

GESETZENTWURF

der Landesregierung

Entwurf eines Gesetzes zur Anpassung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes an verfassungsgerichtliche Vorgaben und weitere bundesrechtliche Anforderungen zur Bestandsdatenauskunft

A Problem und Ziel

Die manuelle Bestandsdatenauskunft ermöglicht es unter anderem der Polizei und auch den Verfassungsschutzbehörden in Bund und Ländern, Auskünfte von Anbietern von Telekommunikationsdiensten beispielsweise über den Inhaber eines Telefonanschlusses oder einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse zu erlangen. Mitgeteilt werden personenbezogene Daten von Kundinnen und Kunden, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen, wie Name, Anschrift, PIN oder PUK (sogenannte Bestandsdaten). Nicht mitgeteilt werden dagegen Daten, die sich auf die Nutzung von Telekommunikationsdiensten (sogenannte Verkehrsdaten) oder sogar den Inhalt von Kommunikationsvorgängen beziehen.

Zum 1. Juli 2013 wurden der Verfassungsschutzbehörde des Landes Mecklenburg-Vorpommern mit § 24b des Landesverfassungsschutzgesetzes (LVerfSchG M-V) und der Polizei mit § 28 des Sicherheits- und Ordnungsgesetzes in der vor dem 4. Juni 2020 geltenden Fassung (SOG M-V a. F.) jeweils ausdrückliche Ermächtigungsgrundlagen zur manuellen Beauskunftung von Bestandsdaten vom Landesgesetzgeber zur Verfügung gestellt. Die Schaffung ausdrücklicher Ermächtigungsgrundlagen erfolgte in Anbetracht der Entscheidung des Bundesverfassungsgerichtes (BVerfG) vom 24. Januar 2012 (1 BvR 1299/05). Das BVerfG hatte darin festgestellt, dass die Ermächtigung zur manuellen Bestandsdatenauskunft im § 113 des Telekommunikationsgesetzes (TKG) des Bundes sowie in den Fachgesetzen der Sicherheits- und Verfassungsschutzbehörden unzureichend ist und entwickelte das sog. Doppeltürmodell.

Danach stehen zwischen der auskunftersuchenden Stelle und dem auskunftserteilenden Anbieter von Telekommunikationsdiensten zwei Türen, die nur geöffnet sind, wenn sowohl eine Ermächtigungsgrundlage für das Auskunftersuchen (1. Tür) als auch für die Auskunftserteilung (2. Tür) existiert. Demnach reichte es nicht mehr aus, dass nur die Stelle, bei der die Bestandsdaten zu Telekommunikationsanschlüssen vorliegen, über eine bundesgesetzliche Befugnis zur Übermittlung an andere Stellen verfügt. Vielmehr mussten nun auf der Seite der abrufenden Stellen – wie etwa Polizei und Verfassungsschutzbehörden – ebenso (fach-)gesetzliche Grundlagen zum Abruf der Daten vorhanden sein.

Gegen die geschaffenen Ermächtigungsnormen in § 24b LVerfSchG M-V und § 28 SOG M-V a. F. wurde im Juni 2014 Verfassungsbeschwerde beim Landesverfassungsgericht Mecklenburg-Vorpommern (LVerfG) erhoben. Am 28. Januar 2016 setzte das LVerfG das unter dem Aktenzeichen LVerfG 3/14 geführte Verfahren jedoch aus, da beim BVerfG unter dem Az. 1 BvR 1873/13 ebenso eine Verfassungsbeschwerde gegen Bestandsdatenauskunftsnormen des Bundes anhängig war.

Die Ermächtigungsnorm zur manuellen Bestandsdatenauskunft für die Polizei wurde während der Aussetzung des Beschwerdeverfahrens durch den Landtagsbeschluss vom 11. März 2020 zur Neufassung des Sicherheits- und Ordnungsgesetzes (SOG M-V), die insbesondere aufgrund der Umsetzung von EU-Vorschriften zum Datenschutz erforderlich war, neu in § 33h SOG M-V verortet und geändert. Es wurden zudem Bestandsdaten nach dem Telemediengesetz in den Anwendungsbereich der Norm einbezogen. § 33h SOG M-V trat am 5. Juni 2020 in Kraft (GVOBl. M-V S. 334).

Das BVerfG hat dann mit Beschluss vom 27. Mai 2020 erneut über die Übermittlung und den Abruf von Bestandsdaten entschieden (Bestandsdatenauskunft II – 1 BvR 1873/13). Es erklärte die nach der ersten BVerfG-Entscheidung aus dem Jahr 2012 geschaffene bundesgesetzliche Übermittlungsbefugnis für Bestandsdaten in § 113 des Telekommunikationsgesetzes (TKG) und mehreren Fachgesetzen des Bundes, die den manuellen Abruf von Bestandsdaten regeln (beispielsweise Bundesverfassungsschutzgesetz oder auch das Bundespolizeigesetz) für verfassungswidrig. Das Gericht stellte fest, dass diese Vorschriften die Grundrechte auf informationelle Selbstbestimmung sowie auf Wahrung des Telekommunikationsgeheimnisses verletzen. Die für verfassungswidrig erklärten Vorschriften wurden – unter Einhaltung bestimmter Maßgaben – längstens bis zum 31. Dezember 2021 für weiter anwendbar erklärt.

Zugleich hat das BVerfG festgestellt, dass die Erteilung einer Auskunft über Bestandsdaten aber grundsätzlich verfassungsrechtlich zulässig ist. Die gesetzlichen Regelungen müssen aber von Verfassungs wegen bestimmte Grundsätze beachten; dies sind mit Blick auf die Befugnisnormen in den Bereichen Verfassungsschutz und Gefahrenabwehr insbesondere folgende:

- Nach dem Doppeltürmodell bedarf es sowohl für die Übermittlung der Bestandsdaten durch die Telekommunikationsanbieter (1. Tür) als auch für den Abruf dieser Daten durch die Behörden (2. Tür) jeweils verhältnismäßiger Rechtsgrundlagen, wobei die Übermittlungs- und auch die Abrufregelungen die Verwendungszwecke der Daten hinreichend begrenzen müssen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen.

- Trotz des nicht besonders intensiven Eingriffsgewichtes bedürfen die allgemeinen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten für die Gefahrenabwehr und für die Tätigkeit der Nachrichtendienste grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr.
- Findet eine Zuordnung dynamischer IP-Adressen statt, muss diese im Hinblick auf ihr erhöhtes Eingriffsgewicht darüber hinaus auch dem Schutz oder der Bewehrung von Rechtsgütern von zumindest hervorgehobenem Gewicht dienen.
- Bleiben die Eingriffsschwellen im Bereich der Gefahrenabwehr oder der nachrichtendienstlichen Tätigkeit hinter dem Erfordernis einer konkreten Gefahr zurück, müssen im Gegenzug erhöhte Anforderungen an das Gewicht der zu schützenden Rechtsgüter vorgesehen werden.

Aufgrund dieser BVerfG-Entscheidung hat der Bundesgesetzgeber mit dem „Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichtes vom 27. Mai 2020“ die Bestandsdatenübermittlungsnorm in § 113 TKG a. F. als auch seine bundesgesetzlichen Fachnormen für den Abruf von Bestandsdaten angepasst. Dieses Gesetz ist am 2. April 2021 in Kraft getreten (BGBl. I 2021, S. 448).

Unter wesentlicher Bezugnahme auf diese BVerfG-Entscheidung nahm das LVerfG das oben angeführte Beschwerdeverfahren LVerfG 3/14 wieder auf und stellte mit Beschluss vom 28. Oktober 2021 fest, dass die Bestandsdatenauskunftsnormen § 24b Absatz 1 Satz 1 und Absatz 2 LVerfSchG M-V und § 33h Absatz 1 Satz 1 und Absatz 2 SOG M-V mit Artikel 6, Artikel 5 Abs. 3 der Verfassung des Landes Mecklenburg-Vorpommern i. V. m. Artikel 2 Absatz 1 i. V. m. Artikel 1 und Artikel 10 des Grundgesetzes unvereinbar sind. Das LVerfG hat mit der festgestellten Unvereinbarkeit zugleich eine Übergangsregelung hinsichtlich der Fortgeltung beider Normen getroffen. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Oktober 2022, sind diese unter Beachtung bestimmter Maßgaben weiter anwendbar.

Aus den vorgenannten Gründen bedarf es einer Neufassung des § 24b LVerfSchG M-V und des § 33h SOG M-V, damit der Verfassungsschutzbehörde und auch der Polizei im Land Mecklenburg-Vorpommern die Befugnisse zur manuellen Beauskunftung von Bestandsdaten auch nach Ablauf der Übergangsfrist weiterhin zur Verfügung stehen.

Im Zuge der Neufassung des § 24b LVerfSchG M-V und des § 33h SOG M-V sind zudem folgende inzwischen in Kraft getretene bundesgesetzliche Änderungen zu beachten:

Mit dem „Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz)“ ist am 1. Dezember 2021 unter anderem eine Neufassung des TKG in Kraft getreten (BGBl. I S. 1858). Die Regelung zum manuellen Auskunftsverfahren ist nicht mehr in § 113 TKG enthalten, sondern unter Anpassungen in § 174 TKG verortet worden. § 174 TKG bildet mit Blick auf das Doppeltürmodell als Bestandsdatenübermittlungsbefugnis nun die „1. Tür“, deren Vorgaben von den Ländern bei der Normierung ihrer fachgesetzlichen Normen für Bestandsdatenabrufe, also der „2. Tür“, zu beachten sind.

Der Bundesgesetzgeber hat darüber hinaus ein neues „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“ (Telekommunikation-Telemedien-Datenschutz-Gesetz – TTDSG) geschaffen. Es trat – abgesehen von geregelten Ausnahmen – am 1. Dezember 2021 in Kraft (BGBl. I S. 1982 und auch BGBl. I S. 3544 zu den Änderungen durch Gesetz vom 12. August 2021). In § 2 TTDSG sind beispielsweise neue Begriffsbestimmungen zu Bestands- und Nutzungsdaten enthalten, und die §§ 22 bis 24 TTDSG regeln nun die Beauskunftung von Bestandsdaten und Nutzungsdaten für die Anbietenden von Telemedien. Die bisher geltenden Bestands- und Nutzungsdatenregelungen in den §§ 14 und 15 des Telemediengesetzes sind entfallen.

Insoweit sind die im LVerfSchG M-V und auch im SOG M-V enthaltenen Bezugnahmen auf den § 113 TKG und die Regelungen im Telemediengesetz zu Bestands- und Nutzungsdaten nicht mehr zutreffend. Es bedarf damit weiterer Änderungen in den §§ 24a, 24b LVerfSchG M-V und in den §§ 33d bis 33h SOG M-V.

Zudem sind aufgrund der vorgenommenen Änderungen Folgeänderungen bezüglich der Benachrichtigungspflichten in § 46a SOG M-V erforderlich. Ferner bedarf es weiterer begrifflicher Anpassungen beziehungsweise Präzisierungen in den §§ 46d, 46f, 46g und 48h SOG M-V.

Im Übrigen sind die im LVerfSchG M-V und im SOG M-V enthaltenen Ressortbezeichnungen zu aktualisieren.

B Lösung

Unter Beachtung der vorgenannten bundes- und landesverfassungsgerichtlichen Vorgaben erfolgt eine Änderung der landesgesetzlichen Normen zur Bestandsdatenauskunft. Angemerkt sei an dieser Stelle, dass sich für die laufende Legislaturperiode eine umfassende Novelle des Landesverfassungsschutzgesetzes in Vorbereitung befindet, die einen allgemeinen datenschutzrechtlichen Anpassungsbedarf aufgreifen sowie insbesondere notwendige Änderungen, die sich aus dem aktuellen Urteil des Bundesverfassungsgerichtes vom 26. April 2022 (Aktenzeichen 1 BvR 1619/17) zum Bayerischen Verfassungsschutzgesetz ergeben, vornehmen wird.

Mit Artikel 1 wird die Ermächtigungsnorm für die Verfassungsschutzbehörde in § 24b LVerfSchG M-V neu gefasst. Zudem sind aufgrund der in Kraft getretenen bundesgesetzlichen Änderungen zur Beauskunftung von Bestandsdaten im manuellen Auskunftsverfahren im § 174 TKG und zur Beauskunftung von Bestands- und Nutzungsdaten im Telemedienbereich nach den §§ 21 bis 24 TTDSG ebenso Änderungen in den §§ 24a, 24b LVerfSchG M-V erforderlich.

Mit Artikel 2 wird auch die polizeiliche Ermächtigungsnorm zur Bestandsdatenauskunft in § 33h SOG M-V neugefasst. Durch die vorgenannten in Kraft getretenen bundesgesetzlichen Änderungen werden weitere notwendige Anpassungen in folgenden SOG-Regelungen vorgenommen:

- Einsatz technischer Mittel zur Überwachung der Telekommunikation (§ 33d),
- Auskunft über Nutzungsdaten (§ 33e),
- Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten (§ 33f),

- Unterbrechung oder Verhinderung der Telekommunikation (§ 33g),
- § 46a (Benachrichtigungspflichten bei verdeckten und eingriffsintensiven Maßnahmen),
- § 46d (Dokumentationspflichten).

