VERNEHMLASSUNGSBERICHT

DER REGIERUNG

BETREFFEND

DIE ABÄNDERUNG DES GESETZES ÜBER DIE ELEKTRONISCHE KOMMUNIKATION (KOMG) UND DER STRAFPROZESSORDNUNG

(ANLASSDATENSPEICHERUNG)

Ministerium für Inneres, Wirtschaft und Umwelt

Vernehmlassungsfrist: 19. April 2024

INHALTSVERZEICHNIS

Seite

Zusammenfassung 4

Zuständiges Ministerium 5

Betroffene Stellen 5

1. Ausgangslage 6
   1.1 Werdegang der Vorratsdatenspeicherung in Liechtenstein 6
   1.2 Das Urteil C-793/19 und C-794/19 des EuGH 9

2. Begründung der Vorlage 14

3. Schwerpunkte der Vorlage 17
   3.1 Anlassdatenspeicherung 17
   3.2 IP-Adressen 18
   3.3 Daten zur Identifikation von Teilnehmern 18
   3.4 Wegfall des Kataloges von Straftaten 19

4. Erläuterungen zu den einzelnen Artikeln 20
   4.1 Abänderung des KomG 20
   4.2 Abänderung der StPO 29

5. Verfassungsmässigkeit / Rechtliches 31

6. Auswirkungen auf die nachhaltige Entwicklung 32

7. Regierungsvorlagen 33
   7.1 Gesetz über die elektronische Kommunikation 33
   7.2 Strafprozessordnung 43

ZUSAMMENFASSUNG

Die liechtensteinischen Bestimmungen zur Vorratsdatenspeicherung wurden 2010 im Gesetz über die elektronische Kommunikation (KomG) sowie der Verordnung über elektronische Kommunikationsnetze und -dienste (VKND) eingeführt. Damit wurden die Vorgaben der in das EWR-Abkommen übernommenen Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der vom Gerichtshof der Europäischen Union (EuGH) zwischenzeitlich für ungültig erklärten Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten) umgesetzt.

Bereits mit seinem Urteil vom 8. April 2014 in der Rechtssache C-293/12 erklärte der Gerichtshof der Europäischen Union (EuGH) die Richtlinie 2006/24/EG als ungültig, da sie einen Eingriff von grossem Ausmass und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten beinhalte, der sich nicht auf das absolut Notwendige beschränke. Weiter stellte der EuGH mit Urteil vom 21. Dezember 2016 in den verbundenen Rechtssachen C-203/15 und C-698/15 fest, dass auch die Richtlinie 2002/58/EG im Lichte der Charta der Grundrechte der Europäischen Union dahingehend auszulegen sei, dass diese einer nationalen Regelung entgegenstehe, die für die Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmenden vorsehe. Diese Ansicht hat der EuGH mit seinem Urteil vom 20. September 2022 in den verbundenen Rechtssachen C-793/19 und C-794-19 konkretisiert. Er kam zum Schluss, dass die Grundrechtecharta der Europäischen Union dahingehend auszulegen sei, dass diese einer nationalen Rechtsvorschrift, die für die Zwecke der Verfolgung schwerer Straftaten oder zur Abwehr einer konkreten Gefahr der nationalen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung eines Grossteils der Verkehrs- und Standortdaten mit einer Speicherungsfrist von mehreren Wochen vorsehe, entgegenstehe. Ausnahmen hierzu können gemäss EuGH in Bezug auf die Speicherung von IP-Adressen und Daten zur Identifikation von Teilnehmern vorgesehen werden.

Die Urteile des EuGH sind insofern für Liechtenstein von Bedeutung, als die in der Grundrechtecharta der Europäischen Union normierten Grundrechte weitgehend

identisch mit den von der Liechtensteinischen Verfassung und der in Liechtenstein anwendbaren Europäischen Menschenrechtskonvention normierten Grundrechten sind und die Urteile somit weitgehend auch auf die liechtensteinischen Verhältnisse übertragbar sind.

Vor diesem Hintergrund setzte die Regierung unter dem Vorsitz des Amtes für Kommunikation eine Arbeitsgruppe aus Vertretern des Amtes für Justiz, der Datenschutzstelle, der Landespolizei, des Fürstlichen Landgerichtes und der Staatsanwaltschaft ein und beauftragte diese, die geltende Regelung zur Vorratsdatenspeicherung zu überprüfen.

Mit der gegenständlichen Vorlage wird der Wechsel von der aktuell geltenden, allgemeinen und unterschiedslosen Vorratsdatenspeicherung zu einer anlassbasierten Datenspeicherung aufgezeigt und es werden die dafür notwendigen gesetzlichen Anpassungen im Gesetz über die elektronische Kommunikation sowie in der Strafprozessordnung vorgenommen.

ZUSTÄNDIGES MINISTERIUM

Ministerium für Inneres, Wirtschaft und Umwelt

BETROFFENE STELLEN

Amt für Kommunikation
Amt für Justiz
Datenschutzstelle
Fürstliches Landgericht
Landespolizei
Staatsanwaltschaft

Vaduz, 23. Januar 2024

LNR 2024-21

P

1. AUSGANGSLAGE

1.1 Werdegang der Vorratsdatenspeicherung in Liechtenstein

Die liechtensteinischen Bestimmungen zur Vorratsdatenspeicherung wurden 2010 im Gesetz über die elektronische Kommunikation[1] eingeführt und ergänzt durch Ausführungsbestimmungen in der Verordnung über elektronische Kommunikationsnetze und -dienste[2] (VKND), LGBl. 2007 Nr. 67.

Mit der liechtensteinischen Vorratsdatenspeicherung wurden die Vorgaben der in das EWR-Abkommen übernommenen Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) und der vom EuGH zwischenzeitlich für ungültig erklärten Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, umgesetzt.

Vor dem Hintergrund, dass die Vorratsdatenspeicherung seit jeher im Spannungsfeld zwischen den Interessen eines adäquaten Grundrechtsschutzes

---

1 Gesetz vom 17. März 2006 über die elektronische Kommunikation (Kommunikationsgesetz; KomG), LGBl. 2006 Nr. 91.

2 Verordnung vom 3. April 2007 über elektronische Kommunikationsnetze und -dienste (VKND), LGBl. 2007 Nr. 67.

einerseits und einer adäquaten Strafverfolgung andererseits steht und auch in Liechtenstein kontrovers diskutiert wurde und wird, wurde bereits bei der Einführung der heute geltenden Regelung eine vermittelnde Lösung angestrebt und bspw. der Richtervorbehalt konsequent vorgeschrieben. Einzige Ausnahme vom Richtervorbehalt ist die Standortfeststellung, bei der jedoch die Dringlichkeit der Suche und Rettung einer in Not geratenen Person eine solche Ausnahme nicht nur rechtfertigt, sondern geradezu verlangt.

Mit der Revision des KomG 2017[3] wurde die Vorratsdatenspeicherung im Lichte der hierzu ergangenen Rechtsprechung des EuGH angepasst.

Mit seinem Urteil vom 8. April 2014 in der Rechtssache C-293/12 erklärte der EuGH die Richtlinie 2006/24/EG für ungültig, da sie einen Eingriff von grossem Ausmass und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten beinhalte, der sich nicht auf das absolut Notwendige beschränke.

Mit seinem Urteil vom 21. Dezember 2016 in den verbundenen Rechtssachen C-203/15 und C-698/15 bestätigte der EuGH sodann, dass auch die Richtlinie 2002/58/EG im Lichte der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen sei, dass Art. 15 Abs. 1 der Richtlinie 2002/58/EG einer nationalen Regelung entgegenstehe, die für die Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmenden und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsehe. Zudem hat der EuGH zu Recht anerkannt, dass Art. 15 Abs. 1 der Richtlinie 2002/58/EG in der durch die Richtlinie 2009/136/EG geänderten Fassung im Lichte

---

[3] Vgl. BuA 2017 Nr. 27 sowie 2017 Nr. 88.

der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen sei, dass er einer nationalen Regelung entgegenstehe, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand habe, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschliesslich auf die Zwecke der Bekämpfung schwerer Straftaten zu beschränken und ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen.

