

# Gemäß § 53 Abs. 4 GOG an die Abgeordneten verteilt

## Gesamtändernder Abänderungsantrag

der Abgeordneten Herbert, Amon, MBA  
Kolleginnen und Kollegen

betreffend ein Bundesgesetz, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden

Der Nationalrat wolle in zweiter Lesung beschließen:

Bundesgesetz, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden

Der Nationalrat hat beschlossen:

### Inhaltsverzeichnis

Art.	Gegenstand / Bezeichnung
1	Änderung des Sicherheitspolizeigesetzes
2	Änderung der Straßenverkehrsordnung 1960
3	Änderung des Telekommunikationsgesetzes 2003

### Artikel 1

#### Änderung des Sicherheitspolizeigesetzes

Das Sicherheitspolizeigesetz – SPG, BGBl. Nr. 566/1991, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 130/2017, wird wie folgt geändert:

1. Im Inhaltsverzeichnis wird im Eintrag zur Überschrift des 4. Teils das Wort „Verwenden“ durch das Wort „Verarbeiten“ ersetzt.
2. Im Inhaltsverzeichnis lautet der Eintrag zu § 53a:  
„§ 53a. Datenverarbeitungen der Sicherheitsbehörden“
3. Im Inhaltsverzeichnis lautet der Eintrag zu § 58e:  
„§ 58e. Zentrale Datenverarbeitung zur Einsatzunterstützung“
4. Im Inhaltsverzeichnis lautet der Eintrag zu § 59:  
„§ 59. Richtigstellung, Aktualisierung und Protokollierung bei Datenverarbeitungen gemeinsam Verantwortlicher“
5. Im Inhaltsverzeichnis lautet der Eintrag zu § 63:  
„§ 63. Pflicht zur Richtigstellung, Löschung und Protokollierung“
6. Im Inhaltsverzeichnis lautet der Eintrag zu § 68:  
„§ 68. Erkennungsdienstliche Maßnahmen auf Antrag oder mit Einwilligung des Betroffenen“
7. Im Inhaltsverzeichnis lautet der Eintrag zu § 70:  
„§ 70. Spurenausscheidungsevidenz“
8. Im Inhaltsverzeichnis wird nach dem Eintrag zu § 93 folgender Eintrag eingefügt:  
„§ 93a. Informationspflicht bei Bildaufnahmen an öffentlichen Orten“
9. § 7 Abs. 4 lautet:

„(4) Soweit ein ärztlicher Dienst eingerichtet ist, hat dieser an der Feststellung der geistigen und körperlichen Eignung von Aufnahmewerbern in den Exekutivdienst und von Bewerbern für bestimmte

Verwendungen, unbeschadet der Mitwirkungsbefugnisse des Bundeskanzleramtes nach dem Ausschreibungsgesetz 1989 (AusG), BGBl. Nr. 85/1989, mitzuwirken. Zu diesem Zweck dürfen unter Einbindung von Polizeiarzten als medizinische Sachverständige zur Feststellung der geistigen und körperlichen Eignung auch Gesundheitsdaten im Sinne des Art. 4 Z 15 der Verordnung (EU) Nr. 679/2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 04.05.2016 S. 1, (im Folgenden: DSGVO) nach Maßgabe des Art. 9 Abs. 2 lit. h in Verbindung mit Abs. 3 DSGVO verarbeitet werden, soweit diese zur Beurteilung der Eignung für den Exekutivdienst erforderlich sind. Die näheren Bestimmungen über die Durchführung der Eignungsprüfung und die Erstellung und Auswertung der Tests sind durch Verordnung des Bundesministers für Inneres festzusetzen.“

10. In § 13a wird in Abs. 2 und 3 jeweils das Wort „Verwendung“ durch das Wort „Verarbeitung“ ersetzt; in Abs. 3 wird das Zitat „§ 14 DSG 2000“ durch das Zitat „§ 54 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999,“ ersetzt und nach der Wortfolge „Daten, zu sichern“ ein Beistrich und die Wortfolge „sofern nicht Art. 32 DSGVO unmittelbar zur Anwendung kommt“ eingefügt.

11. Dem § 13a wird folgender Abs. 4 angefügt:

„(4) Die Protokollaufzeichnungen gemäß § 50 DSG für Datenverarbeitungen nach Abs. 1 und 2 sind drei Jahre aufzubewahren und danach zu löschen.“

12. Dem § 25 Abs. 1 wird folgender Satz angefügt:

„Zu diesem Zweck können die Sicherheitsbehörden Plattformen auf regionaler Ebene unter Beiziehung von Menschen, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken, einrichten, in deren Rahmen erforderliche Maßnahmen erarbeitet und koordiniert werden (Sicherheitsforen).“

13. In § 35a Abs. 5 wird das Wort „Dienstleister“ durch das Wort „Auftragsverarbeiter“ ersetzt.

14. In der Überschrift des 4. Teils wird das Wort „Verwenden“ durch das Wort „Verarbeiten“ ersetzt.

15. § 51 lautet:

„§ 51. (1) Die Sicherheitsbehörden haben beim Verarbeiten (§ 36 Abs. 2 Z 2 DSG) personenbezogener Daten die Verhältnismäßigkeit (§ 29) zu beachten. Die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 39 DSG ist zulässig, soweit dies zur Erfüllung der Aufgaben im Rahmen der Sicherheitspolizei unbedingt erforderlich ist; dabei sind angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen.

(2) Sofern nicht ausdrücklich anderes angeordnet wird, finden auf das Verarbeiten personenbezogener Daten die Bestimmungen des DSG Anwendung.

(3) Sofern nicht ausdrücklich anderes angeordnet wird, übt der Bundesminister für Inneres die Funktion des Auftragsverarbeiters gemäß § 36 Abs. 2 Z 9 in Verbindung mit § 48 DSG aus. Abweichend von § 48 Abs. 2 DSG kann der Auftragsverarbeiter nach Erteilung einer allgemeinen schriftlichen Genehmigung des Verantwortlichen weitere Auftragsverarbeiter hinzuziehen. In diesem Fall obliegt es dem Auftragsverarbeiter, den Verantwortlichen über jede beabsichtigte wesentliche Änderung zu unterrichten.

(4) Bei Datenverarbeitungen von gemeinsam Verantwortlichen (§ 47 DSG) obliegt jedem Verantwortlichen die Erfüllung von Pflichten nach den §§ 42 bis 45 DSG nur hinsichtlich der von ihm ursprünglich verarbeiteten Daten. Nimmt ein Betroffener unter Nachweis seiner Identität ein Recht nach den §§ 43 bis 45 DSG gegenüber einem unzuständigen gemeinsam Verantwortlichen wahr, ist er an den zuständigen gemeinsam Verantwortlichen zu verweisen, sofern nicht ein Fall des § 43 Abs. 4 DSG vorliegt.“

16. In § 52 wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.

17. In § 53 wird in Abs. 1 und 2 jeweils die Wortfolge „ermitteln und weiterverarbeiten“ durch das Wort „verarbeiten“ ersetzt; in Abs. 3a wird das Zitat „BGBl. I Nr. 70“ durch das Zitat „BGBl. I Nr. 70/2003“ ersetzt; in Abs. 4 wird die Wortfolge „ermitteln und weiterzuverarbeiten“ durch das Wort „verarbeiten“ ersetzt.

18. § 53 Abs. 5 lautet:

„(5) Die Sicherheitsbehörden sind im Einzelfall berechtigt, für die Zwecke des Abs. 1 personenbezogene Bild- und Tondaten zu verarbeiten, die Rechtsträger des öffentlichen oder privaten Bereichs mittels Einsatz von Bildaufnahmegeräten rechtmäßig verarbeitet und der Sicherheitsbehörde

freiwillig übermittelt haben. Nicht zulässig ist die Verarbeitung von personenbezogenen Bilddaten über nichtöffentliches Verhalten. Die Rechtsträger des öffentlichen oder privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsauftrag zukommt, die zulässigerweise einen öffentlichen Ort mit Bildaufnahmegegeräten überwachen, sind im Einzelfall für die Zwecke der Vorbeugung wahrscheinlicher oder Abwehr gefährlicher Angriffe, der Abwehr krimineller Verbindungen sowie der Fahndung verpflichtet, die auf diese Weise erlangten Bild- und Tondaten auf Verlangen unverzüglich der Sicherheitsbehörde in einem üblichen technischen Format weiterzugeben oder Zugang zur Bildaufnahme zu gewähren, um sie für die genannten Zwecke zu verarbeiten. Ab dem Zeitpunkt der Kenntnis von einem solchen Verlangen darf der verpflichtete Rechtsträger die verlangten Bild- und Tondaten nicht löschen. Bei jeder Verarbeitung von Bild- und Tondaten ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren.“

19. In der Überschrift des § 53a wird das Wort „Datenanwendungen“ durch das Wort „Datenverarbeitungen“ ersetzt.

20. Im Schlussteil des § 53a Abs. 2 entfällt der Beistrich und die Wortfolge „auch wenn es sich um besonders schutzwürdige Daten im Sinne des § 4 Z 2 DSG 2000 handelt“.

21. § 53a Abs. 5 erster Satz lautet:

„Datenverarbeitungen gemäß Abs. 1 dürfen durch mehrere Sicherheitsbehörden als gemeinsam Verantwortliche geführt werden, soweit dies wegen eines sprengelübergreifenden Einsatzes erforderlich ist.“

22. § 53a Abs. 5a erster Satz lautet:

„Datenverarbeitungen gemäß Abs. 1a zum Schutz von verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (§ 22 Abs. 1 Z 2), der Vertreter ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte (§ 22 Abs. 1 Z 3) sowie von kritischen Infrastrukturen (§ 22 Abs. 1 Z 6) dürfen durch den Bundesminister für Inneres und die Landespolizeidirektionen als gemeinsam Verantwortliche geführt werden.“

23. § 53a Abs. 6 erster Satz lautet:

„Datenverarbeitungen gemäß Abs. 2 dürfen durch mehrere Sicherheitsbehörden als gemeinsam Verantwortliche geführt werden, soweit eine solche gemeinsame Verarbeitung für den Zweck des Abs. 2 erforderlich ist.“

24. In § 53a Abs. 6 zweiter Satz wird die Wortfolge „Abs. 2 Z 1 sind längstens nach drei Jahren,“ durch die Wortfolge „Abs. 2 Z 1 sind längstens nach fünf Jahren,“ ersetzt.

25. In § 53b wird die Wortfolge „ermitteln und weiterzuverarbeiten“ durch das Wort „verarbeiten“ ersetzt.

26. § 54 Abs. 4b lautet:

„(4b) Die Sicherheitsbehörden sind ermächtigt, verdeckt mittels Einsatz von bildverarbeitenden technischen Einrichtungen Daten zur Identifizierung von Fahrzeugen, insbesondere das Kennzeichen, die Type, Marke sowie Farbe des Fahrzeuges, und Fahrzeuglenker für Zwecke der Fahndung zu verarbeiten. Ein Abgleich mit Fahndungsevidenzen ist nur anhand des Kennzeichens zulässig. Die verarbeiteten Daten dürfen auch zur Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen verarbeitet werden. Soweit sie nicht zur weiteren Verfolgung aufgrund eines Verdachts gerichtlich strafbarer Handlungen erforderlich sind, sind sie nach längstens zwei Wochen zu löschen.“

27. In § 54 wird in den Abs. 5, 6 und 7 jeweils das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.

28. In § 54b wird in Abs. 1 die Wortfolge „sensible und strafrechtsbezogene Daten“ durch die Wortfolge „besondere Kategorien personenbezogener Daten (§ 39 DSG)“ ersetzt und entfällt in Abs. 3 der erste Satz.

29. In § 55 Abs. 4 wird jeweils das Wort „ermittelt“ durch das Wort „verarbeitet“ ersetzt.

30. In § 55a Abs. 4 wird das Wort „Zustimmung“ durch das Wort „Einwilligung“ ersetzt.

31. In § 55b Abs. 1 wird jeweils das Wort „Zustimmung“ durch das Wort „Einwilligung“ sowie das Wort „Zustimmungserklärung“ durch das Wort „Einwilligungserklärung“ ersetzt.

32. § 56 Abs. 1 Z 1 lautet:

„1. wenn der Betroffene in die Übermittlung - bei besonderen Kategorien personenbezogener Daten (§ 39 DSGVO) ausdrücklich - eingewilligt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verarbeitung der Daten bewirkt;“

33. § 56 Abs. 1 Z 5 lautet:

„5. wenn lebenswichtige Interessen eines Menschen die Übermittlung erfordern;“

34. § 56 Abs. 1 Z 7 lautet:

„7. für Zwecke wissenschaftlicher Forschung und Statistik;“

35. In § 56 Abs. 1 lautet der Schlussteil:

„Für die Übermittlung personenbezogener Daten für Zwecke der internationalen polizeilichen Amtshilfe sind die Bestimmungen des Polizeikooperationsgesetzes – PolKG, BGBl. I Nr. 104/1997, anzuwenden.“

36. § 56 Abs. 2 entfällt.

