Erläuterungen

Allgemeiner Teil

1. Hauptgesichtspunkte des Entwurfs:

Mit dieser Novelle sollen das Sicherheitspolizeigesetz (SPG), das Bundesstraßen-Mautgesetz 2002 (BStMG), die Straßenverkehrsordnung 1960 (StVO 1960) und das Telekommunikationsgesetz 2003 (TKG 2003) geändert werden.

Im Rahmen der Änderung des SPG sollen wesentliche Maßnahmen zur Stärkung der Sicherheit – sowohl in objektiver als auch in subjektiver Hinsicht – implementiert werden:

In erster Linie sollen mit den vorgeschlagenen Änderungen im SPG wesentliche Teile des Punktes 4.2 „Ausbau der technischen Ermittlungsmöglichkeiten“ des Arbeitsprogramms der Bundesregierung 2017/2018 „Für Österreich“ umgesetzt werden.

Außerdem hat der Bundesminister für Inneres mit der Initiative GEMEINSAM.SICHER in Österreich ein Projekt ins Leben gerufen, welches durch eine Intensivierung der Bürgerbeteiligung bei der Problem- und Lösungsfindung in sicherheitsrelevanten, regionalen Belangen zur Optimierung sowohl der objektiven als auch der subjektiven Sicherheit führen soll. Die ersten für notwendig erachteten Maßnahmen sollen nunmehr implementiert werden.

Schließlich soll die Regelung hinsichtlich der Kostenersatzpflicht bei sicherheitspolizeilichen Einsätzen adaptiert werden.

Die in den Artikeln 2 (BStMG) und 3 (StVO 1960) vorgesehenen Ergänzungen schaffen die notwendigen Voraussetzungen für die Umsetzung der Punkte „Videoüberwachung“ und „Kennzeichenerfassungsgeräte“ im Arbeitsprogramm der Bundesregierung 2017/2018 „Für Österreich“. Mit der Änderung in Artikel 4 (TKG 2003) werden der ebenfalls im Arbeitsprogramm der Bundesregierung 2017/2018 „Für Österreich“ unter dem Punkt 4.2. „Ausbau der technischen Ermittlungsmöglichkeiten“ vorgesehenen Maßnahmen „Registrierung von prepaid – Wertkarten“ und „Quick freeze – Anlassspeicherung von Telekommunikationsdaten“ entsprochen.

2. Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich auf Art. 10 Abs. 1 Z 7 („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“) und Z 9 („Angelegenheiten der wegen ihrer Bedeutung für den Durchzugsverkehr durch Bundesgesetz als Bundesstraßen erklärten Straßenzüge“ und „Post- und Fernmeldewesen“) des Bundes-Verfassungsgesetzes – B-VG, BGBl. Nr. 1/1930.

Besonderer Teil

Zu Artikel 1 (Änderung des Sicherheitspolizeigesetzes)

Zu Z 1 (Inhaltsverzeichnis):

Diese Bestimmung dient der Aktualisierung des Inhaltsverzeichnisses.

Zu Z 2 (§ 25):

Mit der Änderung des Abs. 1 soll ein wesentlicher Schritt in Richtung bürgernahe Polizeiarbeit unternommen werden, indem die Möglichkeit geschaffen wird, auf regionaler Ebene Plattformen zu bilden, in deren Rahmen (situationsbezogen) erforderliche Maßnahmen angeregt und koordiniert werden sollen. Zur Teilnahme an diesen Sicherheitsforen sind Menschen und Einrichtungen aufgefordert, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken, um gemeinsam mit der Sicherheitsbehörde Problemlösungen in Sicherheitsfragen zu erarbeiten (Sicherheitspartner). Darunter können je nach konkretem Anlassfall private Vereine, wie etwa Jugend- oder Elternvereine, NGOs, Wohnpartner oder auch Menschen, die im Rahmen von Community Policing Projekten freiwillig an der Präventionsarbeit teilnehmen, fallen. Die Einbeziehung von Sicherheitspartnern trägt dem Umstand Rechnung, dass Prävention auf sicherheitspolizeilichem Gebiet nicht eine ausschließliche Angelegenheit der Sicherheitsbehörde ist; vielmehr hat sich die gesamte Gesellschaft dieser Aufgabe anzunehmen. Es hat sich gezeigt, dass eine (ausschließlich) einseitige sicherheitspolizeiliche Beratung sowohl zur Förderung des Bewusstseins für Sicherheitsrisiken als auch der Bereitschaft, solchen Risiken entsprechend vorzubeugen, oftmals nicht hinreichend ist. Manche risikoerhöhenden Situationen bedürfen

