Erläuterungen

Allgemeiner Teil

Die Verordnungsermächtigungen der §§ 94 Abs. 4 und 102c TKG 2003 werden gegenständlich mit einer einheitlichen Verordnung geregelt. Diese Verordnung wird von der Bundesministerin für Verkehr, Innovation und Technologie erlassen, wobei jene Teile der Verordnung, die in Ausführung des § 94 Abs. 4 TKG 2003 ergehen, im Einvernehmen mit dem Bundesminister für Inneres und dem Bundesminister für Justiz zu erlassen sind, während ein solches Einvernehmen in Bezug auf die § 102c TKG ausführenden Bestimmungen nicht erforderlich ist. Letzteres betrifft die Bestimmungen im 2. Abschnitt (§§ 5 bis 7), wobei auch zu diesen in der Vorbreitung grundsätzliches Einvernehmen hergestellt wurde.

Besonderer Teil

Zu § 1:

In den Erläuterungen zu § 94 Abs. 4 TKG 2003 wird der Spielraum abstrakt beschrieben, den der Verordnungsgeber bei der Ausgestaltung dieser Bestimmung hat: „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, Staatsanwaltschaften 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 Verordnungsgeber dar. Die gesetzlich vorgezeichneten Indikatoren sind dabei technologieneutral formuliert. Wesentlich ist, dass die eingesetzte Technologie den Zielvorgaben entspricht.

Am 7.4.2011 wurde die TKG Novelle zur Umsetzung der Vorratsdatenspeicherung im Ausschuss für Forschung, Innovation und Technologie (FIT Ausschuss) des Nationalrats diskutiert (siehe dazu den Ausschussbericht: 1157 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXIV. GP). In diesem Rahmen wurde ein Antrag für eine Ausschussfeststellung zum Thema Datensicherheit eingebracht, der eine Grundsatzerklärung für die Implementierung der Durchlaufstelle enthält. Diese Ausschussfeststellung wurde mit den Stimmen der Regierungsfraktionen angenommen und lautet wie folgt: „Für die Datensicherheit und die Nachvollziehbarkeit der Zugriffe auf den Datenvorrat ist das Zusammenspiel der Bestimmungen der §§ 94 Abs. 4 und 102c TKG von besonderer Bedeutung. Während § 94 Abs. 4 TKG 2003 den Aspekt der technischen Datenintegrität und der Determinierung der Verordnungsermächtigung über die Art der Verschlüsselung betrifft und die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten identifiziert, um durch sichere ‚Identifikation und Authentifizierung von Sender und Empfänger‘ sicherzustellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden, Staatsanwaltschaften und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht, regelt § 102c TKG 2003 Zugriffs- und Sicherheitsbestimmungen. Einerseits muss jeder Zugriff auf Vorratsdaten durch zwei Personen mit einer besonderen Ermächtigung hierzu autorisiert sein, um zu gewährleisten, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Andererseits müssen Zugriffe auf Vorratsdaten beim Anbieter revisionssicher protokolliert werden. 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, wozu etwa bei Anordnungen der Staatsanwaltschaft auch die Angabe der Geschäftszahl der ermittelnden Kriminalpolizei zählt. Der Ausschuss geht davon aus, dass sämtliche Zugriffe und Übermittlungen von wem auch immer auf Vorratsdaten gemäß § 94 Abs. 4 TKG lückenlos protokolliert werden. Der Ausschuss geht weiters davon aus, dass ein automatisches zentrales System der Protokollierung solcher Abfragen und Übermittlungen notwendig ist, wobei unter dieser Protokollierung nicht die in § 102c Abs. 2 TKG 2003genannte zu verstehen ist. Sie wird vielmehr

nur jene Daten umfassen, die zur statistischen Auswertung und zur Verknüpfung mit der gemäß § 102c Abs. 2 TKG 2003 erfolgenden Protokollierung dient. Wünschenswert ist die Einrichtung einer ‚Datendrehscheibe' (‚Durchlaufstelle', kurz: DLS). Da jeder Auskunftsfall über die DLS mit einer fortlaufenden einmaligen Nummer versehen wird, kann im Falle einer Nachprüfenden Kontrolle über die Protokollierung bei der DLS zur Protokollierung beim Anbieter gemäß § 102c Abs. 2 TKG 2003 verknüpft werden. Zugang zu den übermittelten personenbezogenen Daten soll die DLS selbst nicht bieten, die Daten liegen dort nur verschlüsselt bis zur Abholung bereit und werden bei der Abholung automatisch gelöscht."

Festzuhalten ist, dass diese Ausschussfeststellung sachlich auf der gemeinsamen Arbeit zur Entwicklung der Schnittstellenbeschreibung und eines sicheren Systems der Datenübermittlung in den Round Table Diskussionen basiert, die das Ludwig Boltzmann Institut für Menschenrechte (BIM) im Rahmen einer Studie zur Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung im Auftrag des BMVIT ausgearbeitet hat. Die Ausschussfeststellung bezieht sich auf den Diskussions- und Einigungsstand beim 3. von insgesamt 6 Round Table Veranstaltungen am 24.3.2011, bei dem die Grundsatzeinigung auf das Konzept der Durchlaufstelle (siehe § 10) bereits Konsens unter allen Beteiligten war.

Zu § 1 Abs. 2:

Zunächst wird klargestellt, dass diese Verordnung nicht ausschließlich Vorratsdaten betrifft. Soweit es nämlich um die Übermittlung von Verkehrsdaten, Zugangsdaten und Standortdaten für Auskünfte gegenüber Sicherheits- und Strafverfolgungsbehörden geht, die beim Anbieter für betriebliche Zwecke gespeichert sind, sind die Datensicherheitsvorschriften auch für diese Daten relevant. Hinsichtlich jener Bestimmungen, die Datensicherheitsmaßen innerhalb des Betriebes des Anbieters betreffen, ist die Verordnung allerdings nur für Vorratsdaten maßgeblich, denn nur für diese gelten gemäß § 102c TKG 2003 die strengen Zugriffsbestimmungen. Ansonsten gilt der allgemeine Sicherheitsmaßstab, den das TKG 2003 und das DSG 2000 vorgeben (siehe dazu die Erläuterungen zu § 4).

Schließlich wird bewusst die Formulierung „Verwendung" normiert. Nach § 4 Z 8 DSG 2000 ist „Verwenden von Daten" definiert wird als „ jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten" und der Begriff „Verarbeiten von Daten" gemäß § 4 Z 9 DSG 2000 auch die Speicherung umfasst. In der österreichischen datenschutzrechtlichen Terminologie ist dies der weiteste Begriff, der alle Fälle möglicher Datenverwendungen - insbesondere die Übermittlung von Daten - umfasst. Weil gerade im Regelungsbereich des § 94 Abs. 4 TKG 2003 die Übermittlung im Vordergrund steht, wird hier der Rechtsbegriff der Datenverwendung nutzbar gemacht. Aus dem Regelungsumfang der Verordnung ist zugleich klar, dass die weitere Verwendung der betreffenden Daten nach der Übermittlung über die DLS - insbesondere die weitere Verwendung der Daten für die Zwecke der Strafverfolgung - nicht von dieser Verordnung bestimmt wird.

Zu § 2 Abs. 1:

Diese Bestimmung definiert die Bezeichnung der beiden Datenarten, deren Unterscheidung vom Zweck der Verarbeitung und Speicherung abhängt. An diese Unterscheidung sind einige rechtliche Konsequenzen geknüpft, die durch eine Konkretisierung und klare Formulierung der an sich schon im TKG 2003 vorgezeichneten Definitionen leichter normativ zu erfassen sind. In Z 1 wird bewusst der Begriff „Betriebsdaten" eingeführt, weil in zahlreichen öffentlichen Diskussionen zum Thema Vorratsdatenspeicherung oft nur der Begriff der „Verrechnungsdaten" verwendet wird, der jedoch zu kurz greift. Wohl bilden die Daten zum Zweck der Rechnungslegung (§ 99 Abs. 2 TKG 2003) den praktisch wichtigsten Fall, doch auch jene Daten, die beim Anbieter zum Zweck der Aufrechterhaltung des Betriebes und insbesondere der technischen Wartung der Betriebsanlagen (§ 99 Abs. 3 TKG 2003) verarbeitet und gespeichert werden, sind nach der bisherigen Rechtslage vor Umsetzung der Vorratsdatenspeicherung regelmäßig Gegenstand von behördlichen, staatsanwaltschaftlichen und gerichtlichen Auskunftsersuchen. Z 2 gibt die Legaldefinition des § 92 Abs. 3 Z 6b TKG 2003 wieder und verbindet diese mit der Zweckwidmung des § 102b TKG 2003. Damit soll lediglich die strenge Zweckbindung, die nur durch die Ausnahmen in § 99 Abs. 5 TKG 2003 durchbrochen wird, eindeutig klargestellt werden, ein über die Definition im TKG 2003 hinausgehender normativer Gehalt entsteht daraus nicht.

Zu § 3 Abs. 1:

Absatz 1 nimmt jene Fälle vom Datensicherheitsregime des 3. Abschnitts dieser Verordnung aus, die bereits durch die gesetzliche Regelung des § 94 Abs. 4 TKG 2003 als Ausnahmen vorgesehen sind. Aufgezählt werden jene Fälle, in denen eine Beantwortung von Auskunftsbegehren durch den Anbieter nach einem anderen Regime vorgesehen oder zumindest zulässig ist und keine Verschlüsselung nach dem 3. Abschnitt zwingend durchzuführen ist. Die auf § 98 TKG 2003 bezogene Ausnahme bezieht sich auf die Identifizierung und Lokalisierung von Anschlüssen bzw. Endgeräten, von denen ein Notruf abgesetzt

wurde. Für diese Fälle wird es künftig nach der Umsetzung des neuen Telekom Rechtsrahmens eine eigene Schnittstelle geben, um eine sofortige Reaktion der Notrufträger zu ermöglichen, wobei damit eine automatische nachträgliche Information der Betroffenen verbunden ist. Die Umsetzung dieser gemeinschaftsrechtlichen Verpflichtung steht unmittelbar bevor, daher ist dieser Fall aus dem Anwendungsbereich dieser Verordnung ausgeklammert.

Die Fälle des § 99 Abs. 5 Z 3 und 4 TKG 2003 bei Gefahr im Verzug gemäß Z 2 bezieht sich auf Anfragen nach § 53 Abs. 3a und 3b SPG, wenn aufgrund der besonderen Umstände des Falles der Zweck der Auskunft (zB die Abwehr einer gegenwärtigen oder unmittelbar drohenden Gefahr) dadurch gefährdet wäre, dass die Abwicklung der Auskunft über das System der DLS zu lange dauern würde und daher eine schnellere Form der Beauskunftung unerlässlich ist, zB eine telefonische Auskunft über die Standortdaten des Endgerätes einer akut gefährdeten Person. Die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten erfolgt über die ETSI Schnittstelle zur Inhaltsüberwachung durch Übergabe der sogenannten „S-Records".