37. § 56 Abs. 3 lautet:

„(3) Erweisen sich übermittelte personenbezogene Daten im Nachhinein als unvollständig oder unrichtig, so ist unverzüglich gemäß § 37 Abs. 8 und 9 DSGVO vorzugehen.“

38. § 56 Abs. 5 erster Satz lautet:

„Die Übermittlung personenbezogener Daten nach Abs. 1 Z 3a ist erst zulässig, wenn sich der Österreichische Fußballbund und die Österreichische Fußball-Bundesliga vertraglich gegenüber dem Bundesminister für Inneres verpflichtet haben,

1. die Daten nur zum festgelegten Zweck, in ihrem Wirkungsbereich und im Einklang mit den Bestimmungen der DSGVO zu verarbeiten,
2. die Daten vor unberechtigter Verarbeitung zu sichern, insbesondere durch organisatorische und technische Vorkehrungen sicherzustellen, dass der Zutritt zu Räumen, in denen sich eine Zugriffsmöglichkeit auf die übermittelten Daten befindet, nur von in ihrem Auftrag Tätigen möglich ist,
3. ihren Löschungsverpflichtungen nachzukommen,
4. jede Verarbeitung der Daten in ihrem Wirkungsbereich zu protokollieren und
5. den Sicherheitsbehörden Zutritt zu Räumen und Zugriff auf Datenverarbeitungsgeräte zu gewähren und ihnen auf Verlangen die notwendigen Auskünfte zu erteilen, soweit dies zur Überprüfung der Einhaltung der in Z 1 bis 4 normierten Pflichten erforderlich ist.“

39. In § 57 Abs. 1 wird im Einleitungssatz das Wort „Datenanwendung“ durch das Wort „Datenverarbeitung“ ersetzt sowie nach der Wortfolge „dürfen die Sicherheitsbehörden“ die Wortfolge „als gemeinsam Verantwortliche“ und nach der Wortfolge „Auskünfte auch an andere Behörden“ das Wort „gemeinsam“ eingefügt; in Z 10a wird das Wort „zugestimmt“ durch das Wort „eingewilligt“ ersetzt.

40. In § 57 Abs. 2 wird nach der Wortfolge „dürfen die Sicherheitsbehörden“ die Wortfolge „als gemeinsam Verantwortliche“ eingefügt sowie das Wort „speichern“ durch die Wortfolge „gemeinsam verarbeiten“ und die Wortfolge „zu vergleichen“ durch das Wort „abzugleichen“ ersetzt.

41. In § 57 wird nach Abs. 2 folgender Abs. 2a eingefügt:

„(2a) Der Bundesminister für Inneres ist ermächtigt, nach Abs. 1 und Abs. 2 verarbeitete Daten mit den gemäß § 98a Straßenverkehrsordnung 1960 – StVO 1960, BGBl. Nr. 159/1960, übermittelten Daten für Zwecke des § 54 Abs. 4b zu vergleichen.“

42. In § 57 Abs. 3 wird im ersten Satz die Wortfolge „zu benützen und zu vergleichen“ durch die Wortfolge „zu verarbeiten“ sowie im zweiten Satz das Zitat „Abs. 1 und Abs. 2“ durch das Zitat „Abs. 1, Abs. 2 und Abs. 2a“ ersetzt.

43. In § 58 Abs. 1 wird im Einleitungsteil die Wortfolge „evident gehalten“ durch das Wort „verarbeitet“ und das Wort „Auftraggeber“ durch das Wort „Verantwortliche“ ersetzt.

44. In § 58 Abs. 2 entfällt im ersten Satz die Wortfolge „als Auftraggeber“ und wird im letzten Satz das Wort „Auftraggeber“ durch das Wort „Verantwortliche“ ersetzt.

45. Dem § 58 wird folgender Abs. 3 angefügt:

„(3) Personenbezogene Daten, die gemäß § 57 Abs. 2a übermittelt wurden, sind spätestens zwei Wochen nach der Übermittlung zu löschen.“

46. § 58a lautet:

„§ 58a. Die Sicherheitsbehörden sind als gemeinsam Verantwortliche ermächtigt, für die Organisation des Streifen- und Überwachungsdienstes (§ 5 Abs. 3), für Zwecke der Gefahrenabwehr (§ 21 Abs. 1 und 2) und der Vorbeugung vor gefährlichen Angriffen (§ 22 Abs. 2 und 3) auch mittels Kriminalitätsanalyse hinsichtlich sämtlicher angezeigter, von Amts wegen zu verfolgender und vorsätzlich begangener gerichtlich strafbarer Handlungen folgende Informationen gemeinsam zu verarbeiten: strafbare Handlung samt näherer Umstände und Sachverhaltsbeschreibung, Tatort und Zeit, betroffenes Gut (Markenname) oder Firmenbezeichnung und hinsichtlich allfälliger Verdächtiger Anzahl, Nationalität, Geschlecht und Alter sowie Geschäftszahl, Dienststelle und Sachbearbeiter. Die Abfrageberechtigungen im Zusammenhang mit Sexualstraftaten nach dem 10. Abschnitt des Strafgesetzbuches sind auf jenen Personenkreis einzuschränken, der mit der Bearbeitung dieser strafbaren Handlungen befasst ist. Die Daten sind nach 18 Monaten zu löschen.“

47. § 58b Abs. 1 lautet:

„(1) Die Sicherheitsbehörden sind als gemeinsam Verantwortliche ermächtigt, für die Administration des Vollzugs und die Evidenthaltung der in Hafträumen der Landespolizeidirektionen oder Bezirksverwaltungsbehörden angehaltenen Menschen eine Datenverarbeitung gemeinsam zu führen. Zu diesen Zwecken dürfen sie personenbezogene Daten über angehaltene Menschen einschließlich eines anlässlich der Aufnahme anzufertigenden Lichtbildes verarbeiten, soweit sie sich auf strafbare Handlungen oder auch für den Vollzug relevante Lebensumstände einschließlich ihres Gesundheitszustandes und ihrer ethnischen oder religiösen Zugehörigkeit beziehen.“

48. § 58c lautet:

„§ 58c. (1) Die Sicherheitsbehörden sind als gemeinsam Verantwortliche ermächtigt, für den Vollzug von § 38a hinsichtlich Personen, gegen die sich eine Maßnahme nach § 38a richtet, Identifikationsdaten einschließlich der Erreichbarkeitsdaten und Vormerkungen wegen Gewaltdelikten, Angaben zu Grund und Umfang (räumlich und zeitlich) der verhängten Maßnahme einschließlich früherer Maßnahmen gemäß § 38a und Verfahrensdaten, sowie hinsichtlich zu schützender Menschen ausschließlich Alter, Geschlecht, Staatsangehörigkeit sowie Angehörigkeitsverhältnis zum Gefährder gemeinsam zu verarbeiten.

(2) Übermittlungen von Daten gemäß Abs. 1 sind an Sicherheitsbehörden für Zwecke des Vollzugs der §§ 8 und 12 Waffengesetz 1996, BGBl. I Nr. 12/1997, sowie an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege zulässig. Sofern besondere gesetzliche Regelungen dies vorsehen, ist darüber hinaus eine Übermittlung dieser Daten auch an Kinder- und Jugendhilfeträger in Angelegenheiten der Kinder- und Jugendhilfe zulässig.

(3) Die Daten sind zu löschen, wenn ein Betretungsverbot gemäß § 38a Abs. 6 aufgehoben wurde. Sonst sind die Daten von Personen, gegen die sich eine Maßnahme nach § 38a richtet, und der jeweils Gefährdeten ein Jahr nach Aufnahme in die zentrale Gewaltschutzdatei zu löschen, im Falle mehrerer Speicherungen ein Jahr nach der letzten.“

49. In § 58d Abs. 1 lautet der Einleitungsteil:

„Die Sicherheitsbehörden sind als gemeinsam Verantwortliche ermächtigt, zur Vorbeugung und Verhinderung von mit Strafe bedrohten Handlungen gegen Leib und Leben sowie gegen die sexuelle Integrität und Selbstbestimmung unter Androhung oder Anwendung von Gewalt sowie zur frühzeitigen Erkennung von diesbezüglichen Serienzusammenhängen mittels Analyse personenbezogener Daten gemeinsam zu verarbeiten. Es dürfen Informationen zu Tötungsdelikten, Sexualstraftaten unter Anwendung von Gewalt, Vermisstenfällen, wenn die Gesamtumstände auf ein Verbrechen hindeuten, und zu verdächtigem Ansprechen von Personen, wenn konkrete Anhaltspunkte für eine mit sexuellem Motiv geplante mit Strafe bedrohte Handlung vorliegen, verarbeitet werden. Nachstehende Datenarten dürfen zu den ausgewiesenen Betroffenenkreisen verarbeitet werden:“

50. § 58e samt Überschrift lautet:

#### **„Zentrale Datenverarbeitung zur Einsatzunterstützung**

§ 58e. (1) Der Bundesminister für Inneres und die Landespolizeidirektionen sind als gemeinsam Verantwortliche ermächtigt, für die Administration von Notrufen (§§ 5 Abs. 7, 92a) sowie für die Unterstützung bei der Koordination von Einsätzen Daten über Personen sowie Sachen und Gebäude

gemeinsam zu verarbeiten. Es dürfen zu Personen, die von einem Notruf oder Einsatz betroffen sind, die erforderlichen Identifikations- und Erreichbarkeitsdaten einschließlich Daten gemäß § 98 TKG 2003 und soweit erforderlich besondere Kategorien personenbezogener Daten (§ 39 DSGVO) verarbeitet werden. Darüber hinaus dürfen die erforderlichen Sachdaten einschließlich KFZ-Kennzeichen, der Mindestdatensatz eines eCalls, Daten zu Zeit, Ort, Grund und Art des Einsatzes, Erreichbarkeitsdaten von sonstigen zu verständigenden Stellen (Abs. 3) sowie Verwaltungsdaten verarbeitet werden.

(2) Die gemäß § 93 Abs. 3 TKG 2003 im Rahmen der Entgegennahme von Notrufen aufgezeichneten Gespräche sind nach drei Monaten, die übrigen Daten nach Beendigung und Evaluierung des Einsatzes, längstens jedoch nach 18 Monaten zu löschen.

(3) Übermittlungen der gemäß Abs. 1 und 2 verarbeiteten Daten sind an Sicherheitsbehörden für Zwecke der Sicherheitsverwaltung und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege, an sonstige Notrufdienste sowie an sonstige Stellen zulässig, soweit dies zur Abwehr einer Gefahr, zur Hilfeleistung oder für die Verrechnung erforderlich ist.“

51. Die Überschrift zu § 59 lautet:

**„Richtigstellung, Aktualisierung und Protokollierung bei Datenverarbeitungen gemeinsam Verantwortlicher“**

52. § 59 Abs. 1 lautet:

„(1) Die Sicherheitsbehörden haben als gemeinsam Verantwortliche die von ihnen in Datenverarbeitungen gemeinsam verarbeiteten Daten unter den Voraussetzungen der §§ 61 und 63 Abs. 1 und 3 zu aktualisieren oder richtig zu stellen und zu protokollieren. Eine Aktualisierung oder Richtigstellung von Namen, Geschlecht, früheren Namen, Staatsangehörigkeit, Geburtsdatum, Geburtsort und Wohnanschrift, Namen der Eltern und Aliasdaten darf auch jede andere Sicherheitsbehörde vornehmen. Hievon ist jene Sicherheitsbehörde, die die Daten ursprünglich verarbeitet hat, zu informieren. Bei Einstellung von Ermittlungen oder Beendigung eines Verfahrens einer Staatsanwaltschaft oder eines Strafgerichtes hat die Sicherheitsbehörde die Daten, die sie verarbeitet hat, durch Anmerkung der Einstellung oder Verfahrensbeendigung und des bekannt gewordenen Grundes zu aktualisieren.“

53. In § 59 entfällt Abs. 2; Abs. 3 lautet:

„(3) Erweisen sich aus Datenverarbeitungen gemäß Abs. 1 übermittelte personenbezogene Daten im Nachhinein als unvollständig oder unrichtig, so ist die Richtigstellung oder Aktualisierung in allen Auskünften, die nach der Richtigstellung oder Aktualisierung erfolgen, zu kennzeichnen.“

54. In § 60 Abs. 2 wird das Wort „ermitteln“ durch das Wort „verarbeiten“ und das Wort „Verarbeitung“ durch das Wort „Datenverarbeitung“ ersetzt.