Basierend auf diesen beiden Urteilen des EuGH wurde die gesetzliche Grundlage der Vorratsdatenspeicherung in Liechtenstein 2017 überprüft und in der Auffassung, dass weiterhin Bedarf für eine Vorratsdatenspeicherung vorhanden ist, mit folgenden Regelungen angepasst:

- Schaffung eines eindeutigen und abschliessenden Katalogs von "schweren" Straftaten, also jener Straftaten, bei welchen die Verwertung von auf Vorrat gespeicherten Daten zur Anwendung kommen kann;
- Ausbau der Bestimmungen zur Datensicherheit und zur Gewährleistung eines Sicherheitsniveaus, welches der Bedeutung der auf Vorrat gespeicherten Daten bzw. dem potentiellen Risiko einer Verletzung der Privatsphäre Rechnung trägt;
- Sicherstellung einer unabhängigen Überwachung durch die Datenschutzstelle und die Schaffung von Instrumenten zur Kontrolle;
- Rechtsschutz und Kontrolle im Zusammenhang mit der Speicherung und der Verwertung von auf Vorrat gespeicherten Daten;
- Einführung eines Systems von Sanktionen bei Zuwiderhandlungen gegen Vorschriften über die Vorratsspeicherung von Daten und den dazu gehörenden Datenschutzbestimmungen;

- Berücksichtigung von Zeugnisverweigerungsrechten und Berufsgeheimnisträgern bei der Speicherung von Daten auf Vorrat bzw. deren Verwertung.

Das Urteil des EuGH vom 20. September 2022 in den verbundenen Rechtssachen C-793/19 und C-794/19 liess im Rahmen der Behandlung der Totalrevision des KomG[4] im Landtag die Diskussion über die heutige Vorratsdatenspeicherung erneut aufkommen (siehe nachfolgendes Kapitel für inhaltliche Aspekte zu diesem Urteil). Die in der 2. Lesung von verschiedenen Abgeordneten geforderte komplette Streichung der gesetzlichen Bestimmungen zur Vorratsdatenspeicherung fand keine Mehrheit im Landtag. Vor diesem Hintergrund beschloss die Regierung, die Arbeitsgruppe zur Vorratsdatenspeicherung aus 2014, bestehend aus Vertretern des Amtes für Kommunikation, des Amtes für Justiz, der Datenschutzstelle, der Landespolizei, des Fürstlichen Landgerichtes und der Staatsanwaltschaft, erneut einzusetzen, um die aktuelle gesetzliche Grundlage zur Vorratsdatenspeicherung im Lichte des genannten EuGH-Urteils vom 20. September 2022 zu überprüfen.

1.2 Das Urteil C-793/19 und C-794/19 des EuGH

Dem Urteil des EuGH lag die Vorlagefrage zu Grunde, ob Art. 15 Abs. 1 der Richtlinie 2002/58/EG im Lichte der Art. 6 bis 8 und 11 sowie des Art. 52 Abs. 1 der Charta und des Art. 4 Abs. 2 EUV[5] dahin auszulegen ist, dass er einer nationalen Rechtsvorschrift entgegensteht, die – von bestimmten Ausnahmen abgesehen – die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste für die in Art. 15 Abs. 1 der genannten Richtlinie aufgeführten Zwecke, insbesondere zur Verfolgung schwerer Straftaten oder zur Abwehr einer konkreten Gefahr für die nationale Sicherheit, zu einer allgemeinen und unterschiedslosen Vorratsspei-

---

4 vgl. BuA Nr. 122/2022 und BuA Nr. 22/2023.

5 Vertrag über die Europäische Union (EUV).

cherung eines Grossteils der Verkehrs- und Standortdaten der Endnutzer dieser Dienste verpflichtet und eine Speicherungsfrist von mehreren Wochen sowie Regeln vorsieht, die einen wirksamen Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang gewährleisten sollen. In seinen Erwägungen hielt der EuGH dazu unter Rückblick auf seine bisherige Rechtsprechung Folgendes fest:

«Nach Art. 52 Abs. 1 der Grundrechtecharta sind Einschränkungen der Ausübung der in den Art. 7, 8 und 11 der Charta verankerten Rechte zulässig, sofern sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte achten. Unter Wahrung des Grundsatzes der Verhältnismässigkeit müssen sie erforderlich sein und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (Rn. 63). Somit ist in Bezug insbesondere auf die wirksame Bekämpfung von Straftaten, deren Opfer u.a. Minderjährige und andere schutzbedürftige Personen sind, zu berücksichtigen, dass sich aus Art. 7 der Charta positive Verpflichtungen der Behörden im Hinblick auf den Erlass rechtlicher Massnahmen zum Schutz des Privat- und Familienlebens ergeben können. Solche Verpflichtungen können sich aus Art. 7 auch in Bezug auf den Schutz der Wohnung und der Kommunikation sowie aus den Art. 3 und 4 hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit der Menschen sowie des Verbots der Folter und unmenschlicher oder erniedrigender Behandlung ergeben (Rn. 64).

Angesichts dieser verschiedenen positiven Verpflichtungen müssen die verschiedenen betroffenen berechtigten Interessen und Rechte somit miteinander in Einklang gebracht werden, und es ist ein rechtlicher Rahmen zu schaffen, der diesen Einklang ermöglicht (Rn. 65).

In diesem Rahmen ergibt sich bereits aus dem Wortlaut von Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58, dass die Mitgliedstaaten eine Vorschrift erlassen können,

die von dem in Rn. 52 des vorliegenden Urteils genannten Grundsatz der Vertraulichkeit abweicht, wenn eine solche Vorschrift „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismässig“ ist, wobei es im elften Erwägungsgrund der Richtlinie heisst, dass eine derartige Massnahme in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss (Rn. 66).

Um dem Erfordernis der Verhältnismässigkeit zu genügen, müssen nationale Rechtsvorschriften klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Massnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. Diese Rechtsvorschriften müssen nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Massnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisiert verarbeitet werden, vor allem wenn eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht. Diese Erwägungen gelten in besonderem Mass, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht (Rn. 69).

Daher hat der Gerichtshof, was den Schutz der nationalen Sicherheit anbelangt, dessen Bedeutung die der übrigen von Art. 15 Abs. 1 der Richtlinie 2002/58 erfassten Ziele übersteigt, festgestellt, dass diese Bestimmung im Lichte der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta Rechtsvorschriften nicht entgegensteht, die es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich

der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht (Rn. 72).

Was das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, hat der Gerichtshof festgestellt, dass im Einklang mit dem Grundsatz der Verhältnismässigkeit nur die Bekämpfung schwerer Kriminalität und die Verhütung ernster Bedrohungen der öffentlichen Sicherheit geeignet sind, die mit der Speicherung von Verkehrs- und Standortdaten verbundenen schweren Eingriffe in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, zu rechtfertigen. Daher können nur Eingriffe in die genannten Grundrechte, die nicht schwer sind, durch das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein (Rn. 73).

Was das Ziel der Bekämpfung schwerer Kriminalität anbelangt, hat der Gerichtshof entschieden, dass nationale Rechtsvorschriften, die zu diesem Zweck die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen, die Grenzen des absolut Notwendigen überschreiten und nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden können. Angesichts des sensiblen Charakters der Informationen, die sich aus den Verkehrs- und Standortdaten ergeben können, ist deren Vertraulichkeit nämlich von entscheidender Bedeutung für das Recht auf Achtung des Privatlebens. In Anbetracht zum einen der in Rn. 62 des vorliegenden Urteils angesprochenen abschreckenden Wirkungen, die die Speicherung dieser Daten

auf die Ausübung der in den Art. 7 und 11 der Charta verankerten Grundrechte haben kann, und zum anderen der Schwere des mit ihr verbundenen Eingriffs muss eine solche Speicherung in einer demokratischen Gesellschaft, wie es das durch die Richtlinie 2002/58 geschaffene System vorsieht, die Ausnahme und nicht die Regel sein, und solche Daten dürfen nicht Gegenstand einer systematischen und kontinuierlichen Speicherung sein. Dies gilt auch in Anbetracht der Ziele der Bekämpfung schwerer Kriminalität und der Verhütung ernster Bedrohungen der öffentlichen Sicherheit sowie der Bedeutung, die ihnen beizumessen ist (Rn. 74).»

Aufgrund dieser Erwägungen kommt der EuGH in Rn. 75 insgesamt zum Ergebnis, dass Rechtsvorschriften zu Datenspeicherungen mit der Grundrechtecharta vereinbar sind, die:

- auf der Grundlage objektiver und nichtdiskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen (d.h. keine allgemeine und unterschiedslose Vorratsspeicherung dieser Daten);
- für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;
- eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;
- vorsehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben werden kann, während eines

festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern (quick freeze).

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen (Rn. 75).

