Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften

Vorblatt

A. Zielsetzung

Durch die fortschreitende Digitalisierung in allen Arbeits- und Lebensbereichen wird die Cybersicherheit immer bedeutsamer. Sie ist daher ein unverzichtbarer Querschnittsbereich der Digitalisierungsstrategie digital@bw. Die Abwehr von Gefahren für die Cybersicherheit soll durch die Errichtung der Cybersicherheitsagentur Baden-Württemberg zentralisiert und weiter professionalisiert werden. Überdies soll der Komm.ONE die Möglichkeit gegeben werden, in Ausnahmesituationen Sitzungen digital durchzuführen.

B. Wesentlicher Inhalt

Um die Cybersicherheit zu verbessern, werden mit dem Gesetz die Landesoberbehörde Cybersicherheitsagentur Baden-Württemberg errichtet sowie deren Aufgaben und Befugnisse geregelt. Dadurch werden die Effektivität und Effizienz staatlicher Aufgabenwahrnehmung erhöht, indem der Einsatz von Ressourcen für die Cybersicherheit effizient an zentraler Stelle gebündelt wird. Sie soll primär die öffentlichen Stellen als Ergänzung zu den bereits bestehenden Strukturen im Bereich der Informationssicherheit unterstützen. Zur umfassenden Förderung der Cybersicherheit kann sie bei öffentlichen Stellen des Landes Untersuchungen durchführen, die Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme wiederherstellen sowie Standards und Maßnahmen durchsetzen. Sie betreibt eine zentrale Koordinierungs- und Meldestelle. Außerdem kann sie in Einzelfällen auch nichtöffentliche Stellen beraten und bei Sicherheitsvorfällen unterstützen. Sie sensibilisiert zu Themen der Cybersicherheit auch die Bürgerinnen und Bürger. Außerdem ermöglicht das Gesetz der Komm.ONE, in bestimmten Fällen Sitzungen in digitaler Form zuzulassen.

C. Alternativen

Eine vollständige Übertragung der mit diesem Gesetz der Cybersicherheitsagentur zugewiesenen Aufgaben an private Unternehmen scheidet aus Sicherheitsgründen aus. Die Landesverwaltung würde sich zudem in technische und fachliche Abhängigkeiten begeben und eigene informationstechnische Kompetenz verlieren.

Eine weitere Alternative wäre die Beibehaltung der bisherigen Regelung, jedoch würde dies den Erfordernissen einer fortschreitenden Digitalisierung – insbesondere der er-

höhten Gefährdungslage durch Cyberangriffe – nicht gerecht. Um das verstärkte Nutzungsverhalten der Beschäftigten sowie der Bürgerinnen und Bürger über das Internet abzusichern und um dezentrale Mehrfachstrukturen zu reduzieren, muss die Abwehr von Gefahren für die Cybersicherheit verbessert werden und möglichst gebündelt bei einer Cybersicherheitsagentur erfolgen.

D. Kosten für die öffentlichen Haushalte (ohne Erfüllungsaufwand)

Zum Aufbau einer Cybersicherheitsarchitektur sind Personal- und Sachausgaben in Höhe von insgesamt 4 000 000 Euro im Haushaltsjahr 2020 und 9 000 000 Euro im Haushaltsjahr 2021 veranschlagt.

Mit erheblichen Einnahmen durch Gebühren ist nicht zu rechnen, weil für öffentliche Stellen nach § 10 des Landesgebührengesetzes persönliche Gebührenfreiheit gilt.

Im Übrigen sind Kosten für den Landeshaushalt im Rahmen des vom Haushaltsgesetzgeber genehmigten Ausbaus nicht zu erwarten, aber Festlegungen der Cybersicherheitsagentur zur Verbesserung der IT-Sicherheit können zu Anpassungen der IT-Infrastruktur der Dienststellen führen. Diese Kosten sind aktuell nicht zu beziffern.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht kein Erfüllungsaufwand.

E.3 Erfüllungsaufwand für die Verwaltung

Über die Einrichtung und Erhaltung der Cybersicherheitsagentur hinaus entsteht der Verwaltung kein Erfüllungsaufwand. Diese Mehraufwendungen werden im Rahmen der zur Verfügung stehenden Haushaltsmittel gedeckt; insoweit wird Finanzneutralität sichergestellt.

F. Nachhaltigkeitscheck

Das Gesetz wirkt sich positiv auf die Zielbereiche ökologische und soziale Modernisierung der Wirtschaft sowie Verschuldung, leistungsfähige Verwaltung und Justiz aus, weil die Cybersicherheitsagentur die Prozessoptimierung, Qualifikation des Personals für eine leistungsfähige Verwaltung und Justiz sowie Wettbewerbsfähigkeit des Wirtschaftsstandortes fördert. Darüber hinaus ergeben sich keine erheblichen Auswirkungen auf die ökonomischen, ökologischen und sozialen Verhältnisse.

G. Sonstige Kosten für Private

Keine.

Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften

Vom

Artikel 1
Gesetz für die Cybersicherheit in Baden-Württemberg
(Cybersicherheitsgesetz – CSG)

INHALTSÜBERSICHT

Teil 1
Allgemeine Vorschriften

§ 1
Cybersicherheitsagentur

(1) Das Land errichtet und unterhält die Landesoberbehörde Cybersicherheitsagentur Baden-Württemberg (Cybersicherheitsagentur). Die Cybersicherheitsagentur ist zuständig für die Cybersicherheit in Baden-Württemberg.

(2) Die Cybersicherheitsagentur hat ihren Sitz in Stuttgart.

(3) Das Innenministerium führt die Dienst- und Fachaufsicht über die Cybersicherheitsagentur.

§ 2
Begriffsbestimmungen

(1) Öffentliche Stelle im Sinne dieses Gesetzes ist jede Stelle des Landes, der Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Dies umfasst auch natürliche oder juristische Personen des Privatrechts, soweit sie öffentlich-rechtliche Verwaltungsaufgaben, insbesondere solche der Daseinsvorsorge, wahrnehmen oder öffentliche Dienstleistungen erbringen und dabei der Kontrolle einer Stelle im Sinne des Satzes 1 unterliegen. Kontrolle im Sinne des Satzes 2 liegt vor, wenn

1. die Person des Privatrechts bei der Wahrnehmung der öffentlichen Aufgabe oder bei der Erbringung der öffentlichen Dienstleistung gegenüber Dritten besonderen Pflichten unterliegt oder über besondere Rechte verfügt, insbesondere ein Kontrahierungszwang oder ein Anschluss- und Benutzungszwang besteht, oder

2. eine oder mehrere der in Satz 1 genannten juristischen Personen des öffentlichen Rechts allein oder zusammen, unmittelbar oder mittelbar

    a) die Mehrheit des gezeichneten Kapitals der Person des Privatrechts besitzt oder besitzen oder

    b) über die Mehrheit der mit den Anteilen der Person des Privatrechts verbundenen Stimmrechte verfügt oder verfügen oder

    c) mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans der Person des Privatrechts stellen kann oder können.

(2) Stellen des Landes mit Sonderstatus im Sinne dieses Gesetzes sind

1. der Landtag,

2. der Rechnungshof,

3. die oder der Landesbeauftragte für den Datenschutz,

4. die Gerichte und Staatsanwaltschaften,

5. die Steuerverwaltung,

6. das Statistische Landesamt,

7. die Hochschulen und

8. die sonstigen Stellen des Landes

soweit eine Verpflichtung nach diesem Gesetz im Widerspruch zu der verfassungsrechtlichen Stellung oder anderen gesetzlichen Regelungen für diese Stellen stünde. Für diese sollen einvernehmlich gesonderte Vereinbarungen zwischen der Cybersicherheitsagentur und der jeweils zuständigen obersten Landesbehörde getroffen werden.

(3) Nicht als öffentliche Stellen des Landes im Sinne dieses Gesetzes gelten die Beliehenen.

(4) Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Systeme, die der Verarbeitung und Übertragung von Informationen dienen.

(5) Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen betreffen, durch Umsetzung entsprechender Sicherheitsmaßnahmen in der Informationstechnik.

(6) Kommunikationstechnik des Landes im Sinne dieses Gesetzes ist die Informationstechnik, die von einer oder mehreren öffentlichen Stellen des Landes oder im Auftrag einer oder mehrerer öffentlichen Stellen des Landes betrieben wird und der Kommunikation oder dem Datenaustausch der öffentlichen Stellen untereinander oder mit dritten Personen dient. Die Kommunikationstechnik der in Absatz 2 genannten Stellen, des Landesamts für Verfassungsschutz, des Polizeivollzugsdienstes und der Strafverfolgungsbehörden ist nicht Kommunikationstechnik des Landes, soweit sie unter deren eigener Fachaufsicht oder unter der Fachaufsicht einer ihr übergeordneten Behörde steht oder in deren eigener oder länderübergreifender Zuständigkeit betrieben wird.

(7) Schnittstellen der Kommunikationstechnik des Landes im Sinne dieses Gesetzes sind sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Landes sowie zwischen dieser und der Informationstechnik der einzelnen Stellen, Gruppen von Stellen oder dritten Personen. Dies gilt nicht für die Komponenten an den Netzwerkübergängen, die unter deren eigener Fachaufsicht oder unter der Fachaufsicht einer ihr übergeordneten Behörde steht oder in eigener oder länderübergreifender Zuständigkeit der in Absatz 2 genannten Stellen, des Landesamts für Verfassungsschutz, des Polizeivollzugsdienstes oder der Strafverfolgungsbehörden betrieben werden.

(8) Das Landesverwaltungsnetz im Sinne dieses Gesetzes ist eine Kommunikationstechnik des Landes, die eine gesicherte Verbindung zwischen den lokalen Netzen der damit verbundenen Stellen sowie zu Netzen anderer Verwaltungen ermöglicht und durch das Land oder im Auftrag des Landes betrieben wird.

(9) Informationssicherheit im Sinne dieses Gesetzes umfasst alle technischen und nichttechnischen Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

(10) Cyberraum ist der virtuelle Raum aller weltweit vernetzten Informationstechnik. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, das durch beliebige andere Datennetze erweitert werden kann.