55. In § 61 wird das Wort „verwendeten“ durch das Wort „verarbeiteten“ ersetzt.

56. § 63 samt Überschrift lautet:

**„Pflicht zur Richtigstellung, Löschung und Protokollierung“**

§ 63. (1) Wird festgestellt, dass unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete personenbezogene Daten verarbeitet werden, so ist unverzüglich eine Richtigstellung oder Löschung vorzunehmen. Desgleichen sind personenbezogene Daten zu löschen, sobald sie für die Erfüllung der Aufgabe, für die sie verwendet worden sind, nicht mehr benötigt werden, es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden.

(2) Die Sicherheitsbehörden haben automationsunterstützt verarbeitete personenbezogene Daten, die sechs Jahre unverändert geblieben sind, daraufhin zu überprüfen, ob diese nicht gemäß Abs. 1 richtig zu stellen oder zu löschen sind. Für Daten, die in der Zentralen Informationssammlung verarbeitet werden, gelten die §§ 58 und 59.

(3) § 50 DSGVO gilt mit der Maßgabe, dass die Zuordnung zu einem bestimmten Organwalter bei ausschließlich programmgesteuerten Abfragen nicht erforderlich ist. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen. Von der Protokollierung ausgenommen sind ausschließlich programmgesteuerte Abfragen gemäß § 54 Abs. 4b und § 57 Abs. 2a, es sei denn, es handelt sich um einen Trefferfall.“

57. § 64 Abs. 2 lautet:

„(2) Erkennungsdienstliche Maßnahmen sind technische Verfahren zur Feststellung von biometrischen oder genetischen Daten (§ 36 Abs. 2 Z 12 und 13 DSGVO), wie insbesondere die Abnahme von

Papillarlinienabdrücken, die Vornahme von Mundhöhlenabstrichen, die Herstellung von Abbildungen, die Vornahme von Messungen oder die Erhebung von Stimmproben, sowie die Feststellung äußerlicher körperlicher Merkmale und die Erhebung von Schriftproben eines Menschen zum Zweck der Wiedererkennung.“

58. In § 65 wird in Abs. 2 die Wortfolge „eines bestimmten gefährlichen Angriffes“ durch die Wortfolge „einer mit gerichtlicher Strafe bedrohten vorsätzlichen Handlung“ und die Wortfolge „den gefährlichen Angriff“ durch die Wortfolge „diese Handlung“ ersetzt; in Abs. 6 wird die Wortfolge „sensibler Daten, soweit deren Verwendung zur Wahrung lebenswichtiger Interessen anderer notwendig ist“ durch die Wortfolge „besonderer Kategorien personenbezogener Daten, soweit deren Verarbeitung zur Wahrung lebenswichtiger Interessen erforderlich ist,“ ersetzt.

59. § 65 Abs. 5 entfällt.

60. In § 67 wird in Abs. 1 das Wort „Information“ durch die Wortfolge „Daten im Sinne des § 36 Abs. 2 Z 12 DSGVO“ und der Ausdruck „iSd“ durch die Wortfolge „im Sinne des“ ersetzt; in Abs. 2 wird das Wort „Information“ durch das Wort „Daten“ und die Wortfolge „ermittelt wurde, darf“ durch die Wortfolge „ermittelt wurden, dürfen“ ersetzt; in Abs. 2 und 3 wird jeweils das Wort „Dienstleister“ durch das Wort „Auftragsverarbeiter“ ersetzt.

61. § 68 samt Überschrift lautet:

#### **„Erkennungsdienstliche Maßnahmen auf Antrag oder mit Einwilligung des Betroffenen**

§ 68. (1) Sofern jemand dies beantragt und einen Bedarf glaubhaft macht, sind die Sicherheitsbehörden ermächtigt, von ihm Abbildungen oder Papillarlinienabdrücke herzustellen, diese mit dessen Einwilligung gemäß § 75 Abs. 1 zu verarbeiten und ihm diese mit der Bestätigung auszufolgen, dass sie von ihm stammen.

(2) Der Antrag ist abzuweisen, wenn sich der Antragsteller über seine Person nicht genügend auszuweisen vermag.

(3) Die Sicherheitsbehörden sind ermächtigt, zum Zwecke der Vorbeugung gefährlicher Angriffe gegen Leben oder Gesundheit erkennungsdienstliche Daten eines Menschen, der befürchtet, Opfer eines Verbrechens zu werden, mit seiner Einwilligung zu ermitteln und gemäß § 75 Abs. 1 zu verarbeiten.

(4) Die Sicherheitsbehörden sind ermächtigt, für Zwecke des § 66 Abs. 1 erkennungsdienstliche Daten eines Menschen, der befürchtet, Opfer eines Unfalles zu werden, mit seiner Einwilligung zu ermitteln und gemäß § 75 Abs. 1 zu verarbeiten.

(5) Die Ermittlung erkennungsdienstlicher Daten gemäß Abs. 3 und 4 hat zu unterbleiben, wenn sich der Betroffene über seine Person nicht genügend auszuweisen vermag.“

62. In § 69 Abs. 2 wird das Wort „Zustimmung“ durch das Wort „Einwilligung“ und die Wortfolge „ermittelt und benützt“ durch das Wort „verarbeitet“ ersetzt.

63. § 70 samt Überschrift lautet:

#### **„Spurenausscheidungsevidenz**

§ 70. Der Bundesminister für Inneres ist ermächtigt, erkennungsdienstliche Daten, die von Organen der Sicherheitsbehörden gemäß § 65 Abs. 2 und § 67 Abs. 1 zweiter Satz ermittelt wurden, samt erkennungsdienstlichen Identitätsdaten (§ 65 Abs. 6) in einer Spurenausscheidungsevidenz zu verarbeiten, wenn diese durch ihre berufliche Tätigkeit regelmäßig Gelegenheit haben, im Zusammenhang mit der Klärung der Umstände einer mit gerichtlicher Strafe bedrohten vorsätzlichen Handlung solche Spuren zu hinterlassen. Eine Verarbeitung dieser Daten zu anderen Zwecken als jenen der Ermittlung ist unzulässig.“

64. In § 71 Abs. 5 wird das Wort „notwendig“ durch das Wort „erforderlich“ ersetzt.

65. § 73 Abs. 1 Z 5 lautet:

„5. im Fall des § 65 Abs. 2, sobald sie ihre Funktion für den Anlassfall erfüllt haben, im Falle einer Verarbeitung der Daten in der Spurenausscheidungsevidenz nach § 70, sobald das Organ der Sicherheitsbehörde die berufliche Tätigkeit nicht mehr regelmäßig ausübt;“

66. § 75 Abs. 1 lautet:

„(1) Die Sicherheitsbehörden sind als gemeinsam Verantwortliche ermächtigt, die von ihnen gemäß den §§ 65 Abs. 1, 65a, 66 Abs. 1, 67 Abs. 1 erster Satz und Abs. 1a sowie § 68 ermittelten erkennungsdienstlichen Daten, die allenfalls vorhandenen erkennungsdienstlichen Identitätsdaten (§ 65



Abs. 6) und den für die Ermittlung maßgeblichen Grund im Rahmen einer Zentralen erkennungsdienstlichen Evidenz gemeinsam zu verarbeiten. Personenbezogene Daten, die Sicherheitsbehörden nach anderen Bestimmungen rechtmäßig ermittelt haben, dürfen sie in der zentralen erkennungsdienstlichen Evidenz weiterverarbeiten, wenn diese Verarbeitung für sicherheitspolizeiliche Zwecke in diesem Zeitpunkt zulässig wäre.“

67. In § 75 Abs. 2 wird die Wortfolge „zu benützen und zu vergleichen“ durch die Wortfolge „zu verarbeiten“ ersetzt.

68. § 76 lautet:

„§ 76. (1) Erkennungsdienstliche Maßnahmen über Antrag (§ 68 Abs. 1) sind von der Bezirksverwaltungsbehörde, innerhalb ihres örtlichen Wirkungsbereiches von der Landespolizeidirektion als Sicherheitsbehörde erster Instanz (§ 8) vorzunehmen, an die sich der Antragsteller wendet.

(2) Erkennungsdienstliche Maßnahmen mit Einwilligung des Betroffenen (§ 68 Abs. 3 und 4) sind von der Bezirksverwaltungsbehörde, innerhalb ihres örtlichen Wirkungsbereiches von der Landespolizeidirektion als Sicherheitsbehörde erster Instanz (§ 8) vorzunehmen, in deren Sprengel der Betroffene seinen Hauptwohnsitz hat oder der für seine Gefährdung maßgeblichen Tätigkeit nachgeht.

(3) Die Übermittlung erkennungsdienstlicher Daten obliegt im Falle des § 72 dem Bundesminister für Inneres, in den Fällen des § 71 Abs. 3 und 4 jener Sicherheitsbehörde, von der die maßgebliche Amtshandlung geführt wird.

(4) Die Verständigung von der Löschung der gemäß § 70 verarbeiteten erkennungsdienstlichen Daten aus der Spurenausscheidungsevidenz obliegt dem Bundesminister für Inneres. Die Verständigung gemäß § 73 Abs. 3 von der Löschung der Daten aus der Zentralen Erkennungsdienstlichen Evidenz obliegt jener Behörde, die sie ursprünglich verarbeitet hat.

(6) Die Löschung erkennungsdienstlicher Daten über Antrag des Betroffenen ist von der Landespolizeidirektion zu veranlassen, in deren Wirkungsbereich die Daten verarbeitet werden. Dieser obliegt die Information nach § 42 in Verbindung mit § 45 DSGVO. Erfolgt die Verarbeitung durch den Bundesminister für Inneres als Verantwortlichen, so obliegt diesem die Behandlung des Antrags und die Information nach § 42 in Verbindung mit § 45 DSGVO.“

69. § 80 lautet:

„§ 80. (1) Sofern Auskunft über die gemäß § 75 Abs. 1a verarbeiteten Daten begehrt wird, sind die Sicherheitsbehörden ermächtigt, vom Auskunftswerber Abbildungen oder Papillarlinienabdrücke herzustellen oder seine genetischen Daten zu ermitteln und auszuwerten, und diese Daten mit den gemäß § 75 Abs. 1a verarbeiteten Daten zu vergleichen. Von der Erteilung der Auskunft ist abzusehen, wenn der Auskunftswerber an der Ermittlung dieser Daten nicht mitgewirkt hat. Die aus Anlass des Auskunftsverlangens ermittelten Daten über den Auskunftswerber sind gesondert zu verwahren und dürfen innerhalb eines Zeitraums von einem Jahr, im Falle der Erhebung einer Beschwerde gemäß § 32 Abs. 1 Z 4 DSGVO an die Datenschutzbehörde bis zum rechtskräftigen Abschluss des Verfahrens, nicht vernichtet werden.

(2) Die Auskunft über erkennungsdienstliche Daten gemäß §§ 42 und 44 DSGVO ist von jener Landespolizeidirektion zu erteilen, in deren Wirkungsbereich die erkennungsdienstlichen Daten verarbeitet werden, wurden die Daten vom Bundesminister für Inneres verarbeitet, von diesem.“

70. In § 84 Abs. 1 wird in Z 6 der Beistrich durch das Wort „oder“ ersetzt und folgende Z 7 eingefügt:

„7. einer Verpflichtung nach § 53 Abs. 5 nicht unverzüglich nachkommt“

71. In § 84 Abs. 1 wird im Schlussteil nach dem Zitat „500 Euro,“ die Wortfolge „im Wiederholungsfall mit Geldstrafe bis zu 2 300 Euro,“ eingefügt.

72. § 90 lautet:

„§ 90. Die Datenschutzbehörde entscheidet gemäß § 32 Abs. 1 Z 4 DSGVO über Beschwerden wegen Verletzung von Rechten durch Verarbeiten personenbezogener Daten in Angelegenheiten der Sicherheitsverwaltung entgegen den Bestimmungen des DSGVO. Davon ausgenommen ist die Beurteilung der Rechtmäßigkeit der Ermittlung von Daten durch die Ausübung verwaltungsbehördlicher Befehls- und Zwangsgewalt.“



73. In § 91c Abs. 1 werden das Zitat „§ 53 Abs. 5“ durch das Zitat „§ 53 Abs. 5 erster Satz“ und das Wort „Kennzeichenerkennungsgeräten“ durch die Wortfolge „bildverarbeitenden technischen Einrichtungen“ ersetzt.

