LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/5682**
8. Wahlperiode **26.11.2025**

GESETZENTWURF

der Landesregierung

Entwurf eines Gesetzes zur Neuordnung und Förderung der Informationssicherheit im Land Mecklenburg-Vorpommern

A Problem und Ziel

Alle Teile unserer Gesellschaft erleben eine stetig wachsende Bedeutung des Digitalen: digitale Informationen, digitale Anwendungen, digitale Infrastrukturen, digitaler IT-Schutzschirm, digitale Resilienz. Die zunehmende Vernetzung und Digitalisierung von Bereichen sowohl des öffentlichen als auch des privaten und wirtschaftlichen Lebens führen in unserer stark arbeitsteiligen Gesellschaft zu kontinuierlich steigenden multiplen und wechselseitigen Abhängigkeiten.

Unsere hoch technologisierte Gesellschaft muss folglich resilient sein. Es müssen Kompetenzen und Fähigkeiten in Organisationen entwickelt, aufrechterhalten und optimiert werden, sich sowohl an digitale Herausforderungen als auch an Veränderungen anzupassen, insbesondere Krisen zu bewältigen. Organisationen müssen somit widerstandsfähig sein, sich schnell von technischen Störungen, Cyberangriffen und anderen digitalen Bedrohungen zu erholen.

Damit einhergehend hat sich IT-Sicherheit seit dem letzten Jahrzehnt fundamental zur Informationssicherheit hin gewandelt. Solange die Informationstechnik aus abgrenzbaren, oftmals nicht oder wenig vernetzten Rechnersystemen bestand, bezog sich die IT-Sicherheit grundsätzlich auf die eingesetzte Hard- und Software. Aus heutiger Sicht waren die damaligen Rechnersysteme oder Großrechneranlagen wenig komplex und gut beherrschbar. Sie besaßen kaum einen signifikanten Einfluss auf die Arbeits-, Handlungs- und Leistungsfähigkeit von Organisationen. Die IT-Sicherheit fristete somit eine Nischenaufgabe von wenigen Experten; Mängel und Defizite in der IT-Sicherheit hatten keine mediale Aufmerksamkeit in der Öffentlichkeit. Im Gegensatz zu diesem Zeitabschnitt richtet sich heute der Blick nicht nur auf die Hard- und Software, sondern auf Daten und Informationen allgemein.

Daten und Informationen müssen sicher sein, das heißt, die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit müssen gewährleistet sein.

Viele Organisationen sind heute auf die Sicherheit der von ihnen eingesetzten Informationstechnik und konsumierten digitalen Dienstleistungen angewiesen. In vielen Fällen wirken heutige (erhebliche) Sicherheitsvorfälle unmittelbar existenzbedrohlich. Dies gilt sowohl für die Wirtschaft als auch für andere gesellschaftliche Organisationen und natürlich auch für die öffentliche Hand.

Daneben tritt seit einigen Jahren eine darüber hinausreichende gesellschaftliche Abhängigkeit vom Funktionieren kritischer Sektoren unserer Gesellschaft hervor, wie beispielsweise die Energieversorgung oder auch die ordnungsgemäße Durchführung demokratischer Wahlen. Kritische Infrastrukturen, vielfach im kommunalen Umfeld angesiedelt, können heutzutage nicht mehr effektiv und effizient ohne Informationstechnik betrieben werden. Diese sowie deren Kunden sind deshalb auf eine wirkungsvolle Informationssicherheit angewiesen.

Der wirtschaftlich angemessene Schutz von Informationstechnik vor Bedrohungen ist infolgedessen ein gesamtgesellschaftlicher Auftrag – international, national und regional.

Die öffentliche Verwaltung hat somit zentrale, digitale Verwaltungsdienstleistungen bereitzustellen. Störungen oder Ausfälle können erhebliche wirtschaftliche und soziale Folgeeffekte mit sich bringen. Informationssicherheit ist notwendig, um einen reibungslosen Betrieb von Verwaltungsdienstleistungen sicherzustellen und Ausfälle durch Cyberangriffe zu verhindern.

Die Folgen erheblicher Cyberangriffe auf die öffentliche Verwaltung in Mecklenburg-Vorpommern haben sich z. B. beim Angriff auf den Landkreis Ludwigslust-Parchim im Oktober 2021 oder auf den Landkreis Vorpommern-Rügen im November 2023 gezeigt. Infolge dieser Ereignisse und der eingehenden Schädigung der IT-Infrastruktur konnten mehrere Bürgerdienste über Wochen teilweise nur in einem Notbetrieb mit erheblichen Einschränkungen erbracht werden. Neben diesen Einschränkungen zeigen wiederholt erfolgreiche Cyberangriffe auf kritische Infrastrukturen, wie beispielsweise auf das LUP-Klinikum Helene von Bülow gGmbH im Februar 2025, dass die medizinische Versorgung über Monate deutlich eingeschränkt wird und Patientinnen und Patienten mittelbar in Lebensgefahr geraten können.

Die Gefahren und Risiken durch den Einsatz von Informationstechnik gehen dabei aber nicht nur von cyberkriminellen Aktivitäten aus. Auch Nachlässigkeiten im Regelbetrieb von informations- und kommunikationstechnischen Systemen und digitaler Infrastrukturen, wie fehlerhafte Konfigurationen, die Nutzung nicht mehr vom Hersteller unterstützter Software, der sorglose Umgang mit E-Mails oder unbedachtes Surfen im Internet, bergen erhebliche Risiken. Vergessen werden darf nicht zuletzt auch die Gefahr, die durch Innentäter drohen kann.

Das Vorhalten effektiver Schutz- und Sicherheitsmaßnahmen durch den Staat ist verfassungsrechtliche Pflicht. Vertrauliche staatliche Informationen, aber auch die der Bürgerinnen und Bürger sind vor Ausspähung, Manipulation und Löschung zu schützen. Hierzu muss die Kommunikation mit und zwischen Verwaltungseinheiten reibungslos funktionieren, um insbesondere in Krisensituationen einen reibungslosen Informationsaustausch sowie die Handlungsfähigkeit des Staates zu gewährleisten.

Die Gewährleistung der Informationssicherheit erfordert einen umfassenden und ganzheitlichen Ansatz, der umgesetzte technische und organisatorische Schutz- und Sicherheitsmaßnahmen auf Basis von Sicherheitsanforderungen mit rechtlichen Regelungen verbindet. Deshalb ist hierfür neben den Behörden, Einrichtungen und Institutionen des Landes auch die kommunale Ebene einzubeziehen.

Für digitale Verwaltungsdienstleistungen sowie für das Zusammenwirken staatlicher und kommunaler Stellen im Land Mecklenburg-Vorpommern, den damit verbundenen Datenaustausch, auch mit anderen Ländern und dem Bund, bildet das Corporate Network Landeskommunikationsvermittlungs- und Informationsnetz (CN LAVINE) die essenzielle Informations- und Kommunikationsinfrastruktur, das essenzielle Rückgrat beim Einsatz von Informationstechnik. Die herausgehobene und fundamentale Bedeutung von Kommunikations- und Datennetzen der öffentlichen Verwaltung nimmt beim Einsatz von Informationstechnik eine besondere Rolle ein, die es besonders zu schützen gilt.

Zusammengefasst müssen zum Schutz zahlreicher höchster Rechtsgüter einheitlich definierte qualitative und quantitative Sicherheitsstandards normiert werden, die im Bereich der Informationssicherheit ein einheitliches und messbares Sicherheitsniveau für alle Behörden, Einrichtungen und Institutionen der Landes- und Kommunalverwaltung des Landes Mecklenburg-Vorpommern, auch wenn sie privatrechtlich organisiert sind, festlegen.

Die Regelungen des Bundes, insbesondere die des BSI-Gesetzes und die darauf bezogene BSI-KritisV, sind in ihrer Wirkungsmacht begrenzt, da sie durch die grundgesetzliche Kompetenzverteilung zwischen Bund und Ländern nur begrenzt in die Länder hineinwirken können.

B Lösung

Das Land Mecklenburg-Vorpommern gibt sich ein Gesetz zur Neuordnung und Förderung der Informationssicherheit im Land Mecklenburg-Vorpommern, das in Artikel 1 das Gesetz zur Gewährleistung der Informationssicherheit in Mecklenburg-Vorpommern (Informationssicherheitsgesetz Mecklenburg-Vorpommern – ISichG M-V) enthält und in Artikel 2 das Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (E-Government-Gesetz Mecklenburg-Vorpommern – EGovG M-V) an die Bestimmungen des ISichG M-V anpasst. Das Land Mecklenburg-Vorpommern reagiert damit auf die Risiken, die sich aus der stetigen Verwaltungsdigitalisierung ergeben. Es legt grundlegende Anforderungen fest, die zur Erreichung der in den Begriffsbestimmungen definierten Schutzziele zwingend umzusetzen und aufrechtzuhalten sind.

In diesem Kontext ist ebenfalls die bestehende Informationssicherheitsorganisation der Landesverwaltung weiterzuentwickeln und die kommunale Ebene in diese Informationssicherheitsorganisation zu integrieren. Somit wird der seit dem Jahr 2014 begonnene Prozess staatlicher und kommunaler Zusammenarbeit auf dem Gebiet der Informationssicherheit durch das Gesetz verstetigt, um gemeinsam ein angemessenes Informationssicherheitsniveau sicherzustellen. Nur durch eine enge Zusammenarbeit und den Aufbau gemeinsamer Strukturen kann den komplexen und dynamischen Gefährdungen wirksam begegnet werden.

Die Verantwortung für die Gewährleistung der Informationssicherheit verbleibt unverändert bei jeder einzelnen Stelle. Aufgrund des ZDMVG kann das ZDMV in bestimmten Aufgabenbereichen unterstützend tätig werden und einzelne Funktionen für mehrere Stellen zentral wahrnehmen. Dies ersetzt jedoch nicht die Eigenverantwortung der jeweiligen Behörde für die Gewährleistung der Informationssicherheit.

Der im Gesetz definierte Sicherheitsstandard ist anerkannt und verpflichtet alle öffentlichen und sonstigen Stellen auf ein einheitliches und messbares Sicherheitsniveau. Dabei ist ein nach dem Stand der Technik angemessenes Informationssicherheitsniveau herzustellen, zu dokumentieren und aufrechtzuerhalten. Um dieser gesetzlichen Verpflichtung einen prüfbaren Charakter zu geben, sind der beauftragten Person für Informationssicherheit des Landes (Chief Information Security Officer, CISO M-V – der heutige Beauftragte der Landesverwaltung für Informationssicherheit, BeLVIS), der jeweiligen beauftragten Person für Informationssicherheit einer öffentlichen Stelle (Informationssicherheitsbeauftragte) sowie dem Sicherheitsteam der Landes- und Kommunalverwaltung (CERT M-V) die erforderlichen Befugnisse und Aufgaben in diesem Gesetz festgeschrieben.

Neben den eingangs ausgeführten Gesetzesinhalten werden weitere wesentliche Regelungen durch das Informationssicherheitsgesetz getroffen. So

- sollen die BSI-Standards der 200er Reihe, insbesondere die Sicherheitsanforderungen aus dem BSI IT-Grundschutz-Kompendium, verpflichtend für alle staatlichen und kommunalen Stellen gelten,
- sollen die fachlichen Kompetenzen in einer Informationssicherheitsmanagementorganisation der Landes- und Kommunalverwaltung gebündelt werden,
- sollen die Aufgaben, Kontroll- und Prüfbefugnis, insbesondere die Weisungsbefugnis des Chief Information Security Officers M-V, gefestigt und erweitert werden,
- sollen die Aufgaben und Befugnisse der beauftragten Person für Informationssicherheit definiert werden,
- sollen die Aufgaben, die Unabhängigkeit, insbesondere die datenschutzrechtlichen Befugnisse des CERT M-V bei der Sicherheitsvorfallbehandlung, festgelegt werden,
- sollen die öffentlichen Stellen für eine ziel- und zweckgerichtete, zeitgerechte Erkennung von Gefahren, insbesondere von Cyberangriffen, zum Betrieb von Security Operations Center (SOC) verpflichtet werden,
- sollen die Regelungen zur Verarbeitung von Protokoll-, Verkehrs- und Inhaltsdaten, insbesondere deren Analyse, Auswertung, Zusammenführung, Speicherfristen und Übermittlung an das CERT M-V, festgelegt werden,
- sollen verbindliche Meldepflichten über Sicherheitsvorfälle eingeführt werden sowie
- soll die Regelung zur Datenübermittlung über das CN LAVINE im EGovG M-V weiterentwickelt werden.

Das Informationssicherheitsgesetz Mecklenburg-Vorpommern orientiert sich dabei an der Gesetzgebung anderer Länder, die vergleichbare gesetzliche Regelungen in Kraft gesetzt haben, wie beispielsweise die Freistaaten Sachsen und Bayern oder die Länder Niedersachsen, Hessen oder Baden-Württemberg. Den Anforderungen an die geschlechtergerechte Formulierung der Vorschriften wurde Rechnung getragen.

C Alternativen

Würde der Gesetzentwurf nicht beschlossen werden, gäbe es keine gesetzliche Regelung, wie sich die öffentliche Verwaltung im Land Mecklenburg-Vorpommern inhaltlich und organisatorisch zur Gewährleistung der Informationssicherheit aufstellt. Dies ist jedoch, soweit es um die zuständigen Behörden geht, zur Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) erforderlich.

Es ist ebenfalls mit Blick in andere Länder davon auszugehen, dass die Arbeits- und Handlungsfähigkeit der öffentlichen Verwaltung durch die andauernde, stetig wachsende Bedrohungslage zunehmend gefährdet ist. Eine Resilienz der öffentlichen Verwaltung gegen betriebliche Störungen, Cyberangriffe oder sonstige – auch zukünftige – digitale Bedrohungen wird nicht hergestellt.

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

Die Organisation, die Aufgaben und die Befugnisse, die die im Bereich der Informationssicherheit tätigen Personen erhalten, müssen durch Gesetz bestimmt werden. Nur so kann sichergestellt werden, dass der herausragenden Bedeutung der Informationssicherheit Rechnung getragen wird. Zudem bedarf die erforderliche Verarbeitung personenbezogener Daten im Rahmen der Informationssicherheit nach Artikel 6 Absatz 1 Buchstabe e, Absatz 3 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) einer spezifischen Rechtsgrundlage im Landesrecht.

E Finanzielle Auswirkungen auf die Haushalte des Landes und der Kommunen

1. Haushaltsausgaben ohne Vollzugsaufwand

Keine.

2. Vollzugsaufwand

Der Vollzugsaufwand für das ISichG M-V wird im Rahmen der Ansätze des Haushaltentwurfes 2026/2027 und zugehöriger haushaltsgesetzlicher Ermächtigung dargestellt.

F Sonstige Kosten

Keine.

G Bürokratiefolgen

Durch den Gesetzentwurf werden keine Verwaltungsaufgaben auf Unternehmen übertragen.

Soweit aufgrund im Gesetzentwurf beschriebener Anforderungen organisatorische Maßnahmen bei Unternehmen erforderlich werden, die in den Anwendungsbereich des Gesetzentwurfes fallen, handelt es sich um Anforderungen, die im ureigensten Interesse dieser Unternehmen liegen und somit keine Bürokratiekosten darstellen.

Informationspflichten können für diese Unternehmen oder auch für private Dienstleister, die für Stellen im Anwendungsbereich des Gesetzentwurfes tätig sind, im Rahmen von Kontroll- und Prüfbefugnissen des Chief Information Security Officers M-V bestehen, weil z. B. Auskünfte erteilt oder Unterlagen vorgelegt oder übermittelt werden müssen. Hierbei handelt es sich jedoch um Gefahrenabwehrmaßnahmen, an denen diese Unternehmen mitwirken müssen, nicht um bürokratische Maßnahmen.

**DIE MINISTERPRÄSIDENTIN
DES LANDES
MECKLENBURG-VORPOMMERN**

Schwerin, den 25. November 2025

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

19053 Schwerin

Entwurf eines Gesetzes zur Neuordnung und Förderung der Informationssicherheit im Land Mecklenburg-Vorpommern

Sehr geehrte Frau Präsidentin,

als Anlage übersende ich Ihnen den von der Landesregierung am 25. November 2025 beschlossenen Entwurf des vorbezeichneten Gesetzes mit Begründung.

Ich bitte Sie, die Beschlussfassung des Landtages herbeizuführen.

Federführend ist das Ministerium für Finanzen und Digitalisierung.

Mit freundlichen Grüßen

Manuela Schwesig

ENTWURF

eines Gesetzes zur Neuordnung und Förderung der Informationssicherheit im Land Mecklenburg-Vorpommern

Der Landtag hat das folgende Gesetz beschlossen:

Artikel 1
Gesetz zur Gewährleistung der Informationssicherheit in Mecklenburg-Vorpommern (Informationssicherheitsgesetz Mecklenburg-Vorpommern – ISichG M-V)

Inhaltsübersicht:

Abschnitt 1
Allgemeine Vorschriften

§ 1[1]
Geltungsbereich

(1) Dieses Gesetz gilt für
1. Behörden des Landes sowie der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (staatliche Stellen),
2. Gemeinden, Ämter und Landkreise und alle von ihnen betriebenen oder errichteten Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie Eigenbetriebe (kommunale Stellen) und
3. Unternehmen oder Einrichtungen in einer Rechtsform des privaten Rechts, die systemrelevante Träger der Daseinsvorsorge sind, Aufgaben der öffentlichen Verwaltung wahrnehmen oder an denen öffentliche Stellen einzeln oder gemeinsam über 50 Prozent der Anteile oder Stimmen beteiligt sind (sonstige Stellen).

(2) Beteiligt sich ein Unternehmen oder eine Einrichtung in einer Rechtsform des privaten Rechts, auf die dieses Gesetz Anwendung findet, an einem weiteren Unternehmen oder einer weiteren Einrichtung in einer Rechtsform des privaten Rechts, so findet Absatz 1 Nummer 3 entsprechende Anwendung. Nehmen nicht öffentlich-rechtliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit sonstige Stellen im Sinne dieses Gesetzes.

[1] Dieses Gesetz dient der Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 22.12.2022; L, 2023/90206, 22.12.2023).

(3) Dieses Gesetz gilt nicht für
1. den Landtag,
2. den Landesrechnungshof,
4. Hochschulen, soweit Forschung und Lehre betroffen sind,
5. den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern,
6. die Gerichte und Staatsanwaltschaften.

Die in § 3 festgelegten Grundsätze der Informationssicherheit gelten für die nach Satz 1 Ausgenommenen entsprechend.

Die §§ 11 bis 16 gelten ebenfalls entsprechend, sofern die beauftragte Person für Informationssicherheit der jeweiligen Stelle der Erhebung, Verarbeitung, Veränderung, Speicherung oder Auswertung von Daten zugestimmt hat.

§ 2
Begriffsbestimmungen

Im Sinne dieses Gesetzes bezeichnet der Ausdruck:

1. „öffentliche Stellen“ staatliche und kommunale Stellen;
2. „Daten“ durch Informationstechnik codierte und verarbeitbare Zeichen oder Symbole, die eine Information repräsentieren;
3. „Informationstechnik oder informationstechnische Systeme, Komponenten und Infrastrukturen“ alle technischen Mittel zur Verarbeitung, insbesondere zur Erfassung, Speicherung, Änderung, Archivierung, Übertragung oder Löschung von Daten;
4. „zentrale Informationstechnik“ die Informationstechnik gemäß Nummer 3, die durch eine staatliche Stelle betrieben wird, zur Mitnutzung durch andere öffentliche Stellen bereitgestellt wird und die Eigenschaften essenzieller und kritischer Basis-Informationstechnik besitzt;
5. „Informationssicherheit“ die Gewährleistung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit von Daten und Informationen, unabhängig davon, ob diese mithilfe von Informationstechnik verarbeitetet werden oder nicht;
6. „Informationssicherheitsmanagementsystem“ die Definition und Umsetzung von verbindlichen Prozessen und Regeln, die die Informationssicherheit dauerhaft steuern, kontrollieren, aufrechterhalten und stetig weiterentwickeln;
7. „sicherheitsrelevantes Ereignis“ einen Versuch, ein oder mehrere Schutzziele der Informationssicherheit zu verletzen;
8. „Sicherheitsvorfall“ jedes Vorkommnis, bei dem ein oder mehrere Schutzziele der Informationssicherheit in unzulässiger Weise verletzt werden, wobei ein Sicherheitsvorfall erheblich ist und ein großes Ausmaß besitzt, wenn dieser entweder eine hohe Außenwirkung, eine Vielzahl betroffener Anwender, eine aufwendige Behebung oder einen hohen finanziellen Schaden zur Folge hat, zentrale Informationstechnik oder Dienste, eine Infrastruktur oder eine informationstechnische Komponente mit einem hohen Schutzbedarf betrifft;
9. „Gefahr“ eine Sachlage, bei der die Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein sicherheitsrelevantes Ereignis, ein Sicherheitsvorfall oder ein Schaden für die Arbeits- und Handlungsfähigkeit der öffentlichen Stellen, die Funktionsfähigkeit der Daten- oder Kommunikationsnetze der öffentlichen Verwaltung, eines Rechtsguts oder die Rechtsordnung eintritt;

10. „Schadprogramm“ Software oder sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu verarbeiten oder auf informationstechnische Abläufe oder Funktionen einzuwirken;
11. „Sicherheitslücke“ Eigenschaften von informationstechnischen Systemen oder von Softwareprogrammen, durch deren Ausnutzung es möglich ist, dass Unbefugte Zutritt zu Gebäuden oder zu einzelnen Räumen, Zugang zu Informationstechnik erlangen und Zugriff auf die verarbeiteten Daten erhalten können oder die Funktion der informationstechnischen Systeme in unzulässiger Weise beeinflussen;
12. „Protokolldaten“ beschriebene oder historische Zustände und Aktionen von informationstechnischen Systemen, wobei Protokolldaten Nutzungsdaten gemäß § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 44 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234) geändert worden ist, enthalten und jedes Protokolldatum einen hinreichend hochauflösenden und korrekten Datums- und Zeitstempel enthält;
13. „Verkehrsdaten“ Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten informationstechnischen Systeme verarbeitet werden, wobei diese Daten zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sein müssen;
14. „Inhaltsdaten“ Daten, die den Inhalt einer Kommunikation betreffen und die weder Nutzungsdaten im Sinne des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes noch Verkehrsdaten im Sinne des Telekommunikationsgesetzes sind.
15. „Daten- und Kommunikationsnetze“ die Gesamtheit der technischen Systeme, Komponenten und Dienste, die der elektronischen Übertragung, Verarbeitung, Speicherung oder dem Austausch von Daten zwischen informationstechnischen Systemen oder deren Nutzenden dienen.

§ 3
Grundsätze der Informationssicherheit

(1) Die Stellen gemäß § 1 haben die Informationssicherheit zu gewährleisten, indem sie wirtschaftlich angemessene, auf einem gefahrenübergreifenden Ansatz beruhende organisatorische und technische Maßnahmen festlegen und umsetzen. Die Maßnahmen müssen den Stand der Technik berücksichtigen oder einschlägige branchenspezifische Sicherheitsstandards oder Normen abbilden. Sie umfassen Konzepte und Verfahren für eine regelmäßige Bewertung zu deren Wirksamkeit.

(2) Die Verantwortung für die Informationssicherheit trägt die Leitung einer öffentlichen oder sonstigen Stelle. Dafür plant, erstellt und pflegt sie ein Informationssicherheitsmanagementsystem und berücksichtigt die dafür erforderlichen Haushaltsmittel im Rahmen der Haushaltsaufstellung. Sie benennt eine beauftragte Person für Informationssicherheit (ISB). Für Schulen in öffentlicher Trägerschaft im Sinne des Schulgesetzes erfüllt der Schulträger die Aufgaben nach den Sätzen 2 und 3.

(3) Jede Leitung einer öffentlichen Stelle muss nachweislich sowie regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Informationssicherheit und deren Auswirkungen zu erhalten. Die Teilnahme ist gegenüber der beauftragten Person des Landes für Informationssicherheit Mecklenburg-Vorpommern (Chief Information Security Officer M-V) nachzuweisen. Das zur Wahrnehmung von delegierten Aufgaben in einem Informationssicherheitsmanagementsystem eingesetzte Personal, insbesondere die beauftragte Person für Informationssicherheit, muss über die erforderliche Fachkunde und Zuverlässigkeit verfügen. Die erforderliche Fachkunde wird durch eine für das Aufgabengebiet geeignete Ausbildung, durch nachweisbare praktische Erfahrung sowie durch eine regelmäßige Teilnahme an vom Chief Information Security Officer M-V anerkannten Schulungen oder Workshops erworben.

(4) Für die Gewährleistung der Informationssicherheit ist der IT-Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik verpflichtend. Die für alle öffentlichen Stellen anzuwendende Fassung wird durch die Kommission für Informationssicherheit festgelegt. Für die sonstigen Stellen gelten die Sätze 1 und 2 nur, wenn kein branchenspezifischer Sicherheitsstandard oder keine Norm existiert. Die Kennzeichnung und Klassifizierung von Informationen erfolgt für die öffentlichen Stellen nach den Vorgaben des Traffic-Light-Protocols (TLP) in der jeweils gültigen Fassung. Diese Verpflichtung tritt für die kommunalen Stellen [einsetzen: Datum des ersten Tages des vierundzwanzigsten auf die Verkündung folgenden Kalendermonats] in Kraft. Bis zu diesem Zeitpunkt ist das IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung für die kommunalen Stellen anzuwenden.

(5) Sofern Organisationen Informationstechnik nutzen, die im Eigenbetrieb von einer oder von mehreren Stellen oder im Auftrag von einer oder mehreren Stellen durch einen IT-Dienstleister betrieben wird, hat die verfahrensverantwortliche Stelle den IT-Dienstleister zu verpflichten, den IT-Grundschutz gemäß Absatz 4 anzuwenden und die nutzende Organisation zur Umsetzung der Sicherheitsanforderungen aus dem zugrunde liegenden Sicherheitskonzept zu verpflichten. Für die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH ist die Anwendung und Umsetzung des IT-Grundschutzes gemäß Absatz 5 im Rahmen der Aufgabenübertragung gemäß dem Datenverarbeitungszentrumsgesetz verpflichtend.

(6) Eine Betriebsaufnahme sowie alle nach erfolgter Betriebsaufnahme vorgenommenen wesentlichen Änderungen an der Informationstechnik oder an den Sicherheitsprozessen dürfen nur im Einvernehmen zwischen der verfahrensverantwortlichen Stelle und der für diese öffentliche Stelle ernannten beauftragten Person für Informationssicherheit erfolgen. Die Entscheidung trifft grundsätzlich die Leitung der verfahrensverantwortlichen Stelle. Für die zentrale Informationstechnik bedarf zusätzlich jede Betriebsaufnahme oder wesentliche Änderung des Einvernehmens mit dem Chief Information Security Officer M-V. Wird das Einvernehmen nicht hergestellt, entscheidet die beauftragte Person der Landesregierung Mecklenburg-Vorpommern für Informationstechnologie und Digitalisierung (CIO M-V) über die Maßnahmen zur Risikobehandlung. Soll von Entscheidungen des Chief Information Security Officers M-V abgewichen werden, ist diese Entscheidung gesondert zu begründen.

(7) Die Landesverwaltung ist verpflichtet, die für die Gewährleistung der Informationssicherheit erforderlichen Mittel aus den für IT-Maßnahmen veranschlagten Landeshaushaltsmitteln für Informationssicherheit (Sicherheitskosten) bereitzustellen. Bei allen Digitalisierungsvorhaben, insbesondere bei IT-Projekten, sind die Sicherheitskosten einzuplanen und bei Betriebsverträgen auszuweisen.

(8) Auf den Einsatz von Informationstechnik ist im begründeten Einzelfall zu verzichten, wenn die notwendigen Maßnahmen zur Gewährleistung der Informationssicherheit in keinem angemessenen Verhältnis zu den gegenüberstehenden Risiken stehen. Die Entscheidung trifft grundsätzlich die Leitung der verfahrensverantwortlichen Stelle. Für die zentrale Informationstechnik entscheidet der Chief Information Security Officer M-V im Einvernehmen mit der oder dem CIO M-V. Wird das Einvernehmen nicht hergestellt und wird von den Entscheidungen des Chief Information Security Officers M-V abgewichen, entscheidet abschließend die für Digitalisierung zuständige oberste Landesbehörde über die Maßnahmen zur Risikobehandlung. Diese Entscheidung ist gesondert und dokumentiert zu begründen.

§ 4
Verordnungsermächtigungen

(1) Die für die Digitalisierung zuständige oberste Landesbehörde wird ermächtigt, durch Rechtsverordnung die Verarbeitung, die Erhebung, Speicherung, Archivierung, Übertragung und Auswertung von Protokoll-, Verkehrs- und Inhaltsdaten öffentlicher Stellen zu regeln. Die Regelungen sollen sich insbesondere beziehen auf

1. die Ertüchtigung der IT-Infrastruktur zur Wahrnehmung der Protokollierung, den Umfang der Protokoll- und Verkehrsdatenerhebung sowie deren Auswertung,
2. den Umfang der zur Gefahrenabwehr erforderlichen Analyse von verschlüsseltem Netzwerkverkehr,
3. die Bereitstellung und -übermittlung von Protokoll- und Verkehrsdaten bei einem erheblichen Sicherheitsvorfall an das Sicherheitsteam der Landes- und Kommunalverwaltung (CERT M-V),
4. die Voraussetzungen zur Aufgabenübertragung an privatrechtlich organisierte Dienstleister, öffentliche Stellen des Landes, anderer Länder oder des Bundes,
5. die Kontrolle der ordnungsgemäßen Anwendung und Umsetzung der durch Rechtsverordnung getroffenen Regelungen.

(2) Die für den Verfassungsschutz zuständige oberste Landesbehörde wird ermächtigt, im Benehmen mit der für die Digitalisierung zuständigen obersten Landesbehörde durch Verordnung für Bereiche, Systeme oder Informationen, die dem Geheimschutz unterliegen, zu bestimmen,

1. in welchem Umfang und in welcher Art sowie an welche Stellen die auf Grundlage der Verordnungen nach § 4 und die nach § 16 dieses Gesetzes vorgesehenen Meldungen zu erfolgen haben, sowie
2. den Umfang und die Ausgestaltung der nach diesem Gesetz vorgesehenen Kontrollbefugnisse und Kontrollen.

(3) Die für die Digitalisierung zuständige oberste Landesbehörde wird ermächtigt, im Einvernehmen mit den jeweils datenschutzrechtlich Verantwortlichen nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 und § 4 Absatz 1 des Landesdatenschutzgesetzes durch Rechtsverordnung die Verteilung der Pflichten und Aufgaben nach Artikel 26 der Verordnung (EU) 2016/679 festzulegen.

Abschnitt 2
Organisationsstrukturen der Informationssicherheit

§ 5
Beauftragte Person für Informationssicherheit des Landes

(1) Der Chief Information Security Officer M-V wird von der oder dem CIO M-V ernannt. Die Wahrnehmung dieser Funktion obliegt einem Beschäftigten der für die Digitalisierung zuständigen obersten Landesbehörde. Der Chief Information Security Officer M-V nimmt die übertragenen Aufgaben unabhängig und weisungsfrei wahr. Für seine Aufgabenwahrnehmung wird er angemessen ausgestattet. Der Chief Information Security Officers M-V hat ein direktes Vortragsrecht bei der oder dem CIO M-V und der Leitung der für die Digitalisierung zuständigen obersten Landesbehörde des Landes Mecklenburg-Vorpommern.

(2) Der Chief Information Security Officer M-V darf wegen seiner Tätigkeiten oder wegen der Erfüllung seiner Aufgaben nicht benachteiligt oder begünstigt werden. Eine Abordnung, Umsetzung oder Versetzung des Chief Information Security Officers M-V ist unzulässig. Der Chief Information Security Officer M-V steht in einem Beamtenverhältnis zum Land Mecklenburg-Vorpommern.