zu ihrer zufriedenstellenden Auflösung eines gemeinsamen Vorgehens aller betroffenen Akteure. So können etwa mangelhaft beleuchtete Parkanlagen ein erhöhtes Sicherheitsrisiko darstellen, insbesondere wenn es in weiterer Folge in solchen Bereichen zu vermehrten gefährlichen Angriffen gegen Gesundheit oder Eigentum (z. B. Vandalismus) kommt. Zur raschen und umfassenden Beseitigung solcher Umstände durch entsprechende Maßnahmen bedarf es der gezielten Zusammenarbeit zwischen dem für Stadtgärten zuständigen Amt, der Abfallwirtschaft und Straßenreinigung sowie den Sicherheitsbehörden. Eine solche Form der gemeinschaftlichen Lösungsfindung soll durch die Möglichkeit zur Bildung von Sicherheitsforen institutionalisiert werden. Der Klarstellung, wie sich die Amtsverschwiegenheit zum Informationsaustausch im Sicherheitsforum verhält, dient der letzte Satz. Danach soll es zulässig sein, über Tatsachen, die zwar noch nicht allgemein, aber zumindest im Kreis der Teilnehmer eines Sicherheitsforums dem Grunde nach bekannt sind, zu sprechen. Genauso soll es möglich sein, falsche Tatsachen, deren Richtigstellung im Interesse des Betroffenen ist, auszuräumen. Die Zulässigkeit der Übermittlung personenbezogener Daten im Rahmen von Sicherheitsforen richtet sich nach § 56 Abs. 1 Z 9.

Zu Z 3, 11 und 12 (§ 53 Abs. 5, § 84 Abs. 1 Z 7und § 91c Abs. 3):

Mit der Änderung des § 53 Abs. 5 soll das Arbeitsprogramm der Bundesregierung 2017/2018 „Für Österreich“, das unter Punkt 4.2 „Ausbau der technischen Ermittlungsmöglichkeiten“ unter anderem zur Videoüberwachung eine Herausgabepflicht von Videomaterial sowie die Möglichkeit eines Echtzeitstreamings für bestimmte Rechtsträger vorsieht, umgesetzt werden.

Künftig soll es für sämtliche der in § 53 Abs. 1 genannten Zwecke zulässig sein, im Einzelfall freiwillig von privaten oder öffentlichen Rechtsträgern übergebene Bild- und Tondaten zur Aufgabenerfüllung zu verwenden. Da bei privat aufgezeichneten Aufnahmen, etwa Handyaufnahmen, nicht auszuschließen ist, dass diese auch Tonaufnahmen enthalten, soll durch die Änderung verhindert werden, dass die Sicherheitsbehörde die übergebenen Daten deshalb nicht nach Abs. 5 verwenden kann, weil auch Tondaten enthalten sind.