Zu § 3 Abs. 2:

Absatz 2 dieser Bestimmung regelt die gesetzlich definierten Ausnahmefälle für Anfragen abseits der DLS sowie die Verpflichtung zur nachträglichen Dokumentation über die DLS. Ganz generell ist hier voraus zu schicken, dass das Konzept der DLS auch darauf abzielt, die Abwicklung von Auskunftsbegehren im Vergleich zur bisherigen Praxis (Fax- und E-Mail- Anfragen) zu beschleunigen und den Verwaltungsaufwand sowohl auf Behörden- als auch auf Anbieterseite zu reduzieren. Es ist daher nicht generell davon auszugehen, dass eine Abwicklung abseits der DLS tatsächlich jene Beschleunigung mit sich bringt, welche die gesetzlichen Ausnahmen rechtfertigen soll. Die Praxis ab dem Vollbetrieb des neuen Konzepts ab 1.4.2012 wird zeigen, ob gerade in dringenden Fällen eine Abwicklung über die DLS nicht sogar vorteilhaft sein wird. Die technische Spezifikation sollte hierzu also jedenfalls den Usecase "nachträgliche Anfragedokumentation" berücksichtigen und idealer weise auch eine Prioritäteninformation bei der Notifikation über die DLS vorsehen. Bereits die Erläuterungen zu § 94 Abs. 4 TKG 2003 führen zu den Ausnahmen aus: „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."

Die in den Ausnahmen genannten Fälle des § 99 Abs. 5 Z 3 und 4 TKG 2003 betreffen Auskünfte nach § 53 Abs. 3a und Abs. 3b SPG, bei denen eine Anfrage bzw. Beantwortung via DLS bei Gefahr in Verzug unterbleiben kann. Standortdatenanfragen nach § 53 Abs. 3b SPG werden dabei schon aufgrund des dort normierten Tatbestandes (Abwehr einer „gegenwärtigen Gefahr" für den Inhaber der Endeinrichtung) regelmäßig einen Fall von „Gefahr in Verzug" darstellen. Festzuhalten ist, dass in diesen Fällen nur ausnahmsweise überhaupt historische Standortdaten begehrt werden, nämlich nur dann, wenn eine live-Ortung (durch sog. „stummes SMS") erfolglos bleibt, etwa weil das Endgerät defekt oder ausgeschaltet ist. In Fällen von Gefahr im Verzug kann die Anfrage telefonisch übermittelt werden. Es erfolgt eine Nachreichung der Anfrage über die DLS, wobei davon auszugehen ist, dass die Beantwortung der Anfrage bereits vor der Nachreichung der Anfrage erfolgt. Dies bedeutet, dass bei der technischen Spezifikation der DLS Festlegungen zur Unique-ID getroffen werden müssen. Dazu könnte jedem Anbieter ein eigener Bereich von Referenznummern zugeteilt werden. Der Anbieter verwendet diese Referenznummern in aufsteigender Reihenfolge im Falle, dass die betreffende Anfrage noch nicht über die DLS eingelangt ist. In der Durchlaufstelle muss dann die Zuordnung zwischen Anfrage und (bereits erfolgter) Durchführung erfolgen. Es ist hier nur der Usecase "nachträgliche Anfragedokumentation" zu berücksichtigen (Daten wurden bereits übermittelt) + Übermittlung von Protokolldaten bei Zugriff auf Vorratsdaten.

SPG Anfragen können

a) bei Gefahr im Verzug

- mündlich
- lt. SPG von jeder Sicherheitsbehörde
- schriftlich

- oder über die DLS

b) wenn keine Gefahr im Verzug vorliegt

- durch Anfrage (und Antwort) über die DLS

zum Anbieter gelangen.

Die Dokumentation über die DLS ist dabei sinnvoll und notwendig, da teilweise (insbesondere bei Anfragen zu IP-Adressen und E-Mail Daten) auch Vorratsdaten betroffen sein werden und der Anbieter bei Zugriff auf Vorratsdaten die Protokolldaten gemäß § 7 Abs. 3 Z 3 bis 5 zu übermitteln hat und der besondere Rechtsschutz (Informationspflicht der Behörde) ausgelöst wird.

Auch im Rahmen von StPO-Abfragen kann es - eng begrenzte - Fälle geben, in denen eine mündliche Übermittlung der Anordnung erfolgt. Anordnungen von Zwangsmaßnahmen sind von der Staatsanwaltschaft begründet und schriftlich auszufertigen und an die Kriminalpolizei zu richten. In dringenden Fällen kann aber eine solche Anordnung vorläufig mündlich übermittelt werden (§ 102 Abs. 1 StPO). Dies gilt auch für die Anordnung einer „Auskunft über Daten einer Nachrichtenübermittlung“ (§ 134 Z 2 StPO) sowie künftig bei einer „Auskunft über Vorratsdaten“ (§ 134 Z 2a StPO). In dringenden Fällen kann eine solche mündliche Anordnung auch auf Grund einer mündlichen gerichtlichen Bewilligung (§ 105 StPO) erteilt werden. So kann im Fall des § 135 Abs. 2 Z 1 StPO (noch andauernde Entführung) eine Dringlichkeit vorliegen, die zumindest erfordert, dass die Übermittlung des Auskunftsbegehrens vorerst „auf kürzestem Weg“ an den Anbieter gerichtet wird, während die Antwort über die sichere Verbindung gemäß § 94 Abs. 4 TKG 2003 übermittelt werden muss, weil diesbezüglich keine gesetzliche Ausnahme vorgesehen ist. Aus Sicht des TKG 2003 ist dies rechtlich zulässig, da § 94 Abs. 4 TKG 2003 ausdrücklich nur die Beantwortung, aber nicht die Übermittlung der Anordnung regelt. Diesbezüglich wäre gemäß § 102 Abs. 1 StPO die schriftliche und begründete Anordnung der Staatsanwaltschaft nachzureichen. Das Erfordernis einer gerichtlichen Bewilligung sagt per se nichts über die Dringlichkeit und das auch über Entführungsfälle hinausgehende Erfordernis einer mündlichen Beauskunftung vorab aus. Die gerichtliche Bewilligung kann im Rahmen des Rufbereitschafts- und Journaldienstes fernmündlich binnen kürzester Zeit erteilt werden, gerade wenn eine unverzügliche Anordnung durch die Staatsanwaltschaft fallspezifisch nötig ist. § 102 Abs. 1 StPO sieht generell vor, dass Anordnungen und Genehmigungen in dringenden Fällen vorläufig mündlich übermittelt werden können. In der Praxis werden solche mündlichen Anordnungen von den Anbietern akzeptiert– wenn eine schriftliche Bestätigung der Exekutive über “mündliche Anordnung und Bewilligung” vorliegt. Auch in diesen Fällen ist Vorkehrung dafür zu treffen, dass eine Beantwortung vor Übermittlung der Anfrage erfolgen kann, wobei gerade hier erforderlich ist, dass die schriftliche Anfrage über die DLS nachzureichen und zu dokumentieren ist.

Zu § 4:

Absatz 1 folgt zunächst dem ersten Grundsatz, den die Richtlinie 2006/24/EG in Art 7 lit a) aufstellt: „Die auf Vorrat gespeicherten Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten“.

Die darüber hinausgehenden Sicherheitsvorschriften, die im 2. Abschnitt geregelt werden und auf die Absatz 2 in diesem Zusammenhang nur verweist, erfließen aus dem Spielraum der Mitgliedsstaaten, höhere Sicherheitsanforderungen zu erlassen (Art 7 Abs. 1 RL 2006/24/EG, arg. „zumindest folgende Grundsätze“) und sind das Ergebnis einer intensiven Diskussion im Rahmen vieler Arbeitsgruppentreffen im Zuge der Umsetzung der Vorratsdatenspeicherung, die nicht zuletzt durch die Entscheidung des deutschen Bundesverfassungsgerichts (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010) zur dortigen Aufhebung der deutschen Umsetzung der Vorratsdatenspeicherungs-Richtlinie motiviert und vorgezeichnet sind.

Die für die Ausarbeitung des Konzepts hinter dieser Verordnung wesentlichsten Aussagen des BVerfG sollen hier auszugsweise wiedergegeben werden: Hinsichtlich der Datensicherheit fordert das Gericht „gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben“ (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010, Abs. 225). Dieser hat sich an dem Entwicklungsstand der Fachdiskussion zu orientieren, neue Erkenntnisse und Einsichten fortlaufend aufzunehmen und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten zu stehen. Nur wenn diesbezüglich hinreichende anspruchsvolle und normenklare Regelungen getroffen sind, ist der in einer solchen Speicherung liegende Eingriff verhältnismäßig im engeren Sinne, so das Gericht (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010, Abs. 239). Um in qualifizierter Weise dem Grunde nach den Schutzstandard konkretisieren zu können, muss der Gesetzgeber die Schutzmechanismen selbst benennen und nur deren Ausgestaltung auf Verordnungen oder Aufsichtsbehörden delegieren. Dem ist die Konzeption des § 94

Abs. 4 und 102c TKG 2003 auch gefolgt. Wo die allgemeinen Sicherheitsanforderungen an die Verarbeitung von Telekommunikationsdaten nicht ausreichend sind, um dem speziellen Schutzbedürfnis zu begegnen, das aus der flächendeckenden und anlasslosen Vorratsspeicherung resultiert, werden die besonderen Anforderungen in Ausführung der Vorgaben des § 102c TKG 2003 im nachfolgenden 2. Abschnitt normiert, auf den Absatz 2 klarstellend verweist.

Zu § 5 Abs. 1 bis 4:

Die österreichische Umsetzung ist in einem Punkt weniger streng als das Urteil des deutschen Bundesverfassungsgerichts vorzeichnet, wonach verlangt wird: „Die Daten sind getrennt von den weiteren IT-Systemen des Speicherverpflichteten zu speichern, und zwar hardwaremäßig getrennt und entkoppelt vom Internet." Es genügt also nicht den Anforderungen des Bundesverfassungsgerichts, die Daten, die zur Vorratsdatenspeicherung gedacht sind, durch eine Kennzeichnung in der Datenbank von denjenigen Daten zu trennen, die für Abrechnungszwecke gespeichert werden (Andreas Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399).

Nach den Vorgaben des § 102c TKG 2003 und der Konkretisierung durch § 5 ist eine physische Trennung bei der Speicherung von Vorratsdaten und Betriebsdaten nicht notwendig. Hintergrund dieser Entscheidung des Gesetzgebers und in weiterer Folge des Verordnungsgebers ist die Tatsache, dass eine physische Trennung im Hinblick auf die Datensicherheit nur dann endgültig Sinn ergeben würde, wenn damit auch zwingend verbunden wäre, dass der physische und technische Zugang auf der Ebene der IT-Infrastruktur zu einem solcherart getrennten Speichersystem organisatorisch nur völlig unterschiedlichen Personen im Betrieb des Anbieters möglich ist. Das würde faktisch bedeuten, dass ein zur Speicherung verpflichtetes Unternehmen eine eigene und völlig abgegrenzte IT-Abteilung nur für die Vorratsdatenspeicherung schaffen müsste. Dies wurde in der Debatte zur Umsetzung als unverhältnismäßiger Eingriff in die Eigentumsfreiheit der Anbieter gesehen und hat daher keinen Eingang in die österreichische Umsetzung gefunden. Anzumerken ist, dass sich das deutsche Bundesverfassungsgericht mit dem Problem der flankierenden organisatorischen Trennung gar nicht auseinandergesetzt hat.

Gleichwohl sind die speicherpflichtigen Unternehmen gesetzlich verpflichtet, sicherzustellen, dass der Eingriff auf die Daten einem gesicherten Zugriffsregime unterliegt. Das BVerfG führt hier beispielhaft das Vier-Augen-Prinzip an. Der Zugriff soll nicht durch Einzelne, sondern nur durch zwei oder mehr Personen möglich sein. Darüber hinaus ist der Zugriff auf die Daten revisionssicher zu protokollieren. Damit verlangt das Bundesverfassungsgericht, dass einerseits ein Zugriff auf die Daten nur möglich ist, wenn der Zugriff auch protokolliert wird. Andererseits darf dieses Protokoll nicht im Nachhinein zu verändern sein, muss also revisionssicher sein (siehe dazu die Erläuterungen zu § 7). Um dieses getrennte Zugriffsregime effektiv zu verwirklichen, sind geeignete Maßnahmen sowohl auf technischer als auch organisatorischer Ebene beim Anbieter notwenig, die jedenfalls eine logische Trennung bei der Datenbankhaltung erfordern. Nicht hinreichend wäre dafür, dass die Daten einfach in den betrieblichen Datenbanken verbleiben und dort als Vorratsdaten markiert werden. Daher ordnet Absatz 3 auch an, dass diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen sind. Die konkret von einem Anbieter entwickelte Methode dieser Trennung muss für die Kontrolle durch die Datenschutzkommission nachvollziehbar sein und daher auch dokumentiert werden. Dies sollte der Datenschutzkommission ermöglichen, die tatsächliche Einhaltung der Standards jederzeit zu kontrollieren.