Es erfolgen zudem begriffliche Anpassungen beziehungsweise Präzisierungen in den §§ 46f, 46g und 48h SOG M-V.

Die Änderungen im SOG M-V betreffen die Polizei; die Ordnungsbehörden sind lediglich durch die Klarstellung in der Dokumentationsregelung in § 46d mitbetroffen.

Im Übrigen werden die im LVerfSchG M-V und im SOG M-V enthaltenen Ressortbezeichnungen aktualisiert.

C Alternativen

Ohne die vorgesehenen Änderungen im LVerfSchG M-V und im SOG M-V stünden der Verfassungsschutzbehörde und der Polizei des Landes Mecklenburg-Vorpommern die Befugnisse zur manuellen Bestandsdatenauskunft wegen des vom LVerfG festgelegten Auslaufens der Übergangsregelung am 31. Oktober 2022 nicht mehr zur Verfügung. Durch den Wegfall dieser Befugnisse würde dann auch dem erklärten Ziel, gerade durch gemeinsame gesetzliche Befugnisse im Recht des Bundes und der Länder eine effektive Erhöhung der Sicherheit in der Bundesrepublik Deutschland zu erreichen, nicht mehr gefolgt werden.

Zudem würde durch die Nichtaktualisierung der in beiden Landesgesetzen enthaltenen Bezugnahmen auf die im Telekommunikations- und Telemedienbereich einschlägigen Bundesnormen zur Datenübermittlung an Verfassungsschutzbehörden und Polizeien der Länder ein nicht mehr aktueller Gesetzgebungsstand fortbestehen. Damit würde dem vom BVerfG entwickelten sogenannten Doppeltürmodell (siehe Ausführungen unter A.) unzureichend nachgekommen.

D Notwendigkeit (§ 3 Absatz 1 Satz 1 GGO II)

Die Neufassung des § 24b LVerfSchG M-V (Artikel 1) und des § 33h SOG M-V (Artikel 2) ist aufgrund der bundes- und landesverfassungsgerichtlichen Vorgaben erforderlich, um die Befugnisse zum Erlangen von manuellen Bestandsdatenauskünften für die Verfassungsschutzbehörde und die Polizei des Landes Mecklenburg-Vorpommern auch nach Auslaufen der Übergangsfrist am 31. Oktober 2022 zu erhalten.

Das Einholen von Datenauskünften von Dritten ist mit Eingriffen in die Grundrechte der hiervon betroffenen Personen verbunden. Dies setzt nach dem Grundsatz vom Vorbehalt des Gesetzes das Vorliegen entsprechender gesetzlicher Ermächtigungen für die Verfassungsschutzbehörde und die Polizei in Mecklenburg-Vorpommern voraus. Diesem Grundsatz wird durch die in den Artikeln 1 und 2 vorgesehenen Gesetzesänderungen Rechnung getragen.

Die beabsichtigten Änderungen in den §§ 24a, 24b LVerfSchG M-V und in den §§ 33d bis 33h und in § 46a SOG M-V sind zudem mit Blick auf die bundesgesetzlichen Änderungen im TKG und das neu geschaffene TTDSG (siehe im Einzelnen Ausführungen unter Buchstabe A) geboten, um den nicht mehr zutreffenden Regelungs- und Verweisungsstand zu beseitigen. Die Änderung in § 46d dient zudem der weiteren Umsetzung der Vorgaben in der Entscheidung LVerfG 3/14. Die Änderungen in den §§ 46f, 46g und 48h SOG M-V erfolgen zudem zur Anpassung an Begrifflichkeiten des TKG und des TTDSG sowie zur Präzisierung.

E Finanzielle Auswirkungen auf die Haushalte des Landes und der Kommunen

1. Haushaltsausgaben ohne Vollzugaufwand

Durch die mit diesem Gesetzentwurf vorgesehenen Änderungen entstehen keine weiteren Kosten, da die Anpassungen zu bereits schon bestehenden Eingriffsnormen erfolgen.

Der Aufwand zur manuellen Beauskunftung von Bestandsdaten wird wie bisher den Verpflichteten für durch sie erteilte Auskünfte entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes (JVEG) entschädigt. Die Ausgaben hierfür hängen davon ab, wie viele praktische Anwendungsfälle im Land Mecklenburg-Vorpommern zu verzeichnen sein werden. Somit können die Mittelbedarfe nicht verlässlich beziffert werden.

Die vorstehenden Ausführungen gelten für die Beauskunftung von Nutzungsdaten durch Anbieter von Telemedien entsprechend.

2. Vollzugaufwand

Die Maßnahmen auf der Grundlage der in beiden Landesgesetzen vorgesehenen Datenbeauskunftungsbefugnisse werden auch weiterhin durch das vorhandene Personal getroffen.

Es werden – ausschließlich mit Blick auf Artikel 2 (Änderung des SOG M-V) – zusätzliche nicht konkret bezifferbare personelle Ressourcen gebunden, die jedoch auf die Umsetzung der verfassungsrechtlichen Vorgaben und auf die notwendigen Anpassungen aufgrund der neu geordneten Übermittlungsbefugnisse im Bundesrecht (TKG und TTDSG) zurückzuführen sind. Durch die Einführung des bundesgesetzlich im § 23 TTDSG geforderten Richtervorbehaltes bei der Beauskunftung von Bestandsdaten bei Anbietern von Telemedien wie Passwörtern und anderen Zugangsdaten (siehe § 33h Absatz 4 SOG M-V) könnte ein personeller Mehraufwand durch notwendige Anordnungen in den Amtsgerichten Schwerin, Rostock und Neubrandenburg aber auch in der Polizei durch entsprechende Antragstellungen und das Einholen nachträglicher richterlicher Entscheidungen entstehen. Inwieweit und wie oft diese Auskunftsbefugnisse, zur Gefahrenabwehr in Anspruch genommen werden müssen und dann einen personellen Aufwand auslösen, ist nicht abzusehen. Mit Blick auf die gesetzlich geforderten hohen Voraussetzungen für die Nutzung dieser Befugnis, wird sie nur im Einzelfall zur Anwendung gelangen. Generell gilt, dass der Bedarf personeller Ressourcen durch Organisationsmaßnahmen im Rahmen der vereinbarten Stellenpläne und Personalentwicklungsplanungen kompensiert wird, sodass keine Stellenmehrbedarfe entstehen. Finanzielle Bedarfe werden grundsätzlich im Rahmen bereits veranschlagter Mittel sowie der mittelfristigen Finanzplanung abgedeckt.

F Sonstige Kosten (zum Beispiel Kosten für die Wirtschaft, Kosten für soziale Sicherungssysteme)

Auch mit der Änderung der Vorschriften zur Beauskunftung von Bestandsdaten und Nutzungsdaten bleibt es bei der bestehenden Verpflichtung zur Entschädigung der zur Auskunft Verpflichteten entsprechend § 23 JVEG. Es entsteht gegenüber den bisherigen gesetzlichen Regelungslagen kein zusätzlicher Erfüllungsaufwand.

G Bürokratiekosten

Durch das Gesetz werden keine Informationspflichten für Unternehmen eingeführt.

**DIE MINISTERPRÄSIDENTIN
DES LANDES
MECKLENBURG-VORPOMMERN**

Schwerin, den 14. Juni 2022

An die
Präsidentin des Landtages
Mecklenburg-Vorpommern
Frau Birgit Hesse
Lennéstraße 1

19053 Schwerin

Betr.: Entwurf eines Gesetzes zur Anpassung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes an verfassungsgerichtliche Vorgaben und weitere bundesrechtliche Anforderungen zur Bestandsdatenauskunft

Sehr geehrte Frau Präsidentin,

als Anlage übersende ich Ihnen den von der Landesregierung am 14. Juni 2022 beschlossenen Entwurf des vorbezeichneten Gesetzes mit Begründung.

Ich bitte Sie, die Beschlussfassung des Landtages herbeizuführen.

Federführend ist das Ministerium für Inneres, Bau und Digitalisierung.

Mit freundlichen Grüßen

Manuela Schwesig

ENTWURF

eines Gesetzes zur Anpassung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes an verfassungsgerichtliche Vorgaben und weitere bundesrechtliche Anforderungen zur Bestandsdatenauskunft

Der Landtag hat das folgende Gesetz beschlossen:

Artikel 1 Änderung des Landesverfassungsschutzgesetzes

Das Landesverfassungsschutzgesetz vom 11. Juli 2001 (GVOBl. M-V S. 261), das zuletzt durch das Gesetz vom 13. Januar 2017 (GVOBl. M-V S. 2) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 24b wie folgt gefasst:

„§ 24b Auskunftsverlangen zu Bestandsdaten“.

2. In § 2 Absatz 1 Satz 2 wird das Wort „Innenministerium“ durch die Wörter „Ministerium für Inneres, Bau und Digitalisierung“ ersetzt.

3. In § 10a Absatz 3 Satz 6 werden die Wörter „Inneres und Sport“ durch die Wörter „Inneres, Bau und Digitalisierung“ ersetzt.

4. § 24a wird wie folgt geändert:

a) Absatz 1 wird aufgehoben.

b) Der Absatz 2 wird Absatz 1 und in Satz 1 werden nach den Wörtern „soweit dies“ die Wörter „im Einzelfall“ eingefügt und in Nummer 4 wird die Angabe „§ 96 Abs. 1 Nr. 1 bis 4 sowie § 113a des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198) geändert worden ist,“ durch die Angabe „§ 9 Absatz 1 Satz 1 Nummer 1 bis 4 des Telekommunikation-Telemedien-Datenschutz-Gesetzes“ ersetzt.

c) Die Absätze 3 bis 8 werden die Absätze 2 bis 7 und in ihnen werden jeweils die Angabe „Absatz 2“ durch die Angabe „Absatz 1“ und die Angabe „Absatzes 2“ durch die Angabe „Absatzes 1“ ersetzt.

d) Der Absatz 9 wird Absatz 8 und in ihm werden die Angabe „Absatzes 2“ durch die Angabe „Absatzes 1“ und die Wörter „Absätze 3 bis 5“ durch die Wörter „Absätze 2 bis 4“ ersetzt.

5. § 24b wird wie folgt gefasst:

**„§ 24b
Auskunftsverlangen zu Bestandsdaten**

(1) Soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach § 5 Absatz 1 erforderlich ist, darf die Verfassungsschutzbehörde unter Angabe dieser Vorschrift im Einzelfall Auskunft verlangen von demjenigen, der geschäftsmäßig

1. Telekommunikationsdienste erbringt oder daran mitwirkt, über Bestandsdaten nach § 3 Nummer 6 und § 172 des Telekommunikationsgesetzes,
2. Telemediendienste erbringt oder daran mitwirkt, über Bestandsdaten nach § 2 Absatz 2 Nummer 2 des Telekommunikation-Telemedien-Datenschutz-Gesetzes.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden. Die Rechtsgrundlage und die tatsächlichen Anhaltspunkte, die das Auskunftsverlangen veranlassen, sind aktenkundig zu machen.

(3) Die Auskunft zu Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf nur im Falle des Absatzes 1 Nummer 1 und nur dann verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten im Einzelfall vorliegen. Für diese Auskunftsverlangen gilt § 24a Absatz 3 Satz 2 und 4 sowie Absatz 4 entsprechend.

(4) Von einer Auskunftserteilung nach Absatz 2 und 3 ist die betroffene Person zu benachrichtigen. Die Benachrichtigung erfolgt, sobald und soweit eine Gefährdung des Zwecks der Auskunft und der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes ausgeschlossen werden können. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(5) Der aufgrund eines Auskunftsverlangens Verpflichtete hat die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln.

(6) Die Verfassungsschutzbehörde hat für ihr erteilte Auskünfte eine Entschädigung zu gewähren, deren Umfang sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes bemisst. Die Vorschriften über die Verjährung in § 2 Absatz 1 und Absatz 4 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechend Anwendung.

(7) Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird nach Maßgabe des Absatzes 2 Satz 1 eingeschränkt.“

6. § 29 wird wie folgt geändert:

- a) In Absatz 1 Satz 1 und Absatz 2 Satz 1 wird jeweils das Wort „Innenministerium“ durch die Wörter „Ministerium für Inneres, Bau und Digitalisierung“ ersetzt.
- b) In Absatz 3 Satz 1 wird das Wort „Innenministeriums“ durch die Wörter „Ministeriums für Inneres, Bau und Digitalisierung“ ersetzt.
- c) In Absatz 4 Satz 2 wird das Wort „Innenministerium“ durch die Wörter „Ministerium für Inneres, Bau und Digitalisierung“ ersetzt.

