenübermittlung“ dann nicht vorliegt, wenn solche Daten zwar vom Anbieter als Zwischenschritt ausgewertet werden, das Ergebnis der Auskunft aber nur auf die Ermittlung der Identität hinter den auszuwertenden Verkehrsdaten abzielt und sich damit nur auf Stammdaten bezieht.

Gemeinsam mit der Legaldefinition „Öffentliche IP-Adresse“ in § 92 Abs. 3 Z 15, mit der IP-Adressen jedenfalls Zugangsdaten sind und nur bei vertraglich zugesicherten, konkreten IP- Adressen zugleich als Stammdatum zu qualifizieren sind, wird diese Frage geklärt, und zwar im Sinne der Entscheidung des 11. Senats des OGH vom 14.7.2009, dass der Vorgang insgesamt eine Verkehrsdatenauswertung bleibt, auch wenn die Behörden am Ende nur die Stammdaten erhalten; damit ist eine solche Auskunft den strengeren Regeln unterworfen, insbesondere der Kontrolle der staatsanwaltlichen Anordnung oder kriminalpolizeilichen Handlung durch den Haft- und Rechtsschutzrichter. Siehe dazu auch die Ausführungen zu § 99 Abs. 5 Z 2.

**Zu § 102c Abs. 1:**

Daten sollen – wenn sie ausschließlich aufgrund § 102a beim Provider vorhanden sind – gekennzeichnet sein und strengeren Zugriffs- und Sicherheitsbestimmungen unterliegen. Dies ist erforderlich, damit die speicherpflichtigen Anbieter sicherstellen können, dass nur besonders ermächtigte Personen Zugang zu diesen Daten haben. Ansonsten richten sich die Datensicherheitsbestimmungen nach dem bestehenden Maßstab des § 14 DSGVO. Die Vorschriften zur Datensicherheit aus dem ursprünglichen Begutachtungsentwurf vom Dezember 2009 wurden in Anlehnung an die Entscheidung des deutschen Bundesverfassungsgerichts zu BVerfG, 1 BvR 256/08 vom 2.3.2010 zur dortigen Umsetzung der Vorratsdatenspeicherungsrichtlinie nachträglich ergänzt. Diese Bestimmung adressiert dabei die Anforderungen an die internen Datenschutz- und Datensicherheitsvorkehrungen beim Anbieter. Zugriffe auf Vorratsdaten dürfen beim Anbieter nur durch besonders ermächtigte Mitarbeiter unter Einhaltung des Vier-Augen-Prinzips möglich sein. Das bedeutet, dass jeder Zugriff auf Vorratsdaten durch zwei Personen mit einer besonderen Ermächtigung hierzu autorisiert sein muss. Das Ziel ist, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Nicht notwendig ist dabei, dass die Autorisierung durch beide Personen gleichzeitig erfolgen muss, die Autorisierung durch die zweite Person kann auch nachträglich erfolgen. Insgesamt muss aber systematisch sichergestellt sein, dass der Anbieter intern über ein effektives Kontrollsystem zur Sicherstellung der Verantwortung verfügt.

Die unmittelbare verfassungsrechtliche Pflicht der Provider aufgrund der Drittwirkung des § 1 Abs. 5 DSGVO gebietet auch eine entsprechende Dokumentation schon durch die Anbieter selbst, und nicht nur durch die Strafverfolgungsbehörden, denen die Daten im Auskunftsfall übermittelt werden.

Die Datenschutzkommission ist zwar nicht zuständig für die Kontrolle, ob im Einzelfall auch die materiellen Voraussetzungen für Auskünfte an die Sicherheitsbehörden gegeben waren, aber dafür, an wen und in welchen Fällen Daten von den Anbietern übermittelt wurden, auch im Hinblick auf allfällige Auskunftsansprüche Betroffener gegen die Anbieter sowie zur Überprüfung der Datensicherheitsmaßnahmen nach Art. 9 Abs. 1 der RL 2006/24/EG.