Zu § 5 Abs. 5:

Eine völlige Harmonisierung, wie lange ein Anbieter im Detail welche Daten für betriebliche Zwecke speichern darf, ist kaum zu erreichen und wäre wohl ein unverhältnismäßiger Eingriff in die Erwerbsfreiheit. Die Schwierigkeit liegt nämlich darin, dass die betriebliche Notwendigkeit einer Datenspeicherung einerseits von den technischen Systemen und deren Wartung und andererseits von der Ausgestaltung verschiedener Tarif- und Geschäftsmodelle abhängt. Dabei ist zum Teil gar nicht möglich, dass ein Anbieter in Bezug auf bestimmte Datenkategorien (etwa der Unterscheidung gemäß § 102a Abs. 2 bis 4 TKG 2003 folgend) genau festlegen kann, wie lange diese Datenkategorien jeweils für betriebliche Zwecke aufbewahrt werden. Das Problem liegt nämlich darin, dass zur selben Datenkategorie in unterschiedlichen Tarifmodellen auch unterschiedliche Aufbewahrungszeiträume notwendig sind. Dieselben Daten können also in einem Fall noch Betriebsdaten und in einem anderen Geschäftsmodell bereits Vorratsdaten sein.

Der Anbieter muss jedoch betriebsintern Klarheit darüber schaffen, welche Daten im Hinblick auf die intern bestimmten technischen und geschäftlichen Notwendigkeiten wie lange gespeichert werden. Diese Klarheit ist schon deswegen notwendig, weil ansonsten eine Abgrenzung im Hinblick auf das geforderte

erhöhte Sicherheitsregime bei Vorratsdaten nur schwer möglich ist. Obgleich ein Anbieter Spielraum zur Gestaltung seiner Geschäftsmodelle hat, ist die Unterscheidung von Vorratsdaten nicht völlig beliebig in der Hand des Anbieters. Vielmehr haben die internen Betriebsdaten-Richtlinien den Anforderungen an eine datenschutzrechtliche Rechtfertigung für die Verarbeitung personenbezogener Daten gerecht zu werden. Es muss für einen verständigen Beobachter nachvollziehbar sein, warum bestimmte Daten(Kategorien) für bestimmte Zwecke eine bestimmte Zeit lang aufbewahrt werden. Aus diesem Grund müssen die internen Betriebsdaten-Richtlinien auch der Datenschutzkommission zugänglich sein, damit sie im Falle einer objektiven Kontrolle die Nachvollziehbarkeit der Rechtfertigung prüfen kann.

Überdies muss der Anbieter schließlich in der Lage sein, seine Speicherpolitik gegenüber seinen Kunden zu rechtfertigen, insbesondere für den Fall, dass ein Kunde eine Auskunft gemäß § 26 DSG 2000 begehrt oder im gerichtlichen Verfahren gemäß § 32 DSG 2000 die Richtigstellung oder Löschung seiner Daten begehrt.

Zu § 6 Abs. 1:

Absatz 1 normiert einen für die Praxis wichtigen Größenschluss, dessen Zulässigkeit sich aus den gesetzlichen Voraussetzungen für die Auskunft über Vorratsdaten gemäß § 135 Abs. 2a StPO ergibt. Dieser verweist nämlich auf die Fälle des § 135 Abs. 2 Z 2 bis 4 StPO, woraus sich ergibt, dass immer dann, wenn die Voraussetzungen für eine Auskunft über Vorratsdaten vorliegen, zugleich auch die Vorraussetzungen für eine Auskunft über „Betriebsdaten“ nach § 135 Abs. 2 StPO gegeben sind. Für die Praxis sollen möglichst Fälle vermieden werden, in denen eine Anfrage auf betrieblich gespeicherte Daten negativ beantwortet wird und dann eine zweite Anfrage auf Vorratsdaten erforderlich ist. Es sollen zudem auch Fälle vermieden werden, in denen sich der Zeitraum einer negativen Anfrage auf betriebsnotwendige Daten und die darauf folgenden Anfrage auf Vorratsdaten genau mit jenem Zeitraum überschneidet, innerhalb dessen Daten nicht mehr für betriebsnotwendige Zwecke benötigt werden und somit zu Vorratsdaten werden. Ansonsten könnte es etwa sein, dass Vorratsdaten angefordert werden, zunächst aber nur Betriebsdaten vorliegen und zum Zeitpunkt der nochmaligen Übermittlung des Auskunftsbegehrens gerichtet auf Betriebsdaten (also gemäß § 135 Abs. 2 StPO) diese Daten in der Zwischenzeit doch zu Vorratsdaten geworden sind, und der Anbieter die Antwort schließlich doch auf Basis der ersten Anfrage übermitteln müsste.

Ergänzend erfolgt in Absatz 1 die Klarstellung, dass Protokollierungsverpflichtungen nur dann ausgelöst werden, wenn eine Anfrage über Vorratsdaten erfolgt, die auch einen Zugriff auf (potentiell vorhandene) Vorratsdaten beim Anbieter auslöst, weil es ansonsten in der Statistik auch keine sinnvolle Auswertung zu negativen Beantwortungen geben würde. Wenn beim Anbieter nicht einmal zur Nachschau auf die Vorratsdatenbank zugegriffen wird, etwa weil aufgrund der internen Betriebsdaten-Richtlinie klar ist, dass alle angeforderten Daten noch in den betrieblichen Systemen vorhanden sind, würde ein Protokollierung als Fall der Verwendung von Vorratsdaten nur die Statistik verfälschen. D.h. eine Anfrage nach § 135 Abs. 2a StPO soll nur dann von der Protokollierung erfasst sein, wenn der Anbieter diese nicht allein durch Abfrage der betriebsnotwendigen Daten beantworten kann, sondern tatsächlich gezielt zusätzlich Vorratsdaten abfragen muss. Umgekehrt reicht allerdings schon aus, dass der Anbieter eine Abfrage in der Vorratsdatenbank vornehmen muss, um die Protokollierungspflicht auszulösen, auch wenn diese Abfrage zu keinem Ergebnis führt. Dieser Fall muss in die Statistik als erfolglose Anfrage nach Vorratsdaten Eingang finden.

Zu § 6 Abs. 2:

Aus Sicht der anfrageberechtigten Behörden, Staatsanwaltschaften und Gerichte ist eine Information darüber, ob die abzufragenden Daten betriebsnotwendige Daten oder Vorratsdaten sind, erforderlich. Daher ist hier die Frage relevant, wann einem Datum (besser: einem Datensatz) die rechtliche Qualifikation als „Vorratsdatum“ zukommt. An diese Qualifikation sind nämlich in weiterer Folge erhöhte Konsequenzen im Rechtsschutz geknüpft, beispielsweise die verpflichtende Information der Betroffenen bei Auskünften nach SPG, sowie die besonderen Zugriffs- und Protokollierungsbestimmungen beim Anbieter intern. Für diese Qualifikation findet sich eine Erklärung in den Erläuterungen (GP XXIV, Nr. 1074, 1. Absatz zu § 92 Abs 3 Z 6b TKG 2003): „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 der Daten als Vorratsdaten ist also durch den Zweck determiniert, zu dem die Daten gespeichert werden (dürfen).“ Nach der Legaldefinition in § 134 Z 2a StPO ist eine Auskunft über Vorratsdaten, „die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach

Maßgabe des § 102a Abs. 2 bis 4 TKG 2003 zu speichern haben, und die nicht nach § 99 Abs. 2 TKG 2003 einer Auskunft nach Z 2 (Anm.: „Auskunft über Daten einer Nachrichtenübermittlung“) unterliegen.“

Für Anfragen, die nicht zwischen Vorratsdaten und betriebsnotwendigen Daten unterscheiden (z.B. nach § 53 Abs. 3a und 3b SPG), muss die Information übermittelt werden, ob Vorratsdaten für die Beantwortung dieser Anfrage verwendet wurden. Umgekehrt kann es sein, dass Anfragen der Staatsanwaltschaft zunächst auf Vorratsdaten gemäß § 135 Abs. 2a StPO gerichtet sind, aufgrund des in Absatz 1 normierten zulässigen Größenschlusses aber tatsächlich keine Vorratsdaten übermittelt werden. In diesen Fällen ist ebenfalls relevant, ob Vorratsdaten verwendet wurden, weil davon die Befassung des Rechtsschutzbeauftragten der Justiz abhängt. Aus diesen Gründen hat der Anbieter bei jeder Übermittlung von Vorratsdaten diesen Umstand als Zusatzinformation (gemäß Anlage, Kapitel 1.4) über die DLS zu übermitteln.

Zu § 6 Abs. 3:

Zu unterscheiden von der rechtlichen Qualifikation als „Vorratsdatum“ ist die Frage nach dem Zeitpunkt der Vorratsspeicherung und der Datenhaltung in der „Vorratsdatenbank“. Hier ist zunächst das Doppelspeicherungsverbot für Vorratsdaten zu beachten. Ein solches ist zwar im normativen Teil der EU-Richtlinie 2006/24/EG nicht ausdrücklich enthalten. Allerdings enthält Erwägungsgrund 13 der RL die Vorgabe: „Die Vorratsspeicherung von Daten sollte so erfolgen, dass vermieden wird, dass Daten mehr als einmal auf Vorrat gespeichert werden.“ Das heißt aber nicht, dass eine gleichzeitige Speicherung von Daten als Betriebsdaten und Vorratsdaten dadurch ausgeschlossen ist. Eine gleichzeitige Speicherung von Daten sowohl in der Vorratsdatenbank als auch in den betrieblichen Datenbanken der Anbieter kann die operative Abwicklung für die Anbieter erleichtern. Die Anbieter könnten nämlich alle Daten schon bei der ersten Verarbeitung aus dem Live-System „abgreifen“ und in die Vorratsdatenbank überführen. Aus den betrieblichen Datenbanken müssen die Daten dann gelöscht werden, sobald die betriebliche Notwendigkeit nicht mehr gegeben ist.

Dazu normiert § 92 Abs. 3 Z 6b des TKG 2003: "Vorratsdaten sind Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden." Für die Beurteilung der Rechtmäßigkeit der in Absatz 3 vorgeschlagenen (nicht verpflichtenden) Zulässigkeit zur gleichzeitigen Speicherung von Betriebsdaten in der Vorratsdatenbank geht es dabei vor allem um die Auslegung des Begriffes "ausschließlich", der aus der Perspektive der Vorratsdatenbank zu verstehen ist. Daten in dieser Datenbank dienen allein dem in § 102a Abs 1 TKG 2003 normierten (und eingeschränkt von § 99 Abs. 5 TKG 2003 mit Ausnahmen durchbrochenen) Zweck der „Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt.“ Zugriffe auf diese Datenbank sind stets nur unter den strengeren Voraussetzungen der §§ 102b und 102c TKG 2003 zulässig, selbst wenn diese Daten zugleich im betrieblichen System des Anbieters vorhanden sind. Insofern wären die Daten in dieser Datenbank – auch bei gleichzeitiger Speicherung in den betrieblichen Systemen des Anbieters – tatsächlich „ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a“ gespeichert. Diese Datenbank würde ab dem Ende der Kommunikation stets alle Daten enthalten, die für Auskünfte gegenüber den berechtigten Behörden, Staatsanwaltschaften und Gerichten zur Verfügung stehen müssen. Dies geht konform mit der Formulierung in § 102a Abs. 1 TKG 2003, derzufolge „nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern“ sind.