(3) Der Chief Information Security Officer M-V vertritt das Land Mecklenburg-Vorpommern in allen Angelegenheiten der Informations- oder Cybersicherheit in der öffentlichen Verwaltung gegenüber dem Bund und anderen Ländern. Er ist für die Weiterentwicklung des Informationssicherheitsmanagementsystems der Landesverwaltung Mecklenburg-Vorpommern zuständig. Zu diesem Zweck obliegt es dem Chief Information Security Officer M-V,

1. landesspezifische Richtlinien und Sicherheitsstandards zu erstellen und diese im Benehmen mit der Kommission für Informationssicherheit gemäß § 6 in Kraft zu setzen,
2. landesspezifische technische und organisatorische Standards und Richtlinien zur Protokollierung und Betrieb eines Security Operation Centers (SOC) zu erstellen und weiterzuentwickeln,
3. öffentliche Stellen bei der Anwendung der landesspezifischen Richtlinien und Sicherheitsstandards, insbesondere bei der Umsetzung der Sicherheitsanforderungen, zu beraten,
4. nähere Bestimmungen zur Qualifikation der Informationssicherheitsbeauftragten in den staatlichen Stellen festzulegen,
5. nähere Festlegungen zur Erfassung von Sicherheitskosten (Kostencontrolling) zu treffen,
6. Inhalte, Dauer und Zeiträume für die regelmäßig von den Leitungen verpflichtend zu absolvierenden Schulungen zu bestimmen und
7. die Maßnahmen des CERT M-V gemäß § 9 Absatz 7 durch Bestimmungen zu ändern.

Der Chief Information Security Officer M-V berichtet regelmäßig der oder dem CIO M-V im Lenkungsausschuss E-Government nach § 17 des E-Government-Gesetzes Mecklenburg-Vorpommern und in der Kommission für Informationssicherheit über seine Tätigkeit. Darüber hinaus berichtet er jährlich der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern zu durchgeführten Maßnahmen der Protokollierung gemäß §§ 12 bis 15 und 19 dieses Gesetzes.

(4) Der Chief Information Security Officer ist die zuständige Behörde nach Artikel 8 Absatz 1 und 2 der Richtlinie (EU) 2022/2555 für die Aufsicht über die staatlichen Stellen. Er meldet dem Bundesamt für Sicherheit in der Informationstechnik die nach § 6 Absatz 8 identifizierten staatlichen Stellen erstmals sechs Monate nach Inkrafttreten dieses Gesetzes und anschließend alle zwei Jahre.

(5) Zur Überprüfung des Erfüllungsgrades der Richtlinien, Sicherheitsstandards sowie der Wirksamkeit des Informationssicherheitsmanagementsystems haben die öffentlichen und sonstigen Stellen dem Chief Information Security Officer M-V die hierfür erforderlichen Unterlagen innerhalb einer angemessenen Frist zu übersenden oder einer beauftragten Person vorzulegen. Der Chief Information Security Officer M-V ist berechtigt, Sicherheitsprüfungen bei den öffentlichen oder sonstigen Stellen selbst vorzunehmen oder diese durchführen zu lassen. Die öffentlichen Stellen unterrichten den Chief Information Security Officer M-V über durchgeführte Sicherheitsprüfungen sowie über deren Ergebnisse. Von den Kontroll- und Prüfbefugnissen des Chief Information Security Officers M-V sind unmittelbar die von den öffentlichen und sonstigen Stellen beauftragten Dienstleister umfasst.

(6) Um Gefahren für die Informationstechnik öffentlicher Stellen abzuwehren, kann der Chief Information Security Officer M-V gegenüber allen unmittelbar oder mittelbar an die Daten- oder Kommunikationsnetze der öffentlichen Verwaltung angeschlossenen öffentlichen Stellen oder sonstigen anschlussberechtigen Organisationen Anordnungen treffen oder Maßnahmen unmittelbar ergreifen. Zur Eindämmung oder Abwehr von erheblichen Sicherheitsvorfällen darf er vorübergehende Netztrennungen oder die Abschaltung von Informationstechnik anordnen. Über die Anordnungen nach Satz 2 sind die Leitung sowie die für diese Stelle benannte beauftragte Person für Informationssicherheit unverzüglich zu informieren.

(7) Die Netztrennungs- und Abschaltungsbefugnis im Sinne des Absatzes 6 des Chief Information Security Officers M-V umfasst ebenfalls alle Betreiber von Daten- oder Kommunikationsnetzen der öffentlichen Verwaltung.

(8) Der Chief Information Security Officer M-V ist verpflichtend in alle Gesetzgebungsverfahren und anderen Regierungsvorhaben des Landes mit wesentlichen Auswirkungen auf die Gestaltung der Informationssicherheit der öffentlichen Verwaltung einzubeziehen.

§ 6
Kommission für Informationssicherheit

(1) Die Kommission für Informationssicherheit wird von dem Chief Information Security Officer M-V geleitet. Sie besteht aus den folgenden stimmberechtigten Mitgliedern:

1. ein Vertretender aus jedem Ressort der Landesverwaltung oder deren Geschäftsbereichen,
2. ein Vertretender des Zweckverbandes Elektronische Verwaltung Mecklenburg-Vorpommern,
3. zwei Vertretende des Städte- und Gemeindetages Mecklenburg-Vorpommern e. V.,
4. zwei Vertretende des Landkreistages Mecklenburg-Vorpommern e. V.

(2) Die stimmberechtigten Mitglieder nach Absatz 1 Nummer 1 werden durch die Ressorts vorgeschlagen und von der oder dem CIO M-V ernannt.

(3) Die nach Absatz 1 Nummer 1 bis 4 aufgeführten Organisationen benennen neben dem namentlich stimmberechtigten Mitglied namentlich die jeweiligen Stellvertretungen. Weitere, nicht stimmberechtigte Mitglieder oder Gäste können an den Sitzungen der Kommission für Informationssicherheit zugelassen werden. Die Sitzungen der Kommission für Informationssicherheit sind nicht öffentlich.

(4) Die stimmberechtigten Mitglieder der Kommission für Informationssicherheit sind durch ihre Organisationen nach Sachkunde und fachlichen Kompetenzen und Fähigkeiten in der Informationstechnik, Informationssicherheit, in der Durchführung von Sicherheitsprüfungen und im Kommunal- und Landesrecht auszuwählen.

(5) Die Kommission für Informationssicherheit berät den Chief Information Security Officer M-V. Entscheidungen des Chief Information Security Officers M-V erfolgen im Benehmen mit der Kommission für Informationssicherheit.

(6) Die Kommission für Informationssicherheit gibt sich eine Geschäftsordnung. Absatz 5 findet bei Beschlussfassungen zur Geschäftsordnung keine Anwendung.

(7) Zu den Aufgaben der Kommission für Informationssicherheit gehören insbesondere die
1. Mitwirkung bei der Erarbeitung und Fortschreibung von Richtlinien und Sicherheitsstandards zur Informationssicherheit des Landes Mecklenburg-Vorpommern,
2. Prüfung von Richtlinien und Sicherheitsstandards zur Informationssicherheit auf Einhaltung und deren Erfüllungsgrad,
3. Entwicklung und Überwachung von Kennzahlen zur Bewertung der Informationssicherheit im Land Mecklenburg-Vorpommern,
4. Beratung, Mitwirkung bei der Erstellung und Prüfung von Sicherheitskonzepten, zentraler Informationstechnik und E-Government-Basisdiensten,
5. Freigabe zur Betriebsaufnahme neuer zentraler Informationstechnik und E-Government-Basisdienste,
6. Entscheidung über die Änderung von Sicherheitsmaßnahmen zentraler Informationstechnik und E-Government-Basisdiensten,
7. Mitwirkung bei Umsetzungs- und Wirksamkeitskontrollen von Sicherheitsmaßnahmen zentraler Informationstechnik und E-Government-Basisdiensten und
8. Mitwirkung bei der Erprobung neuer Sicherheitstechnologien im Sinne des § 19.

(8) Die Kommission für Informationssicherheit beschließt ein Konzept zur Identifizierung der staatlichen Stellen nach Artikel 2 Absatz 2 Buchstabe f Ziffer ii der Richtlinie (EU) 2022/2555. Die obersten Landesbehörden identifizieren auf der Grundlage dieses Konzeptes die in ihrem Geschäftsbereich betroffenen staatlichen Stellen und übermitteln dem Chief Information Security Officer M-V die Daten der von ihnen erstmals oder erneut identifizierten staatlichen Stellen:

1. den Namen der staatlichen Stelle,
2. die Anschrift und die aktuellen Kontaktdaten der zuständigen beauftragten Person für Informationssicherheit der staatlichen Stelle einschließlich E-Mail-Adresse und Telefonnummer,
3. die IP-Adressbereiche der staatlichen Stelle.

Die erste Identifizierung nehmen die obersten Landesbehörden sechs Monate nach Inkrafttreten dieses Gesetzes vor und überprüfen diese alle zwei Jahre.

§ 7
Beauftragte Personen für Informationssicherheit

(1) In jeder öffentlichen Stelle ist eine beauftragte Person für Informationssicherheit sowie eine Stellvertretung namentlich zu benennen. Die beauftragte Person für Informationssicherheit und deren Stellvertretung können für mehrere Stellen zuständig sein, sofern für ihre Aufgabenwahrnehmung ausreichende Ressourcen zur Verfügung stehen. Dabei muss sichergestellt sein, dass keine Interessenkonflikte entstehen. Abweichend von Satz 2 ist in der zentralen Stelle für informationstechnische Dienste der Steuerverwaltung eine beauftragte Person für Informationssicherheit sowie Stellvertretung einzurichten.

(2) Die Landespolizei benennt in den Polizeibehörden gemäß § 2 Absatz 1 Nummer 2 bis 6 des Polizeiorganisationsgesetzes jeweils eine beauftragte Person für Informationssicherheit und eine Stellvertretung. Die beauftragte Person für Informationssicherheit und deren Stellvertretung können für mehrere Polizeibehörden zuständig sein, sofern keine Interessenkonflikte entstehen. Des Weiteren benennt die oberste Polizeibehörde eine hauptamtliche beauftragte Person für Informationssicherheit als Chief Information Security Officer der Landespolizei, welche für die gesamte Landespolizei sowie für die Informationstechnik der Landespolizei, die in anderen Behörden eingesetzt wird, zuständig ist. Für die Polizeibehörden nach Nummer 2 bis 4 und 6 sollen die beauftragten Personen für Informationssicherheit hauptamtlich tätig sein, sofern für ihre Aufgabenwahrnehmung ausreichende Ressourcen zur Verfügung stehen.

(3) Die beauftragte Person für Informationssicherheit der obersten und oberen Landesbehörden sowie deren Stellvertretung müssen Beschäftigte des Landes sein.

(4) Für Schulen in öffentlicher Trägerschaft im Sinne des Schulgesetzes ist die beauftragte Person für Informationssicherheit die zuständige beauftragte Person für Informationssicherheit des jeweiligen Schulträgers. Hiervon kann abgewichen werden, wenn aufgrund der Größe einer Schule (ab 750 Schüler) eine beauftragte Person für Informationssicherheit durch den Schulträger benannt wird.

(5) Die beauftragte Person für Informationssicherheit berichtet der Leitung in angemessenen, zeitlich regelmäßigen Abständen sowie dem Chief Information Security Officer M-V jährlich und anlassbezogen zum Stand der Informationssicherheit in ihrem Zuständigkeitsbereich.

(6) Jede beauftragte Person für Informationssicherheit besitzt ein unmittelbares Vortragsrecht gegenüber der Leitung. Darüber hinaus besitzen die beauftragten Personen für Informationssicherheit ein unmittelbares Vortragsrecht gegenüber dem Chief Information Security Officer M-V.

(7) Eine beauftragte Person für Informationssicherheit fördert alle Belange der Informationssicherheit innerhalb ihres Zuständigkeitsbereichs, koordiniert, überwacht und kontrolliert alle Maßnahmen zur Gewährleistung der Informationssicherheit. Sie ist für die Einhaltung der Melde- und Berichtspflichten in ihrem Zuständigkeitsbereich zuständig. Bei einem Sicherheitsvorfall ist sie berechtigt, Einsicht in die IT-Dokumentation, in das Sicherheitskonzept und Protokolldaten ihres Zuständigkeitsbereichs zu nehmen oder diese bei der verfahrensverantwortlichen Stelle zur Einsichtnahme anzufordern.

(8) Der Chief Information Security Officer M-V, die Kommission für Informationssicherheit sowie das CERT M-V sind unverzüglich über die Ernennung oder über einen personellen Wechsel einer beauftragten Person für Informationssicherheit in öffentlichen Stellen zu unterrichten.

§ 8
Verfahrensverantwortliche Stellen

(1) Für alle Verwaltungsprozesse, insbesondere die durch Informationstechnik unterstützten, sind verfahrensverantwortliche Stellen zu benennen. Die verfahrensverantwortlichen Stellen erstellen das Sicherheitskonzept und setzen alle Sicherheitsanforderungen um, die sich aus dem für den Betrieb erforderlichen Sicherheitskonzept sowie aus den Richtlinien und Sicherheitsstandards für ihren jeweiligen Verwaltungsprozess ergeben.

(2) Die verfahrensverantwortliche Stelle ist im Fall eines sicherheitsrelevanten Ereignisses oder eines Sicherheitsvorfalls zur uneingeschränkten Zusammenarbeit mit der beauftragten Person für Informationssicherheit, dem Chief Information Security Officer M-V sowie mit dem CERT M-V verpflichtet. Alle notwendigen Auskünfte sind unverzüglich zu erteilen.

§ 9
Sicherheitsteam der Landes- und Kommunalverwaltung, Verordnungsermächtigung

(1) Das Land Mecklenburg-Vorpommern betreibt für alle öffentlichen Stellen ein Sicherheitsteam der Landes- und Kommunalverwaltung (CERT M-V). Die für die Digitalisierung zuständige oberste Landesbehörde wird ermächtigt, durch Rechtsverordnung die Aufgaben und Dienste des CERT M-V zu bestimmen. In der Rechtsverordnung sind mindestens folgende Aufgaben festzulegen:

Das CERT M-V
1. behandelt und zeigt Lösungen bei Sicherheitsvorfällen auf,
2. betreibt einen Warn-, Informations- und Alarmierungsdienst für bewertete Sicherheitslücken in der Informationstechnik,
3. betreibt ein Schwachstellenmanagementsystem, führt Schwachstellenanalysen für die Informationstechnik der öffentlichen Stellen durch und erarbeitet Lösungen zu deren Beseitigung,
4. prüft die Informationstechnik auf Risiken und unterstützt bei deren Beseitigung,
5. erfasst und analysiert die Sicherheitslage und erstellt ein landesspezifisches Lagebild sowie abgeleitete Maßnahmenempfehlungen,
6. wirkt bei der technischen und technologischen Koordinierung der Informationssicherheit in den öffentlichen Stellen mit,
7. ist zentrale Meldestelle im Verwaltungs-CERT-Verbund sowie weiterer CERT-Verbünde.

Weitere Aufgaben dürfen dem CERT M-V nur im Einvernehmen mit dem Chief Information Security Officer M-V übertragen werden. Er hat die Fachaufsicht über das CERT M-V.

(2) Das CERT M-V unterstützt den Chief Information Security Officer M-V, die beauftragte Person für Informationssicherheit sowie die Datenschutzbeauftragten der öffentlichen Stellen bei sicherheitstechnischen Fragestellungen.

(3) Zur Wahrnehmung seiner Aufgaben und Dienste hat das CERT M-V alle für die Abwehr von Gefahren erforderlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, zu versuchten und erfolgreichen Angriffen auf die Informationstechnik sowie die bei den Angriffen detektierten Vorgehensweisen und Protokolldaten zu sammeln und auszuwerten. Das CERT M-V ist im Sinne des Satzes 1 berechtigt, Informationen mit dem Bundesamt für Sicherheit in der Informationstechnik sowie mit den Sicherheitsbehörden von Bund und den Ländern auszutauschen.

(4) Alle öffentlichen Stellen sowie die durch die öffentlichen Stellen beauftragten IT-Dienstleister stellen dem CERT M-V alle für die Zwecke nach Absatz 3 notwendigen Informationen und Daten unverzüglich und unentgeltlich je nach Anforderung entweder kontinuierlich oder auf Aufforderung zur Verfügung. Die im Rahmen dieser Aufgabenwahrnehmung erforderliche Datenverarbeitung erfolgt beim CERT M-V.

(5) Für seine Aufgabenwahrnehmung muss das CERT M-V redundant sowohl räumlich als auch mit eigener, von der zentralen Informationstechnik entkoppelter Informationstechnik ausgestattet sein, um seine hohe Verfügbarkeit jederzeit zu gewährleisten. Dies umfasst

1. eine geeignete, sichere und resiliente Kommunikations- und Informationsinfrastruktur mit einer anforderungs- und leistungsgerechten Anzahl an Kommunikationskanälen,
2. eine geeignete Informationstechnik zur Verwaltung und Analyse von Sicherheitsvorfällen, Weiterleitung von Anfragen und Informationen, insbesondere zur sicheren Übermittlung und Bereitstellung von Informationen, und
3. gemäß § 9 des Sicherheitsüberprüfungsgesetzes sicherheitsüberprüftes Personal, das die ständige Bereitschaft der CERT-Aufgaben gewährleistet.

§ 10
Weitere Sicherheitsteams

(1) Jede öffentliche Stelle betreibt ein Security Operations Center oder schließt sich einem gemeinsamen oder externen SOC an. Dies erfolgt mit dem Ziel, versuchte oder erfolgreiche Angriffe auf ihre eigenen oder im Auftrag der öffentlichen Stellen betriebene Informationstechnik detektieren und abwehren zu können. Die SOC sind insbesondere bei Sicherheitsvorfällen zur bilateralen Zusammenarbeit mit dem CERT M-V verpflichtet. Sie stellen dem CERT M-V alle zur Gefahrenabwehr sowie für die Erstellung eines landesspezifischen Lagebildes gemäß § 9 Absatz 1 Nummer 4 erforderlichen Informationen und Daten unentgeltlich zur Verfügung.

(2) Für alle staatlichen Stellen betreibt die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH ein SOC. Kommunale Stellen können einzeln oder gemeinsam oder durch einen IT-Dienstleister ein SOC betreiben.

(3) Die Kernaufgaben eines SOC umfassen insbesondere
1. den Betrieb eines zentralen Protokollierungssystems sowie von Sicherheitssystemen zur Erkennung und Abwehr von Angriffen,
2. die selbstständige Erkennung, Bearbeitung, Analyse und Überwachung von sicherheitsrelevanten Ereignissen und
3. die Meldung von Sicherheitsvorfällen, die Bereitstellung von detektierten oder analysierten Vorgehensweisen und deren Protokolldaten von Angriffen gegenüber der zuständigen beauftragten Person für Informationssicherheit sowie gegenüber dem CERT M-V.

(4) Die SOC unterliegen bei der Datenverarbeitung im Rahmen ihrer Aufgabenwahrnehmung der Kontrolle des Chief Information Security Officers M-V.

Abschnitt 3
Maßnahmen zur Abwehr von Gefahren für die informationstechnischen Systeme und Infrastrukturen

§ 11
Grundsätze für die Verarbeitung personenbezogener Daten, Datenschutzkontrolle

(1) Das CERT M-V ist berechtigt, personenbezogene Daten zum Zwecke der Auswertung oder Untersuchung von Informationen zu Sicherheitslücken, Schadprogrammen, versuchten oder erfolgten Angriffen auf die informationstechnischen Systeme und Infrastrukturen sowie die bei den Angriffen detektierten Vorgehensweisen und Protokolldaten zu verarbeiten, wenn die Verarbeitung zur Gewährleistung der Informationssicherheit erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse einer betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Die Verarbeitung aller diesbezüglichen Informationen sowie personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Datenschutz-Grundverordnung ist zulässig, wenn
1. die Verarbeitung zur Analyse, Entwicklung von Schutzmaßnahmen sowie nachgelagert zur Abwehr einer erheblichen Gefahr für die Netz-, Daten- oder Informationssicherheit erforderlich ist oder
2. ein Ausschluss von der Verarbeitung die Aufgabenwahrnehmung des CERT M-V einschränkt oder diese erheblich gefährden würde.

(2) Personenbezogene Daten, die ursprünglich für Zwecke erhoben wurden, die der Richtlinie (EU) 2016/680 in der Fassung vom 27. April 2016 unterliegen, dürfen ebenfalls verarbeitet werden und sind an die nach diesem Gesetz für die Informationssicherheit zuständigen Stellen zu übermitteln, wenn eine Übermittlung zu den Zwecken nach Absatz 1 erforderlich ist oder eine Abtrennung der personenbezogenen Daten vor einer Übermittlung aus Gründen der Informationssicherheit nicht möglich ist.

(3) Besondere Kategorien personenbezogener Daten, deren Verarbeitung nach Artikel 9 Absatz 1 der Datenschutz-Grundverordnung untersagt ist, dürfen ebenfalls verarbeitet werden, wenn und soweit die Verarbeitung zu den Zwecken nach Absatz 2 erforderlich ist oder nicht ausgeschlossen werden kann.

(4) Wenn und soweit der Zweck einer Verarbeitung personenbezogener Daten dies zulässt oder es den Zweck der Verarbeitung nicht gefährdet, sind personenbezogene Daten automatisiert zu pseudonymisieren.

(5) Personenbezogene Daten, die nicht mehr für Zwecke, für die sie erhoben wurden, erforderlich sind, sind unverzüglich zu löschen. Wenn und soweit personenbezogene Daten anstelle der Löschung zu Dokumentationszwecken ausschließlich zur Datenschutzkontrolle weiterhin vorgehalten werden, unterliegen diese Daten einem Verwertungsverbot. Sie sind zwei Jahre nach der Dokumentation zu löschen, es sei denn, die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern zeigt an, dass diese Daten zur Erfüllung ihrer oder seiner Aufgaben weiterhin benötigt werden.

(6) Wenn und soweit in diesem Gesetz Kontrollpflichten geregelt sind, so bleiben die Aufgaben und Befugnisse der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit nach dem Landesdatenschutzgesetz unberührt.

(7) Jede öffentliche Stelle kann ihre Befugnisse gemäß §§ 12 bis 15 im Einvernehmen mit der für die Digitalisierung zuständigen obersten Landesbehörde an eine andere öffentliche Stelle gemäß § 1 oder Organisation übertragen. Das Recht der kommunalen Zusammenarbeit bleibt unberührt.

§ 12
Datenerhebung und -auswertung von Protokolldaten

(1) Die öffentlichen Stellen können, um Gefahren für die Informationstechnik durch Sicherheitslücken, Schadprogramme oder durch versuchte oder erfolgte Angriffe zu erkennen und abzuwehren, die auf ihrer Informationstechnik zur Erkennung und zur Analyse von Auffälligkeiten gespeicherten Protokolldaten automatisiert auswerten. Nach Satz 1 dürfen ausschließlich die vollständig automatisiert erhobenen Protokolldaten von

1. informationstechnischen Systemen zur Erkennung von unerwünschten Werbe-, Betrugs- oder schädlichen elektronischen Nachrichten,
2. informationstechnischen Systemen zur Erkennung und Beseitigung von Schadprogrammen,
3. Firewall-Systemen sowie informationstechnischen Systemen für den Netzwerkbetrieb,
4. informationstechnischen Systemen von Authentifizierungs-, Web-, Proxy-, Verzeichnisdiensten,
5. informationstechnischen Systemen zur Erfüllung einer oder mehrerer Fachaufgaben,
6. Betriebssystemsoftware auf Rechnersystemen und
7. zentraler Informationstechnik

herangezogen werden. Für eine zweckgerichtete Auswertung dürfen die nach Satz 2 vorliegenden Protokolldaten zusammengeführt und gemeinsam verarbeitet werden.

(2) Die nach Absatz 1 erhobenen Protokolldaten sind nach ihrer automatisierten Auswertung unverzüglich vollständig und unwiderruflich nach dem Stand der Wissenschaft und Technik zu löschen, es sei denn, die automatisierte Auswertung zeigt tatsächliche Anhaltspunkte für eine Gefahr nach Absatz 1 Satz 1 auf. Protokolldaten, die weder personenbezogen sind noch dem Fernmeldegeheimnis unterliegen, sind von den Verarbeitungseinschränkungen dieser Vorschrift ausgenommen.

(3) Der Chief Information Security Officer M-V erlässt im Benehmen mit der Kommission für Informationssicherheit eine Richtlinie, die insbesondere Festlegungen zu den sicherheitsrelevanten Ereignissen und Protokolldaten der nach Absatz 1 Satz 2 genannten Informationstechnik beinhaltet.

(4) Eine Auswertung des während der vollständig automatisierten Erhebung der Protokolldaten nach Absatz 1 Satz 2 anfallenden Inhalts ist nur nach § 15 zulässig.

§ 13
Datenerhebung und -auswertung in Daten- oder Kommunikationsnetzen der öffentlichen Verwaltung

(1) Zur Erkennung und Abwehr von Gefahren für die Daten- oder Kommunikationsnetze der öffentlichen Verwaltung durch Sicherheitslücken, Schadprogramme oder durch versuchte oder erfolgte Angriffe ist die für Digitalisierung zuständige oberste Landesbehörde ermächtigt, an Übergabe- und Knotenpunkten der Daten- oder Kommunikationsnetze der öffentlichen Verwaltung nach auffälligen, abnormalen Datenverkehren zu suchen. Zu diesem Zweck darf der gesamte im Daten- oder Kommunikationsnetz der öffentlichen Verwaltung anfallende Datenverkehr vollständig automatisiert erhoben werden. Es dürfen insbesondere die nachstehenden Verkehrs- und Inhaltsdaten unverzüglich automatisiert ausgewertet werden:

1. Erhebungszeitpunkt, IP-Adresse einschließlich Subnetzmaske, Präfixlänge, Port und Medienzugriffskontrolladresse (Media Access Control Address, MAC-Adresse) vollständiger Domänenname sowie Kopf- und Statusdaten von Netzwerkpaketen für ein- und ausgehende Verbindungen,
2. ein- und ausgehende Verbindungen auf Basis des Hypertext-Übertragungsprotokolls (Hypertext Transfer Protocol, HTTP) zusätzlich zu Nummer 1 den vollständigen einheitlichen Ressourcenzeiger (Uniform Resource Locator, URL) und die Kopfdaten exklusive Cookies,
3. ein- und ausgehende Verbindungen auf Basis des Zeitsynchronisierungsprotokolls (Network Time Protocol, NTP) mit allen Inhalten zu Anfragen und Antworten,
4. ein- und ausgehende Verbindungen von Namensauflösungsprotokollen (Domain Name Service, DNS) mit allen Inhalten zu Anfragen und zu Antworten und
5. ein- und ausgehende Verbindungen von Nachrichtenaustauschprotokollen mit allen Inhalten.

Ungeachtet der Sätze 1 bis 3 darf zur Erkennung und Analyse von auffälligen, abnormalen Verhalten im Datenverkehr eines der nach § 12 Absatz 1 Nummer 3 bis 5 genannten informationstechnischen Systeme oder Dienste deren ein- und ausgehenden Datenverkehr automatisiert erhoben und ausgewertet werden.

(2) Jede öffentliche Stelle kann an den von ihr betriebenen, mit den Daten- oder Kommunikationsnetzen der öffentlichen Verwaltung verbundenen Übergabepunkten nach Maßgabe des Absatzes 1 nach auffälligem, abnormalem Datenverkehr suchen, soweit dies dem Zweck dient, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren abzuwehren. Der an den Übergabepunkten anfallende Datenverkehr darf automatisiert erhoben, entschlüsselt und unverzüglich automatisiert ausgewertet werden.

(3) Werden nach den Absätzen 1 oder 2 Inhalte einer Telekommunikation (Inhaltsdaten) verarbeitet, so ist ihre inhaltliche Auswertung unzulässig. Eine Auswertung des während der vollständig automatisierten Erhebung des Datenverkehrs nach Absatz 1 Satz 2 anfallenden Inhalts ist nur nach § 15 zulässig.

§ 14
Weiterführende Analyse und Auswertung von Protokolldaten

(1) Ergibt die nach § 12 Absatz 1 oder nach § 13 Absatz 1 oder 2 durchgeführte automatisierte Auswertung hinreichende oder tatsächliche Anhaltspunkte dafür, dass zur Abwehr von Gefahren für die Informationstechnik eine weiterführende Analyse erforderlich ist, dürfen diese Daten im Einzelfall weiter automatisiert ausgewertet werden. Die zu diesem Zweck erhobenen und ausgewerteten Daten der Einzelfälle sowie die Auswertungsergebnisse dürfen weiter zusammengeführt und automatisiert ausgewertet werden, soweit dies zur Erkennung oder Abwehr der Gefahr erforderlich ist.

(2) Die verantwortliche Stelle muss die nach Absatz 1 erhobenen Daten unverzüglich automatisiert pseudonymisieren, soweit sie nicht bereits pseudonym sind, und darf sie für diesen Zweck speichern und weiter automatisiert auswerten, soweit dies zur Erkennung oder Abwehr der Gefahr erforderlich ist.

(3) Bestätigt die weiterführende Analyse und Auswertung nach Absatz 1, dass die hinreichenden oder tatsächlichen Anhaltspunkte durch ein Schadprogramm, durch eine Sicherheitslücke oder durch einen Angriff verursacht wurden oder sich aus ihnen entsprechende Hinweise ergeben, so dürfen diese Daten gespeichert, entpseudonymisiert und auch nicht automatisiert ausgewertet werden. Dies gilt nur, soweit und solange die Datenverarbeitung zur Erkennung und Abwehr eines Schadprogramms, einer Sicherheitslücke oder daraus resultierender Gefahren oder Angriffe erforderlich ist. Die weiterführende Auswertung nach Satz 1 bedarf der Anordnung der Leitung.

(4) Nach den Absätzen 1 bis 3 dürfen keine Inhaltsdaten verarbeitet oder ausgewertet werden.

(5) Soweit die nach Absatz 2 ausgewerteten Daten sowie die Auswertungsergebnisse nicht mehr für die dort genannten Zwecke oder eine Übermittlung nach § 10 erforderlich sind, sind sie unverzüglich zu löschen.

§ 15
Analyse und Auswertung von Inhaltsdaten

(1) Ergibt eine automatisierte Auswertung nach § 12 Absatz 1 oder § 13 Absatz 1 und 2 hinreichende oder tatsächliche Anhaltspunkte dafür, dass die Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr erforderlich sind, so kann die Stelle abweichend von § 14 Absatz 4 auch Inhaltsdaten und Auswertungsergebnisse speichern und in dieser Zeitspanne weiter einzelfallbezogen automatisiert auswerten, soweit und solange dies zur Erkennung oder Abwehr der Gefahr erforderlich ist. Die Auswertung der kommunikativen Bedeutung der Inhaltsdaten ist unzulässig. Die nach Satz 1 gespeicherten Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym sind. Die Speicherung nach Satz 1 bedarf der unverzüglichen Genehmigung der Leitung. Wird die Genehmigung abgelehnt oder nicht unverzüglich erteilt, so sind die gespeicherten Inhaltsdaten sowie die Auswertungsergebnisse sofort zu löschen.

(2) Ergibt die Auswertung nach Absatz 1 Satz 1 keine hinreichenden tatsächlichen Anhaltspunkte dafür, dass die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr für die IT-Sicherheit erforderlich sind, so sind die gespeicherten Inhaltsdaten sowie die Auswertungsergebnisse unverzüglich zu löschen.

(3) Bestätigt eine automatisierte Auswertung nach § 12 Absatz 1 oder § 13 Absatz 1 und 2 oder eine weitere automatisierte Auswertung nach Absatz 1 hinreichende tatsächliche Anhaltspunkte dafür, dass die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr erforderlich sind, so dürfen die Daten über den Ablauf der in Absatz 1 Satz 1 bestimmten Frist hinaus gespeichert, entpseudonymisiert und auch nicht automatisiert ausgewertet werden, soweit und solange dies zur Erkennung oder Abwehr der Gefahr erforderlich ist. Die Auswertung der kommunikativen Bedeutung der Inhaltsdaten ist unzulässig. Die weitere Auswertung nach Satz 1 bedarf der Anordnung der Leitung. Ergibt die Auswertung nach Satz 1 tatsächliche Anhaltspunkte für eine andere durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr, so dürfen die Daten auch gespeichert und nicht automatisiert ausgewertet werden, soweit und solange dies zur Erkennung oder Abwehr der anderen Gefahr erforderlich ist; die Sätze 2 und 3 gelten entsprechend.