Ergänzend ist festzuhalten, dass der EuGH in seinen Ausführungen die Begrifflichkeiten «schwere Kriminalität» und «schwere Bedrohungen der öffentlichen Sicherheit» nach wie vor nicht näher definiert, wodurch dem Gesetzgeber ein gewisser Spielraum eingeräumt wird.

2. BEGRÜNDUNG DER VORLAGE

Das Urteil des EuGH vom 20. September 2022 in den verbundenen Rechtssachen C-793/19 und C-794/19 ist, wie die bereits früher ergangenen EuGH-Urteile zur Vorratsdatenspeicherung vom 8. April 2014 in der Rechtssache C-193/12 und vom 21. Dezember 2016 in den verbundenen Rechtssachen C-203/5 und C-698/15, insofern für Liechtenstein von Bedeutung, als die in der Grundrechtecharta der Europäischen Union normierten Grundrechte weitgehend identisch mit den von der Liechtensteinischen Verfassung und der in Liechtenstein anwendbaren Europäischen Menschenrechtskonvention normierten Grundrechten sind und das Urteil somit weitgehend auch auf die liechtensteinischen Verhältnisse übertragbar ist.

Nach Prüfung des Urteils durch die von der Regierung eingesetzte Arbeitsgruppe wurde klar, dass die geltende Vorratsdatenspeicherung insbesondere mit Blick auf den in Rn. 75 des Urteils C-793/19 und C-794/19 aufgeführten Katalog zulässiger Rechtsvorschriften einer Anpassung bedarf bzw. die geltende Vorratsdaten-

speicherung durch eine mit Rn. 75 des Urteils im Einklang stehende Datenverarbeitung, im Sinne einer Anlassdatenspeicherung, zu ersetzen ist.

Auch wenn die Vorratsdatenspeicherung in der bisherigen Form aufzuheben ist, wird die Auffassung vertreten, dass eine reine Streichung der Vorratsdatenspeicherung ohne eine Alternative zur Speicherung von Verkehrs-, Standort- und Teilnehmerdaten nicht zielführend wäre. Dies insbesondere, da die Einsatzzwecke von diesen Daten im Strafverfahren zentral und, vom konkreten Einzelfall abhängig, sehr vielfältig sein können, vor allem, wenn zwischen Täter und Opfer lediglich telefonischer Kontakt bestand. Dies trifft in klassischer Weise auf den Tatbestand der beharrlichen Verfolgung zu, bei dem eine Aufklärung des Tatverdachts bzw. eine Beweisführung ohne diese Daten unmöglich wäre. Dazu gehören aber auch andere, regelmässig unter Verwendung von Mitteln der elektronischen Kommunikation begangene Delikte, wie z.B. die Verbreitung von Kinderpornographie. Auch wenn es nicht um eine Kommunikation zwischen Täter und Opfer geht, können darüber hinaus in vielen Fällen durch die Auswertung der Daten relevante Erkenntnisse gewonnen werden. Dies z.B. anhand des Bewegungsprofils (Zellenstandort) oder der Kontakte des Tatverdächtigen (insbesondere bei Betäubungsmitteldelikten) oder aber auch zur Unterstützung bewilligter Observationen. Es darf in diesem Zusammenhang auch nicht vergessen werden, dass Liechtenstein regelmässig mit rechtshilfeweisen Anfragen zu solchen Daten konfrontiert wird und die Beantwortung ohne diese Daten nicht möglich wäre.

Es wird daher vorgeschlagen, die bisherige allgemeine und unterschiedslose Vorratsdatenspeicherung – abgesehen von der Speicherung der IP-Adressen wie auch der Daten zur Identifikation der Teilnehmenden – durch eine Anlassdatenspeicherung zu ersetzen. Die Zulässigkeit bzw. Durchführung dieser Anlassdatenspeicherung bedarf, im Einklang mit dem in Liechtenstein

bestehenden Untersuchungsrichtermodell im strafprozessualen Vorverfahren, weiterhin zwingend eines gerichtlichen Beschlusses und sieht nicht bloss eine richterliche Ex-post-Kontrolle vor. Das Rechtsschutzniveau ist somit unter diesem Aspekt höher als vom EuGH gefordert.[6]

Das EuGH-Urteil in den verbundenen Rechtssachen C-793/19 und C-794/19 lässt zudem für gewisse Datenverarbeitungen Spielraum offen. So ist es nach dem EuGH insbesondere zulässig, zur Bekämpfung schwerer Kriminalität eine allgemeine und unterschiedslose Speicherung der IP-Adressen sowie der Daten zur Identifikation der Teilnehmenden vorzusehen und Anbietern von elektronischen Kommunikationsdiensten mittels einer der wirksamen gerichtlichen Kontrolle unterliegenden Entscheidung der zuständigen Behörde aufzutragen, während eines festgelegten Zeitraumes die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten für maximal sechs Monate in die Zukunft zu speichern (Rn. 75 und 131).

Insbesondere von den Strafverfolgungsbehörden wurde damit argumentiert, dass die Abfragen der IP-Adressen durch die Strafverfolgungsbehörden in vielen Verfahren ein wesentlicher und unverzichtbarer Bestandteil der Ermittlungen und der Beweisführung sind. Je nach Sachverhalt wäre eine Aufklärung eines Tatverdachtes ohne Verwertung solcher Daten nur schwer möglich, wenn nicht gar unmöglich.

Aufgrund des Ersatzes der Speicherung der Daten auf Vorrat durch eine Speicherung der Daten basierend auf einem konkreten Anlass mit gerichtlichem

---

[6] Anders etwa die österreichische Regelung der Anlassdatenspeicherung nach §§ 135 Abs 2b, 137 Abs 1 öStPO (idF BGBl I 2018/27), die eine, wenn auch nachträglich rechtsschutzbewährte, staatsanwaltliche Anordnung für die Datensicherung genügen lässt.

Beschluss müssen neben einigen Bestimmungen im KomG auch § 102a StPO sowie einige Bestimmungen in der VKND revidiert werden.

Die Regierungsvorlage zur Anlassdatenspeicherung wird von allen in der Arbeitsgruppe vertretenen Stellen (Amt für Kommunikation, Amt für Justiz, Datenschutzstelle, Landespolizei, Landgericht, Staatsanwaltschaft) gutgeheissen und in der Umsetzung unterstützt.

3. SCHWERPUNKTE DER VORLAGE

Die Vorlage dient der Aufhebung der geltenden Regelung zur Vorratsdatenspeicherung und der grundrechtskonformen Normierung der Anlassdatenspeicherung (mit gerichtlichem Beschluss) sowie der Speicherung und Auskunftspflicht von Anbietern über IP-Adressen sowie Daten zur Identifikation von Teilnehmern.

3.1 Anlassdatenspeicherung

In Umsetzung der bisher ergangenen EuGH-Urteile, wie auch insbesondere in Bezug auf das jüngste EuGH-Urteil aus dem Jahr 2022, wird in der gegenständlichen Gesetzesrevision von einer allgemeinen und unterschiedslosen Vorratsspeicherung abgesehen. Stattdessen wird eine Anlassdatenspeicherung und Sicherung vorhandener Daten implementiert. Im Gegensatz zur bisherigen allgemeinen und unterschiedslosen Vorratsdatenspeicherung werden Daten lediglich im Einzelfall zur Verfolgung schwerer Kriminalität auf Anordnung des Gerichts gesichert, für eine bestimmte Zeitspanne in die Zukunft gespeichert und herausgegeben.

3.2 IP-Adressen

Wenn sich eine Person im Internet einwählt, so wird dieser vom Diensteanbieter eine IP-Adresse zugewiesen, unter welcher die Person im Internet auftritt und sichtbar ist. Beendet die Person die Internetsitzung (Formulierung im Gesetz: «Beendigung der aktiven Nutzung»), so wird bei dynamischen IP-Adressen die zuvor vergebene Adresse wieder einem anderen Kunden zugewiesen. Ist z.B. ein zentraler Router installiert, wird die Internetsitzung von diesem aufrechterhalten, sodass auch eine dynamische IP-Adresse über einen längeren Zeitraum dem gleichen Kunden zugewiesen sein kann.

Aufgrund der Verpflichtung zur Speicherung von IP-Adressen muss der Diensteanbieter speichern, welchem Kunden er zu einem bestimmten Zeitpunkt eine konkrete IP-Adresse zugewiesen hat. Wird im Internet eine Straftat begangen, so ist hier vom Tatverdächtigen vorerst nur die IP-Adresse sichtbar. Die konkrete Person dahinter kann von den Strafverfolgungsbehörden nur festgestellt werden, wenn die Diensteanbieter die IP-Adressen speichern. Der häufigste Anwendungsfall in diesem Zusammenhang betrifft die Internetkriminalität, wie beispielsweise verbotene Pornographie, Drohungen, Betrug, Stalking etc.