Außerdem findet sich in den Erläuterungen zur Regierungsvorlage dazu (GP XXIV, Nr. 1074, 2. Absatz zu § 92 Abs. 3 Z 6b TKG 2003): „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 rechtfertigt, notwendig ist.“

Festzuhalten ist, dass die Zulässigkeit einer sofortigen Speicherung in der Vorratsdatenbank keine Nachteile im Hinblick auf das Schutzniveau nach sich zieht. Vielmehr hätte es Vorteile aus der Sicht des Rechtsschutzes, wenn Auskunftsbegehren beim Anbieter grundsätzlich unter Zugriff auf die Vorratsdatenbank abgewickelt würden, weil dort (im Gegensatz zu den betrieblichen Systemen) ein Zugriff stets nur nach dem Vier-Augen-Prinzip unter revisionssicherer Protokollierung erfolgen darf – auch wenn die Daten zugleich noch in den betrieblichen Systemen des Anbieters vorhanden sein sollten.

Falls Daten, die also auch in den betrieblichen Systemen des Anbieters noch vorhanden sind, beauskunftet werden, muss dies für die Richtigkeit der Statistik sowie allfällige prozedurale Folgen (Informationspflicht nach SPG) in der Vorratsdatenbank jeweils markiert sein. Auskunftsbeantwortungen

könnten dann immer einheitlich über den (protokollierten) Zugriff auf diese Datenbank abgewickelt werden. Der Anbieter muss dann aber jedenfalls in der Vorratsdatenbank über ein „Flag“ pro Datensatz (unterschieden nach den Datenkategorien des § 102a Abs 2 bis 4 TKG 2003) markieren, ob das Datum zugleich noch im betrieblichen System vorhanden ist oder nicht. Bei der Löschung im betrieblichen System müsste dieses „Flag“ dann den Status ändern. Diese Information in der Datenbank (zB: Vorratsdatum J/N) muss dann auch bei der Übermittlung der Antwort zu einem Auskunftsbegehren für die Statistik und zur Kenntnis der Behörden Staatsanwaltschaften und Gerichten mitgeliefert werden (siehe Absatz 2). Sollte ein Auskunftsbegehren nur die Übermittlung von betriebsnotwendigen Daten, nicht aber die Übermittlung von Vorratsdaten erlauben, wäre die Auskunft aus der Vorratsdatenbank nur zulässig, wenn markiert ist, dass die Daten auch in den betrieblichen Systemen noch vorhanden sind.

Zu bemerken ist, dass die durch Absatz 3 eröffnete Möglichkeit in der Praxis nicht von allzu großer Bedeutung sein wird. Die ursprüngliche Intention dieser Möglichkeit aus den Diskussionen zur Umsetzung lag nämlich in der Absicherung, dass Anfragen auf Vorratsdaten auf jeden Fall (wenn überhaupt Daten vorhanden sind) erfolgreich sind, auch wenn dafür Betriebsdaten ausgewertet werden müssen. Dies wird aber nun durch die Normierung des Größenschlusses in Absatz 1 grundsätzlich klargestellt. Die Bedeutung kann aber für kleinere Anbieter bestehen bleiben, wenn gerade mit wenigen Mitarbeitern ein einheitliches Konzept für die Abwicklung von Auskünften gestaltet wird. Große Anbieter werden dies in der Praxis wohl nicht in Erwägung ziehen, weil sich ja auch der benötigte Speicherplatz im Hinblick auf noch betrieblich vorhandene Daten verdoppelt. Vielmehr wird die Abfragelogik (unter Vermeidung von Doppelspeicherung) sowohl Betriebsdaten als auch die Vorratsdatenbank abfragen – letzteres allerdings nur, wenn potentiell Daten in der Vorratsdatenbank vorhanden sein könnten.

Zu § 7 Abs. 1 und 2:

Absatz 1 und 2 dieser Bestimmung sind unmittelbar unter dem Eindruck des Urteils des deutschen Bundesverfassungsgerichts (BVerfG, 1 BvR 256/08 Urteil vom 2. März 2010) entstanden. Dort wird ausgeführt: „Wenn der Gesetzgeber eine flächendeckende Speicherung der Telekommunikationsverkehrsdaten ausnahmslos vorschreibt, gehört es zu den erforderlichen Voraussetzungen, dass die betroffenen Anbieter nicht nur ihre Pflicht zur Speicherung, sondern auch die korrespondierenden Anforderungen zur Datensicherheit erfüllen können. Anknüpfend an die sachverständigen Stellungnahmen liegt es nahe, dass nach dem gegenwärtigen Stand der Diskussion grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter der Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung sichergestellt sein müssen, um die Sicherheit der Daten verfassungsrechtlich hinreichend zu gewährleisten (1 BvR 256/08, Absatz 224). Erforderlich sind gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben. Dabei steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen. Der Gesetzgeber hat dabei jedoch sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liegt. Die zu stellenden Anforderungen sind entweder durch differenzierte technische Vorschriften – möglicherweise gestuft auf verschiedenen Normebenen – oder in allgemein-genereller Weise vorzugeben und dann in transparenter Weise durch verbindliche Einzelentscheidung der Aufsichtsbehörden gegenüber den einzelnen Unternehmen zu konkretisieren. Verfassungsrechtlich geboten sind weiterhin eine für die Öffentlichkeit transparente Kontrolle (…) sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst (1 BvR 256/08, Absatz 225).“

Diesen Anforderungen wird die österreichische Umsetzung gerecht, indem sie in § 102c TKG 2003 die Notwendigkeit der Unterscheidung von Vorratsdaten und Betriebsdaten, des Vier-Augen-Prinzips beim Zugriff sowie die revisionssichere Protokollierung solcher Zugriffe schon im Gesetz normiert, während die genaueren technischen Vorgaben mit dieser Verordnung geregelt werden. Auch was die Kontrolle durch die Datenschutzkommission betrifft, wird diese abgestufte Regelungstechnik den Anforderungen gerecht. Die für die Öffentlichkeit transparente Kontrolle wird insbesondere dadurch hergestellt, dass die statistischen Daten aus der Protokollierung über die DLS (siehe § 22) gemäß § 102c Abs. 4 TKG 2003 auch dem Nationalrat und dem Datenschutzrat zugänglich sein müssen. Was das ausgeglichene Sanktionensystem betrifft, so greifen hier die bereits bestehenden ausdifferenzierten Haftungsvorschriften des DSG 2000, insbesondere durch § 1 Abs. 5, der im Verfassungsrang die Drittwirkung des Grundrechts normiert und den Rechtsweg an die Zivilgerichte eröffnet. Das Ziel des Vier-Augen Prinzips ist, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Der Zugriff muss dabei nicht durch zwei autorisierte Mitarbeiter des Unternehmens gleichzeitig erfolgen, die

Autorisierung durch die zweite Person kann auch nachträglich erfolgen. „Zeitnah zum Zugriff durch die erste Person“ gibt dabei keine absolute Zeitschranke vor, diese Formulierung indiziert vielmehr, dass zwischen dem Zugriff und der Autorisierung des Zugriffs durch eine zweite Person nicht mehr Zeit vergeht, als im Sinne der arbeitsökonomischen Ausgestaltung der betrieblichen Abläufe noch zumutbar erscheint. Die Anbieter sind zwar nicht verpflichtet, einen „Journaldienst“ zur Beantwortung von Auskunftsersuchen einzurichten, dennoch bieten in der Praxis einige (vor allem große) Anbieter die Möglichkeit, dass Anfragen außerhalb der Geschäftszeiten vor allem durch technisches Wartungspersonal rasch abgewickelt werden, wobei hier regelmäßig nur eine nachträgliche zweite Autorisierung erfolgen kann. Insgesamt muss aber jedenfalls systematisch sichergestellt sein, dass der Anbieter intern über ein effektives Kontrollsystem zur Sicherstellung der Verantwortung verfügt. Dies kann etwa dadurch erreicht werden, dass der Anbieter in kurzen Abständen eine regelmäßige Überprüfung von Zugriffen ohne zweite Autorisierung auch durch technische Ausgestaltung (zB automatische Notifikation) institutionalisiert. Die unmittelbare verfassungsrechtliche Pflicht der Provider aufgrund der Drittwirkung des § 1 Abs. 5 DSG 2000 gebietet auch eine entsprechende Dokumentation schon durch die Anbieter selbst, und nicht nur durch die Strafverfolgungsbehörden, denen die Daten im Auskunftsfall übermittelt werden.

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 Einhaltung der in Absatz 2 normierten Kriterien ist dabei durch die technische Ausgestaltung des Zugriffsregimes auf die Datenbank sicherzustellen.

Zu § 7 Abs. 3:

Der Inhalt der Protokollierung ist bereits durch § 102c Abs. 2 TKG 2003 detailliert vorgegeben und wird in dieser Verordnung einerseits zur Rechtsklarheit wiederholt, andererseits im Sinne der Eindeutigkeit der zu protokollierenden Informationen um Verweise auf Bestimmungen innerhalb der Verordnung im Zusammenhang mit der Durchlaufstelle ergänzt. Ergänzungen sind insbesondere im Hinblick auf die Erfassung von Speicherzeiträumen bzw. des Datums notwendig. So soll das Datum der Anfrage gemäß Z 3 sich auf die jeweilige Hinterlegung in der Durchlaufstellte beziehen. Diese Daten sind für den Anbieter überdies nur sehr schwer automatisiert zu erfassen (bzw. zu verpacken, da z.B. die Zustellung in das Postfach der DLS nach Erstellung des Protokollfiles beim Anbieter geschieht). Daher wird hierzu in § 23 normiert, dass diese Informationen über die DLS direkt protokolliert und an den Anbieter weitergeleitet werden. Der Anbieter kann sodann diese Protokollinformationen von der DLS für seine interne Protokollierung automatisiert weiterverwenden.

Zu Z 4 wird konkretisiert, dass das Datum zur Aufschlüsselung der abgefragten Datensätze sich auf den Beginn des Kommunikationsvorgangs bezieht, zumal dieser Wert auch im Rahmen der Vorratsdaten gemäß § 102a Abs. 2 bis 4 TKG 2003 relevant ist. Die Ergänzung zu Z 5 basiert auf dem Umstand, dass dem Anbieter nur das Datum der Anordnung gemäß § 138 Abs. 3 StPO (sog. Anbieterausfertigung) bzw. das Datum der Anordnung nach § 53 Abs. 3a oder 3b SPG bekannt ist. Für die Berechnung der Speicherdauer muss der Zeitpunkt der Anordnung der Auskunft mit dem Zeitpunkt der Speicherung als Vorratsdatensatz bzw als Betriebsdatensatz verglichen werden. Da die Anordnung nur ein Datum aber keinen genauen Zeitpunkt enthält, ist für die Berechnung auch nur das Datum der Speicherung als Vorratsdatum relevant, weshalb in Z 5 im Gegensatz zu § 102c Abs. 2 Z 5 TKG 2003 nur das Datum und nicht der Zeitpunkt genannt ist, um Klarheit für die Protokollierung zu schaffen.