74. In § 91c Abs. 2 wird jeweils das Wort „Datenanwendung“ durch das Wort „Datenverarbeitung“ ersetzt.

75. § 91d Abs. 3 lautet:

„(3) Nimmt der Rechtsschutzbeauftragte wahr, dass durch Verarbeiten personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Verarbeitung keine Kenntnis haben, so ist er zu deren Information oder, sofern eine solche aus den Gründen des § 43 Abs. 4 des DSGVO nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzbehörde nach § 90 verpflichtet. In einem solchen Verfahren vor der Datenschutzbehörde ist auf § 43 Abs. 4 DSGVO über die Beschränkung des Auskunftsrechtes Bedacht zu nehmen.“

76. § 92a Abs. 1 lautet:

„(1) Wird durch eine technische Alarmanrichtung das Einschreiten der Organe des öffentlichen Sicherheitsdienstes verursacht, ohne dass zum Zeitpunkt der Alarmauslösung eine Gefahr für Leben, Gesundheit, Freiheit von Menschen, Eigentum oder Vermögen bestanden hat, so gebührt als Ersatz der Aufwendungen des Bundes ein Pauschalbetrag, der nach Maßgabe der durchschnittlichen Aufwendungen mit Verordnung des Bundesministers für Inneres festgesetzt wird. Die Verpflichtung zu seiner Entrichtung trifft denjenigen, zu dessen Schutz die technische Alarmanrichtung eingerichtet ist.“

77. In § 92a wird nach Abs. 1 folgender Abs. 1a eingefügt:

- „(1a) Wer ein Einschreiten von Organen des öffentlichen Sicherheitsdienstes verursacht, weil er
1. vorsätzlich eine falsche Notmeldung auslöst oder
  2. sich zumindest grob fahrlässig (§ 6 Abs. 3 StGB) einer Gefahr für Leben oder Gesundheit ausgesetzt hat,

hat als Ersatz der Aufwendungen des Bundes einen Pauschalbetrag, der nach Maßgabe der durchschnittlichen Aufwendungen, abhängig von den eingesetzten Mitteln, mit Verordnung des Bundesministers für Inneres festgesetzt wird, zu leisten. Die Verpflichtung zur Leistung trifft im Fall der Z 1 denjenigen, der die falsche Notmeldung ausgelöst hat, und im Fall der Z 2 denjenigen, dessen Leben oder Gesundheit geschützt wird.“

78. Nach § 93 wird folgender § 93a samt Überschrift eingefügt:

#### **„Informationspflicht bei Bildaufnahmen an öffentlichen Orten**

**§ 93a.** (1) Rechtsträger des öffentlichen oder privaten Bereichs, soweit letzteren ein öffentlicher Versorgungsauftrag zukommt, die zulässigerweise einen öffentlichen Ort überwachen, sind verpflichtet, die örtlich zuständige Sicherheitsbehörde über die Verwendung von Bildaufnahmegegeräten an solchen Orten zu informieren.

(2) Soweit dies auf Grundlage einer ortsbezogenen Risikoanalyse aus Gründen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit oder der Strafverfolgung erforderlich ist, hat die Sicherheitsbehörde mit Bescheid eine vier Wochen nicht überschreitende Aufbewahrungsverpflichtung festzulegen.

(3) Der Verpflichtete gemäß Abs. 2 hat die örtlich zuständige Sicherheitsbehörde zu informieren, sobald die Bildaufnahme an öffentlichen Orten dauerhaft beendet wird.“

79. Dem § 94 werden folgende Abs. 43 und 44 angefügt:

„(43) Die §§ 7 Abs. 4, 13a Abs. 2 bis 4, 25 Abs. 1, 35a Abs. 5, die Überschrift des 4. Teils, die §§ 51, 52, 53 Abs. 1, 2, 3a, 4 und 5, 53a Abs. 2, 5, 5a und 6 samt Überschrift, 53b, 54 Abs. 4b, 5, 6 und 7, 54b Abs. 1 und 3, 55 Abs. 4, 55a Abs. 4, 55b Abs. 1, 56 Abs. 1, 3 und 5, 57, 58, 58a, 58b Abs. 1, 58c, 58d Abs. 1, 58e samt Überschrift, 59 Abs. 1 und 3 samt Überschrift, 60 Abs. 2, 61, 63 samt Überschrift, 64 Abs. 2, 65 Abs. 2 und 6, 67, 68 samt Überschrift, 69 Abs. 2, 70 samt Überschrift, 71 Abs. 5, 73 Abs. 1 Z 5, 75 Abs. 1 und 2, 76, 80, 90, 91c Abs. 1 und 2, 91d Abs. 3, 92a Abs. 1 und 1a sowie die Einträge im Inhaltsverzeichnis zum 4. Teil und zu den §§ 53a, 58e, 59, 63, 68 und 70 in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2018 treten mit 25. Mai 2018 in Kraft. Gleichzeitig treten die §§ 56 Abs. 2, 59 Abs. 2 und 65 Abs. 5 außer Kraft.“

(44) Die §§ 53 Abs. 5, 84 Abs. 1 und 93a samt Überschrift sowie der Eintrag im Inhaltsverzeichnis zu § 93a in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2018 treten mit 1. März 2019 in Kraft.“

## Artikel 2

### Änderung der Straßenverkehrsordnung 1960

Die Straßenverkehrsordnung 1960 – StVO 1960, BGBl. Nr. 159/1960, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 68/2017, wird wie folgt geändert:

1. Dem § 98a Abs. 1 wird folgender Satz angefügt:

„Der Einsatz dieser technischen Einrichtungen ist der Landespolizeidirektion, in deren örtlichem Wirkungsbereich die festgelegte Messstrecke endet, sieben Tage vor seinem Beginn für Zwecke des Abs. 2 erster Satz mitzuteilen.“

2. § 98a Abs. 2 lautet:

„(2) Die Behörde, in deren örtlichem Wirkungsbereich die festgelegte Messstrecke endet, hat die nach Abs. 1 ermittelten Daten der Landespolizeidirektion gemäß Abs. 1 auf Ersuchen für Zwecke des § 54 Abs. 4b Sicherheitspolizeigesetz – SPG, BGBl. Nr. 566/1991, und der Strafrechtspflege zu übermitteln. Im Übrigen dürfen diese Daten über den Zeitpunkt der Feststellung der durchschnittlichen Fahrgeschwindigkeit auf einer festgelegten Wegstrecke hinaus nur im Überschreitungsfall und nur insoweit verwendet werden, als dies zur Identifizierung eines Fahrzeuges oder eines Fahrzeuglenkers erforderlich ist, und zwar ausschließlich für Zwecke eines Verwaltungsstrafverfahrens wegen der Überschreitung der zulässigen Höchstgeschwindigkeit. Daten, die keine Überschreitungsfälle betreffen, sind unverzüglich und in nicht rückführbarer Weise zu löschen.“

3. Dem § 103 wird folgender Abs. 19 angefügt:

„(19) § 98a Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2018 tritt mit 25. Mai 2018 in Kraft.“

## Artikel 3

### Änderung des Telekommunikationsgesetzes 2003

Das Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I Nr. 70/2003, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 6/2016, wird wie folgt geändert:

1. In § 92 Abs. 3 Z 3 wird der Strichpunkt am Ende der lit. f durch einen Beistrich ersetzt und folgende lit. g angefügt:

„g) Geburtsdatum;“

2. Nach § 97 Abs. 1 wird folgender Abs. 1a eingefügt:

„(1a) Vor Durchführung des Vertrages sowie vor der erstmaligen Wiederaufladung nach dem 1. September 2019 ist durch oder für den Anbieter die Identität des Teilnehmers zu erheben und sind die zur Identifizierung des Teilnehmers erforderlichen Stammdaten (§ 92 Abs. 3 Z 3 lit. a, b und g) anhand geeigneter Identifizierungsverfahren zu registrieren. Die Festlegung geeigneter Identifizierungsverfahren erfolgt durch Verordnung des Bundesministers für Verkehr, Innovation und Technologie im Einvernehmen mit dem Bundesminister für Inneres.“

3. Dem § 109 Abs. 3 wird folgende Z 22 angefügt:

„22. entgegen § 97 Abs. 1a die erforderlichen Stammdaten nicht, nicht vollständig oder nicht im Rahmen eines geeigneten Identifizierungsverfahrens registriert.“

4. Dem § 137 wird folgender Abs. 9 angefügt:

„(9) § 92 Abs. 3 Z 3, § 97 Abs. 1a sowie § 109 Abs. 3 in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2018 treten mit 1. Jänner 2019 in Kraft.“

## Erläuterungen

### Allgemeiner Teil

#### 1. Hauptgesichtspunkte des Entwurfs:

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

Im Rahmen der Änderung des SPG in Artikel 1 sollen zum einen wesentliche Maßnahmen zur Stärkung der Sicherheit – sowohl in objektiver als auch in subjektiver Hinsicht – implementiert 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 Artikel 2 (StVO 1960) vorgesehene Ergänzung schafft die notwendigen Voraussetzungen für die Umsetzung von geplanten Änderungen im SPG.

Ergänzend soll durch Artikel 3 (TKG 2003) dem sicherheits- und kriminalpolizeilichen Bedürfnis der Registrierung von Prepaid-Handywertkarten zum Zwecke der Gefahrenabwehr und Strafverfolgung nachgekommen werden.

Außerdem sollen durch die Änderungen des SPG (Artikel 1) die notwendigen Adaptierungen aufgrund der unionsrechtlichen Vorgaben hinsichtlich des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung; im Folgenden: DSGVO), ABl. Nr. L 119 vom 04.05.2016 S. 1, vorgenommen werden. Für den Bereich des SPG sind überwiegend die Vorgaben aufgrund der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden: DS-RL), ABl. Nr. L 119 vom 04.05.2016 S. 89, sowie deren innerstaatlichen Umsetzung durch das 3. Hauptstück des Datenschutz-Anpassungsgesetzes 2018 (im Folgenden DSG) maßgebend. Das DSG wurde mit 31. Juli 2017 kundgemacht und tritt am 25. Mai 2018 in Kraft.

Während die DSGVO allgemeine Bestimmungen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr mit solchen Daten in der Union enthält, trägt die DS-RL den Besonderheiten bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, Rechnung.

Aufgrund dieser neuen datenschutzrechtlichen Vorgaben haben die gesetzlich geregelten Datenverarbeitungen ab dem 25. Mai 2018 den durch die DSGVO und die DS-RL geänderten Anforderungen zu genügen, weshalb nahezu sämtliche Materien Gesetze, die in den legislatischen Zuständigkeitsbereich des Bundesministeriums für Inneres fallen, anzupassen sind. Da gemäß § 69 Abs. 8 DSG – im Rahmen der europa- und verfassungsrechtlichen Vorgaben – vom DSG abweichende Regelungen in Bundes- und Landesgesetzen zulässig sind, sollen die einschlägigen materienspezifischen Regelungen im Bereich des Datenschutzes als *leges speciales* den allgemeinen Regelungen des neuen DSG vorgehen.

Im Hinblick auf die Verbote der speziellen Transformation, der inhaltlichen Präzisierung sowie der inhaltlichen Wiederholung einer EU-Verordnung ist – im Falle der unmittelbaren Anwendbarkeit der DSGVO – beabsichtigt, nur die unbedingt erforderlichen Regelungen der Verordnung durchzuführen bzw. sollen Abweichungen nur im Falle materienspezifischer Notwendigkeit erfolgen. Das bisher vorgesehene Datenschutzniveau soll dabei jedoch keinesfalls unterschritten werden.

Überdies sollen die materienspezifischen Datenschutzregelungen mit der neuen datenschutzrechtlichen Terminologie der DS-RL sowie deren innerstaatliche Umsetzung durch das 3. Hauptstück des Datenschutzgesetzes in Einklang gebracht werden sowie eine Adaptierung der bisherigen Verweise erfolgen:

Der Begriff der „Verarbeitung“ personenbezogener Daten bedeutet gemäß § 36 Abs. 2 Z 2 DSG (bzw. Art. 3 Z 1 DS-RL) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Indem die „Verarbeitung“ auch die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung beinhaltet, entspricht sie damit dem bisher in § 4 Z 8 DSG 2000 definierten Begriff der „Verwendung“ personenbezogener Daten. Zum anderen soll von diesem Begriff auch das „Ermitteln“ personenbezogener Daten als Unterfall des „Verarbeitens von Daten“ iSd § 4 Z 9 DSG 2000 erfasst sein, sodass der Begriff des „Verarbeitens“ nunmehr auch das Ermitteln und Weiterverarbeiten einbezieht, soweit die Erwähnung des Ermitteln im Sinne des Ermittlungsdienstes nicht explizit erforderlich erscheint.

Dem Begriff der „Datenanwendung“ (§ 4 Z 7 DSG 2000) entspricht nunmehr der Terminus der „Datenverarbeitung“.

Dem „Auftraggeber“ einer Datenanwendung (§ 4 Z 4 DSG 2000) entspricht im Anwendungsbereich des DSG gemäß § 36 Abs. 2 Z 8 und § 47 DSG (bzw. der DS-RL gemäß Art. 3 Z 8 und Art. 21 Abs. 1 DS-RL) der „Verantwortliche“ bzw. „gemeinsam Verantwortliche“ einer Datenverarbeitung.