Die Ermittlung eines Tatverdächtigen ohne die Speicherung von IP-Adressen wäre aussichtlos und schlicht unmöglich. Darüber hinaus wird darauf hingewiesen, dass Liechtenstein Ersuchen aus dem Ausland um Erhebung solcher Daten auf dem Wege der Rechtshilfe erhält, die ohne die Speicherung von IP-Adressen nicht beantwortet werden könnten und somit Liechtenstein einem erheblichen Reputationsrisiko ausgesetzt würde.

3.3 Daten zur Identifikation von Teilnehmern

Genau wie die IP-Adressen ist auch die Identifikation der Teilnehmer für die Strafverfolgung ein zentrales Element. Da es sich hierbei lediglich um die

Identifikation von Teilnehmern, also die Zuordnung der Zugänge zu elektronischen Kommunikationsmitteln zu einer Person handelt, ist dies als geringer Eingriff zu werten. Zu denken ist insbesondere an die Zuordnung einer Telefonnummer an einen Kunden.

3.4 Wegfall des Kataloges von Straftaten

Im Rahmen der Einführung der Bestimmungen zur anlasslosen Vorratsdatenspeicherung wurde seinerzeit versucht, durch verschiedene Massnahmen einen Ausgleich zu diesem Grundrechtseingriff zu schaffen.

Diese Massnahmen umfassten einerseits umfassende Bestimmungen zum Datenschutz. So wurde eine Pflicht zur Protokollierung aller Vorgänge und eine Pflicht zur Führung von Statistiken vorgeschrieben. Ebenso wurde die Aufsicht der Datenschutzstelle umfangreich und explizit vorgeschrieben. Als weitere Massnahme wurde die Anwendbarkeit der Vorratsdatenspeicherung auf einen reduzierten Katalog von Straftaten beschränkt. Dabei handelte es sich einerseits um Straftaten, die als schwer anzusehen sind (Verbrechen), aber andererseits auch um solche Straftaten, deren Aufklärung in besonderem Mass vom Vorhandensein von Daten abhängt, wie sie von Vorratsdaten erfasst werden. So ist z.B. die Beharrliche Verfolgung nach § 107a StGB (besser bekannt als «Stalking») nur mit einem Strafmass von 2 Jahren bewehrt und damit kein Verbrechen im Sinn des § 17 StGB, sondern nur ein Vergehen. Da dieses Vergehen aber auch im Wege einer elektronischen Kommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels elektronisch begangen werden kann, sind die von der Vorratsdatenspeicherung erfassten Daten für die Aufklärung praktisch unerlässlich. Liegen keine solchen Daten in die Vergangenheit vor, ist die Aufklärung entsprechend erschwert. Mit dieser Lösung war dem Eingriff in die Grundrechte durch die Vorratsdatenspeicherung einerseits die Schwere und

andererseits die Aufklärbarkeit einer Straftat – und damit das öffentliche Interesse an der Strafverfolgung generell – als Gegengewicht entgegengestellt worden.

Mit dem Wechsel zur Anlassdatenspeicherung ist nun vorgesehen, dass jener Katalog von Straftaten im Gesetz entfällt. Die Anlassdatenspeicherung soll über gerichtlichen Beschluss bei allen Verbrechen und Vergehen Anwendung finden können, wenn ein Anlass gegeben ist und die entsprechenden Voraussetzungen erfüllt sind. Dazu führt der EuGH in seinem Urteil vom 20. September 2022 in den verbundenen Rechtssachen C-793/19 und C-794/19 aus, dass die mittels gerichtlichem Beschluss festgelegte Massnahme zur Speicherung der Anlassdaten der Bekämpfung der schweren Kriminalität dienen sowie entsprechend verhältnismässig sein muss. Verbrechen (Straftaten, die mit Freiheitsstrafe von mehr als drei Jahren bedroht sind) fallen generell unter die Kategorie der schweren Kriminalität, wohingegen dies bei Vergehen nicht generell angenommen werden kann und daher durch das Gericht im Einzelfall anhand der Verhältnismässigkeit zu beurteilen ist. Keine Anwendung finden können solche Massnahmen bei blossen Übertretungen wie im Verwaltungsstrafrecht. Eine Anwendung auf Übertretungen verbietet sich insbesondere, da Übertretungen im Verhältnis zu Vergehen oder gar Verbrechen keine «schwere Straftat» im Sinn der Rechtsprechung des EuGH sein können.

4. ERLÄUTERUNGEN ZU DEN EINZELNEN ARTIKELN

4.1 Abänderung des KomG

Die vorgeschlagenen gesetzlichen Anpassungen basieren auf dem Gesetz vom 5. April 2023 über die elektronische Kommunikation (Kommunikationsgesetz; KomG), LGBl. 2023 Nr. 216, welches gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses Nr. 275/2021 vom 24. September 2021 zur

Änderung von Anhang XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) des EWR-Abkommens in Kraft treten wird.

Zu Art. 3 Abs. 1 Ziff. 49 und 49a

Ziff. 49: Die gegenständliche Definition stellt eine an die Systematik der Anlassdatenspeicherung angepasste Definition dar, wobei die Grundlage die Definition der Vorratsdaten bildet. Im Wesentlich ändert sich dabei nur das «Wann» der Datenspeicherung, d.h. die Daten sind nicht mehr auf Vorrat, sondern nur auf Anlass zu speichern, was sich im Begriff der Anlassdatenspeicherung niederschlägt. Die zu speichernden Daten bleiben weiterhin dieselben wie unter der Vorratsdatenspeicherung. Hierzu wurde zur Konkretisierung in der Definition ein Verweis auf Art. 67 Abs. 4 eingefügt, welcher eine Liste mit den umfassenden Anlassdaten enthält.

Ziff. 49a: Aufgrund der Tatsache, dass die Vorratsdatenspeicherung durch eine Anlassdatenspeicherung, eine Pflicht zur Speicherung der Daten zur Identifikation der Teilnehmenden wie auch der Pflicht zur Speicherung von IP-Adressen ersetzt wird, ist eine entsprechende Ergänzung der Definitionen notwendig.

Zu Art. 66 Abs. 2 und 3 sowie Artikelüberschrift

Unabhängig von der Vorrats- resp. neu Anlassdatenspeicherung haben Diensteanbieter bei Vertragsabschluss nach Art. 66 Abs. 1 Teilnehmerdaten zu verifizieren, aufzuzeichnen und während der gesamten Vertragsdauer sowie sechs Monate nach deren Beendigung aufzubewahren. Die Verifizierung und Aufbewahrung dieser Daten dient, neben der Überprüfung des Teilnehmenden resp. dessen Identität bei Vertragsabschluss, unter anderem dem Anbieten von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen und um Anbietern von öffentlich zugänglichen Auskunftsdiensten sowie Herausgebern von Teilnehmerverzeichnissen diese zur Verfügung zu stellen (vgl. Art. 17 Abs. 2 Bst. h KomG).

Abs. 2: Da die Pflicht zur Verifizierung und Aufbewahrung von Teilnehmerdaten in Abs. 1 in keinem Zusammenhang mit der Vorrats- resp. Anlassdatenspeicherung bzw. der Pflicht zur Auskunft über die Identifikation von Teilnehmern gegenüber der Landespolizei steht, mussten diese beiden Pflichten bzw. Verarbeitungszwecke im Sinne des Art. 5 Abs. 1 Bst. b Datenschutz-Grundverordnung (DSGVO) sowie Art. 47 Bst. b Datenschutzgesetz (DSG) systematisch getrennt werden. Daraus folgt, dass Abs. 2, in welchem bis anhin die auf schriftliches Ersuchen der Landespolizei zu erteilende Auskunft über Teilnehmerdaten normiert war, in Art. 66 aufzuheben ist resp. die Auskunftspflicht auf Ersuchen der Landespolizei neu in Art. 67b normiert wird (vgl. Erläuterungen zu Art. 67b).

Entsprechend dieser Trennung muss auch die **Artikelüberschrift** von Art. 66 angepasst werden.

Abs. 3: Aufgrund der Aufhebung von Abs. 2 resp. dadurch, dass die Auskunftspflicht über Teilnehmerdaten neu in Art. 67b aufgeht, muss Abs. 3 redaktionell angepasst werden.