(4) Soweit die nach Absatz 3 ausgewerteten Daten sowie die Auswertungsergebnisse nicht mehr für die dort genannten Zwecke oder eine Übermittlung nach § 10 erforderlich sind, sind sie unverzüglich zu löschen. Die Tatsache, dass die in Absatz 3 Satz 1 und 2 genannten Daten ausgewertet wurden, und die Löschung dieser Daten sind zu dokumentieren. Die in der Dokumentation enthaltenen Daten dürfen ausschließlich zur Datenschutzkontrolle verwendet werden. Sie sind zwei Jahre nach der Dokumentation zu löschen, es sei denn, die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern zeigt an, dass die Daten zur Erfüllung ihrer oder seiner Aufgaben weiterhin benötigt werden.

Abschnitt 4
Meldepflichten

§ 16
Meldepflichten, Verordnungsermächtigung

(1) Werden in öffentlichen Stellen, die an die Daten- oder Kommunikationsnetze der öffentlichen Verwaltung angeschlossen sind, Informationen bekannt, die zur Abwehr von Gefahren für die Informationstechnik von wesentlicher Bedeutung sind oder sein könnten, teilen sie diese Information unverzüglich dem CERT M-V mit, soweit nicht andere Vorschriften dieser Informationsweitergabe entgegenstehen. Eine Informationsweitergabe ist entbehrlich, sofern gleichlautende Informationen öffentlich bekannt und zugänglich sind.

(2) Öffentliche Stellen haben Sicherheitsvorfälle unverzüglich an das CERT M-V zu melden, wenn es sich um Sicherheitsvorfälle handelt, die
1. zu einer möglichen Beeinträchtigung der Informationssicherheit ihrer Daten- oder Kommunikationsnetze führen könnten oder bereits geführt haben,
2. zu einer Beeinträchtigung ihrer Verwaltungsprozesse führen könnten oder bereits geführt haben oder
3. zu einer Beeinträchtigung von Bürgerdiensten führen könnten oder bereits geführt haben.

Von der Meldepflicht umfasst sind ebenfalls alle Sicherheitsvorfälle bei den Dienstleistern öffentlicher Stellen.

(3) Öffentliche Stellen haben der für den Verfassungsschutz zuständigen obersten Landesbehörde unverzüglich zu melden, soweit Anhaltspunkte für einen nachrichtendienstlichen Hintergrund eines Angriffs vorliegen. Anhaltspunkte im Sinne des Satzes 1 liegen insbesondere vor, wenn es sich um qualifizierte Angriffe mit Eindringungsversuchen handelt, die nicht auf eine kriminelle Gewinnerzielungsabsicht schließen lassen.

(4) Die für die Digitalisierung zuständige oberste Landesbehörde wird ermächtigt, durch Rechtsverordnung die Einzelheiten der Meldepflichten näher zu bestimmen. Die Rechtsverordnung muss Vorgaben zu meldepflichtigen Ereignissen, zum Informationsgehalt der Auskünfte, insbesondere zur Meldekommunikation und -prozessen, enthalten.

(5) Die öffentlichen Stellen übermitteln regelmäßig an das CERT M-V Informationen über sicherheitsrelevante Ereignisse. Dazu gehören insbesondere:

1. statistische Angaben und
2. Protokolldaten aus den Sicherheitssystemen in automatisierter Form.

(6) Für sonstige Stellen gelten die Meldepflichten nach den Absätzen 1 bis 4 nur, soweit deren Informationstechnik mit den Daten- oder Kommunikationsnetzen der öffentlichen Verwaltung verbunden ist und somit eine Datenübertragung über die Daten- oder Kommunikationsnetze der öffentlichen Verwaltung in andere angeschlossene Netzwerke erfolgt. Im Übrigen steht es den sonstigen Stellen frei, sicherheitsrelevante Ereignisse oder Sicherheitsvorfälle an das CERT M-V zu melden.

Abschnitt 5
Schlussvorschriften

§ 17
Auskunftsverlangen

Zugang zu den Informationen und Akten in Angelegenheiten dieses Gesetzes wird nicht gewährt. Die Akteneinsichtsrechte von Verfahrensbeteiligten bleiben unberührt.

§ 18
Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) wird nach Maßgabe der §§ 11 bis 15 eingeschränkt.

§ 19
Experimentierklausel zur Erprobung neuer Sicherheitstechnologien

Die für die Digitalisierung zuständige oberste Landesbehörde kann zur Erprobung neuer Technologien zur Datenanalyse oder -auswertung, die der Abwehr von Gefahren für die informationstechnischen Systeme, Infrastrukturen und Komponenten öffentlicher Stellen dienen, im Einvernehmen mit dem Chief Information Security Officer M-V und mit Zustimmung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern sachlich und örtlich begrenzte Ausnahmen zur Auswertung von anderen, nicht in § 12 Absatz 1 und § 13 Absatz 1 genannten Daten für einen Zeitraum von höchstens drei Jahren zuzulassen.

§ 20
Beschränkung der Rechte betroffener Personen

(1) Abweichend von Artikel 15 der Verordnung (EU) 2016/679 besteht das Recht auf Auskunft nicht, wenn und soweit die Erfüllung einer Auskunftserteilung die Aufgabenwahrnehmung nach diesem Gesetz beeinträchtigen würde. Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Wird der betroffenen Person keine Auskunft erteilt, so ist diese auf Verlangen der Aufsichtsbehörde zu erteilen, soweit nicht die zuständige oberste Landesbehörde für die Informationssicherheit im Einzelfall feststellt, dass dadurch die öffentliche Sicherheit gefährdet würde. Die Mitteilung der Aufsichtsbehörde an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern der Verantwortliche nicht einer weitergehenden Auskunft zugestimmt hat.

(2) Abweichend von Artikel 21 der Verordnung (EU) 2016/679 besteht das Recht auf Widerspruch nicht, wenn und soweit ein Widerspruch gegen die Verarbeitung personenbezogener Daten die Aufgabenwahrnehmung nach diesem Gesetz beeinträchtigen würde und an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt. Darüber hinaus darf die Daten verarbeitende Stelle die personenbezogenen Daten ergänzend zu Artikel 21 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 weiterhin so lange verarbeiten, bis sie geprüft hat, ob zwingende schutzwürdige Gründe für die Verarbeitung bestehen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

Artikel 2
Änderung des E-Government-Gesetzes Mecklenburg-Vorpommern

Das E-Government-Gesetz Mecklenburg-Vorpommern vom 25. April 2016 (GVOBl. M-V S. 198), das zuletzt durch Artikel 1 des Gesetzes vom 9. April 2024 (GVOBl. M-V S. 110) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 5 durch die folgende Angabe ersetzt:

   „§ 5 Nachweisabruf; Nachweiserbringung
   § 5a Grenzüberschreitende Nachweisabrufe“.

2. § 5 wird durch den folgenden § 5 ersetzt:

„§ 5
Nachweisabruf; Nachweiserbringung

(1) Wird ein antragsgebundenes Verwaltungsverfahren elektronisch durchgeführt, erfolgt die Nachweiserbringung auf elektronischem Wege nach Wahl des Antragstellers,
1. indem die nachweisanfordernde Stelle den jeweiligen Nachweis automatisiert bei der nachweisliefernden Stelle abruft, sofern der jeweils erforderliche Nachweis des Antragstellers elektronisch vorliegt und automatisiert abgerufen werden kann, oder
2. indem der Antragsteller den jeweiligen Nachweis elektronisch einreicht.

Die §§ 24 bis 27 des Landesverwaltungsverfahrensgesetzes bleiben unberührt. Die Verantwortung für die Zulässigkeit der Nachweiserhebung und des Nachweisabrufs nach Satz 1 Nummer 1 in Verbindung mit den Absätzen 3 bis 5 trägt die nachweisanfordernde Stelle.

(2) Nachweise im Sinne dieses Gesetzes sind Unterlagen und Daten jeder Art unabhängig vom verwendeten Medium, die zur Ermittlung des Sachverhalts geeignet sind. Nachweisanfordernde Stelle kann die für die Entscheidung über den Antrag zuständige Behörde oder auch eine andere öffentliche Stelle sein, die dafür zuständig ist, Nachweise einzuholen und an die für die Entscheidung über den Antrag zuständige Behörde weiterzuleiten. Nachweisliefernde Stelle ist diejenige öffentliche Stelle, die dafür zuständig ist, den Nachweis auszustellen.

(3) Hat sich der Antragsteller für den automatisierten Nachweisabruf entschieden, darf die nachweisanfordernde Stelle den Nachweis des Antragstellers bei der nachweisliefernden Stelle abrufen und die nachweisliefernde Stelle darf den Nachweis an die nachweisanfordernde Stelle übermitteln, wenn
1. dies zur Erfüllung der Aufgabe der nachweisanfordernden Stelle erforderlich ist und
2. die nachweisanfordernde Stelle den Nachweis auch aufgrund anderer Rechtsvorschriften beim Antragsteller erheben dürfte.

Die in Absatz 2 Satz 2 genannte andere öffentliche Stelle darf den Nachweis an die für die Entscheidung über den Antrag zuständige Stelle übermitteln. Die Datenübermittlungen zwischen öffentlichen Stellen nach diesem Absatz sind durch die jeweiligen Stellen in einer Weise zu protokollieren, die eine Kontrolle der Zulässigkeit von Datenabrufen technisch unterstützt.

Die Pflicht nach Satz 3 gilt ab dem Tag, der dem Tag folgt, an dem das Bundesministerium des Innern und für Heimat im Bundesanzeiger bekannt gibt, dass die technischen und rechtlichen Voraussetzungen für eine Anzeige der Datenübermittlungen nach diesem Absatz im Datenschutzcockpit nach § 10 des Onlinezugangsgesetzes vorliegen. § 9 Absatz 2 und 3 des Identifikationsnummerngesetzes gilt ab diesem Zeitpunkt entsprechend.

(4) Soll der Nachweis aus einem Register, welches in der Anlage zum Identifikationsnummerngesetz vom 28. März 2021 (BGBl. I S. 591; 2023 I Nr. 230) aufgeführt ist, abgerufen werden, darf die nachweisanfordernde Stelle die Identifikationsnummer nach § 1 des Identifikationsnummerngesetzes zur Zuordnung der Datensätze zum Antragsteller und zum Abruf des Nachweises an die nachweisliefernde Stelle übermitteln. Das Nachweisabrufersuchen darf zusätzlich weitere Daten im Sinne von § 4 Absatz 2 und 3 des Identifikationsnummerngesetzes, in der Regel das Geburtsdatum, zur Validierung der Zuordnung enthalten. Zu diesem Zweck darf die nachweisliefernde Stelle diese Daten verarbeiten.

(5) Bevor die für die Entscheidung über den Antrag zuständige Behörde den abgerufenen Nachweis verwenden darf, um die antragsgebundene Verwaltungsleistung zu erbringen, hat der Antragsteller im Fall des Absatzes 1 Satz 1 Nummer 1, wenn der Nachweis ohne zeitlichen Verzug automatisiert abgerufen werden kann, die Möglichkeit, den Nachweis vorab einzusehen. Der Antragsteller kann in diesem Fall entscheiden, ob der Nachweis für das Antragsverfahren verwendet werden soll.“

3. Nach § 5 wird der folgende § 5a eingefügt:

„§ 5a
Grenzüberschreitende Nachweisabrufe

(1) Die zuständige Behörde darf bei einer Behörde eines anderen Mitgliedstaats der Europäischen Union einen Nachweis nach Artikel 14 Absatz 2 der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 automatisiert abrufen, wenn dies zur Erfüllung ihrer Aufgaben für eines der Verfahren nach Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 erforderlich ist.

(2) Die automatisierte Übermittlung eines Nachweises nach Artikel 14 Absatz 2 der Verordnung (EU) 2018/1724 an eine Behörde eines anderen Mitgliedstaats der Europäischen Union ist zulässig, wenn diese Behörde zuständig ist und die Übermittlung zur Erfüllung ihrer Aufgaben für eines der Verfahren nach Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 erforderlich ist.

(3) Bei der Verarbeitung personenbezogener Daten nach den Absätzen 1 und 2 können intermediäre Plattformen zum Einsatz kommen.“

4. § 13 wird durch den folgenden § 13 ersetzt:

„§ 13
Datenübermittlung

Die Behörden des Landes, die Gemeinden, Ämter und Landkreise nutzen für die Datenübermittlung innerhalb des Landes, mit den Behörden und Kommunen anderer Länder sowie mit den Behörden des Bundes das Corporate Network Landeskommunikationsvermittlungs- und Informationsnetz, soweit nicht wichtige Gründe entgegenstehen. Abweichungen von Satz 1 sind zu begründen und der für die Digitalisierung zuständigen obersten Landesbehörde zur Entscheidung vorzulegen.“

5. § 16 wird wie folgt geändert:

a) Absatz 2 wird durch den folgenden Absatz 2 ersetzt:

„(2) Die für Digitalisierung zuständige oberste Landesbehörde bestimmt, wer die Funktion der oder des CIO M-V wahrnimmt. Diese Person muss in einem öffentlich-rechtlichen Dienst- und Treueverhältnis zum Land Mecklenburg-Vorpommern stehen.“

b) Absatz 3 wird wie folgt geändert:

aa) Nummer 2 wird durch die folgende Nummer 2 ersetzt:

„2. die strategische Ausrichtung und Durchsetzung der IT-Politik, insbesondere von IT-Richtlinien, IT-Standards und -Architekturen des Landes,“.

bb) Nummer 5 wird gestrichen.

cc) Die Nummern 6 und 7 werden zu den Nummern 5 und 6.

c) In Absatz 4 wird die Angabe „ressortübergreifende IT-Angelegenheiten“ durch die Angabe „die Digitalisierung “ ersetzt.

Artikel 3
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

EU-Rechtsakte:

1. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2026, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35)
2. Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89; L 127 vom 23.5.2018, S. 9; L 74 vom 4.3.2021, S. 36)
3. Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 22.12.2022; L, 2023/90206, 22.12.2023)
4. Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (ABl. L 295 vom 21.11.2018, S. 1), die zuletzt durch die Verordnung (EU) 2025/2205 vom 22. Oktober 2025 (ABl. L, 2025/2205, 05.11.2025) geändert worden ist.

Begründung:

A Allgemeiner Teil

Alle Teile unserer Gesellschaft erleben eine stetig wachsende Bedeutung des Digitalen: digitale Informationen, digitale Anwendungen, digitale Infrastrukturen, digitaler IT-Schutzschirm, digitale Resilienz. Die zunehmende Vernetzung und Digitalisierung von Bereichen sowohl des öffentlichen als auch des privaten und wirtschaftlichen Lebens führen in unserer stark arbeitsteiligen Gesellschaft zu kontinuierlich steigenden multiplen Abhängigkeiten.

Unsere hoch technologisierte Gesellschaft muss folglich resilient sein. Es müssen Kompetenzen und Fähigkeiten in Organisationen entwickelt, aufrechterhalten und optimiert werden, sich sowohl an digitale Herausforderungen als auch an Veränderungen anzupassen, insbesondere Krisen zu bewältigen. Organisationen müssen somit widerstandsfähig sein, sich schnell von technischen Störungen, Cyberangriffen und anderen digitalen Bedrohungen zu erholen. Dies gilt umso mehr aufgrund der steigenden Abhängigkeit der Gesellschaft vom Funktionieren kritischer Infrastrukturen wie beispielsweise die Energieversorgung oder auch die ordnungsgemäße Durchführung demokratischer Wahlen. In vielen Fällen wirken heutige (erhebliche) Sicherheitsvorfälle unmittelbar existenzbedrohlich. Heutzutage sind alle Bereiche der Gesellschaft auf Informationstechnik, damit auf eine wirkungsvolle Informationssicherheit angewiesen. Dies gilt sowohl für die Bürgerinnen und Bürger, die Wirtschaft, andere gesellschaftliche Organisationen und natürlich auch für die öffentliche Hand.

Der wirtschaftlich angemessene Schutz von Informationstechnik vor Bedrohungen ist infolgedessen ein gesamtgesellschaftlicher Auftrag – international, national und regional.

Die Gewährleistung der Informationssicherheit erfordert einen umfassenden und ganzheitlichen Ansatz, der technische und organisatorische Umsetzungsmaßnahmen auf Basis von Sicherheitsanforderungen mit rechtlichen Regelungen verbindet. Deshalb ist hierfür neben den Behörden, Einrichtungen und Institutionen des Landes auch die kommunale Ebene einzubeziehen.

Für digitale Verwaltungsdienstleistungen sowie für das Zusammenwirken staatlicher und kommunaler Stellen im Land Mecklenburg-Vorpommern, den damit verbundenen Datenaustausch, auch mit anderen Ländern und dem Bund bildet das Corporate Network Landeskommunikationsvermittlungs- und Informationsnetz (CN LAVINE) die essenzielle Informations- und Kommunikationsinfrastruktur, das essenzielle Rückgrat beim Einsatz von Informationstechnik. Die herausgehobene und fundamentale Bedeutung von Kommunikations- und Datennetzen der öffentlichen Verwaltung nimmt beim Einsatz von Informationstechnik eine besondere Rolle ein, die es besonders zu schützen gilt.

Mit dem Gesetz zur Neuordnung und Förderung der Informationssicherheit im Land Mecklenburg-Vorpommern werden die grundlegenden Anforderungen festgelegt, die zur Erreichung der Informationssicherheit zwingend erforderlich sind, sowohl inhaltlich als auch organisatorisch.

Insbesondere
- sollen die BSI-Standards der 200er Reihe, insbesondere die Sicherheitsanforderungen aus dem BSI IT-Grundschutz-Kompendium, verpflichtend für alle staatlichen und kommunalen Stellen gelten,
- sollen die fachlichen Kompetenzen in einer Informationssicherheitsmanagementorganisation der Landes- und Kommunalverwaltung gebündelt werden,
- sollen die Aufgaben, Kontroll- und Prüfbefugnis, insbesondere die Weisungsbefugnis des Chief Information Security Officers M-V, gefestigt und erweitert werden,
- sollen die Aufgaben und Befugnisse der Informationssicherheitsbeauftragten definiert werden,
- sollen die Aufgaben, die Unabhängigkeit, insbesondere die datenschutzrechtlichen Befugnisse des Sicherheitsteams der Landes- und Kommunalverwaltung (CERT M-V) bei der Sicherheitsvorfallbehandlung, festgelegt werden,
- sollen die öffentlichen Stellen für eine ziel- und zweckgerichtete, zeitgerechte Erkennung von Gefahren, insbesondere von Cyberangriffen, zum Betrieb von Security Operations Center (SOC) verpflichtet werden,
- sollen die Regelungen zur Verarbeitung von Protokoll-, Verkehrs- und Inhaltsdaten, insbesondere deren Analyse, Auswertung, Zusammenführung, Speicherfristen und Übermittlung an das CERT M-V, festgelegt werden,
- sollen verbindliche Meldepflichten über Sicherheitsvorfällen eingeführt werden sowie
- soll die Regelung zur Datenübermittlung über das CN LAVINE im Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (EGovG M-V) weiterentwickelt werden.

Gesetzesfolgen

Die mit dem Vollzug des Gesetzes zu erwartenden Haushaltsausgaben sind im Rahmen der Ansätze des Haushaltentwurfes 2026/2027 und zugehöriger haushaltsgesetzlicher Ermächtigungen vollständig dargestellt.

Ein zusätzlicher Finanzbedarf über den Ansätzen des Haushaltentwurfes 2026/2027 und zugehöriger haushaltsgesetzlicher Ermächtigungen wird nicht erwartet.

Die Gewährleistung der Informationssicherheit stellt eine organisatorische Anforderung an die Verwaltungstätigkeit der kommunalen Körperschaften dar. Bereits heute obliegt es den kommunalen Körperschaften im Rahmen ihrer Selbstverwaltung, die notwendigen Maßnahmen zur Sicherstellung der Informationssicherheit zu ergreifen. Die im Gesetz vorgesehenen Standards und organisatorischen Vorgaben dienen daher nicht der Einführung neuer Pflichten, sondern lediglich der Konkretisierung und Systematisierung bereits bestehender Anforderungen. Durch die gesetzlichen Regelungen erfolgt somit keine Aufgabenübertragung, die einen finanziellen Ausgleich auslösen könnte. Vielmehr werden die vorhandenen Verpflichtungen an den aktuellen Stand der Technik angepasst und rechtlich präzisiert.

B Besonderer Teil

Zu Artikel 1 – Informationssicherheitsgesetz Mecklenburg-Vorpommern

Zu § 1

Zu Absatz 1 Nummer 1

Die Verwaltung des Landes Mecklenburg-Vorpommern wird durch die Träger der unmittelbaren und mittelbaren Landesverwaltung gemäß § 1 des Landesorganisationsgesetzes (LOG M-V) wahrgenommen. Gemäß Absatz 1 sind Verpflichtete dieses Gesetzes und somit Adressaten die Behörden, Einrichtungen und Institutionen der Landesverwaltung von Mecklenburg-Vorpommern sowie die unter ihrer Aufsicht stehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, die als staatliche Stellen bezeichnet werden. Hiervon sind auch Schulen in öffentlicher Trägerschaft erfasst.

Zu Absatz 1 Nummer 2

Der Absatz 1 Nummer 2 definiert die Gemeinden, Ämter und Landkreise als Körperschaften des öffentlichen Rechts mit Gebietshoheit in den Geltungsbereich des Informationssicherheitsgesetzes. Dies gilt unabhängig davon, ob diese Gebietskörperschaften im Rahmen ihrer Aufgabenerfüllung nach Weisung der unmittelbaren oder mittelbaren Landesverwaltung handeln oder nicht. Darüber hinaus sind vom Geltungsbereich des Informationssicherheitsgesetzes auch die kommunalen Einrichtungen ohne Gebietskörperschaft erfasst. Nach dem Prinzip der eigenen Wahrnehmungskompetenz und Wahlfreiheit können Kommunen öffentliche Aufgaben auch mittelbaren Verwaltungsträgern wie Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts übertragen.

Zu Absatz 1 Nummer 3

Es wird einheitlich der Begriff „Unternehmen oder Einrichtungen in einer Rechtsform des privaten Rechts“ verwendet. Dieser Begriff ist bereits im Landesrecht (vgl. §§ 65 ff. LHO M-V, § 69 KV M-V) etabliert.

Mit Blick auf die Auslagerung von Verwaltungsaufgaben und den damit verbundenen Datenaustausch über gemeinsam genutzte Informationstechnik ist es folgerichtig geboten, auch natürliche und juristische Personen des Privatrechts sowie sonstige, in der Regel nicht rechtsfähige Vereinigungen in den Geltungsbereich des Gesetzes einzubeziehen. Diese Stellen sind oftmals Träger der Daseinsvorsorge oder nehmen Aufgaben der öffentlichen Verwaltung wahr. Sie werden im Kontext der ihnen übertragenen öffentlichen Aufgaben als Verwaltungsträger bezeichnet. Dabei soll der Begriff der „sonstigen Stellen“ im Sinne des § 1 Absatz 1 Satz 1 Nummer 3 nur solche Unternehmen und Einrichtungen in privatrechtlicher Rechtsform umfasst, die in öffentlicher Verantwortung stehen, also entweder Aufgaben der öffentlichen Verwaltung wahrnehmen oder an denen öffentliche Stellen einzeln oder gemeinsam mit mehr als 50 Prozent der Anteile oder Stimmen beteiligt sind. Rein privat getragene, wenngleich systemrelevante Einrichtungen, etwa Krankenhäuser oder Pflegeeinrichtungen in ausschließlich privater Trägerschaft, fallen demnach nicht unter die Vorschrift.

Die nicht detailliert vorgenommene Definition der systemrelevanten Träger der Daseinsvorsorge stellt sicher, dass eine Einstufung nicht rein quantitativ (nach Schwellenwerten) vorgenommen wird, sondern qualitativ. Nötigenfalls ist eine Abwägung vorzunehmen und im Einzelfall zu subsumieren, ob eine Einrichtung als relevant für die Daseinsvorsorge einzustufen ist. Es ist demnach auch vollkommen gleichgültig, welche Größe oder Unternehmensform ein Träger der Daseinsvorsorge hat. Es geht allein um die Verantwortung, die aus der Tätigkeit gegenüber der Gesellschaft, Bevölkerung oder einzelnen Personen erwächst.

Zu Absatz 2

Der Absatz 2 schließt die Lücke bei verketteten Beteiligungen staatlicher und kommunaler Stellen bei juristischen Personen oder Vereinigungen des privaten Rechts. Darüber hinaus wird klargestellt, dass, wenn nicht öffentlich-rechtliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, diese als sonstige Stellen vom Informationssicherheitsgesetz erfasst sind.

Beispiele: Schulen in privater Trägerschaft, Schornsteinfeger, TÜV, öffentlich bestellter Vermessungsingenieur.

Zu Absatz 3

Der Landtag wird vom Geltungsbereich des Informationssicherheitsgesetzes ausgenommen, um seiner Stellung als selbstständiges Verfassungsorgan und Träger der gesetzgebenden Gewalt Rechnung zu tragen. Als unabhängiges Organ darf er nicht in ein durch die Landesregierung gesteuertes Informationssicherheitsmanagement einbezogen werden. Die Ausnahme dient der Wahrung der Gewaltenteilung und entspricht der Regelungspraxis anderer Länder.

Der Landesrechnungshof wird aufgrund seiner verfassungsrechtlichen Stellung nach Artikel 68 der Verfassung des Landes Mecklenburg-Vorpommern vom Geltungsbereich ausgenommen. Dies soll gewährleisten, dass die richterliche Unabhängigkeit seiner Mitglieder nicht beeinträchtigt wird und die Prüftätigkeit ohne Einflussnahme der Exekutive erfolgen kann. Eine Bereichsausnahme für seine Prüfungstätigkeit ist daher erforderlich, um die verfassungsrechtlich geschützte Eigenständigkeit zu wahren.

Schließlich werden auch die Hochschulen ausgenommen, um ihrer verfassungsrechtlich garantierten Selbstverwaltung sowie der Freiheit von Forschung und Lehre gerecht zu werden. Eine zentrale Steuerung der Informationssicherheit durch die Exekutive wäre mit dieser Autonomie unvereinbar.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist nach Artikel 52 der Datenschutz-Grundverordnung in der Ausübung seiner Aufgaben vollständig unabhängig. Eine Einbindung in die zentralen Strukturen der Informationssicherheit des Landes würde diese Unabhängigkeit beeinträchtigen und Interessenkonflikte begründen. Der Landesbeauftragte trägt selbst Verantwortung für die Sicherheit der von ihm verarbeiteten Daten und hat hierfür eigene organisatorische und technische Maßnahmen zu treffen. Daher ist er vom Anwendungsbereich des Informationssicherheitsgesetzes auszunehmen.

Die Bereichsausnahme für die Gerichte und Staatsanwaltschaften ist erforderlich, um die verfassungsrechtlich garantierte Unabhängigkeit der Gerichte (Artikel 97 GG) und die Gewaltenteilung zu wahren. Die im Gesetzentwurf vorgesehenen Eingriffs- und Durchgriffsbefugnisse des Chief Information Security Officers M-V u. a. bei Netztrennungen könnten andernfalls mittelbar in die IT-Hoheit und Funktionsfähigkeit der Gerichte und Staatsanwaltschaften eingreifen. Da die richterliche Tätigkeit und der Umgang mit justiziellen Daten besonders sensibel sind, muss ausgeschlossen werden, dass über ressortübergreifende Informationssicherheitsmaßnahmen Einfluss auf gerichtliche Verfahren genommen wird. Dementsprechend soll die Bereichsausnahme auch insoweit gelten, als deren justizielle Daten und IT durch die für die Justiz zuständige oberste Landesbehörde verwaltet werden. Eine Einbindung dieser Datenverwaltung in die zentralen Strukturen der Informationssicherheit des Landes könnte zu einer faktischen Einflussnahme auf die technische Infrastruktur der Justiz führen und damit die Unabhängigkeit der Rechtspflege mittelbar beeinträchtigen. Die Einbeziehung dieser Organisationseinheit in die Bereichsausnahme ist daher notwendig und systemgerecht.

Die entsprechende Anwendung der in § 3 festgelegten Grundsätze der Informationssicherheit auf die ausgenommenen Stellen stellt sicher, dass auch diese ein angemessenes und einheitliches Schutzniveau für ihre informationstechnischen Systeme gewährleisten. Dadurch werden Integrität, Verfügbarkeit und Vertraulichkeit der verarbeiteten Informationen gewährleistet, ohne die verfassungsrechtlich garantierte organisatorische und fachliche Unabhängigkeit der betroffenen Stellen zu beeinträchtigen.

Die ergänzende Anwendung der §§ 11 bis 16 ermöglicht eine einheitliche Vorgehensweise bei der Erkennung, Meldung und Abwehr von Sicherheitsvorfällen im gesamten öffentlichen Bereich. Das Zustimmungserfordernis der beauftragten Person für Informationssicherheit wahrt dabei die Eigenverantwortung und Entscheidungsfreiheit dieser Stellen. Dadurch wird sichergestellt, dass Datenverarbeitungen nur unter Berücksichtigung der jeweiligen organisatorischen Besonderheiten und rechtlichen Zuständigkeiten erfolgen und die institutionelle Unabhängigkeit unangetastet bleibt.

Zu § 2

Zur Förderung des Bestimmtheitsgebotes, der fachlichen Klarheit sowie der Anwenderfreundlichkeit sind die wichtigsten fachlichen Begrifflichkeiten und Tatbestandsmerkmale legal definiert.

Zu § 2 Nummer 1

Für eine bessere Lesbarkeit des Gesetzestextes werden die staatlichen und kommunalen Stellen (§ 1 Absatz 1 Nummer 1 und 2) zu „öffentliche Stellen“ zusammengefasst.

Zu § 2 Nummer 2

In der Informatik werden Daten als Fakten oder als Träger einer Information in kodierter (das heißt maschinenverarbeitbarer) Form verstanden. Daten werden heutzutage mit Informationstechnik verarbeitet. Diese Datenverarbeitung umfasst insbesondere die Erstellung, Speicherung, Veränderung, Übermittlung bzw. den Transport, die Archivierung und letztendlich die Löschung von Daten.

Zu § 2 Nummer 3

Als ein zentraler Begriff dieses Gesetzes umfasst die Informationstechnik (IT) jedes datenverarbeitende System, unabhängig von seiner Beschaffenheit, das heißt von seiner Form, Farbe und Größe oder seinem Zweck zur Datenverarbeitung.

Informationstechnik beschreibt in einem allgemeinen Sinne Systeme aus Hard- und Software sowie die auf ihnen ablaufenden, der Verarbeitung von Informationen (Daten) dienenden Datenverarbeitungsprozesse. Darüber hinaus beinhaltet der Begriff Informationstechnik ebenfalls alle technischen Mittel für eine Kommunikationsanwendung sowie die verschiedenen Protokolle, Systeme und Anwendungen, die damit verbunden sind. Insofern umfasst der Begriff Informationstechnik auch alle nicht elektronischen Mittel der Informationsverarbeitung.

Der Begriff ist nicht abschließend und umfasst beispielsweise Serversysteme, Netzwerkgeräte, Notebooks, Smartphones, Tablets, Drucker, intelligente, mit dem Internet verbundene (Haushalts-)Geräte (Internet of Things, IoT), Steuerungsanlagen der Gebäudeleittechnik, Industriesteuerungen (Operational Technology, OT) sowie die jeweils dazugehörige Betriebs- und Anwendungssoftware und Datennetze, aber auch verteilte Systeme aus mehreren verschiedenen solcher Komponenten oder das Internet in Teilen oder insgesamt.

Der Begriff Informationstechnik ist bewusst generisch formuliert und weit gefasst, um technologische Weiterentwicklungen zu berücksichtigen. Informationstechnik wird folglich in einem weiten Sinne verstanden, sodass jedes System erfasst ist, welches in elektronischer Weise Daten oder nicht elektronisch Informationen erfasst, speichert, verarbeitet, nutzt, übermittelt oder löscht.

Zu § 2 Nummer 4

Die Begriffsdefinition zentrale Informationstechnik beinhaltet zunächst alle Definitionseigenschaften der Nummer 3 Informationstechnik.

Der zentralen Informationstechnik kommt im Rahmen dieses Gesetzes eine besondere Bedeutung zu, da es sich um essenzielle und kritische Basis-Informationstechnik handelt. Basis-Informationstechnik umfasst IT-Lösungen, die zum Betrieb von Basisdiensten zwingend benötigt werden. Ein Basisdienst ist ein grundlegender IT-Dienst, der die Bereitstellung von Fach- und Querschnittsdiensten unterstützt und auf Infrastrukturdiensten aufbaut. Ein Infrastrukturdienst ist ein IT-Dienst, der Basis-, Fach- und Querschnittsdienste unterstützt, indem dieser technische Basisfunktionalitäten bereitstellt. Zentrale Informationstechnik besitzt oftmals mit Blick auf die diesbezüglichen Schutzziele einen hohen Schutzbedarf gemäß der BSI IT-Grundschutz-Methodik (siehe BSI-Standard 200-2; Schutzbedarfsfeststellung).