Dem „Dienstleister“ (§ 4 Z 5 DSG 2000) entspricht im Anwendungsbereich des DSG gemäß § 36 Abs. 2 Z 9 iVm § 48 DSG (bzw. der DS-RL gemäß Art. 3 Z 9 iVm Art. 22 DS-RL) der „Auftragsverarbeiter“. Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser gemäß § 48 DSG nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen des Datenschutzgesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der „Auftragsverarbeiter“ im Sinne des DSG entspricht im Wesentlichen dem „Dienstleister“ gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000.

Dem DSG sowie der DS-RL sind der Begriff des „Informationsverbundsystems“ (bisher § 4 Z 13 DSG 2000) nicht mehr bekannt; dieser wird nunmehr durch die Datenverarbeitung durch „gemeinsam Verantwortliche“ (§ 47 DSG bzw. Art. 21 Abs. 1 DS-RL) ersetzt. Diese erfasst den Fall, dass mehrere Verantwortliche gemeinsam die Zwecke und die Mittel einer Datenverarbeitung festlegen. Materielle Änderungen gegenüber der bisherigen Rechtslage, insbesondere eine Einschränkung des Grundsatzes, dass jedem Verantwortlichen der Zugriff auf den Gesamtbestand der in der gemeinsamen Datenverarbeitung verarbeiteten Daten – unabhängig davon, welcher Verantwortliche sie im Einzelfall ursprünglich zur Verfügung gestellt hat – offensteht, ist damit nicht verbunden.

Diese Änderungen sollen mit 25. Mai 2018 in Kraft treten.

## **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“) sowie auf Art. 11 Abs. 1 Z 4 („Straßenpolizei“) des Bundes-Verfassungsgesetzes – B-VG, BGBl. Nr. 1/1930.

## **Besonderer Teil**

### **Zu Artikel 1 (Änderung des Sicherheitspolizeigesetzes)**

#### **Zu Z 1 bis 8 (Inhaltsverzeichnis):**

Es handelt sich um die erforderlichen Ergänzungen des Inhaltsverzeichnisses.

#### **Zu Z 9 (§ 7 Abs. 4):**

Die vorgeschlagenen Änderungen dienen im Wesentlichen der Anpassung an die Vorgaben der unmittelbar anwendbaren DSGVO. Um die geistige und körperliche Eignung von Aufnahmewerbern in den Exekutivdienst und von Bewerbern für bestimmte Verwendungen beurteilen zu können, durften schon bislang – unter Einbindung von Polizeiärzten als medizinische Sachverständige – auch Gesundheitsdaten verarbeitet werden, soweit diese zur Beurteilung der Eignung für den Exekutivdienst erforderlich sind. Da es sich hierbei nicht um die Verarbeitung von Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung gemäß DS-RL handelt, unterfallen diese dem Rechtsschutzsystem der DSGVO.

Gesundheitsdaten sind nach der Definition des Art. 4 Z 15 DSGVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Die Verarbeitung personenbezogener Daten ist im gegenständlichen Fall in Erfüllung des Art. 6 Abs. 1 lit. e DSGVO für die Wahrnehmung der im öffentlichen Interesse liegenden Aufgabe der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit durch körperlich und geistig geeignete Organe erforderlich. Da Gesundheitsdaten jedoch auch besondere Kategorien von personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO darstellen, ist deren Verarbeitung nur bei Vorliegen bestimmter Fälle entsprechend Art. 9 Abs. 2 DSGVO zulässig. Die Verarbeitung der Gesundheitsdaten ist im gegebenen Zusammenhang für die Beurteilung der Arbeitsfähigkeit des Beschäftigten erforderlich (Art. 9 Abs. 2 lit. h DSGVO). Die Verarbeitung zu diesem Zweck ist zulässig, da diese Daten entsprechend Art. 9 Abs. 3 DSGVO von Fachpersonal (oder unter dessen Verantwortung) verarbeitet werden, welches Berufsgeheimnispflichten unterliegt. Künftig ist deren Verarbeitung somit nach Maßgabe des Art. 9 Abs. 2 lit. h in Verbindung mit Abs. 3 DSGVO zulässig.

Im Übrigen handelt es sich um eine redaktionelle Bereinigung.

#### **Zu 10 und 11 (§ 13a):**

Die vorgeschlagenen Änderungen dienen hauptsächlich der terminologischen Anpassung an die DS-RL sowie deren innerstaatliche Umsetzung durch das 3. Hauptstück des Datenschutzgesetzes.

Zu Abs. 3: Die Datensicherheit von Aufzeichnungen, die nach Abs. 3 zum Zwecke der Dokumentation von Amtshandlungen vorgenommen werden, erfolgte bislang nach den Bestimmungen des § 14 DSG 2000, welchem nunmehr im Wesentlichen § 54 DSG entspricht. Dieser verpflichtet den Verantwortlichen sowie den Auftragsverarbeiter dazu, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Da im Rahmen von Aufzeichnungen von Amtshandlungen jedoch auch personenbezogene Daten verarbeitet werden können, die nicht vom Zwecke der DS-RL und damit des 3. Hauptstücks des DSG erfasst sind – etwa bei Aufzeichnungen im Rahmen von Demonstrationen oder der Dokumentation von Handlungen der ersten allgemeinen Hilfeleistungspflicht –, unterliegen die Datensicherheitsmaßnahmen in solchen Fällen den Bestimmungen der unmittelbar zur Anwendung kommenden DSGVO.

Zu Abs. 4: Bislang erfolgte die Protokollierung von Dokumentationen iSd § 13a – insbesondere die Speicherdauer – nach den Vorgaben des § 14 DSG 2000. Dieser sah in Abs. 5 eine generelle Aufbewahrungsfrist für Protokolldaten vor, sofern gesetzlich nicht ausdrücklich anderes angeordnet war. Eine solche Bestimmung findet sich jedoch nicht mehr im DSG, sodass mit dem vorgeschlagenen Abs. 4 eine solche Aufbewahrungsfrist von drei Jahren normiert wird.

#### **Zu Z 12 (§ 25):**

Mit der Änderung des Abs. 1 soll das Regierungsprogramm umgesetzt und 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 risikoe erhöhenden 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 (zB. 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.

**Zu Z 13, 14, 16, 17, 19, , 25, 27, 29, 30, 31, 39, 40, 42, 43, 44, 54, 55, 60, 62, 64, 67, 74, 75 (§ 35a Abs. 5, Überschrift des 4. Teils, § 52, § 53, Überschrift des § 53a, § 53b, § 54 Abs. 5, 6 und 7, § 55 Abs. 4, § 55a Abs. 4, § 55b Abs. 1, § 57 Abs. 1, 2 und 3 erster Satz, § 58 Abs. 1 und 2, § 60 Abs. 2, § 61, § 67, § 69 Abs. 2, § 71 Abs. 5, § 75 Abs. 2, § 91c Abs. 2 und § 91d Abs. 3):**

Es handelt sich um die Anpassung an die Terminologie des DSG, ohne eine materielle Änderung der bestehenden Rechtslage herbeizuführen.

Der Begriff des „Ermittelns“ soll nunmehr vom Terminus des „Verarbeitens“ erfasst sein, sodass es keiner getrennten Erwähnung von „Ermitteln“ und „(Weiter-)Verarbeiten“ bedarf und dennoch die materielle Rechtslage beibehalten wird.

**Zu Z 15 (§ 51):**

Die Änderungen dienen der Anpassung an die §§ 39 und 48 DSG.

Zu Abs. 1: Der Begriff der „sensiblen Daten“ gemäß § 4 Z 2 DSG 2000 wurde nunmehr durch den Begriff der „besonderen Kategorien personenbezogener Daten“ gemäß § 39 DSG (Art. 10 DS-RL) ersetzt. Hiervon erfasst sind personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Verarbeitung solcher Kategorien von Daten für die Zwecke des 3. Hauptstücks des DSG – und damit für Zwecke der Sicherheitspolizei – ist dann zulässig, wenn die Verarbeitung unbedingt erforderlich ist, wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und – sofern der Betroffene die Daten nicht offensichtlich selbst öffentlich gemacht hat – die Verarbeitung gesetzlich vorgesehen ist. Durch die Änderung des zweiten Satz des Abs. 1 soll das Erfordernis der Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen der Sicherheitspolizei erfüllt werden. Eine solche ist – entsprechend der datenschutzrechtlichen Vorgaben – zulässig, wenn dies zur Erfüllung der Aufgaben im Rahmen der Sicherheitspolizei unbedingt erforderlich ist; wie bislang sind angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen. Einer ausdrücklichen Anordnung, dass bei der Verarbeitung strafrechtlich relevanter Daten angemessene Vorkehrungen zur Wahrung ebendieser Interessen getroffen werden müssen, bedarf es künftig nicht. Handelt es sich um strafrechtlich relevante Daten, so geschieht die Verarbeitung im Rahmen des SPG regelmäßig auf Grundlage des 3. Hauptstücks des DSG bzw. der DS-RL, wodurch bereits besondere Maßnahmen bei der Datenverarbeitung vorgesehen sind.

Mit der Regelung des Abs. 1 zweiter Satz soll klargestellt sein, dass die Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen der Aufgabenerfüllung der Sicherheitspolizei bei unbedingter Erforderlichkeit zulässig ist; es bedarf grundsätzlich keiner zusätzlichen ausdrücklichen Ermächtigungen. Soll die Verarbeitung solcher besonderen Daten jedoch nicht in jedem Fall – etwa nur zu bestimmten Zwecken oder nur bei bestimmten Kategorien – zulässig sein, wird dies durch ausdrückliche Erwähnung der besonderen Fälle deutlich gemacht. So ist etwa im Rahmen der Vertrauenspersonenevidenz gemäß § 54b die Verarbeitung besonderer Kategorien personenbezogener Daten ausdrücklich nur zu den Zwecken zur Verhinderung von Gefährdungen der Betroffenen und zur Bewertung der Vertrauenswürdigkeit der Informationen zulässig. Demgegenüber sieht etwa § 53a Abs. 2 den Fall der Einschränkung auf bestimmte Kategorien vor, indem die Daten, die verarbeitet werden dürfen, taxativ genannt werden. Soweit bestimmte besondere Kategorien von den aufgezählten Datenarten erfasst sind, können diese auch im Rahmen des § 53a Abs. 2 verarbeitet werden – andere, nicht von der Aufzählung erfasste, besondere Kategorien hingegen nicht. Durch § 51 Abs. 1 zweiter Satz soll diese abschließende Aufzählung keine Erweiterung erfahren.

Sofern nicht ausdrücklich anderes angeordnet wird, finden auf das Verarbeiten personenbezogener Daten die Bestimmungen des Datenschutzgesetzes Anwendung. Die Anforderungen des § 43 Abs. 1 DSG werden insbesondere durch die gesetzliche Grundlage für die Datenverarbeitungen im SPG erfüllt.

Zu Abs. 3: Durch den neu vorgeschlagenen Abs. 3 soll im Allgemeinen normiert werden, dass die Rolle des Auftragsverarbeiters für alle Datenverarbeitungen nach dem SPG dem Bundesminister für Inneres zukommen soll; es ist jedoch möglich, gesonderte Regelungen vorzusehen. Der Auftragsverarbeiter im Sinne des DSG entspricht im Wesentlichen dem „Dienstleister“ gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem „Betreiber“ gemäß § 50 Abs. 1 DSG 2000. Damit kommt gemäß Abs. 3 die Funktion des Betreibers nunmehr ausdrücklich dem



Bundesminister für Inneres in seiner Funktion als Auftragsverarbeiter zu, sofern nicht ausdrücklich anderes angeordnet wird.

§ 48 Abs. 2 DSG sieht vor, dass ein Auftragsverarbeiter keinen weiteren Auftragsverarbeiter in Anspruch nehmen kann, ohne eine vorherige gesonderte schriftliche Genehmigung des Verantwortlichen eingeholt zu haben. Diese Vorschrift ist jedoch enger als die unionsrechtlichen Vorgaben des Art. 22 Abs. 2 DS-RL, welcher es dem Verantwortlichen ermöglicht, eine allgemeine schriftliche Genehmigung für die Inanspruchnahme weiterer Auftragsverarbeiter zu erteilen. In diesem Fall hat der Auftragsverarbeiter den Verantwortlichen nur über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter zu unterrichten. Den unionsrechtlichen Vorgaben entsprechend soll abweichend von § 48 Abs. 2 DSG auch die Erteilung einer allgemeinen schriftlichen Genehmigung des Verantwortlichen ermöglicht werden. Aufgrund der verfassungsrechtlichen Weisungsbefugnis des Bundesministers für Inneres als oberste Sicherheitsbehörde ist es ausreichend, bei gemeinsamen Datenverarbeitungen mit dem Bundesminister für Inneres als gemeinsam Verantwortlichen diesen von beabsichtigten Änderungen iSd Abs. 3 letzter Satz zu unterrichten.