Zu Art. 67

Mit **Abs. 1** werden Anbieter verpflichtet, die in Abs. 4 gelisteten Anlassdaten für die Zukunft – vorbehaltlich einer Verlängerung des Beschlusses – für maximal sechs Monate zu speichern und herauszugeben (Bst. a). Zudem sind die Anbieter nach Bst. b auch verpflichtet, soweit Daten nach Abs. 4 für die Vergangenheit aufgrund anderer Zwecke vorhanden sind, diese aufgrund eines gerichtlichen Beschlusses nach § 102a StPO zu sichern und herauszugeben. Aufgrund anderer Zwecke können solche Daten beispielsweise für Rechnungszwecke vorhanden sein.

Im Rahmen der Datenschutzgesetzgebung können personenbezogene Daten gespeichert werden, sofern ein geschäftsmässiger Zweck die Verarbeitung notwendig macht (Zweckbindungsgrundsatz, d.h. nur sofern ein festgelegter, eindeutiger und legitimer Zweck vorliegt). Als Beispiel kann hierfür der Call Detail Record genannt werden, welcher Informationen/Daten beinhaltet, die für das Abrechnungssystem im Telekommunikationsbereich benötigt werden. Die Verpflichtung zur Löschung von personenbezogenen Daten, bspw. den Call Detail Record Daten, besteht dann, wenn der geschäftsmässige Zweck entfällt. Berücksichtigt man ein monatliches Abrechnungssystem, eine Frist zur Beanstandung oder Rückfragen dazu sowie eine Zeitspanne für die Bearbeitung / Beantwortung diesbezüglich seitens Anbieter, kann eine Speicherdauer von rund drei Monaten als zweckmässig erachtet werden. Ein entsprechender Hinweis auf die Datenverarbeitung einschliesslich der Speicherdauer ist selbstredend von den Verantwortlichen in die Informationen gemäss Art. 13 DSGVO aufzunehmen.

Abs. 2 regelt die Löschfristen der Anlassdaten und **Abs. 3** hält fest, dass lediglich Metadaten von den Anlassdaten mitumfasst sind und keine Daten, die Aufschlüsse über den Inhalt der Kommunikation geben. Die Auflistung der Daten, die unter die Anlassdaten fallen können, wurde von der Verordnungsstufe (bis anhin Art. 54a Abs. 1 VKND) unverändert (abgesehen von kleinen redaktionellen Anpassungen) auf Gesetzesebene gehoben (**Abs. 4**).

Mit dieser Anpassung wird die vom EuGH in seinem Urteil vom 20. September 2022 in den verbundenen Rechtssachen C-793/19 und C-794/19 in Rn. 75 Ziff. 4 als grundrechtskonformer Ansatz genannte Vorgabe für eine Anlassdatenspeicherung umgesetzt.

Zu Art. 67a

Bisher war die Speicherung von IP-Adressen mit der Vorratsdatenspeicherung gekoppelt. Aufgrund der Aufhebung der Vorratsdatenspeicherung ist neu eine separate gesetzliche Regelung für die Speicherung von IP-Adressen notwendig.

In **Abs. 1** wird die Speicherung festgelegt. Diensteanbieter haben die IP-Adressen für die Dauer von sechs Monaten (bisheriger Zeitraum der Vorratsdaten-speicherung) zum Zweck der Erfüllung der gesetzlichen Aufgaben der Strafverfolgungsbehörden, insbesondere der Aufklärung eines Verbrechens oder eines Vergehens, zu speichern. Aus Sicht der Strafverfolgungsbehörden wird die Dauer aufgrund der Praxiserfahrung in den meisten Fällen als ausreichend betrachtet.

In **Abs. 2** wird die Auskunft von IP-Adressen festgelegt. Die Diensteanbieter haben diese Daten den Strafverfolgungsbehörden über deren schriftliches Ersuchen unverzüglich bekannt zu geben. Da es sich bei diesen Daten – lediglich Name und Adresse - um die am wenigsten sensiblen Daten im Bereich der elektronischen Kommunikation handelt, wäre es aus Gründen der Verfahrensökonomie unverhältnismässig, entsprechende Auskünfte generell dem Richtervorbehalt zu unterstellen. Bei einer Abfrage nach IP-Adressen ist diese jeweils bei den Strafverfolgungsbehörden bekannt und durch eine Abfrage wird diese über die gespeicherten Daten beim Anbieter einer Person und deren Adresse zugeordnet.

Ein Nachforschen der Online-Aktivitäten der Teilnehmenden ist über die Abfrage der IP-Adressen weder möglich noch zulässig. Der EuGH führt insbesondere die Möglichkeit des Nachforschens der Online-Aktivitäten einer teilnehmenden Person als Begründung auf, dass es sich um einen schweren Eingriff handelt, weshalb die IP-Adressenabfrage lediglich für die Bekämpfung schwerer Kriminalität vorzusehen ist. Art. 67a i.V.m. Art. 67b der Gesetzesvorlage ergeben keine Grundlage zur umfassenden Nachverfolgung der Online-Aktivität eines

Nutzers. Aufgrund dieser nationalen Einschränkung der Abfrage wie auch des Umfangs der Auskunft bezüglich IP-Adressen ist kein Ausspähen des Surfverhaltens möglich wie auch zulässig. Daher handelt es sich nicht mehr um einen schweren Eingriff, sondern um das Pendant zur Abfrage der Daten zur Identität der Teilnehmenden (Art. 67b). Das Kriterium der Bekämpfung schwerer Kriminalität kann daher entfallen. Da dies somit keinen schweren Eingriff darstellt, ist auf einen Richtervorbehalt zu verzichten.

In **Abs. 3** wird die Speicherfrist von gespeicherten IP-Adressen erläutert. Grundsätzlich müssen IP-Adressen von den Diensteanbietern 14 Tage nach Ablauf der Speicherungsdauer von sechs Monaten gelöscht werden. Es gibt jedoch zwei Ausnahmen dieses Grundsatzes:

- erstens kann es sein, dass ein Diensteanbieter die IP-Adressen aus z.B. vertraglichen Gründen länger als die Frist gemäss Abs. 1 aufbewahren muss. In diesem Fall darf der Diensteanbieter von der Löschfrist von 14 Tagen abweichen;
- zweitens sind IP-Adressen auch Bestandteil der Anlassdaten (Art. 67). Gibt es also eine Anordnung nach § 102a StPO und folglich eine Speicherung von verschiedenen Daten zu einem Kunden, dürfen die IP-Adressen nicht gemäss dem Grundsatz gelöscht werden. Die Löschung richtet sich dann nach der Löschung der Anlassdaten in Art. 67 Abs. 2.

Mit dieser Anpassung wird die vom EuGH in seinem Urteil vom 20. September 2022 in den verbundenen Rechtssachen C-793/19 und C-794/19 in Rn. 75 Ziff. 2 als grundrechtskonformer Ansatz genannte Vorgabe für eine Speicherung von IP-Adressen umgesetzt.

Zu Art. 67b

Da, wie bereits in den Erläuterungen zu Art. 66 Abs. 2 ausgeführt wurde, eine systematische Trennung der Pflicht zur Verifizierung von Teilnehmerdaten bei Vertragsabschluss sowie deren Aufbewahrung und der Pflicht zur Bekanntgabe der Daten zur Identifikation der Teilnehmenden vorzunehmen ist, wird die Pflicht zur Bekanntgabe von Daten zur Identifikation von Teilnehmenden neu in Art. 67b geregelt. Die Pflicht zur Bekanntgabe beschränkt sich neu lediglich auf die Daten, die zur Identifikation der Teilnehmenden notwendig sind und nicht mehr auf alle Teilnehmerdaten. Zudem hat die Pflicht zur Bekanntgabe der Daten zur Identifikation der Teilnehmenden gegenüber den Strafverfolgungsbehörden auf deren schriftliches Ersuchen zu erfolgen. Da die Bekanntgabe der Daten ausschliesslich zur Identifikation der Teilnehmenden gegenüber den Strafverfolgungsbehörden auf deren schriftlichen Antrag keinen schweren Eingriff darstellt, ist auf einen Richtervorbehalt zu verzichten.

Mit dieser Anpassung wird die vom EuGH in seinem Urteil vom 20. September 2022 in den verbundenen Rechtssachen C-793/19 und C-794/19 in Rn. 75 Ziff. 3 als grundrechtskonformer Ansatz genannte Vorgabe für eine Speicherung von Daten zur Identifikation von Teilnehmenden umgesetzt.