Für bestimmte Rechtsträger wird darüber hinausgehend – entsprechend den Vorgaben des Arbeitsprogramms – eine Verpflichtung geschaffen, unverzüglich Bilddaten auf Ersuchen der Sicherheitsbehörde zu übermitteln bzw. für den Fall der Notwendigkeit eines Echtzeitstreamings unverzüglich Zugang zu den gerade erst anfallenden Bilddaten zu gewähren; diese Verpflichtung beschränkt sich auf bestimmte, taxativ genannte sicherheitspolizeiliche Zwecke. Umfasst von der Verpflichtung sind Rechtsträger des öffentlichen oder privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsauftrag zukommt (etwa öffentliche Verkehrsbetriebe, Bahnhofs- oder Flughafenbetreiber oder auch die ASFINAG), die nach den Bestimmungen des DSG 2000 zulässigerweise den öffentlichen Raum überwachen. Entsprechend der Regelung bei Auskunftsverlangen nach dem DSG 2000 (§ 26 Abs. 7 DSG 2000) wird ein Löschungsverbot für diese Rechtsträger ab Kenntnisnahme von der Herausgabepflicht statuiert. Zur Durchsetzung der in § 53 Abs. 5 dritter Satz normierten Herausgabepflicht wird in § 84 Abs. 1 Z 7 eine Verwaltungsübertretung eingeführt für den Fall, dass der Zugang zu den verarbeiteten Bilddaten nicht unverzüglich, somit ohne unnötigen Aufschub, gewährt wird. Der Rechtsschutz für diese Maßnahme richtet sich nach § 91c Abs. 3. Demnach ist der Rechtsschutzbeauftragte unverzüglich von der Sicherheitsbehörde von der Inanspruchnahme dieser Verpflichtung zu verständigen. Dauert die Maßnahme länger als drei Tage an, ist überdies die Genehmigung des Rechtsschutzbeauftragten erforderlich.

Zu Z 4 (§ 53a Abs. 6):

In der jüngsten Vergangenheit hat sich gezeigt, dass die derzeit in § 53a Abs. 6 vorgesehene Speicherfrist für Daten von Verdächtigen für eine zielgerichtete und erfolgreiche Ermittlungstätigkeit, insbesondere bei Ermittlungen im Bereich der organisierten Kriminalität (etwa Schutzgelderpressung, Gewaltdelikte, Erpressung, Schlepperei, Suchtgifthandel), zu kurz greift. Mit ein Grund dafür liegt darin, dass sich Ermittlungen im Bereich der organisierten Kriminalität über Jahre erstrecken, insbesondere, wenn es sich um länderübergreifende Operationen handelt. Oftmals müssen Daten, die noch dringend benötigt würden, aufgrund Fristablaufs aus der Datenanwendung gelöscht werden, was zu Ermittlungsdefiziten führt.

Zu Z 5 (§ 54 Abs. 4b):

Die Erfahrungen seit der Einführung der Kennzeichenerkennungsgeräte im Jahr 2005, BGBl. I Nr. 151/2004, haben gezeigt, dass es für die Anhaltung der Fahrzeuge im Trefferfall unbedingt erforderlich ist, über das Kennzeichen hinausgehende Informationen zum Fahrzeug, insbesondere zur Fahrzeugmarke, Fahrzeugtype und Fahrzeugfarbe, zu erhalten. Zudem sind im Trefferfall auch Informationen zum Fahrzeuglenker zum Zweck der Gefahrenabwehr und der Strafverfolgung von wesentlicher Bedeutung (vgl. zur Notwendigkeit einer weitergehenden Erfassung von Daten auch § 19a BStMG idF BGBl. I Nr. 65/2017 bzw. § 50 Abs. 2 Eisenbahngesetz 1957). Abfragekriterium in der

Fahndungsevidenz bleibt weiterhin das Kennzeichen des Fahrzeugs. Darüber hinaus liegt eine Schwäche der derzeitigen Regelung darin, dass nur dann ein Treffer mit der Fahndungsevidenz angezeigt werden kann, wenn im Zeitpunkt der Erfassung des Kennzeichens das Fahrzeug bereits zur Fahndung ausgeschrieben wurde. Gerade bei Fahrzeugdiebstählen während der Abendstunden oder nachts erfolgt eine Anzeigeerstattung und damit einhergehend eine Ausschreibung des Fahrzeugs zur Fahndung zeitverzögert, sodass das Fahrzeug ohne Auslösung eines Treffers durch das Kennzeichenerfassungsgerät verbracht werden kann. Insbesondere aus Sicht der Strafverfolgung ist es daher erforderlich, die Daten für 48 Stunden zu speichern, um im Anlassfall (neue Fahndung) über einen Abgleich Hinweise über den Verbleib des Fahrzeuges zu generieren.