Artikel 2 **Änderung des Sicherheits- und Ordnungsgesetzes**

Das Sicherheits- und Ordnungsgesetz vom 27. April 2020 (GVOBl. M-V S. 334), das durch Artikel 2 des Gesetzes vom 17. April 2021 (GVOBl. M-V S. 370, 372) geändert worden ist, wird wie folgt geändert:

1. § 33d wird wie folgt geändert:

- a) In Absatz 1 Satz 1 Nummer 5 werden die Wörter „oder Gesundheit gefährdet ist“ durch die Wörter „gefährdet ist oder denen eine nicht nur geringfügige Gesundheitsbeeinträchtigung droht“ ersetzt.
- b) Absatz 2 wird wie folgt geändert:
 - aa) Satz 1 wird wie folgt gefasst:

„Eine Datenerhebung nach Absatz 1 kann sich auf

 - a) die Inhalte und Umstände der Telekommunikation sowie
 - b) Verkehrs- und Standortdaten im Sinne des § 9 des Telekommunikation-Telemedien-Datenschutz-Gesetzes beziehen.“
 - bb) Folgender Satz 4 wird angefügt:

„Datenerhebungen nach Satz 1 und 2 sind auf den jeweils im Einzelfall erforderlichen Umfang zu begrenzen.“
- c) Absatz 7 wird wie folgt gefasst:

„(7) Aufgrund der Anordnung hat jeder Anbieter von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes der Polizei nach Maßgabe des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung die Maßnahmen unverzüglich zu ermöglichen und die erforderlichen Auskünfte unverzüglich und vollständig zu erteilen. Die in Anspruch genommenen Anbieter werden entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes entschädigt.“

2. § 33e wird wie folgt gefasst:

**„§ 33e
Auskunft über Nutzungsdaten**

(1) Die Polizei kann im Einzelfall von demjenigen, der geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, Auskunft über Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes verlangen (§ 24 Absatz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes), soweit die in die Auskunft aufzunehmenden Daten im Einzelfall

1. zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit zum Schutz von Leib, Leben oder Freiheit einer Person oder solcher Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, oder
 2. zur Verhütung einer Straftat nach § 67c, soweit die Voraussetzungen nach § 67a Absatz 1 Nummer 1 vorliegen,
- erforderlich sind.

(2) Für die Anordnung der Maßnahme gilt § 33d Absatz 4 bis 6 entsprechend mit der Maßgabe, dass an die Stelle der Rufnummer (§ 33d Absatz 5 Nummer 2 und Absatz 6 Satz 1 Nummer 2) soweit möglich eine eindeutige Kennung des Nutzerkontos der betroffenen Person, ansonsten eine möglichst genaue Bezeichnung des Telemediendienstes tritt, auf den sich das Auskunftsverlangen bezieht. In der Anordnung ist die für das Auskunftsverlangen im Einzelfall zutreffende Nummer des Absatzes 1 anzugeben.

(3) Aufgrund der Anordnung hat derjenige, der geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, der Polizei unverzüglich und vollständig die zu beauskunftenden Nutzungsdaten auf dem von ihr bestimmten Weg zu übermitteln. § 33d Absatz 7 Satz 2 gilt entsprechend.“

3. In § 33f Absatz 3 wird das Wort „Diensteanbieter“ durch die Wörter „Anbieter von Telekommunikationsdiensten“ ersetzt.

4. Dem § 33g wird folgender Absatz 6 angefügt:

„(6) Die Polizei kann aufgrund der Anordnung nach Absatz 1 oder 2 auch von Anbietern von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes verlangen, dass diese die Unterbrechung und Verhinderung von Telekommunikationsverbindungen vornehmen, soweit das Telekommunikationsgesetz oder hierzu erlassene Bestimmungen dem Verlangen nicht entgegenstehen. Für eine Entschädigung der Anbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden, soweit nicht eine Entschädigung nach dem Telekommunikationsgesetz zu gewähren ist.“

5. § 33h wird wie folgt gefasst:

**„§ 33h
Auskunft über Bestandsdaten**

(1) Die Polizei kann im Einzelfall unter Angabe dieser Vorschrift von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die von ihm erhobenen Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 des Telekommunikationsgesetzes erhobenen Daten verlangen (§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes), soweit die in die Auskunft aufzunehmenden Daten im Einzelfall zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit erforderlich sind. Bezieht sich das Auskunftsverlangen auf Daten mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 174 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur unter den Voraussetzungen des Satzes 1 und nur dann verlangt werden, wenn im Einzelfall auch die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft über Daten nach Absatz 1 kann im Einzelfall unter Angabe dieser Vorschrift auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 174 Absatz 1 Satz 3 des Telekommunikationsgesetzes), soweit die in die Auskunft aufzunehmenden Daten im Einzelfall zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit zum Schutz von Leib, Leben oder Freiheit einer Person oder solcher Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, erforderlich sind.

(3) Die Polizei kann im Einzelfall unter Angabe dieser Vorschrift von demjenigen, der geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, Auskunft über Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Telemedien-Datenschutz-Gesetzes verlangen (§ 22 Absatz 1 Satz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes), soweit die in die Auskunft aufzunehmenden Daten im Einzelfall zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit erforderlich sind.

(4) Bezieht sich das Auskunftsverlangen nach Absatz 3 auf als Bestandsdaten erhobene Passwörter oder auf andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 23 Absatz 1 Satz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes), darf diese Auskunft nur dann verlangt werden, wenn diese

1. im Einzelfall zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit zum Schutz von Leib, Leben oder Freiheit einer Person oder solcher Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, erforderlich ist,

und wenn darüber hinaus

2. im Einzelfall die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

Auskunftsverlangen nach Satz 1 bedürfen der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde; Antrag und Anordnung haben die Angabe dieser Vorschrift sowie die für das Auskunftsverlangen erforderlichen Angaben unter entsprechender Anwendung des § 33d Absatz 5 und 6 zu enthalten. Die in Satz 1 genannten Daten dürfen nicht an andere Stellen übermittelt werden.

(5) Die Auskunft über Daten nach Absatz 3 und 4 kann im Einzelfall unter Angabe dieser Vorschrift auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 22 Absatz 1 Satz 3 und 4 des Telekommunikation-Telemedien-Datenschutz-Gesetzes), soweit die in die Auskunft aufzunehmenden Daten im Einzelfall zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit zum Schutz von Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, erforderlich ist.

(6) Aufgrund eines Auskunftsverlangens haben die in Absatz 1 und 3 genannten Anbieter die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. § 33d Absatz 7 Satz 2 gilt entsprechend.“

6. In § 46a Absatz 1 Satz 1 Nummer 4 werden die Wörter „nach § 33d oder Inanspruchnahme von Diensteanbietern nach den §§ 33e bis 33g und § 33h Absatz 1 Satz 2 und Absatz 2“ durch die Wörter „oder Inanspruchnahmen der Anbieter von Telekommunikationsdiensten oder Telemedien nach den §§ 33d bis 33g und § 33h Absatz 1 Satz 2, Absatz 2, Absatz 4 und 5“ ersetzt.
7. In § 46d Absatz 1 Satz 1 Nummer 1 werden nach dem Wort „Sachverhalt“ die Wörter „einschließlich des Vorliegens der Erhebungsvoraussetzungen“ eingefügt.
8. In § 46f Absatz 2 Nummer 5 werden die Wörter „nach § 33d oder Inanspruchnahme von Diensteanbietern nach den §§ 33e bis 33g“ durch die Wörter „oder Inanspruchnahmen der Anbieter von Telekommunikationsdiensten oder Telemedien nach den §§ 33d bis 33g und § 33h Absatz 1 Satz 2, Absatz 2, Absatz 4 und 5“ ersetzt.
9. § 46g Absatz 1 Satz 1 Nummer 8 wird wie folgt gefasst:
 - „8. falls zutreffend die Angaben, ob sie beim Anbieter von Telekommunikationsdiensten oder Telemedien erhoben wurden und um welche konkrete Datenart es sich handelt; im Fall des § 33d auch die Angabe, auf welcher konkreten Rechtsgrundlage des Telekommunikationsgesetzes der Anbieter die Daten gespeichert hat.“.

10. § 48h wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In dem Satzteil vor Nummer 1 werden die Wörter „Ministerium für Inneres und Europa“ durch die Wörter „Ministerium für Inneres, Bau und Digitalisierung“ ersetzt.

bb) In Satz 1 Nummer 4 werden nach dem Wort „Telekommunikationsbereich“ die Wörter „oder Inanspruchnahmen der Anbieter von Telekommunikationsdiensten oder Telemedien“ eingefügt.

cc) In Satz 4 wird das Wort „Justizministerium“ durch die Wörter „Ministerium für Justiz, Gleichstellung und Verbraucherschutz“ ersetzt.

b) In Absatz 4 werden die Wörter „Ministerium für Inneres und Europa und das Justizministerium“ durch die Wörter „Ministerium für Inneres, Bau und Digitalisierung und das Ministerium für Justiz, Gleichstellung und Verbraucherschutz“ ersetzt.

c) In Absatz 5 werden die Wörter „Ministerium für Inneres und Europa“ durch die Wörter „Ministerium für Inneres, Bau und Digitalisierung“ ersetzt.

11. Es werden ersetzt:

a) in § 4 Absatz 2 Satz 2, § 5 Absatz 4, § 11 Satz 2, § 31 Absatz 4, § 32a Absatz 6 Satz 1, § 38 Satz 3, § 42 Absatz 2 Satz 4 und Absatz 7, § 48 Absatz 5 Satz 5, § 112 und § 115 Absatz 3 Satz 3 die Wörter „Ministerium für Inneres und Europa“ jeweils durch die Wörter „Ministerium für Inneres, Bau und Digitalisierung“;

b) in § 20 Absatz 3 Satz 1 die Wörter „Ministeriums für Inneres und Europa“ durch die Wörter „Ministeriums für Inneres, Bau und Digitalisierung“ und

c) in § 52 Absatz 3 Satz 1 die Wörter „Ministerium für Soziales, Integration und Gleichstellung“ durch die Wörter „Ministerium für Justiz, Gleichstellung und Verbraucherschutz“.

Artikel 3 Einschränkung eines Grundrechts

Durch Artikel 1 und 2 wird das Recht auf Wahrung des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) eingeschränkt.

Artikel 4 Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung:

I. Allgemeines

Für die polizeiliche Gefahrenabwehr sind die Abfragen von Bestandsdaten¹ beispielsweise zur Verhinderung von angedrohten Suiziden, zum Auffinden von vermissten und hilflosen Personen oder zur Verhinderung von angedrohten Straftaten gegen Leben, Gesundheit und Freiheit (Amoklagen) von großer Bedeutung. Auch für den Verfassungsschutz sind Bestandsdaten bedeutsam. Wird im Rahmen einer vom Verfassungsschutz zu beobachtenden Szene etwa eine Mobilfunknummer bekannt, wird über die Bestandsdatenabfrage der Anschlussinhaber personalisiert. Dann kann der Verfassungsschutz mittels der ihm zur Verfügung stehenden Befugnisse in der Folge feststellen, ob die Person einer zu beobachtenden Szene zuzuordnen ist.

Das Bundesverfassungsgericht (BVerfG) hatte mit Beschluss vom 24. Januar 2012 (1 BvR 1299/05) eine Verfassungsbeschwerde gegen die gesetzlichen Bestimmungen des Telekommunikationsgesetzes (TKG) zur Speicherung bestimmter Bestandsdaten nach § 111 TKG (a. F.) sowie zur Verwendung dieser Daten im Wege des automatisierten nach § 112 TKG (a. F.) oder manuellen Auskunftsverfahrens nach § 113 TKG (a. F.) im Wesentlichen zurückgewiesen. Es beurteilte die Erhebung und Speicherung von Telekommunikationsdaten (§ 111 TKG a. F.) sowie deren Verwendung im automatisierten Auskunftsverfahren (§ 112 TKG a. F.) ohne Einschränkung als verfassungsgemäß. Hingegen genügten die Regelungen zum manuellen Auskunftsverfahren (§ 113 TKG a. F.), so das BVerfG, nicht in Gänze den verfassungsrechtlichen Anforderungen, sodass es bis zum 30. Juni 2013 Nachbesserungen verlangte. Das Gericht stellte fest, dass

- der Gesetzgeber nach dem vom BVerfG entwickelten sog. Doppeltürmodell im manuellen Auskunftsverfahren (§§ 113 Abs. 1, 111, 95 Abs. 1 TKG a. F.) sowohl belastbare Rechtsgrundlagen für die Übermittlung von Bestandsdaten durch die Telekommunikationsdiensteanbieter (§ 113 TKG a. F., Norm für die Datenübermittlung = 1. Tür) an die Sicherheitsbehörden für deren repressive, präventive und nachrichtendienstliche Aufgabenerledigung als auch für den Abruf dieser Daten durch die Sicherheitsbehörden bei den Diensteanbietern schaffen muss (Normen für den Datenabruf = 2. Tür). Für den Abruf der Daten bei den Telekommunikationsdiensteanbietern bedarf es qualifizierter Rechtsgrundlagen in den jeweiligen Fachgesetzen (wie Polizeigesetze oder Verfassungsschutzgesetze des Bundes und der Länder), die selbst eine Auskunftspflicht der Telekommunikationsunternehmen normenklar begründen müssen. Allgemeine Datenerhebungsregelungen reichen dort nicht (mehr) aus.

¹ Bestandsdaten sind u.a. Name, Anschrift, Bankverbindung, Anschlussnummer (Rufnummer), Passwörter, PIN und PUK. Die Legaldefinition findet sich aktuell in dem seit 1. Dezember 2021 geltenden § 3 Nr. 6 TKG: Bestandsdaten sind „Daten eines Endnutzers, die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste“.