Zu Art. 67c

Art. 67c vereint die Grundsätze zu den Art. 67, 67a und 67b betreffend die Art der Speicherung der Daten (in einer Weise, dass diese unverzüglich den Strafverfolgungsbehörden bekannt gegeben werden können) und die Verwendungsbeschränkung (Verwendung nur für die gesetzlich vorgeschriebenen Zwecke). Diese Grundsätze waren seit Einführung der Vorratsdatenspeicherung normiert und finden auch unter dem System der Anlassdatenspeicherung sowie in Bezug auf die Speicherung und Auskunft von IP-Adressen und Daten zur Identifikation von Teilnehmenden analog Anwendung.

Zudem hält Art. 67c fest, dass aus der Sicherung, Speicherung oder Bekanntgabe kein Anspruch auf Entschädigung besteht. Diese Neuerung wiederspiegelt grundsätzlich die in den letzten Jahren vorherrschende Praxis, nach welcher keine Entschädigungen für Datenabfragen durch die Strafverfolgungsbehörden im Rahmen der Vorratsdatenspeicherung gesprochen wurden.

Zu Art. 68 Abs. 1 bis 5

Diese Bestimmung entspricht, mit wenigen begrifflichen und redaktionellen Anpassungen, grundsätzlich dem bisherigen Art. 68. So wurde der Artikel an die neuen gesetzlichen Speicher- und Herausgabepflichten angepasst. Die Abs. 3 und 4 regelten eine Zertifizierungspflicht der Anbieter wie auch eine diesbezügliche Informationspflicht gegenüber der Datenschutzstelle. Da es in Liechtenstein nach wie vor keine Möglichkeit zur Zertifizierung gibt, werden diese Bestimmungen ersatzlos gestrichen.

Zu Art. 68a

Mit dieser Bestimmung wurde die Regelung aus 54b VKND auf Gesetzesebene gehoben und auf die neuen Speicher- und Herausgabeverpflichtungen für Anbieter entsprechend angepasst. So gilt neu eine Dokumentationspflicht in Bezug auf Anlassdaten, Herausgabe von IP-Daten, Daten zur Identifikation der Teilnehmenden anstelle der bisherigen Vorratsdaten.

Zu Art. 91 Abs. 1 Bst. u, v, v^{bis} und v^{ter}

In Art. 91 Abs. 1 **Bst. u** erfolgt eine Anpassung betreffend den Verweis auf die bei sonstiger Strafe einzuhaltende Bestimmung von «Art. 66 Abs. 1 oder 2» auf «Art. 66 Abs. 1». Diese Anpassung ergibt sich aus der Aufhebung des Art. 66 Abs. 2 im gegenständlichen Entwurf (siehe Erläuterungen zu Art. 66 oben).

In Art. 91 Abs. 1 **Bst. v** erfolgt einerseits eine begriffliche Anpassung von «Vorratsdaten» auf «Anlassdaten», welche der Aufhebung der Vorratsdatenspei-

cherung und der Einführung der Anlassdatenspeicherung geschuldet ist. Die Strafbarkeit nach dieser Bestimmung umfasst neu nur noch das nicht rechtzeitige Löschen und das zweckwidrige Verwenden von Anlassdaten. Der Tatbestand des nicht Speicherns entfällt bzw. ist neu Gegenstand der Strafnorm in § 102a Abs. 3 StPO-Entwurf, wo das nicht Speichern, Sichern und Herausgeben mit Strafe bewehrt ist. Es wird auf die weitergehenden Erläuterungen zu jener Bestimmung verwiesen.

Im neu eingeführten Art. 91 Abs. 1 **Bst. v^{bis}** werden Verfehlungen rund um die mit Art. 67a Entwurf KomG neu eingeführte Verpflichtung zur Speicherung von IP-Adressen und deren Bekanntgabe an die Strafverfolgungsbehörden mit Strafe bewehrt. Strafbar macht sich, wer entgegen der Verpflichtung keine Speicherung von IP-Adressen vornimmt oder diese nicht auf Ersuchen bekannt gibt. Strafbar ist weiterhin eine verspätete Löschung als auch eine zweckwidrige Verwendung jener Daten.

Im neu eingeführten Art. 91 Abs. 1 **Bst. v^{ter}** werden Verfehlungen rund um die mit Art. 67b Entwurf KomG neu eingeführte Verpflichtung zur Bekanntgabe von Daten zur Identifikation von Teilnehmenden an die Strafverfolgungsbehörden mit Strafe bewehrt. Strafbar ist, wer seine Verpflichtung zur Bekanntgabe verletzt.

Soweit Anpassungen an die bereits unter Art. 91 Abs. 1 normierten Strafen in Bst. u und Bst. v erfolgen, erscheint eine Änderung des Strafmasses nach Abs. 1 Einleitungssatz bzw. eine anderweitige Einordnung – z.B. in Abs. 3 – nicht angezeigt. Aufgrund des Zusammenhangs der neuen Strafbestimmungen in Bst. v^{bis} und Bst. v^{ter} im Rahmen der Einführung einer Anlassdatenspeicherung erscheint ein identisches Strafmass und Einordnung wie bei den in Bst. u und Bst. v vorgesehenen Strafen gerechtfertigt.

4.2 Abänderung der StPO

Zu Art. 102a Abs. 1 und 3

Der geltende § 102a StPO regelt die Verwertung von Anlassdaten durch die Strafverfolgungsbehörde. Die Gerichte können zur Aufklärung einer abschliessenden Liste von Verbrechen und Vergehen durch Beschluss Diensteanbieter zur Herausgabe von Anlassdaten verpflichten (Abs. 1). Die Bestimmung enthält weiterhin Regelungen darüber, wem solche Beschlüsse, wann und in welchem Umfang zuzustellen sind sowie betreffend die Geheimhaltung der damit verbundenen Tatsachen und Vorgänge (Abs. 2) und legt schliesslich eine Strafe bei Verweigerung der mit Beschluss angeordneten Herausgabe fest (Abs. 3).

Die Ablösung der Vorratsdatenspeicherung durch eine Anlassdatenspeicherung macht bei dieser Bestimmung Anpassungen in Abs. 1 und 3 notwendig.

Mit dem Wegfall der anlasslosen Vorratsdatenspeicherung entfällt neu in **Abs. 1** auch die abschliessende Liste von Verbrechen und Vergehen. Eine Anlassdatenspeicherung kann daher inskünftig durch das Gericht für Verbrechen und Vergehen im Sinn des § 17 StGB mit Beschluss angeordnet werden, wenn die genannten Voraussetzungen gegeben sind. Dabei muss die Massnahme an sich verhältnismässig sein und der Bekämpfung schwerer Kriminalität dienen. Verbrechen (Straftaten, die mit Freiheitsstrafe von mehr als drei Jahren bedroht sind) fallen generell unter die Kategorie der schweren Kriminalität, wohingegen dies bei Vergehen im Einzelfall anhand der Verhältnismässigkeit durch das Gericht zu beurteilen ist. Dazu ist auch auf die Ausführungen zum Punkt «Wegfall des Kataloges von schweren Straftaten» im Kapitel 3 zu verweisen. Ebenfalls entfällt die Voraussetzung, dass der betroffene Teilnehmer oder der Nutzer des Anschlusses selbst dringend der Begehung einer Straftat verdächtig sein muss. Es kann daher inskünftig auch eine Anlassdatenspeicherung für andere Anschlüsse

angeordnet werden, wenn die erforderlichen Voraussetzungen, das heisst ein Anlass vorliegt, erfüllt sind. Dies erscheint im Licht der nunmehrigen Anlassbezogenheit der Datenspeicherung gerechtfertigt. Grundvoraussetzung ist stets das Vorliegen eines Anlasses als einschränkendes Erfordernis.

Wie der Name bereits andeutet, kann die Anlassdatenspeicherung – anders als die anlasslose Vorratsdatenspeicherung – nur noch im Fall eines konkreten Anlasses angeordnet werden. Ein Anlass ist gegeben, wenn bestimmte Anhaltspunkte vorliegen, welche die Annahme zulassen, dass durch die Anordnung einer Anlassdatenspeicherung – bzw. die daraus gewonnen Daten – eine Straftat aufgeklärt werden kann. Die Begrifflichkeit der bestimmten Anhaltspunkte wurde nach dem Vorbild des § 1 Abs. 3 i.V.m. § 135 Abs. 2b öStPO übernommen, so dass zur Auslegung auf die österreichische Literatur und Rechtsprechung zurückgegriffen werden kann: «Ein Anfangsverdacht liegt vor, wenn aufgrund bestimmter Anhaltspunkte angenommen werden kann, dass eine Straftat begangen worden ist (Abs 3). Dieser Anfangsverdacht darf nur aufgrund konkreter Anhaltspunkte angenommen werden. Allein Vermutungen, lediglich vage Hinweise oder Spekulationen (auf blosse Annahmen oder Mutmassungen beruhende Erwartungen) genügen nicht, aus den Umständen muss sich aber noch keine genaue Tatkonkretisierung ergeben.