(11) Cybersicherheit im Sinne dieses Gesetzes umfasst alle Aspekte der Sicherheit in der Informationstechnik und den Schutz gesellschaftlich relevanter Prozesse vor Angriffen im gesamten Cyberraum.

(12) Schadprogramme im Sinne dieses Gesetzes sind Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen, zu verändern oder zu löschen oder unbefugt auf sonstige informationstechnische Abläufe einzuwirken.

(13) Sicherheitslücken im Sinne dieses Gesetzes sind Eigenschaften von Programmen oder sonstiger Informationstechnik, durch deren Ausnutzung es möglich ist, dass sich dritte Personen gegen den Willen der oder des Berechtigten Zugang zu fremder Informationstechnik verschaffen oder die Funktion der Informationstechnik beeinflussen können.

(14) Protokolldaten im Sinne dieses Gesetzes sind Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikations-

vorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation notwendig sind. Protokolldaten können Verkehrsdaten nach § 3 Nummer 30 des Telekommunikationsgesetzes und Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes enthalten.

§ 3
Aufgaben

(1) Die Cybersicherheitsagentur fördert die Cybersicherheit und die damit zusammenhängenden Aspekte der Informationssicherheit. Hierzu nimmt sie insbesondere folgende wichtige im öffentlichen Interesse liegende Aufgaben wahr:

1. Abwehr von Gefahren für die Cybersicherheit,

2. Schutz gesellschaftlicher Prozesse vor Angriffen im Cyberraum,

3. a) Mitwirkung an der Entwicklung und Setzung von Standards für die Cybersicherheit der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen sowie

   b) Überprüfung der Einhaltung der geltenden Standards für die Cybersicherheit,

4. Betrieb einer zentralen Koordinierungs- und Meldestelle nach § 4,

5. Kontaktstelle im Rahmen des Verfahrens zu § 8b des BSI-Gesetzes und Unterrichtung der zuständigen Aufsichtsbehörden, obersten Landesbehörden sowie der Koordinierungsstelle Kritische Infrastrukturen über die Informationen, die sie als Kontaktstelle erhalten hat,

6. Information und Beratung zur Cybersicherheit und

7. Kompetenzzentrum für Sensibilisierungen und Schulungen zur Cybersicherheit.

(2) Die Cybersicherheitsagentur kann auf Ersuchen bei der Abwehr von Gefahren für die Cybersicherheit unterstützen oder auf qualifizierte sicherheitsdienstleistende Personen verweisen. Sie soll auf Ersuchen die Polizei, die Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz bei der Wahrnehmung ihrer gesetzlichen Aufgaben technisch unterstützen, insbesondere bei der Durchführung von technischen Untersuchungen oder der Datenverarbeitung. Die Unterstützung darf nur gewährt werden, soweit sie erforderlich

ist, um Tätigkeiten zu verhindern oder zu erforschen, die die Cybersicherheit beeinträchtigen könnten. Die Unterstützungsersuchen sind durch die Cybersicherheitsagentur aktenkundig zu machen. Andere öffentliche Stellen des Landes hat die Cybersicherheitsagentur auf Ersuchen bei der Abwehr von Gefahren für die Cybersicherheit zu unterstützen.

(3) Die Regelungen des Errichtungsgesetzes BITBW bleiben unberührt.

§ 4
Zentrale Koordinierungs- und Meldestelle

(1) Die Cybersicherheitsagentur ist die zentrale Koordinierungs- und Meldestelle für die Zusammenarbeit der öffentlichen Stellen in Angelegenheiten der Cybersicherheit in Baden-Württemberg.

(2) Die Cybersicherheitsagentur hat zur Wahrnehmung dieser Aufgabe

1. alle für die Abwehr von Gefahren für die Cybersicherheit erforderlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Cybersicherheit und der dabei beobachteten Vorgehensweise, strukturiert zu sammeln und auszuwerten,

2. öffentliche Stellen unverzüglich über die sie betreffenden Informationen nach Nummer 1 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist, und

3. die Maßnahmen der öffentlichen Stellen des Landes für die Abwehr der Gefahren für die Cybersicherheit zu koordinieren, soweit nicht andere gesetzliche Vorschriften entgegenstehen.

(3) Werden anderen öffentlichen Stellen des Landes oder unmittelbar an das Landesverwaltungsnetz angeschlossenen Stellen Informationen nach Absatz 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder die Cybersicherheit anderer öffentlicher Stellen von Bedeutung sind oder sein können, melden sie diese nach Maßgabe der aufgrund § 13 Nummer 3 erlassenen Rechtsverordnung ab dem 1. Januar 2022 unverzüglich der Cybersicherheitsagentur, soweit andere Vorschriften dem nicht entgegenstehen. Anderweitig begründete Meldepflichten bleiben hiervon unberührt.

(4) Ausgenommen von den Unterrichtungspflichten nach Absatz 2 Nummer 2 und Absatz 3 sind Informationen, die aufgrund von Regelungen zum Geheimschutz, Weitergabevorbehalten der Herausgeberinnen oder Herausgeber oder Vereinbarungen mit dritten Personen

nicht weitergegeben werden dürfen oder deren Weitergabe im Widerspruch zu der verfassungsrechtlichen Stellung einer oder eines Abgeordneten des Landtages oder eines Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde.

(5) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.

Teil 2
Befugnisse

§ 5
Abwehr von Gefahren für die Cybersicherheit

(1) Um die öffentlichen Stellen und das Landesverwaltungsnetz vor Gefahren für die Cybersicherheit zu schützen, kann die Cybersicherheitsagentur gegenüber öffentlichen Stellen des Landes und an das Landesverwaltungsnetz angeschlossenen Stellen die erforderlichen Anordnungen treffen und Maßnahmen ergreifen. Sie trifft Anordnungen und ergreift Maßnahmen erst nach Ablauf einer zuvor gesetzten, angemessenen Frist zur Beseitigung der Gefahr. Sie darf nur im Einvernehmen mit der jeweils fachlich zuständigen obersten Landesbehörde oder im Einzelfall aufgrund Beschlusses des IT-Rates Baden-Württemberg Anordnungen treffen oder Maßnahmen vornehmen. Davon kann ausnahmsweise abgesehen werden, wenn zur Gefahrenabwehr sofortiges Handeln erforderlich ist. Dies muss durch die Präsidentin oder den Präsidenten der Cybersicherheitsagentur angeordnet werden. Die Entscheidung ist zu protokollieren und der betroffenen obersten Landesbehörde unverzüglich mitzuteilen. Die betroffene oberste Landesbehörde kann bei dem IT-Rat Baden-Württemberg die Überprüfung dieser Entscheidung beantragen. Satz 1 gilt nicht für die Informationstechnik des Landesamts für Verfassungsschutz, des Polizeivollzugsdienstes und der Strafverfolgungsbehörden, soweit sie in deren eigener oder länderübergreifender Zuständigkeit betrieben wird.

(2) Die Cybersicherheitsagentur kann zur Abwehr von Gefahren für die Cybersicherheit

1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Landes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Landes oder von Angriffen auf die Cybersicherheit des Landes erforderlich ist, und

2. die an den Schnittstellen der Kommunikationstechnik des Landes anfallenden Daten erheben und automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist.

Auch die anderen öffentlichen Stellen des Landes und die an das Landesverwaltungsnetz angeschlossenen Stellen können Daten entsprechend Satz 1 innerhalb ihres jeweiligen Zuständigkeitsbereichs erheben und automatisiert auswerten. Sofern nicht die nachfolgenden Absätze eine weitere Verarbeitung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die öffentlichen Stellen des Landes sind verpflichtet, die Cybersicherheitsagentur bei ihren Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang der Cybersicherheitsagentur zu internen Protokolldaten nach Satz 1 Nummer 1 sowie Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen.

(3) Protokolldaten nach Absatz 2 Satz 1 Nummer 1 und Satz 2 dürfen über den für die automatisierte Auswertung nach Absatz 2 Satz 1 Nummer 1 und Satz 2 erforderlichen Zeitraum hinaus, längstens jedoch für drei Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass diese für den Fall der Bestätigung eines Verdachts nach Absatz 5 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Auswertung oder eine personenbezogene Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten der Cybersicherheitsagentur angeordnet werden. Die Entscheidung ist zu protokollieren.

(4) Die Verarbeitungsbeschränkungen nach Absatz 2 und 3 gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten.

(5) Eine über Absatz 2 bis 4 hinausgehende Verarbeitung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass

1. diese ein Schadprogramm enthalten,

2. diese durch ein Schadprogramm übermittelt wurden oder

3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können,

und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies

1. zur Abwehr des Schadprogramms,

2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder

3. zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Die nicht automatisierte Verarbeitung der Daten nach den Sätzen 1 und 2 darf nur durch Bedienstete mit der Befähigung zum Richteramt angeordnet werden.

(6) Die Cybersicherheitsagentur übermittelt unverzüglich die nach Absatz 5 verarbeiteten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms begangenen Straftat nach den §§ 202a, 202b, 202c, 263a, 269, 271, 274 Absatz 1 Nummer 2 und den §§ 303a, 303b oder 348 des Strafgesetzbuches.

(7) Für sonstige Zwecke übermittelt die Cybersicherheitsagentur die Daten unverzüglich

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,

2. an die Polizei zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- und Vermögenswerte.

Die Übermittlung nach Satz 1 Nummer 1 bedarf der vorherigen gerichtlichen Zustimmung. Ist die gerichtliche Zustimmung nicht rechtzeitig einholbar, hat die Cybersicherheitsagentur die Datenübermittlung unverzüglich vorzunehmen und die gerichtliche Zustimmung binnen drei Werktagen nach erfolgter Datenübermittlung einzuholen. Für das Verfahren nach Satz 1 Nummer 1 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk die Cybersicherheitsagentur ihren Sitz hat.

(8) Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an dritte Personen ist unzulässig.