Zu Z 6 (§ 56 Abs. 1 Z 9 und 10):

Um eine rasche und effektive Koordinierung im Rahmen von Sicherheitsforen zu bewirken, bedarf es mitunter auch der Bekanntgabe personenbezogener Daten, die mit dem Grund der Einberufung eines Sicherheitsforums in Zusammenhang stehen, an die Teilnehmer dieser Plattform. Beschränkt auf den Informationsaustausch nach § 25 Abs. 1 letzter Satz soll es gemäß der neuen Z 9 im Einzelfall zur Vorbeugung gefährlicher Angriffe gegen Leben, Gesundheit und Vermögen von Menschen erlaubt sein, die zur Erfüllung des Zwecks jedenfalls erforderlichen personenbezogenen Daten an Teilnehmer eines Sicherheitsforums bekannt zu geben, wenn sich diese zur vertraulichen Behandlung dieser Daten verpflichtet haben.

Im Zuge des Hinwirkens der Sicherheitsbehörden auf die Beilegung von Streitigkeiten von Personen in deren engerem Umfeld soll es künftig gemäß Z 10 zulässig sein, personenbezogene Daten neben Behörden (§ 56 Abs. 1 Z 2) auch an andere Einrichtungen oder Menschen weiterzugeben, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken, wesentlich zur Gefahrenminderung beitragen können und sich zur vertraulichen Behandlung dieser Daten verpflichtet haben. Als typisches Beispiel für eine solche Vorgangsweise ist hier das Projekt „GEMEINSAM.SICHER – Sicherheit im Wohnumfeld“ zu nennen, im Rahmen dessen beabsichtigt ist, bei Nachbarschaftskonflikten jedenfalls erforderliche personenbezogene Daten von den Sicherheitsbehörden an die Wohnpartnern zu übermitteln, um präventiv schon im Vorfeld möglichen gerichtlich strafbaren Handlungen effektiv vorbeugen zu können. Durch die Informationsweitergabe wird die zuständige Einrichtung weder von den Sicherheitsbehörden mit der Erfüllung bestimmter Aufgaben beauftragt, noch besteht ein Rechtsanspruch auf Übermittlung von Informationen an bestimmte Einrichtungen.

Zu Z 7 bis 10 (§§ 57 bis 59):

Mit der Einfügung eines Abs. 2a in § 57 wird Punkt 4.2 des Arbeitsprogramms der Bundesregierung 2017/2018 „Für Österreich“ umgesetzt, indem die Rechtsgrundlage geschaffen wird, von der ASFINAG gemäß § 19a BStMG idF BGBl. I Nr. 65/2017 oder § 98a StVO 1960 ermittelte und an die Sicherheitsbehörde übermittelte Daten mit den Fahndungsevidenzen abzugleichen. Die Speicherdauer dieser Daten (§ 58 Abs. 3) sowie die Protokollierung im Trefferfall (§ 59 Abs. 2) werden wie beim Einsatz von polizeieigenen Kennzeichenerkennungssystemen gemäß § 54 Abs. 4b festgelegt.

Zu Z 11 (§ 84 Abs. 1):

Neben der bereits genannten Ergänzung um Z 7 soll § 84 Abs. 1 an § 84 Abs. 1a angepasst und eine Erhöhung der Strafdrohung im Wiederholungsfall vorgesehen werden. In Anlehnung an die strafrechtlichen Bestimmungen (§ 52 Abs. 1 StPO iVm § 301 Abs. 2 StGB) soll es durch die neue Z 8 mit Verwaltungsstrafe bedroht sein, wenn jemand der Verpflichtung zur vertraulichen Behandlung von personenbezogenen Daten gemäß § 56 Abs. 1 Z 9 und 10 zuwiderhandelt.