Durch Z 8 soll ermöglicht werden, der Forderung von Art 10 der RL 2006/24/EG nachzukommen und auch statistische Daten über die Fälle in welchen Vorratsdaten beauskunftet werden, zu erheben. Die Angabe des zugrundeliegenden Straftatbestands soll bereits beim Auskunftsbegehren auf Seiten der Behörde bzw. der Staatsanwaltschaft oder des Gerichts eingetragen werden. Ein entsprechendes Eingabefeld dafür ist in § 19 vorgesehen, das automatische Abgreifen dieser Information über die DLS für die Statistik ist in § 23 Abs. 2 geregelt.

Zu § 8 Abs. 1:

Siehe die Ausführung zur grundsätzlichen Einigung über das System der DLS und insbesondere die Feststellungen aus dem FIT-Ausschuss bei den Erläuterungen zu § 1.

Zu § 8 Abs. 2 und 3:

Die Vorgaben zur sicheren Übertragung der Daten im Schutzbereich des Telekommunikationsgeheimnisses macht § 94 Abs. 4 TKG 2003: „Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender

und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln." Die Erläuternden Bemerkungen zu § 94 Abs. 4 TKG 2003 (1074 der Beilagen XXIV. GP) führen dazu aus: „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."

Unter einer anspruchsvollen Verschlüsselung ist eine Verschlüsselung zu verstehen, die nach dem derzeitigen Stand der Technik ohne erheblichen Aufwand nicht zu überwinden ist. Dabei ist durch weitere organisatorische Maßnahmen sicherzustellen, dass die Schlüssel und gegebenenfalls das Passwort ebenfalls sicher aufbewahrt werden. Absatz 2 ordnet daher ausdrücklich eine asymmetrische Verschlüsselung an. Bei einem asymmetrischen Verschlüsselungsverfahren besitzt jede der kommunizierenden Parteien ein Schlüsselpaar, das aus einem geheimen Teil (private key) und einem nicht geheimen Teil (public key) besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln. Die kommunizierenden Parteien müssen keinen gemeinsamen geheimen Schlüssel kennen, das Verfahren wird daher auch als Public-Key-Verfahren bezeichnet. Dafür ist eine Public-Key-Infrastruktur erforderlich, über die (vereinfacht dargestellt) die Ausstellung vertrauenswürdiger digitaler Zertifikate zur sicheren Übertragung organisiert wird. Die zentrale Herausforderung liegt darin, sicherzustellen, dass der öffentliche Schlüssel wirklich echt ist. Der Vorteil ist eine deutliche Minimierung des Sicherheitsrisikos, da jeder Benutzer nur seinen eigenen privaten Schlüssel geheim halten muss. Im Gegensatz dazu muss bei einem symmetrischen Verschlüsselungssystem jeder Teilnehmer alle Schlüssel geheim halten, was mit steigendem Aufwand verbunden ist, je mehr Teilnehmer daran beteiligt sind (große Zahl an Schlüsseln). Nachteilig ist, dass asymmetrische Kryptosysteme aufgrund der Verschlüsselungsalgorithmen im Vergleich zu den symmetrischen Verfahren eher langsam sind.

Hybride Verschlüsselungssysteme: Der Geschwindigkeitsnachteil asymmetrischer Verfahren wird in der Praxis durch die Verwendung hybrider Systeme umgangen. Dabei werden die zu übertragenden Daten mit einem zufällig generierten Schlüssel (sog. „session key") symmetrisch verschlüsselt (deutlich schneller) und der jeweils verwendete Schlüssel unter Verwendung einer asymmetrischen Verschlüsselung an die Teilnehmer verteilt. Diese Variante löst das Schlüsselverteilungsproblem und erhält dabei den Geschwindigkeitsvorteil der symmetrischen Verschlüsselung. Das Verfahren entspricht dem Stand der Technik und wird der Anforderung einer technisch anspruchsvollen Verschlüsselung jedenfalls gerecht. Es bleibt jedoch der technischen Spezifikation zur DLS vorbehalten, wie das asymmetrische Verschlüsselungsverfahren der Inhaltsverschlüsselung ausgestaltet wird.

Zu § 8 Abs. 4:

Eine wesentliche Forderung zur Datensicherheit sind die Identifikation und die Authentifizierung des jeweiligen Partners. Das Signaturgesetz kennt dazu die Funktionalität der qualifizierten Signatur, die eine Personenbindung enthält, und der fortgeschrittenen Signatur, die für Unternehmen besser geeignet ist. Das Bundesministerium für Inneres hat die fortgeschrittene Signatur im Portalverbund implementiert und verwendet diese zur Identifikation von Organisationen. Die fortgeschrittene Signatur sollte durch die begleitenden Sicherheitskriterien im Rahmen des Portalverbunds datenschutzrechtlichen Standards genügen. Generell ist es sinnvoll, den Portalverbund, das ist eine Kommunikationsplattform für Bundesdienststellen, auch für die Übermittlung von Anfragen zur Vorratsdatenspeicherung einzusetzen. Die Vorteile der DLS mit Eingliederung in den Portalverbund im Hinblick auf sichere Identifikation, Authentifizierung sowie der sicheren verschlüsselten Übermittlung von personenbezogenen Daten waren in der Diskussion von Beginn an unbestritten. Näheres dazu siehe in den Erläuterungen zu § 13.

Zu § 9:

Am 7.4.2011 wurde die TKG Novelle zur Umsetzung der Vorratsdatenspeicherung im FIT Ausschuss des Nationalrats diskutiert (siehe dazu den Ausschussbericht: 1157 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXIV. GP). In diesem Rahmen wurde von Ausschussfeststellung beschlossen, in der die grundsätzlichen Annahmen zur DLS wie folgt beschrieben werden: „Für die Datensicherheit und die Nachvollziehbarkeit der Zugriffe auf den Datenvorrat ist das Zusammenspiel der Bestimmungen der §§ 94 Abs. 4 und 102c TKG 2003 von besonderer Bedeutung. Während § 94 Abs. 4 den Aspekt der technischen Datenintegrität und der Determinierung der Verordnungsermächtigung über

die Art der Verschlüsselung betrifft und die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten identifiziert, um durch sichere ‚Identifikation und Authentifizierung von Sender und Empfänger' sicherzustellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden, Staatsanwaltschaften und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht, regelt § 102c Zugriffs- und Sicherheitsbestimmungen. Einerseits muss jeder Zugriff auf Vorratsdaten durch zwei Personen mit einer besonderen Ermächtigung hierzu autorisiert sein, um zu gewährleisten, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Andererseits müssen Zugriffe auf Vorratsdaten beim Anbieter revisionssicher protokolliert werden. 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, wozu etwa bei Anordnungen der Staatsanwaltschaft auch die Angabe der Geschäftszahl der ermittelnden Kriminalpolizei zählt. Der Ausschuss geht davon aus, dass sämtliche Zugriffe und Übermittlungen von wem auch immer auf Vorratsdaten gemäß § 94 Abs. 4 TKG 2003 lückenlos protokolliert werden. Der Ausschuss geht weiters davon aus, dass ein automatisches zentrales System der Protokollierung solcher Abfragen und Übermittlungen notwendig ist, wobei unter dieser Protokollierung nicht die in § 102c Abs. 2 genannte zu verstehen ist. Sie wird vielmehr nur jene Daten umfassen, die zur statistischen Auswertung und zur Verknüpfung mit der gemäß § 102c Abs. 2 erfolgenden Protokollierung dient. Wünschenswert ist die Einrichtung einer ‚Datendrehscheibe' (‚Durchlaufstelle', kurz: DLS). Da jeder Auskunftsfall über die DLS mit einer fortlaufenden einmaligen Nummer versehen wird, kann im Falle einer nachprüfenden Kontrolle über die Protokollierung bei der DLS zur Protokollierung beim Anbieter gemäß § 102c Abs. 2 verknüpft werden. Zugang zu den übermittelten personenbezogenen Daten soll die DLS selbst nicht bieten, die Daten liegen dort nur verschlüsselt bis zur Abholung bereit und werden bei der Abholung automatisch gelöscht."

Die Abwicklung der Anfragen und Auskünfte soll über die DLS erleichtert werden, insbesondere die Einbindung über den Portalverbund bringt Synergie-Effekte, weil damit auf Seiten des BMI bereits gute Erfahrungen bestehen. Die DLS ist zugleich die ökonomischste Art der Umsetzung, weil eine sichere Anbindung unter Transport- und Inhaltsverschlüsselung zwischen voraussichtlich 15 anfrageberechtigten Behörden und ca. 200 speicher- und auskunftspflichtigen Anbietern (nach aktuellen Angaben der RTR) über eine zentrale Lösung beim Datenaustausch wesentlich einfacher zu garantieren ist als bei einer dezentralen Kommunikation, zB per E-Mail. Mit der zentralen Lösung der DLS werden sowohl das Fehler- als auch das Sicherheitsrisiko minimiert.

Zu § 10:

Dass das BMVIT die Verantwortung für den Betrieb der Durchlaufstelle übernimmt, ist die sauberste Lösung für die datenschutzrechtlichen Problemstellungen, die mit der zentralen Abwicklung aller Datenauskünfte nach § 94 Abs. 4 TKG 2003 verbunden sind. Der Vorschlag, den Betrieb der DLS und die Beauftragung zur technischen Spezifikation und Umsetzung durch das BMVIT durchzuführen, hat den Grund, dass damit die Bedarfsträger vom Auftraggeber getrennt werden. Weil dem BMVIT keine Aufgaben obliegen, für die eine Verarbeitung von Vorratsdaten notwendig wäre, ist es eine neutrale Stelle ohne eigenes Interesse an den zu übermittelnden Inhalten. Das Interesse des BMVIT am Betrieb der DLS ist darin zu sehen, dass diesem Bundesministerium obliegt, über die Einhaltung der Bestimmungen des TKG 2003 zu wachen, wozu insbesondere auch das Kommunikationsgeheimnis des § 93 TKG 2003 zählt.

Durch die Eigenschaft als Auftraggeber der DLS wird das BMVIT jedoch nicht zum datenschutzrechtlichen Auftraggeber im Hinblick auf die übermittelten Daten. Einerseits besteht nämlich die „Dienstleistung" der DLS nur darin, allen Beteiligten Postfächern für den Datenaustausch zu bieten und bestimmte Aufgaben zur sicheren Übertragung der Daten zu übernehmen. Darüber hinaus müssen die Daten auf eine Weise verschlüsselt werden, dass die DLS gar keine Möglichkeit hat, die Inhalte einzusehen. Die Protokollierung der DLS beinhaltet rein statistische Werte ohne Personenbezug. Die fortlaufende einmalige Nummer jedes Auskunftsvorgang („Unique ID") kann lediglich eine nachprüfende Kontrolle (zB durch Datenschutzkommission, Rechtsschutzbeauftragten oder Gericht) erleichtern, der Personenbezug kann aber über die DLS selbst nicht hergestellt werden.

Nur in einer einzigen Hinsicht ist das BMVIT als datenschutzrechtlich verantwortlicher Auftraggeber zu sehen, nämlich in Bezug auf die Verarbeitung der Information, welche Benutzer überhaupt Auskunftsbegehren über die DLS abwickeln. Ansonsten sind alle personenbezogenen Informationen in der DLS nur verschlüsselt vorhanden, damit sind sie aus der Perspektive der DLS nur indirekt personenbezogen.