(9) Vor der Datenverarbeitung nach Absatz 2 hat die Cybersicherheitsagentur eine Datenschutz-Folgenabschätzung nach Artikel 35 der 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, zuletzt ber. ABl. L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung durchzuführen und die oder den Landesbeauftragten für den Datenschutz nach Artikel 36 der Verordnung (EU) 2016/679 zu konsultieren. Die Cybersicherheitsagentur übermittelt das von der oder dem Landesbeauftragten für den Datenschutz mitgeteilte Ergebnis der Konsultation dem IT-Rat Baden-Württemberg.

(10) Die Cybersicherheitsagentur unterrichtet die oder den Landesbeauftragten für den Datenschutz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über

1. die Anzahl der Vorgänge, in denen sie Daten nach Absatz 6 oder Absatz 7 übermittelt hat, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,

2. die Anzahl der von ihr durchgeführten personenbezogenen Auswertungen nach Absatz 5 Satz 1, in denen der Verdacht widerlegt wurde.

(11) Die Cybersicherheitsagentur unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Innenausschuss des Landtages über ihre Anwendung dieses Paragrafen.

(12) Soweit Informationstechnik von Stellen des Landes mit Sonderstatus unter deren eigener Fachaufsicht oder unter der Fachaufsicht einer ihr übergeordneten Behörde oder in deren eigener oder länderübergreifender Zuständigkeit betrieben wird, dürfen nach diesem Paragrafen keine Anordnungen getroffen werden und Maßnahmen nur im Einvernehmen mit diesen Stellen durchgeführt werden.

§ 6
Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer öffentlichen Stelle um einen herausgehobenen Fall, so soll die Cybersicherheitsagentur auf Ersuchen der betroffenen Stelle die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind.

(2) Ein herausgehobener Fall nach Absatz 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist.

(3) Die Cybersicherheitsagentur darf bei Maßnahmen nach Absatz 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten verarbeiten, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten in Fällen des Absatzes 4 an eine andere öffentliche Stelle zur Erfüllung von deren gesetzlichen Aufgaben weitergegeben worden sind, darf die Cybersicherheitsagentur die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser öffentlichen Stelle weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an dritte Personen sind unzulässig.

(4) Die Cybersicherheitsagentur darf Informationen, von denen sie im Rahmen dieser Vorschrift Kenntnis erlangt, nur mit Einwilligung der ersuchenden Stelle weitergeben, es sei denn, die Informationen lassen keine Rückschlüsse auf die Identität der ersuchenden Stelle zu oder die Informationen sind entsprechend § 5 Absatz 6 und 7 zu übermitteln. Zugang zu den in Verfahren nach Absatz 1 geführten Akten wird dritten Personen nicht gewährt.

(5) Die Cybersicherheitsagentur kann sich bei Maßnahmen nach Absatz 1 mit der Einwilligung der ersuchenden Stelle der Hilfe qualifizierter dritter Personen bedienen, wenn dies zur rechtzeitigen oder vollständigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die Cybersicherheitsagentur kann die ersuchende Stelle auch auf qualifizierte dritte Personen verweisen. Die Cybersicherheitsagentur und von der ersuchenden Stelle oder von der Cybersicherheitsagentur nach Satz 1 beauftragte dritte Personen können einander bei Maßnahmen nach Absatz 1 mit der Einwilligung der ersuchenden Stelle Daten übermitteln. Hierfür gilt Absatz 3 entsprechend.

(6) Soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems erforderlich ist, kann die Cybersicherheitsagentur von der herstellenden Person des informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken.

(7) In begründeten Einzelfällen kann die Cybersicherheitsagentur auch bei anderen als den in Absatz 1 genannten Stellen mit wichtiger Bedeutung für das öffentliche Gemeinwesen tätig werden, wenn sie darum ersucht wurde und es sich um einen herausgehobenen Fall im Sinne des Absatzes 2 handelt. Eine Übermittlung von Informationen nach Absatz 4 in Verbindung mit § 5 Absatz 6 und 7 kann im Einzelfall bei einem geltend gemachten schutzwürdigen Interesse der ersuchenden Stelle unterbleiben.

(8) Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, ist in Fällen der Absätze 1, 4, 5 und 7 vor Tätigwerden der Cybersicherheitsagentur das Benehmen mit den zuständigen atomrechtlichen Aufsichtsbehörden des Bundes und der Länder herzustellen. Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, haben bei Maßnahmen der Cybersicherheitsagentur nach § 6 die Vorgaben aufgrund des Atomgesetzes Vorrang.

(9) Soweit die Cybersicherheitsagentur erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für die Tätigkeit der Cybersicherheitsagentur erhoben. Die durch die Hinzuziehung qualifizierter dritter Personen entstehenden Kosten hat die ersuchende Stelle zu tragen.

§ 7
Untersuchung der Sicherheit in der Informationstechnik

(1) Die Cybersicherheitsagentur kann zur Erfüllung ihrer Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und Nummer 3 Buchstabe b die Sicherheit der Informationstechnik der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen im Einvernehmen mit der jeweils fachlich zuständigen obersten Landesbehörde untersuchen und bewerten. Satz 1 gilt nicht für die Informationstechnik des Landesamts für Verfassungsschutz, des Polizeivollzugsdienstes und der Strafverfolgungsbehörden, soweit sie in deren eigener oder länderübergreifender Zuständigkeit betrieben wird. Über die gewonnenen Erkenntnisse erstellt die Cybersicherheitsagentur einen Bericht, der der untersuchten Stelle zur Verfügung gestellt wird.

(2) Die Cybersicherheitsagentur kann zur Erfüllung ihrer Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 6 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Sie kann sich hierbei der Unterstützung dritter Personen bedienen, soweit berechtigte Interessen der herstellenden Person der betroffenen Produkte und Systeme dem nicht entgegenstehen. Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 6 genutzt werden. Die Cybersicherheitsagentur

darf ihre Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist der herstellenden Person der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.

§ 8
Warnungen, Empfehlungen und Hinweise

(1) Die Cybersicherheitsagentur kann die Öffentlichkeit oder die betroffenen Kreise vor Gefahren für die Cybersicherheit, insbesondere zu Sicherheitslücken, Schadprogrammen oder im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten, warnen und Sicherheitsmaßnahmen und den Einsatz bestimmter Sicherheitsprodukte empfehlen. Warnungen und Empfehlungen dürfen die Bezeichnung der herstellenden oder der inverkehrbringenden Person des betroffenen Produkts oder Dienstes nur umfassen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Cybersicherheit von dem Produkt oder Dienst ausgehen. Bevor die Cybersicherheitsagentur informiert, hat sie die herstellende oder die inverkehrbringende Person anzuhören, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks nicht gefährdet wird. Auf berechtigte Interessen der betroffenen Stellen ist Rücksicht zu nehmen.

(2) Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern, weil sie staatlichen Geheimhaltungserfordernissen unterliegen oder weil die Cybersicherheitsagentur gegenüber dritten Personen zur Vertraulichkeit verpflichtet ist, kann sie den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen, ein übergeordnetes methodisch-analytisches Aufklärungsinteresse oder die besondere Zuverlässigkeit der zu warnenden Personen sein.

(3) Die Cybersicherheitsagentur kann ihrerseits die Öffentlichkeit auf

1. Warnungen, Empfehlungen und Hinweise oder

2. eine Rücknahme- oder Rückrufaktion

durch die herstellende oder inverkehrbringende Person hinweisen. Die Cybersicherheitsagentur kann die Öffentlichkeit auf von einer anderen öffentlichen Stelle veröffentlichte Informationen hinweisen, soweit berechtigte Interessen der Öffentlichkeit im Zuständigkeitsbereich der Cybersicherheitsagentur berührt sind.

(4) Die Cybersicherheitsagentur kann Personen zur Wahrnehmung der Aufgaben nach Absatz 1 bis 3 einbeziehen, wenn dies für eine wirksame und rechtzeitige Information erforderlich ist.

(5) Stellen sich die von der Cybersicherheitsagentur an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch oder die zu Grunde liegenden Umstände als unrichtig wiedergegeben heraus, so ist dies unverzüglich zu veröffentlich. Sobald die Voraussetzungen nach Absatz 1 entfallen sind, sind die Öffentlichkeit oder die betroffenen Kreise unverzüglich darüber zu informieren. Die Bekanntmachungen nach Satz 1 und Satz 2 sollen in derselben Weise erfolgen, in der die Information nach Absatz 1 erfolgt ist. Die Informationen sind sechs Monate nach der Veröffentlichung nach Satz 1 zu entfernen.

Teil 3
Datenschutz

§ 9
Anwendbarkeit des Landesdatenschutzgesetzes

Das Landesdatenschutzgesetz findet Anwendung, soweit dieses Gesetz keine abweichenden Regelungen enthält.

§ 10
Kernbereichsschutz

Technisch ist sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verarbeitet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Cybersicherheitsagentur legt Fälle, in denen sich die Frage stellte, ob Daten aus dem Kernbereich privater Lebensgestaltungen erhoben wurden, der oder dem behördlichen Datenschutzbeauftragten der Cybersicherheitsagentur sowie einer oder einem weiteren Bediensteten der Cybersicherheitsagentur mit Befähigung zum Richteramt zur Kontrolle vor. Wenn die oder der behördliche Datenschutzbeauftragte der Entscheidung der Cybersicherheitsagentur widerspricht, ist die Löschung nachzuholen. Die Umstände der Erlangung solcher Daten und deren Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verarbeitet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 11

Schutz von Zeugnisverweigerungsrechten

Werden Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 und § 53a Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich ein Zeugnisverweigerungsrecht dieser Personen erstreckt, ist die Verwertung dieser Daten unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Dies gilt nicht, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person die Gefahr für die Cybersicherheit oder für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- und Vermögenswerte verursacht hat.

§ 12
Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch die Cybersicherheitsagentur ist zulässig, wenn die Verarbeitung zur Erfüllung ihrer im öffentlichen Interesse liegenden Aufgaben erforderlich ist.