Zur Abgrenzung Verkehrsdaten: Dies sind u.a. die Nummer/Kennung beteiligter Anschlüsse (anrufender und angerufener Kommunikationsteilnehmer), Beginn und Ende der jeweiligen Verbindung als auch sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendige Verkehrsdaten. Die Legaldefinition findet sich aktuell in dem seit 1. Dezember 2021 geltenden § 3 Nr. 70 TKG: Verkehrsdaten sind „Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind“. Für die Erhebung von Verkehrsdaten bedarf es eigener Rechtsgrundlagen.

- die Sicherheitsbehörden Auskünfte über Zugangssicherungs-codes wie Passwörter, PIN und PUK (§ 113 Abs. 1 TKG) nur dann verlangen dürfen, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Mit anderen Worten: Für eine auf die Zugangssicherungs-codes gerichtete Abfrage (§ 113 TKG) müssen die jeweils (fach-)gesetzlichen Voraussetzungen des damit konkret angestrebten Nutzungszweckes erfüllt sein (beispielsweise für eine Telekommunikationsüberwachung oder für eine Sicherstellung).
- in der Zuordnung von Telekommunikationsnummern zu ihren Anschlussinhabern ein Eingriff in Artikel 2 Abs. 1 i. V. m. Artikel 1 Absatz 1 GG (Grundrecht auf informationelle Selbstbestimmung) liegt. In der Zuordnung von dynamischen IP-Adressen wird zudem in Artikel 10 GG (Fernmeldegeheimnis) eingegriffen. Denn für die Identifizierung einer dynamischen IP-Adresse müssen die Telekommunikationsunternehmen bestimmte Verkehrsdaten ihrer Kunden sichten und somit auf konkrete Telekommunikationsvorgänge zugreifen, die vom Schutzbereich nach Artikel 10 GG umfasst sind. Der Abruf von Bestandsdaten, der nur über die Zuordnung einer zu einem bestimmten Zeitpunkt (bekannten) dynamischen IP-Adresse möglich ist, bedarf daher einer ausdrücklichen gesetzlichen Regelung. Das Zitiergebot gemäß Artikel 19 Abs. 1 Satz 2 GG ist bei der Normierung von Eingriffen in das Fernmeldegeheimnis zu beachten.

Unter Beachtung dieser BVerfG-Entscheidung wurden der Verfassungsschutzbehörde des Landes Mecklenburg-Vorpommern in § 24b des Landesverfassungsschutzgesetzes (LVerfSchG M-V) und auch der Polizei in § 28 des Sicherheits- und Ordnungsgesetzes in der bis zum 4. Juni 2020 gelten Fassung (SOG M-V a. F.) jeweils ausdrückliche Ermächtigungsgrundlagen zur manuellen Beauskunftung von Bestandsdaten zur Verfügung gestellt; sie traten am 1. Juli 2013 in Kraft.

Gegen diese geschaffenen Ermächtigungsnormen wurde im Juni 2014 Verfassungsbeschwerde beim Landesverfassungsgericht Mecklenburg-Vorpommern (LVerfG) erhoben. Am 28. Januar 2016 setzte das LVerfG das unter dem Aktenzeichen LVerfG 3/14 geführte Verfahren jedoch aus, da beim BVerfG unter dem Aktenzeichen 1 BvR 1873/13 ebenso eine Verfassungsbeschwerde gegen Bestandsdatenauskunftsnormen des Bundes anhängig war.

Die Ermächtigungsnorm zur manuellen Bestandsdatenauskunft für die Polizei wurde während der Aussetzung des Beschwerdeverfahrens durch den Beschluss des Landtages Mecklenburg-Vorpommern vom 11. März 2020 zur Neufassung des Sicherheits- und Ordnungsgesetzes (SOG M-V), die insbesondere aufgrund der Umsetzung von EU-Vorschriften zum Datenschutz erforderlich war, neu in § 33h SOG M-V verortet und geändert. Es wurden Bestandsdaten nach dem Telemediengesetz in den Anwendungsbereich der Norm einbezogen. § 33h SOG M-V trat am 5. Juni 2020 in Kraft (GVObI. M-V S. 334).

Das BVerfG hat dann mit Beschluss vom 27. Mai 2020 erneut über die Übermittlung und den Abruf von Bestandsdaten entschieden (Bestandsdatenauskunft II – 1 BvR 1873/13). Es erklärte die nach der ersten BVerfG-Entscheidung aus dem Jahr 2012 geschaffene bundesgesetzliche Übermittlungsbefugnis für Bestandsdaten in § 113 des Telekommunikationsgesetzes (TKG) und mehreren Fachgesetzen des Bundes, die den manuellen Abruf von Bestandsdaten regeln (beispielsweise das Bundesverfassungsschutzgesetz oder auch das Bundespolizeigesetz) für verfassungswidrig. Das Gericht stellte fest, dass diese Vorschriften die Grundrechte auf informationelle Selbstbestimmung sowie auf Wahrung des Telekommunikationsgeheimnisses verletzen.

Die für verfassungswidrig erklärten Vorschriften wurden – unter Einhaltung bestimmter Maßgaben – längstens bis zum 31. Dezember 2021 für weiter anwendbar erklärt.

Zugleich hat das BVerfG festgestellt, dass die Erteilung einer Auskunft über Bestandsdaten grundsätzlich verfassungsrechtlich zulässig ist. Die gesetzlichen Regelungen müssen aber von Verfassungen wegen bestimmte Grundsätze beachten; dies sind mit Blick auf die Befugnisnormen in den Bereichen Verfassungsschutz und Gefahrenabwehr insbesondere folgende:

- Nach dem Doppeltürmodell bedarf es sowohl für die Übermittlung der Bestandsdaten durch die Telekommunikationsanbieter (1. Tür) als auch für den Abruf dieser Daten durch die Behörden (2. Tür) jeweils verhältnismäßiger Rechtsgrundlagen, wobei die Übermittlungs- und auch die Abrufregelungen die Verwendungszwecke der Daten hinreichend begrenzen müssen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen.
- Trotz des nicht besonders intensiven Eingriffsgewichtes bedürfen die allgemeinen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten für die Gefahrenabwehr und für die Tätigkeit der Nachrichtendienste grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr.
- Findet eine Zuordnung dynamischer IP-Adressen statt, muss diese im Hinblick auf ihr erhöhtes Eingriffsgewicht darüber hinaus auch dem Schutz oder der Bewehrung von Rechtsgütern von zumindest hervorgehobenem Gewicht dienen.
- Bleiben die Eingriffsschwellen im Bereich der Gefahrenabwehr oder der nachrichtendienstlichen Tätigkeit hinter dem Erfordernis einer konkreten Gefahr zurück, müssen im Gegenzug erhöhte Anforderungen an das Gewicht der zu schützenden Rechtsgüter vorgesehen werden.

Aufgrund dieser BVerfG-Entscheidung hat der Bundesgesetzgeber mit dem „Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichtes vom 27. Mai 2020“ die Bestandsdatenübermittlungsnorm in § 113 TKG als auch seine bundesgesetzlichen Fachnormen für den Abruf von Bestandsdaten angepasst. Dieses Gesetz ist am 2. April 2021 in Kraft getreten (BGBl. I 2021, S. 448).

Unter wesentlicher Bezugnahme auf die BVerfG-Entscheidung vom 27. Mai 2020 nahm das LVerfG das oben angeführte Beschwerdeverfahren LVerfG 3/14 wieder auf. Es stellte sodann mit Beschluss vom 28. Oktober 2021 fest, dass die Bestandsdatenauskunftsnormen § 24b Absatz 1 Satz 1 und Absatz 2 LVerfSchG M-V und § 33h Absatz 1 Satz 1 und Absatz 2 SOG M-V mit Artikel 6, Artikel 5 Absatz 3 der Landesverfassung i. V. m. Artikel 2 Absatz 1 i. V. m. Artikel 1 und Artikel 10 des Grundgesetzes unvereinbar sind.

Das LVerfG hat mit der festgestellten Unvereinbarkeit aber zugleich eine Übergangsregelung hinsichtlich der Fortgeltung beider Normen getroffen. Die Normen sind bis zu einer Neuregelung, längstens jedoch bis zum 31. Oktober 2022, unter Beachtung bestimmter Maßgaben weiter anwendbar.

Diese Maßgaben sind die folgenden (vergleiche LVerfG 3/14 Randnummern 92 ff.):

- „1. Die zum allgemeinen Abruf von Bestandsdaten ermächtigenden § 24b Abs. 1 Satz 1 LVerfSchG M-V und § 33h Abs. 1 Satz 1 SOG M-V können weiter angewendet werden, wenn eine Auskunft bezogen auf die Gefahrenabwehr zur Abwehr einer konkreten Gefahr im Sinne der polizeilichen Generalklausel (§§ 13, 16 SOG M-V) erforderlich oder bezogen auf den Nachrichtendienst zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist (vgl. BVerfGE 155, 119 Rn. 269).*
- 2. Die zum Abruf von Bestandsdaten anhand einer dynamischen IP-Adresse ermächtigenden § 24b Abs. 2 LVerfSchG M-V und § 33h Abs. 2 SOG M-V dürfen weiter angewendet werden, wenn über die zuvor unter 1. formulierte Maßgaben hinaus die Auskunft zur Abwehr einer Gefahr für Rechtsgüter von hervorgehobenem Gewicht oder zur Verfolgung von Straftaten oder zumindest besonders gewichtigen Ordnungswidrigkeiten erfolgt (vgl. BVerfGE 155, 119 Rn. 272).“*

Damit der Verfassungsschutzbehörde und auch der Polizei im Land Mecklenburg-Vorpommern die Befugnisse zur manuellen Beauskunftung von Bestandsdaten auch nach Ablauf der Übergangsfrist weiterhin zur Verfügung stehen, bedarf es nunmehr einer Neufassung des § 24b LVerfSchG M-V und des § 33h SOG M-V, die den vom LVerfG festgestellten Anforderungen allgemein in Randnummer 61 sowie zur allgemeinen Bestandsdatenauskunft in den Randnummern 62 bis 66 und zum Datenabruf anhand einer dynamischen IP-Adresse in den Randnummern 70 bis 74 Rechnung trägt.

Nicht erforderlich ist insoweit, dass die Umsetzung inhaltlich vollends den vom LVerfG für die Übergangszeit aufgestellten Maßgaben entspricht. Der Gesetzgeber hat einen Gestaltungsspielraum, solange er die verfassungsgerichtlich festgestellten Grenzen einhält. Abstand genommen wird insoweit von der durch das LVerfG zwar übergangsweise ermöglichten, aber nicht für verpflichtend befundenen Anwendung der oben genannten Landesnormen zum Zweck der Verfolgung von Straftaten oder zumindest besonders gewichtigen Ordnungswidrigkeiten. Insbesondere wird das SOG M-V nicht um entsprechende Regelungen ergänzt. Denn der Bundesgesetzgeber hat bereits die Bestandsdatenauskunft im Bereich der Strafverfolgung mit der Schaffung des § 100j StPO umfassend geregelt. Er hat damit von seinem Recht der Festlegung von Vorgaben zur Strafverfolgung und zu den insoweit zur Verfügung stehenden Instrumenten Gebrauch gemacht.

Im Zuge der Neufassung des § 24b LVerfSchG M-V und des § 33h SOG M-V sind über die vom LVerfG festgestellten verpflichtenden Anforderung hinaus zudem folgende inzwischen in Kraft getretene bundesgesetzliche Änderungen zu beachten:

- Mit dem „Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz)“ ist am 1. Dezember 2021 unter anderem eine Neufassung des TKG in Kraft getreten (BGBl. I S. 1858). Die Regelung zum manuellen Auskunftsverfahren ist nicht mehr in § 113 TKG enthalten, sondern unter Anpassungen in § 174 TKG verortet worden. § 174 TKG bildet mit Blick auf das Doppeltürmodell als Bestandsdatenübermittlungsbefugnis nun die „1. Tür“, deren Vorgaben von den Ländern bei der Normierung ihrer fachgesetzlichen Normen für Bestandsdatenabrufe, also der „2. Tür“, zu beachten sind.
- Der Bundesgesetzgeber hat darüber hinaus ein neues „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“ (Telekommunikation-Telemedien-Datenschutz-Gesetz - TTDSG) geschaffen. Es trat – abgesehen von geregelten Ausnahmen – am 1. Dezember 2021 in Kraft (BGBl. I S. 1982 und auch BGBl. I S. 3544 zu den Änderungen durch Gesetz vom 12. August 2021). In § 2 TTDSG sind beispielsweise neue Begriffsbestimmungen zu Bestands- und Nutzungsdaten enthalten und die §§ 22 bis 24 TTDSG regeln die Auskunftsverfahren von Bestandsdaten und Nutzungsdaten für die Anbieter von Telemedien. Die bisher geltenden Bestands- und Nutzungsdatenregelungen in den §§ 14 und 15 des Telemediengesetzes sind entfallen.

Insoweit sind die im LVerfSchG M-V und auch im SOG M-V enthaltenen Bezugnahmen auf den § 113 TKG und die Regelungen im Telemediengesetz zu Bestands- und Nutzungsdaten nicht mehr zutreffend. Demzufolge bedarf es auch Änderungen in den §§ 24a, 24b LVerfSchG M-V und in den §§ 33d bis 33h SOG M-V.