Zu Z 13 (§ 92a Abs. 1):

Mit der Änderung der Formulierung des Abs. 1 soll der Tatsache Rechnung getragen werden, dass technische Alarmeinrichtungen zwar oftmals primär zum Schutz von Eigentum und/oder Vermögen eingerichtet werden, damit zwangsläufig aber auch ein Schutz von anderen Rechtsgütern, etwa des Lebens oder der Gesundheit, angestrebt wird. Die bisherige Formulierung war hinsichtlich dieser „gemischten“ Verwendungen nicht ganz eindeutig. Mit der neuen Formulierung soll ausdrücklich klargestellt werden, dass auch Alarmeinrichtungen, die nicht nur dem Schutz von Eigentum und/oder Vermögen, sondern dem Schutz anderer Rechtsgüter – wie etwa Leben oder Gesundheit von Menschen – dienen, von der Regelung im Fall eines Fehlalarms umfasst sind.

Zu Z 14 (§ 92a Abs. 1a):

Angelehnt an Abs. 1 sollen durch die Einführung eines Abs. 1a Personen, die ein Einschreiten der Organe des öffentlichen Sicherheitsdienstes verursachen, in zwei abschließend genannten Fällen zum Ersatz der Kosten des Polizeieinsatzes verpflichtet werden können. Zum einen dann, wenn der Einsatz durch vorsätzlich falsche Notmeldung, etwa durch Notruf oder Notzeichen, ohne Vorliegen einer

Gefahrensituation ausgelöst wurde. Der zweite Fall erfasst jene Fälle, in denen sich der Betroffene grob fahrlässig einer Gefahr für Leben oder Gesundheit ausgesetzt hat und dadurch ein Einschreiten der Organe des öffentlichen Sicherheitsdienstes verursacht wird. Grob fahrlässig handelt derjenige, der sich ungewöhnlich und auffallend sorgfaltswidrig verhält, sodass eine Gefahr für Leben oder Gesundheit geradezu wahrscheinlich vorhersehbar war. Der Betroffene setzt somit ein Verhalten, das über das gewöhnliche Maß der Sorglosigkeit hinausgeht.

In diesen Fällen soll derjenige, der das Einschreiten durch eine falsche Notmeldung ausgelöst hat (Z 1), bzw. derjenige, der durch sein grob fahrlässiges Verhalten ein Einschreiten verursacht hat (Z 2), zum Ersatz der Kosten nach Maßgabe der konkret eingesetzten Mittel verpflichtet werden. Die Wahl des konkret herangezogenen Einsatzmittels richtet sich nach topographischen und sonstigen einsatzspezifischen Parametern.

Zu Z 15 (§ 93a):

Im Arbeitsprogramm der Bundesregierung 2017/2018 „Für Österreich“ ist unter dem Punkt „Videoüberwachung“ festgehalten, dass für öffentliche Betreiber eine Speicherverpflichtung sowie eine Mindestspeicherdauer normiert werden soll und dass für Kooperationen mit Unternehmen im Nahebereich der öffentlichen Hand (z.B. ÖBB, ASFINAG, regionale Verkehrsbetriebe) eine entsprechende Regelung gefunden werden soll. Um eine für den jeweiligen Einzelfall sachgerechte Lösung zu ermöglichen, wird folgende Regelung vorgeschlagen: Bereits nach derzeitiger Rechtslage hat die Datenschutzbehörde im Registrierungsverfahren bei entsprechendem Vorbringen zu prüfen, ob eine über die 72 Stunden hinausgehende Speicherdauer für öffentliche oder private Rechtsträger, die zulässigerweise den öffentlichen Raum überwachen, aus besonderen Gründen zur Zweckerreichung erforderlich ist. Für jene Videoüberwachungen, die in den Anwendungsbereich der vom Bundeskanzler erlassenen Standard- und Muster-Verordnung 2004, BGBl. II Nr. 312/2004, zur Videoüberwachung (Anlage 1 SA032) fallen und daher gemäß § 1 Abs. 1 StMV 2004 von einer Meldepflicht an die Datenschutzbehörde ausgenommen sind (Trafiken, Banken etc.), wurde in der diesbezüglichen Anlage festgelegt, dass auch die Strafverfolgung ein legitimer Zweck für eine längere Aufbewahrungsdauer ist. Nunmehr sollen die öffentlichen oder privaten Auftraggebern, soweit letzteren ein öffentlicher Versorgungsauftrag zukommt (etwa Verkehrsbetriebe oder Bahnhofs- oder Flughafenbetreiber), die zulässigerweise den öffentlichen Raum überwachen, verpflichtet werden, die örtlich zuständige Sicherheitsbehörde über ihre Verwendung von technischen Einrichtungen zur Bildverarbeitung zu informieren, um dieser die Gelegenheit zu geben, eine auf den jeweiligen Einzelfall abstellende Prüfung vorzunehmen. Dabei hat diese zu prüfen, ob es aus Sicht der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit oder der Strafverfolgung erforderlich ist, die Daten über einen längeren Zeitraum zu speichern. Bei Vorliegen entsprechender Gründe hat die Sicherheitsbehörde mit Bescheid eine zwei Wochen nicht überschreitende Aufbewahrungsverpflichtung festzulegen.