(2) Die Verarbeitung personenbezogener Daten durch die Cybersicherheitsagentur zu anderen Zwecken als denjenigen, zu denen die Daten ursprünglich erhoben wurden, ist unbeschadet von Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 und § 5 LDSG zulässig, wenn

1. die Verarbeitung erforderlich ist

    a) zur Sammlung, Auswertung oder Untersuchung von Informationen zur Abwehr von Gefahren für die Cybersicherheit oder

    b) zur Unterstützung, Beratung, Warnung, Empfehlung oder zum Hinweis in Fragen der Cybersicherheit und

2. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

(3) Eine Verarbeitung von besonderen Kategorien personenbezogener Daten durch die Cybersicherheitsagentur ist abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 und unbeschadet des § 17 Absatz 2 LDSG zulässig, wenn

1. die Verarbeitung erforderlich ist zur Abwehr einer erheblichen Gefahr für die Cybersicherheit,

2. ein Ausschluss dieser Daten von der Verarbeitung die Erfüllung der Aufgaben der Cybersicherheitsagentur unmöglich machen oder diese erheblich gefährden würde und

3. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss dieser Daten von der Verarbeitung überwiegt.

(4) Die Cybersicherheitsagentur sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person nach § 3 LDSG vor.

Teil 4
Schlussvorschriften

§ 13
Rechtsverordnungen

Das Innenministerium kann im Einvernehmen mit dem IT-Rat Baden-Württemberg durch Rechtsverordnung regeln:

1. die Standards für die Informationssicherheit im Sinne des § 2 Absatz 9,

2. die Standards für die Cybersicherheit nach § 3 Absatz 1 Satz 2 Nummer 3 einschließlich der Verfahren zur Überprüfung von Standards,

3. das Nähere zu den Meldepflichten nach § 4 Absatz 3,

4. das Nähere zur Untersuchung der Sicherheit in der Informationstechnik nach § 7 und

5. die ressortübergreifende Organisation im Bereich der Cyber- und Informationssicherheit.

§ 14
Verwaltungsvorschriften

Das Innenministerium trifft nähere Regelungen zur Organisation und zum Betrieb der Cybersicherheitsagentur durch Verwaltungsvorschriften.

§ 15

Berichtspflichten

(1) Die Cybersicherheitsagentur unterrichtet das Innenministerium und den IT-Rat Baden-Württemberg über ihre Tätigkeit.

(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Innenministerium über Gefahren für die Cybersicherheit, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 8 Absatz 1 Satz 3 und Absatz 2 ist entsprechend anzuwenden.

§ 16
Einschränkung von Grundrechten

Das Fernmeldegeheimnis gemäß Artikel 10 des Grundgesetzes wird durch die §§ 5, 6 und 7 eingeschränkt.

Artikel 2
Änderung des BITBWG

In § 2 Absatz 1 Nummer 2 des Gesetzes zur Errichtung der Landesoberbehörde IT Baden-Württemberg (Errichtungsgesetz BITBW – BITBWG) vom 12. Mai 2015 (GBl. S. 326), das durch Artikel 9 des Gesetzes vom 19. Februar 2019 (GBl. S. 37, 46) geändert worden ist, werden die Wörter „in der Landesverwaltung“ durch die Wörter „im Zusammenhang mit den in Nummer 1 geregelten Aufgaben sowie den in Absatz 3 und 4 geregelten Dienstleistungen“ ersetzt.

Artikel 3
Änderung des EGovG BW

Das Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg (E-Government-Gesetz Baden-Württemberg – EGovG BW) vom 17. Dezember 2015 (GBl. S. 1191), das zuletzt durch Artikel 3 des Gesetzes vom 17. Juni 2020 (GBl. S. 401) geändert worden ist, wird wie folgt geändert:

1. In § 16 Absatz 1 wird die Angabe „§ 9“ durch die Angabe „§ 3“ ersetzt.

2. In § 20 Absatz 4 Satz 1 werden die Wörter „und die Landesoberbehörde BITBW“ durch die Wörter „, die Landesoberbehörden BITBW und Cybersicherheitsagentur“ ersetzt.

3. In § 22 Absatz 3 werden die Wörter „Landesoberbehörde BITBW“ durch die Wörter „Landesoberbehörden BITBW und Cybersicherheitsagentur“ ersetzt.

4. § 23 Absatz 2 Satz 3 Nummer 3 wird wie folgt gefasst:

„je eine Vertretung der Landesoberbehörden BITBW und Cybersicherheitsagentur sowie“.

Artikel 4
Absehen von der Zusage der Umzugskostenvergütung in besonderen Härtefällen

(1) Bei einer durch den Vollzug dieses Gesetzes veranlassten Versetzung an einen anderen Dienstort ist auf Antrag der Beamtin oder des Beamten von der Zusage der Umzugskostenvergütung abzusehen, wenn im Zeitpunkt der Versetzung

1. die Beamtin oder der Beamte

   a) das 61. Lebensjahr, im Falle einer Schwerbehinderung im Sinne des § 2 Absatz 2 des Neunten Buches Sozialgesetzbuch das 58. Lebensjahr, vollendet hat oder

   b) in der Erwerbsfähigkeit um mindestens 50 Prozent gemindert ist oder

   c) durch eine schwere Erkrankung, die voraussichtlich länger als ein Jahr andauern wird, am Umzug gehindert ist,

2. der Ehegatte oder die Ehegattin, der Lebenspartner oder die Lebenspartnerin nach dem Lebenspartnerschaftsgesetz oder ein beim Familienzuschlag nach dem Landesbesoldungsgesetz Baden-Württemberg berücksichtigungsfähiges Kind, mit dem die Beamtin oder der Beamte in häuslicher Gemeinschaft lebt, voraussichtlich länger als ein Jahr schwer erkrankt oder wegen dauernder Pflegebedürftigkeit in einer Einrichtung untergebracht ist, die vom neuen Dienstort mindestens doppelt so weit entfernt ist als vom bisherigen Dienst- oder Wohnort oder

3. die Beamtin oder der Beamte in einer eigenen Wohnung wohnt. Eine eigene Wohnung ist eine Wohnung, die im Allein- oder Miteigentum der Beamtin oder des Beamten steht.

Als eigene Wohnung gilt auch eine Wohnung, die im Eigentum des Ehegatten oder der Ehegattin oder des Lebenspartners oder der Lebenspartnerin nach dem Lebenspartnerschaftsgesetz steht, mit dem oder der die Beamtin oder der Beamte in häuslicher Gemeinschaft lebt.

(2) Absatz 1 findet keine Anwendung, wenn die Zusage der Umzugskostenvergütung nach dem Landesumzugskostengesetz ausgeschlossen ist, weil die zu versetzende Person bereits am neuen Dienstort oder in dessen Einzugsgebiet wohnt.

(3) Bei einem Absehen von der Zusage der Umzugskostenvergütung ist der versetzten Person schriftlich mitzuteilen, aus welchem Grund und gegebenenfalls mit welcher zeitlichen Befristung die Erstattungszusage unterbleibt.

(4) Von der Zusage der Umzugskostenvergütung wird im Falle des Absatzes 1 Nummer 1 Buchstabe a bis zur Versetzung oder bis zum Eintritt in den Ruhestand, im Übrigen für die Dauer von bis zu einem Jahr ab dem Zeitpunkt der Versetzung abgesehen. Hat die versetzte Person im Zeitpunkt des Ablaufs der Jahresfrist das in Absatz 1 Nummer 1 Buchstabe a genannte Lebensjahr vollendet, wird von der Zusage der Umzugskostenvergütung bis zur Versetzung oder bis zum Eintritt in den Ruhestand abgesehen. Eine mit der Versetzung oder Übernahme bereits erteilte Erstattungszusage kann bei Vorliegen der Voraussetzungen des Absatzes 1 auf Antrag der Beamtin oder des Beamten widerrufen werden.

(5) Für die Zeit, in der nach Absatz 4 von der Zusage der Umzugskostenvergütung abgesehen wird, besteht nach Maßgabe der Landestrennungsgeldverordnung ein Anspruch auf Trennungsgeld. Das Absehen von der Zusage der Umzugskostenvergütung ist spätestens innerhalb eines Monats nach Zustellung der Versetzungsverfügung schriftlich bei der Behörde zu beantragen, die über die Erstattungszusage zu entscheiden hat. Dem Antrag sind Nachweise über das Vorliegen der Voraussetzungen des Absatzes 1 beizufügen.

(6) Die versetzte Person ist verpflichtet, den Wegfall der Voraussetzungen des Absatzes 1 unverzüglich der für die Zusage der Umzugskostenvergütung zuständigen Behörde anzuzeigen; sie ist berechtigt, trotz Fortbestehens der Voraussetzungen die Zusage der Umzugskostenvergütung zu beantragen.

(7) Über die Zusage der Umzugskostenvergütung ist in den Fällen des Absatzes 1 Nummer 1 Buchstabe b und c sowie Nummer 2 und 3 zum Zeitpunkt des Wegfalls der dort genannten Voraussetzungen, spätestens jedoch zum Zeitpunkt des Ablaufs der Jahresfrist gemäß Absatz 4 von Amts wegen nach den allgemeinen Vorschriften des Landesumzugskostengesetzes zu entscheiden.

(8) Bei Tarifbeschäftigten ist entsprechend zu verfahren.

Artikel 5
Personalverwaltung

§ 1
Änderung des Ernennungsgesetzes

In § 4 Satz 1 Nummer 7 des Ernennungsgesetzes in der Fassung vom 29. Januar 1992 (GBl. S. 141), das zuletzt durch Artikel 3 des Gesetzes vom 19. November 2019 (GBl. S. 479, 480) geändert worden ist, werden nach den Wörtern „Landesamt für Verfassungsschutz“ die Wörter „, der Cybersicherheitsagentur“ eingefügt.

§ 2
Personalverwaltung für Tarifbeschäftigte

(1) Das Innenministerium ist personalverwaltende Stelle für die Tarifbeschäftigten der Cybersicherheitsagentur.