Das Bundesrechenzentrum ist überhaupt funktionell Dienstleister im Sinne des § 4 Z 5 DSG, dies jeweils für den Auftraggeber, für dessen Anwendung Daten an die DLS übergeben oder von der DLS übernommen werden. Das heißt, wenn die DLS beispielsweise eine Anordnung der Staatsanwaltschaft in das Postfach des Anbieters zustellt, geschieht dies im Dienst der Behörde, Staatsanwaltschaft oder des Gerichts, von welcher/m die Anordnung stammt. Die Stellung eines datenschutzrechtlichen Auftraggebers kommt dem Bundesrechenzentrum im Hinblick auf den Betrieb der DLS in keiner Phase zu.

Zu § 11:

Die Auditierung betrifft nur die Datensicherheit bei der Durchlaufstelle, nicht aber die Anbieterimplementierungen. Siehe ansonsten die Erläuterungen zu § 18.

Zu § 12:

Die DLS ist ein Modell für technische und prozedurale Abläufe, nicht jedoch eine Art neue Behörde oder Dienststelle. Hierfür muss sich in einer sicheren öffentlichen Infrastruktur (wie jener des Bundesrechenzentrum) ein Server befinden, über den - technisch gesehen - die Anfragen abgewickelt werden. Eine Kommunikation über diesen Server ist dabei nur möglich, wenn die entsprechenden Stellen über eine Berechtigung (Authentifizierung) verfügen.

Für die Ausführung der Mailbox-Funktion der DLS kann es vorteilhaft sein, Webapplikationen und Webservices technisch zu kombinieren, da ein Webservice von der Clientseite flexibel angesprochen werden könnte und somit ein höheres Maß an Benutzerkomfort durch Ausgestaltung des Clients auf der jeweiligen Teilnehmerseite (Behörden oder Anbieter) gestaltbar wäre.

Zu § 13:

Die Unique-ID erfüllt die zentrale Funktion, zusammengehörige Transaktionen zu korrelieren, wobei jede spezifische Behördenanfrage an einen bestimmten Anbieter eine Transaktion darstellt. Beispiel: Eine Anfrage ergeht an zwei Anbieter. Die Unique-ID könnte aus einem einmaligen „Anfrageteil“ sowie einer Anbieter-ID bestehen (1234567-1, 1234567-2); alternativ müsste es eine eigene ID zu dieser Anfrage für jeden Anbieter geben (1234567, 1234568). Die konkrete Ausgestaltung ist in der technischen Spezifikation zur DLS zu klären.

Von Seiten des BMJ wurde in der Diskussion die Anforderung formuliert, dass lückenlos nachvollziehbar sein muss, welche Personen von Anfang bis Ende an einem Auskunftsvorgang beteiligt waren, um allfälligem Missbrauch effektiv begegnen zu können. Die sichere Anbindung der Behördenseite über den Portalverbund bietet sich dabei an, weil hierzu beim Bundesrechenzentrum bereits die vollständige Infrastruktur und ein reicher Erfahrungsschatz besteht. Für die Seite der Anbieter ist ein Portal zu schaffen, dass dem Portalverbund der Behörden nachgebildet ist und denselben Sicherheitsanforderungen entspricht. Auch hierzu besteht beim bereits ein großer Erfahrungsschatz, etwa aus der Realisierung des Elektronischen Rechtsverkehrs (ERV) für die Kommunikation zwischen Gerichten und professionellen Parteienvertretern (Rechtsanwälte, Notare).

Das Prozedere der internen Authentifizierung zur Sicherstellung der konkreten Berechtigung der handelnden Personen muss klar geordnet sein, kann aber im Konzept des Portalverbunds auch intern bei der jeweiligen Organisation (Behörden- oder Anbieterseite) erfolgen und muss nicht zwingend über die DLS technisch realisiert werden, sofern die Anforderungen der Sicherheitsklasse 3 des Portalverbunds erreicht werden; Im Detail vgl. "Spezifikation Sicherheitklassen für den Zugriff von Benutzern auf Anwendungen", Version 2.1.0, 8.2.2008, ["SecClass 2.1.0"; Anhang zur Portalverbundvereinbarung pvv 1.0, 21.11.2002]. Es sind die Konventionen des Portalverbunds einzuhalten, wobei die Bundesrechenzentrum GmbH Teilnehmer am Portalverbund ist. Die Stammportale werden von den einzelnen Institutionen betrieben (oder von deren Dienstleistern).

Der Portalverbund Österreich ist eine E-Government Anwendung und wird auf der Website „Digitales Österreich“ (http://www.digitales.oesterreich.gv.at/site/5288/default.aspx) wie folgt beschrieben: „Der Portalverbund ist ein Zusammenschluss von Verwaltungsportalen zur gemeinsamen Nutzung von bestehender Infrastruktur. Grundsätzlich haben Portale den Vorteil, dass mehrere Applikationen über einen Punkt zugänglich werden. Die Identität der Benutzenden wird im Zuge des Anmeldevorganges am Portal nur einmal überprüft. Die Benutzenden müssen sich daher nur einmal "ausweisen" um auf mehrere Ressourcen zugreifen zu können. Betreibenden von Anwendungen wird es im Portalverbund ermöglicht, die Authentifizierung und Autorisierung zu Portalen in Vertrauensstellung auszulagern. Anstelle einer eigenen Benutzerverwaltung für jede Anwendung wird nur mehr eine Benutzerverwaltung am Stammportal benötigt. Dadurch wird die Benutzerverwaltung vereinfacht und ein Single Sign-On unterstützt. Die Benutzerverwaltung bleibt technisch und organisatorisch weiterhin im Verantwortungsbereich der personalführenden Stelle. Organisationen, die am Portalverbund teilnehmen,

können ihre lokale Benutzerverwaltung nicht nur für interne Anwendungen, sondern auch für externe Applikationen und Anwendungen verwenden. Betreiber von Applikationsportalen bleibt somit die externe Benutzerverwaltung erspart.

Die Teilnahme am Portalverbund wird durch die Portalverbundvereinbarung geregelt. Diese enthält Rechte und Pflichten, die von den teilnehmenden Portalbetreibenden einzuhalten sind. Zwischen den Betreibenden von Stammportalen, welche die Benutzenden verwalten und Anwendungsbetreibenden wird so ein Vertrauensverhältnis hergestellt. Alle Vereinbarungen werden bei einem Depositar, das ist jenes Bundesministerium, das für die IT-Koordination des Bundes zuständig ist, aufbewahrt. Technisch und organisatorisch ist die Kommunikation im Portalverbund durch das Portalverbundprotokoll (PVP) und durch die Festlegung von Sicherheitsklassen geregelt. Die Definition von Sicherheitsklassen im Portalverbund ermöglicht es einer Anwendung zu prüfen, ob Benutzende die für die Nutzung der Anwendungsfunktion erforderlichen Sicherheitsauflagen erfüllen. Für Mitarbeitende von Institutionen, die am Portalverbund teilnehmen, ergeben sich keine Veränderungen.

Der Betreibende von Anwendungen bestimmt, welche Anwendungen über welches Anwendungsportal zugänglich sind. Der Betreibende legt unter Beachtung sämtlicher Datenschutzbestimmungen fest, welche Stellen beziehungsweise Kategorien von Stellen über ein Anwendungsportal zugriffsberechtigt sind und definiert für seine Anwendungen je nach Aufgabenstellungen der Benutzenden Rollen mit entsprechenden Rechteprofilen. Der Stammportalbetreibende muss unter anderem sicherstellen, dass über das eigene Portal nur berechtigte Benutzende ordnungsgemäß auf Anwendungen zugreifen. Der Anwendungsportalbetreiber muss sicherstellen, dass nur über ein Stammportal autorisierte Benutzende auf die durch das Portal erreichbaren Datenanwendungen zugreifen können. Die Übereinstimmung des Rechteprofils der Benutzenden mit den Zuständigkeiten der zugriffsberechtigten Stelle muss geprüft werden. Erforderliche Datensicherheitsmaßnahmen sind ebenfalls zu organisieren und umzusetzen. Betreiber von Stammportalen können sich für den technischen Betrieb eines Dienstleistenden bedienen. In diesem Fall ist vom Dienstleistenden eine Vereinbarung zu unterzeichnen, die gewährleistet, dass auch dieser alle technischen und organisatorischen Vorkehrungen einhält, auf denen das Vertrauensverhältnis der Portalverbund-Teilnehmenden beruht.“

Zu § 14:

Die Anzahl der zugangsberechtigen Dienststellen der Sicherheitsbehörden wird durch Erlass der Bundesministerin für Inneres festgelegt jener im Bereich der Justizbehörden wird durch das Bundesministerium für Justiz festgelegt und der Bundesrechenzentrum GmbH für die Spezifikation der Durchlaufstelle bekanntgegeben.

Zu § 15:

Ein wesentlicher Vorteil des Konzepts der DLS ist die Verringerung der Kommunikationswege. In den Diskussionen ging man von 15 anfrageberechtigten Behörden und 200 auskunftspflichtigen Netzen (alle die der Verpflichtung zur Entrichtung des Finanzierungsbeitrages zur RTR unterliegen) aus. Insbesondere kleinere Anbieter haben geringere Ressourcen. Daher ist es die effizienteste Vorgangsweise, nur mit einer Stelle zu kommunizieren. Spezielle technische Voraussetzungen auf Anbieterseite sind keine nötig, da die DLS über eine sichere Verbindung (die wahrscheinlich über das Protokoll „https“ realisiert werden wird) praktisch mit jedem gängigen Browserprogramm erreichbar wäre. In welchem Ausmaß ein Anbieter seine Prozesse bis zur Erstellung des „CSV-Files“ mit den begehrten Daten automatisiert, bleibt ihm selbst überlassen, was insbesondere für kleinere Anbieter wichtig ist, bei denen eine teure Automatisierung in keinem Verhältnis zur Zahl der jährlichen Auskünfte steht.

Zu § 16:

Bei der Anbindung der Anbieter ist sicherzustellen, dass auf Anbieterseite möglichst flexibel auf die DLS zugegriffen werden kann, damit auch außerhalb der Geschäftszeiten eine möglichst rasche Beantwortung des Auskunftsbegehrens erfolgen kann.

Die Sicherheitsstufe 3 aus der “Definition der Sicherheitsstufen in der Kommunikation Bürger – Behörde im Bereich E-Government” ist abrufbar unter http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=21832 und dort wie folgt beschrieben:

„Die höchste Sicherheitsstufe im Bereich E-Government, die auch für die Kommunikation Verwaltung – Verwaltung angewandt werden kann, wenn dies die Vertraulichkeit erfordert, wurde darauf ausgelegt, dass sie kompromittierten Endgeräten stand hält. Bei Anwendung dieser Sicherheitsstufe haben Client und Server Klarheit darüber, wer kommuniziert und können auch von der Vertraulichkeit im Rahmen der Sicherheit der kryptographischen Schlüssel und Algorithmen ausgehen.

Die Sicherheit wird mit einer TLS-Verbindung erreicht und basiert auf Zertifikaten mit Verwaltungseigenschaft. Die Bindung der Zertifikate an Client und Server ist technisch so abzusichern,

dass sie auch kompromittierten Endsystemen standhält. Die für den Ablauf notwendigen Zertifikate werden direkt vom Server bzw. Client in die sichere TLS-Verbindung eingebunden. Es wird somit, anders als bei Stufe II, eine automatische und in die Verbindungsprotokolle integrierte Überprüfung der Serveridentität möglich. Dieser Mechanismus kann nun auch automatisch man-in-the-middle Attacken erkennen.