Die Notwendigkeit, auch bei Videoüberwachungen außerhalb der Vollziehung hoheitlicher Aufgaben sicherheits- und kriminalpolizeiliche Interessen stärker zu berücksichtigen, hat auch der deutsche Gesetzgeber erkannt, indem er in seinem Vorschlag eines „Videoüberwachungsverbesserungsgesetzes“ (vgl. Drucksache 18/10941, 18. Wahlperiode) vorsieht, bei geplanten Videoüberwachungen an bestimmten Orten (öffentlich zugängliche Anlagen mit großem Publikumsverkehr, wie etwa Einkaufszentren, öffentliche Verkehrsunternehmen) – demnach in einem zur geplanten österreichischen Regelung weiteren Anwendungsbereich – Sicherheitsbelange stärker zu berücksichtigen und bei der Abwägungsentscheidung mit größerem Gewicht einzubeziehen. In diesem Zusammenhang wird bei einer Verhältnismäßigkeitsprüfung auch zu berücksichtigen sein, dass der Zugriff im Einzelfall auf Aufnahmen des privaten Auftraggebers bei Vorliegen einer sicherheits- oder kriminalpolizeilichen Aufgabe der Vorzug vor einer großflächigeren polizeilichen Videoüberwachung zu geben ist.

Zu Z 16 (§ 94 Abs. 42):

Es handelt sich um die Inkrafttretensbestimmung.

Zu Z 17 (§ 96 Abs. 10):

Es handelt sich um die erforderliche Übergangsbestimmung, die bis zum Inkrafttreten des neuen Datenschutzrahmens mit 25. Mai 2018 erforderlich ist, um das Verhältnis zwischen Registrierungsverfahren bei der Datenschutzbehörde und der neuen Informationspflicht nach § 93a zu regeln.

Zu Artikel 2 (Änderung des Bundesstraßen-Mautgesetzes 2002)

Zu Z 1 und 2 (§ 19a):

Grundvoraussetzung für die Umsetzung des Punktes 4.2 des Arbeitsprogramms der Bundesregierung 2017/2018 „Für Österreich“ ist, dass die von der ASFINAG auf Grundlage des § 19a BStMG idF BGBl. I Nr. 65/2017 ermittelten Daten zulässigerweise an die Sicherheitsbehörde übermittelt werden dürfen. Die weitere Verwendung der Daten richtet sich nach dem SPG bzw. der StPO. Da gemäß § 19a Abs. 1 BStMG idF BGBl. I Nr. 65/2017 der Einsatz von bildgebenden technischen Einrichtungen zur Feststellung der ordnungsgemäßen Entrichtung der zeitabhängigen Maut an regelmäßig wechselnden Mautabschnitten zu erfolgen hat, ist der Sicherheitsbehörde der geplante Einsatz jeweils jedenfalls sieben Tage vor Beginn bekannt zu geben, damit diese die notwendigen Vorkehrungen für einen allenfalls beabsichtigten Fahndungsabgleich treffen kann.

Zu Z 3 (§ 33 Abs. 10):

Es handelt sich um die Inkrafttretensbestimmung.