(2) Das Innenministerium überträgt die Personalverwaltung für die Tarifbeschäftigten mit Ausnahme der Arbeitnehmerinnen und Arbeitnehmer im vergleichbar höheren Dienst an die Cybersicherheitsagentur. Die Übertragung kann jederzeit durch das Innenministerium erweitert oder widerrufen werden.

Artikel 6
Änderung des Landesbesoldungsgesetzes Baden-Württemberg

Das Landesbesoldungsgesetz Baden-Württemberg vom 9. November 2010 (GBl. S. 793, 826), das zuletzt durch Artikel 2 des Gesetzes vom 17. Juni 2020 (GBl. S. 401) geändert worden ist, wird wie folgt geändert:

1. In Anlage 1 (Landesbesoldungsordnung A) wird im Abschnitt Besoldungsgruppe A 16 nach der Amtsbezeichnung „Parlamentsrat[6)]“ die Amtsbezeichnung „Vizepräsident der Cybersicherheitsagentur“ angefügt.

2. In Anlage 2 (Landesbesoldungsordnung B) wird im Abschnitt Besoldungsgruppe B 3 nach der Amtsbezeichnung „Polizeipräsident“ mit Funktionszusätzen die Amtsbezeichnung „Präsident der Cybersicherheitsagentur“ eingefügt.

Artikel 7
Änderung der Unfallfürsorgezuständigkeitsverordnung

Die Anlage der Unfallfürsorgezuständigkeitsverordnung vom 18. Dezember 1980 (GBl. 1981 S. 2), die zuletzt durch Artikel 12 des Gesetzes vom 19. Februar 2019 (GBl. S. 37, 47) geändert worden ist, wird wie folgt geändert:

1. In Spalte 2 wird Nummer 1.10 wie folgt angefügt:

   „1.10 Cybersicherheitsagentur“.

2. In Spalte 3 wird Nummer 1.10 wie folgt angefügt:

   „1.10 der Cybersicherheitsagentur mit Ausnahme des Präsidenten der Cybersicherheitsagentur und dessen Stellvertreter“.

Artikel 8
Änderung der Bekanntmachung der Ministerien über die Vertretung des Landes in gerichtlichen Verfahren und förmlichen Verfahren vor den Verwaltungsbehörden

In Abschnitt I Absatz 1 Nummer 1 der Bekanntmachung der Ministerien über die Vertretung des Landes in gerichtlichen Verfahren und förmlichen Verfahren vor den Verwaltungsbehörden vom 28. Februar 2012 (GBl. S. 138), zuletzt geändert durch Artikel 22 des Gesetzes vom 21. Mai 2019 (GBl. 161, 188) werden die Wörter „dem Informatikzentrum Landesverwaltung Baden-Württemberg (IZLBW)“ durch die Wörter „der IT Baden-Württemberg (BITBW)“ ersetzt und anschließend eine neue Zeile mit den Wörtern „der Cybersicherheitsagentur“ eingefügt.

Artikel 9
Überprüfung der Auswirkungen des Gesetzes

Die Auswirkungen von Artikel 1 dieses Gesetzes werden nach einem Erfahrungszeitraum von drei Jahren durch die Landesregierung unter Mitwirkung der kommunalen Landesverbände, der oder des Landesbeauftragten für den Datenschutz und gegebenenfalls weiterer sachverständiger Personen überprüft. Die Landesregierung unterrichtet den Landtag über das Ergebnis der Evaluierung.

Artikel 10

Änderung des ADV-Zusammenarbeitsgesetzes

Das ADV-Zusammenarbeitsgesetz vom 6. März 2018 (GBl. S. 65, 66, ber. S. 126), das durch Artikel 1 des Gesetzes vom 17. Juni 2020 (GBl. S. 401) geändert worden ist, wird wie folgt geändert:

1. In § 5 wird nach Absatz 3 folgender Absatz 3a eingefügt:

   „(3a) Durch die Anstaltssatzung kann bestimmt werden, dass notwendige Sitzungen des Verwaltungsrats ohne persönliche Anwesenheit der Verwaltungsratsmitglieder im Sitzungsraum durchgeführt werden können; dies gilt nur, sofern eine Beratung und Beschlussfassung durch zeitgleiche Übertragung von Bild und Ton mittels geeigneter technischer Hilfsmittel, insbesondere in Form einer Videokonferenz, möglich ist. Dieses Verfahren darf nur gewählt werden, wenn die Sitzung andernfalls aus schwerwiegenden Gründen nicht ordnungsgemäß durchgeführt werden könnte. Schwerwiegende Gründe liegen insbesondere vor bei Naturkatastrophen, aus Gründen des Infektionsschutzes oder bei sonstigen außergewöhnlichen Notsituationen, wenn eine ordnungsgemäße Durchführung ansonsten unzumutbar wäre. Der Vorstand hat sicherzustellen, dass die technischen Anforderungen und die datenschutzrechtlichen Bestimmungen für eine ordnungsgemäße Durchführung der Sitzung einschließlich Beratung und Beschlussfassung eingehalten werden. In einer Sitzung nach Satz 1 dürfen Wahlen im Sinne von Absatz 2 Satz 3 nicht durchgeführt werden. Im Übrigen bleiben die für den Geschäftsgang von Sitzungen des Verwaltungsrats geltenden Vorschriften unberührt.

2. § 5 Absatz 4 Satz 8 wird wie folgt gefasst:

   „Absatz 3a Satz 1 bis 4 sowie die für den Geschäftsgang des Verwaltungsrats geltenden Vorschriften finden entsprechende Anwendung.“

Artikel 11
Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Stuttgart, den

Die Regierung des Landes Baden-Württemberg:

Begründung

Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften

A. Allgemeiner Teil

1. Zielsetzung

a) Ausgangslage und Anlass

2015 war zunächst lediglich die Sicherheit in der Informationstechnik (IT) im Fokus. Damals wurde eine IT-Sicherheitsstrategie entwickelt und der IT-Sicherheit zumindest in der Landesverwaltung eine hohe Priorität eingeräumt.

Im Koalitionsvertrag für 2016 bis 2021 zwischen BÜNDNIS 90/DIE GRÜNEN und der CDU wird dann umfassender die Cybersicherheit als „eine der zentralen Voraussetzungen für eine immer digitalere Welt“ bewertet. Den Schutz vernetzter Informationsstrukturen zu gewährleisten ist demnach staatliche Aufgabe. Der Aufbau von Sicherheitsarchitekturen und Sicherheitskonzepten soll in Abstimmung mit dem Bund und Europa verstärkt vorangetrieben werden. Dazu gehören neben der Analyse von Schwachstellen auch die Registrierung von Sicherheitslücken bei IT-Angriffen und der Schutz von Staat, Bürgerinnen und Bürger sowie Unternehmen vor Cyberattacken.

In einer Studie des Zentrums für Europäische Wirtschaftsforschung (ZEW) in Mannheim als Vorbereitung für die Digitalisierungsstrategie wurde 2017 ausgeführt: „Durch die fortschreitende Digitalisierung in allen Arbeits- und Lebensbereichen wächst der Stellenwert der Cybersicherheit. Beim Vergleich der Sicherheitslage der Verbraucher nach Bundesländern ist Baden-Württemberg nur im unteren Mittelfeld anzutreffen. Auch ist die Bereitschaft der Unternehmen in Baden-Württemberg, an Initiativen wie der Allianz für Cybersicherheit teilzunehmen, verhältnismäßig gering. Die Erarbeitung einer umfassenden Cybersicherheitsstrategie durch die baden-württembergische Landesregierung kann jedoch als wichtiger Meilenstein betrachtet werden.“

In der 2017 von der Landesregierung beschlossenen Digitalisierungsstrategie digital@bw ist die Cybersicherheit ein unverzichtbarer Querschnittsbereich. Cybersicherheit ist ein erfolgskritischer Parameter für die nachhaltige Entwicklung und Wettbewerbsfähigkeit des Landes und damit ein wesentlicher Standortfaktor.

Im Bereich Cybersicherheit gibt es eine Vielzahl von Einrichtungen, Institutionen und Behörden. Auf europäischer Ebene werden aktuell Agenturen eingerichtet oder europaweite Forschungskooperationen vereinbart. Auf der Bundesebene gibt es insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), die Agentur für Innovation in der Cybersicherheit, die Agentur für Sprunginnovationen, das Bundeskriminalamt (BKA), das Bundesamt für Verfassungsschutz (BfV), den Bundesnachrichtendienst (BND), die Allianz für Cybersicherheit (ACS) sowie das Zentrum für Cybersicherheit der Bundeswehr (ZCSBw). Auf Länderebene sind insbesondere das Hessen-Cyber-Competence-Center (Hessen3C) oder das Landesamt für Sicherheit in der Informationstechnik (LSI) in Bayern zu nennen, die jeweils die Maßnahmen für die Cybersicherheit in ihren Ländern bündeln.

Die Vielzahl der bereits bestehenden und personell aufwachsenden Organisationen und Institutionen auf nationaler, europäischer und internationaler Ebene machen deutlich, dass in Baden-Württemberg eine zentrale Ansprechstelle erforderlich ist, um die Informationen zu sammeln, auszuwerten und an die betroffenen Stellen weiterzuleiten und um die Aktivitäten in Baden-Württemberg koordinieren und umsetzen zu können. Dadurch könnte die operative Leistungsfähigkeit von staatlichen Institutionen mit denen von Wirtschaftsunternehmen, von Forschung und Wissenschaft besser verzahnt werden.

Für den Aufbau einer Cybersicherheitsarchitektur sind im Einzelplan des Ministeriums für Inneres, Digitalisierung und Migration als Sachmittel 994 700 Euro im Haushaltsjahr 2020 und 1 413 000 Euro im Haushaltsjahr 2021 veranschlagt. Überdies sind für den Aufbau 32 neue Personalstellen im Jahr 2020 und weitere 51 Personalstellen im Jahr 2021 vorgesehen.