Die Zertifikate des Clients und des Serves der TLS-Verbindung werden in vertrauenswürdigen Komponenten gehalten und sind technisch vor Modikation geschützt. Dies kann zum Beispiel durch den Einsatz von hardware security modules (HSM), auch Kryptoboxen genannt, erreicht werden. Diese Sicherheitsmodule sind in verschiedenen Formaten (Box, Tischgerät, PC-Karte, Chipkarte) erhältlich und werden in der Regel als interne Karten, als periphere Geräte oder über einen Adapter (für die Chipkarte) an den Hostrechner (Zentralrechner, Server, PCs) angeschlossen. Eine weitere Möglichkeit zur Absicherung besteht im Schaffen einer vertrauenswürdigen Softwareumgebung, unter anderem mit sicherem boot - Prozess, zuverlässigem Betriebssystem und digital signierter Software. Diese Sicherheitsstufe ist für Transaktionen mit sensiblen Daten nach dem Datenschutzgesetz geeignet (analog Sicherheitsklasse 3 im Portalverbund).“

Zu § 17:

Die in § 17 klar vorgezeichneten Abläufe der Zustellung von Auskunftsbegehren und Antworten in die Postfächer der jeweils Beteiligten sind zentral für die Architektur der DLS und erfüllen auch eine wesentliche datenschutzrechtliche Funktion. Damit ist nämlich auch von der technischen Konzeption her eindeutig, dass die Auskunft über Daten, die vom Schutzbereich des DSG 2000 und des Kommunikationsgeheimnisses des § 93 TKG 2003 erfasst sind, immer in Form eines „push“ aus der Sicht des Anbieters erfolgt. Lediglich die Abholung der Anordnung durch den Anbieter einerseits und die Abholung der Antwort durch die Behörde andererseits kann durch den Einsatz von Webservices teilautomatisiert werden. Dadurch entsteht aber keine vollautomatisierte Schnittstelle mit unmittelbarem Zugriff der Behörden auf die Datenbanken der Anbieter. Die Mediatisierung über die DLS als Postfachsystem stellt eine faktisch effektive Begrenzung der staatlichen Kontrollmacht dar.

Zu § 18:

Die fortgeschrittene Signatur stellt die praktikabelste Lösung dar und beinhaltet die Möglichkeit eines Zertifikats auf Unternehmensbasis. Die Zuordnung zu Einzelpersonen ist in den Protokolldateien ersichtlich und muss daher nicht unbedingt durch die Signatur erfolgen. Durch die Signatur wird auch ein Hashwert zur Wahrung der Datenintegrität überflüssig. Mit der Signatur kann im Gegensatz zum bloßen Hashwert auch die Identität des Signators überprüft werden. Man weiß dann nicht nur, dass die Daten korrekt sind, sondern dass sie auch tatsächlich vom Signator stammen. Bei der Verwendung eines bloßen Hashwerts könnte ein „Man-In-The-Middle“ die Nachricht und den Hash abfangen, beides ändern, und die geänderten Versionen der Nachricht und des Hashwerts weiterschicken. Hashwerte (in diesem Kontext) alleine schützen nur vor zufälligen Veränderungen, Signaturen auch vor absichtlichen Manipulationen.

Für die verschlüsselte Übermittlung von Auskunftsdaten wird der öffentliche Schlüssel (auch: public key) des jeweiligen Empfängers verwendet. Nur dieser kann dann mit seinem private Schlüssel (auch: private key) die Auskunft im Klartext lesen. Die bei der DLS angesiedelte Aufgabe der Schlüsselverwaltung bedeutet, dass die öffentlichen Schlüssel zur Verschlüsselung der Daten am DLS-Server technisch gesehen durch sog. „Zertifikate“ hinterlegt werden. Die Verschlüsselung der Anfrage und der Antwort kann nur bei der Behörde bzw. beim Anbieter stattfinden. Für die Verschlüsselung wird der „private key“ benötigt und dieser kann niemals von der DLS erzeugt oder gespeichert werden. Die DLS ist nur für die Transportverschlüsselung zuständig und kennt natürlich die dafür notwendigen Schlüssel.

Zu § 19:

Im Zuge der Diskussion zum zeitlichen und finanziellen Rahmen der Umsetzung eines Datensicherheitskonzepts wurde die so genannte "Implementierung Light" der Durchlaufstelle diskutiert. Darunter sind jene Änderungen im Konzept zu verstehen, die sich seit der ersten Vorstellung des Konzepts der Durchlaufstelle aus der Diskussion ergeben haben. Dazu gehört einerseits die Implementierung im Rahmen des Portalverbundes. Damit kann die interministerielle Seite und die Anbieterseite der Implementierung getrennt werden. Für die Spezifikation und Implementierung der interministeriellen Seite ist keine Einbindung der Netzbetreiber mehr erforderlich. Die zweite Eigenschaft der "Durchlaufstelle Light" betrifft die Formalisierung der Anfragen. Für Anfragen nach dem SPG ist heute bereits eine Verwendung von normierten Formularen gemäß Erlass des BIM vorgesehen. Bei Anfragen nach der StPO gibt es zwar Formulare, denen jedoch kein zwingender Erlass zugrunde liegt und die in der Praxis auch nicht durchgehend verwendet werden. Anfragen nach der StPO enthalten als Beilage die Anordnung des Staatsanwalts mit der prosaischen Beschreibung des Auskunftsbegehrens.

Mittelfristig wurde in der Diskussion das Ziel formuliert, auch für Datenanfragen nach der StPO eine Formalisierung über Eingabemasken zu erreichen. Es sollte allerdings zugleich verhindert werden, dass Anbieter durch den Vergleich einer allenfalls per Webmaske ausgeführten Anordnung mit dem beiliegenden Original der StA Anordnung einen erhöhten Aufwand haben. Zur Optimierung der Betriebsabläufe ist jedenfalls ein Rückkanal vorzusehen. Das heißt etwa, dass bei Differenzen zwischen den begehrten Daten und der beiliegenden Anordnung der StA eine Antwort an die abfrageberechtigte Stelle zu schicken ist, mit der darauf hingewiesen wird, dass diese Fehler zu korrigieren sind. Zu diesem Zweck regelt die Verordnung in § 20 die Möglichkeit von „Zusatzinformationen“. Für die Implementierung der Durchlaufstelle bedeutet dies, dass in der Phase der ersten Implementierung jedenfalls StPO-Anordnungen übermittelt werden können müssen, ohne dabei an bestimmte online-Formulare über die Webmaske gebunden zu sein.

Zusammengefasst bedeutet das:

Die DLS ist zwingend die Drehscheibe zur Kommunikation für alle Auskunftsfälle. Kern ist dabei, dass die jeweilige Seite ihre Anforderung/Antwort sicher über die DLS samt dem notwendigen Anhang (Anbieter-Anordnung nach § 139 Abs. 3 StPO, CSV-Datei mit den begehrten Daten) übermittelt.

Die Spezifikation der DLS muss jedoch nicht enthalten, wie auf Seiten der Behörden die jeweiligen Web-Formulare aussehen. Eine Formalisierung wird jedoch auf Behördenseite aus eigenem Interesse einer einheitlichen und geordneten Abwicklung angestrebt.

Auch auf der Seite der Anbieter muss nicht spezifiziert werden, ob, inwieweit und wie die Beantwortung von Auskunftsbegehren (teil-)automatisiert wird. Durch die Anlage zu dieser Verordnung wird einheitlich festgelegt, wie die CSV-Datei aussehen muss. Wie die einzelnen Anbieter diese Datei „befüllen“ bleibt deren Entscheidung.

Der Vorschlag enthält lediglich, dass bei der Übermittlung eines Auskunftsbegehrens via DLS ausgewählt werden muss, auf welcher Rechtsgrundlage die Anordnung ergeht. Dies dient der statistischen Erfassung über die DLS und beinhaltet keine Determinierung der Formulare oder Webmasken, die bei den Behörden für die Anordnungen verwendet werden. Eine Determinierung ergibt sich allerdings aus der Spezifikation der Felder der CSV-Datei gemäß dem Vorschlag in der Anlage.

Zu § 20:

Die CSV-Dateien werden mittels sicherem Filetransfer und Inhaltsverschlüsselt an die Durchlaufstelle übermittelt. Zusatzinformationen könnten allenfalls über ein Web-Interface zu der entsprechenden Abfrage eingegeben werden. Diese Zusatzinformationen könnten etwa Gründe für eine Leer-Meldung beschreiben. Ob und in welchem Ausmaß ein Web-Interface auf Seiten der DLS zur Verfügung gestellt werden soll, wird Gegenstand der Diskussion zur Spezifikation der DLS sein. Jedenfalls ist dabei zu bedenken, dass die DLS gegenüber Inhalten der Auskünfte "blind" sein soll, personenbezogene Informationen sollten also nicht als Zusatzinformation übermittelt werden, weil diese gegenüber der DLS nicht inhaltsverschlüsselt werden, sondern nur durch die Transportverschlüsselung vor Zugriffen von außen sicher sind. Alternativ ist auch möglich nach dem sonstigen Aufbau der EP 020 die möglichen Dateiformate und Dateinamen für Zusatzinformationen zu definieren. Auf diese Weise könnten auch personenbezogene Zusatzinformationen mit Inhaltsverschlüsselung übertragen werden, die aus Sicht der DLS nicht zugänglich sind. Für Anfragen, die nicht zwischen Vorratsdaten und betriebsnotwendigen Daten unterscheiden (z.B. nach § 53 Abs. 3a und 3b SPG) muss jedenfalls die Information übermittelt werden, ob Vorratsdaten für die Beantwortung dieser Anfrage verwendet wurden. Diese Information wird von den Anbietern als "Zusatzinformation" übermittelt (siehe § 6 Abs. 2).

Allenfalls könnte für die Übertragung von Zusatzinformationen eine Textdatei (.doc/.txt) zum Einsatz kommen, welches leicht wie eine “reale Antwort” mit dem Schlüssel der Behörde verschlüsselt wird. In diesem Fall hier wäre die Benennung dieser Datei in der Spezifikation zur DLS zu regeln.

Zu § 21:

In den Grundsatzdiskussionen zur DLS wurde die Möglichkeit einer elektronischen Stammdatenauskunft im Bereich der Telefon-Anbieter als optionale Variante besprochen. Festgehalten wird aus dieser Diskussion, dass es aus Sicht des BMI nicht darum geht, eine unmittelbare Schnittstelle zur Kundendatenbank des Anbieters herzustellen. Vielmehr besteht der Wunsch nach einem elektronischen Hin- und Rückkanal, der zu einer möglichst raschen Abwicklung führt. In wie weit ein Anbieter solche Auskunftsvorgänge automatisiert, soll dem jeweiligen Anbieter überlassen bleiben - insbesondere im Hinblick auf kleine Anbieter, die nur wenig betroffen sind - solange die Auskunft in vertretbarer Zeit abgewickelt werden kann. Große Anbieter könnten durch eine (Teil-)Automatisierung in eigener Verantwortung die Auskünfte optimieren. Wesentlich ist, dass eine Anbindung an ein elektronisches System für Stammdatenauskünfte über die DLS nicht gesetzlich verpflichtend als ausschließliche

Übermittlungsvariante für alle Anbieter eingerichtet werden muss. Durch die Verordnung soll lediglich die optionale Möglichkeit einer solchen Anbindung normiert werden. Wenn zumindest die großen (insbesondere Mobilfunk-) Anbieter sich anschließen, würde der Zweck erfüllt.