Zudem sind aufgrund der vorgenommenen Änderungen Folgeänderungen in § 46a SOG M-V erforderlich. Ferner erfolgt eine weitere Präzisierung der Dokumentationsregelung in § 46d Absatz 1 Nummer 1 SOG M-V. In den §§ 46d, 46f, 46g und 48h SOG M-V bedarf es darüber hinaus weiterer begrifflicher Anpassungen beziehungsweise Präzisierungen.

Im Übrigen sind die im LVerfSchG M-V und im SOG M-V enthaltenen Ressortbezeichnungen zu aktualisieren.

II. Zu den einzelnen Bestimmungen:

Zu Artikel 1 – Änderung des LVerfSchG M-V

Zu Nummer 1 (Inhaltsverzeichnis LVerfSchG M-V)

Die Änderung der Inhaltsübersicht ist aufgrund der Neuregelungen in § 24b erforderlich.

Zu Nummer 2 (betrifft § 2 LVerfSchG M-V)

Zu Nummer 3 (betrifft § 10a LVerfSchG M-V)

Durch die Änderungen wird die aktuelle Bezeichnung des Innenressorts in die gesetzlichen Regelungen übernommen.

Zu Nummer 4 (betrifft § 24a LVerfSchG M-V – Informationsübermittlung durch nicht öffentliche Stellen an die Verfassungsschutzbehörde)**Zu Buchstabe a**

Die Regelungen zur Bestandsdatenauskunft werden unter § 24b zusammengefasst. Demzufolge ist § 24a Absatz 1 aufzuheben.

Zu Buchstabe b

Die Änderung ist eine Folgeänderung zu Buchstabe a.

Zudem wird der Verweis im (neuen) Absatz 1 auf die Vorschriften des bisherigen TKG redaktionell angepasst. § 9 Telekommunikation-Telemedien-Datenschutz-Gesetz übernimmt die bisher in § 96 TKG enthaltene Regelung zur Verarbeitung von Verkehrsdaten. Diese neue Regelungslage entspricht somit der Regelung in § 8a Absatz 1 Satz 1 Nummer 4 des bereits angepassten Bundesverfassungsschutzgesetzes.

Ferner erfolgt im Satz 1 die zusätzliche Aufnahme der Worte „im Einzelfall“, da sowohl die allgemeine Auskunftsbefugnis als auch die konkreten Tatbestandsvoraussetzungen im Einzelfall vorliegen müssen.

Zu den Buchstaben c und d

Die Änderungen sind Folgeänderungen zu Buchstabe a.

Zu Nummer 5 (betrifft § 24b LVerfSchG M-V – Auskunftsverlangen zu Bestandsdaten)

Der bisherige § 24b muss – unter Einbeziehung des bisherigen § 24a Absatz 1 – neu gefasst werden, da das LVerfG unter Berufung auf das BVerfG fordert, dass Anlass, Zweck und Umfang des jeweiligen Eingriffs für den Datenabruf bereichsspezifisch, präzise und normenklar festzulegen sind (LVerfG 3/14, Randnummer 61).

Zu Absatz 1

Während schon die bisherige Norm eine entsprechende Auskunftserteilung im Einzelfall gestattete (LVerfG 3/14, Randnummer 64), verlangt der neu gefasste § 24b Absatz 1 darüber hinaus, dass das Auskunftsverlangen aufgrund tatsächlicher Anhaltspunkte zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach § 5 Absatz 1 erforderlich sein muss.

Indem die Auskunft nunmehr nur noch bei tatsächlichen Anhaltspunkten und zudem nur noch zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten zur Verfügung steht, wird die Vorgabe zur Schaffung einer konkreten begrenzenden Eingriffsschwelle umgesetzt (LVerfG 3/14, Randnummern 61 und 65). Ferner wird die Eingriffsbefugnis durch die Verweisung auf § 5 Absatz 1 auf den Schutz der dort genannten Rechtsgüter von hervorgehobenem Gewicht begrenzt.

Während im Hinblick auf die ergangene Rechtsprechung der Verfassungsgerichte im neuen § 24b Absatz 1 die nötige Anpassung der manuellen Bestandsdatenauskunft von Telekommunikationsunternehmen vorgesehen ist (Absatz 1 Nummer 1), werden darüber hinaus Telemediendienste wertungskonsistent einbezogen (Absatz 1 Nummer 2). Der vom BVerfG als Qualifikationselement der Eingriffsgewichtung angesehene Umstand, dass Telekommunikationsbestandsdaten flächendeckend vorrätig gehalten werden (siehe oben genannte BVerfG-Entscheidung vom 27. Mai 2021, Randnummer 139), trifft zwar nicht gleichermaßen auf Telemedienbestandsdaten zu.

Gleichwohl hat die Regelung durch die verbundene Auskunftspflicht vergleichbares Gewicht, sodass eine einheitliche Regelung angemessen ist, wie sie hier aufgenommen wird.

Zudem wird ausdrücklich normiert, dass die Auskunft nur im Einzelfall unter Angabe der gesetzlichen Vorschrift verlangt werden darf. Die zweimalige Nennung des Einzelfalles erfolgt auch hier aufgrund der Notwendigkeit, dass sowohl die allgemeine Auskunftserteilung als auch die konkreten Tatbestandsvoraussetzungen im Einzelfall vorliegen müssen.

Zu Absatz 2

Absatz 2 Satz 1 übernimmt die bisherige Regelung zur Auskunft anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse. Eine gegenüber der allgemeinen Bestandsdatenabfrage nach Absatz 1 erhöhte Eingriffsschwelle ist insoweit nicht geboten (LVerfG 3/14, Randnummer 71) und der verfassungsgerichtlich geforderte hinreichend gewichtige Rechtsgüterschutz ist auch hier gewährleistet.

Einer weiteren Forderung der Verfassungsgerichte nachkommend werden mit Absatz 2 Satz 2 der den Abruf veranlassenden Behörde Dokumentationspflichten auferlegt. Die Dokumentation dient insbesondere der etwaigen Zurückstellung der Benachrichtigung der betroffenen Person nach Absatz 4, sodass nach gebotener Zeit das Fortbestehen der Voraussetzungen überprüft werden kann.

Zu Absatz 3

Absatz 3 Satz 1 übernimmt die im bisherigen Absatz 1 Satz 2 enthaltene Regelung zu Zugangssicherungsinformationen (PIN/PUK).

Weiterhin wird mit Absatz 3 Satz 2 aufgrund der damit normierten entsprechenden Anwendbarkeit des § 24a Absatz 3 Satz 2 und 4 sowie Absatz 4 die aufsichtsrechtliche Kontrolle ermöglicht, die aufgrund der Eingriffsintensivität der dort geregelten Auskunftsfälle als erforderlich gesehen wird.

Zu den Absätzen 4 bis 7

Die Absätze 4 bis 7 entsprechen – mit redaktionellen Anpassungen – den bisherigen Absätzen 3 bis 6.

Zu Nummer 6 (betrifft § 29 LVerfSchG M-V)

Es wird die aktuelle Bezeichnung des Innenressorts in die gesetzliche Regelungslage übernommen.

Zu Artikel 2 – Änderung des SOG M-V**Zu Nummer 1 (betrifft 33d SOG M-V – Einsatz technischer Mittel zur Überwachung der Telekommunikation)****Zu Buchstabe a (Änderung des § 33d Absatz 1 Satz 1 Nummer 5)**

Auf Anregung des Landesbeauftragten für Datenschutz und Informationsfreiheit wird die Voraussetzung zur Telekommunikationsüberwachung in § 33d Absatz 1 Satz 1 Nummer 5 enger gefasst, sodass drohende geringfügige Gesundheitsbeeinträchtigungen nicht mehr vom Anwendungsbereich der Norm erfasst werden.

Zu Buchstabe b, Doppelbuchstabe aa (Änderung des § 33d Absatz 2 Satz 1)

In § 33d Absatz 2 wird geregelt, welche Daten die Polizei im Rahmen der Nutzung der Befugnisse zur Überwachung erheben darf. Dazu gehören – neben den Inhalten und Umständen der Telekommunikation – „Verkehrs- und Standortdaten nach dem Telekommunikationsgesetz“. Hierunter fielen bisher die Daten des § 96 TKG in der bis 30. November 2021 geltenden Fassung (TKG a. F.). Die Erhebung von nach §§ 113b TKG a. F. gespeicherten Verkehrsdaten (sogenannte Vorratsdaten) sind aktuell vom SOG M-V nicht umfasst.

Da § 96 TKG a. F. seit dem 1. Dezember 2021 nicht mehr im TKG enthalten ist, sondern inhaltsgleich in § 9 des TTDSG übernommen wurde (vergleiche Deutscher Bundestag Drucksache 19/27441, Seite 35, dort Ausführungen zu § 9 TTDSG), ist der Verweis auf „Verkehrs- und Standortdaten nach dem Telekommunikationsgesetz“ nicht mehr zutreffend. Insofern erfolgt die Aufnahme des § 9 TTDSG in Absatz 2 Satz 1 Buchstabe b. Gleichzeitig wird durch die Aufnahme dieser konkreten Norm eine Präzisierung der Befugnisnorm erreicht.

Zu Buchstabe b, Doppelbuchstabe bb (Einfügung Satz 4 in § 33d Absatz 2)

Die Aufnahme des Satzes 4 in Absatz 2 dient ebenfalls der Präzisierung. Mit diesem wird gesetzlich klargestellt, dass von der Datenerhebungsbefugnis zur Überwachung der Telekommunikation nicht stets in voller Gänze Gebrauch gemacht werden darf. Vielmehr kommt es je nach vorliegendem Gefahrenfall darauf an, welche Daten tatsächlich zur Abwehr der Gefahr erhoben werden müssen. So wird es beispielsweise bei der Suche nach vermissten Personen mehrheitlich ausreichen, ausschließlich die Erhebung von Standortdaten vorzunehmen. Satz 4 stellt mithin deutlich heraus, dass die Erhebung der in Absatz 2 genannten Daten am Erfordernis im Einzelfall auszurichten ist. Damit wird die bundesverfassungsgerichtliche Rechtsprechung vom 27. Mai 2020, in der bezüglich der Bestandsdatenerhebungsnormen des Bundes unter anderem auf die Notwendigkeit der Normierung der Erforderlichkeit der Bestandsdatenerhebungen im Einzelfall eingefordert wird (siehe 1 BvR 1873/13, dort unter anderem Randnummer 211), vergleichbar in der Befugnisnorm zur Telekommunikationsüberwachung umgesetzt. Denn auch nach § 33d werden Daten bei Anbietern von Telekommunikationsdiensten erhoben.

Zu Buchstabe c (Änderung des § 33d Absatz 7)

In der seit dem 1. Dezember 2021 geltenden Fassung des TKG wird der Begriff des Diensteanbieters nicht mehr verwendet. In § 3 Nummer 1 TKG wird nun der „Anbieter von Telekommunikationsdiensten“ definiert. Insoweit erfolgen Anpassungen des Absatzes 7 bezüglich dieser neuen Begrifflichkeit.

Mit Blick auf die Regelungslagen in den §§ 33e und 33h SOG M-V bezüglich der Verpflichtung der Anbieter zur Auskunftserteilung wird aus gesetzessystematischen Gründen zudem das Wort „vollständig“ in Satz 1 hinzugefügt.

Zu Nummer 2 (betrifft § 33e SOG M-V – Auskunft über Nutzungsdaten)

Der Bundesgesetzgeber hat mit Blick auf das vom BVerfG für Datenbeauskuntungen entwickelte Doppeltürmodell nicht nur das Auskunftsverfahren für Bestandsdaten, sondern auch das Auskunftsverfahren für Nutzungsdaten neu im TTDSG geregelt. Die bisher in § 33e in Bezug genommene Norm des § 15 des Telemediengesetzes ist durch die am 1. Dezember 2021 in Kraft getretenen Neuregelungen im § 24 TTDSG entfallen. So legt der Bundesgesetzgeber nun in § 24 TTDSG die Voraussetzungen ausdrücklich fest, unter denen eine Auskunft über Nutzungsdaten an die für die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständigen Behörden erteilt werden darf („1. Tür“). In Anbetracht dieser „1. Tür“ ist eine Prüfung und ggf. Überarbeitung der fachrechtlichen Abrufbefugnisse für Nutzungsdaten in den Polizeigesetzen der Länder geboten.

Für § 33e SOG M-V ergeben sich im Einzelnen folgende Änderungsbedarfe:

Zu Absatz 1

Die Fallgestaltungen einer möglichen Auskunft über Nutzungsdaten sind in § 24 Absatz 3 TTDSG, dort konkret in Nummer 2 Buchstabe a bis e, abschließend aufgeführt. Unter Beachtung dieser Fallgestaltungen ist eine schlichte Verweisung auf die in § 33d Absatz 1 genannten Voraussetzungen und Personen als solche nicht mehr möglich. Vielmehr bedarf es einer normenklaren Rechtsgrundlage für den Abruf von Nutzungsdaten.