Die Errichtung als Landesoberbehörde berücksichtigt die ressortübergreifende und zunehmende Bedeutung der Cybersicherheit.

b) Erforderlichkeit

Eine Landesoberbehörde kann nach § 25 Absatz 1 des Landesverwaltungsgesetzes nur durch Gesetz eingerichtet werden. Die Landesoberbehörde Cybersicherheitsagentur Baden-Württemberg im Geschäftsbereich des Ministeriums für Inneres, Digitalisierung und Migration ist notwendig, weil eine geeignete Organisation oder Institution für diese Querschnittsaufgabe fehlt, die organisationsübergreifend die vorhandenen privaten und staatlichen Akteure bei der Cybersicherheit unterstützen und koordinieren könnte. Bisher arbeiten Staat, Verwaltungen, Kommunen, Wirtschaft, Wissenschaft und Forschung weitgehend in ihren jeweiligen Systemen.

Nur mit einem ganzheitlichen Ansatz können die aktuellen und künftigen Herausforderungen, Bedrohungs- und Gefährdungslagen für die Cybersicherheit effektiv und effizient bewältigt werden. Die Chancen der Digitalisierung können so erfolgreicher genutzt werden, wenn die Risiken und Gefahren für alle Bereiche von Staat, Wirtschaft und Gesellschaft beherrscht werden können.

c) Ziele des Entwurfs

Ziel der optimierten Cybersicherheitsstruktur mit einer Cybersicherheitsagentur Baden-Württemberg ist zum einen der Schutz der IT des Landes und zum anderen auch den Kommunen, den Bürgerinnen und Bürgern, der Wirtschaft sowie der Wissenschaft Informationen und Unterstützung in den Bereichen Cybersicherheit, Cybercrime, Cybersabotage und Cyberspionage sowie aktuelle Gefährdungsszenarien zur Verfügung zu stellen. Die Cybersicherheitsagentur soll damit Aufgaben übernehmen, die bisher nicht wahrgenommen wurden. Darüber hinaus bündelt sie Aufgaben, die andernfalls dezentral erledigt werden müssten.

Zentralisierung und Professionalisierung der Abwehr der Gefahren für die Cybersicherheit eröffnen neue technologische und organisatorische Möglichkeiten und bieten Vorteile und Synergien für die gesamte Landesverwaltung, die dezentrale informationstechnische Einheiten in einzelnen Behörden nicht erzielen können. Nur in einer Cybersicherheitsagentur mit standardisierten und hoch effizienten Strukturen kann die Wirtschaftlichkeit der Gefahrenabwehr verbessert werden. Auf bestehenden Strukturen in der Cybersicherheit aufbauend werden Parallelstrukturen vermieden. Dabei werden vorwiegend Aufgaben wahrgenommen, die komplementär sind, d.h. von anderen Stellen nicht besser wahrgenommen werden können. Vereinzelt übernimmt die Cybersicherheitsagentur Aufgaben, etwa das bisherige Computer Emergency Response Team der Landesverwaltung Baden-Württemberg (CERT BWL) der Landesoberbehörde IT Baden-Württemberg (BITBW), um Synergieeffekte zu erzielen. Durch die Cybersicherheitsagentur werden ein zentraler Informationsaustausch und eine zentrale Koordinierung von Maßnahmen zwischen den

unterschiedlichen Akteuren sichergestellt. Die Verantwortlichkeiten und Zuständigkeiten der IT-Leitstellen der Ressorts, der IT-Dienstleister des Landes sowie deren jeweilige Fachaufsicht für den IT-Betrieb in dem jeweiligen Bereich werden durch die Einrichtung der Cybersicherheitsagentur nicht tangiert.

Privatwirtschaftliche Angebote von IT-Sicherheitsleistungen dürfen dabei nicht von staatlicher Seite ersetzt werden, sondern sollen wo möglich, in ihrer Entstehung und Entwicklung unterstützt werden.

Überdies soll der Komm.ONE die Möglichkeit gegeben werden, in Ausnahmesituationen Sitzungen digital durchzuführen.

2. Inhalt

Das Gesetz enthält in Artikel 1 das Gesetz für die Cybersicherheit in Baden-Württemberg (Cybersicherheitsgesetz – CSG) sowie in Artikel 2 bis 9 die notwendigen Anpassungen weiterer Gesetze und der Vertretungsregelung in gerichtlichen Verfahren und förmlichen Verfahren vor den Verwaltungsbehörden sowie Regelungen über eine Evaluierung. Artikel 10 ermöglicht der Komm.ONE in bestimmten Fällen Sitzungen in digitaler Form zuzulassen. Das Inkrafttreten regelt Artikel 11.

Durch das CSG werden die Landesoberbehörde „Cybersicherheitsagentur Baden-Württemberg“ errichtet sowie deren Aufgaben und Befugnisse geregelt. Sie dient primär der Unterstützung der öffentlichen Stellen als Ergänzung zu den bereits bestehenden Strukturen im Bereich der Informationssicherheit. Überdies werden Regelungen zum Datenschutz und zur Rolle des Innenministeriums (Regelungsbefugnis für Standards, Meldepflichten, Organisation und Betrieb der Cybersicherheitsagentur) sowie Berichtspflichten geregelt.

Zur Förderung der Cybersicherheit nimmt die Cybersicherheitsagentur nach § 3 Absatz 1 Satz 2 CSG insbesondere folgende im öffentlichen Interesse liegende Aufgaben wahr:

- Abwehr von Gefahren für die Cybersicherheit,
- Schutz gesellschaftlicher Prozesse vor Angriffen im Cyberraum,
- Mitwirkung an der Entwicklung und Setzung von Standards für die Cybersicherheit der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen sowie Überprüfung der Einhaltung der Standards,
- Betrieb einer zentralen Koordinierungs- und Meldestelle,

- Kontaktstelle im Rahmen des Verfahrens zu § 8b des BSI-Gesetzes und Unterrichtung der zuständigen Aufsichtsbehörden, obersten Landesbehörden und der Koordinierungsstelle Kritische Infrastrukturen (KoSt KRITIS) über die Informationen, die sie als Kontaktstelle erhalten hat,
- Information und Beratung zur Cybersicherheit und
- Kompetenzzentrum für Sensibilisierungen und Schulungen.

Überdies hat die Cybersicherheitsagentur nach § 3 Absatz 2 CSG auf Ersuchen öffentliche Stellen des Landes zu unterstützen. Die Polizei, Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz sollen bei der Wahrnehmung ihrer gesetzlichen Aufgaben technisch unterstützt werden. Schließlich können auch sonstige Stellen auf Ersuchen unterstützt werden.
In § 4 CSG wird die zentrale Aufgabe als Koordinierungs- und Meldestelle konkretisiert.

Nach Teil 2 des CSG verfügt die Cybersicherheitsagentur zur umfassenden Förderung der Cybersicherheit über weitreichende Befugnisse: Sie kann zur Abwehr von Gefahren für die Cybersicherheit gegenüber öffentlichen Stellen des Landes und an das Landesverwaltungsnetz angeschlossenen Stellen nach § 5 CSG Anordnungen treffen, Maßnahmen ergreifen und Daten verarbeiten. Sie kann die Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen auf Ersuchen der betroffenen Stelle nach § 6 CSG wiederherstellen. Die Unterstützung können öffentliche Stellen des Landes und der Kommunen sowie in begründeten Einzelfällen auch sonstige Stellen mit wichtiger Bedeutung für das öffentliche Gemeinwesen erhalten.

Die Cybersicherheitsagentur kann nach § 8 CSG die Öffentlichkeit oder die betroffenen Kreise vor Gefahren für die Cybersicherheit auch mit Angabe der Namen der herstellenden oder inverkehrbringenden Personen warnen, Empfehlungen aussprechen und Hinweise geben.

Ergänzende Regelungen erhält das CSG in Teil 2 zum Datenschutz und in Teil 3 zum Erlass von Rechtsverordnungen und Verwaltungsvorschriften durch das Innenministerium sowie zu Berichtspflichten der Cybersicherheitsagentur gegenüber dem Innenministerium und zur möglichen Einschränkung des Telekommunikationsgrundrechtes.

Mit diesem Gesetz werden auch die notwendigen Anpassungen weiterer Gesetze vorgenommen, wenngleich die bisherigen Strukturen für die Informationssicherheit weitestgehend in der bisherigen Form bestehen bleiben. Insbesondere sind auch zukünftig beizubehalten und mit angemessenen Ressourcen auszustatten:

- eine übergeordnete Informationssicherheitsbeauftragte oder ein übergeordneter Informationssicherheitsbeauftragter für die Landesverwaltung Baden-Württemberg (Chief Information Security Officer, CISO)
- die Funktionen der sogenannten Ressorts-CISOs, Dienststellen-CISOs und Sicherheitsbeauftragten vor Ort in den Behörden sowie
- die Aufgaben des Sicherheitszentrums IT in der Finanzverwaltung Baden-Württemberg (SITiF BW).

3. Alternativen

Eine vollständige Übertragung der mit diesem Gesetz der Cybersicherheitsagentur zugewiesenen Aufgaben an private Unternehmen ist aus Sicherheitsgründen nicht opportun, für besonders sicherheitskritische Bereiche scheidet sie aus. Die Landesverwaltung würde sich zudem in technische und fachliche Abhängigkeiten begeben und eigene informationstechnische Kompetenz verlieren. Das schließt im Einzelfall die Beauftragung privater Unternehmen nicht aus.

Es wurden verschiedene Rechtsformen geprüft, sowohl privatrechtliche (zum Beispiel die GmbH), als auch rechtsfähige und nicht rechtsfähige Anstalten des öffentlichen Rechts sowie die Form einer Behörde. Als Rechtsform wurde nach eingehender Prüfung und Abwägung der Konsequenzen die Landesoberbehörde gewählt, um der wachsenden und besonderen Bedeutung der Cybersicherheit insbesondere in der Landesverwaltung und in landesweiter Zuständigkeit Rechnung zu tragen.

Eine weitere Alternative wäre die Beibehaltung der bisherigen Regelung, jedoch würde dies den Erfordernissen einer fortschreitenden Digitalisierung – insbesondere der erhöhten Gefährdungslage durch Cyberangriffe – nicht gerecht. Um das verstärkte Nutzungsverhalten der Beschäftigten sowie der Bürgerinnen und Bürger über das Internet abzusichern und um dezentrale Mehrfachstrukturen zu reduzieren, muss die Abwehr von Gefahren für die Cybersicherheit verbessert und möglichst gebündelt bei einer Cybersicherheitsagentur erfolgen.