Zu Abs. 4: Die vorgeschlagene Neueinführung eines Abs. 4 dient der Umsetzung des § 47 DSG.

Bislang sah § 50 DSG 2000 die Möglichkeit vor, dass mehrere Auftraggeber gemeinsam ein Informationsverbundsystem betreiben und damit Daten gemeinsam verarbeiten können. Nunmehr normiert § 47 DSG die gemeinsame Verarbeitung, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen. Hierbei fungieren die Verantwortlichen als gemeinsam Verantwortliche, die ihre jeweiligen Aufgaben nach dem Datenschutzgesetz, insbesondere hinsichtlich der Wahrnehmung der Rechte Betroffener und wer welchen Informationspflichten gemäß § 43 DSG nachkommt, festzulegen haben. Nur sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht gesetzlich normiert sind, hat dies mittels Vereinbarung zu geschehen.

In diesem Sinne soll der vorgeschlagene Abs. 4 gesetzlich die Zuständigkeiten zwischen den gemeinsam Verantwortlichen von Datenverarbeitungen auf Grundlage des SPG dahingehend aufteilen, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach dem Datenschutzgesetz von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst ursprünglich verarbeiteten Daten stehen. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige gemeinsam Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach dem Datenschutzgesetz zukommt. Möchte ein Betroffener ein Recht nach dem Datenschutzgesetz wahrnehmen, hat er hierfür seine Identität nachzuweisen, um missbräuchliche oder unberechtigte Geltendmachung angeblicher Rechte hintanhalten zu können.

Nimmt ein Betroffener ein Recht gegenüber einem unzuständigen gemeinsam Verantwortlichen wahr – somit nicht gegenüber demjenigen, der seine Daten ursprünglich verarbeitet und damit in die gemeinsame Datenverarbeitung eingespeichert hat –, hat dieser durch Konsultation des zuständigen gemeinsam Verantwortlichen zu prüfen, ob die Unterrichtung des Betroffenen womöglich gemäß § 43 Abs. 4 DSG aufgeschoben, eingeschränkt oder unterlassen werden soll. Liegt kein solcher Fall vor, ist der Betroffene gemäß dem letzten Satz des neuen Abs. 4 an den zuständigen gemeinsam Verantwortlichen zu verweisen.

Begehrt der Betroffene jedoch die Aktualisierung oder Richtigstellung von Namen, Geschlecht, früheren Namen, Staatsangehörigkeit, Geburtsdatum, Geburtsort, Wohnanschrift, Namen der Eltern oder Aliasdaten gemäß § 59 Abs. 1 zweiter Satz, kann dies von jedem gemeinsam Verantwortlichen vorgenommen werden. Eine Verweisung auf denjenigen gemeinsam Verantwortlichen, der die Daten ursprünglich eingespeichert hat, ist in diesem Fall nicht erforderlich. Eine vorgenommene Berichtigung iSd § 59 Abs. 1 zweiter Satz bewirkt jedoch keine Änderung der Zuständigkeit des ursprünglichen gemeinsam Verantwortlichen. Werden in Folge weitere Ansprüche iSd DSG geltend gemacht, obliegt deren Wahrnehmung weiterhin dem ursprünglich gemeinsam Verantwortlichen, auch wenn zwischenzeitlich eine Berichtigung der Daten iSd § 59 Abs. 1 zweiter Satz von einer anderen Sicherheitsbehörde vorgenommen wurde.

**Zu Z 18 und 70 (§ 53 Abs. 5 und § 84 Abs. 1 Z 7):**

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 sicherheitspolizeilichen Aufgabenerfüllung zu verarbeiten. Wie schon bisher ist die Verarbeitung von Daten über nichtöffentliches Verhalten unzulässig. Durch das Abstellen auf Bildaufnahmegeräte im Sinne des § 12 DSG sind künftig auch Tonaufnahmen erfasst, da gemäß § 12 Abs. 1 DSG die mit einer Bildaufnahme mitverarbeiteten akustischen Informationen auch vom Begriff „Bildaufnahme“ umfasst sind. Dadurch wird verhindert, dass die Sicherheitsbehörden Daten deshalb nicht nach Abs. 5 verwenden können, weil auch Tondaten enthalten sind. Soll die Übergabe von Bild- und Tondaten an die Sicherheitsbehörde der Aufklärung einer Straftat



oder der – nicht von der Aufgabe der Fahndung gemäß § 24 SPG – umfassten Fahndung nach einem potentiellen Täter dienen, kommen die Bestimmungen der StPO zur Anwendung.

Für bestimmte Rechtsträger wird darüber hinausgehend eine Verpflichtung geschaffen, unverzüglich Bild- und Tondaten auf Ersuchen der Sicherheitsbehörde zu übermitteln bzw. für den Fall der Notwendigkeit eines Echtzeitstreamings unverzüglich Zugang zu den gerade erst anfallenden Bilddaten zu gewähren, damit die Sicherheitsbehörde diese Daten für die taxativ genannten Zwecke weiterverwenden kann. Die Herausgabepflicht ist demnach an das konkrete Vorliegen einer der genannten Aufgaben geknüpft. 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 DSGVO zulässigerweise Bildaufnahmegeräte an öffentlichen Orten (§ 27 SPG) verwenden. Die auf diese Weise erlangten Daten sind der Sicherheitsbehörde bei Vorliegen eines konkreten Anlassfalls („Aufgabe“) herauszugeben oder es ist Zugang bspw. im Wege des Echtzeitstreamings zu gewähren. Zudem wird ein Lösungsverbot für diese Rechtsträger ab Kenntnisaufnahme 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. 1. Demnach ist der Rechtsschutzbeauftragte von der Sicherheitsbehörde von der Inanspruchnahme dieser Verpflichtung zu verständigen, um die Rechtmäßigkeit der Maßnahme zu prüfen.

#### **Zu Z 20 bis 24 (§ 53a Abs. 2, 5 bis 6):**

Die Änderungen dienen im Wesentlichen der begrifflichen Anpassung an das DSGVO.

Zu Abs. 2: Da bereits § 51 Abs. 1 eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien von Daten im Rahmen der Sicherheitspolizei normiert, bedarf es grundsätzlich keiner weiteren Anführung. Die Verarbeitung ist dabei natürlich an die Grenzen und Erfordernisse des § 39 DSGVO sowie des § 51 Abs. 1 gebunden, sodass diese nur bei unbedingter Erforderlichkeit zulässig ist. Demgegenüber sieht etwa § 53a Abs. 2 den Fall der Einschränkung auf bestimmte Kategorien vor, indem die Daten, die verarbeitet werden dürfen, taxativ genannt werden. Soweit bestimmte besondere Kategorien von den aufgezählten Datenarten erfasst sind, können diese auch im Rahmen des § 53a Abs. 2 verarbeitet werden – andere, nicht von der Aufzählung erfasste, besondere Kategorien hingegen nicht. Durch § 51 Abs. 1 zweiter Satz soll diese abschließende Aufzählung keine Erweiterung erfahren.

Zu Abs. 5 und 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.

Im Übrigen dienen die sonstigen vorgeschlagenen Änderungen der Abs. 5 und 6 lediglich einer sprachlichen Vereinfachung.

Zu Abs. 5a: Der Auftragsverarbeiter im Sinne des § 36 Abs. 2 Z 9 DSGVO entspricht im Wesentlichen dem „Dienstleister“ gemäß § 4 Z 5 DSGVO 2000 und – soweit es sich bei der Datenanwendung um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSGVO 2000. Die Funktion des Betreibers übte in Bezug auf die zentrale Datenverarbeitung nach Abs. 5a bisher ausdrücklich das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung aus. Nunmehr weist § 51 Abs. 3 erster Satz dem Bundesminister für Inneres die Funktion des Auftragsverarbeiters zu, sofern nicht ausdrücklich anderes angeordnet wird. Da das Bundesamt jedoch eine Organisationseinheit der Sicherheitsbehörde Bundesminister für Inneres ist (vgl. § 1 Abs. 3 Polizeiliches Staatsschutzgesetz in Verbindung mit § 6 Abs. 1) und damit im Innenverhältnis auch weiterhin mit der faktischen Aufgabe der Auftragsverarbeitung betraut werden kann, bedarf es keiner von der Generalklausel des § 51 Abs. 3 erster Satz abweichenden Regelung. Wenngleich nunmehr das Bundesamt nicht mehr ausdrücklich in Abs. 5a angeführt wird, wird damit keine tatsächliche Änderung des aktuellen Rechtsbestands herbeigeführt.

#### **Zu Z 26 und Z 73 (§ 54 Abs. 4b und § 91c Abs. 1):**

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 Bundesstraßen-Mautgesetz 2002 bzw. § 50 Abs. 2 Eisenbahngesetz 1957). Abfragekriterium in der Fahndungsevidenz bleibt weiterhin ausschließlich das Kennzeichen des Fahrzeugs. Andere Daten dürfen nicht für den Abgleich herangezogen werden. Im Trefferfall dürfen die verarbeiteten Daten auch zur Abwehr und Aufklärung gefährlicher Angriffe sowie zur Abwehr krimineller Verbindungen verarbeitet werden.

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, nachts oder an Wochenenden erfolgt eine Anzeigerstattung 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 bis zu zwei Wochen speichern zu können, um im Anlassfall (neue Fahndung) über einen Abgleich Hinweise über den Verbleib des Fahrzeuges zu generieren. Die Ermittlungsmaßnahme obliegt weiterhin der nachprüfenden Kontrolle durch den Rechtsschutzbeauftragten (§ 91c Abs. 1). Um diesem eine sinnvolle Prüfung der gesetzlichen Voraussetzungen zu ermöglichen, sind in die Meldung an den Rechtsschutzbeauftragten insbesondere Angaben zur Löschung der Daten nach der Maximalfrist von zwei Wochen sowie Angaben zu den verarbeiteten Daten aufzunehmen.

#### **Zu Z 28 (§ 54b Abs. 1 und 3):**

Es handelt sich in erster Linie um eine terminologische Anpassung an die neuen Begrifflichkeiten des DSGVO. Wie bereits geltend soll auch weiterhin klargestellt sein, dass besondere Kategorien personenbezogener Daten nur soweit verarbeitet werden dürfen, als dies zur Verhinderung von Gefährdungen der Betroffenen und zur Bewertung der Vertrauenswürdigkeit der Informationen unbedingt erforderlich ist. § 51 Abs. 1 zweiter Satz soll diese Zweckbeschränkung nicht erweitern.

Da strafrechtsbezogene Daten künftig keinem gesonderten Regime unterliegen und auch nicht vom Begriff der besonderen Kategorien von Daten erfasst sind, sind diese als personenbezogene Daten zu verarbeiten.

Jede Verarbeitung der in der Vertrauenspersonenevidenz verarbeiteten personenbezogenen Daten ist – auch weiterhin – zu protokollieren. Da die Protokollierung für Datenverarbeitungen im Rahmen der Sicherheitspolizei nach dem 4. Teil des SPG nunmehr generell in § 63 Abs. 3 normiert ist, bedarf es keiner gesonderten Bestimmung in § 54b Abs. 3, sodass diese zu entfallen hat. Die Protokollierung erfolgt künftig auf Grundlage des § 63 Abs. 3.

#### **Zu Z 32 bis 38 (§ 56):**

Die Änderungen des Abs. 1 dienen der Anpassung an das DSGVO, wobei Z 1 lediglich begrifflicher Natur ist.

Zu Abs. 1: Die Übermittlung personenbezogener Daten – unabhängig davon, ob es sich auch um besondere Kategorien personenbezogener Daten handelt – zur Wahrung lebenswichtiger Interessen einer Person bedarf entsprechend § 38 DSGVO keiner ausdrücklichen Rechtsgrundlage mehr. Wenngleich eine Übermittlung zu diesem Zweck nunmehr auch ohne gesetzliche Regelung zulässig ist, soll Abs. 1 Z 5 zur Vermeidung von Rechtsunsicherheiten grundsätzlich beibehalten werden. Da die Übermittlung jedoch generell zulässig ist, unabhängig von der Einordnung des zu übermittelnden Datums als besondere Kategorie, hat der Halbsatz zu den vormals sensiblen Daten zu entfallen.