Bestimmte Anhaltspunkte setzen voraus, dass zumindest nach der sich bietenden Sachlage die Annahme einer verfolgbaren Tat indiziert ist. Es muss im Gesamtbild aller Faktoren nach kriminalistischer Erfahrung als möglich erscheinen, dass eine verfolgbare Straftat vorliegt.» (Markel in Fuchs/Ratz, WK StPO § 1 RN 26 (Stand 01.09.2015, rdb.at)). Als bestimmt werden Anhaltspunkte somit nur dann gelten können, wenn sich in Betrachtung des Gesamtbildes klar ergibt, dass durch die Verwendung von Anlassdaten eine bessere Aufklärung erwartet werden kann. Sind solche Indizien bzw. Anhaltspunkte gegeben, so muss die Anordnung der

Anlassdatenspeicherung weiterhin für die Aufklärung erforderlich und auch verhältnismässig sein wie auch der Bekämpfung schwerer Kriminalität dienen. Die Anordnung einer Anlassdatenspeicherung ist damit auf das absolut Notwendige begrenzt.

Da bei der neu eingeführten Anlassdatenspeicherung nicht nur die Herausgabe von Daten an die Strafverfolgungsbehörden, sondern zunächst auch deren Speicherung bzw. Sicherung mit gerichtlichem Beschluss angeordnet wird, ist die in **Abs. 3** vorgesehene Strafnorm entsprechend anzupassen. Im Entwurf werden daher – ausgehend von der bisherigen Strafbarkeit der Verweigerung der Herausgabe – neu auch die Verweigerung der Speicherung und die Verweigerung der Sicherung unter Strafe gestellt. Die Ausnahmen von der Strafbarkeit, die Strafe (Beugestrafe) und das Strafmass bleiben unverändert. Für weitere Strafen betreffend Verfehlungen im Zusammenhang mit einer Anlassdatenspeicherung, welche nicht im Zusammenhang mit einem Beschluss des Landgerichts stehen, sei auf die Anpassungen in Art. 91 des Entwurfs zum Kommunikationsgesetz verwiesen.

5. VERFASSUNGSMÄSSIGKEIT / RECHTLICHES

Die geltenden Bestimmungen und die Praxis zur Speicherung und Verwertung von Anlassdaten, IP-Adressen und Daten zur Identifikation von Teilnehmenden waren bislang noch nicht Gegenstand einer Normenkontrolle durch den Staatsgerichtshof. Vor diesem Hintergrund wurde die gegenständliche Gesetzesrevision weitgehend an den Implikationen der einschlägigen Rechtsprechung des EuGH (insb. Urteil vom 20. September 2022 in den verbundenen Rechtssachen C-793/19 und C-794/19) sowie der Datenschutzgrundverordnung ausgerichtet.

Aufgrund der Ausrichtung der gegenständlichen Gesetzesvorlagen an den vom EuGH vorgegebenen Einschränkungen (vgl. Rn. 75 des Urteils vom 20. September 2022) kann davon ausgegangen werden, dass die EWR-rechtlichen und verfassungsrechtlichen Vorgaben erfüllt werden.

6. AUSWIRKUNGEN AUF DIE NACHHALTIGE ENTWICKLUNG

Die vorgeschlagenen Gesetzesanpassungen dienen der Unterstützung des UNO-Nachhaltigkeitszieles 16 «Frieden, Gerechtigkeit und starke Institutionen», insbesondere alle Formen der Gewalt verringern sowie leistungsfähige, rechenschaftspflichtige und transparente Institutionen auf allen Ebenen aufbauen. Negative Auswirkungen auf andere SDGs sind nicht ersichtlich.

7. REGIERUNGSVORLAGEN

7.1 Gesetz über die elektronische Kommunikation

Gesetz

vom …

über die Abänderung des Kommunikationsgesetzes

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I.

Abänderung bisherigen Rechts

Das Gesetz vom 5. April 2023 über die elektronische Kommunikation (Kommunikationsgesetz; KomG), LGBl. 2023 Nr. 216, in der geltenden Fassung, wird wie folgt abgeändert:

Art. 3 Abs. 1 Ziff. 49 und 49a

1) Im Sinne dieses Gesetzes gelten als:

49. «Anlassdaten»: die in Art. 67 Abs. 4 genannten Verkehrs-, Standort- und Teilnehmerdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs erzeugt oder verarbeitet werden, einschliesslich der Daten erfolgloser

Anrufversuche, soweit diese Daten anlässlich der Erbringung von Telefondiensten gespeichert oder anlässlich der Erbringung von Internetdiensten protokolliert werden.

49a. "IP-Adressen": eine IP-Adresse (Internetprotokoll-Adresse) ist eine individuelle Adresse (normierte Zeichenfolge), über die jedes Gerät in einem Netzwerk eindeutig identifiziert werden kann.

Art. 66 Abs. 2 und 3

Verifizierung und Speicherung von Teilnehmerdaten

2) Aufgehoben

3) Die Regierung regelt das Nähere über die Speicherung von Teilnehmerdaten mit Verordnung.

Art. 67

Anlassdatenspeicherung

1) Diensteanbieter haben Anlassdaten über gerichtlichen Beschluss zum Zwecke der Aufklärung eines Verbrechens oder eines Vergehens nach § 102a StPO

a) für einen Zeitraum von maximal sechs Monaten ab Beschlussfassung zu speichern und herauszugeben;

b) soweit vorhanden für die Vergangenheit zu sichern und herauszugeben.

2) Anlassdaten sind vorbehaltlich einer Verlängerung des Beschlusses nach § 102a StPO nach Ablauf der im ursprünglichen Beschluss festgelegten Frist binnen 14 Tagen zu löschen, soweit sie nicht auf vertraglicher oder anderer Grundlage weiterverarbeitet werden müssen.

3) Die Sicherung und Speicherung nach Abs. 1 durch einen Anbieter darf keinerlei Daten umfassen, welche Aufschluss über den Inhalt einer Kommunikation geben.

4) Die Anlassdaten umfassen:

a) zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk:

aa) die Rufnummer des anrufenden Anschlusses;

bb) der Name und die Anschrift des Teilnehmers oder registrierten Benutzers;

2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:

aa) die zugewiesene(n) Benutzerkennung(en);

bb) die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden;

cc) der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine Internetprotokoll-Adresse (IP-Adresse), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war;

b) zur Identifizierung des Adressaten einer Nachricht benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk:

aa) die angewählte(n) Nummer(n) (die Rufnummer(n) des angerufenen Anschlusses) und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird;

bb) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer;

2. betreffend Internet-E-Mail und Internet-Telefonie:

aa) die Benutzerkennung oder Rufnummer des vorgesehenen Empfängers eines Anrufs mittels Internet-Telefonie;

bb) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer und die Benutzerkennung des vorgesehenen Empfängers einer Nachricht;

c) zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk: Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs;

2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:

aa) Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers;

bb) Datum und Uhrzeit der An- und Abmeldung beim Internet-E-Mail-Dienst oder Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone;

d) zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk: der in Anspruch genommene Telefondienst;

2. betreffend Internet-E-Mail und Internet-Telefonie: der in Anspruch genommene Internetdienst;

e) zur Bestimmung der Kommunikationsendeinrichtung oder der vorgeblichen Kommunikationsendeinrichtung von Benutzern benötigte Daten:

1. betreffend Telefonfestnetz: die Rufnummern des anrufenden und des angerufenen Anschlusses;

2. betreffend Mobilfunk:

aa) die Rufnummern des anrufenden und des angerufenen Anschlusses;

bb) die internationale Mobilteilnehmerkennung (IMSI - International Mobile Subscriber Identity) des anrufenden Anschlusses;

cc) die internationale Mobilfunkgerätekennung (IMEI - International Mobile Equipment Identity) des anrufenden Anschlusses;

dd) die IMSI des angerufenen Anschlusses;

ee) die IMEI des angerufenen Anschlusses;

ff) im Falle vorbezahlter anonymer Dienste: Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID oder Geolokation), an dem der Dienst aktiviert wurde;

3. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:

aa) die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;

bb) der digitale Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs;

f) zur Bestimmung des Standorts mobiler Geräte benötigte Daten:

1. die Standortkennung (Cell-ID oder Geolokation) während des Zeitraums, in dem die Speicherung der Kommunikationsdaten erfolgt;
2. Daten zur geografischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell-ID oder Geolokation) während des Zeitraums, in dem die Speicherung der Kommunikationsdaten erfolgt.