4. Finanzielle Auswirkungen

Das Gesetz hat keine finanziellen Auswirkungen.

Der Haushaltsgesetzgeber hat beschlossen, bereits im Jahr 2020 eine zukunftsfähige Cybersicherheitsarchitektur in Baden-Württemberg aufzubauen und dafür eine Cybersicherheitsagentur zu bilden. Hierfür wurden für die Haushaltsjahre 2020 und 2021

Neustellen und Sachmittel bereitgestellt und für die Haushaltsjahre 2020 und 2021 entsprechend veranschlagt. Im Einzelplan 03 des Ministeriums für Inneres, Digitalisierung und Migration stehen im Haushaltsjahr 2020 insgesamt 4 000 000 Euro zur Verfügung, aus denen 32 neue Planstellen und weitere Sach- und Personalausgaben finanziert werden. Ab dem Haushaltsjahr 2021 stehen insgesamt 9 000 000 Euro für in Summe 83 Planstellen sowie Sach- und Personalausgaben zur Verfügung. Für die folgenden Haushaltsjahre wurde in der Mittelfristigen Finanzplanung der Ansatz entsprechend fortgeschrieben.

Der Haushaltsgesetzgeber wird darüber zu entscheiden haben, ob und in welchem Umfang es für die Kapazitäten der Cybersicherheitsagentur in den nachfolgenden Jahren einen Anpassungsbedarf gibt. Ein etwaiger – durch Kapazitätsveränderungen stufenweise entstehender – Mehr- / Minderbedarf kann zum jetzigen Zeitpunkt noch nicht beziffert werden. Grundlage dafür wird ein ergebnisoffener strukturierter Bewertungsprozess auf Basis einer Wirkungsanalyse der Cybersicherheitsagentur sein.

Die Cybersicherheitsagentur soll in einer landeseigenen Liegenschaft in Stuttgart untergebracht werden.

Mit erheblichen Einnahmen durch Gebühren ist nicht zu rechnen, weil für öffentliche Stellen nach § 10 des Landesgebührengesetzes persönliche Gebührenfreiheit gilt.

Im Übrigen sind Kosten für den Landeshaushalt nicht zu erwarten.

5. Erfüllungsaufwand

a) Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

b) Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht kein Erfüllungsaufwand.

c) Erfüllungsaufwand für die Verwaltung

Über die Einrichtung und Erhaltung der Cybersicherheitsagentur hinaus entsteht durch das Gesetz kein Aufwand für die Verwaltung, denn neuer Erfüllungsaufwand der öffentlichen Stellen des Landes setzt den späteren Erlass einer Rechtsverordnung aufgrund von Artikel 1 § 13 voraus. Diese Mehraufwendungen werden im

Rahmen der etatisierten Haushaltsmittel gedeckt; insoweit wird Finanzneutralität sichergestellt.

6. Wesentliche Ergebnisse des Nachhaltigkeitschecks

Im Ergebnis werden die fachbezogenen und fachübergreifenden Wirkungen und Nebenwirkungen des Gesetzes und deren Auswirkungen auf die ökonomischen, ökologischen und sozialen Verhältnisse als insgesamt positiv eingeschätzt.

Durch das Gesetz wird ein wesentlicher Beitrag zur Abwehr von Gefahren für die Cybersicherheit in Baden-Württemberg geleistet. Die besondere Bedeutung der Cybersicherheit ist in letzter Zeit zunehmend in den Fokus der Verwaltung, Wirtschaft, Wissenschaft, Politik und Gesellschaft gerückt. Durch die fortschreitende Vernetzung sehen sich diese Stellen immer häufiger den Gefahren durch Cyberangriffe ausgesetzt.

Die Cybersicherheitsagentur wird insbesondere als zentrale Koordinierungs- und Meldestelle umfangreiche Erkenntnisse erhalten und daraus ein Lagebild über die Cybersicherheit im Land erstellen. Durch die konsequente Bündelung aller nicht fachspezifischen Aufgaben der Cybersicherheit bei der Cybersicherheitsagentur sind Synergieeffekte zu erwarten. Diese werden helfen, auch künftig der wachsenden Bedeutung und den wachsenden Anforderungen an die Gewährleistung der Cybersicherheit Rechnung zu tragen. Durch die Synergieeffekte und die Vermeidung von hohen Folgekosten nach Cybersicherheitsangriffen wirkt sich die Cybersicherheitsagentur somit langfristig positiv auf den Zielbereich Verschuldung aus, auch wenn diese Auswirkungen nicht konkret bezifferbar sind.

Die Cybersicherheitsagentur leistet einen wichtigen Beitrag zur digitalen Transformation. Sie wehrt Gefahren für die Cybersicherheit ab, insbesondere auch durch Prozessoptimierung, Wiederherstellung von Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen, Sensibilisierung, Schulung und Beratung zur Cybersicherheit. Sie wirkt sich damit positiv auf die Zielbereiche ökologische und soziale Modernisierung der Wirtschaft sowie Verschuldung, leistungsfähige Verwaltung und Justiz aus.

Dementsprechend sind durch die Errichtung der Cybersicherheitsagentur sowie der hierdurch bedingten Folgeänderungen einige, jedoch keine erheblichen Auswirkungen auf die ökonomischen, ökologischen und sozialen Verhältnisse zu erwarten.

Die Gesetzesänderung ermöglicht es der Komm.ONE, im Falle schwerwiegender Gründe auf eine Präsenzsitzung des Verwaltungsrats zu verzichten und diesen als Videokonferenz oder auf vergleichbare Weise durchzuführen. Die Regelung kommt nur in schwerwiegenden Ausnahmesituationen zur Anwendung. Regelmäßig wird nach der derzeitigen Rechtslage zu verfahren sein. Erhebliche Auswirkungen auf ökonomische, ökologische und soziale Verhältnisse sind durch die Gesetzesänderung daher nicht zu erwarten.

7. Sonstige Kosten für Private

Keine. Das Gesetz begründet keine Pflichten, welche von Privaten zu befolgen sind. Lediglich betroffene Stellen, die die Cybersicherheitsagentur um Unterstützung ersuchen, haben nach § 6 Absatz 9 Satz 2 CSG etwaige Kosten für die Hinzuziehung qualifizierter dritter Personen zu tragen.

B. Einzelbegründung

Zu Artikel 1 – Gesetz für die Cybersicherheit in Baden-Württemberg (Cybersicherheitsgesetz – CSG)

Artikel 1 enthält das Gesetz für die Cybersicherheit in Baden-Württemberg. Das Gesetz enthält zunächst einen Teil mit allgemeinen Vorschriften. Im zweiten Teil sind die Befugnisse der Cybersicherheitsagentur einschließlich der damit zusammenhängenden speziellen Datenverarbeitungsbefugnisse geregelt. Der dritte Teil enthält allgemeine datenschutzrechtliche Regelungen. Der vierte und letzte Teil enthält Schlussvorschriften.

Zu Teil 1 – Allgemeine Vorschriften

Zu § 1 – Cybersicherheitsagentur

Zu Absatz 1

Die neue zentrale, ressortübergreifende Cybersicherheitsagentur wird als Landesoberbehörde errichtet und vom Land unterhalten. Die Behördeneigenschaft gibt die notwendige Flexibilität für etwaige Erweiterungen des Aufgabenbestands um zusätzliche hoheitliche Aufgaben im Rahmen der sich entwickelnden Gefahren im Cyberraum.

Zu Absatz 2

Stuttgart soll Sitz der Cybersicherheitsagentur sein, weil hier bereits wesentliche Teile der Informationstechnik des Landes angesiedelt sind.

Zu Absatz 3

Die Dienst- und Fachaufsicht über die Cybersicherheitsagentur liegt beim Innenministerium, weil die Cybersicherheitsagentur ausschließlich Aufgaben im Bereich der öffentlichen Sicherheit und Ordnung wahrnimmt.

Zu § 2 – Begriffsbestimmungen

§ 2 erläutert die zentralen Begriffe des Gesetzes.

Zu Absatz 1

Absatz 1 definiert den Begriff der öffentlichen Stelle. Dies umfasst nach Satz 1 die Stellen des Landes, der Gemeinden und Gemeindeverbände, deren Einbeziehung in den Anwendungsbereich des CSG keine Ausgleichspflicht nach Artikel 71 Absatz 3 der Verfassung des Landes Baden-Württemberg auslöst, sowie der sonstigen juristischen Personen des öffentlichen Rechts. Die sonstigen juristischen Personen des öffentlichen Rechts sind die Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Damit sind beispielsweise die Rechtsformen der Kommunalen Zusammenarbeit nach § 1 des Gesetzes über kommunale Zusammenarbeit (Zweckverbände, gemeinsame selbstständige Kommunalanstalten) und nach § 102 a der Gemeindeordnung (selbstständige Kommunalanstalt), die Evaluationsagentur Baden-Württemberg, das Zentrum für Kunst und Medientechnologie Karlsruhe, das Landesmuseum für Technik und Arbeit Mannheim (Technoseum) und die Stiftung Akademie Schloss Solitude als Stiftungen des öffentlichen Rechts einbezogen. Dies gilt ebenso für die weiteren Körperschaften und Anstalten des öffentlichen Rechts wie beispielsweise die berufsständischen Kammern, die Landesanstalt für Kommunikation oder die L-Bank bei ihrer behördlichen Tätigkeit. Unerheblich ist dabei, ob die Stelle öffentlich-rechtliche Verwaltungstätigkeiten vornimmt oder sie fiskalisch handelt, wie es insbesondere im Vergaberecht bei der Beschaffung von Gütern und Leistungen durch bürgerlich-rechtliche Verträge der Verwaltung vorkommt.