Der Polizei wird somit nach wie vor eine eng begrenzte Abrufnorm zur Verfügung gestellt. Als Voraussetzung wird in beiden benannten Fallgestaltungen der Nummern 1 und 2 zunächst die Erforderlichkeit der Datenerhebung im Einzelfall normiert.

Im Fall der Nummer 1 wird diese Datenerhebung zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr (stellt eine konkrete Gefahr dar; siehe hierzu die ausführliche Begründung unter Nummer 5 zu § 33h Absatz 1) für die öffentliche Sicherheit zum Schutz von besonders gewichtigen Rechtsgütern zugelassen. Dabei ist die Formulierung der Erforderlichkeit im Einzelfall zur Abwehr einer im einzelnen Fall bevorstehenden Gefahr keine vermeintliche sprachliche Doppelung, sondern bewusst gewählt.

Während die Erforderlichkeit im Einzelfall sich auf die Datenerhebung bezieht und ausdrücklicher Bestandteil der in § 24 TTDSG eröffneten „1. Tür“ des Bundes ist, bezieht sich „die im einzelnen Falle bevorstehenden Gefahr“ unter Berücksichtigung der feststehenden Definition in § 3 Nummer 1 SOG M-V auf ein schädigendes Ereignis im konkreten Einzelfall. Dies gilt es mithin auch in der Norm entsprechend umzusetzen. Zudem sind die in § 24 TTDSG enthaltenen Formulierungen bezüglich des Einzelfalles zu berücksichtigen.

Durch die in Nummer 1 gewählte Kombination der konkreten Gefahrenlage mit dem Schutz von besonders gewichtigen Rechtsgütern wird ein engerer Befugnisrahmen gesetzt als die eröffnete „1. Tür“ in § 24 Absatz 3 Nummer 2 Buchstabe a Doppelbuchstabe bb TTDSG ihn vorsieht. Denn dort wird ausschließlich „nur“ der Schutz der Rechtsgüter von hervorgehobenem Gewicht (diese sind weiter gefasst als die besonders gewichtigen Rechtsgüter) für die Auskunftserteilung gefordert und nicht auch noch zusätzlich an eine Gefahrenlage angeknüpft. Es werden zudem nicht alle in § 174 Absatz 5 Nummer 2 Buchstabe a TTDSG aufgezählten Rechtsgüter in die Befugnis übernommen, um nicht ein in sich unstimmliges Regelwerk zu schaffen. Die Übernahme weiterer als die benannten Rechtsgüter in das SOG M-V bleibt mit Blick auf die Dringlichkeit dieses Gesetzentwurfes einer weiteren eingehenden Prüfung zur SOG-Änderung vorbehalten.

Zudem wird die Beauskunftung von Nutzungsdaten nach Nummer 2 auch im Fall des Vorliegens der Voraussetzungen des § 67a Absatz 1 Nummer 1 zur Verhütung von terroristischen Straftaten nach § 67c SOG M-V zugelassen. Diesbezüglich wird von der in § 24 Absatz 3 Nummer 2 Buchstabe d eröffneten Möglichkeit des Datenabrufes Gebrauch gemacht.

Die vorgenannten normierten Befugnisse waren schon bisher über den Verweis in § 33d Absatz 1 enthalten, jedoch wurden sie noch konkreter gefasst.

Es bleibt folglich dabei, dass der Polizei eine sehr eng begrenzte Abrufnorm für Nutzungsdaten zur Verfügung gestellt wird. Eine weitere Umsetzung der zugelassenen Fälle von Auskunftserteilungen über Nutzungsdaten in § 24 Absatz 3 Nummer 2 TTDSG erfolgt derzeit nicht. Auch hierzu bedarf es aus gesetzessystematischen Gründen – wie oben schon zur Übernahme der Rechtsgüter angeführt – einer eingehenden Prüfung, die aufgrund der Dringlichkeit des vorliegenden Gesetzgebungsvorhabens noch nicht vorgenommen werden konnte.

Zusätzlich wird in Absatz 1 – wie etwa im neugefassten § 33h zur Bestandsdatenauskunft normiert –, dass die Polizei Nutzungsdaten nur dann erheben darf, wenn dies im Einzelfall erforderlich ist. Da § 2 Absatz 2 Nummer 3 TTDSG mehrere Arten von Nutzungsdaten unter den dort genannten Buchstaben a bis c aufführt, wird so klargestellt, dass die Auskunft auf die jeweils im Einzelfall erforderlich Nutzungsdaten zu begrenzen ist.

Zu Absatz 2

Wie bisher auch, gelten für die Anordnung der Maßnahme der Nutzungsdatenerhebung die Regelungen, die auch für Maßnahmen der Telekommunikationsüberwachung gelten. Damit bleibt es dabei, dass auch Nutzungsdatenerhebungen unter einem grundsätzlichen Richtervorbehalt stehen. Gefordert wird ein solcher von § 24 TTDSG jedoch nicht.

Durch die neu aufgenommene Maßgabe, dass an die Stelle der Rufnummer in § 33d Absatz 5 Nummer 2 und Absatz 6 Satz 1 Nummer 2 soweit möglich eine eindeutige Kennung des Nutzerkontos der betroffenen Person, ansonsten eine möglichst genaue Bezeichnung des Telemediendienstes tritt, auf den sich das Auskunftsverlangen bezieht, wird die Regelung bezüglich der Angaben im Antrag und der Anordnung präzisiert. Ergänzt wird mit Blick auf die Vorgabe in § 24 Absatz 2 Satz 1 TTDSG zudem, dass in die Anordnung auch die im Einzelfall einschlägige gesetzliche Bestimmung aufzunehmen ist. Sie ist präzise anzugeben (insbesondere Benennung der zutreffenden Nummer des § 33e Absatz 1).

Weiterer Verfahrensregelungen bedarf es in § 33e nach wie vor nicht. Die gerichtliche Zuständigkeit ergibt sich aus § 25b SOG M-V und bezüglich der Nutzungsdatenauskünfte gelangen insbesondere – wie auch für andere Datenerhebungsmaßnahmen nach dem SOG M-V – die Vorschriften zum Schutz zeugnisverweigerungsberechtigter Personen (§ 26b SOG M-V) und die Löschungs-, Dokumentations-, Protokollierungs- und Kennzeichnungsregelungen (§§ 45, 46d bis 46g SOG M-V) zur Anwendung. Die Benachrichtigung in Fällen einer Nutzungsdatenerhebung regelt bereits § 46a Absatz 1 Satz 1 Nummer 4. Die Erhebungen unterliegen zudem einer Berichtspflicht gegenüber dem Landtag Mecklenburg-Vorpommern und dessen SOG-Gremium (siehe auch Änderung unter Nummer 10 zu § 48h Absatz 1 Satz 1 Nummer 4 SOG M-V und die dort erfolgte Präzisierung).

Zu Absatz 3

Mit Blick auf § 24 Absatz 4 TTDSG, wonach derjenige, der geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln hat, wird diese Formulierung auch entsprechend in § 33e SOG M-V und darüber hinaus unverändert übernommen.

Zu Nummer 3 (betrifft § 33f SOG M-V – Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten)

Es erfolgt auch hier – wie in § 33d Absatz 7 (siehe oben Nummer 1 Buchstabe b) eine Anpassung aufgrund des in § 3 Nummer 1 TKG verwendeten Begriffes „Anbieter von Telekommunikationsdiensten“.

Zu Nummer 4 (betrifft § 33g SOG M-V – Unterbrechung oder Verhinderung der Telekommunikation)

In dem bis einschließlich 4. Juni 2020 geltenden § 34a SOG M-V (SOG M-V a. F.) war die Befugnis zur Verhinderung und Unterbrechung der Telekommunikation als Teil der Befugnis zur Telekommunikationsüberwachung normiert. Auf den § 34a Absatz 3 SOG M-V a. F. darf verwiesen werden. Im Zuge der SOG-Neufassung wurde die Befugnis zur Unterbrechung oder Verhinderung der Telekommunikation in eine gesonderte Norm überführt. Der Hintergrund für die Herauslösung war, dass diese – anders als die Maßnahmen im derzeit geltenden § 33d SOG M-V – keine Maßnahmen sind, die auf die Überwachung der Telekommunikation im Sinne der Erhebung von Daten gerichtet sind.

Es geht vielmehr ausschließlich darum, zur Gefahrenabwehr die Telekommunikation zu unterbinden. Im Zuge der Herauslösung dieser Befugnis aus der Telekommunikationsüberwachungsnorm ist durch ein Redaktionsversehen die in § 34a Absatz 6 SOG M-V a. F. enthaltene Anbieterverpflichtung, die Unterbrechung und Verhinderung von Telekommunikation zu ermöglichen, nicht mit in die neue Norm des § 33g übertragen worden. Dies führt dazu, dass die Norm gegebenenfalls so verstanden werden könnte, dass die Polizei ausschließlich selbst und mit eigenen Mitteln Telekommunikation unterbrechen oder verhindern kann.

Dieses Redaktionsversehen wird mit der Anfügung des Absatzes 6 behoben und die seinerzeit geltende Regelungslage zur Anbieterverpflichtung wird wiederhergestellt. Anbieterverpflichtungen zur Unterbrechung und Verhinderung von Telekommunikation enthalten auch andere Polizeigesetze der Länder (siehe beispielsweise Schleswig-Holstein: § 185b des Landesverwaltungsgesetzes, Hamburg: § 23 des Gesetzes über die Datenverarbeitung der Polizei Hamburg oder auch Sachsen-Anhalt: § 33 des Gesetzes über die öffentliche Sicherheit und Ordnung).

Zusätzlich wird in Absatz 6 klargestellt, dass die Unterbrechung und Verhinderung gegenüber den Anbietern von Telekommunikationsdiensten nur insoweit verlangt werden kann, wie das neugefasste TKG oder die hierzu erlassenen Bestimmungen dem Verlangen nicht entgegenstehen.

Zu Nummer 5 (betrifft § 33h SOG M-V – Auskunft über Bestandsdaten)

Die Neufassung des § 33h erfolgt insbesondere unter Beachtung

- der unter I. (Allgemeine Begründung) angeführten bundes- und landesverfassungsgerichtlichen Entscheidungen zur Bestandsdatenauskunft,
- des am 1. Dezember 2021 in Kraft getretenen TKG sowie
- des am 1. Dezember 2021 in Kraft getretenen TTDSG unter Aufhebung der §§ 14 und 15 des Telemediengesetzes.

Unter Berücksichtigung der vom Bundesgesetzgeber geschaffenen Übermittlungsbefugnisse für die Anbieter von Telekommunikationsdiensten und für Anbieter von Telemedien („1. Tür“) sind die Bestandsdatenauskunftsnormen im Fachrecht der Länder („2. Tür“) zu prüfen und gegebenenfalls anzupassen.

§ 33h wird insgesamt neu strukturiert. Es ist aufgrund unterschiedlicher Abrufvoraussetzungen im § 174 TKG und in den §§ 22, 23 TTDSG eine Trennung der Bestandsdaten im Telekommunikationsbereich und im Telemedienbereich vorzunehmen. Während die Absätze 1 und 2 nun ausschließlich zum polizeilichen Abruf von Bestandsdaten nach § 174 TKG ermächtigen, enthalten die Absätze 3 bis 5 die Befugnisse für die Polizei zum Abruf für Bestandsdaten nach den §§ 22, 23 TTDSG. Alle Befugnisse in § 33h fordern – wie vom Bundesverfassungsgericht in der Entscheidung vom 27. Mai 2020 gefordert (siehe unter anderem Randnummer 211) – als Voraussetzung bezüglich der Datenerhebung die Erforderlichkeit dieser im Einzelfall. Alle Befugnisse enthalten dabei zudem als Eingriffsvoraussetzung den Gefahrenbegriff der „im einzelnen Falle bevorstehenden Gefahr“ und zwar begrenzt auf die öffentliche Sicherheit. Zur Zulässigkeit der Beibehaltung dieses Gefahrenbegriffes wird auf die nachstehenden Ausführungen zu Absatz 1 verwiesen.

Dabei ist die jeweils in den Absätzen 1 bis 5 gewählte Formulierung der Erforderlichkeit im Einzelfall zur Abwehr einer im einzelnen Fall bevorstehenden Gefahr – wie auch schon zur Änderung des § 33e ausgeführt – keine vermeintliche sprachliche Doppelung, sondern bewusst gewählt. Während die Erforderlichkeit im Einzelfall sich auf die Datenerhebung bezieht und auch ausdrücklicher Bestandteil der eröffneten „1. Türen“ in § 174 TKG und in den §§ 22, 23 TTDSG ist, bezieht sich „die im einzelnen Falle bevorstehenden Gefahr“ unter Berücksichtigung der feststehenden Definition in § 3 Nummer 1 SOG M-V auf ein schädigendes Ereignis im konkreten Einzelfall. Dies gilt es mithin auch entsprechend in der Norm umzusetzen. Zudem sind die gewählten Formulierungen bezüglich des Einzelfalles in den vorgenannten bundesgesetzlichen „1. Türen“ zu berücksichtigen.

Absatz 6 enthält als gemeinsame Vorschrift (für die Absätze 1 bis 5) die Auskunftspflicht für die vorgenannten Anbieter und die Regelung zu deren Entschädigung.