Zu § 2 Nummer 5

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, auf digitalen Datenträgern als auch in den Köpfen der Menschen gespeichert sein. Dieses Gesetz hat primär den Schutz von elektronisch verarbeiteten Daten zum Ziel.

Daten sind wichtige Werte für Behörden und müssen angemessen geschützt werden. Es muss u. a. sichergestellt werden, dass sowohl die behördeninternen als auch die Daten der Bürgerinnen und Bürger vertraulich behandelt werden. Für die Informationssicherheit wird insbesondere auf die Mittel der Kryptographie zurückgegriffen. Kryptographie befasst sich insbesondere mit Verschlüsselungs-, Signatur- und Authentifizierungsverfahren.

Informationstechnik und Daten dürfen nur für autorisierte Nutzer zugänglich sein. Daten (Informationen) dürfen nicht absichtlich oder versehentlich geändert werden können; jede Veränderung muss nachvollziehbar sein. Informationstechnik muss den autorisierten Zugriff zum richtigen Zeitpunkt, am richtigen Ort und den richtigen Personen die Daten in aufbereiteter Form zur Verfügung stellen. Diese Daten müssen echt sein; der Urheber eines Datums muss eindeutig ermittelt werden können. In diesem Kontext wird vom Schutzziel auch die Nichtabstreitbarkeit (Non-Repudiation) umfasst. Bei der Übertragung von Informationen in Form von Daten bedeutet dies, dass eine Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

Damit sind die vier grundlegenden Schutz- oder Gewährleistungsziele (Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit) der Informationssicherheit definiert. Weil die Informationssicherheit nicht ausschließlich eine Frage des Technikeinsatzes ist, ist es wichtig, neben der IT-Sicherheit auch die organisatorischen, infrastrukturellen und personellen Rahmenbedingungen festzulegen.

Zu § 2 Nummer 6

Eine ungesteuerte und unstrukturierte Umsetzung, insbesondere von technischen Einzelmaßnahmen, wie beispielsweise der Einsatz einer Antivirensoftware oder einer Firewall, ist nicht ausreichend, um die Informationssicherheit zu erreichen. Vielmehr ist ein ganzheitlicher Ansatz zu verfolgen. Die auf Grundlage von Managementmethoden und -prinzipien basierte Umsetzung von technischen, organisatorischen und personellen Sicherheitsanforderungen in Maßnahmen erfordert ein umfassendes Risikomanagement im Rahmen eines Informationssicherheitsmanagementsystems (Informationssicherheitsmanagementsystem).

Ein Informationssicherheitsmanagementsystem ist ein Managementsystem bzw. ein System der Unternehmensführung zur Steuerung und Kontrolle der Informationssicherheit in einer Organisation. Es umfasst auf der horizontalen Koordination die Organisation, Planung/ Kontrolle und Personal/Führung sowie auf der vertikalen Koordination die operative, taktische, und strategische Unternehmensführung. Darüber hinaus enthalten im Grundsatz alle Managementsysteme immer Regelkreisläufe (Demingkreis) innerhalb einer Organisation, die einen bestimmten Teil dieser Organisation dauerhaft in einem kontinuierlichen Verbesserungsprozess weiterentwickeln sollen. Bekannt sind vergleichbare Managementsysteme, z. B. als Qualitätsmanagement, Umweltmanagement oder Arbeitsschutzmanagement. Ein Informationssicherheitsmanagementsystem fügt sich in dieses Konstrukt nahtlos ein.

Die Kernaufgabe eines Informationssicherheitsmanagementsystems liegt in der Planung, Umsetzung, Kontrolle und Anpassung (im Sinne von Fortentwicklung) von Sicherheitskonzepten. Dabei besteht ein Informationssicherheitsmanagementsystem aus drei Säulen: der Strukturbeschreibung, der Risikoanalyse und -bewertung sowie einem Risikobehandlungsplan.

Ein Informationssicherheitsmanagementsystem ist somit ein Rahmenwerk zur Etablierung und Fortführung eines verbindlichen kontinuierlichen Prozesses zur Planung, Lenkung und Kontrolle der Konzepte und Aufgaben, die auf die Wahrung der Ziele der Informationssicherheit in einer Organisation gerichtet sind.

Die Anforderungen an ein Informationssicherheitsmanagementsystem umfassen neben der Erstellung, Umsetzung und Wirksamkeitsprüfung von Sicherheitskonzepten ebenfalls die Festlegung und Dokumentation von Verantwortlichkeiten hinsichtlich des Informationssicherheitsmanagements, die Erstellung von verbindlichen Richtlinien für die Informationssicherheit, die Festlegung und Dokumentation der Abläufe bei Sicherheitsvorfällen sowie die Etablierung von transparenten Prozessen, mit denen Umsetzung, Wirksamkeit, Wirtschaftlichkeit und Beachtung der Informationssicherheitsmaßnahmen regelmäßig kontrolliert wird; darüber hinaus, wie die Einleitung gegebenenfalls erforderlicher Schutz-/Sicherheitsmaßnahmen, z. B. die Aktualisierung/Fortschreibung der Sicherheitskonzepte, gewährleistet wird.

Informationsweitergabe und Erläuterungen zu Sicherheitsmaßnahmen, Fort- und Weiterbildung von beauftragten Personen für Informationssicherheit, Sensibilisierung aller Beschäftigten einer Organisation zu Themen der Informationssicherheit, insbesondere zu den aktuellen Bedrohungen, gehören ebenfalls hinzu. Essenziell für ein Informationssicherheitsmanagementsystem ist das Vorhandensein einer wie in Teil 2 dieses Gesetzes beschriebenen Informationssicherheitsorganisation, die eine wesentliche Grundvoraussetzung für ein angemessenes und wirksames Informationssicherheitsmanagementsystem ist.

Zu § 2 Nummer 7

Ein sicherheitsrelevantes Ereignis liegt vor, wenn der Versuch unternommen wird, eines oder mehrere Schutzziele der Informationssicherheit möglicherweise zu beeinträchtigen oder zu verletzen. Sie werden u. a. aus (korrelierten) Protokoll- und Protokollierungsdaten gewonnen, die eine nachvollziehbare Relevanz für die Informationssicherheit besitzen sowie Auswirkungen auf die Gewährleistung der Informationssicherheit haben könnten.

Sicherheitsrelevante Ereignisse liegen immer dann vor, wenn beispielsweise aus dem Internet durchgeführte Untersuchungen auf die Informationstechnik erfolgen, die die Internetauftritte der Landesverwaltung verarbeitet – sogenannte Portscans – oder auch Zugriffsversuche auf die Informationstechnik durch Cyberkriminelle nach vermuteten Schwachstellen oder bekannte Sicherheitslücken.

Viele dieser Ereignisse werden von den Security Analysten als tägliches Grundrauschen behandelt. Treten bestimmte sicherheitsrelevante Ereignisse quantitativ verstärkt auf, kann dies beispielsweise auf eine neue, bislang unbekannte Sicherheitslücke hindeuten, deren Ausnutzung zu einem (erheblichen) Sicherheitsvorfall führen kann.

Zu § 2 Nummer 8

Ein Sicherheitsvorfall liegt vor, wenn die Schutz-/Sicherheitsmaßnahmen aus dem zugrunde liegenden Sicherheitskonzept, einer Sicherheitsrichtlinie oder eines Sicherheitsstandards versagt haben oder mindestens eines der Schutzziele der Informationssicherheit verletzt wurde. Bei einem Sicherheitsvorfall kann es sich beispielsweise um den ungewollten Abfluss von Daten oder um einen durch ein Schadprogramm befallenen Arbeitsplatzrechner handeln. Erhebliche Sicherheitsvorfälle sind dadurch gekennzeichnet, dass diese in ihrer Wirkung und Folge einen großen finanziellen Schaden verursachen. Beispiel für einen erheblichen Sicherheitsvorfall sind Angriffe von Cyberkriminellen mittels Ransomware oder die Zerstörung von zentraler Informationstechnik.

Zu § 2 Nummer 9

Um ein hohes Sicherheitsniveau zu erreichen, sind vorbeugende Schutz-/ Sicherheitsmaßnahmen im Vorfeld von bekannten Gefahren unabdingbar. Diese Maßnahmen sind der Gefahrenvorsorge zuzuordnen und dienen dazu, die Entstehung von Gefahren zu verhindern bzw. eine wirksame Bekämpfung sich zu einem späteren Zeitpunkt realisierender, momentan aber noch nicht konkret drohender Gefahren zu ermöglichen. Legaldefinitionen des Gefahrenbegriffs befinden sich u. a. in § 2 Nummer 3a BremPolG oder in § 4 Nummer 3a SächPVDG.

Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) kennt 47 elementare Gefährdungen. Diese Gefährdungen beschreiben eine Situation oder eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt wie beispielsweise Informationstechnik oder Menschen wirkt sowie räumlich und/oder zeitlich einer begründeten Gefahr ausgesetzt sind.

Zu § 2 Nummer 10

Die Begriffsbestimmung eines Schadprogramms orientiert sich an dem § 2 Absatz 5 BSIG. Grundsätzlich wird in diesem Gesetz der weite Verarbeitungsbegriff des Datenschutzrechts übernommen, der das Erfassen, die Speicherung, die Veränderung, die Verwendung, die Übermittlung, die Einschränkung, die Archivierung, das Löschen oder die Vernichtung von Daten beinhalten kann.

Eine Datenverarbeitung ist immer dann unbefugt, wenn irregulär auf Daten und/oder einen Datenverarbeitungsprozess eingewirkt wird. Nicht erfasst sind damit unbeabsichtigt durch Programmierfehler, fehlerhafte Konfiguration, unübliche Nutzung der Software oder durch mangelhaften Kontrollfluss entstehende Sicherheitslücken in Programmen. Ein Schadprogramm ist nach diesem Gesetz jede Art von Software, die genutzt wird, Schaden zu verursachen. Maßgeblich sind der tatsächlich beabsichtigte Einsatzzweck sowie der zielgerichtete Einsatz des Schadprogramms selbst, also das unbefugte und unerwünschte Ausführen von Funktionen, aber nicht die Intention eines Programmierers bei der Entwicklung der Software.

Schadprogramme können typischerweise Schäden verursachen. Dies ist jedoch kein zwingendes Kriterium für die Kategorisierung von Schadprogrammen. Einige Schadprogramme zeichnen sich auch gerade dadurch aus, dass sie möglichst unauffällig und klein sind. Schadfunktionen sind zunächst nicht enthalten, können aber gegebenenfalls aus der Ferne nachgeladen werden.

Beispiel hierfür ist ein Bot, ein Schadprogramm, das zunächst unbemerkt, ferngesteuert auf einem Rechnersystem arbeitet. Zusammengeschlossen als Botnetz können diese Schadprogramme zu bestimmten Aktionen missbraucht werden, um mittels DDoS-Angriffe (Distributed Denial of Service, Massenanfragen) gegen informationstechnische Systeme durch Überlastung zu wirken und diese in ihren informationstechnischen Prozessen bzw. Routinen lahmzulegen.

Zu § 2 Nummer 11

In Anlehnung an § 2 Absatz 6 BSIG sind Sicherheitslücken definiert als Eigenschaften von Informationstechnik, insbesondere von Softwareprogrammen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zutritt zu seinen Gebäuden oder zu einzelnen Räumen, Zugang zu fremden informationstechnischen Systemen und Zugriff auf deren Daten verschaffen oder die Funktion der informationstechnischen Systeme in unzulässiger Weise beeinflussen.

Sofern unbefugte Personen in ein Gebäude oder in einzelne Räume gelangen, kann dieser Vorgang verschiedene Gefährdungen nach sich ziehen. Unbefugte Personen können einerseits durch vorsätzliche Handlungen wie Diebstahl oder Manipulation an der Informationstechnik oder von Informationen, andererseits durch unbeabsichtigtes Fehlverhalten, z. B. aufgrund mangelnder Fachkenntnisse, Schäden verursachen. Durch diese Handlungen können nicht offensichtliche Manipulationen weit höhere Schäden verursachen als die mittelbare Zerstörung. Durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und Türen werden gewaltsam geöffnet und dabei beschädigt. Diese zu reparieren oder zu ersetzen, beansprucht in der Regel Zeit und finanzielle Mittel, in der diese ihre Schutzfunktion nicht oder nur eingeschränkt bereitstellen. Es entstehen somit analoge Sicherheitslücken, die nicht unmittelbar im Zusammenhang mit der Informationstechnik stehen.

Der Zugang kann unbeabsichtigt passieren, beispielsweise durch einen Programmierfehler, oder aber auch bewusst als sogenannte Hintertür durch den Programmierer in der Informationstechnik integriert sein. Eine Beeinflussung muss nicht zwingend darin bestehen, dass sich der Angreifer Zugang zum System verschafft und dieses manipulieren könnte. Es genügt, dass die Funktionsweise in sonstiger Weise beeinflusst werden kann, z. B. durch ungewolltes Abschalten, Umleiten von Eingaben und/oder Ausgaben oder durch sonstige mittelbare Beeinflussung.

Der Begriff Sicherheitslücke ist weit gefasst, da Sicherheitslücken in den unterschiedlichen Konstellationen, oftmals abhängig von der Konfiguration der Informationstechnik, dem Zusammenwirken mit anderen Softwareprogrammen oder durch die jeweilige Einsatzumgebung, entstehen können.

Zu § 2 Nummer 12

Eine wichtige Rolle für den Schutz der Informationstechnik und somit für die Gewährleistung der Informationssicherheit spielt das Sammeln, die Analyse sowie die Auswertung von sicherheitsrelevanten Informationen, u. a. auch über aktuelle Bedrohungen oder über Sicherheitslücken. Dabei liegt ein Schwerpunkt der Informationsbeschaffung auf der Vorsorge für die Abwehr künftiger Angriffe und somit in der Vermeidung von (erheblichen) Sicherheitsvorfällen.

Die Informationsbeschaffung erfolgt unabhängig vom Vorliegen einer konkreten Gefahr oder von den Gefährdungen der Informationssicherheit. Als Maßnahmen zur Sammlung von Informationen kommen die Protokollierung aus der Nutzung von Informationstechnik oder Sicherheitsprüfungen in Form von strukturierten Penetrationstests, Audits oder IS-Revisionen in Betracht. So werden beispielsweise bei Penetrationstests Informationen über das jeweilige Prüfobjekt erhoben, um Schwachstellen bei diesem festzustellen und diese gegenüber dem Betroffenen bekannt zu machen. Protokolldaten sind besonders bedeutsam, um Abweichungen im ordnungsgemäßen IT-Betrieb verbunden mit Angriffen auf die Informationstechnik auszuwerten und zu analysieren. Aus den gewonnenen Erkenntnissen sind Schlüsse zu effektiven Schutz-/Sicherheitsmaßnahmen zur Abwehr von laufenden oder zukünftigen Angriffen zu entwickeln. Das Sammeln und Auswerten von Informationen kann Grundrechtseingriffe bewirken, die einer gesetzlichen Rechtfertigung bedürfen (siehe § 17 ISichG M-V).

Nummer 12 geht über die Begriffsbestimmung des § 2 Absatz 8 BSIG hinaus. Ein Protokolldatum legt fest oder zeichnet auf, wer was wann und in welcher Reihenfolge durchführen muss oder durchgeführt hat. Im Gesetz sind beide Ausprägungen gemeint, sowohl Methoden der Kommunikation informationstechnischer Systeme (technisches Protokoll, z. B. TCP/IP oder HTTPS) als auch die Daten zum Nachweis der Verarbeitung in informationstechnischen Systemen (in sogenannten Logfiles), z. B. Serversysteme, Firewallsysteme oder Proxydienste. Protokolldaten dokumentieren Ereignisse über Anfragen von Nutzern, anderen Systemen, Softwareänderungen, Fehlermeldungen. Setzt man Protokolldaten verschiedener Systeme in Korrelation und wertet diese aus, können Unregelmäßigkeiten oder Abweichungen im IT-Betrieb und damit potenzielle Angriffe erkannt werden. Eine Korrelation von Protokolldaten setzt zwingend ein Protokolldatum mit einem hinreichend hochauflösenden Datums- und Zeitstempel voraus.

Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes (TKG) und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) enthalten.

Zu § 2 Nummer 13

Verkehrsdaten sind nach der Legaldefinition in § 3 Nummer 70 des Telekommunikationsgesetzes (TKG) Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, wie beispielsweise das Transmission Control Protocol (TCP). Somit sind Verkehrsdaten die Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. Diese Daten sind nicht nur zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern, sondern insbesondere essenziell bei der Detektion von Angreifern in Daten- und Kommunikationsnetzen. Die Verarbeitungsbefugnis gilt nach § 13 zur Prüfung des Netzwerkverkehrs im CN LAVINE z. B. auf Schadprogramme oder Botnetze. Die Verkehrs- und Steuerdaten dürfen grundsätzlich nicht zu anderen Zwecken verarbeitet werden. Ihre Verarbeitung erfolgt grundsätzlich automatisiert.

Ab dem Moment, wo die Verkehrsdaten nicht mehr zur Abwicklung des Telekommunikationsdienstes (Informations- und Kommunikationsdienst) erforderlich sind, handelt es sich nicht mehr um Verkehrsdaten im Sinne des Telekommunikationsgesetzes (TKG) bzw. um Nutzungsdaten im Sinne des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDSG). Sie erhalten dann die Eigenschaft als Inhaltsdaten.

Zu § 2 Nummer 14

Der Begriff des Inhaltsdatums ist bisher nach deutschem Recht nicht legal definiert. § 160 Absatz 3 Nummer 8 des österreichischen Telekommunikationsgesetzes 2021 definiert Inhaltsdaten als die Inhalte übertragener Nachrichten.

Nachrichten sind jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Es handelt sich somit um Daten, die den Inhalt einer Kommunikation betreffen. Weil bei einer Kommunikation aber auch Verkehrsdaten übertragen werden, wurde eine Negativabgrenzung zu den Nutzungs- und Verkehrsdaten aufgenommen.

Zu § 2 Nummer 15

Die Aufnahme der Definition des Begriffs „Daten- und Kommunikationsnetz“ dient der rechtlichen Klarstellung und Präzisierung des Anwendungsbereichs des Gesetzes im Hinblick auf die Nutzung, den Betrieb und die Sicherheit informationstechnischer Infrastrukturen. Der Begriff ist zentral für die Bestimmung der Systeme, die in den Anwendungsbereich datengestützter Verfahren, digitaler Verwaltungsprozesse oder vernetzter Informationssysteme fallen.

Zu § 3

Zu Absatz 1

Die öffentliche Verwaltung ist für die Bereitstellung zentraler digitaler Verwaltungsdienstleistungen verantwortlich, deren Störungen oder Ausfälle erhebliche wirtschaftliche und gesellschaftliche Auswirkungen haben können. Die Vorschrift stellt klar, dass die Gewährleistung der Informationssicherheit eine wesentliche Aufgabe jeder Stelle ist und dem Schutz der Funktionsfähigkeit staatlicher und kommunaler Verwaltungsprozesse dient. Jede Stelle kann sich zur Wahrnehmung dieser Verantwortlichkeit eines geeigneten Dienstleisters bedienen, z. B. des ZDMV nach Maßgabe des ZDMVG.

Informationssicherheit umfasst dabei alle organisatorischen, technischen, personellen und infrastrukturellen Maßnahmen, die erforderlich sind, um Angriffe auf die Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit von Daten zu verhindern oder ihre Folgen zu begrenzen. Sie ist damit ein gesamtgesellschaftlicher Auftrag, der auf internationaler, nationaler und landesweiter Ebene wahrgenommen werden muss. Die Regelung steht im Einklang mit Erwägungsgrund 49 der Datenschutz-Grundverordnung, wonach die Verarbeitung personenbezogener Daten durch öffentliche Stellen, Computer Emergency Response Teams oder Betreiber von Kommunikations- und Datennetzen in einem begrenzten Umfang zulässig ist, soweit dies zur Gewährleistung der Netz- und Informationssicherheit erforderlich und verhältnismäßig ist. Hierzu zählen insbesondere Maßnahmen zur Abwehr unbefugter Zugriffe, zur Verhinderung der Verbreitung schädlicher Programmcodes sowie zur Erkennung und Abwehr von Angriffen auf informationstechnische Systeme. Neben der unmittelbaren Gefahrenabwehr gehören das Sammeln, Bewerten und Weitergeben von Informationen über Bedrohungen, Risiken und Schutzvorkehrungen sowie die gegenseitige Beratung und Warnung zu den wesentlichen Elementen einer funktionierenden Informationssicherheit.

Branchenspezifische Sicherheitsstandards (B3S) können zur Orientierung bei der Auswahl geeigneter Schutzmaßnahmen herangezogen werden, sofern sie den jeweiligen Anforderungen entsprechen und regelmäßig überprüft werden. Die Maßnahmen müssen den Stand der Technik berücksichtigen. Ein wirksames Informationssicherheitsmanagementsystem setzt zudem eine kontinuierliche Verbesserung und Überprüfung der getroffenen Maßnahmen voraus, wofür regelmäßige Sicherheitsprüfungen, Audits oder Penetrationstests erforderlich sind. Diese tragen dazu bei, die Wirksamkeit der bestehenden Schutzvorkehrungen sicherzustellen und das Sicherheitsniveau dauerhaft zu erhöhen.

Zu Absatz 2

Absatz 2 Satz 1 stellt die grundsätzliche Verantwortung der Leitung einer öffentlichen oder sonstigen Stelle klar. Leitungen tragen immer die Gesamtverantwortung für die u. a. vom Gesetzgeber übertragenen Aufgaben und die Qualität der erbrachten Leistungen einer öffentlichen oder sonstigen Stelle. Diese Gesamtverantwortung erfasst insbesondere die Sicherstellung der Einhaltung von Rechtsnormen, die Organisation der Arbeitsabläufe, den störungsfreien Ablauf wichtiger Verwaltungs- oder Geschäftsprozesse, die Bereitstellung notwendiger Ressourcen und Führung von Mitarbeitenden. Von diesem Grundsatz ist ebenfalls die Verantwortung für die Gewährleistung der Informationssicherheit nach innen und außen erfasst. Verantwortungen können delegiert, jedoch nicht übertragen werden. Letztendlich bleibt die Verantwortung immer bei der Leitung.

Insbesondere hat die Leitung Folgendes zu beachten, um ihrer Verantwortung nachzukommen:

Verantwortlichkeit	Konkretisierung
Verantwortung für Risikomanagement	Sie muss sicherstellen, dass ein angemessenes Risikomanagementsystem existiert, in dessen Rahmen Risiken identifiziert, bewertet und adressiert werden.
Billigung und Überwachung von Maßnahmen	Die Leitung muss die vom Risiko- und Sicherheitsmanagement vorgeschlagenen Maßnahmen zur Cybersicherheit formal genehmigen und deren Umsetzung überwachen.
Schulung und Kompetenz der Leitungsebene	Die Leitung muss über ausreichende Kenntnisse und Fähigkeiten zur IT-Sicherheit, Risikobeurteilung und Governance verfügen. Dazu sind Schulungen durchzuführen und nachzuweisen.
Festlegung von Rollen und Verantwortlichkeiten	Die Leitung muss klar definieren, welche Gremien oder Personen innerhalb der Organisation für Cybersicherheitsaufgaben verantwortlich sind (z. B. Chief Information Security Officer, IT-Sicherheitsfunktionen, Incident-Response, Krisenstab).
Integration in strategische und Investitionsentscheidungen	Die Leitung muss bei Mitzeichnungen und Genehmigung von IT-Maßnahmen darauf achten, dass Sicherheitsanforderungen frühzeitig in Projekte, Beschaffung, Investitionen und Vertragsabschlüsse berücksichtigt werden.

Verantwortlichkeit	Konkretisierung
Kontrolle, Audit und Überprüfung	Die Leitung muss sicherstellen, dass regelmäßige Audits, Überprüfungen, Evaluierungen und Anpassungen des Sicherheitsniveaus durchgeführt werden. Diese müssen nachgewiesen, dokumentiert und überwacht werden.
Meldepflichten und Eskalation	Die Leitung muss sicherstellen, dass Vorfälle mit erheblicher Auswirkung gemeldet werden und über das Berichtswesen informiert werden (z. B. Zwischenberichte, Abschlussberichte). Die Leitung trägt Mitverantwortung bei Nichteinhaltung.
Förderung einer Sicherheitskultur	Die Leitung muss geeignete Programme und Bewusstseinsmaßnahmen initiieren, um Cybersicherheit in der Organisation zu verankern.

Die Leitung ist grundsätzlich auch die Entscheidungsinstanz für den Umgang mit (IT-)Risiken. Nur sie kann die Rahmenbedingungen schaffen, Zuständigkeiten und Befugnisse zuweisen. Für den Bereich der Informationssicherheit konkretisiert der Satz 2 die Pflichten einer Leitung. Danach muss die Leitung ein Informationssicherheitsmanagementsystem planen, implementieren und pflegen. Für diese Aufgabe ist die jeweilige Leitung für die Bereitstellung und die Berücksichtigung der erforderlichen Haushaltsmittel im Rahmen der Haushaltsaufstellung verantwortlich. Um diese interdisziplinäre und komplexe Aufgabe zu erfüllen, wird der Leitung aufgegeben, eine beauftragte Person für Informationssicherheit (ISB) zu benennen. Die Delegierung dieser Aufgabe an eine beauftragte Person für Informationssicherheit entbindet die Leitung nicht von einer Kontrollpflicht, das heißt einer Prüfung, ob und wie die Aufgabe erfüllt bzw. umgesetzt wird. Üblicherweise erfolgt diese Kontrolle über ein regelmäßiges Berichtswesen.

Die Schulleitung als Behördenleitung trägt die Verantwortung für die Informationssicherheit, kann dies aber nur wirksam sicherstellen, wenn der Schulträger in seiner Verantwortung nach § 102 Absatz 2 Nummer 1 SchulG M-V die entsprechenden Planungen und Pflege des Informationssicherheitsmanagementsystems vornimmt. Die explizite Verankerung im Gesetzestext sichert hier die Klarheit der Aufgabenverteilung auch im Sinne des Schulgesetzes. Dies entbindet die Schulleitung nicht von den Aufgaben, sich entsprechend fortzubilden und Kompetenzen aufzubauen, um die notwendigen Entscheidungsprozesse fachkompetent überwachen zu können.

Zu Absatz 3

Ausgehend von Absatz 2 muss jede Leitung in die Lage versetzt werden, ihrer Verantwortung, insbesondere ihrer durch die festgelegte Aufgabendelegierung an die beauftragte Person für Informationssicherheit stärker auszuführenden Aufsichts-, Kontroll- und Prüfpflicht, angemessen nachkommen zu können. In diesem Kontext muss jede Leitung einer öffentlichen Stelle grundlegende Kenntnisse und Fähigkeiten im Bereich des Risikomanagements sowie der Managementpraktiken im Bereich der Informationssicherheit erwerben und aufrechterhalten.

Alle Schulungen zum Wissenserwerb und zur Wissensbewahrung sollen über eine zentrale E-Learning-Plattform bereitgestellt werden.

Die erforderlichen Schulungen sollen sicherstellen, dass die Leitung die wesentlichen Risiken, die mit dem Einsatz von Informationstechnik verbunden sind, kennen, angemessene Schutz-/ Sicherheitsmaßnahmen ergreifen und ihre Aufsichts-, Kontroll- und Prüfpflichten im Bereich der Informationssicherheit erfüllen können. Die regelmäßigen Wiederholungsschulungen sollen die Leitungen über die aktuelle Bedrohungslage informieren, das Bewusstsein sowie Sensibilität für ihre Verantwortung stärken. Schulungen vermitteln somit das notwendige und aktuelle Wissen, um diese Gesamtverantwortung effektiv wahrzunehmen.

Satz 3 legt fest, dass das in einem Informationssicherheitsmanagementsystem, das heißt in der Informationsmanagementorganisation tätige Personal, insbesondere die beauftragte Person für Informationssicherheit, über eine entsprechende Ausbildung und Fachkunde verfügen muss. Zusammen mit der Eigenschaft der Zuverlässigkeit zeichnet sich eine beauftragte Person für Informationssicherheit durch folgende Eigenschaften aus:

a) Fachwissen und Berufserfahrung:
Eine beauftragte Person für Informationssicherheit benötigt fundierte Kenntnisse in den Bereichen IT-Sicherheit, technischer Datenschutz, Risikomanagement, Sicherheitsstandards (beispielsweise ISO 27000-Normenreihe, IT-Grundschutz) sowie Erfahrungen im Projekt- und Change-Management.

b) Eigenverantwortung und Integrität:
Da eine beauftragte Person für Informationssicherheit Zugang zu sensiblen Informationen, teilweise auch Zugang zu Verschlusssachen besitzt, ist ein hohes Maß an Eigenverantwortung und Integrität unerlässlich. Dabei ist die Wahrung der Vertraulichkeit sensibler Informationen geboten.

c) Analytische Fähigkeiten und Kommunikationsfähigkeit:
Ein Informationssicherheitsmanagementsystem ist Teil des Risikomanagements. Eine beauftragte Person für Informationssicherheit sollte Risiken identifizieren, bewerten und praktikable Lösungen entwickeln können. Das Risikomanagement steht somit im Mittelpunkt der Arbeit einer beauftragten Person für Informationssicherheit. Darüber hinaus muss eine beauftragte Person für Informationssicherheit in der Lage sein, komplexe, teilweise nicht greifbare Sachverhalte verständlich zu vermitteln, sowohl gegenüber der Leitung als auch gegenüber Fachabteilungen und IT-Teams und Mitarbeitern.

Der abschließende Satz 4 definiert die Funktion des Chief Information Security Officers M-V, der festlegt, durch welche konkreten Schulungsmaßnahmen und Personenzertifizierungen die erforderliche Fachkunde erreicht und nachgewiesen wird. Dabei soll die Teilnahme an internen und externen Workshops dem Erfahrungsaustausch und den sogenannten Netzwerken (Aufbau und Pflege von persönlichen, beruflichen Kontakten) dienen. In der Gesamtsicht soll einheitliches, messbares und sich stets weiterentwickelndes Ausbildungsniveau der beauftragten Person für Informationssicherheit erzielt werden.

Für die Gewährleistung der Informationssicherheit ist der IT-Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik verpflichtend. Die für alle öffentlichen Stellen anzuwendende Fassung wird durch die Kommission für Informationssicherheit festgelegt. Für die sonstigen Stellen gelten die Sätze 1 und 2 nur, wenn kein branchenspezifischer Sicherheitsstandard oder keine Norm existiert. Die Kennzeichnung und Klassifizierung von Informationen erfolgt für die öffentlichen Stellen nach den Vorgaben des Traffic-Light-Protocols (TLP) in der jeweils gültigen Fassung.

Diese Verpflichtung tritt für die kommunalen Stellen [einsetzen: Datum des ersten Tages des vierundzwanzigsten auf die Verkündung folgenden Kalendermonats] in Kraft. Bis zu diesem Zeitpunkt ist das IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung für die kommunalen Stellen anzuwenden.

Zu Absatz 4

Dem IT-Planungsrat sind gemäß Artikel 91c Absatz 2 GG in Verbindung mit § 2 Absatz 1 des Vertrages über die Errichtung des IT-Planungsrates und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern (Vertrag zur Ausführung von Artikel 91c GG – IT-Staatsvertrag) Kompetenzen zur Festlegung von gemeinsamen Standards für die auszutauschenden Datenobjekte, Datenformate und Standards für Verfahren, die zur Datenübertragung erforderlich sind, sowie IT-Sicherheitsstandards übertragen worden. Zur Gewährleistung der Informationssicherheit hat der IT-Planungsrat als Bund-Länder-Gremium demnach IT-Sicherheits- bzw. Informationssicherheitsstandards festzulegen.

Die Beschlüsse des IT-Planungsrates entfalten für den Bund und die Länder gemäß § 2 Absatz 2 Satz 2 des IT-Staatsvertrages eine strikte Bindungswirkung. Flankiert wird diese Bindungswirkung gemäß § 15 Absatz 2 Satz 2 des Gesetzes zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (EGovG M-V). Bisher hat der IT-Planungsrat zwei solchermaßen verpflichtende Beschlüsse gefasst. Durch den Beschluss Nummer 2013/01 sowie folgend 2019/04 hat der IT-Planungsrat eine „Leitlinie für Informationssicherheit in der öffentlichen Verwaltung“ verabschiedet, die u. a. Informationssicherheitsstandards enthält, welche im Land Mecklenburg-Vorpommern umgesetzt werden müssen.