Die Ausgestaltung des anzuwendenden Sorgfaltsmaßstabs ist einer Verordnung vorbehalten.

**Zu § 102c Abs. 2:**

Im Sinne der Datensicherheit ist wesentlich, dass Zugriffe auf Vorratsdaten beim Anbieter revisionssicher zu protokollieren sind. Der Begriff der Revisionssicherheit orientiert sich dabei an den Grundsätzen einer ordnungsgemäßen Buchführung in den Unternehmensrechtlichen Vorschriften (insbesondere dem UGB) und dient dem Ziel, die Nutzung nur durch Berechtigte und die Einhaltung der Verfahrensvorschriften sicherzustellen. Die wichtigsten Kriterien sind dabei der Schutz vor Veränderung und Verfälschung, die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens.

Wie die nähere insbesondere technische Ausgestaltung dieses Zugriffsregimes erfolgt ist einer entsprechenden Datensicherheitsverordnung vorbehalten.

Die Protokollierung hat derartig zu erfolgen, dass die Bundesregierung jedenfalls über jene Daten verfügt, welche sie zur Erfüllung ihrer Verpflichtung nach Art. 10 RL 2006/24/EG, der Kommission jährlich eine Statistik zu übermitteln, benötigt. Synergien sollten sich ergeben, wenn die Protokollierung im Zusammenhang mit der Verrechnung der einzelnen Auskunft erfolgen kann. Gleichzeitig soll damit auch eine wesentliche Rechtsschutzaufgabe erfüllt werden. Die Aufbereitung der Statistik für die EU-Kommission obliegt dem Justizministerium, welchem die Protokolldaten daher nach Abs. 4 zu übermitteln sind.

**Zu § 102c Abs. 2 Z 1:**

Bei Anfragen der Journal-Staatsanwaltschaft muss zumindest die Geschäftszahl der Polizei angegeben werden, damit die Vorratsdaten beauskunftet werden dürfen. Diesfalls muss diese Geschäftszahl als entsprechende Referenz protokolliert werden.

**Zu § 102c Abs. 2 Z 2:**

Bei Anfragen durch Sicherheitsbehörden nach § 99 Abs. 5 Z 3 und 4 ist eine eindeutige Referenz zur Aktenzahl bei der Sicherheitsbehörde zu protokollieren. Damit soll vor allem im Falle von Auskunftsbegehren nach § 26 DSG der notwendige Bezug zum polizeilichen Hintergrund des Auskunftsbegehrens möglich sein.

**Zu § 102c Abs. 2 Z 3:**

Die Protokollierung des Datums der Anfrage sowie des Datums und des genauen Zeitpunktes der erteilten Auskunft ist notwendig, um die nach Art. 10 Der Richtlinie 2006/24/EG geforderten statistischen Daten über erfüllte wie auch ergebnislose Anfragen zu ermöglichen.

**Zu § 102c Abs. 2 Z 4:**

Die Aufschlüsselung nach Kategorien soll in groben Zügen darstellen, ob es sich um Internetdaten (§ 102a Abs. 2), Telefoniedaten (Abs. 3) oder E-Mail Daten (Abs. 4) handelt.

**Zu § 102c Abs. 2 Z 5:**

**Art. 10** der RL 2006/24/EG fordert auch statistische Werte über das „Alter“ der übermittelten Daten. Die Auswertung des Alters kann hier am einfachsten durch den Anbieter erfolgen, da die zu protokollierenden Informationen im Zuge der Beauskunftung automatisiert aus den übermittelten Daten berechnet bzw. abgeleitet werden.