Die Benachrichtigungspflicht bei der Inanspruchnahme von Anbietern nach § 33h Absatz 1 Satz 2 und Absatz 2 regelt bereits § 46a SOG M-V Absatz 1 Satz 1 Nummer 4 SOG M-V. Durch die Herauslösung des Telemedienbereiches in die neuen Absätze 3 bis 5 des § 33h ist diese Benachrichtigungspflicht nun auch auf die Absätze 4 und 5 zu erstrecken; auf die erfolgte Ergänzung des § 46a (Änderung unter Nummer 6) wird verwiesen.

Eine Berichtspflicht bezogen auf Bestandsdatenauskünfte ist unter Verweis auf die BVerfG-Entscheidung vom 27. Mai 2020, wonach Bestandsdatenauskünften nur ein gemäßigtes Eingriffsgewicht zukommt (siehe dort Randnummer 251), nach wie vor nicht im § 48h SOG M-V zu verankern. Zur datenschutzaufsichtlichen Kontrolle ist auf die bereits bestehenden Regelungen in den §§ 48b ff. SOG M-V hinzuweisen.

Zudem wird darauf hingewiesen, dass es weiterer spezieller Verfahrensregelungen in § 33h nicht bedarf. Soweit eine gerichtliche Entscheidung in der Norm gefordert wird, ergibt sich die Zuständigkeit und das Verfahren aus § 25b SOG M-V. Bezüglich der Bestandsdatenauskünfte gelangen insbesondere die Vorschriften zum Schutz zeugnisverweigerungsberechtigter Personen (§ 26b SOG M-V), die Löschungs-, Dokumentations-, Protokollierungs- und Kennzeichnungsregelungen (§§ 45, 46d bis 46g SOG M-V) zur Anwendung. Die Dokumentationspflicht in § 46d Absatz 1 Satz 1 Nummer 1 wird mit Blick auf die Entscheidung LVerfG 3/14 jedoch noch klarstellend ergänzt; auf die Ausführungen zur Änderung unter Nummer 7 wird verwiesen.

Darüber hinaus wird zu den Absätzen Folgendes ausgeführt:

Zu Absatz 1 Satz 1

Mit Absatz 1 Satz 1 wird die Befugnis zur allgemeinen Bestandsdatenauskunft geregelt. Unter Berücksichtigung der „1. Tür“ in der Übermittlungsregelung des § 174 Absatz 1 Satz 1 können Bestandsdaten nach § 3 Nummer 6 und § 172 TKG Gegenstand des Abrufs sein. Bestandsdatenauskünfte im Telemedienbereich enthält Satz 1 nicht mehr; diese Regelungslage wurde in Anbetracht der Neuregelungen in den §§ 22, 23 TTDSG herausgelöst und in den Absätzen 3 bis 5 normiert.

Der Abruf der Daten nach § 3 Nummer 6 und § 172 TKG wird der Polizei erlaubt, wenn dies im Einzelfall erforderlich ist zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit (zur vermeintlichen sprachlichen Doppelung siehe bereits vorstehende allgemeine Ausführungen zur Änderung des § 33h). Die öffentliche Ordnung ist mithin von der Abrufbefugnis nicht umfasst, da § 174 Absatz 3 Nummer 2 Buchstabe a TKG als „1. Tür“ für diesen Zweck keine Abrufmöglichkeit vorsieht. Es wird zudem klargestellt, dass die Anordnung stets nur im Einzelfall zulässig ist und die einschlägige gesetzliche Bestimmung zu enthalten hat. Diese ist präzise anzugeben.

Das Tatbestandsmerkmal des Einzelfalls ist den verfassungsrechtlichen Anforderungen entsprechend vorgesehen (LVerfG 3/14, Randnummer 66).

Festgehalten wird im Übrigen an dem Gefahrenbegriff der „im einzelnen Falle bevorstehenden Gefahr“. Das LVerfG führt – unter Bezugnahme auf die oben genannten BVerfG-Entscheidung vom 27. Mai 2020 (1 BvR 1873/13) – in seiner Entscheidung LVerfG 3/14 unter Randnummer 67 aus, dass bezogen auf die Gefahrenabwehr grundsätzlich eine im Einzelfall vorliegende konkrete Gefahr im Sinne der polizeilichen Generalklausel vorliegen muss und diese Schwelle auch den Gefahrenverdacht erfasst. Die bisherige Regelung in § 33h Absatz 1 Satz 1 SOG M-V beanstandet das LVerfG sodann mit der Begründung, dort werde „zwar eine im einzelnen Falle bevorstehende Gefahr vorausgesetzt, nicht aber eine konkrete Gefahr“ (LVerfG 3/14, Randnummer 67).

Der Unterschied zwischen einer „im einzelnen Falle bevorstehenden Gefahr“ und einer „konkreten Gefahr“ wird vom LVerfG nicht erläutert.

Bereits seit dem 30. Oktober 2001 (siehe GVOBl. M-V S. 386) definiert § 3 Absatz 3 Nummer 1 SOG M-V den Gefahrenbegriff „eine im einzelnen Falle bevorstehende Gefahr“ wie folgt:

„eine Sachlage, bei der bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens ein die öffentliche Sicherheit oder Ordnung schädigendes Ereignis im konkreten Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit eintreten wird;“.

Diese Definition gilt immer dann, wenn der Begriff „eine im einzelnen Falle bevorstehende Gefahr“ im SOG M-V als Eingriffsschwelle genannt wird, so etwa auch in § 16 Absatz 1 Nummer 2, auf den selbst das LVerfG in Randnummer 93 konkretisierend verweist. Ähnliche Regelungen existieren in einigen anderen Länderpolizeigesetzen ebenso (siehe beispielsweise § 176 oder § 180a des Allgemeinen Verwaltungsgesetzes für das Land Schleswig-Holstein; § 8 des Saarländischen Polizeigesetzes sowie § 36 des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei).

Die Definition entspricht nach Auffassung des Gesetzgebers der vom BVerfG in ständiger Rechtsprechung erwähnten Eingriffsschwelle der konkreten Gefahr.

Das BVerfG prüfte beispielsweise nach seiner Entscheidung zur Bestandsdatenauskunft am 27. Mai 2020 die geltende Regelungslage zur Bestandsdatenauskunft in Schleswig-Holstein mit der – wie in § 33h SOG M-V – enthaltenen Eingriffsschwelle „eine im einzelnen Falle bevorstehende Gefahr“ und führte in seiner Entscheidung vom 19. April 2021, 1 BvR 1732/14, dort Randnummern 46, 48 und 49 aus:

„Die allgemeine Bestandsdatenauskunft von Telekommunikationsdienste-anbietern ist jedenfalls dann verhältnismäßig, wenn sie auf dem Gebiet der Gefahrenabwehr an das Bestehen einer konkreten Gefahr im Sinne der polizeirechtlichen Generalklausel geknüpft ist [...].

§ 180a Abs. 1 Satz 1 LVwG und § 8a Abs. 1 Satz 2 LVerfSchG genügen diesen Anforderungen. Das gilt insbesondere hinsichtlich der vorgesehenen Eingriffsschwellen.

aa) Soweit § 180a Abs. 1 Satz 1 LVwG als Eingriffsschwelle eine „im einzelnen Falle bevorstehende Gefahr“ voraussetzt, entspricht dies entgegen der Auffassung der Beschwerdeführenden sowohl nach der sonstigen Verwendung dieser Formulierung innerhalb des Landesverwaltungsgesetzes als auch nach der Begründung des Gesetzentwurfs (vgl. LTDrucks Schl.-H. 18/713, S. 13) dem Erfordernis einer konkreten Gefahr.“

Dieses Verständnis entspricht auch der herkömmlichen allgemeinen Auffassung in der polizeirechtlichen Literatur (zum Beispiel Biermann/Wehser, „Praxis der Kommunalverwaltung“, § 3 SOG M-V, Nummer 5.3.1; Denninger in: Lisken/Denninger Handbuch des Polizeirechts 6. Auflage 2018, Kapitel D. Randnummer 42).

Bundesländer, die die konkrete Gefahr als solche bezeichnen und definieren (vergleiche etwa § 2 Nummer 1 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes), verwenden genau die Definition, die auch § 3 Nummer 1 SOG M-V für die „im einzelnen Falle bevorstehende Gefahr“ verwendet.

Vor diesem Hintergrund wird in § 33h SOG M-V an dem im § 3 Absatz 3 Nummer 1 SOG M-V definierten und in der bundesverfassungsgerichtlichen Rechtsprechung anerkannten Gefahrenbegriff der „im einzelnen Falle bevorstehende Gefahr“ für die allgemeine Bestandsdatenauskunft festgehalten. Darüber hinaus ist auch die Gesetzessystematik zu berücksichtigen. Seit Einführung des Sicherheits- und Ordnungsgesetzes in Mecklenburg-Vorpommern im Jahr 1992 ist der Gefahrenbegriff der „im einzelnen Falle bevorstehende Gefahr“ Bestandteil der Generalklausel (§§ 13, 16 SOG M-V) und er wird auch in weiteren Eingriffsnormen des SOG M-V verwendet. Es wird in der ordnungsbehördlichen und polizeilichen Praxis täglich mit diesem verfassungsgerichtlich anerkannten Gefahrenbegriff gearbeitet. Zudem ist darauf hinzuweisen, dass das SOG M-V gemäß dessen § 12 Absatz 2 als sogenanntes „Auffangrecht“ fungiert, wenn besondere Gesetze und Rechtsverordnungen zur Gefahrenabwehr fehlen oder nicht abschließende Regelungen enthalten. Auch vor diesem Hintergrund wird am Gefahrenbegriff der „im einzelnen Falle bevorstehende Gefahr“ festgehalten.

Neben dem seit 19. März 2021 geltenden § 185 des Landesverwaltungsgesetzes in Schleswig-Holstein behält auch beispielsweise der seit dem 21. Januar 2022 geltende und an die BVerfG-Entscheidung vom 27. Mai 2020 angepasste § 36 des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei diesen Gefahrenbegriff bei.

Zu Absatz 1 Satz 2

Absatz 1 Satz 2 enthält wie bisher – jedoch nun unter Beachtung des neuen § 174 Absatz 1 Satz 2 und Absatz 4 TKG und durch den Verweis auf die Voraussetzungen in Satz 1 auch auf die Erforderlichkeit im Einzelfall und die dort enthaltene Gefahrenschwelle bezogen – die polizeiliche Befugnis, die Auskunft auch über Bestandsdaten mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, verlangen zu können. Diese Auskunft über Passwörter und andere Zugangsdaten (Zugangssicherungs_codes) darf mithin nur unter den Voraussetzungen des Satzes 1 und nur dann verlangt werden, wenn im Einzelfall auch die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Die Regelungslage ist weder vom BVerfG in der oben genannten Entscheidung vom 27. Mai 2020 noch vom LVerfG in der Entscheidung LVerfG 3/14 beanstandet worden. Sie wurde daher auch in die Formulierung des § 174 Absatz 4 TKG als „1. Tür“ für derartige Datenbeauskunftungen übernommen. Bezüglich der Begründung zur Anwendung der Regelungslage darf ergänzend auf die seinerzeitige Gesetzesbegründung in der Landtagsdrucksache 6/1630, dort auf den Seiten 16 und 17 zu § 28a Absatz 1 Satz 2 SOG M-V a. F. verwiesen werden.

Deren Aussage lässt sich noch einmal wie folgt kurz zusammenfassen:

Soll beispielsweise eine Auskunft über Zugangssicherungs_codes eingeholt werden, um eine Überwachung eines noch nicht abgeschlossenen Telekommunikationsvorgangs – und damit einen Eingriff in das Fernmeldegeheimnis – zu gefahrenabwehrrechtlichen Zwecken zu ermöglichen, ist immer § 33d SOG M-V zu berücksichtigen. Dies bedeutet, dass eine Auskunft nach § 174 TKG über Zugangssicherungs_codes in diesen Fällen von der Polizei nur dann verlangt werden darf, wenn die in § 33d Absatz 1 enthaltenen, strengeren Voraussetzungen erfüllt sind. Insbesondere bedeutet dies auch, dass nach § 33d eine richterliche Anordnung vorliegen muss beziehungsweise eine nachträgliche richterliche Entscheidung einzuholen ist. Ist hingegen zum Beispiel mit der Nutzung der Zugangssicherungs_codes ein Auslesen der Daten, die auf einem sichergestellten Mobilfunktelefon abgelegt und damit im Herrschaftsbereich des Betroffenen gespeichert sind, mit dem Ziel deren Sicherstellung beabsichtigt, so könnte eine Auskunft nach § 174 TKG in diesen Fällen von der Polizei verlangt werden, wenn die für die Sicherstellung geltenden Voraussetzungen (§ 61 ff. SOG M-V) vorliegen. Bei Datensicherstellungen ist bereits in § 61 Absatz 1 Satz 4 SOG M-V normiert, dass durch die sicherstellende Behörde die richterliche Bestätigung der Rechtmäßigkeit der Maßnahme zu beantragen ist. Demnach wird eine richterliche Kontrolle sichergestellt. Welche gesetzlichen Voraussetzungen nach dem Sicherheits- und Ordnungsgesetz für eine Auskunft über die Zugangssicherungs_codes nach § 174 TKG vorliegen müssen, bestimmt sich letztlich also danach, wofür die Codes konkret genutzt werden sollen. Es gilt, dass § 33d SOG M-V immer dann zu beachten ist, wenn mit den Sicherungs_codes auf Daten zugegriffen werden soll, die dem Schutzbereich von Artikel 10 GG unterfallen.