Die Übermittlung gemäß Abs. 1 Z 7 für Zwecke der wissenschaftlichen Forschung und Statistik ist im Anwendungsbereich des § 36 Abs. 1 DSGVO – somit insbesondere für Zwecke der Sicherheitspolizei – nach den Bestimmungen des DSGVO zulässig, im Anwendungsbereich der DSGVO nach den unmittelbar geltenden Bestimmungen dieser. Der Verweis auf die Regelung des § 46 DSGVO 2000 hat zu entfallen.

Im Übrigen handelt es sich um eine redaktionelle Ergänzung.

Zu Abs. 2: Die Regelungen zur Protokollierung finden sich nunmehr gebündelt in § 63 Abs. 3, sodass Abs. 2 zu entfallen hat. Auch die Bestimmung hinsichtlich automatisierter Abfragen von KFZ-Kennzeichendaten gemäß § 54 Abs. 4b findet sich nunmehr § 63 Abs. 3. Diese sind auch weiterhin nur insoweit zu protokollieren, als es sich um Treffer handelt. Damit bleibt das hohe Niveau des Datenschutzes für Personen, deren KFZ-Kennzeichen zwar durch Kennzeichenerkennungsgeräte erfasst wurden ohne einen Trefferfall zu bewirken, auch weiterhin aufrecht.

Zu Abs. 3: Abs. 3 regelte bislang die Vorgehensweise bei der Übermittlung von unvollständigen oder unrichtigen Daten; dies ist nunmehr insbesondere § 37 DSGVO zu entnehmen. Gemäß § 37 Abs. 6 DSGVO dürfen unrichtige, unvollständige, nicht mehr aktuelle oder zu löschende personenbezogene Daten nicht übermittelt werden. Zu diesem Zweck sind die Daten vor einer Übermittlung soweit möglich entsprechend

zu überprüfen. Wird festgestellt, dass personenbezogene Daten übermittelt worden sind, die nicht diesen Anforderungen entsprechen, ist dies dem Empfänger unverzüglich mitzuteilen. Letzterer hat unverzüglich die Löschung unrechtmäßig übermittelter Daten, die Berichtigung unrichtiger Daten, die Ergänzung unvollständiger Daten oder eine Einschränkung der Verarbeitung vorzunehmen (§ 37 Abs. 8 DSGVO). Hat im umgekehrten Fall der Empfänger Grund zur Annahme, dass übermittelte personenbezogene Daten unrichtig, nicht aktuell oder zu löschen sind, ist dies dem Übermittler mitzuteilen, welcher unverzüglich die erforderlichen Maßnahmen zu setzen hat (§ 37 Abs. 9 DSGVO). Wenngleich diese Bestimmungen des DSGVO auch unmittelbar im Rahmen des SPG zur Anwendung kommen, wird im Sinne der Rechtssicherheit und Verständlichkeit des Gesetzes ein Verweis auf § 37 Abs. 8 und 9 DSGVO aufgenommen.

**Zu Abs. 5:** Insbesondere zum Zweck der Vermeidung zukünftiger Ausschreitungen bei Sportgroßveranstaltung ermöglicht Abs. 1 Z 3a die Übermittlung bestimmter personenbezogener Daten an den Österreichischen Fußballbund sowie die Österreichische Fußball-Bundesliga zur Prüfung und Veranlassung eines Sportstättenbetretungsverbot. Abs. 5 sieht vor, dass eine solche Übermittlung nach Eingehen vertraglicher Verpflichtungen des Österreichischen Fußballbundes und der Österreichischen Fußball-Bundesliga zur Einhaltung bestimmter Sicherheitsmaßnahmen zulässig ist. Die Verarbeitung der übermittelten personenbezogenen Daten durch Fußballbund und Bundesliga erfolgt nicht zu einem Zweck des 3. Hauptstücks des DSGVO, sodass die Bestimmungen der DSGVO unmittelbar zur Anwendung kommen. Die Änderungen des Abs. 5 dienen im Übrigen der terminologischen Anpassung an die Begrifflichkeiten der DSGVO.

**Zu Z 41, 42, 45 und 56 (§§ 57 Abs. 2a, 57 Abs. 3 zweiter Satz, 58 Abs. 3 und 63):**

Mit der Einfügung eines Abs. 2a in § 57 wird die Rechtsgrundlage geschaffen, um gemäß § 98a StVO 1960 ermittelte und an die Sicherheitsbehörde übermittelte Daten mit den Fahndungsevidenzen für die Zwecke des § 54 Abs. 4b (Fahndung, Abwehr und Aufklärung gefährlicher Angriffe und Abwehr krimineller Verbindungen) abzugleichen. Die Speicherdauer dieser Daten (§ 58 Abs. 3) sowie die Protokollierung im Trefferfall (§ 63 Abs. 3) werden wie beim Einsatz von polizeieigenen Kennzeichenerkennungssystemen gemäß § 54 Abs. 4b festgelegt.

**Zu Z 46 bis 50 (§ 58a, § 58b Abs. 1, § 58c, § 58d Abs. 1, § 58e samt Überschrift):**

Es handelt sich ausschließlich um Anpassungen an die Terminologie des DSGVO, ohne eine materielle Änderung der bestehenden Rechtslage herbeizuführen. Gemäß § 51 Abs. 3 kommt die Funktion des Betreibers dem Bundesminister für Inneres in seiner Funktion als Auftragsverarbeiters zu.

**Zu Z 48 (§ 58c):**

Im Übrigen wurden redaktionelle Bereinigungen vorgenommen.

**Zu Z 49 (§ 58d Abs. 1):**

Die Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt entsprechend § 51 Abs. 1 zweiter Satz.

**Zu Z 51 bis 53 (§ 59 samt Überschrift):**

Die Änderungen der Überschrift sowie der Abs. 1 und 3 dienen in erster Linie der begrifflichen Anpassung an das DSGVO.

In Konkretisierung des § 50 DSGVO finden sich die Regelungen zur Protokollierung nunmehr gebündelt in § 63 Abs. 3 für alle Datenverarbeitungen, unabhängig davon ob sie lokal oder zentral geführt werden, sodass Abs. 2 zu entfallen hat. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen. Die Zuordnung zu einem bestimmten Organwalter ist bei ausschließlich programmgesteuerten (vormalige Diktion: automatisierten) Abfragen auch weiterhin nicht erforderlich (vgl. Art. 25 Abs. 1 DSRL, wonach die Identifizierung der Person, welche die Daten abgefragt oder offengelegt hat, nur so weit wie möglich zu ermöglichen ist). Von der Protokollierung ausgenommen bleiben ausschließlich programmgesteuerte (vormalige Diktion: automatisierte) Abfragen gemäß § 54 Abs. 4b, es sei denn, es handelt sich um einen Trefferfall. Auch die Bestimmung hinsichtlich ausschließlich programmgesteuerter Abfragen von KFZ-Kennzeichendaten gemäß § 54 Abs. 4b findet sich nunmehr in § 63 Abs. 3. Diese sind auch weiterhin nur insoweit zu protokollieren, als es sich um Treffer handelt.

**Zu Z 56 (§ 63 samt Überschrift):**

Die Änderungen der Überschrift und des Abs. 1 dienen der Anpassung an das DSGVO.

Die Regelungen zur Protokollierung iSd § 50 DSGVO finden sich nunmehr gebündelt in einem neuen Abs. 3 für alle Datenverarbeitungen, unabhängig davon ob sie lokal oder zentral geführt werden, wobei festzuhalten ist, dass die Verarbeitung von Daten innerhalb der Organisationsstruktur des Verantwortlichen bzw. durch gemeinsam Verantwortliche keine Übermittlung iSd § 50 DSGVO darstellt. Die vormalige

Regelung des § 59 Abs. 2 wurde übernommen, indem die Zuordnung zu einem bestimmten Organwalter bei ausschließlich programmgesteuerten (vormalige Diktion: automatisierten) Abfragen auch weiterhin nicht erforderlich ist (vgl. Art. 25 Abs. 1 DS-RL, wonach die Identifizierung der Person, welche die Daten abgefragt oder offengelegt hat, nur so weit wie möglich erforderlich ist, sowie § 59 Abs. 2 alt). Erfasst von dieser Ausnahmebestimmung sind solche Abfragen, die nicht durch eine Willensbetätigung eines Menschen initiiert werden, sondern ausschließlich durch ein Computersystem aufgrund seiner Programmierung vollautomatisch durchgeführt werden. Hierbei ist die Zuordnung zu einem bestimmten Organwalter nicht möglich, da kein Organ, sondern ausschließlich ein Computersystem, tätig wird. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen. Auch die Bestimmung hinsichtlich der ausschließlich programmgesteuerten (vormalige Diktion: automatisierter) Abfragen von KFZ-Kennzeichendaten gemäß § 54 Abs. 4b findet sich nunmehr in § 63 Abs. 3. Diese sind auch weiterhin nur insoweit zu protokollieren, als es sich um Treffer handelt.

**Zu Z 57 (§ 64 Abs. 2):**

Die Änderungen dienen der Anpassung an die Bestimmungen des § 36 Abs. 2 Z 12 und 13 DSG.

§ 36 Abs. 2 Z 12 DSG definiert „genetische Daten“ als personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden; Z 13 beschreibt „biometrische Daten“ als mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten. Von diesen Begriffen erfasst sind etwa erkennungsdienstliche Maßnahmen wie die Abnahme von Papillarlinienabdrücken, die Vornahme von Mundhöhlenabstrichen, die Herstellung von Abbildungen, die Vornahme von Messungen oder die Erhebung von Stimmproben.

Die neue Terminologie des DSG aufgreifend wird die Definition der „erkennungsdienstlichen Maßnahmen“ iSd SPG als technische Verfahren zur Feststellung von biometrischen oder genetischen Daten (§ 36 Abs. 2 Z 12 und 13 DSG) sowie die Feststellung äußerlicher körperlicher Merkmale und die Erhebung von Schriftproben eines Menschen zum Zweck der Wiedererkennung aktualisiert. Eine materielle Änderung der bestehenden Rechtslage erfolgt durch die Neutextierung jedoch nicht.

**Zu Z 58 und 59 (§ 65):**

Die Änderung des Abs. 2 erfolgt in Anpassung an die Voraussetzungen des Abs. 1.

Da sich die Informations- und Verständigungspflichten unmittelbar insbesondere aus § 43 DSG ergeben, hat Abs. 5 keinen originären Anwendungsbereich und damit zu entfallen. Der Betroffene ist nunmehr nach den Bestimmungen des DSG (§§ 42 ff DSG) über seine Rechte zu informieren.

Im Übrigen handelt es sich um erforderliche begriffliche Anpassungen an das DSG.

**Zu Z 61 (§ 68 samt Überschrift):**

Es handelt sich im Wesentlichen um Anpassungen an die Terminologie des DSG, ohne eine materielle Änderung der bestehenden Rechtslage herbeizuführen, sowie um sprachliche Vereinfachungen. Gemäß den Abs. 3 und 4 können Sicherheitsbehörden von Personen, die befürchten, Opfer eines Verbrechens bzw. eines Unfalls zu werden, mit deren Einwilligung erkennungsdienstliche Daten ermitteln, um gefährlichen Angriffen gegen Leben oder Gesundheit vorzubeugen bzw. die Identifizierung eines Leichnams zu erleichtern. Bislang konnten diese Daten nur lokal bei der ermittelnden Sicherheitsbehörde gespeichert werden. Um im Anlassfall jedoch tatsächlich die Erfüllung des Speicherzwecks der Gefahrenvorbeugung bzw. Identifizierung unabhängig vom Ort der Gefahr oder des Unfalls sicherstellen zu können, bedarf es einer zentralen Datenverarbeitung. Daher sollen – wie bereits in Abs. 1 vorgesehen – auch die gemäß § 68 Abs. 3 und 4 ermittelten erkennungsdienstlichen Daten mit Einwilligung des Betroffenen in der Zentralen erkennungsdienstlichen Evidenz (§ 75) verarbeitet werden können.

**Zu Z 63 (§ 70 samt Überschrift):**

Neben § 75 zur Zentralen erkennungsdienstlichen Evidenz traf § 70 Bestimmungen zur Aufbewahrung erkennungsdienstlicher Daten in lokal geführten erkennungsdienstlichen Evidenzen. Damit war es grundsätzlich jeder Sicherheitsbehörde ermöglicht, solche erkennungsdienstlichen Daten, die sie im Rahmen einer erkennungsdienstlichen Behandlung oder Maßnahme ermittelt hat, in einer lokalen Datenbank aufzubewahren. Darüber hinaus konnte der Bundesminister für Inneres durch Verordnung die Grundlage für regionale oder überregionale Evidenzen spezieller Daten nach Abs. 2 schaffen. Da diese Rechtsgrundlagen nach den Abs. 1 bis 3 jedoch über keine praktische Relevanz mehr verfügen, sollen diese bereinigt werden.