Aufgrund der dortigen Formulierung des Anwendungsbereichs der Leitlinie wirkte diese bisher gegenüber den kommunalen Trägern der Selbstverwaltung lediglich als Empfehlung und besaß keinen verbindlichen Charakter.

Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) verpflichtet Bund, Länder und Kommunen, ihre Verwaltungsleistungen über Verwaltungsportale digital anzubieten und diese Portale zu einem Verbund zu verknüpfen. Mit der Errichtung des Portalverbundes nimmt die Vernetzung der Informationstechnik auf allen Ebenen der öffentlichen Verwaltung weiter zu, was in angemessenen technisch und organisatorischen Schutz-/Sicherheitsmaßnahmen abzubilden ist.

Mit § 5 OZG wurde das Bundesministerium des Innern und für Heimat ermächtigt, für die im Portalverbund und für die zur Anbindung an den Portalverbund genutzten IT-Komponenten die zur Gewährleistung der Informationssicherheit erforderlichen Standards per Rechtsverordnung festzulegen, sodass von den hierzu erlassenen Regelungen durch Landesrecht nicht abgewichen werden kann (Artikel 84 Absatz 1 Satz 5 und 6 des Grundgesetzes).

Obwohl bestehende Rechtsnormen und Beschlüsse des Planungsrates zu Informationssicherheitsstandards keine unmittelbare Verbindlichkeit für die Träger der kommunalen Selbstverwaltung entfalten, sind die vom Bund und den Ländern angewandten Informationssicherheitsstandards durch die gemeinsame Nutzung von Informationstechnik mittelbar auch durch die kommunalen Träger der Selbstverwaltung anzuwenden.

Dies zeigt sich konkret immer dann, wenn die Träger der kommunalen Selbstverwaltung beispielsweise die sicheren Daten- oder Kommunikationsnetze der Länder und des Bundes zur Erbringung von Verwaltungsdienstleistungen mitnutzen und sie sich somit den Anschlussbedingungen an diese Netze „freiwillig“ unterwerfen. Somit schließt der Absatz 4 Satz 1 im Wesentlichen nur eine bestehende gesetzliche Lücke, indem alle staatlichen und kommunalen Stellen den nun festgelegten Informationssicherheitsstandard IT-Grundschutz des BSI verbindlich anwenden.

Da die jeweiligen Aktualisierungen des BSI-Grundschutzes regelmäßig Anpassungen in der technischen und organisatorischen Umsetzung erfordern, ist es den öffentlichen Stellen nicht in jedem Fall möglich, die jeweils neueste Fassung unverzüglich vollständig anzuwenden.

Um eine geordnete und einheitliche Einführung sicherzustellen, entscheidet die Kommission für Informationssicherheit, ab welchem Zeitpunkt eine neue Fassung des BSI-Grundschutzes verbindlich anzuwenden ist und wie lange die Anwendung einer vorhergehenden Fassung noch zulässig bleibt. Dadurch wird den öffentlichen Stellen ein angemessener Zeitraum eingeräumt, die erforderlichen Maßnahmen zu planen, Ressourcen zu beschaffen und die notwendigen Anpassungen umzusetzen.

Der IT-Grundschutz des BSI ist somit eine seit über 30 Jahren bewährte Methodik.

Verbunden mit der letzten Neuerung im Jahr 2017 trägt der vormalige IT-Grundschutz-Katalog nun die Bezeichnung IT-Grundschutz-Kompendium. Inhaltlich erfolgte ein Paradigmenwechsel. Die ehemaligen Maßnahmenvorgaben wurden in (Sicherheits-)Anforderungen umformuliert: Während zuvor eine klare Vorgabe zur Umsetzung einer Maßnahme existierte, wird nunmehr mit Blick auf den internationalen Standard ISO/IEC 27001 lediglich das Ziel der Anforderung definiert. Wie diese Anforderung von einer Organisation umgesetzt wird, entscheidet diese eigenverantwortlich selbst.

Nach dem IT-Grundschutz-Kompendium müssen immer beispielsweise folgende Anforderungen durch eine Organisation umgesetzt werden: Erstellung, Aktualisierung und Fortschreibung von
a) Konzepten in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
b) Konzepten für die Zugangs- und Zugriffskontrolle sowie Management von IT-Systemen,
c) Konzepten zur Bewältigung von Sicherheitsvorfällen (Emergency Response),
d) Konzepten zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Informationssicherheit (Sicherheitsprüfungen),
e) Konzepten für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung,
f) Konzepten zur Aufrechterhaltung des IT-Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement (Business Recovery).

Aus den derzeit 111 IT-Grundschutz-Bausteinen mit ihren jeweiligen Anforderungen des IT-Grundschutz-Kompendiums lassen sich darüber hinaus wesentliche Schutz-/Sicherheitsmaßnahmen ableiten:

a) Maßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen einschließlich Management und Offenlegung von Schwachstellen,
b) Maßnahmen zur Sicherheit in Lieferketten einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Stellen und ihren unmittelbaren Anbietern oder Diensteanbietern,

c) Maßnahmen für grundlegende Verfahren im Bereich der Informationssicherheitshygiene und Schulungen im Bereich der Informationssicherheit,
d) Sicherheit des Personals, Verwendung von risikoorientierten Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme.

Dieser Sicherheitsstandard gilt auch in vielen KRITIS-Sektoren als Maßstab, wenn es um die Absicherung von Informationen (Daten) und insbesondere um den Aufbau eines Informationssicherheitsmanagementsystems geht. Im Mittelpunkt des modular aufgebauten IT-Grundschutz-Kompendiums stehen die IT-Grundschutz-Bausteine. Gegenstand eines IT-Grundschutz-Bausteins können übergeordnete Themen sein, wie beispielsweise das Informationssicherheits- oder Business Continuity Management (BCM), aber auch mehr oder weniger spezielle technische Systeme, die üblicherweise in Behörden im Einsatz sind. In den Texten wird jeweils ein Thema zu allen relevanten Sicherheitsaspekten beleuchtet. Die IT-Grundschutz-Bausteine sind in zehn unterschiedliche Schichten aufgeteilt und reichen thematisch von Anwendungen (APP) über Industrielle IT (IND) bis hin zum Sicherheitsmanagement (Informationssicherheitsmanagementsystem).

Die BSI-Standards zusammen mit dem BSI-IT-Grundschutz-Kompendium bilden den IT-Grundschutz (vollständige Bezeichnung: ISO 27001 auf der Basis von IT-Grundschutz).

Der Gesetzgeber hat in § 8a Absatz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik vorgesehen, dass Verbände verschiedener Industrien branchenspezifische Sicherheitsstandards (B3S) entwickeln können. Die Erstellung eines B3S ist für die jeweilige Branche eine Chance, ausgehend von der eigenen Fachexpertise selbst Vorgaben zum „Stand der Technik“ und darüber hinaus zu formulieren. So existieren zwischenzeitlich für die KRITIS-Sektoren Energie, Wasser, Ernährung, IT und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr entsprechende B3S. Absatz 5 Satz 2 verpflichtet die sonstigen Stellen, entweder die B3S oder andere branchenspezifische Sicherheitsnormen anzuwenden. Sofern branchenspezifische Sicherheitsstandards oder -normen nicht existieren, ist verpflichtend der IT-Grundschutz anzuwenden.

Aus der verpflichtenden Anwendung des IT-Grundschutzes ergibt sich keine verfahrensbezogene Pflicht zu einer ISO 27001-Zertifizierung auf Basis von IT-Grundschutz.

Die Informationsklassifizierung ist ein wichtiger Bestandteil des Informationssicherheitsmanagementsystems und hilft, den Wert und die Sensibilität von Informationen zu bestimmen. Darüber hinaus ermöglicht die Klassifizierung, angemessene Schutz- und Sicherheitsmaßnahmen zu ergreifen und somit den Zugriff auf sensible Informationen (Daten) zu kontrollieren. Für die öffentlichen Stellen wird das Traffic-Light-Protocol (TLP) für die Informationsklassifizierung und für die Informationsverarbeitung verbindlich festgelegt. Bei der Anwendung des Traffic-Light-Protocols werden alle Informationen in eine von fünf Klassen eingeteilt, welche die Bedingungen für ihre Verarbeitung regeln. Das Traffic Light Protocol (TLP) dient der freiwilligen, standardisierten Kennzeichnung und Weitergabe von sensiblen Informationen in der Cybersicherheits- und Informationsaustauschpraxis und beruht auf Vertrauen, nicht auf rechtlichen Vorgaben. Die Verschlusssachenanweisung (VSA) hingegen regelt verbindlich und rechtlich den Umgang mit amtlichen Verschlusssachen und deren Schutzstufen (VS-NfD bis VS-Geheim), um die nationale Sicherheit und dienstliche Geheimhaltung zu gewährleisten.

Der Absatz 4 sieht für die kommunalen Stellen eine Übergangsfrist vor, um die erforderlichen Schritte bis zur vollständigen Anwendung und Umsetzung des IT-Grundschutzes, Standard-Absicherung innerhalb von 24 Monaten des auf die Verkündung folgenden Monats vorzubereiten.

Die kommunalen Spitzenverbände haben im Jahr 2018 die Version 1.0 des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ veröffentlicht. Das IT-Grundschutz-Profil wurde von der Arbeitsgruppe kommunale Basis-Absicherung (AG koBA) der kommunalen Spitzenverbände erstellt und fortgeschrieben. In ebenenübergreifenden IT-Verfahren und Anforderungen von Bund und Ländern, beispielsweise zu Wahlen und dem Zensus, wird bereits auf dieses IT-Grundschutz-Profil als de-facto Mindestsicherheitsstandard verwiesen.

Das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ richtet sich an Kommunalverwaltungen, die einen systematischen Einstieg in die Informationssicherheit suchen. Es ermöglicht Kommunen eine zunächst breite, grundlegende Erst-Absicherung und erleichtert den Einstieg in die Informationssicherheit. Das IT-Grundschutz-Profil basiert auf den BSI-Standards der 200er-Reihe und auf dem IT-Grundschutz-Kompendium. Es definiert Mindestsicherheitsanforderungen, die in einer Kommunalverwaltung zwingend umzusetzen sind.

Das IT-Grundschutz-Profil erleichtert somit den Einstieg in die Informationssicherheit und hilft, die wesentlichen, im kommunalen Umfeld bekannten organisatorischen und technischen Schwachstellen aufzuzeigen, die es zu beseitigen gilt, um möglichst schnell das durch dieses Gesetz geforderte Sicherheitsniveau in der Breite anzuheben. In diesem Kontext ist die verpflichtende Anwendung dieses IT-Grundschutz-Profils als Zwischenschritt geeignet.

Zu Absatz 5

Neben der allgemeinen Verpflichtung der öffentlichen Stellen, die Sicherheitsanforderungen aus dem nationalen Sicherheitsstandard IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) umzusetzen und aufrechtzuerhalten, erweitert und konkretisiert Absatz 5 diese Verpflichtung dahingehend, dass auch bei der (Mit-)Nutzung von Informationstechnik der öffentlichen Stellen durch Organisationen, die nicht vom Geltungsbereich dieses Gesetzes erfasst sind, das Sicherheitsniveau nicht gefährdet werden darf. Es erfolgt somit eine Verpflichtung der öffentlichen Stellen,

- bei der Auslagerung ihrer Informationstechnik (Outsourcing) den IT-Dienstleister auf den IT-Grundschutz vertraglich zu verpflichten und
- die nutzenden Organisationen auf die Umsetzung und Aufrechterhaltung der Sicherheitsanforderungen des zugrunde liegenden Sicherheitskonzeptes in der Risikosphäre des Nutzenden zu verpflichten.

Ein Sicherheitskonzept wird beispielsweise bei einer Client-Server-Architektur auch die Sicherheitsanforderungen auf der Client-Seite umfassen. Dort sind die Sicherheitsanforderungen durch stellen- oder einrichtungsspezifische Schutz- und/oder Sicherheitsmaßnahmen umzusetzen.

Die Verpflichtung auf den IT-Grundschutz erfolgt grundsätzlich auf vertraglicher Basis zwischen der verfahrensverantwortlichen Stelle (siehe § 8), der nutzenden sonstigen Stelle oder Einrichtung sowie dem jeweiligen IT-Dienstleister. Sonstige Einrichtung sind Organisationen, die nicht vom Geltungsbereich dieses Gesetzes erfasst sind.

Aufgrund der besonderen Rolle der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH in der Landes-Informationstechnik werden die IT-Landesdienstleister explizit auf die Anwendung und Umsetzung der Sicherheitsanforderungen des IT-Grundschutzes verpflichtet.

Zu Absatz 6

Sowohl die Betriebsaufnahme neuer Informationstechnik als auch Änderungen an der bestehenden Informationstechnik können die Informationssicherheit negativ beeinflussen. Eine wesentliche Änderung in der Informationstechnik bezieht sich auf signifikante Anpassungen informationstechnischer Systeme oder Komponenten oder auf Prozesse, wodurch neue Risiken entstehen oder sich bestehende Risiken erhöhen. Diese Änderungen erfordern daher eine Neubewertung, um sicherzustellen, dass die Sicherheitsanforderungen aus dem zugrunde liegenden Sicherheitskonzept weiterhin erfüllt und wirksam sind. In der Regel werden fehlerbereinigende Updates und insbesondere Sicherheitsupdates nicht als wesentliche Änderung betrachtet. Da die Auswirkungen systemindividuell oder behördenspezifisch ausfallen, insbesondere bei Änderungen an der Informationstechnik, sollte die jeweilige beauftragte Person für Informationssicherheit festlegen, über welche konkreten Änderungen informiert werden soll. Die verfahrensverantwortliche Stelle hat in diesen Fällen dann ein Einvernehmen mit der beauftragten Person für Informationssicherheit herzustellen.

Nach den allgemeinen verwaltungsrechtlichen Grundsätzen bedeutet „Einvernehmen“ die Verpflichtung, eine Rechtshandlung vorher mit dem Organ in dem Sinne zu beraten, die Gelegenheit zur Stellungnahme zu geben und eine übereinstimmende Verständigung herbeizuführen. Die Herstellung des Einvernehmens sollte der Regelfall sein. Für den Einzelfall, dass das Einvernehmen nicht hergestellt werden kann, greifen die Regelungen des Absatzes 6 Satz 4, da keine blockierende Situation (Pattsituation) entstehen darf. Die Erfahrung hat gezeigt, dass das „Benehmen“ nicht ausreichend ist, um die Schutzziele der Informationssicherheit ausreichend zu würdigen. Vielmehr würde es bei einem Benehmen darauf hinauslaufen, eine kurzfristige Informationsweitergabe zu generieren und anschließend mit der Rechtshandlung fortzufahren, ohne die begründeten Einlassungen der beauftragten Person für Informationssicherheit zu berücksichtigen.

Bei zentraler Informationstechnik ist zusätzlich das Einvernehmen des Chief Information Security Officers M-V erforderlich. Dies liegt begründet in der Natur der zentralen Informationstechnik, da diese essenziell für die Arbeits- und Handlungsfähigkeit der Landes- und Kommunalverwaltung ist.

Abweichend von den Regelungen zur zentralen Informationstechnik entscheidet in allen anderen Fällen letztinstanzlich immer die jeweilige Leitung der verfahrensverantwortlichen Stelle.

Zu Absatz 7

Sicherheit erfordert Investitionen in Technologien, Prozesse, Schulungen und Personal, um ein angemessenes Sicherheitsniveau zu gewährleisten. Absatz 7 stellt klar, dass die Landesverwaltung diese für die Informationssicherheit erforderlichen Mittel aus den IT-Haushaltsansätzen bereitzustellen und in den Betriebsverträgen auszuweisen hat. Sicherheitskosten sind fester Bestandteil aller IT- und Digitalisierungsmaßnahmen und von Beginn an einzuplanen. Damit wird ein einheitliches Sicherheitsniveau sichergestellt und die transparente Finanzierung von Informationssicherheitsmaßnahmen gewährleistet.

Zu Absatz 8

Der Absatz 8 ist ein Ausfluss aus dem (IT-)Risikomanagement, das ein wesentlicher Bestandteil eines Informationsmanagementsystems darstellt. Das Risikomanagement beinhaltet ein systematisches Vorgehen bzw. einen Prozess zur Identifizierung, Bewertung und Behandlung von Risiken, das heißt eine aktive Steuerung von Risiken. Somit umfasst ein Risikomanagement die Anwendung von Methoden und Werkzeugen zur Risikobehandlung in Form von organisatorischen und technischen Schutz-/Sicherheitsmaßnahmen zur Risikovermeidung, -minimierung, -transfer und/oder -kontrolle, um eine kontinuierliche Arbeits- und Handlungsfähigkeit der jeweiligen Organisation zu gewährleisten und finanzielle Verluste sowie Reputationsschäden zu vermeiden. Nach Ausschöpfung aller Instrumente der Risikobehandlung wird – mit Ausnahme der Risikovermeidung – immer ein Restrisiko bleiben, welches durch die Leitung in der Form einer Risikoübernahme begründet zu dokumentieren ist, um Transparenz und Nachvollziehbarkeit zu gewährleisten. Danach ist die Auswahl sowie der Einsatz von Schutz-/Sicherheitsmaßnahmen für die Gewährleistung der Schutzziele der Informationssicherheit von einer vorgängigen Risikoanalyse abhängig, Kosten und Nutzen in einem spezifisch risikoadäquaten Ausgleich zu bringen. Die Gewährleistung der Schutzziele wird durch angemessene Schutz-/Sicherheitsmaßnahmen, die dem Stand von Wissenschaft und Technik entsprechen, sichergestellt.

Es sind jedoch Einzelfälle denkbar, bei denen die wirtschaftlich umsetzbaren Schutz-/ Sicherheitsmaßnahmen nicht ausreichend sind, um die mit dem Einsatz von Informationstechnik verbundenen Risiken ausreichend zu behandeln. In diesen Fällen muss vom Einsatz der Informationstechnik Abstand genommen werden.

Satz 4 greift den Regelfall dahingehend auf, dass Konflikte im Rahmen einer angemessenen Risikobehandlung zwischen dem Chief Information Security Officer M-V und der oder dem CIO das Einvernehmen nicht hergestellt werden kann. Diese Situation wird dahingehend aufgelöst werden, dass eine abschließende Entscheidung durch die für die Digitalisierung zuständige oberste Landesbehörde in jedem Einzelfall über konkrete Maßnahmen zur Risikobehandlung zu treffen ist. Wird von den jeweiligen Entscheidungen des Chief Information Security Officers M-V abgewichen, ist dies gesondert fachlich zu begründen. Die Begründung ist nachvollziehbar zu dokumentieren.

Sofern es sich nicht um zentrale Informationstechnik handelt, trifft diese Entscheidung die Leitung der verfahrensverantwortlichen Stelle bzw. Organisationseinheit.

Zu § 4

Zu Absatz 1

Als Ausfluss aus § 11 Absatz 7 erfolgt durch den Absatz 1 die Ermächtigung der für die Digitalisierung zuständigen obersten Landesbehörde, weiterführende Konkretisierungen für die Erhebung, Speicherung, Archivierung, Übertragung und Auswertung von Protokoll-, Verkehrs- und Inhaltsdaten durch Rechtsverordnung zu regeln. Die für diesen Regelungsbedarf als wesentlich angesehenen Inhalte sind in den Nummern 1 bis 5 verankert.

Dieser durch Rechtsverordnung notwendige Regelungsbedarf ist erforderlich, um einheitliche Sicherheits- und IT-Standards für alle öffentlichen Stellen und deren – auch privatrechtlich organisierte – (IT-)Dienstleister verbindlich zu definieren, um ein einheitliches Sicherheitsniveau bei der Protokollierung, der Detektion und bei der Gefahrenwehr zu etablieren und weiterzuentwickeln. Das CERT M-V muss in die Lage versetzt werden, zur Aufgabenerfüllung die erforderlichen Informationen und Daten zu erhalten.

Der Regelungsinhalt betrifft insbesondere den verschlüsselten Netzwerkverkehr, wie dieser bei einer Kommunikation zwischen einem Webbrowser und einem Web-Server zur Anwendung kommt, durch geeignete technische Schutz-/Sicherheitsmaßnahmen aufzubrechen und diesen insbesondere auf Angriffsmuster und Schadcode zu analysieren. Verschlüsselter Netzwerkverkehr ist das primäre Werkzeug für Cyberangriffe; ca. 95 Prozent der gefährlichen Codes verbergen sich hinter einer SSL- oder TLS-Verschlüsselung. Deep Observability – also Sichtbarkeit bis auf die Netzwerkebene – ist im Kontext mit der Gewährleistung der Informationssicherheit zu einem absoluten Must-have erwachsen.

Zu Absatz 2

Für Systeme und Informationen sowie Daten, die der Geheimhaltung nach dem Sicherheitsüberprüfungsgesetz (SÜG) und der Verschlusssachenanweisung (VSA) unterliegen, sollten aufgrund der Geheimhaltungsbedürfnisse wie auch der für derartige Systeme in den Geheimschutzvorschriften bereits ohnehin geltenden erhöhten Sicherheitsanforderungen der Umfang und die Form der entsprechenden Rechte und Pflichten durch eine Verordnung geregelt werden. Die für den Verfassungsschutz zuständige oberste Landesbehörde wird daher in Absatz 2 ermächtigt, im Benehmen mit der für Digitalisierung zuständigen obersten Landesbehörde spezielle Regelungen zu treffen, um Meldungen und Kontrolle unter Wahrung des Geheimschutzes rechtssicher zu gestalten.

Zu Absatz 3

Absatz 3 ermächtigt die für die Digitalisierung zuständige oberste Landesbehörde durch Rechtsverordnung, im Einvernehmen mit den jeweils datenschutzrechtlichen Verantwortlichen zu regeln, welcher der gemeinsamen Verantwortlichen für die Wahrnehmung oder Erfüllung der jeweiligen datenschutzrechtlichen Rechte und Pflichten zuständig ist. Bei der Verarbeitung personenbezogener Daten durch mehrere Verantwortliche ist nach Artikel 26 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 in einer Vereinbarung in transparenter Form festzulegen, wer von ihnen welche Verpflichtungen nach der Verordnung (EU) 2016/679 erfüllt. Die Regelung in Absatz 3 setzt diese Verpflichtung aus Praktikabilitätsgründen in Form einer Verordnungsermächtigung um.

Zu Abschnitt 2

In einem Informationssicherheitsmanagementsystem (Informationssicherheitsmanagement-system) bildet die Organisation der Informationssicherheit eine wesentliche und tragende Säule zur Umsetzung einer Sicherheitsstrategie bzw. einer Informations- und Datensicherheitsstrategie. In diesem Kontext ist die Etablierung einer geeigneten Organisationsstruktur erforderlich, die neben der Formulierung von Zielen die Gestaltung des Systems und die Steuerung von Prozessen zur Zielerreichung gemeinsam angeht.

In Abschnitt 2 wird die Organisation der Informationssicherheit der öffentlichen Stellen im Land Mecklenburg-Vorpommern beschrieben. Aufgaben, Kompetenzen, Rechte und Pflichten der jeweiligen Akteure auf der strategischen, taktischen und operativen Ebene werden festgelegt.

Zu § 5

Zu Absatz 1

Die Funktion des Chief Information Security Officers M-V bildet die zentrale und strategische Instanz in der Informationssicherheitsorganisation aller öffentlichen und sonstigen Stellen im Land Mecklenburg-Vorpommern. Die durch eine Beschäftigte oder einen Beschäftigten des Landes Mecklenburg-Vorpommern zu besetzende Funktion ist in der Organisationsstruktur der für die Digitalisierung zuständigen obersten Landesbehörde anzusiedeln. Satz 2 legt somit indirekt auch fest, dass diese Funktion nicht ausgelagert werden darf (kein Outsourcing).

Der Chief Information Security Officer M-V wird von der oder dem CIO M-V ernannt und nimmt die in Absatz 3 definierten Aufgaben und Befugnisse unabhängig und weisungsfrei wahr. Die Unabhängigkeit und Weisungsfreiheit des Chief Information Security Officers M-V ist u. a. durch eine geeignete Ausgliederung aus dem Geschäftsbetrieb (Organisationsstruktur) der für die Digitalisierung zuständigen obersten Landesbehörde sicherzustellen. Nur bei einer Beschäftigung im öffentlichen Dienst des Landes besteht die erforderliche dienstrechtliche Einbindung, die eine uneingeschränkte Wahrnehmung der Aufgaben in voller Verantwortlichkeit gegenüber der Behördenleitung ermöglicht. Zudem sind hierdurch die Einhaltung dienst-rechtlicher Pflichten, die Wahrung von Verschwiegenheit und Geheimschutz sowie die Verbind-lichkeit behördeninterner Weisungs- und Meldewege gewährleistet.

Um die Aufgaben eines Chief Information Security Officers sachgerecht wahrnehmen zu können, sind allerdings umfangreiche Kompetenzen und Fähigkeiten, insbesondere Wissen über die eingesetzten IT-Verfahren, die verarbeiteten Informationen und Daten sowie die Verfahrens-weisen und die Organisationskultur der jeweiligen Behörde, notwendig. Die Funktion des Chief Information Security Officers ist eine wesentliche, gesetzliche und auf Dauer ausgerichtete Funktion innerhalb einer staatlichen Stelle.

Dementsprechend muss der Chief Information Security Officer nicht nur zuverlässig sein, sondern zeichnet sich durch folgende Eigenschaften aus:

a) Fachwissen und Berufserfahrung:
d. h. fundierte Kenntnisse in den Bereichen IT-Sicherheit, technischer Datenschutz, Risikomanagement, Sicherheitsstandards (beispielsweise ISO 27000-Normenreihe, IT-Grundschutz) sowie Erfahrungen im Projekt- und Change-Management.

b) Eigenverantwortung und Integrität:
Da der Chief Information Security Officer Zugang zu sensiblen Informationen, teilweise auch Zugang zu Verschlusssachen besitzt, ist ein hohes Maß an Eigenverantwortung und Integrität unerlässlich. Dabei ist die Wahrung der Vertraulichkeit sensibler Informationen geboten.

c) Analytische Fähigkeiten und Kommunikationsfähigkeit:
Ein Informationssicherheitsmanagementsystem ist Teil des Risikomanagements. Der Chief Information Security Officer sollte Risiken identifizieren, bewerten und praktikable Lösungen entwickeln können. Darüber hinaus muss er in der Lage sein, komplexe, teilweise nicht greifbare Sachverhalte verständlich zu vermitteln, sowohl gegenüber der Leitung als auch gegenüber Fachabteilungen und beauftragten Personen für Informationssicherheit.

Der Chief Information Security Officer M-V sollte Workshops und Erfahrungsaustausche nutzen, um das erforderliche Fach- und Erfahrungsniveau kontinuierlich zu sichern, fortzuentwickeln und an neue Anforderungen anzupassen.

Darüber hinaus ist der Chief Information Security Officer M-V für die in Absatz 3 übertragenen Aufgaben und Befugnisse angemessen auszustatten.

Die Funktion des Chief Information Security Officers M-V erfordert ein unmittelbares Handeln. In diesem Kontext wird der Chief Information Security Officer M-V neben dem direkten Vorspracherecht bei der oder dem CIO M-V zusätzlich mit einem direkten Vorspracherecht bei der Leitung der für die Digitalisierung zuständigen obersten Landesbehörde des Landes Mecklenburg-Vorpommern ausgestattet.

Zu Absatz 2

In Anlehnung an den bereits gesetzlich verankerten Kündigungsschutz eines Datenschutzbeauftragten (vergleiche § 6 Absatz 4 des Bundesdatenschutzgesetzes) oder eines Mitglieds eines Personalrates (vergleiche § 55 des Bundespersonalvertretungsgesetzes) soll dieser Schutz ebenfalls für den Chief Information Security Officer M-V gelten. Der Chief Information Security Officer M-V genießt einen besonderen Schutz, der sowohl die Unzulässigkeit von Abordnung, Umsetzung als auch Versetzung beinhaltet.

Der gesetzliche Schutz für den Chief Information Security Officer M-V soll sicherstellen, dass dieser seine Aufgaben und Befugnisse unabhängig und ohne Bedenken vor einer Benachteiligung durch den Dienstherrn wahrnehmen kann. Dieser Schutz ist somit ein tragendes Element, um die in Absatz 1 festgelegte Unabhängigkeit und Wirksamkeit des Chief Information Security Officers M-V sicherzustellen.

Zu Absatz 3

Absatz 3 legt die wesentlichen Aufgaben fest und überträgt die Vertretung des Landes Mecklenburg-Vorpommern in allen Bund-/Ländergremien im Bereich der Informationssicherheit dem Chief Information Security Officer M-V.

Der Chief Information Security Officer M-V gibt grundsätzlich in Einvernehmen mit der Kommission für Informationssicherheit für alle öffentlichen Stellen verbindliche Richtlinien und Sicherheitsstandards mit Blick auf eine landesspezifische Konkretisierung der Sicherheitsanforderungen aus dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik vor. Ziel dieser Konkretisierungen ist es, ein einheitliches, gemeinsames Verständnis sowie einheitliches hohes Niveau der Informationssicherheit bei allen öffentlichen Stellen zu schaffen. Eine Umsetzung stellenspezifischer Eigen- oder Besonderheiten ist möglich. Nur durch zentrale Vorgaben (Richtlinien und Standards) kann sichergestellt werden, dass Sicherheitslücken, insbesondere Schwachstellen, die Sicherheit der Daten- und Kommunikationsnetze, insbesondere des CN LAVINE, nicht gefährden.

Eine gesetzlich verankerte Beratungspflicht des Chief Information Security Officers M-V soll den öffentlichen Stellen die Umsetzung und Einhaltung der landesspezifischen Sicherheitsstandards und Richtlinien erleichtern. Zusätzlich erhält der Chief Information Security Officer M-V dadurch Rückmeldungen aus der Praxis. Diese Rückmeldungen fließen wiederum in die Fortschreibung der Richtlinien und Sicherheitsstandards ein. Die Verantwortung für die Umsetzung bleibt jedoch bei den öffentlichen Stellen. Für die sonstigen Stellen haben die landesspezifischen Sicherheitsstandards und Richtlinien grundsätzlich einen empfehlenden Charakter.

Die in § 3 Absatz 4 Satz 3 nicht weiter konkretisierte Fachkunde der beauftragten Person für Informationssicherheit wird in der Festlegung erforderlicher Qualifikationen des Chief Information Security Officers M-V für die staatlichen Stellen übertragen. Damit wird der bis 2023 durch den BeLVIS wahrgenommenen Aufgabe zur zentralen Durchführung und zentralen Finanzierung von Qualifikationsmaßnahmen Rechnung getragen.

Darüber hinaus wird das Berichtswesen, insbesondere die Berichtspflicht des Chief Information Security Officers M-V gegenüber der oder dem CIO M-V, dem Lenkungsausschuss E-Government und in der Kommission für Informationssicherheit, definiert. Der Chief Information Security Officer M-V wird jährlich gegenüber der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern zu durchgeführten Maßnahmen der Protokollierung gemäß §§ 12 bis 15, 19 berichten, auch wenn und wie bei den Maßnahmen der Protokollierung in die Grundrechte eingegriffen wird.

Eine regelmäßige Unterrichtung zu dringlichen, wichtigen und aktuellen Themen der Informationssicherheit ermöglicht es den jeweiligen Gremien, aktuelle und zukünftige (Sicherheits-) Risiken beim Einsatz von Informationstechnik zu beurteilen, Maßnahmen einzuleiten und gegebenenfalls vorausschauend Entscheidungen zu treffen.

Zu Absatz 4

Der Absatz 4 dient der Umsetzung von Artikel 8 Absatz 1 und 2 der NIS-2-Richtlinie. Danach sind Behörden für die Überwachung der Anwendung der NIS-2-Richtlinie vorzusehen. Im Land Mecklenburg-Vorpommern wird diese Aufgabe dem Chief Information Security Officer M-V unter Mitwirkung der Kommission für Informationssicherheit übertragen, da sich diese Aufgabe in die bereits bestehende und nun durch dieses Gesetz erweitere Informationssicherheits-organisation einfügt.