Zu Artikel 3 (Änderung der Straßenverkehrsordnung 1960)

Zu Z 1 und 2 (§ 98a):

Grundvoraussetzung für die Umsetzung des Punktes 4.2 des Arbeitsprogramms der Bundesregierung 2017/2018 „Für Österreich“ ist, dass die von der ASFINAG auf Grundlage des § 98a StVO ermittelten Daten zulässigerweise an die Sicherheitsbehörde übermittelt werden dürfen. Die weitere Verwendung der Daten richtet sich nach dem SPG bzw. der StPO.

Zu Z 3 (§ 103 Abs. 18):

Es handelt sich um die Inkrafttretensbestimmung.

Zu Artikel 4 (Änderung des Telekommunikationsgesetzes 2003)

Zu Z 1 (§ 17 Abs. 1a):

Um eine nicht zu rechtfertigende Benachteiligung österreichischer Accessprovider zu verhindern und um die Kompetenzen österreichischer Provider u.a. in den Bereich Jugendschutz und Datensicherheit zu stärken, sollen diese ohne Verstoß gegen die Netzneutralität die gleichen Services anbieten können, die sonst nur reine Serviceprovider anbieten können.

Zu Z 2 (§ 92 Abs. 3 Z 3 lit. g):

Um eine eindeutige Identifizierung einer Person zu ermöglichen, kommt dem Geburtsdatum wesentliche Bedeutung zu. Daher sind die Stammdaten um dieses Datum zu ergänzen.

Zu Z 3 (§ 97 Abs. 1a):

Sicherheits- und kriminalpolizeiliche Zwecke erfordern es, dass Personen, die mit einem Anbieter einen Vertrag über die Bereitstellung eines Kommunikationsdienstes geschlossen haben, wovon auch der Erwerb von Prepaid-Karten bzw. entsprechendem Guthaben umfasst ist, im Anlassfall identifizierbar sind. Zur Erhebung der Identität dieser Vertragspartner (Teilnehmer) ist die Registrierung seiner Stammdaten (§ 92 Abs. 3 Z 3) erforderlich. Die Speicherung der nach Abs. 1a ermittelten Daten richtet sich nach den in § 97 Abs. 2 genannten Fristen.

Zu Z 4 (§ 99 Abs. 1a bis 1f):

Nach der derzeitigen Rechtslage sind die Telekommunikationsanbieter verpflichtet, Verkehrsdaten unverzüglich nach Beendigung der Verbindung bzw. sobald der Bezahlvorgang durchgeführt wurde und innerhalb einer Frist von drei Monaten die Entgelte nicht schriftlich beeinsprucht wurden zu löschen. Durch die vorgeschlagene Änderung soll diese generelle Löschungsverpflichtung insofern punktuell unterbrochen werden, als bei Vorliegen eines Anfangsverdachts bestimmter gerichtlich strafbarer Handlungen Telekommunikationsanbieter aufgrund staatsanwaltschaftlicher Anordnung verpflichtet werden können, Telekommunikationsdaten (Verkehrsdaten, Zugangsdaten und Standortdaten) bis zu 12 Monate zu speichern. Im Falle, dass sich der Anfangsverdacht verdichtet, kann die Staatsanwaltschaft mit gerichtlicher Bewilligung auf diese gespeicherten Daten zugreifen, ansonsten sind die Daten nach Ablauf der in der staatsanwaltschaftlichen Anordnung festgesetzten Frist zu löschen. Damit sind die Grundrechtserfordernisse im Lichte der jüngsten EuGH-Judikatur erfüllt.

Zu Z 5 (§ 109 Abs. 4 Z 9 bis 13):

An dieser Stelle werden die durch die Einführung von Quick freeze in § 99 Abs. 1a bis 1f erforderlichen Strafbestimmungen normiert.

Zu Z 6 (§ 137 Abs. 9):

Es handelt sich um die Inkrafttretensbestimmung. Die Verpflichtung zur Erhebung der Identität der Teilnehmer erfordert organisatorische Vorkehrungen durch die Anbieter. Die vorgeschlagene Legisvakanz bis zum 1. Jänner 2018 soll den Anbietern ermöglichen, diese Vorbereitungen zu treffen.