Es wird darauf hingewiesen, dass die Benachrichtigung der von der Erhebung von Zugangssicherungs_codes betroffenen Personen bereits in § 46a Absatz 1 Satz 1 Nummer 4 geregelt ist. Zur Anwendung weiterer SOG-Regelungen wird auf die Ausführungen vor Absatz 1 verwiesen.

Zu Absatz 2

Auch Absatz 2 enthält wie die bisherige Ermächtigungsnorm, dass die Auskunft auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse im Einzelfall unter Angabe der gesetzlichen Bestimmung verlangt werden kann. Der Abruf von Bestandsdaten, die anhand dynamischer IP-Adressen bestimmt werden, greift in das nach Artikel 10 des Grundgesetzes bestehende Telekommunikationsgeheimnis ein. Er liegt hinsichtlich der Eingriffsintensität unterhalb derjenigen einer Telekommunikationsüberwachung, ist jedoch eingriffsintensiver als die allgemeine Bestandsdatenauskunft nach Absatz 1 (siehe hierzu auch BVerfG-Entscheidung vom 27. Mai 2020, Randnummern 90, 97, 99, 102 und 167 ff., 268, 272).

Aufgrund der bundesverfassungsgerichtlichen Entscheidung und zur Umsetzung der Maßgaben in der landesverfassungsgerichtlichen Entscheidung LVerfG 3/14 (Randnummern 61 und 70 bis 74; siehe auch oben unter I. Allgemeines Begründung) sowie unter Beachtung der in § 174 Absatz 5 Nummer 2 geschaffenen „1. Tür“ im TKG wird diese Befugnis nun zusätzlich an die Voraussetzung des Schutzes von besonders gewichtigen Rechtsgütern gebunden. Es werden die bereits in § 33d Absatz 1 Satz 1 Nummer 1 enthaltenen Rechtsgüter in die Norm übernommen. Von der Übernahme weiterer in § 174 Absatz 5 Nummer 2 Buchstabe a benannter Rechtsgüter wird derzeit aus gesetzessystematischen Gründen Abstand genommen, um nicht ein in sich unstimmliges Regelungswerk zu schaffen. Die Übernahme weiterer Rechtsgüter in das SOG M-V bleibt mit Blick auf die Dringlichkeit dieses Gesetzentwurfes einer weiteren eingehenden Prüfung zur SOG-Änderung vorbehalten.

Die verfassungsrechtlich geforderte Benachrichtigung der von der Datenauskunft anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse betroffenen Personen ist bereits in § 46a Absatz 1 Satz 1 Nummer 4 ausdrücklich geregelt. Zur Anwendung weiterer SOG-Regelungen wird auf die Ausführungen vor Absatz 1 verwiesen.

Zu den Absätzen 3 bis 5

Wie bereits eingangs zu § 33h ausgeführt, wurden unter Beachtung der §§ 22, 23 TTDSG als 1. „Tür“ die Regelungen zu den Bestandsdatenauskünften im Telemedienbereich aus Absatz 1 des § 33h SOG M-V herausgelöst und in die Absätze 3 bis 5 aufgenommen.

Absatz 3 übernimmt für den Bereich der Telemedien die allgemeine Bestandsdatenauskunft, die § 22 Absatz 1 Satz 1 TTDSG über Bestandsdaten nach § 2 Absatz 2 Nummer 2 zulässt. Wie bei der Befugnis zur allgemeinen Bestandsdatenauskunft im Telekommunikationsbereich nach Absatz 1 werden auch hier die Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit und die Erforderlichkeit der Bestandsdatenerhebung im Einzelfall unter Angabe der gesetzlichen Bestimmung als Voraussetzungen normiert. Auf die diesbezüglichen Ausführungen zum Absatz 1 Satz 1 wird vollumfänglich verwiesen.

In Absatz 4 wird auch im Bereich der Telemedien die polizeiliche Beauskunftung von Bestandsdaten mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, zugelassen. Allerdings darf diese Auskunft über Zugangssicherungs_codes durch Anbieter von Telemedien nach § 23 Absatz 2 Satz 1 Nummer 2 TTDSG – anders als nach § 174 TKG – nur erteilt werden „... zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit der Person, für die sexuelle Selbstbestimmung, für den Bestand des Bundes oder eines Landes, die freiheitlich demokratische Grundordnung sowie Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, erlauben, nach Anordnung durch ein Gericht.“

Diese Vorgaben werden umgesetzt. So sieht die Befugnisnorm vor, dass die Auskunft nur im Einzelfall zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für die öffentliche Sicherheit (siehe zum Gefahrenbegriff Ausführungen zum Absatz 1 Satz 1) zum Schutz besonders gewichtiger Rechtsgüter und nur dann verlangt werden darf, wenn darüber hinaus im Einzelfall die gesetzlichen Voraussetzungen zur Nutzung der Daten vorliegen. Dabei werden auch hier – wie in § 33e – die Rechtsgüter normiert, die auch § 33d Absatz 1 Satz 1 Nummer 1 SOG M-V kennt und benennt (auf die Ausführungen zu Absatz 2 wird verwiesen). Es wird eine richterliche Anordnung verlangt; eine Ausnahme von dieser ist nicht zugelassen. Die Antragstellung hat durch die Leitung der zuständigen Polizeibehörde (eingeschlossen ist in diese Formulierung wie sonst auch im SOG M-V die Vertretung im Amt) zu erfolgen. Satz 2, dort 2. Halbsatz, bestimmt für die Antragstellung und Anordnung die entsprechende Anwendung des § 33d Absatz 5 und 6 SOG M-V. Zudem wird klargestellt, dass der Antrag und die Anordnung die einschlägige gesetzliche Bestimmung zu enthalten haben, auf die das Auskunftsverlangen gestützt wird. Diese ist präzise anzugeben.

Mit Satz 3 wird die in § 23 Absatz 2 Satz 2 TTDSG enthaltene Datenübermittlungsbeschränkung für die Anbieter von Telemedien bezüglich der Zugangssicherungs_codes für die Polizei übernommen, um eine Umgehung der bundesgesetzlichen Regelungslage durch die etwaige Anwendung der Datenübermittlungsregelungen in §§ 39 ff. SOG M-V ausdrücklich auszuschließen.

Absatz 5 übernimmt unter Beachtung des § 22 Absatz 1 Satz 3 und 4 sowie Absatz 4 TTDSG – entsprechend der Regelungslage in Absatz 2 für den Telekommunikationsbereich – die Bestandsdatenbeauskunftung nach Absatz 3 und 4 im Einzelfall anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse. Auf die Ausführungen zu Absatz 2 wird verwiesen.

Es wird darauf hingewiesen, dass die Benachrichtigung der von der Datenerhebung nach Absatz 4 und 5 betroffenen Personen nicht in § 33h zu regeln ist. Sie ist bereits in § 46a Absatz 1 Satz 1 Nummer 4 bestimmt (siehe Ausführungen unter Nummer 6 zur Anpassung der Verweisung in § 46a SOG M-V).

Zur Anwendung weiterer SOG-Regelungen wird auf die Ausführungen vor Absatz 1 verwiesen.

Zu Absatz 6

In Absatz 6 wird die bisher in § 33h Absatz 3 enthaltene Auskunftspflicht der in der Norm genannten Anbieter, jedoch mit Blick auf den neuen § 174 Absatz 6 TKG unter Anpassung der Formulierung, übernommen. Die bisherige Entschädigungsregelung wird unverändert beibehalten.

Zu Nummer 6 (betrifft § 46a SOG M-V – Benachrichtigungspflichten bei verdeckten und eingriffsintensiven Maßnahmen)

Die Formulierung „Diensteanbieter“ wird aus § 46a Absatz 1 Satz 1 Nummer 4 wie schon in den oben geänderten Regelungen aufgrund der neuen Begrifflichkeiten im TKG und TTDSG ersetzt. Gleichzeitig wird die Regelungslage in Nummer 4 präzisiert. So enthält von den aufgezählten Regelungen nicht nur § 33d Eingriffe in den Telekommunikationsbereich; § 33d enthält zudem auch eine Regelung zur Inanspruchnahme von Anbietern von Telekommunikationsdiensten. Durch die gewählte Neuformulierung werden nun alle Eingriffe und Inanspruchnahmen von Anbietern von Telekommunikationsdiensten oder Telemedien bei der Benachrichtigungspflicht eindeutig erfasst.

Gemäß § 46a Absatz 1 Satz 1 Nummer 4 sind Maßnahmen der Bestandsdatenauskunft nach § 33h Absatz 1 Satz 2 und Absatz 2 benachrichtigungspflichtig. Diese Benachrichtigungspflichten betreffen die Auskunft von Bestandsdaten

- mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, oder
- anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse.

Da die Beauskunftung derartiger Bestandsdaten für den Bereich der Telemedien mit Blick auf die neu geschaffene Regelungslage in den §§ 22 und 23 TTDSG aus § 33h Absatz 1 Satz 1 herausgelöst und nun in dessen Absätzen 4 und 5 geregelt wird, ist die in § 46a Absatz 1 Satz 1 Nummer 4 zur Benachrichtigung enthaltene Verweisung – neben § 33h Absatz 1 Satz 2 und Absatz 2 – auch auf die neuen Absätze 4 und 5 zu erstrecken. Damit gilt die Benachrichtigungspflicht für jede Beauskunftung im Bereich des TKG und des TTDSG von Bestandsdaten mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, sowie für jede Beauskunftung im Bereich des TKG und des TTDSG von Bestandsdaten anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse.

Zu Nummer 7 (betrifft § 46d SOG M-V - Dokumentationspflichten)

Das LVerfG fordert in seiner Entscheidung LVerfG 3/14 unter den Randnummern 85 und 87 bezüglich der Datenerhebungen anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse eine Dokumentation der zugrundeliegenden Tatsachen.

Der bereits seit dem 22. April 2021 mit dem Artikel 2 des Gesetzes zur Änderung des Petitions- und Bürgerbeauftragengesetzes und zur Änderung anderer Gesetze (GVOBl. M-V S. 370, 372) ergänzte § 46d Absatz 1 Satz 1 Nummer 1 SOG M-V wird weiter konkretisiert, um die Dokumentation unmissverständlich auch auf das Vorliegen der Erhebungsvoraussetzungen zu erstrecken.

Mit der Ergänzung wird zugleich die vom Landesbeauftragten für Datenschutz und Informationsfreiheit vorgeschlagene Formulierung übernommen.

Zu Nummer 8 (betrifft § 46f SOG M-V – Protokollierungspflichten bei verdeckten und eingriffsintensiven Maßnahmen),

Zu Nummer 9 (betrifft § 46g SOG M-V – Kennzeichnungspflichten)

Der Begriff „Diensteanbieter“ wird auch in den §§ 46f, 46g aufgrund der neuen Begrifflichkeiten im TKG und TTDSG angepasst.

In § 46f wird die Protokollierungspflicht mit Blick auf die Änderung der Benachrichtigungsregelung in § 46a (siehe Nummer 6) auch auf § 33h Absatz 1 Satz 2, Absatz 2, Absatz 4 und 5 erstreckt.

Zu Nummer 10 (betrifft § 48h SOG M-V – Parlamentarische Kontrolle, Unterrichtung der Öffentlichkeit)

Zu Buchstabe a (Änderung des § 48h Absatz 1)

In Satz 1 und Satz 4 wird eine Aktualisierung der Ressortbezeichnungen vorgenommen.

Die vorgenommene Änderung in § 48h Absatz 1 Satz 1 Nummer 4 erfolgt zur sprachlichen Angleichung an § 46a Absatz 1 Satz 1 Nummer 4. Sie dient zudem der Präzisierung, da nicht alle Maßnahmen nach § 33d bis 33g Eingriffe im Telekommunikationsbereich beinhalten (beispielsweise § 33e). Durch das Einfügen der Anbieter von Telekommunikationsdiensten oder Telemedien bezieht sich die Berichtspflicht nun eindeutig auf die in den Normen der §§ 33d bis 33g entsprechend enthaltenen Befugnisse.

Zu den Buchstaben b und c (Änderung von § 48h Absatz 4 und 5)

Es erfolgt die Übernahme der aktuellen Ressortbezeichnungen in die gesetzlichen Bestimmungen.

Zu Nummer 11 (betrifft §§ 4, 5, 11, 20, 31, 32a, 38, 42, 48, 52, 112, 115 SOG M-V)

Es erfolgt jeweils eine Aktualisierung der Ressortbezeichnungen in den gesetzlichen Regelungslagen.

Zu Artikel 3 – Einschränkung eines Grundrechts

Mit Artikel 3 wird dem verfassungsrechtlichen Zitiergebot gemäß Artikel 19 Absatz 1 Satz 2 des Grundgesetzes Rechnung getragen.

Zu Artikel 4 – Inkrafttreten

Artikel 4 bestimmt das Inkrafttreten des Gesetzes am Tag nach der Verkündung.