Die staatlichen Stellen (auf Landesebene), die nach Artikel 2 Absatz 2 Buchstabe f Nummer ii der NIS-2-Richtlinie unter die NIS-2-Richlinie fallen, werden von dem Chief Information Security Officer dem Bund zur Übermittlung an die Europäische Union gemeldet. Die Meldung erfolgt auf Grundlage eines von der Kommission für Informationssicherheit nach § 6 Absatz 8 beschlossenen Identifizierungskonzeptes, das auf dem den Ländern zur Anwendung empfohlenen Beschluss 2023/39 des IT-Planungsrates vom 3. November 2023 basiert.

Zu Absatz 5

Erfüllungs- und Erfolgskontrollen von Schutz-/Sicherheitsmaßnahmen, die sich u. a. aus den Umsetzungen von Richtlinien und Sicherheitsstandards ergeben, stellen eine wesentliche Grundlage zur Feststellung der Wirksamkeit sowie zur Weiterentwicklung eines Informations-sicherheitsmanagementsystems dar. Somit zielt die Prüftätigkeit des Chief Information Security Officers M-V darauf ab, die Informationssicherheit kontinuierlich zu verbessern, rechtzeitig Fehlentwicklungen zu erkennen und diese zu vermeiden und die Wirtschaftlichkeit zu optimieren.

Damit der Chief Information Security Officer M-V seinen Aufgaben gerecht werden kann, erhält er nach Absatz 4 die hierfür notwendigen Rechte, die für die Ausübung der Prüfrechte erforderlichen Auskünfte und Unterlagen zu verlangen. Darüber hinaus wird der Chief Information Security Officer M-V berechtigt, selbst Sicherheitsprüfungen bei den öffentlichen und sonstigen Stellen vorzunehmen.

Unter dem Begriff Sicherheitsprüfungen sind IS-Audits, IS-Revisionen, IS-Webchecks, IS-Penetrationstests auf Basis der jeweiligen Praxis-Leitfäden des BSI zu verstehen. Während und nach der Durchführung von Sicherheitsprüfungen sind zum einen Störungen im Betriebs-ablauf zu vermeiden. Darüber hinaus wird die Vertraulichkeit der überlassenen bzw. eingesehenen Unterlagen strikt gewahrt. Satz 3 dient zur Vermeidung von Mehrfachprüfungen.

Der abschließende Satz 4 erweitert die Kontroll- und Prüfbefugnisse dahingehend, dass der Chief Information Security Officer M-V berechtigt ist, unmittelbar bei den von den öffentlichen oder sonstigen Stellen beauftragten Dienstleistern Prüfungen selbst oder im Auftrag vorzunehmen, Auskünfte zu verlangen und Unterlagen einzusehen bzw. diese übermittelt zu bekommen. Mit diesem Recht einhergehend haben die öffentlichen und sonstigen Stellen entsprechende vertragliche Vereinbarungen mit ihren Dienstleistern zu treffen, damit der Chief Information Security Officer M-V seine Erfüllungs- und Erfolgskontrollen unmittelbar bei den Dienstleistern ausüben kann.

Zu Absatz 6

Absatz 6 stellt die zentrale Befugnisnorm des Chief Information Security Officers M-V gegenüber den an den Daten- und Kommunikationsnetzen der öffentlichen Verwaltung angeschlossenen öffentlichen und sonstigen Stellen dar. Derzeit wird unter den Daten- und Kommunikationsnetzen der öffentlichen Verwaltung primär das CN LAVINE verstanden. Aufgrund bereits erkennbarer und notwendiger netzwerktechnischer Änderungen in Netzdesign und -architektur des CN LAVINE wurde im Wortlaut dieses Gesetzes ein generischer, weit umfassender Begriff eingeführt. Erfasst sind somit ebenfalls Kommunal- und Bildungsnetze.

Die Befugnisnorm zur Gefahrenabwehr für die Informationstechnik umfasst Anordnungen sowie eine Selbstvornahme von Maßnahmen durch den Chief Information Security Officer M-V. Dabei ist stets der Verhältnismäßigkeitsgrundsatz zu beachten, insbesondere ist bei Eingriffen das mildeste und geeignetste Mittel zur Erreichung des Zwecks zu wählen. Hierzu gehört es, dass die Maßnahmen des Chief Information Security Officers M-V erst dann ergriffen werden sollen, wenn die getroffenen Anordnungen (und Unterstützungsangebote) trotz angemessener Umsetzungsfrist erfolglos geblieben sind. Grundsätzlich werden die erforderlichen Maßnahmen, um Gefahren für die Informationstechnik, die mit den Daten- und Kommunikationsnetzen der öffentlichen Verwaltung verbunden sind, abzuwehren, durch die öffentlichen und sonstigen Stellen selbst getroffen. Somit kommen Eingriffe immer nur dann in Betracht, wenn und soweit ein Tätigwerden der zuständigen beauftragten Person für Informationssicherheit nicht ausreichend ist oder nicht abgewartet werden kann.

Das Prinzip der Eigenverantwortlichkeit oder des Ressortprinzips wird zwar durch diese Anordnungs- und Maßnahmenbefugnis eingeschränkt. Würden jedoch andernfalls andere öffentliche oder sonstige Stellen in deren Handlungs- und Arbeitsfähigkeit ohne eine ziel- und zweckgerichtete Gefahrenabwehr beeinträchtigt, rechtfertigt diese Einschränkung dies aufgrund kollidierender Rechte.

Absatz 6 Satz 2 statuiert eine besondere Befugnisnorm des Chief Information Security Officers M-V. Dabei wird von einem erheblichen Sicherheitsvorfall gemäß § 2 Nummer 8 ausgegangen. Es muss demnach eine Gefahr gemäß § 2 Nummer 9 vorliegen, die tatsächlichen, nicht gewünschten Beeinträchtigungen der Vertraulichkeit, Verfügbarkeit, Integrität oder Verbindlichkeit von Informationstechnik oder der durch Informationstechnik verarbeiteten Daten hat. Dies ist beispielsweise bei Ausbrüchen von selbstausbreitenden Schadprogrammen (Computerwurm) oder auch bei Lagen, in denen Angreifern die Möglichkeit genommen werden soll, sich innerhalb eines Netzwerks von einem kompromittierten System zu anderen zu bewegen, um an sensible Daten oder wertvolle Ressourcen zu gelangen (Lateral Movement). Nur durch eine Abtrennung einzelner Netzwerksegmente kann weiterer Schaden verhindert werden.

Eine Netztrennung oder die Abschaltung von Informationstechnik ist das schärfste Instrument des Chief Information Security Officers M-V. Aufgrund der hierdurch entstehenden gravierenden Auswirkungen für die Arbeits- und Handlungsfähigkeit einer öffentlichen oder sonstigen Stelle dienen diese Maßnahmen als letztes Mittel. Die in diesem Kontext wirkende Gefahr in Verzug liegt immer dann vor, wenn der Chief Information Security Officer M-V aus Dringlichkeit, das heißt, wenn die Notwendigkeit besteht, unverzüglich und sofort zu handeln, ohne dass die Maßnahme durch die öffentliche oder sonstige Stelle getroffen werden kann. Soweit es in der Situation möglich ist, sollten die Leitung sowie die zuständige beauftragte Person für Informationssicherheit im Vorfeld informiert werden; in jedem Fall aber unverzüglich informiert werden.

Weil es sich insbesondere bei einer Netztrennung um eine Ultima-Ratio handelt, wird diese nur im absoluten Ausnahmefall nach gründlicher Abwägung erfolgen. Im Interesse der Funktionsfähigkeit der gesamten öffentlichen Verwaltung im Land Mecklenburg-Vorpommern kann der Schutz vor erheblichen Schäden vorrangig gegenüber der Funktionsfähigkeit einer öffentlichen oder sonstigen Stelle oder einzelner Dienste sein.

Zu Absatz 7

Absatz 7 erweitert die Maßnahmenbefugnis aus Absatz 5 dahingehend, dass von der Netztrennungs- und Abschaltungsbefugnis des Chief Information Security Officers M-V die Betreiber von Daten- oder Kommunikationsnetzen erfasst sind. Das durch diese ergänzende Regelung entstehende Durchgriffsrecht des Chief Information Security Officers M-V ermöglicht ein schnelles, unverzügliches Handeln ohne Umwege über die öffentlichen und sonstigen Stellen. Sofern der Betreiber von Daten- oder Kommunikationsnetzen nicht vom Geltungsbereich des § 1 erfasst ist, sind durch die Stellen entsprechende vertragliche Vereinbarungen zu treffen, damit der Chief Information Security Officer M-V das Durchgriffsrecht ausüben kann.

Zu Absatz 8

Das Wirkungsumfeld der Informationssicherheit ist ein interdisziplinäres Feld, das sowohl technische, organisatorische, infrastrukturelle als auch rechtliche Aspekte umfasst. Die legal festgelegte Einbindung des Chief Information Security Officers M-V in allen Gesetzgebungsverfahren und anderen Regierungsvorhaben ist dahingehend zwingend erforderlich, um bestehende landesspezifische Sicherheitsrichtlinien und -standards sowie Schutz-/Sicherheitsmaßnahmen nicht zu beeinträchtigen. Eine Einbindung des Chief Information Security Officers M-V soll zeitgerecht vor allen offiziellen Beteiligungen erfolgen.

Zu § 6

Zu Absatz 1

Eine vertrauensvolle Zusammenarbeit, ein offener Erkenntnis- und Erfahrungsaustausch sowie das notwendige Zusammenwirken für ein gemeinsames Risikoverständnis und -management ist essenziell zur Gewährleistung der Informationssicherheit auf einem nachhaltig hohen Sicherheitsniveau. Die Landesregierung Mecklenburg-Vorpommern hat im Juni 2014 die „Leitlinie für die Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern“ erlassen und das „Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern“ beschlossen. Dieses Konzept sieht u. a. den Aufbau einer ressortübergreifenden Informationssicherheitsorganisation vor, in der die Kommission für Informationssicherheit der Landesverwaltung einen wesentlichen Bestandteil darstellt. Die Mitglieder der Kommission für Informationssicherheit bringen die für ihre Ressorts spezifischen Aspekte und Anliegen ein. Dieses Konzept hat sich bewährt und soll nun auf die kommunale Ebene und somit auf die gesamte öffentliche Verwaltung des Landes Mecklenburg-Vorpommern ausgeweitet werden.

Der Absatz 1 benennt unter dem Vorsitz des Chief Information Security Officers M-V die 15 stimmberechtigten Mitglieder aus den öffentlichen Stellen. Dabei wird die Kommission für Informationssicherheit von Beschäftigten des Landes und der Kommunalverwaltung besetzt.

So wird gewährleistet, dass alle Ressorts über relevante Entwicklungen unterrichtet sind.

Näheres regelt die Geschäftsordnung.

Zu Absatz 2

Während für die kommunalen Spitzenverbände im Land Mecklenburg-Vorpommern das Verfahren zur Besetzung ihrer in die Kommission für Informationssicherheit entsandten stimmberechtigten Mitglieder nicht weiterführend festgelegt wird, konkretisiert der Absatz 2 das Besetzungsverfahren für die stimmberechtigten Mitglieder aus der Landesverwaltung. Danach sollen die Ressorts Besetzungsvorschläge unterbreiten, die nach Anhörung des Chief Information Security Officers M-V vom Kabinett bestätigt und von der oder dem CIO M-V ernannt werden.

Zu Absatz 3

Absatz 3 legt ergänzend zu Absatz 1 fest, dass neben den stimmberechtigten Mitgliedern auch deren Vertreter namentlich zu benennen sind. Eine Vertretung von stimmberechtigten Mitgliedern in der Kommission für Informationssicherheit soll jedoch die Ausnahme darstellen. Es wird davon ausgegangen, dass sich das stimmberechtigte Mitglied mit seinem Vertreter insbesondere bei der Wahrnehmung des Stimmrechts abstimmt.

Die Kommission für Informationssicherheit hat in ihrer (bestehenden) Geschäftsordnung (vergleiche § 6 Absatz 6 Satz 1) grundlegende Bestimmungen definiert, welche nicht stimmberechtigen Mitglieder an den Sitzungen teilnehmen können. Trotz neuer Zusammensetzung der Kommission für Informationssicherheit ist davon auszugehen, dass diese grundlegenden Bestimmungen übernommen werden. Darüber hinaus müssen jedoch weiterführende Festlegungen getroffen werden, wie (prozessual), in welchem Umfang sowie unter welchen Voraussetzungen Gäste an den Sitzungen der Kommission für Informationssicherheit teilnehmen können.

Es ist denklogisch nachvollziehbar, dass die innerhalb von Sitzungen der Kommission für Informationssicherheit kommunizierten Informationen bzw. die erörterten Themen einen schützenswerten Charakter besitzen, da neben beispielsweise organisatorischen Themeninhalten u. a. auch bestehende, durch Angreifer ausnutzbare Sicherheitslücken erörtert und bewertet werden. Aus diesem Grund sind die Sitzungen der Kommission für Informationssicherheit nicht öffentlich.

Zu Absatz 4

Die Kommission für Informationssicherheit ist ein fachlich zu besetzendes Gremium, deren stimmberechtigte Mitglieder eine hohe interdisziplinäre Fachexpertise aufweisen. Absatz 4 spezifiziert die fachlichen Kriterien der stimmberechtigten Mitglieder der Kommission für Informationssicherheit.

Zu Absatz 5

Der Chief Information Security Officer M-V vertritt das Land Mecklenburg-Vorpommern außen, insbesondere auf allen Ebenen der öffentlichen Verwaltung. In diesem Kontext wirkt er beispielsweise bei Beschlussfassungen im IT-Planungsrat (vergleiche Artikel 91 c GG) oder in den jeweiligen Konferenzen der Fachminister mit.

Absatz 5 regelt das Zusammenwirken zwischen dem Chief Information Security Officer M-V und der Kommission für Informationssicherheit. Die Kommission für Informationssicherheit berät den Chief Information Security Officer M-V in Fragen der Informationssicherheit und stellt aufgrund ihrer Zusammensetzung eine fachlich fundierte und abgestimmte Entscheidungsbasis sicher.

Die Formulierung, dass Entscheidungen des Chief Information Security Officers M-V im Benehmen mit der Kommission für Informationssicherheit erfolgen, gewährleistet eine enge Abstimmung und Berücksichtigung der Expertise der Mitglieder, ohne die Entscheidungsverantwortung des Chief Information Security Officers M-V einzuschränken. Der Chief Information Security Officer M-V bleibt als zentrale Informationssicherheitsinstanz des Landes handlungsfähig, während die Kommission für Informationssicherheit ihre fachliche und beratende Funktion vollumfänglich wahrnehmen kann. Dieses Zusammenwirken fördert die Transparenz, Nachvollziehbarkeit und Akzeptanz von Entscheidungen im Bereich der Informationssicherheit des Landes Mecklenburg-Vorpommern.

Zu Absatz 6

Absatz 6 legt den Mitgliedern der Kommission für Informationssicherheit die Verpflichtung auf, die wesentlichen Regelungen der Zusammenarbeit in einer Geschäftsordnung zu regeln. Satz 2 entzieht dem Chief Information Security Officer M-V das Entscheidungsrecht bei Beschlussfassungen zur Geschäftsordnung.

Bei Beschlussfassungen in der Kommission für Informationssicherheit sind die Interessen zwischen Landes- und Kommunalverwaltung abzugrenzen. Sofern Beschlussfassungen ausschließlich die Angelegenheiten der Landesverwaltung betreffen, haben die kommunalen Mitglieder kein Stimmrecht. Gleiches gilt für ausschließliche Angelegenheiten der Kommunalverwaltung.

Zu Absatz 7

Absatz 7 definiert die wesentlichen Aufgaben der Kommission für Informationssicherheit. Die Kommission für Informationssicherheit berät und erstellt zusammen mit dem Chief Information Security Officer M-V die fachlichen Inhalte von landesspezifischen Richtlinien und Standards zur Informationssicherheit. Darüber hinaus werden für die Kommission für Informationssicherheit die notwendigen Mitwirkungspflichten und -aufgaben definiert, um das Ziel eines gemeinsamen, hohen Sicherheitsniveaus in der öffentlichen Verwaltung im Land Mecklenburg-Vorpommern erreichen zu können.

Die definierten Prüfpflichten der Kommission für Informationssicherheit beziehen sich ausschließlich auf die Einhaltung und Umsetzung gemeinsam festgelegter landesspezifischer Richtlinien und Standards zur Informationssicherheit. Ein darüber hinausgehender, artfremder Eingriff in die organisatorischen Angelegenheiten der Kommunen wird von dieser Aufgabe nicht erfasst.

Zu Absatz 8

Der Absatz 8 dient der Umsetzung von Artikel 2 Absatz 2 Buchstabe f Ziffer ii der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) und regelt die Identifizierung der staatlichen Stellen, die in den Anwendungsbereich der Richtlinie fallen. Durch das von der Kommission für Informationssicherheit zu beschließende Konzept wird ein einheitliches, landesweit abgestimmtes Verfahren sichergestellt. Die obersten Landesbehörden erfassen auf dieser Grundlage die in ihren Geschäftsbereichen betroffenen staatlichen Stellen und übermitteln die erforderlichen Angaben an den Chief Information Security Officer Mecklenburg-Vorpommern (CISO M-V). Damit wird eine konsistente und aktuelle Datengrundlage geschaffen, die eine wirksame Aufsicht und Koordination im Bereich der Informationssicherheit ermöglicht. Die regelmäßige Überprüfung alle zwei Jahre gewährleistet, dass Veränderungen in der Behördenstruktur oder im Verantwortungsbereich rechtzeitig berücksichtigt werden.

Zu § 7

Der § 7 konkretisiert die Verpflichtung gemäß § 3 Absatz 3 Satz 3 zur Benennung einer beauftragten Person für Informationssicherheit (ISB). Die Regelungen und Festlegungen des § 7 gelten grundsätzlich für alle öffentlichen und sonstigen Stellen. Ausnahmen oder Konkretisierungen ergeben sich unmittelbar aus dem Gesetzestext.

Zu Absatz 1

Absatz 1 legt die wesentlichen Grundsätze dahingehend fest, dass in jeder öffentlichen Stelle eine beauftragte Person für Informationssicherheit (und eine Stellvertretung) namentlich zu benennen sind. Aufgrund unterschiedlicher Besonderheiten einer öffentlichen Stelle, beispielsweise Anzahl der Beschäftigten oder deren fachspezifischer IT-Verfahren, Heterogenität der IT-Landschaft, kann eine beauftragte Person für Informationssicherheit und deren Stellvertretung (wechselseitig) auch für mehrere öffentliche Stellen tätig werden. Dies setzt jedoch zwingend voraus, dass die beauftragte Person für Informationssicherheit alle anfallenden Aufgaben und Tätigkeiten auch tatsächlich wahrnehmen kann und keine Interessenkonflikte entstehen.

Die Funktion der beauftragten Person für Informationssicherheit sollte im Organigramm einer jeden öffentlichen Stelle vergleichbar zum Personalrat oder zum Datenschutzbeauftragen als Stabsstelle visuell dargestellt werden.

Aufgrund der besonderen Kritikalität der Steuerverwaltung ist in der zentralen Stelle für informationstechnische Dienste der Steuerverwaltung eine eigene beauftragte Person für Informationssicherheit sowie Stellvertretungen einzurichten. Es ist sicherzustellen, dass alle wesentlichen Verwaltungsprozesse und der Aufgabenumfang der Vertretung klar definiert werden und die Vertretung über die erforderlichen Kompetenzen und Fähigkeiten verfügt.

Zu Absatz 2

Die Organisation der Landespolizei Mecklenburg-Vorpommern nimmt eine weitere Sonderstellung in der Informationssicherheitsmanagementorganisation des Landes ein und bedarf daher der Reglung in einem separaten Absatz. Die oberste Polizeibehörde benennt eine beauftragte Person für Informationssicherheit in der Funktion als Chief Information Security Officer der Landespolizei (Chief Information Security Officer Pol) sowie eine Stellvertretung. Diese Funktion ist die zentrale, taktische Instanz ausschließlich für den Bereich der gesamten Landespolizei sowie für die Informationstechnik, die gegebenenfalls auch in anderen öffentlichen und sonstigen Stellen eingesetzt wird, zuständig. Der Chief Information Security Officer M-V und der Chief Information Security Officer Pol agieren und wirken somit auf unterschiedlichen Ebenen der Landesverwaltung mit organisationsspezifischen Aufgaben- und Tätigkeitsbereichen.

Zu Absatz 3

Grundsätzlich ist eine Bestellung bzw. Benennung von nicht organisationsangehörigem Personal (Fremdpersonal) gemäß BSI-Standard 200-2; IT-Grundschutz-Kompendium, Informationssicherheitsmanagementsystem.1.A5 als beauftragte Person für Informationssicherheit zulässig. Um die Aufgaben einer beauftragten Person für Informationssicherheit und deren Stellvertretung sachgerecht wahrnehmen zu können, sind allerdings umfangreiche Kompetenzen und Fähigkeiten, insbesondere Wissen über die eingesetzten IT-Verfahren, die verarbeiteten Informationen und Daten sowie die Verfahrensweisen und die Organisationskultur der jeweiligen Behörde notwendig. Die Funktion der beauftragten Person für Informationssicherheit ist eine wesentliche, gesetzliche und auf Dauer ausgerichtete Funktion innerhalb einer staatlichen Stelle.

Vor diesem Hintergrund ist für die obersten und oberen Landesbehörden sicherzustellen, dass die beauftragte Person für Informationssicherheit sowie deren Stellvertretung Angehörige des Landesdienstes sind. Nur bei einer Beschäftigung im öffentlichen Dienst des Landes besteht die erforderliche dienstrechtliche Einbindung, die eine uneingeschränkte Wahrnehmung der Aufgaben in voller Verantwortlichkeit gegenüber der Behördenleitung ermöglicht. Zudem sind hierdurch die Einhaltung dienstrechtlicher Pflichten, die Wahrung von Verschwiegenheit und Geheimschutz sowie die Verbindlichkeit behördeninterner Weisungs- und Meldewege gewährleistet.

Zu Absatz 4

Für die Schulen in öffentlicher Trägerschaft wird die Aufgabenwahrnehmung der Funktion der beauftragten Person für Informationssicherheit grundsätzlich beim Schulträger verortet. Hiervon kann abgewichen werden, wenn aufgrund der Größe einer Schule (ab 750 Schüler) eine beauftragte Person für Informationssicherheit durch den Schulträger benannt wird. Schulträgeraufgabe ist es, den Schulen funktionierende und sichere Informationstechnik zur Erfüllung der Lehrplananforderungen zur Verfügung zu stellen. Eine technische Grundausstattung der Schulen ist wesentlicher Ausgangspunkt und Voraussetzung allen digitalen Lehrens und Lernens.

Zu Absatz 5

Absatz 5 regelt die Grundzüge der Berichtspflicht. Die jeweils zuständige beauftragte Person für Informationssicherheit berichtet in angemessenen, zeitlich regelmäßigen Abständen gegenüber der Leitung. Nach herrschender Meinung wird eine monatliche Berichtspflicht als ausreichend angesehen. Eine darüber hinausgehende, jährliche sowie anlassbezogene Berichtspflicht der beauftragten Person für Informationssicherheit besteht immer gegenüber dem Chief Information Security Officer M-V. Insofern werden die beauftragten Personen für Informationssicherheit von der stelleninternen Verschwiegenheitspflicht ohne Genehmigung der Leitung gegenüber dem Chief Information Security Officer M-V entbunden.

Mit der Berichtspflicht gegenüber dem Chief Information Security Officer M-V ist gleichzeitig eine vollumfängliche Beratung und deeskalierende Unterstützung durch den Chief Information Security Officer M-V verknüpft. Der Informationsfluss vom Chief Information Security Officer an die Beauftragten für Informationssicherheit wird durch die Mitwirkung und den Austausch in der Kommission für Informationssicherheit gewährleistet.

Zu Absatz 6

Das Vortragsrecht ermöglicht es, dass die beauftragte Person für Informationssicherheit ihre Anliegen, Vorschläge oder Bedenken unmittelbar an die Leitung oder den Chief Information Security Officer M-V heranträgt, unabhängig von hierarchischen Zwischenebenen. Dieses Recht soll u. a. eine effektive Kommunikation sowie die Berücksichtigung aller wichtigen und dringlichen Aspekte der Informationssicherheit in Entscheidungsprozessen sicherstellen.

Zu Absatz 7

Eine beauftragte Person für Informationssicherheit, soweit nicht eine vorrangige Zuständigkeit des Chief Information Security Officers M-V oder des Chief Information Security Officers Pol besteht, ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb ihres Zuständigkeitsbereichs. Die Kernaufgabe einer beauftragten Person für Informationssicherheit besteht darin, die Leitung einer Stelle bei dessen Aufgabenwahrnehmung bezüglich der Informationssicherheit zu beraten, zu unterstützen und die Umsetzung zu kontrollieren. Ihre Aufgaben sind in den BSI-Standards der 200er-Reihe des IT-Grundschutzes beschrieben und umfassen insbesondere:

- die Steuerung des Informationssicherheitsprozesses (aktiv) und die Mitwirkung an allen damit zusammenhängenden Aufgaben und Tätigkeiten,
- die Erstellung von stellenspezifischen Leitlinien sowie organisatorischen und technischen Richtlinien,
- die Mitwirkung bei IT-Projekten mit Blick auf informationssicherheitsrelevante Aspekte, insbesondere auf die Sicherheitsanforderungen aus dem IT-Grundschutz-Kompendium,
- die Analyse und Bewertung von Sicherheitsvorfällen und gegebenenfalls die Meldung an das CERT M-V (Einhaltung der Meldepflichten gemäß § 16),
- die Initiierung und Koordinierung von Sensibilisierungsmaßnahmen und Schulungsmaßnahmen,
- die Mitwirkung und Freigabe von IT-Fachverfahren gemäß den Grundsätzen in § 3 Absatz 7.

Satz 3 berechtigt die jeweils zuständige beauftragte Person für Informationssicherheit, sich im Fall von Sicherheitsvorfällen in ihrem Zuständigkeitsbereich die notwendigen Informationen zu beschaffen, um solche Vorfälle zu analysieren, zu bewerten und die Informationssicherheit wiederherzustellen. Voraussetzung hierfür ist die Einsichtnahme in die IT-Dokumentation, in das Sicherheitskonzept sowie die Einsicht in die Protokolldaten. Nur so ist es möglich, Abweichungen und sicherheitsrelevante Ereignisse zu erkennen und gegebenenfalls deren schädliche Auswirkungen zu begrenzen. Die verfahrensverantwortliche Stelle (§ 8 Absatz 3) ist verpflichtet, diese Informationen und Unterlagen der beauftragten Person für Informationssicherheit zur Verfügung zu stellen.

IT-Dokumentation umfasst alle Unterlagen und Dokumente, die für einen ordnungsgemäßen und sicheren Wirkbetrieb zu erstellen und regelmäßig zu aktualisieren sind. Sie dienen als Grundlage für einen transparenten Überblick über Hard- und Software, Netzwerke, Benutzerrechte, Schnittstellen und Prozesse innerhalb eines IT-Verfahrens, eingebettet in eine IT-Systemlandschaft.

Zu Absatz 8

Der Chief Information Security Officer M-V, die Kommission für Informationssicherheit und das CERT M-V sind unverzüglich über die Ernennung oder über einen personellen Wechsel einer beauftragten Person für Informationssicherheit öffentlicher Stellen zu unterrichten. Insbesondere für das CERT M-V ist es essenziell, im Rahmen einer Sicherheitsvorfallbehandlung eine schnelle und unmittelbare Kommunikation mit der richtigen Ansprechperson herzustellen, um eine effektive und effiziente Gefahrenabwehr zu gewährleisten.

Zu § 8

Zu Absatz 1

Ein Verwaltungs- oder Geschäftsprozess besteht aus einer Folge von Einzelaktivitäten, mit denen festgelegte Ziele und/oder Verwaltungsleistungen erreicht werden sollen. Zur gesetzlichen Aufgabenerfüllung einer Behörde trägt in der Regel eine Reihe von mehreren abhängigen Verwaltungsprozessen bei, die zusammen eine Prozesskette bilden (z. B. Posteingang Antrag auf Wohngeld, Prüfung des Antrages, Bescheidung, Auszahlung, Wiedervorlage). Ein Verwaltungsprozess erhält Eingaben (= Input, z. B. Anträge von Bürgerinnen und Bürgern) von vorgelagerten Prozessen, verarbeitet diese in einer festgelegten Weise und liefert seine Ergebnisse (= Output) an die nachgelagerten Prozesse weiter.

Verwaltungsprozesse lassen sich darüber hinaus unterscheiden in:

- Kernprozesse, die direkt zum Erreichen der Verwaltungsleistungen beitragen (diese können strategischer oder operativer Art sein), sowie
- unterstützende Prozesse, die zwar für die Kernprozesse wichtig sind (z. B. IT-Administration, Personalmanagement), aber nur mittelbar zur Erbringung der Verwaltungsleistungen beitragen.

Die Verwaltungsprozesse werden in der Regel durch Werkzeuge, wie beispielsweise Informationstechnik, unterstützt. Für die jeweilige Verwaltungsleistung ist immer eine Organisationseinheit zuständig (= verfahrensverantwortliche Stelle).

Die verfahrensverantwortliche Stelle ist verantwortlich für den ordnungsgemäßen, wirtschaftlichen und sicheren IT-Betrieb der IT-Verfahren, die ihre Verwaltungsleistung als Werkzeug unterstützen. Ein sicherer IT-Betrieb setzt voraus, dass ein Sicherheitskonzept gemäß IT-Grundschutz erstellt und die Sicherheitsanforderungen durch technische, organisatorische, personelle und infrastrukturelle Maßnahmen umgesetzt und wirksam sind.

In der Regel wird die verfahrensverantwortliche Stelle nicht über die notwendige fachliche Expertise verfügen. In diesem Fall wird sich die verfahrensverantwortliche Stelle eines IT-Verfahrensverantwortlichen als Erfüllungsgehilfen bedienen. Die Gesamtverantwortung bleibt jedoch immer bei der verfahrensverantwortlichen Stelle.

Zu Absatz 2

Aus Absatz 3 ergibt sich die Verpflichtung der verfahrensverantwortlichen Stelle zur Zusammenarbeit mit der beauftragten Person für Informationssicherheit, dem Chief Information Security Officer M-V sowie mit dem CERT M-V bei der Analyse und Bewertung von sicherheitsrelevanten Ereignissen sowie im Rahmen der Sicherheitsvorfallbehandlung.

Zu § 9

Zu Absatz 1

Computer Emergency Response Teams (CERT) oder Computer Security Incident Response Teams (CSIRTs) sind hoch spezialisierte Einheiten, bestehend aus Sicherheits- und Malwareanalysten, IT-Forensikern und Kommunikationsexperten, die auf Sicherheitsvorfälle reagieren, Bedrohungen eindämmen und die Sicherheitslage ihrer jeweiligen Organisationen verbessern sollen.

Das Sicherheitsteam der Landes- und Kommunalverwaltung (Computer Emergency Response Team – CERT M-V) ist die zentrale Stelle in der Informationssicherheitsorganisation im Land Mecklenburg-Vorpommern. Es ist ein essenzieller Akteur auf der operativ wirkenden Ebene. Mit der Regelung in Absatz 1 wird die gesetzliche Grundlage geschaffen, um ein CERT dauerhaft in der Organisationsstruktur der Landesverwaltung zu etablieren. Mit den Festlegungen in Nummer 1 bis 5 werden die wesentlichen Aufgaben des CERT M-V gesetzlich definiert. Diese Aufgaben müssen weitergehend konkretisiert werden und sich gegebenenfalls flexibel an die sich ändernde Bedrohungslage anpassen. Daher wird die für Digitalisierung zuständige oberste Landesbehörde ermächtigt, die Aufgaben des CERT M-V per Rechtsverordnung zu konkretisieren.

Zu Absatz 1 Nummer 1

Das CERT M-V ist die koordinierende Stelle bei Sicherheitsvorfällen, insbesondere, wenn die Gewährleistung der Informationssicherheit zentraler Informationstechnik flankierend erkennbar gefährdet ist oder bereits mindestens ein Schutzziel verletzt wurde. Es unterstützt die betroffene öffentliche Stelle bei der Bewältigung von Sicherheitsvorfällen.