Abs. 4 idgF hingegen ermöglicht es, Daten, die von Organen der Sicherheitsbehörden als „Gelegenheitspersonen“ – somit insbesondere von Kriminalbeamten, die regelmäßig mit der Klärung von Umständen gerichtlich strafbarer Handlungen am Tatort befasst sind – ermittelt wurden, in einer gesonderten Evidenz zu führen. Ziel dieser „Police-Elimination-Datei“ ist die Ausscheidung der von erkennungsdienstlich tätigen Beamten hinterlassenen Spuren bei der Tataufklärung. Diese Bestimmung steht im Zusammenhang mit § 65 Abs. 2 und § 67 Abs. 1 und erlaubt eine solche Datenermittlung bloß in Einzelfällen. § 70 soll nunmehr ausschließlich die Grundlage zur Führung einer solchen Police-Elimination-Datei, somit einer „Spurenausscheidungsevidenz“, sein. Die Führung dieser Evidenz obliegt dem Bundesminister für Inneres als Verantwortlichen. Im Übrigen handelt es sich lediglich um terminologische Anpassungen, insbesondere auch an das DSG sowie die Begrifflichkeit der §§ 65 und 67, und die Berichtigung eines redaktionellen Versehens.

**Zu Z 65 (§ 73 Abs. 1 Z 5):**

Die Änderung dient der Anpassung an die Überarbeitung des § 70.

**Zu Z 66 (§ 75 Abs. 1):**

Die Adaptierungen des Abs. 1 dienen der Anpassung an die Änderungen des § 68, der terminologischen Aktualisierung im Sinne des DSG sowie der sprachlichen Vereinfachung. Künftig können auch Daten, die gemäß § 68 Abs. 3 und 4 zum Zwecke der Vorbeugung gefährlicher Angriffe gegen Leben oder Gesundheit bzw. der Identifizierung von Toten mit Einwilligung des Betroffenen ermittelt wurden, in der Zentralen erkennungsdienstlichen Evidenz verarbeitet werden.

**Zu Z 68 (§ 76):**

Die Änderungen der Abs. 1, 2, 3 und 6 dienen der Anpassung an die Terminologie und Vorgaben des DSG sowie der redaktionellen Bereinigung. Die Änderungen des Abs. 4 erfolgen in Anpassung an die Überarbeitung des § 70.

**Zu Z 69 (§ 80):**

Die Änderungen gründen sich auf die Vorgaben des DSG. Indem Informationen gemäß § 43 DSG sowie alle Mitteilungen und Maßnahmen gemäß den §§ 44 und 45 DSG künftig unentgeltlich zur Verfügung zu stellen sind, hat Abs. 1 zu entfallen und ist Abs. 2 anzupassen. Im Übrigen handelt es sich um Anpassung an die Terminologie und die Bestimmungen des DSG.

**Zu Z 71 (§ 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.

**Zu Z 72 (§ 90):**

Die Änderung dient der Anpassung an die Vorgaben des DSG, wobei das bisher bestehende Regime nicht abgeändert werden soll. Zur Verarbeitung personenbezogener Daten zählt auch das Erheben, weshalb das „Ermitteln“ personenbezogener Daten prinzipiell von § 90 erfasst ist. Dies gilt allerdings auch weiterhin dann nicht, wenn die Ermittlung personenbezogener Daten in Form von verwaltungsbehördlicher Befehls- und Zwangsgewalt, etwa im Rahmen einer zwangsweisen Durchsuchung von Räumen, der zwangsunterstützten Anfertigung von Lichtbildern oder durch zwangsweise Erhebung anderer erkennungsdienstlicher Daten erfolgt. In diesen Fällen, in denen es um die Rechtmäßigkeit der Befugnisausübung geht, sollen – wie auch bisher – ausschließlich die Landesverwaltungsgerichte zur Entscheidung nach § 88 Abs. 1 zuständig sein.

**Zu Z 76 (§ 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 und Gesundheit von Menschen – dienen, von der Regelung im Fall eines Fehlalarms umfasst sind.

**Zu Z 77 (§ 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. Davon umfasst ist auch der Fall, dass jemand eine Gefahrensituation etwa mittels täuschend echten „Spielzeugwaffen“ vortäuscht und dadurch eine Notmeldung (durch Dritte) auslöst. 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 vorsätzlich die 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. Die Höhe der zu ersetzenden Pauschalbeträge ist vom Bundesminister für Inneres durch Verordnung festzusetzen.

#### **Zu Z 78 (§ 93a):**

Bereits nach derzeitiger Rechtslage hat die Datenschutzbehörde im Registrierungsverfahren bei entsprechendem Vorbringen zu prüfen, ob eine über die 72 Stunden hinausgehende Speicherdauer für Rechtsträger des öffentlichen oder privaten Bereichs, 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 durch Abs. 1 die öffentlichen oder privaten Auftraggeber, soweit letzteren ein öffentlicher Versorgungsauftrag zukommt (etwa Verkehrsbetriebe oder Bahnhofs- oder Flughafenbetreiber), die zulässigerweise einen öffentlichen Ort überwachen, verpflichtet werden, die örtlich zuständige Sicherheitsbehörde über ihre Verwendung von Bildaufnahmegeräten an öffentlichen Orten zu informieren, um dieser die Gelegenheit zu geben, eine auf den jeweiligen Ort der Videoüberwachung 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 vier Wochen nicht überschreitende Aufbewahrungsverpflichtung festzulegen (Abs. 2).

Durch die bescheidmäßige Festlegung einer längeren Aufbewahrungsverpflichtung wird der entsprechend Abs. 2 verpflichtete Rechtsträger selbstverständlich nicht daran gehindert, die Videoüberwachung wieder einzustellen. Er hat darüber nur die Sicherheitsbehörde zu informieren (Abs. 3).

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 im Rahmen des „Videoüberwachungsverbesserungsgesetzes“, BGBl. I S. 968, vorgesehen hat, bei Videoüberwachungen an bestimmten Orten (öffentlich zugängliche großflächige Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungstätten, Einkaufszentren oder Parkplätzen, oder Fahrzeuge und öffentlich zugängliche großflächige Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs) – 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 79 (§ 94 Abs. 43 und 44):**

Es handelt sich um die erforderlichen Inkrafttretens- und Außerkrafttretensbestimmung.

### **Zu Artikel 2 (Änderung der Straßenverkehrsordnung 1960)**

#### **Zu Z 1 und 2 (§ 98a):**

Grundvoraussetzung für die effektive Anwendbarkeit des § 54 Abs. 4b SPG ist, dass auch die auf Grundlage des § 98a StVO ermittelten Daten der abschnittsbezogenen Geschwindigkeitsüberwachung zulässigerweise an die Landespolizeidirektion als Sicherheitsbehörde übermittelt werden dürfen. Der Zweck der Übermittlung ergibt sich aus dem Verweis auf § 54 Abs. 4b SPG (Fahndung, Abwehr und Aufklärung gefährlicher Angriffe und Abwehr krimineller Verbindungen).

Erforderlich ist hierbei die rechtzeitige Information der Sicherheitsbehörde, wann welche Geschwindigkeitsüberwachungsanlagen aktiv sind. Die Landespolizeidirektion ist von der für die Verkehrsüberwachung zuständigen Behörde sieben Tage vor Beginn des Einsatzes für Zwecke des Abs. 2 erster Satz zu informieren. An eine allfällige Unterlassung der Informationsverpflichtung sind keine weiteren Konsequenzen geknüpft.

Sowohl die Information über die Aktivität der Überwachungsanlage als auch die Übermittlung der im Rahmen der abschnittsbezogenen Geschwindigkeitsüberwachung erhobenen Daten zum Zweck des § 54 Abs. 4b SPG hat durch jene die Verkehrsüberwachung anordnende Behörde iSd Abs. 1 zu erfolgen, in deren Wirkungsbereich die mittels Verordnung festgelegte Messstrecke endet. Da eine gebündelte Verarbeitung der erhobenen Daten zur Zweckerfüllung erforderlich ist, sollen sowohl die Information als auch die Datenübermittlung wiederum an jene Landespolizeidirektion erfolgen, in deren örtlichem Wirkungsbereich die festgelegte Messstrecke endet. Die Landespolizeidirektion nimmt dabei die Funktion der Landesleitzentrale wahr. Die weitere Verwendung der Daten richtet sich nach dem SPG bzw. der StPO.

Ergeht ein Ersuchen der zuständigen Landespolizeidirektion auf Übermittlung der Daten in diesem Sinne, so sind durch die zuständige Behörde alle im Rahmen der abschnittsbezogenen Geschwindigkeitsüberwachung erhobenen Daten – somit noch bevor diese nach Errechnung der durchschnittlichen Fahrgeschwindigkeit gefiltert werden – zu übermitteln. Davon abgesehen erfolgt die Übermittlung der Daten zum Zweck der Führung eines Verwaltungsstrafverfahrens an die diesbezüglich zuständige Behörde auch weiterhin nur im Überschreitungsfall nach der Feststellung der durchschnittlichen Fahrgeschwindigkeit.

**Zu Z 3 (§ 103 Abs. 19):**

Es handelt sich um die Inkrafttretensbestimmung.

**Zu Artikel 3 (Änderung des Telekommunikationsgesetzes 2003)**

**Zu Z 1 (§ 92 Abs. 3 Z 3):**

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

**Zu Z 2 (§ 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 insbesondere auch der Erwerb von Prepaid-SIM-Karten umfasst ist, im Anlassfall identifizierbar sind. Zur Erhebung der Identität dieser Vertragspartner (Teilnehmer) ist die Registrierung bestimmter Stammdaten (§ 92 Abs. 3 Z 3) jedenfalls vor Durchführung des Vertrags („Aktivierung“, „Freischaltung“ des Anschlusses) erforderlich. Im Begutachtungsverfahren wurde vorgebracht, dass auch für bestehende Teilnehmer mit Prepaid-SIM-Karten eine Identifizierungspflicht statuiert werden sollte. Diese Anregung wird insofern aufgegriffen, als eine Registrierung bereits bestehender Kunden vorzunehmen sein wird, sobald die erste Wiederaufladung des Wertkartenguthabens nach dem 1. September 2019 erfolgt. Die Registrierung bestimmter Stammdaten, wie jene des akademischen Grades sowie des Geburtsdatums (§ 92 Abs. 3 Z 3 lit. b und g), kann natürlich nur im Falle eines Vertragsabschlusses mit einer natürlichen Person in Frage kommen. Wie im Begutachtungsverfahren mehrfach vorgebracht, kommt der Richtigkeit der dabei erhobenen Stammdaten wesentliche Bedeutung zu (vgl. dazu auch die Gesetzgebungsvorgänge in Deutschland vom Juli 2016, Gesetz zum besseren Informationstausch bei der Bekämpfung des internationalen Terrorismus vom 26. Juli 2016). Um dem raschen technischen Fortschritt und den unterschiedlichen Administrativvorgängen bei den jeweiligen Anbietern einerseits und der notwendigen Verlässlichkeit der Identifizierung andererseits entsprechend Rechnung zu tragen, sollen im Rahmen einer Verordnung jene Identifizierungsverfahren geregelt werden, die geeignet sind, die Richtigkeit der Identität des jeweiligen Teilnehmers mit den jeweils zur Verfügung stehenden Mittel zu gewährleisten. In Betracht kommt dabei etwa die Vorlage eines amtlichen Lichtbildausweises ebenso wie ein in den eingelangten Stellungnahmen von Seiten der Anbieter vorgebrachtes videounterstütztes, elektronisches Verfahren.

Die Speicherung der nach Abs. 1a ermittelten Daten richtet sich nach den in § 97 Abs. 2 genannten Fristen.

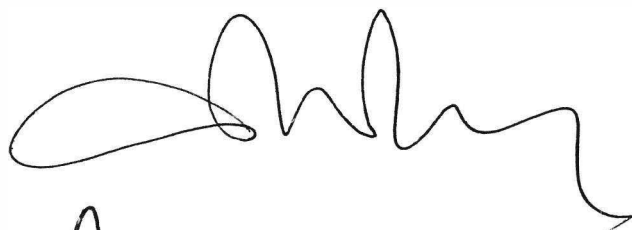
**Zu Z 3 (§ 109 Abs. 3 Z 22):**

An dieser Stelle wird die durch die Einführung von der Registrierungspflicht für Prepaid-SIM-Karten erforderliche Strafbestimmung normiert.



**Zu Z 4 (§ 137 Abs. 9):**

Es handelt sich um die Inkrafttretensbestimmung. Die Verpflichtung zur Erhebung der Identität der Teilnehmer erfordert technische und organisatorische Vorkehrungen durch die Anbieter. Die vorgeschlagene Legisvakanz bis zum 1. Jänner 2019 soll den Anbietern ermöglichen, diese Vorbereitungen zu treffen.



Johann  
Prins  
Nikolaus Prins