Art. 67a

Speicherung von und Auskunft über IP-Adressen

1) Diensteanbieter haben IP-Adressen, soweit diese im Zuge der Bereitstellung des Kommunikationsdienstes für jeden Teilnehmer erzeugt oder verarbeitet werden, für die Dauer von sechs Monaten ab Beendigung der aktiven Nutzung zum Zwecke der Erfüllung der gesetzlichen Aufgaben der Strafverfolgungsbehörden, insbesondere der Aufklärung eines Verbrechens oder eines Vergehens, zu speichern.

2) Diensteanbieter haben nach Abs. 1 gespeicherte Daten den Strafverfolgungsbehörden über deren schriftliches Ersuchen unverzüglich bekannt zu geben.

3) Die IP-Adressen sind, vorbehaltlich einer Massnahme nach § 102a StPO, nach Ablauf der Frist nach Abs. 1 binnen 14 Tagen zu löschen, soweit sie nicht auf vertraglicher oder anderer Grundlage weiterverarbeitet werden müssen. Besteht eine Massnahme nach § 102a StPO richtet sich die Löschung nach Art. 67 Abs. 2.

Art. 67b

Auskunft zur Identifikation von Teilnehmern

Diensteanbieter haben die nach Art. 66 gespeicherten Daten zur Identifikation von Teilnehmern den Strafverfolgungsbehörden zum Zwecke der Erfüllung deren gesetzlichen Aufgaben, insbesondere der Aufklärung eines Verbrechens oder eines Vergehens, über deren schriftliches Ersuchen unverzüglich bekannt zu geben.

Art. 67c

Bekanntgabe, Verwendungsbeschränkung und Entschädigungsansprüche

Daten nach Art. 67, 67a und 67b sind so zu sichern oder speichern, dass sie unverzüglich an die Strafverfolgungsbehörden bekannt gegeben werden können. Sie dürfen nur für die gesetzlich vorgeschriebenen Zwecke verwendet werden. Aus ihrer Sicherung, Speicherung oder Bekanntgabe entsteht kein Anspruch auf Entschädigung.

Art. 68 Abs. 1 bis 5

1) Diensteanbieter haben sicherzustellen, dass Daten nach Art. 67, 67a und 67b in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschliesslich des Schutzes vor unrechtmässiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch technische und organisatorische Massnahmen. Solche Massnahmen umfassen insbesondere:

a) den Einsatz eines besonders sicheren Verschlüsselungsverfahrens;

b) die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen;

c) die Speicherung unter Berücksichtigung des erhöhten Schutzbedarfs und des Standes der Technik vor dem Zugriff aus dem Internet;

d) die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf Personen, die durch den Anbieter besonders ermächtigt sind;

e) die Speicherung im Inland, in einem anderen EWR-Mitgliedstaat oder der Schweiz; und

f) die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten, die dazu durch den Anbieter besonders ermächtigt worden sind.

2) Diensteanbieter haben sicherzustellen, dass für Zwecke der Datenschutzkontrolle jede Verarbeitung von Daten nach Art. 67, 67a und 67b protokolliert wird. Die Protokolldaten sind der Datenschutzstelle auf Ersuchen unverzüglich mitzuteilen. Protokolldaten dürfen ausschliesslich für die Zwecke der Kontrolle des Datenschutzes durch die Datenschutzstelle und zur Gewährleistung der Datensicherheit verwendet werden. Für andere Zwecke dürfen die Protokolldaten nicht verwendet werden. Die Protokolldaten sind nach einem Jahr binnen sieben Tagen zu löschen. Zu protokollieren sind:

a) der Zeitpunkt der Datenverarbeitung;

b) die die Daten verarbeitenden Personen; und

c) Zweck und Art der Datenverarbeitung.

3) Aufgehoben

4) Aufgehoben

5) Die Datenschutzstelle kontrolliert die Anwendung der Bestimmungen betreffend Datenschutz und Datensicherheit in Bezug auf Daten, die nach Art. 67, 67a und 67b verarbeitet werden.

Art. 68a

Überwachung durch die Datenschutzstelle

1) Die Datenschutzstelle ist zuständig für die Überwachung der Einhaltung der Grundsätze der Datensicherheit, die Erstellung einer Statistik über die Speicherung von Anlassdaten sowie die jährliche Berichterstattung an den Landtag.

2) Diensteanbieter nach Art. 67, 67a und 67b sind verpflichtet, der Datenschutzstelle die Auskünfte zu erteilen, die für die Erfüllung ihrer Aufgaben, insbesondere der jährlichen Berichterstattung, notwendig sind. Dies sind insbesondere Auskünfte darüber:

a) in welchen Fällen im Einklang mit § 102a StPO Anlassdaten an die zuständigen Behörden weitergegeben worden sind;

b) in welchen Fällen im Einklang mit Art. 67a IP-Daten an die zuständigen Behörden weitergegeben worden sind;

c) in welchen Fällen im Einklang mit Art. 67b Daten zur Identifikation der Teilnehmer an die zuständigen Behörden weitergegeben worden sind;

d) in welchen Fällen die Anfragen nach Daten nach Bst. a bis c ergebnislos geblieben sind.

3) Statistiken nach Abs. 2 dürfen keine personenbezogenen Daten enthalten.

Art. 91 Abs. 1 Bst. u, v, v^{bis} und v^{ter}

2) Von der Regulierungsbehörde ist wegen Übertretung mit einer Busse bis zu 50 000 Franken zu bestrafen, wer:

u) als Diensteanbieter die Pflicht nach Art. 66 Abs. 1 verletzt;

v) Anlassdaten entgegen Art. 67 nicht rechtzeitig löscht oder zweckwidrig verwendet;

v^{bis}) IP-Daten entgegen Art. 67a nicht speichert, nicht unverzüglich auf schriftliches Ersuchen bekannt gibt, nicht rechtzeitig löscht oder zweckwidrig verwendet;

v^{ter}) als Diensteanbieter die Pflicht nach Art. 67b verletzt;

II.

Änderung von Bezeichnungen

In Art. 66 Abs. 1 ist die Bezeichnung «aufzuzeichnen» durch die Bezeichnung «zu speichern» und Art. 69 Abs. 1 ist die Bezeichnung «Vorratsdaten» durch die Bezeichnung «Anlassdaten» in der grammatikalisch richtigen Form zu ersetzen.

III.

Inkrafttreten

Dieses Gesetz tritt unter Vorbehalt des ungenutzten Ablaufs der Referendumsfrist am … (1./Monat/Jahr) in Kraft, andernfalls am Tag nach der Kundmachung.

7.2 Strafprozessordnung

Gesetz

vom …

über die Abänderung der Strafprozessordnung

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I.

Abänderung bisherigen Rechts

Die Strafprozessordnung (StPO) vom 18. Oktober 1988, LGBl. 1988 Nr. 62, in der geltenden Fassung, wird wie folgt abgeändert:

Titel vor § 102a

IVa. Anlassdatenspeicherung, Verwertung von IP-Adressen und Verkehrs-, Standort- und Teilnehmerdaten

§ 102a Abs. 1 und 3

1) Die Anordnung einer Anlassdatenspeicherung nach Art. 67 KomG ist zulässig, wenn aufgrund bestimmter Anhaltspunkte angenommen werden kann, dass sie zur Aufklärung eines Vergehens oder Verbrechens erforderlich und verhältnismässig erscheint. Die Anordnung einer Anlassdatenspeicherung in Form

einer Datenspeicherung, -sicherung oder -herausgabe erfolgt gegenüber Anbietern im Sinn des Kommunikationsgesetzes mit gerichtlichem Beschluss.

3) Wird die Durchführung einer Anlassdatenspeicherung in Form einer Datenspeicherung, -sicherung oder -herausgabe durch den Anbieter rechtswidrig verweigert, so kann der Anbieter, falls er nicht selbst der strafbaren Handlung verdächtig erscheint oder von der Verbindlichkeit zur Ablegung des Zeugnisses befreit ist, durch Verhängung einer Beugestrafe bis zu 50 000 Franken dazu angehalten werden.

II.

Inkrafttreten

Dieses Gesetz tritt gleichzeitig mit dem Gesetz vom … über die Abänderung des Kommunikationsgesetzes in Kraft.