Zur Gefahrenabwehr hat das CERT M-V sowohl temporär wirkende (Workaround) als auch nachhaltige Lösungsvorschläge zu technischen, organisatorischen und infrastrukturellen Schutz-/Sicherheitsmaßnahmen zu erarbeiten. Dies kann auch die zur Gefahrenabwehr erforderliche Abschaltungsempfehlung von Informationstechnik beinhalten.

Zu Absatz 1 Nummer 2

Darüber hinaus informiert das CERT M-V alle öffentlichen Stellen über einen Warn- und Informationsdienst beispielsweise zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen und der dabei beobachteten Vorgehensweisen der Angreifer. Die aus unterschiedlichen Quellen stammenden sicherheitsrelevanten Informationen werden durch das CERT M-V unverzüglich ausgewertet, mit weiteren Informationen angereichert, empfängergerecht aufbereitet und zielgerichtet an die öffentlichen Stellen weitergegeben. Soweit erforderlich, werden die öffentlichen Stellen im Zuge einer Alarmmeldung unverzüglich über alle für die Abwehr von akuten Gefahren für die Informationstechnik unterrichtet.

Zu Absatz 1 Nummer 3

Durch den (technischen) Betrieb eines Schwachstellenmanagementsystems überprüft präventiv das CERT M-V kontinuierlich die Informationstechnik der öffentlichen Stellen auf Schwachstellen und Fehlkonfigurationen. Es stellt den Betreibern Empfehlungen zur Beseitigung zur Verfügung und unterstützt fachlich bei der Mängelbeseitigung.

Zu Absatz 1 Nummer 4

Die Vorschrift verpflichtet alle öffentlichen Stellen sowie die von ihnen beauftragten IT-Dienstleister, dem CERT M-V die für die Gefahrenabwehr erforderlichen Informationen und Daten unverzüglich und unentgeltlich bereitzustellen. Damit wird sichergestellt, dass das CERT M-V Sicherheitsvorfälle schnell und umfassend analysieren und koordinierte Gegenmaßnahmen ergreifen kann. Die Regelung dient der Schaffung einer einheitlichen Informationslage zur aktuellen Sicherheitslage in der Landesverwaltung und gewährleistet eine effektive Zusammenarbeit zwischen den betroffenen Stellen und dem CERT M-V.

Zu Absatz 1 Nummer 5

Durch die kontinuierliche Verarbeitung sicherheitsrelevanter Informationen im CERT M-V, insbesondere aus der Kommunal- und Landesverwaltung, ist das CERT M-V in der Lage, die landesspezifische Bedrohungslage zu analysieren und zu bewerten. Alle im CERT M-V gewonnenen Erkenntnisse und Ergebnisse aus Sicherheitsanalysen fließen in einem regelmäßig durch das CERT M-V zu erstellenden Sicherheitslagebericht ein. Dieser Bericht wird dem Chief Information Security Officer M-V und den öffentlichen Stellen zur Verfügung gestellt.

Zu Absatz 1 Nummer 6

Nummer 6 betont die koordinierende Rolle des CERT M-V in technologischen Fragen der Informationssicherheit. Ziel ist es, eine einheitliche Vorgehensweise bei der Einführung, Anpassung und Weiterentwicklung sicherheitsrelevanter Verfahren und Technologien zu gewährleisten. Durch die Mitwirkung des CERT M-V werden Doppelstrukturen vermieden, Synergien genutzt und die Abstimmung zwischen den verschiedenen Verwaltungsebenen im Bereich der Informationssicherheit verbessert.

Zu Absatz 1 Nummer 7

Das CERT M-V kooperiert im VerwaltungsCERT-Verbund mit anderen CERTs von Bund und den Ländern sowie im Deutschen CERT-Verbund mit den CERTs anderer Wirtschaftssektoren, um Informationen über Bedrohungen und deren Abwehr auszutauschen. Somit ist das CERT M-V zentraler Ansprechpartner für Informationen aus und für die Mitglieder der CERT-Verbünde. Das CERT M-V ist nicht die Kontaktstelle des Landes Mecklenburg-Vorpommern für kritische Infrastrukturen gemäß § 8a Absatz 2 Nummer 4c BSIG.
Satz 4 entfaltet eine Schutzwirkung für die Mitglieder des CERT M-V dahingehend, dass sich die Sicherheitsexperten primär den wesentlichen Kernaufgaben aus Satz 3 widmen sollen. Darüber hinausgehende, auch temporäre Aufgaben bedürfen des Einvernehmens des Chief Information Security Officers M-V, welche die Fachaufsicht über das CERT M-V ausübt.

Zu Absatz 2

Absatz 2 konkretisiert die Zielgruppe der Unterstützung des CERT M-V.

Zu Absatz 3

Ausgangspunkt seiner Arbeit und Dienste ist das Sammeln, Auswerten und Aggregieren von Informationen zur Gewinnung von Erkenntnissen über Sicherheitsrisiken und -lücken, zu Schadprogrammen, zu versuchten oder erfolgreichen Angriffen sowie über die bei den detektierten Angriffen analysierten Vorgehensweisen. In diesem Kontext wird das CERT M-V auf Protokolldaten zurückgreifen müssen, um diese auszuwerten. Satz 1 stellt somit die zentrale Befugnisnorm des CERT M-V als wesentliche Voraussetzung für die gemäß Absatz 1 übertragenen Aufgaben dar. Dabei beinhaltet der Absatz 3 noch nicht die erforderliche gesetzliche Ermächtigung zur Verarbeitung personenbezogener oder dem Fernmeldegeheimnis unterliegender Daten; dies richtet sich ausschließlich nach den Vorschriften der §§ 11 bis 15.

Satz 2 ermächtigt das CERT M-V zum vollumfänglichen Informationstausch im Kontext mit Satz 1 sowohl mit dem BSI als auch mit den Sicherheitsbehörden von Bund und den Ländern.

Zu Absatz 4

Absatz 4 verpflichtet alle öffentlichen Stellen und deren IT-Dienstleister zur uneingeschränkten Zusammenarbeit mit dem CERT M-V im Rahmen seiner Aufgaben gemäß Absatz 3 in Verbindung mit den Kernaufgaben in Absatz 1. Die seitens des CERT M-V als notwendig bewerteten Informationen oder Daten sind unverzüglich und unentgeltlich dem CERT M-V zur Verfügung zu stellen. Dabei kann es sich um eine einmalige oder um eine kontinuierliche Bereitstellung oder Übermittlung handeln. Bei den angeforderten Daten wird es sich beispielsweise um Protokolldaten, Netzpläne, Konfigurationsdaten etc. handeln, während es sich bei den Informationen um einen bilateralen, fachlichen Informationsaustausch beispielsweise im Rahmen der Sicherheitsvorfallbehandlung handeln wird.

Für die öffentlichen Stellen bedeutet diese Verpflichtung, dass die Zusammenarbeit mit dem CERT M-V und deren beauftragten IT-Dienstleister verpflichtend vertraglich zu regeln ist.

Zu Absatz 5

Im Rahmen seiner Aufgabenwahrnehmung verarbeitet das CERT M-V höchst sensible, sicherheitsrelevante Informationen; darüber hinaus auch personenbezogenen Daten besonderer Kategorien. Um die übertragenen Aufgaben effektiv und effizient durch den Einsatz von Informationstechnik wahrnehmen zu können, wird das CERT M-V in Teilen dezentrale, nicht standardisierte und einsatzspezifische Informationstechnik einsetzen bzw. betreiben. Absatz 6 verpflichtet das CERT M-V, ein spezifisches Sicherheitskonzept auf Basis von IT-Grundschutz und dem Standard-Datenschutzmodell zu erstellen und dieses Sicherheitskonzept jährlich fortzuschreiben. Ergänzend zu diesen Standards erfolgt die Verpflichtung zu einer jährlich durchzuführenden Wirksamkeitsprüfung der implementierten Schutz-/Sicherheitsmaßnahmen.

Zu Absatz 6

Ziel das Absatzes 6 ist es, die Handlungsfähigkeit des CERT M-V auch in (IT-)Krisenlagen dauerhaft sicherzustellen. Das CERT M-V soll seine Kernaufgaben jederzeit und unabhängig von der zentralen Informationstechnik der Landesverwaltung wahrnehmen können. Hierzu sind ständige Erreichbarkeit und Verfügbarkeit (24/7) durch geeignete organisatorische und technische Maßnahmen anzustreben und schrittweise umzusetzen. Dies erfordert eine geeignete, sichere, resiliente sowie eine belastbare Kommunikations- und Informationsinfrastruktur über die das CERT M-V Informationen mit seiner Zielgruppe und anderen einschlägigen Interessenträgern austauscht. Neben der räumlichen Redundanz ist ebenfalls die CERT-eigene Technik redundant und anforderungsgerecht zu ertüchtigen und zu erproben.

Der Zugriff auf eine Vielzahl von hochsensiblen Informationen, die auch fundierte Kenntnisse zu vorhandenen Schwachstellen in der Informationstechnik beinhalten können, erfordern den Einsatz von sicherheitsüberprüftem und zuverlässigem Personal.

Zu § 10

Zu Absatz 1

Absatz 1 verpflichtet jede öffentliche Stelle zum Aufbau und Betrieb eines Security Operation Center (SOC). SOCs sind Organisationseinheiten, die auf der operativen Ebene eines Informationssicherheitsmanagementsystems wirken und für die Überwachung, Erkennung und Reaktion auf sicherheitsrelevante Ereignisse zuständig sind. Es kombiniert hoch spezialisierte Sicherheitsexperten, Prozesse und Technologien, um eine kontinuierliche Sicherheitsüberwachung zu gewährleisten. Dabei ergänzen sich die bereits bestehende betriebliche Systemüberwachung und die Sicherheitsüberwachung.

Die Sätze 2 und 3 verpflichteten die SOCs zur bilateralen Zusammenarbeit mit CERT M-V, das heißt der Informations- und Datenaustausch erfolgt in beide Richtungen.

Zu Absatz 2

Absatz 2 überträgt die Aufgabe zum Betrieb eines SOC für die staatlichen Stellen der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH. Den kommunalen Stellen wird freigestellt, in welcher organisatorischen Ausprägung diese der Verpflichtung nach Absatz 1 nachkommen. So kann jede kommunale Stelle ein eigenes SOC betreiben oder sich mit anderen kommunalen Stellen zu einem gemeinsam betriebenen SOC zusammenschließen. Darüber hinaus kann die SOC-Dienstleistung einem privatrechtlich ausgerichteten IT-Dienstleister übertragen werden. Letzteres erfordert eine vertragliche Vereinbarung dahingehend, dass die Vorgaben gemäß § 4 umgesetzt und aufrecht gehalten werden, insbesondere damit der Chief Information Security Officer M-V seiner Kontrollpflicht nach Absatz 4 nachkommen kann.

Zu Absatz 3

Absatz 3 definiert die wesentlichen, prozessualen Kernaufgaben eines SOC.

Zu Absatz 3 Nummer 1

Protokollierung und Überwachung: Protokollierung von definierten sicherheitsrelevanten Ereignissen verbunden mit einer 24/7/365-Überwachung von Netzwerken, Systemen und Anwendungen, um Bedrohungen präventiv und zeitgerecht zu erkennen.

Zu Absatz 3 Nummer 2

Vorfallmanagement: Identifikation, Analyse und Bearbeitung von sicherheitsrelevanten Ereignissen einschließlich der Koordination und Einleitung von Erst-Maßnahmen; bei einem Sicherheitsvorfall in enger Zusammenarbeit und Abstimmung mit dem CERT M-V u. a. zur koordinierten Eindämmung sowie zum Informations- und Datenaustausch.

Zu Absatz 3 Nummer 3

Meldewesen und Informationsbereitstellung: Sicherheitsrelevante Ereignisse sollen gemäß Nummer 2 von den Security Analysten im Tagesgeschäft analysiert und bewertet werden. Wenn sich aus den Erkenntnissen ein Verdachtsmoment für einen Sicherheitsvorfall ergibt, sind das CERT M-V und die zuständige beauftragte Person für Informationssicherheit unverzüglich zu informieren und in die Analysetätigkeiten einzubinden. In diesem Kontext werden die SOCs verpflichtet, u. a. Protokolldaten sowie die gewonnenen Erkenntnisse über den Angriff mit dem CERT M-V und der zuständigen beauftragten Person für Informationssicherheit zu teilen.

Zu Absatz 4

Der Absatz 4 steht in Verbindung mit der Verordnungsermächtigung in § 4 Absatz 1. Der Chief Information Security Officer M-V wird ermächtigt, die Umsetzung der Vorgaben entsprechend zu kontrollieren.

Zu § 11

Zu Absatz 1

Mit Absatz 1 wird eine Rechtsgrundlage für die Datenverarbeitung auf der Grundlage von Artikel 6 Absatz 1 Buchstabe e in Verbindung mit Artikel 6 Absatz 3 Satz 1 der Verordnung (EU) 2016/679 geschaffen. Dies ist rechtlich notwendig, da § 4 Absatz 1 DSG M-V nur eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellt. § 11 Absatz 1 regelt mithin konkret die Daten verarbeitende Stelle (CERT M-V) und benennt abschließend die Zwecke der Verarbeitung personenbezogener Daten.

Satz 2 benennt konkret die Verarbeitungssituationen bzw. die Art und Weise der Datenverarbeitung. Eine Verarbeitung personenbezogener Daten soll demnach auch rechtmäßig sein, wenn der Ausschluss einer Verarbeitung die Arbeitsweise des CERT M-V einschränken oder diese erheblich gefährden würde. Hintergrund dieser Regelung ist, dass auf Sicherheitsvorfälle reagiert werden muss, ohne dass in zeitlicher Hinsicht unbedingt eine datenschutzrechtliche Abwägung der Verhältnismäßigkeit stattfinden kann. Ein späteres oder zu spätes Reagieren des CERT M-V könnte unter Umständen dazu führen, dass ein Sicherheitsrisiko nicht effizient abgewehrt werden könnte (§ 11 Absatz 1 Satz 2 Buchstabe b).

Darüber hinaus schafft Satz 2 eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten, da es bei der schnellen sofortigen Aufgabenwahrnehmung im Falle eines Einschreitens des CERT M-V grundsätzlich auch immer dazu kommen kann, dass Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 verarbeitet werden oder eine Verarbeitung solcher Daten nicht ausgeschlossen werden kann. Die Verarbeitungsermächtigung beruht auf Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679. Die Aufgabenwahrnehmung des CERT M-V erfolgt mithin aus Gründen eines erheblichen öffentlichen Interesses, der Gewährleistung der Informationssicherheit der öffentlichen Verwaltung, der öffentlichen oder sonstigen Stellen der Daseinsvorsorge, der Gewährleistung der Funktionsfähigkeit der Landesregierung und sonstiger Stellen des Anwendungsbereichs zur Abwehr jeglicher Sicherheitsvorfälle und damit zum Schutz übergeordneter Rechtsgüter wie der öffentlichen Sicherheit und Ordnung und dem Schutz der Bevölkerung.

Zu Absatz 2

Absatz 2 schafft eine Verarbeitungsbefugnis für Daten, die ursprünglich zu Zwecken erhoben wurden, die der Richtlinie (EU) 2016/680 unterliegen, und normiert gleichzeitig eine Pflicht zur Übermittlung solcher Daten zu Zwecken nach Absatz 1 an das CERT M-V, wenn eine Verarbeitung für die Aufgabenwahrnehmung des CERT M-V erforderlich ist oder solche personenbezogenen Daten derart miteinander verbunden sind, dass diese in zeitlicher und funktioneller Hinsicht aus Gründen der Informationssicherheit nicht vor einer Übermittlung abgetrennt werden können. Die Regelung ist rechtlich notwendig, da eine Übermittlung solcher personenbezogenen Daten nur unter den Voraussetzungen des § 39b Absatz 3 SOG M-V möglich ist.

Zu Absatz 3

Absatz 3 bezieht sich auf die Verarbeitungsbefugnis solcher Daten nach Absatz 2 und regelt in Anlehnung an § 11 Absatz 1 Satz 2 die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Regelungsbefugnis ergibt sich entsprechend aus Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679.

Zu Absatz 4

Absatz 4 regelt die Pflicht zur automatisierten Pseudonymisierung von personenbezogenen Daten, wenn und soweit der Zweck der Verarbeitung dies zu lässt oder der Zweck der Verarbeitung nicht mehr gefährdet ist. Es handelt sich hierbei mithin um eine gesetzlich verpflichtende technisch-organisatorische Maßnahme nach Artikel 32 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679. Entsprechende konkretisierende Regelungen finden sich in § 14 Absatz 2 und § 15 Absatz 1 Satz 3 des Gesetzes.

Zu Absatz 5

Absatz 5 regelt gesetzlich verpflichtende Löschregelungen für personenbezogene Daten, die nach diesem Gesetz verarbeitet werden dürfen, und setzt somit die Schutzziele des Artikels 5 Absatz 1 der Verordnung (EU) 2016/679 um. Gleiches gilt für die weitere Aufbewahrung zu Zwecken der Datenschutzkontrolle. Diese Zweckänderungsregelung gewährleistet zum einen die Rechenschaftspflicht aus Artikel 5 Absatz 2 der Verordnung (EU) 2016/679 und unterliegt zum anderen außerdem der Zweckbindung eines legitimen Zwecks nach Artikel 6 Absatz 4 der Verordnung (EU) 2016/679; hier nämlich dem Zweck der Datenschutzkontrolle. Diese Daten unterliegen zu diesem Zweck einem Verwertungsverbot und dürfen zu keinen anderen Zwecken weiterverarbeitet werden.

Zu Absatz 6

Absatz 6 stellt klar, dass mit der Formulierung „Kontrollpflichten“ nach diesem Gesetz nicht Kontrollpflichten der Datenschutzaufsichtsbehörde nach den Regelungen des DSG M-V gemeint sind. Die Regelung ist erforderlich, da beide Gesetze sprachlich das Wort „Kontrollpflichten“ verwenden, den Formulierungen inhaltlich jedoch unterschiedliche Bedeutungen zukommen.

Zu Absatz 7

Die §§ 12 bis 15 konkretisieren die Befugnisse und Prozesse öffentlicher Stellen bei der Protokollierung, Analyse und Auswertung von sicherheitsrelevanten Ereignissen zur Erkennung und Abwehr von Gefahren für die Daten- oder Kommunikationsnetze sowie für die Informationstechnik der öffentlichen Verwaltung durch Sicherheitslücken, Schadprogramme oder durch versuchte oder erfolgte Angriffe. Die daraus entstehende Erlaubnis adressiert zunächst ausdrücklich die öffentlichen Stellen gemäß § 1 in verantwortlicher Rolle. Allerdings werden die öffentlichen Stellen für den Betrieb ihrer Daten- oder Kommunikationsnetze sowie ihrer Informationstechnik entsprechende kommunale, staatliche IT-Dienstleister oder privatrechtlich organisierte IT-Dienstleister oder Rechenzentrumsbetreiber mit dieser Aufgabenwahrnehmung beauftragen. Die notwendigen weiteren Voraussetzungen und Regelungen ergeben sich aus § 4 Absatz 1.

Zu § 12

Zu Absatz 1

§ 12 ermöglicht den öffentlichen Stellen, Protokolldaten automatisiert auszuwerten, um Gefahren für ihre informationstechnischen Systeme zu erkennen und abzuwehren. Erfasst sind ausschließlich Daten, die in den in Absatz 1 Nummer 1 bis 7 genannten Systemen automatisiert anfallen und deren Auswertung technisch erforderlich ist, um sicherheitsrelevante Auffälligkeiten zu identifizieren.

Die Vorschrift schafft damit eine klare gesetzliche Grundlage für den Einsatz gängiger IT-Sicherheitsinstrumente wie Firewalls, Virenschutz- und Monitoring-Systeme.

Zu Absatz 2

Absatz 2 stellt sicher, dass personenbezogene Protokolldaten nur so lange verarbeitet werden dürfen, wie dies für die Gefahrenanalyse erforderlich ist; anschließend sind sie unverzüglich und endgültig zu löschen. Damit wird der Grundsatz der Datenminimierung und der Zweckbindung gemäß Artikel 5 DSGVO umgesetzt.

Zu Absatz 3

Absatz 3 sieht vor, dass der CISO M-V im Benehmen mit der Kommission für Informationssicherheit (KofIS) eine Richtlinie erlässt, die die sicherheitsrelevanten Ereignisse und die konkret zu erfassenden Protokolldaten festlegt. Dies dient der landesweiten Vereinheitlichung und technischen Konkretisierung.

Zu Absatz 4

Absatz 4 stellt klar, dass eine inhaltliche Auswertung von Kommunikationsinhalten grundsätzlich unzulässig ist und nur nach den besonderen Voraussetzungen des § 15 erfolgen darf.

Zu § 13

Zu Absatz 1

§ 13 regelt ergänzend die Befugnisse zur automatisierten Erhebung und Auswertung von Daten in den landesweiten Kommunikationsnetzen der öffentlichen Verwaltung. Die Vorschrift erlaubt der für die Digitalisierung zuständigen obersten Landesbehörde, an zentralen Netzschnittstellen sicherheitsrelevante Verkehrsdaten automatisiert zu erfassen und zu analysieren, um Cyberangriffe frühzeitig zu erkennen.

Erfasst werden ausschließlich technische Verbindungsdaten, die für eine Angriffserkennung erforderlich sind. Eine Auswertung der kommunikativen Bedeutung oder des Inhalts ist ausdrücklich ausgeschlossen.

Damit wird das Schutzziel einer proaktiven Netzsicherheit mit den datenschutzrechtlichen Vorgaben in Einklang gebracht.

Zu Absatz 2

Absatz 2 eröffnet den öffentlichen Stellen die Möglichkeit, an ihren eigenen Übergabepunkten entsprechende Analysen vorzunehmen, wenn dies zur Gefahrenabwehr erforderlich ist.

Zu Absatz 3

Absatz 3 stellt klar, dass Inhaltsdaten nur unter den Voraussetzungen des § 15 verarbeitet werden dürfen.

Zu § 14

Zu Absatz 1

§ 14 Absatz 1 schafft die Grundlage für eine vertiefte Auswertung von Daten, wenn eine erste automatisierte Analyse nach §§ 12 oder 13 konkrete Hinweise auf eine Sicherheitsgefährdung ergeben hat. Die weiterführende Analyse ist auf den Einzelfall und auf den Erforderlichkeitsgrundsatz beschränkt. Eine Speicherung oder weitere Zusammenführung von Daten ist nur zulässig, soweit sie der Abwehr einer konkreten Gefahr dient. Damit werden technische Untersuchungen – etwa zur Identifikation von Angriffsmustern oder Schadsoftware – rechtlich abgesichert, zugleich aber Missbrauchsrisiken begrenzt.

Zu Absatz 2

Absatz 2 regelt die Pflicht zur automatisierten Pseudonymisierung von personenbezogenen Daten, wenn und soweit der Zweck der Verarbeitung dies zulässt oder der Zweck der Verarbeitung nicht mehr gefährdet ist. Es handelt sich hierbei mithin um eine gesetzlich verpflichtende technisch-organisatorische Maßnahme nach Artikel 32 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 (siehe auch zu § 11 Absatz 4).

Zu Absatz 3

Absatz 3 Satz 1 erlaubt es der verantwortlichen Stelle, den Personenbezug zu vorher pseudonymisierten Protokolldaten wiederherzustellen, wenn weiterführende Analysen ergeben haben, dass eine Gefahr für die Informationstechnik durch Schadprogramme, durch eine Sicherheitslücke oder durch einen Angriff hervorgerufen worden sind oder bevorstehen. Es tritt insofern eine Wiederkehr der Zweckbindung und damit eine Befugnis zur Weiterverarbeitung der personenbezogenen Daten unter den Grundsätzen des § 11 ein.

Zu Absatz 4

Mit Absatz 4 wird klargestellt, dass im Rahmen der weiterführenden Analyse nach den Absätzen 1 bis 3 ausschließlich technische Protokoll- und Verkehrsdaten verarbeitet werden dürfen. Die Verarbeitung oder Auswertung von Inhaltsdaten – also solcher Daten, die Rückschlüsse auf die inhaltliche Bedeutung von Kommunikationsvorgängen zulassen – ist ausdrücklich ausgeschlossen.

Die Regelung dient der Abgrenzung der technisch erforderlichen Analyseebene von einer inhaltlichen Überwachung der Kommunikation und gewährleistet die Wahrung des Fernmeldegeheimnisses nach Artikel 10 Absatz 1 GG sowie der Datenschutzgrundsätze aus Artikel 5 DSGVO. Inhaltsdaten dürfen nur unter den besonderen Voraussetzungen des § 15 verarbeitet werden. Damit wird eine klare rechtliche Trennung zwischen technischer Gefahrenabwehr und inhaltlicher Kommunikationsanalyse geschaffen.

Zu Absatz 5

Absatz 5 konkretisiert den Grundsatz der Speicherbegrenzung. Danach sind die im Rahmen einer weiterführenden Analyse erhobenen und ausgewerteten Daten unverzüglich zu löschen, sobald sie für den Zweck der Gefahrenabwehr oder eine gesetzlich vorgesehene Übermittlung – etwa an das CERT M-V gemäß § 10 – nicht mehr erforderlich sind.

Die Vorschrift stellt sicher, dass keine dauerhafte Vorratsspeicherung sicherheitsrelevanter Daten erfolgt und die Datenverarbeitung strikt zweckgebunden bleibt. Sie dient damit der Umsetzung der Löschpflichten nach Artikel 5 Absatz 1 Buchstabe e DSGVO und begrenzt den Eingriff in die Rechte der Betroffenen auf das erforderliche Minimum.

Zu § 15

Zu Absatz 1

Absatz 1 Satz 3 regelt die Pflicht zur automatisierten Pseudonymisierung von personenbezogenen Daten, wenn und soweit der Zweck der Verarbeitung dies zu lässt oder der Zweck der Verarbeitung nicht mehr gefährdet ist. Es handelt sich hierbei mithin um eine gesetzlich verpflichtende technisch-organisatorische Maßnahme nach Artikel 32 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 (siehe auch zu § 11 Absatz 4).

Zu Absatz 2

Absatz 2 verpflichtet die verantwortliche Stelle, Inhaltsdaten unverzüglich zu löschen, wenn sich im Ergebnis der Analyse keine tatsächlichen Anhaltspunkte für eine sicherheitsrelevante Gefahr ergeben. Die Regelung konkretisiert den Grundsatz der Erforderlichkeit und verhindert, dass Kommunikationsinhalte ohne Bezug zu einem Sicherheitsereignis gespeichert oder weiterverarbeitet werden. Damit wird sichergestellt, dass Eingriffe in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung nur in eng begrenzten Ausnahmefällen zulässig sind und sofort beendet werden müssen, sobald der Gefahrenverdacht entfällt.

Zu Absatz 3

Absatz 3 erlaubt es der verantwortlichen Stelle, den Personenbezug zu vorher pseudonymisierten Inhaltsdaten wiederherzustellen, wenn weiterführende Analysen ergeben haben, dass eine Gefahr für die Informationstechnik durch Schadprogramme, durch eine Sicherheitslücke oder durch einen Angriff hervorgerufen worden sind oder bevorstehen. Es tritt insofern eine Wiederkehr der Zweckbindung und damit eine Befugnis zur Weiterverarbeitung der personenbezogenen Daten unter den Grundsätzen des § 11 ein.

Zu Absatz 4

Absatz 4 legt die Lösch- und Dokumentationspflichten nach Abschluss einer zulässigen inhaltlichen Analyse fest. Danach sind alle im Rahmen der Auswertung nach Absatz 3 gespeicherten Daten und Ergebnisse zu löschen, sobald sie für die Gefahrenabwehr oder Übermittlung nach § 10 nicht mehr benötigt werden.

Die Dokumentation der erfolgten Analyse und Löschung dient ausschließlich der Datenschutzkontrolle durch die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit. Eine anderweitige Nutzung dieser Dokumentation ist unzulässig.

Die zweijährige Aufbewahrungsfrist der Dokumentationsdaten stellt ein angemessenes Verhältnis zwischen Nachvollziehbarkeit und Datenschutz her. Sie ermöglicht dem Landesbeauftragten für Datenschutz und Informationsfreiheit die Kontrolle datenschutzkonformer Verfahren, ohne eine übermäßige Speicherung zuzulassen. Damit wird der Grundsatz der Rechenschaftspflicht nach Artikel 5 Absatz 2 DSGVO umgesetzt und gleichzeitig sichergestellt, dass Eingriffe in Kommunikationsinhalte vollständig nachvollziehbar, aber zeitlich streng begrenzt bleiben.

Zu § 16

Zu Absatz 1

Absatz 1 verpflichtet alle öffentlichen Stellen, die an Daten- und Kommunikationsnetze der öffentlichen Verwaltung, insbesondere an das CN LAVINE, angeschlossen sind, die in diesen Stellen bekannten, sicherheitsrelevanten Informationen im Rahmen der Gefahrenabwehr unverzüglich an das CERT M-V zu übermitteln. Mit der in Absatz 1 bezeichneten Meldepflicht ist eine Informationspflicht gemeint, die im jeweiligen Fall keiner gesonderten Aufforderung durch das CERT M-V bedarf.

Von dieser Verpflichtung ist immer dann abzusehen, wenn andere Rechtsnormen einer Informationsweitergabe an das CERT M-V entgegenstehen oder wenn entsprechende Informationen aus der Beschaffung öffentlich zugänglichen Quellen (OSINT, Open Source Intelligence) bekannt sind. OSINT ist eine für das CERT M-V essenzielle Quelle für den Warn- und Informationsdienst; es ist eine Methode, bei der Informationen aus dem Internet, Medien, Publikationen und anderen frei verfügbaren Quellen systematisch gesammelt und analysiert werden, um Erkenntnisse zu gewinnen und Wissen zur Gefahrenabwehr zu generieren.

Das CERT M-V wird durch die Meldungen in die Lage versetzt, Maßnahmen zu Risikomitigation oder -vermeidung von möglichen Gefahren oder Schäden zu empfehlen. Zum anderen sollen durch die Meldepflicht zuverlässige Informationen für ein allgemeines Schadens- oder Lagebild gewonnen werden.

Zu Absatz 2

Nach Absatz 2 sind Sicherheitsvorfälle bei öffentlichen Stellen unverzüglich an das CERT M-V zu melden, wenn diese zu einer möglichen Beeinträchtigung der Schutzziele in ihren Daten- und Kommunikationsnetzen (Nummer 1), ihrer Verwaltungsprozesse (Nummer 2) oder von Bürgerdiensten (Verwaltungsdienstleistungen) führen könnten oder bereits geführt haben.

Von einer möglichen Beeinträchtigung ist immer dann auszugehen, wenn die Stelle bei einem zunächst angenommenen Sicherheitsvorfall von einer Verletzung mindestens eines Schutzziels ausgeht (Arbeitshypothese). Der Sicherheitsvorfall kann sich im Laufe der eingeleiteten Sicherheitsvorfallbehandlung im Rahmen der Überprüfung und Analyse bestätigen oder auch nicht. In diesem Status kann die Beeinträchtigung mindestens eines der Schutzziele eine Außenwirkung entfalten.

Satz 2 erweitert die Meldepflicht dahingehend, dass auch Sicherheitsvorfälle bei beauftragten Dienstleistern an das CERT M-V zu melden sind. Demnach haben die öffentlichen Stellen durch vertragliche Vereinbarung ihre IT-Dienstleister zu verpflichten, Sicherheitsvorfälle in deren Tätigkeitsumfeld unaufgefordert, unverzüglich an das CERT M-V zu melden, Informationen bereitzustellen und mit dem CERT M-V zusammenzuarbeiten.

Zu Absatz 3

Um die Informationsweitergabe gemäß den Absätzen 1 und 2 zu standardisieren, insbesondere präventiv und rechtzeitig über Sicherheitsrisiken informieren zu können, wird die für die Digitalisierung zuständige oberste Landesbehörde durch Rechtsverordnung ermächtigt, die notwendigen Festlegungen und Vorgaben zur Klassifizierung von meldepflichtigen Ereignissen, zum Informationsinhalt, zu den Meldewegen und -prozessen zu definieren.

Meldepflichten sind gekoppelt an einer Risikoeinschätzung der jeweiligen öffentlichen Stelle, ob die jeweilige Information oder ein Sicherheitsvorfall zu einem Sicherheitsrisiko für gemeinsam genutzte Informationstechnik oder bei anderen Organisationen führen kann. Klare, standardisierte Vorgaben und Prozesse sind daher notwendig, um ein ziel- und zweckgerichtetes Meldewesen im Land Mecklenburg-Vorpommern zu etablieren.