**Zu § 102c Abs. 2 Z 6:**

Die Protokollierung der Identität des Betroffenen dient dazu, dass die Datenschutzkommission im Zuge von Überprüfungen auch nachträglich die Möglichkeit hat, einen Teilnehmer über eine allfällige unzulässige Verwendung seiner Daten zu informieren. Oft sind der Name und die Anschrift des von der Auskunft betroffenen Teilnehmers dem auskunftspflichtigen Anbieter nicht bekannt (z. B. anonyme Wertkarte, Strafsache gegen u.T.) und damit auch nicht protokollierbar. Dies betrifft außerdem Auskünfte über Daten zu Teilnehmern, die von der überwachten Teilnehmernummer kontaktiert wurden oder diese kontaktiert haben, aber nicht zum Netz des auskunftspflichtigen Anbieters gehören.

**Zu § 102c Abs. 2 Z 7:**

Durch die Protokollierung der internen Zugriffe auf Vorratsdaten und die entsprechende Ermöglichung einer nachträglichen Zuordnung des Zugriffs auf bestimmte Mitarbeiter im Unternehmen des Anbieters soll sichergestellt werden, dass tatsächlich nur besonders ermächtigte Personen unter Einhaltung des Vier-Augen-Prinzips Zugang zu diesen Daten haben.

**Zu § 102c Abs. 3:**

Auch die Speicherung von Protokolldaten hat dieser Bestimmung zufolge in einer eigenen Datenbank und somit getrennt von Vorrats- und Billingdaten zu erfolgen.

**Zu § 102c Abs. 4 und 5:**

Entgegen dem Entwurf 2007 sind der Justizverwaltung lediglich die Protokolldaten zu übermitteln, eine Verpflichtung der Provider zur Erstellung von Statistiken oder zur sonstigen Auswertung von Daten im Hinblick auf die Statistik nach Art. 10 der RL 2006/24/EG wird dadurch nicht normiert. Dies obliegt vielmehr den Behörden. Die Pflicht zur Berichterstattung an die Europäische Kommission ergibt sich unmittelbar aus Art. 10 der RL 2006/24/EG.

**Zu § 102c Abs. 6:**

Durch diese Bestimmung soll ausdrücklich klargestellt werden, dass die übermittelten Daten selbst nicht gespeichert werden, weil dies ansonsten der Lösungsverpflichtung von Vorratsdaten nach Ablauf von 6 Monaten zuwider laufen würde. Die zu protokollierenden Informationen sind auch für Beweis Zwecke, dass der Anbieter seiner Auskunftspflicht nachgekommen ist, jedenfalls ausreichend. Eine Aufbewahrung der Verkehrsdaten selbst ist hierfür nicht notwendig.

**Zu § 103 Abs. 4:**

Diese Bestimmung kann aufgrund der ausdrücklichen neuen Rechtsgrundlage im vorgeschlagenen § 90 Abs. 7 entfallen. Die Regelung der Auskunft über Vorratsdaten im Zusammenhang mit den Informationspflichten der Anbieter ist in Anlehnung an die bestehende Bestimmung des § 90 Abs. 6 für Stammdatenauskünfte an Verwaltungsbehörden systematisch dort jedenfalls besser aufgehoben als im Zusammenhang mit den Regelungen zum Teilnehmerverzeichnis.

**Zu § 109 Abs. 3 Z 14:**

Die Änderung dient der Anpassung des TKG an die differenzierte Terminologie der neuen StPO.

**Zu § 109 Abs. 3 Z 17:**

Diese Änderung dient der Anpassung an die Neufassung des § 98 und sanktioniert Verletzungen der neu geschaffenen Informationspflicht im Falle einer Standortdatenauskunft nach dieser Bestimmung.

**Zu § 109 Abs. 3 Z 26:**

Durch diese Verwaltungsstrafbestimmung soll bewirkt werden, dass unverschlüsselte Übermittlungen jedenfalls unzulässig sind. Diese Bestimmung dient damit ebenfalls indirekt der Datensicherheit.

**Zu § 137 Abs. 4:**

Diese TKG-Novelle soll mit neunmonatiger Legisvakanz in Kraft treten, um den Anbietern Zeit für erforderliche technische Anpassungen zu geben.