In einer solchen Anfrage würde eine Rufnummer übermittelt. Dazu sind vom Anbieter die zugehörigen Stammdaten für den Anfragezeitraum, längstens aber 6 Monate zurück, zu ergänzen. In der bisherigen Praxis werden vor einer Anordnung zu einer Verkehrsdatenauskunft zunächst zu einer (oder mehreren) bestimmten Nummer Stammdatenauskünfte begehrt, wobei diese Auskunftsbegehren an alle in Frage kommenden Anbieter gerichtet werden (bei Mobilfunk ist die Zahl dabei überschaubar, weil es nicht so viele Anbieter gibt). Aufgrund der Antworten weiß die Behörde dann, für welche Zeiträume bei welchem Anbieter Verkehrsdaten vorhanden sein könnten, und kann das Auskunftsbegehren zielgerichtet stellen. Die Stammdatenauskunft wird in der Praxis auch deshalb regelmäßig vorgelagert, weil die Kriminalpolizei damit bereits einen ersten Filter setzt, welche Teilnehmeranschlüsse ermittlungsrelevant sein könnten. Als Antwort werden Stammdaten, der entsprechende Zeitraum und die Information „aktiv“ oder „inaktiv“ übermittelt. Es können auch bei einem Anbieter zur gleichen Rufnummer während der letzten 6 Monate mehrere Stammdatensätze anfallen (z.B. bei einer Übertragung der Rufnummer).

Die Praxis der vorgelagerten Stammdatenauskünfte wird auch im zukünftigen Auskunftsregime über die DLS weiterhin relevant bleiben. Um solche Stammdatenabfragen zu erleichtern bzw. zu beschleunigen sieht der Entwurf zur Verordnung vor, dass Anbieter im Einvernehmen mit den abfrageberechtigten Behörden für eine Abwicklung von Stammdaten-Auskünften via DLS optieren können. Eine Abwicklung von Stammdatenauskünften über die DLS soll nicht verpflichtend als ausschließliche Übermittlungsvariante für alle Anbieter eingerichtet werden. Außerdem soll keine unmittelbare Schnittstelle zur Kundendatenbank des Anbieters hergestellt werden, diese soll vielmehr über die DLS mediatisiert werden. Es soll lediglich einen elektronischen Hin- und Rückkanal geben, der zu einer möglichst raschen Abwicklung führt. In wie weit ein Anbieter solche Auskunftsvorgänge automatisiert, soll dem jeweiligen Anbieter überlassen bleiben - insbesondere im Hinblick auf kleine Anbieter, die nur wenig betroffen sind - solange die Auskunft in vertretbarer Zeit abgewickelt werden kann. Große Anbieter könnten durch eine (Teil-)Automatisierung in eigener Verantwortung die Auskünfte optimieren.

Zu § 22:

Welche Informationen der Anbieter bei der Abwicklung von behördlichen Auskunftsbegehren zu protokollieren hat, ist bereits detailliert in § 102c Abs. 2 TKG 2003 geregelt und wird im Sinne der Rechtsklarheit in § 7 Abs. 3 mit ergänzende Verweisen auf relevante Bestimmungen dieser Verordnung wiederholt. Diese Bestimmung zur Protokollierung bezieht sich indes auf jene Protokoll-Informationen, die der Anbieter gemäß § 102c Abs. 4 TKG 2003 an die dort genannten Stellen (Datenschutzkommission, Datenschutzrat, BMJ) zu übermitteln hat. Bei der Entwicklung des Konzepts der Durchlaufstelle wurde dabei bedacht, dass die zentrale Sammlung der für die Statistik notwendigen Protokollinformationen für diese Zwecke in der DLS eine enorme Verfahrens- und Verwaltungsvereinfachung darstellt. Dabei werden jene – nicht personenbezogenen – Informationen aus der Protokollierung beim Anbieter mit der (verschlüsselten) Auskunft unverschlüsselt mitgeliefert, sodass diese in der DLS für die Aufbereitung der Statistik gespeichert werden können. Diese Methode ist zugleich ein wertvoller Beitrag zur Datensicherheit, weil damit zugleich eine revisionssichere Protokollierung aller Auskunftsfälle in der DLS selbst erfolgt. Für den Fall, dass die Rechtsschutzbeauftragten, die Datenschutzkommission oder ein Gericht im Verfahren gemäß § 32 DSG 2000 für die Überprüfung der Rechtmäßigkeit eines bestimmten Falles der Datenübermittlung die exakten personenbezogenen Daten benötigt, die auf der Seite der Anbieter gemäß § 7 gespeichert werden und auch auf Seiten der Behörden nach den für diese einschlägigen (internen) Verfahrensvorschriften zu erfassen und aufzubewahren sind, kann die statistische Erfassung über die DLS äußerst hilfreich sein. Über die Unique-ID (§ 13) kann nämlich im Rechtsschutzfall der gesamte Ablauf vom Auskunftsbegehren bis zur Beantwortung lückenlos nachvollzogen werden und die richtigen Protokolldaten werden so auf der jeweils überprüften Seite (Anbieter oder Behörden) leichter auffindbar.

Deutlich vereinfacht wird dabei auch das Verfahren für die Aufbereitung der Statistik, die das BMJ jährlich an die EU-Kommission gemäß Art 10 der Richtlinie 2006/24/EG zu übermitteln hat. Über die DLS werden nach dieser Bestimmung alle Rohdaten automatisch gesammelt, die für die Statistik notwendig sind. Die automatische Aufbereitung der Statistik in der DLS richtet sich nach § 23. Hier ist darauf hinzuweisen, dass in der TKG Novelle zur Umsetzung der Vorratsdatenspeicherung ein Redaktionsversehen unterlaufen ist, das dazu führen würde, dass die notwendigen Rohdaten zur Erfüllung dieser gemeinschaftsrechtlichen Verpflichtung unmöglich machen würde. § 102c Abs. 4 Z 2 ordnet nämlich an, dass die Anbieter die Protokolldaten gemäß § 102c Abs. 2 Z 2 bis 4 an das BMJ zu übermitteln haben. Damit würden die Anbieter für die Statistik die Aktenzahlen zu den Auskunftsfällen nach SPG (Z 2 leg cit) übermitteln, nicht aber die Information zur Speicherdauer der übermittelten Daten

(Z 5 leg cit), die nach Art 10 Abs. 1 zweiter Spiegelstrich RL 2006/24/EG ausdrücklich gefordert sind. Dieses Versehen entstand dadurch, dass die Z 2 in § 102c Abs. 2 TKG 2003 im Zuge der Entstehung der Regierungsvorlage erst nachträglich eingefügt wurde, die entsprechende Anpassung im Absatz 4 aber unterblieb. In Absatz 2 dieser Bestimmung erfolgt daher durch den Verweis auf § 7 Abs. 3 Z 3 bis 5 die Korrektur dieses Redaktionsversehens. Um zu vermeiden, dass die Verordnung aus rein formalistischen Gründen wegen Gesetzwidrigkeit beim Verfassungsgerichtshof angefochten und möglicherweise in diesem Punkt für nichtig erklärt wird, sollte der Gesetzgeber daher schnellstmöglich die Richtigstellung im Gesetz selbst vornehmen, um zu vermeiden, dass die europarechtlichen Verpflichtung zur Übermittlung der Statistik aufgrund eines bloßen Versehens nicht erfüllt werden kann.

Zu § 23:

Einerseits müssen die sog. provider-internen Protokolldaten vorliegen (vgl. § 102c Abs 1 TKG 2003). Anbieter müssen intern revisionssicher protokollieren, dass Zugriffe auf Vorratsdaten unter Einhaltung des Vier-Augen-Prinzips nur durch speziell ermächtigte und bestimmte Personen und nur aufgrund einer entsprechenden behördlichen, staatsanwaltschaftlichen bzw. gerichtlichen Anfrage erfolgt sind. Diesen Zugriffen muss immer ein behördlicher, staatsanwaltschaftlicher bzw. gerichtlicher Auftrag zugrunde liegen, insofern besteht ein Zusammenhang zu den Protokoll-Daten über die Auskunftsfälle. Dem gegenüber stehen jene Protokoll bzw Statistik-Aufzeichnung über erfolgte Vorratsdaten-Abfragen (vgl. § 102c Abs 2 TKG 2003), die einmal jährlich an die Europäische Kommission zu übermitteln sind.

Diese beiden Protokollverpflichtungen überschneiden sich allerdings im Hinblick auf den Informationsgehalt. Die Protokollierung für die Statistik muss diese provider-internen Informationen (also welche Mitarbeiter wann zugegriffen haben) allerdings nicht enthalten."

Es besteht eine Verpflichtung zur jährlichen Berichterstattung gegenüber der Europäischen Kommission, die vom BMJ wahrzunehmen ist. Die Erfassung der Protokolldaten im Rahmen der Durchlaufstelle soll diese Erfassung der Protokolldaten für die Anbieter sowie das BMJ deutlich vereinfachen. Denn ansonsten müssen die Protokolldaten von allen Providern eingesammelt und in einheitlicher Struktur zusammengeführt werden. Die Harmonisierung der Protokoll-Struktur müsste also jedenfalls geregelt werden. Gemäß § 102c Abs. 4 Z 2 TKG 2003 obliegt es weiters auch dem BMJ, dem Nationalrat über die Statistik zu berichten.

Es macht jedenfalls Sinn, die Information zum Zeitpunkt der Zustellung der Anordnung in das Postfach des Anbieters gemäß § 7 Abs. 3 Z 3 schon bei der Anfrage zu protokollieren und damit den Protokoll-Datensatz zu einer Anfrage zu „eröffnen". Alle Anfragen über die DLS sind mit einer "Unique-ID" versehen. Die vom Anbieter übermittelte Antwort ist über dieselbe "Unique_ID" verknüpft und kann so den Datensatz zur Protokollierung mit den weiteren benötigten Informationen ergänzen. Gleichermaßen wird der Zeitpunkt der Zustellung der Antwort in das Postfach des Anbieters von der DLS selbständig protokolliert.

Zu § 24:

Diese Bestimmung dient der Klarstellung der Kostentragung der Investitionskosten für die Durchlaufstelle. Nähere Ausführungen über die finanziellen Auswirkungen sind im Vorblatt dargestellt.

Die Aufteilung der laufenden Kosten der DLS (Betriebskosten) bleibt einer interministeriellen Vereinbarung vorbehalten.

Zur Anlage (Schnittstellendefinition EP020):

Die Schnittstellendefinition erfolgt aus Gründen der besseren Darstellung in Form einer Anlage. In der Beilage zu den Erläuternden Bemerkungen werden für alle in der Anlage definierten Datenfelder Beispiele dargestellt. Die Aufzählung der Beispiele ist nicht abschließend und soll den Anbietern sowie den auskunftsberechtigten Behörden zur Hilfestellung bei der technischen Implementierung dienen. Entsprechend kommt dieser Beilage keine über die Anlage oder die sonstigen Bestimmungen dieser Verordnung hinausgehende Bedeutung zu.

Aus den EB zur RV (1074 der Beilagen XXIV. GP - Regierungsvorlage - Vorblatt und Erläuterungen): „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."

Die Technische Richtlinie in der Anlage basiert auf einer Empfehlung (EP020), die innerhalb der Telekom-Branche im Rahmen des Arbeitskreis-Telekommunikation (AK-TK) durch die Arbeitsgruppe „Schnittstellendefinition" bereits während der Entstehung der TKG-Novelle zur Umsetzung der Vorratsdatenspeicherung ausgearbeitet wurde. Die EP020 wurde im Rahmen der insgesamt 6 Round

Table Diskussionen des BIM im Zuge der Studie zur Datensicherheit (im Auftrag des BMVIT) mit allen Beteiligten (insbesondere BMI und Bundeskriminalamt) diskutiert und abgestimmt (siehe dazu ausführlich die EB zu § 1). Die Technische Richtlinie in der Anlage enthält all jene Teile der EP020, die sich unmittelbar auf die Definition der Syntax und Semantik der CSV Datei für die Übermittlung von Auskünften bezieht. Die EP020 als ganzes ist in der Datensicherheitsstudie abgebildet und in diesem Rahmen auch zur Veröffentlichung freigegeben.