Zu Absatz 4

Die Regelung in Absatz 4 stellt sicher, dass der Verfassungsschutz bei Cyberangriffen mit möglichem nachrichtendienstlichem Hintergrund frühzeitig informiert wird. Sie dient der schnellen Gefahrenbewertung und der Koordinierung von Abwehrmaßnahmen.

Anhaltspunkte liegen insbesondere bei technisch anspruchsvollen, zielgerichteten Angriffen ohne erkennbares wirtschaftliches Motiv vor.

Damit wird die Zusammenarbeit zwischen den öffentlichen Stellen und der für den Verfassungsschutz zuständigen Behörde gestärkt und der Schutz staatlicher Informationssysteme verbessert.

Zu Absatz 5

Während Absatz 2 eine anlass- bzw. ereignisbezogene Meldepflicht aller öffentlichen Stellen und deren IT-Dienstleister gegenüber dem CERT M-V bei Sicherheitsvorfällen beinhaltet, definiert der Absatz 5 eine regelmäßige, zusammenfassende Informationsbereitstellung zu sicherheitsrelevanten Ereignissen.

Sicherheitsrelevante Ereignisse sollen gemäß § 10 Absatz 2 vorrangig von den Security Analysten in den SOC im Tagesgeschäft analysiert und bewertet werden. Wenn sich aus den Erkenntnissen ein Verdachtsmoment für einen Sicherheitsvorfall ergibt, ist das CERT M-V zu informieren und in die Analysetätigkeiten einzubinden. Das tägliche Grundrauschen ist für das CERT M-V von Interesse, um weiterführende und aggregierte Erkenntnisse zur Sicherheitslage zu erlangen. Würde jedes sicherheitsrelevante Ereignis ungefiltert an das CERT M-V übermittelt werden, wäre die Informations- und Datenflut zu groß. Absatz 4 erweitert die Meldepflicht um eine zusammenfassende Informationspflicht der öffentlichen Stellen über sicherheitsrelevante Ereignisse. Diese Informationspflicht umfasst neben den sicherheitsrelevanten Ereignissen in den öffentlichen Stellen insbesondere die sicherheitsrelevanten Ereignisse, die von den SOC bearbeitet bzw. behandelt werden.

Welche konkreten zusammenfassenden Informationen in welchem Rhythmus an das CERT M-V zu übermitteln sind, ist Gegenstand der Rechtsverordnung nach Absatz 4.

Zu Absatz 6

Die Absätze 1 und 2 definieren die Meldepflichten der öffentlichen Stellen gegenüber dem CERT M-V. Der Absatz 5 erweitert den Kreis der Meldenden auf die sonstigen Stellen unter der Voraussetzung, dass die sonstigen Stellen ihre Informationstechnik mit den Daten- und Kommunikationsnetzen der öffentlichen Verwaltung verbunden haben und eine Datenübertragung über die Daten- und Kommunikationsnetze erfolgt. Dies ist beispielhaft zu bejahen, wenn eine sonstige Stelle ein ebenenübergreifendes IT-Verfahren zur Datenübermittlung über das CN LAVINE, über das Verbindungsnetz (Bund-Länder-Kommunen-Verbindungsnetz [VN, früher: Deutschland Online Infrastruktur, kurz: DOI]) nutzt oder eine Datenübertragung über das CN LAVINE in die Telematik-Infrastruktur der Gematik GmbH erfolgt.

Sind die eingangs aufgeführten Voraussetzungen nicht gegeben, können die sonstigen Stellen Informationen zu sicherheitsrelevanten Ereignissen oder zu Sicherheitsvorfällen an das CERT übermitteln; eine Verpflichtung besteht jedoch nicht. Es wird jedoch den sonstigen Stellen empfohlen, mit dem CERT M-V einen regen Informationsaustausch zu betreiben und somit von den CERT-Basisdiensten zu partizipieren.

Zu § 17

Aufgrund des Aufgaben- und Tätigkeitsumfelds, welches sich für die jeweiligen Funktionen und Rollen in der Informationssicherheitsorganisation dieses Gesetzes ergibt, können dort verarbeitete Informationen sowohl einzeln als auch in Summe äußerst sensibel sein. Das Gesetz zur Regelung des Zugangs zu Informationen für das Land Mecklenburg-Vorpommern (Informationsfreiheitsgesetz – IFG M-V) sieht eine Versagung nur dann vor, wenn die herausgegebene Information für sich genommen sensibel ist, und lässt daher eine Ausforschung durch Informationszugangsanträge zu, die für sich genommen auf unsensible Informationen gerichtet sind, aber in Summe die Zusammenfügung zu einem sensiblen Bild der Informationssicherheit auch für besonders kritische, öffentliche und sonstige Stellen ermöglichen. Im Hinblick auf die geopolitische Lage und die zunehmende Gefahr von Cyberangriffen, auch durch feindlich gesonnene Staaten, müssen diese Informationen daher besonders geschützt werden. Die Sicherstellung derartiger Informationen, die insbesondere kritische öffentliche und sonstige Stellen betreffen, ist essenziell und muss reglementiert werden.

Die Akteneinsichtsrechte von Verfahrensbeteiligten bleiben von dieser Regelung unberührt.

Auch aus datenschutzrechtlicher Sicht beschränkt § 17 das Auskunftsrecht aus Artikel 15 der Verordnung (EU) 2016/679 für den Zugang zu Informationen und Akten. Eine Beschränkung des Rechts auf Auskunft einer betroffenen Person ist zulässig nach Artikel 23 Absatz 1 der Verordnung (EU) 2016/679. Die jeweiligen spezifischen Vorschriften gemäß Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 finden sich in den §§ 11 ff. des Gesetzes.

Zu § 18

Nach Artikel 19 Absatz 1 Satz 2 GG in Verbindung mit Artikel 5 der Verfassung des Landes Mecklenburg-Vorpommern dürfen Beschränkungen des Fernmeldegeheimnisses nur aufgrund eines Gesetzes angeordnet werden. Das Gesetz muss wiederum das Grundrecht unter Angabe des Artikels nennen (sogenanntes Zitiergebot).

Das Recht auf Datenschutz steht dagegen lediglich nach Artikel 6 Absatz 4 der Verfassung des Landes Mecklenburg-Vorpommern unter einem Gesetzesvorbehalt im hier maßgeblichen Sinne, nicht jedoch nach Bundesrecht, wo es aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 GG, die keinen hier maßgeblichen Gesetzesvorbehalt und daher nicht zu zitieren sind, hergeleitet wird.

Zu § 19

Informationstechnik entwickelt sich rasant weiter. So waren beispielsweise die Terminologien Künstliche Intelligenz, Blockchain, Quantencomputing und Container-Sicherheit vor ca. fünf Jahren nur für sehr wenige Experten greifbar; die aus diesem Technologieeinsatz entstehenden Risiken waren bzw. sind noch nicht ausreichend untersucht.

Es ist mit der Erstellung dieses Gesetzes nicht absehbar, welche Daten in der Zukunft verarbeitet und tatsächlich ausgewertet werden müssen, um eine effektive und effiziente Gefahrenabwehr für die Sicherheit der Informationstechnik zu gewährleisten. Um die Informationstechnik im Geltungsbereich dieses Gesetzes stets angemessen zu schützen, soll erprobt werden können, auch Daten zu verarbeiten, die weder den heute definierten Protokolldaten zuzuordnen noch an Schnittstellen der Informationstechnik nicht oder zu anderen Zwecken verarbeitet werden.

Aufgrund neuartiger Bedrohungen entwickelte technische Gegenmaßnahmen erfordern kontrollierte Teststellungen (Machbarkeitsstudien; Proof of Concept) von neuen Analyse- und Abwehrmaßnahmen. Ziel der Teststellungen ist jeweils die Prüfung, wie neuen Bedrohungen in der Form begegnet werden kann, dass ein Ausgleich zwischen dem Schutzinteresse der von den Maßnahmen betroffenen natürlichen Personen und dem notwendigen Schutz der Daten in den von den Bedrohungen betroffenen Informationstechnik gewahrt bleibt. Mit § 19 soll ein entsprechender Freigabeprozess unter der Kontrolle des Chief Information Security Officers M-V und der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern ermöglicht werden.

Zu § 20

Gemäß Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 ist es den Mitgliedstaaten erlaubt, durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5 der Verordnung (EU) 2016/679, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen zu beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, und die Schutzziele des Artikels 23 Absatz 1 Buchstabe a bis j der Verordnung (EU) 2016/679 sicherstellt.

Der Gesetzgeber beruft sich insofern auf Artikel 23 Absatz 1 Buchstabe a, c, d, h sowie i der Verordnung (EU) 2016/679 und beschränkt das Recht auf Auskunft gemäß Artikel 15 und das Recht auf Widerspruch gemäß Artikel 21 der Verordnung (EU) 2016/679, als dass eine Erfüllung dieser Betroffenenrechte die Wahrnehmung der Aufgaben nach diesem Gesetz erheblich beeinträchtigen oder unmöglich machen würden.

Zu Artikel 2 – Änderung des E-Government-Gesetzes Mecklenburg-Vorpommern

Zu § 5

Nach Absatz 1 Satz 1 erhält die oder der Antragstellende bei elektronischer Durchführung eines antragsgebundenen Verwaltungsverfahrens hinsichtlich der Art der Nachweiserbringung grundsätzlich die Wahlmöglichkeit zwischen zwei verschiedenen Wegen. Sie oder er kann entweder einen behördenseitigen automatisierten Nachweisabruf veranlassen (Nummer 1) oder den Nachweis selbst elektronisch erbringen (Nummer 2). Perspektivisch ist angedacht, dass diese Auswahl für mehrere Verfahren getroffen werden kann, sodass sich die oder der Antragstellende für gleich oder ähnlich gelagerte Fälle nicht immer wieder aufs Neue entscheiden muss. Dies würde eine Erleichterung darstellen, sodass nicht jeder Registerabruf separat freigegeben werden muss. Diese Auswahl könnte sodann jederzeit für die Zukunft geändert werden. Nummer 1 dient der Umsetzung des Once-Only-Prinzips. Daten, die der Verwaltung bereits vorliegen, können direkt bei der ausstellenden Behörde abgerufen werden. Diese Wahlmöglichkeit gegenüber der nachweisanfordernden Stelle greift nur, wenn der jeweilige Nachweis elektronisch vorliegt und ohne zeitlichen Verzug, das heißt innerhalb kürzester Zeit, automatisiert abgerufen werden kann. Dies meint fachlich synchrone Abrufverfahren. Sobald also eine menschliche Interaktion notwendig ist und es sich um ein asynchrones Abrufverfahren handelt, kann die Behörde zwar eine Abrufmöglichkeit eröffnen, muss dies aber nicht. Für welche Nachweise ein Once-Only-Nachweisabruf möglich ist, steht im Vorfeld fest und ist technisch hinterlegt. Dasselbe gilt für die für das jeweilige Verfahren erforderlichen Nachweise und die Stellen, welche im konkreten Fall nachweisanfordernde und nachweisliefernde Stelle sind. Die Norm berücksichtigt zudem die Möglichkeit, dass für ein Verwaltungsverfahren mehrere Nachweise erforderlich sein können. Insofern kann die Wahlmöglichkeit für den „jeweiligen“ Nachweis ausgeübt werden, sofern die Voraussetzungen für den Once-Only-Nachweisabruf vorliegen. Der Bürgerin bzw. dem Bürger verbleibt nach Nummer 2 die Möglichkeit, den Nachweis selbst digital zu erbringen. Unter Nummer 2 fällt beispielsweise der bisher schon gängige Weg, in einem Onlinedienst einen Nachweis, das heißt eine elektronische Kopie, hochladen zu können. Darunter könnten zukünftig zudem Wallet-Lösungen fallen, bei denen die oder der Antragstellende einen Nachweis in einem persönlichen Datensafe hält und ihn daraus in den Onlinedienst lädt. Im Übrigen bleibt es dabei, dass ein Antrag unvollständig eingereicht werden darf. Der Anwendungsbereich der Norm ist insofern verengt, dass sie sich nur auf die elektronische Durchführung antragsgebundener Verwaltungsverfahren erstreckt. Danach sind Konstellationen der Leistungsverwaltung mit Ausnahme antragsloser Verwaltungsleistungen erfasst und Fälle der Eingriffsverwaltung ausgeschlossen. Antragslose Verwaltungsleistungen werden mit Blick auf ihren Ausnahmecharakter, den sie jedenfalls heute innehaben, ohnehin spezialgesetzlich geregelt werden. Die Kommunikation zwischen einer Behörde und einer Bürgerin oder einem Bürger per E-Mail fällt in diesem Kontext nicht unter den Begriff der elektronischen Durchführung eines Verwaltungsverfahrens. Gemeint ist die Nutzung eines Onlinedienstes, welcher beispielsweise über ein Verwaltungsportal auffindbar ist. Dazu würde auch ein hybrides Verfahren zählen, bei dem nicht nur Nachweise im Sinne der Norm erforderlich sind, sondern auch andere Beweismittel, welche nicht elektronisch erbracht werden können. Dies ist z. B. der Fall, wenn gemäß § 26 Absatz 1 Nummer 4 VwVfG M-V etwas in Augenschein genommen werden muss. Die Vorgängerregelung, wonach die Vorlage eines Originals in Ausnahmefällen verlangt werden konnte, wurde nicht übernommen. Nach dem verwaltungsverfahrensrechtlichen Untersuchungsgrundsatz (§ 24 VwVfG M-V), welcher gemäß der Regelung in Absatz 1 Satz 2 ausdrücklich unberührt bleibt, kann die für die Entscheidung zuständige Behörde aber auch weiterhin die Möglichkeit haben, einen Nachweis im Original zu verlangen, sofern beispielsweise im Einzelfall Zweifel an der Authentizität eines Dokuments bestehen.

Durch die Bezugnahme auf die §§ 24 bis 27 VwVfG M-V wird zudem deutlich, dass die dort genannten Möglichkeiten zur Sachverhaltsermittlung bestehen bleiben. Insofern ist ein hybrides Verfahren mit elektronischen Nachweisen und analoger Beweisführung denkbar. Um medienbruchfreie Verfahren zu fördern, erhält die oder der Antragstellende bei einem Nachweis, der elektronisch erbracht werden kann, aber ausschließlich die in Absatz 1 genannten Möglichkeiten. Absatz 1 Satz 5 enthält eine gesetzliche Bestimmung dazu, wer Verantwortlicher im Falle eines Once-Only-Nachweisabrufs ist. Eine solche Regelung ist gemäß Artikel 4 Nummer 7 DSGVO zulässig, sofern wie hier Zwecke und Mittel der Verarbeitung gesetzlich vorgegeben sind. Absatz 1 Satz 5 weist die Verantwortung für den Nachweisabruf einseitig der nachweisanfordernden Stelle zu. Die meisten Landesdatenschutzgesetze enthalten bereits eine solche Regelung für den Fall automatisierter Abrufverfahren und auch die Durchführungsverordnung (EU) 2022/1463 enthält für das europäische Once-Only-Technical-System eine entsprechende Zuweisung der Verantwortlichkeit für die Vollständigkeit und Rechtmäßigkeit der Nachweisanfrage in Artikel 34. Auf diese Art werden die datenschutzrechtlichen Pflichten klar und eindeutig sowie im Einklang mit der Interessenlage der nachweisanfordernden Stelle zugewiesen.

Zu Absatz 2

Absatz 2 definiert in den Sätzen 1 bis 3 die nachfolgenden zentralen normbestimmenden Begriffe: Nachweis, nachweisanfordernde und nachweisliefernde Stelle. So sind nach Absatz 1 Satz 3 Nachweise Unterlagen und Daten jeder Art unabhängig vom verwendeten Medium, die zur Ermittlung des Sachverhalts geeignet sind. In Anlehnung an die Definition in Artikel 3 Nummer 5 der Verordnung (EU) 2018/1724 vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (ABl. L 295 vom 21.11.2018, S. 1) wird der Nachweisbegriff weit gefasst. Der weite Nachweisbegriff wird aber bezüglich des automatisierten Abrufs insofern eingeschränkt, als dass nur solche Nachweise erfasst sind, die elektronisch vorliegen und ohne zeitlichen Verzug automatisiert abgerufen werden können. Durch das Begriffspaar Unterlagen und Daten wird dem Verständnis des Datenbegriffs in der Informatik Rechnung getragen, der dort enger aufgefasst wird als im allgemeinen Sprachgebrauch. Gemäß Absatz 2 Satz 2 kann die nachweisanfordernde Stelle entweder die öffentliche Stelle selbst sein, die über den Antrag entscheidet, oder aber eine andere öffentliche Stelle, die dafür zuständig ist, den Nachweis einzuholen und anschließend an die zuständige Behörde weiterzuleiten. Solche anderen öffentlichen Stellen können beispielsweise Stellen sein, die für eine Portallösung oder einen EfA-Onlinedienst zuständig sind. In Satz 3 wird klargestellt, dass die nachweisliefernde Stelle diejenige Stelle ist, die für die Ausstellung des Nachweises zuständig ist. Damit wird der Umstand berücksichtigt, dass mehrere Behörden über einen Nachweis verfügen können, aber nur eine Stelle für die Aktualität Sorge trägt und insofern beispielsweise das „führende“ Register für den jeweiligen Nachweis betreibt. Welche konkrete Stelle das jeweils ist, muss vorab technisch hinterlegt sein.

Zu Absatz 3

Absatz 3 enthält gemäß dem Doppeltürmodell des Bundesverfassungsgerichts und im Sinne von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e Absatz 3 DSGVO die datenschutzrechtlichen Rechtsgrundlagen für den Abruf der Nachweise. Es soll ein vollständiger digitaler Nachweis ermöglicht werden. In Satz 1 werden weitere Voraussetzungen festgelegt. Darin soll zum einen der datenschutzrechtliche Zweckbindungsgrundsatz gestützt werden, indem der Nachweisabruf für die Erfüllung der Aufgabe erforderlich sein muss, und durch ein hypothetisches Direkterhebungselement als zusätzliches Tatbestandsmerkmal wird sichergestellt, dass die Behörde den Nachweis hypothetisch bei der oder dem Antragstellenden erheben dürfte, auch wenn allgemein kein Direkterhebungsgrundsatz mehr gilt. Dadurch wird eine Verknüpfung mit dem Fachrecht hergestellt, das hierfür geprüft werden muss. Satz 2 deckt einen weiteren möglichen Datenfluss ab, wenn die nachweisanfordernde Stelle nicht selbst die für die Entscheidung über den Antrag zuständige Behörde ist. In diesem Fall darf die nachweisanfordernde Stelle (z. B. ein Portal) den Nachweis einholen und anschließend an die für die Entscheidung über den Antrag zuständige Stelle übermitteln.

Zu Absatz 4

Absatz 4 gilt nur für solche Nachweise, die aus einem der in der Anlage zum Identifikationsnummerngesetz (IDNrG) aufgeführten Register abgerufen werden sollen. Im Sinne der Ziele des Registermodernisierungsgesetzes, insbesondere der Einführung eines registerübergreifenden Identitätsmanagements zum Zwecke der Erbringung von Verwaltungsleistungen nach dem Onlinezugangsgesetz, ermöglicht die Regelung des Absatzes 4 die Übermittlung der Identifikationsnummer gemäß § 139b der Abgabenordnung (AO) und der weiteren Daten nach § 4 Absatz 2 und 3 IDNrG an die nachweisliefernde Stelle zum Zwecke der Zuordnung der Datensätze, Validierung dieser Zuordnung zu der oder dem Antragstellenden und zum Zwecke des Nachweisabrufs. Im Sinne des datenschutzrechtlichen Grundsatzes der Datenminimierung nach Artikel 5 Buchstabe c DSGVO sollen nur diejenigen Daten nach § 4 Absatz 2 und 3 IDNrG übermittelt werden, die für diese Zweckerreichung erforderlich sind. Die nachweisliefernde Stelle kann anhand dieser Daten den zu der oder dem Antragstellenden gehörigen Nachweis ermitteln und an die nachweisanfordernde Stelle weitergeben. Damit bei der nachweisanfordernden Stelle der Nachweis wiederum richtig zugeordnet werden und eine Überprüfung dazu stattfinden kann, ob es sich um den angefragten Nachweis handelt, können hierzu die Identifikationsnummer und die weiteren Daten nach § 4 Absatz 2 und 3 IDNrG in der Antwortnachricht der nachweisliefernden Stelle an die nachweisanfordernde Stelle enthalten sein. Absatz 3 regelt daher die Verarbeitung im Sinne des § 6 Absatz 2 IDNrG. Als Pendant zur Identifikationsnummer, die nur natürliche Personen erhalten, wird die Wirtschafts-Identifikationsnummer nach § 139c AO als bundeseinheitliche Wirtschaftsnummer nach § 2 Absatz 1 des Unternehmensbasisdatenregistergesetzes (UBRegG) für Unternehmen im Sinne des § 3 Absatz 1 UBRegG bei Once-Only-Nachweisabrufen als eindeutiger Identifikator relevant werden.

Zu Absatz 5

Absatz 5 regelt die sog. Vorschaufunktion. Sie ermöglicht der oder dem Antragstellenden, die automatisiert abgerufenen Nachweise vor deren Verwendung für das Antragsverfahren einzusehen und zu entscheiden, ob sie oder er mit dem Antragsverfahren unter Verwendung des angezeigten Nachweises fortfahren möchte. Die oder der Antragstellende kann auf die Vorschau verzichten. Dies muss er nicht aktiv tun. Eine technische Umsetzung, nach der die oder der Antragstellende die Vorschau aktiv anstoßen muss, ist zulässig. Die Vorschaufunktion veranschaulicht der oder dem Antragstellenden, welche Daten konkret abgerufen wurden sowie welche Daten für das Verwaltungsverfahren verwendet werden sollen, und steigert dadurch die Transparenz des digitalen Verwaltungsverfahrens. Auch der europäische Once-Only-Nachweisabruf sieht – vorbehaltlich mitgliedstaatlicher oder unionsrechtlicher Ausnahmeregelungen im Sinne von Artikel 14 Absatz 5 SDG-VO eine Vorschau vor. Mittels Vorschaufunktion kann die Nutzerin bzw. der Nutzer bei unrichtigen oder veralteten Daten die Verwendung des Nachweises unterbinden und dadurch selbst dazu beitragen, dass Verwaltungsentscheidungen effizient und auf Grundlage von aktuellen, richtigen Daten getroffen werden. Entscheidet sich die oder der Antragstellende nach Einsicht der Daten in der Vorschau gegen die Verwendung dieser Daten im Antrag, so bleiben ihm die Möglichkeiten, den Nachweis gemäß Absatz 1 Satz 1 Nummer 2 selbst elektronisch einzureichen, den Antrag unvollständig einzureichen oder die Antragstellung abzubrechen und den analogen Antragsweg zu beschreiten. Durch die Vorschaufunktion ergibt sich eine erweiterte, über das verfassungsrechtlich geforderte Maß hinausgehende Transparenz, die die Funktion des Datenschutzcockpits im Sinne des Artikels 1 § 2 Nummer 3 RegMoG (§ 10 OZG – neu) ergänzt. Während im Datenschutzcockpit im Nachgang jede Übermittlung der personenbezogenen Daten unter Nutzung der Identifikationsnummer nachvollzogen werden kann, bietet die Vorschaufunktion zudem eine Einsichts- und Kontrollmöglichkeit der oder des Antragstellenden im Vorfeld und das unabhängig von der Verwendung der Identifikationsnummer. Die Vorschaufunktion greift also auch bei solchen Datenübermittlungen, bei denen die oder der Antragstellende auch weiterhin anhand seiner Basisdaten identifiziert wird.

Zu § 5a

Die Regelung dient der Umsetzung des Artikels 14 SDG-VO. Nach Artikel 14 SDG-VO errichten die Kommission und die Mitgliedstaaten gemeinsam ein technisches System für den automatisierten Austausch von Nachweisen zwischen zuständigen Behörden in verschiedenen Mitgliedstaaten (europäisches Once-Only-Technical-System, EU-OOTS) zur Umsetzung des Grundsatzes der einmaligen Erfassung (Once-Only-Prinzip). Nach dem europäischen Once-Only-Prinzip sollen, was bezogen auf Behörden innerhalb Deutschlands auch Regelungsgegenstand des § 5 ist, in der Verwaltung bereits vorliegende Nachweise im Rahmen weiterer Verwaltungsprozesse nicht erneut bei Bürgerinnen, Bürgern oder Unternehmen erhoben, sondern zwischen öffentlichen Stellen ausgetauscht werden. Die datenschutzrechtliche Ermächtigung der Stellen, die Nachweise austauschen zu dürfen, ist dabei nicht Gegenstand der Regelung in Artikel 14 SDG-VO (vergleiche Europäischer Datenschutzbeauftragter, Stellungnahme 8/2017, Stellungnahme des EDSB zu dem Vorschlag für eine Verordnung über die Einrichtung eines zentralen digitalen Zugangstors und den Grundsatz der „einmaligen Erfassung“, S. 15; Europäische Kommission, Arbeitsdokument, Datenschutzfolgenabschätzung zur Durchführungsverordnung (EU) 2022/1463 der Kommission vom 5. August 2022 zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates, SWD(2022) 211 final, S. 3 f.).

Diese muss auf Ebene der Union oder im Recht der Mitgliedstaaten geschaffen werden. In diesem Sinne enthält § 5a erforderliche datenschutzrechtliche Rechtsgrundlagen für den Nachweisaustausch über das EU-OOTS. Als Verordnung gilt Artikel 14 SDG-VO unmittelbar, weshalb darauf verzichtet wurde, auf relevante Systemspezifika des EU-OOTS explizit Bezug zu nehmen. So sollen Nachweise über das EU-OOTS grundsätzlich nur auf ausdrückliches Ersuchen der oder des Nutzenden hin ausgetauscht werden sowie der oder dem Nutzenden grundsätzlich die Möglichkeit einer Vorschau des abgerufenen Nachweises ermöglicht werden. Die Absätze 4 und 5 räumen den Mitgliedstaaten und dem Unionsgesetzgeber selbst einen diesbezüglichen Regelungsspielraum ein. Von diesen Öffnungsklauseln wird mit der Regelung des § 5a kein Gebrauch gemacht. Eine Durchführungsverordnung (Durchführungsverordnung (EU) 2022/1463 der Kommission vom 5. August 2022 zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates) enthält daneben weitere technische und operative Spezifikationen. Insbesondere weist sie in Artikel 34 die datenschutzrechtliche Verantwortung für Vollständigkeit und Rechtmäßigkeit des Nachweisabrufs der nachweisanfordernden Stelle („evidence requester“) zu. § 5a gilt dabei nur für solche Nachweise im Sinne von Artikel 14 Absatz 2 SDG-VO, die für Verfahren nach Artikel 14 Absatz 1 SDG-VO relevant sind. Die relevanten Verfahren nach Artikel 14 Absatz 1 SDG-VO ergeben sich einerseits aus Anhang II der SDG-VO sowie aus den Richtlinien 2005/36/EG, 2006/123/EG, 2014/24/EU und 2014/25/EU. Eine Legaldefinition für den Nachweisbegriff hat der Unionsgesetzgeber in Artikel 3 Nummer 5 SDG-VO aufgenommen. Danach sind Nachweise „alle Unterlagen oder Daten, einschließlich Text- oder Ton-, Bild- oder audiovisuellen Aufzeichnungen, unabhängig vom verwendeten Medium, die von einer zuständigen Behörde verlangt werden, um Sachverhalte oder die Einhaltung der in Artikel 2 Absatz 2 Buchstabe b genannten Verfahrensvorschriften nachzuweisen“. Artikel 14 Absatz 2 verengt seinen Anwendungsbereich wiederum auf solche Nachweise nach dieser Definition, die bereits innerstaatlich in einem elektronischen Format ausgestellt und automatisiert ausgetauscht werden. Insofern stellt der Unionsgesetzgeber in Artikel 14 Absatz 2 keine Digitalisierungspflicht für Nachweise auf, sondern stellt auf die individuellen Verhältnisse in den Mitgliedstaaten ab. Der Bund hat eine gleichlautende Regelung in das E-Government-Gesetz als § 5a aufgenommen. Dieser gilt (mit Ausnahme der §§ 2a, 9a bis 9c) auch für die Behörden des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen (vergleiche § 1 Absatz 1, 2 EGovG). Damit das mit § 5a EGovG verfolgte Ziel auch umfassend erreicht werden kann, soll diese Regelung nun auch für die noch nicht abgedeckten Bereiche ins Landesrecht übernommen werden.

Zu Absatz 1

Absatz 1 enthält die datenschutzrechtliche Rechtsgrundlage im Landesrecht für Nachweisabrufe von Behörden bei Behörden eines anderen Mitgliedstaates.

Zu Absatz 2

Absatz 2 enthält hingegen die datenschutzrechtliche Rechtsgrundlage im Landesrecht für Nachweisübermittlungen von Behörden an Behörden eines anderen Mitgliedstaates.

Zu Absatz 3

Absatz 3 enthält den Hinweis, dass bei der Verarbeitung personenbezogener Daten nach den Absätzen 1 und 2 intermediäre Plattformen zum Einsatz kommen können. Diese Möglichkeit folgt unmittelbar aus der Durchführungsverordnung (EU) 2022/1463, vgl. insbesondere Artikel 2 Buchstabe b und die Legaldefinition in Artikel 1 Absatz 6. Intermediäre Plattformen können sowohl auf der Seite des Mitgliedstaates zum Einsatz kommen, der einen Nachweis aus einem anderen Mitgliedstaat über das EU-OOTS abrufen möchte, als auch auf der Seite des nachweisliefernden Staates. Es obliegt der Verwaltungsorganisation der Mitgliedstaaten, über das Ob und Wie des Einsatzes intermediärer Plattformen zu entscheiden. Die Durchführungsverordnung (EU) 2022/1463 lässt insbesondere offen, ob intermediäre Plattformen im eigenen Namen, das heißt in Ausübung einer eigenen Verantwortlichkeit, oder im Namen anderer Behörden, das heißt im Auftrag oder nur als technischer Dienst, tätig werden sollen. Im nationalen Kontext muss dies erst noch entschieden werden. Mit Blick auf die vorwiegend dezentrale Registerstruktur in Deutschland wird eine Anbindung über intermediäre Plattformen beabsichtigt.

Zu § 13

Die Neufassung des § 13 verfolgt die verpflichtende Nutzung der Kommunikations- und Datennetze der öffentlichen Verwaltung, insbesondere des CN LAVINE durch die öffentlichen Stellen im Land Mecklenburg-Vorpommern bei allen Datenübermittlungen öffentlicher Stellen im Land, zu Stellen in anderen Ländern und dem Bund. Die historisch bedingte Abgrenzung auf „automatisierte Verfahren“ ist aufgrund des technologischen Fortschritts verbunden mit dem Glasfaserausbau im Land Mecklenburg-Vorpommern nicht mehr erforderlich.

Von diesem Grundsatz der Nutzung kann im begründeten Einzelfall abgewichen werden. Dies erfordert eine Ausnahmegenehmigung durch die für die Digitalisierung zuständigen obersten Landesbehörde.

Zu § 16

Aufgrund der Regelungen im ISichG M-V erfolgen Anpassungen im § 16. Absatz 2 wird dahingehend aktualisiert, dass die Funktion der oder des CIO M-V nicht an die Staatssekretärin oder den Staatssekretär der für die Digitalisierung zuständigen obersten Landesbehörde gebunden ist.

Neben der in Absatz 3 Nummer 2 übertragenen Aufgabe, die strategische Ausrichtung der IT-Politik des Landes festzulegen, wird die oder der CIO M-V ergänzend die Aufgabe der Durchsetzung der IT-Richtlinie, IT-Standards und IT-Architekturen übertragen. Die oder der CIO M-V erhält somit ein Durchgriffsrecht, um auf der taktischen und operativen Ebene in den Bereichen der Informationstechnologie und Digitalisierung wirken zu können.

Darüber hinaus verantwortet nunmehr die nach Absatz 3 Nummer 5 definierte Steuerung des ressortübergreifenden IT-Sicherheitsmanagements nach § 5 ISichG M-V der Chief Information Security Officer M-V, da die IT-Sicherheit einen Teilbereich der Informationssicherheit darstellt und somit im Informationssicherheitsmanagementsystem des Landes inkludiert ist.

Zu Artikel 3 – Inkrafttreten

Artikel 3 regelt das Inkrafttreten.