Der Begriff der öffentlichen Stelle wird durch Satz 2 in Anlehnung an § 2 Absatz 4 des Landesinformationsfreiheitsgesetzes auf natürliche oder juristische Personen des Privatrechts, die eine der unmittelbaren Staatsverwaltung zugehörigen Behörde bei der Wahrnehmung ihrer Aufgaben in deren Auftrag und nach deren Weisung unterstützen, erweitert. Bei diesem Adressatenkreis ist nämlich der Schutz der Informationen vor Gefahren eines Cyberangriffs besonders wichtig.

Mit „öffentlich-rechtliche Verwaltungsaufgaben“ sind sämtliche öffentlichen Dienstleistungen oder Zuständigkeiten gemeint, deren Erledigung der juristischen oder natürlichen Person des Privatrechts obliegt. Die Erweiterung in Satz 2 erfolgt im Hinblick auf die Ausgliederung von Organisationseinheiten aus der Verwaltung und auf die Umwandlung in Privatrechtsform, um insbesondere kommunale Unternehmen der Daseinsvorsorge einzubeziehen. Die Zielsetzung des CSG würde angesichts der den Behörden eröffneten Möglichkeiten, bei der Erfüllung öffentlicher Aufgaben auf privatrechtliche Organisations- und Handlungsformen zurückzugreifen, verfehlt, wenn sich der Anwendungsbereich des Gesetzes nicht auch auf diese Personen des Privatrechts erstreckte.

Die allgemeine ordnungsrechtliche Überwachung, der alle Stellen unterliegen, reicht für die Annahme einer Kontrolle in diesem Sinne nicht aus. Satz 3 zählt die Tatbestandsmerkmale auf, aus denen sich eine solche Kontrolle im Einzelnen ergibt.

Zu Absatz 2

In Absatz 1 wird der Begriff der öffentlichen Stellen bewusst sehr weit umschrieben, damit die Cybersicherheitsagentur in einer vernetzen Welt umfassend Gefahren für die Cybersicherheit abwehren kann. Nachfolgend werden diesen Stellen neben der Unterstützung aber auch Pflichten auferlegt (z. B. Informations- und Duldungspflichten). Würden diese Pflichten uneingeschränkt gegenüber den in Absatz 2 genannten Stellen gelten, würden Wertungswidersprüche zu verfassungsrechtlichen Vorgaben (insbesondere Gewaltenteilung) oder gesetzlichen Regelungen entstehen. Dementsprechend gelten gegenüber diesen Stellen die Pflichten nach dem CSG nicht, soweit dies im Widerspruch zu der verfassungsrechtlichen Stellung oder anderen gesetzlichen Regelungen für diese Stellen stünde. Maßnahmen bei diesen Stellen dürfen nur im Einvernehmen mit diesen durchgeführt werden.

Zu Satz 1

Nummer 1 erfasst den Landtag vor allem im Bereich der Wahrnehmung parlamentarischer Angelegenheiten (insbesondere Gesetzgebung, Kontrolle der Landesregierung, Wahlprüfung, Wahrung der Rechte des Landtags und seiner Mitglieder – z. B. in Immunitätsangelegenheiten, bei Petitionen und bei Dienstleistungen zur Unterstützung der Mandatsausübung –, parlamentarische Kontakte zu in- und ausländischen sowie supranationalen Stellen und zu Akteuren der Zivilgesellschaft). Demgegenüber unterliegt der Landtag bei der Wahrnehmung öffentlich-rechtlicher Verwaltungsaufgaben – soweit von parlamentarischen

Angelegenheiten abtrennbar – den Verpflichtungen nach diesem Gesetz. Die Verwaltungsaufgaben beschränken sich auf wenige Bereiche (z. B. Entschädigung nach dem Abgeordnetengesetz, Leistungen an Fraktionen nach dem Fraktionsgesetz).

Nummer 2 erfasst den Rechnungshof, soweit er im Rahmen seiner verfassungsrechtlich garantierten Unabhängigkeit (Artikel 83 Absatz 2 Satz 2 der Verfassung des Landes Baden-Württemberg) tätig wird.

Nummer 3 erfasst die Tätigkeit der oder des Landesbeauftragten für Datenschutz, soweit ihre bzw. seine Unabhängigkeit durch die 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 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung oder sonstige Rechtsnormen garantiert ist.

Nummer 4 erfasst die Gerichte in Bezug auf die in den Verfahrensgesetzen vorausgesetzte unabhängige Aufgabenerledigung. Dementsprechendes gilt für die Staatsanwaltschaften, um ihrer besonderen Rolle und ihrer Verpflichtung auf das Legalitätsprinzip Rechnung zu tragen (vergleiche dazu § 1 Absatz 3 des Errichtungsgesetzes BITBW).

Nummer 5 berücksichtigt den Sonderstatus der Steuerverwaltung nach Artikel 108 des Grundgesetzes.

Nummer 6 berücksichtigt, dass das Statistikgeheimnis nach § 16 des Bundesstatistikgesetzes oder § 14 des Landesstatistikgesetzes besondere Vorgaben enthält.

Nummer 7 erfasst die Hochschulen, soweit deren verfassungsrechtliche Unabhängigkeit reicht.

Nummer 8 enthält einen Auffangtatbestand zur Erhaltung der Einheit der Rechtsordnung, nachdem in Nummer 1 bis 7 nur die wichtigsten Beispiele aufgezählt worden sind. Verfassungsrechtlich eingeräumte Unabhängigkeit besteht beispielsweise auch beim Südwestrundfunk.

Zu Satz 2

Satz 2 berücksichtigt, dass eine Kooperation zwischen der Cybersicherheitsagentur und den Stellen mit Sonderstatus jeweils an deren konkrete Bedürfnisse anzupassen ist. Die Kooperation soll durch eine gesonderte Vereinbarung regelt werden.

Zu Absatz 3

Absatz 3 nimmt die Beliehenen von den Regelungen aus, die ausschließlich für öffentliche Stellen des Landes gelten. Sie werden wie die sonstigen öffentlichen Stellen behandelt, um der besonderen Situation von Beliehenen gerecht zu werden.

Im Übrigen ergibt sich die Zuordnung der öffentlichen Stellen zum Land aus den allgemeinen Regelungen. So sind etwa die Landratsämter als untere Verwaltungsbehörden nach § 1 Absatz 3 Satz 2 der Landkreisordnung für Baden-Württemberg staatliche Behörden und somit öffentliche Stellen des Landes.

Zu Absatz 4

Der Begriff der Informationstechnik wird von Absatz 4 allgemein gefasst und beinhaltet alle technischen Ausgestaltungen und denkbaren künftigen Entwicklungen auf dem Gebiet der Informationstechnik. Unter „alle technischen Systeme“ fallen auch Datenverarbeitungs(DV)-technische Verfahren, d.h. Hard- und Software. Im Gegensatz etwa zum Landesdatenschutzgesetz, das sich nur auf personenbezogene Daten bezieht, ist jede Art von Informationen als sinnvolle Einheit von Daten unabhängig von einem Personenbezug erfasst. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen. Die Übertragung kann unabhängig von einer DV-technischen Verarbeitung erfolgen.

Zu Absatz 5

Mit Sicherheit in der Informationstechnik ist kein absoluter, sondern lediglich ein relativer Sicherheitsbegriff vorgegeben. Aspekte der Sicherheit in der Informationstechnik sind insbesondere alle technischen Maßnahmen zum Schutz von Computersystemen, physischen Systemen, KI-Systemen und Robotern vor Angriffen, welche die Beschädigung der Hard- oder Software oder der von ihnen verarbeiten Daten oder Unterbrechungen oder Missbrauch der angebotenen Dienste und Funktionen zum Gegenstand haben.

Welche Sicherheit im Einzelfall erreicht sein muss, um von „Sicherheit in der Informationstechnik“ ausgehen zu können, hängt von den jeweiligen Sicherheitserfordernissen ab. Daher ist in der Definition von der „Einhaltung bestimmter Sicherheitsstandards“ die Rede, die durch Rechtsverordnung nach § 13 konkretisiert werden. Die „Vertraulichkeit von Informationen“ erfordert Sicherheitsvorkehrungen, um einen unbefugten Informationsgewinn über

die Informationstechnik und einen ungewollten Abfluss der mit ihr verarbeiteten oder übertragenen Informationen zu verhindern. Die „Integrität von Informationen“ erfordert Sicherheitsvorkehrungen, um deren Inhalt und Form vor unzulässigem Verändern zu schützen. Die „Verfügbarkeit von Informationen“ erfordert Sicherheitsvorkehrungen, um die Informationen in der vorgesehenen Weise verarbeiten oder übertragen und damit nutzen zu können. Die Sicherheit umfasst sowohl den technischen Sicherheitsstandard (z. B. automatische Verschlüsselung gespeicherter oder zu übertragender Informationen) als auch – ergänzend oder alternativ – Sicherheitsvorkehrungen bei Anwendung der Informationstechnik (z. B. baulicher oder organisatorischer Art). Es ist Aufgabe der jeweiligen Dienststelle, die Sicherheitstechnik durch erforderliche Umfeldmaßnahmen zu ergänzen.

Zu Absatz 6

Der Begriff „Kommunikationstechnik des Landes“ umfasst grundsätzlich alle informationstechnischen Systeme und deren Bestandteile, soweit sie durch das Land oder im Auftrag des Landes für dieses betrieben werden und der Kommunikation oder dem Datenaustausch dienen. Damit sind nicht an das Landesverwaltungsnetz angeschlossene Geräte, bei denen Sicherheitslücken in der Regel keine Auswirkungen auf die Sicherheit der übrigen Informationstechnik haben, ausgenommen. Nicht erfasst ist Kommunikationstechnik, die von dritten Personen für die Allgemeinheit angeboten wird und auch von öffentlichen Stellen genutzt wird (z. B. öffentliche Telekommunikationsnetze). Die Kommunikationstechnik der Stellen im Sinne des Absatz 2, des Landesamts für Verfassungsschutz, des Polizeivollzugsdienstes und der Strafverfolgungsbehörden ist, soweit sie unter deren eigener Fachaufsicht oder unter der Fachaufsicht einer ihr übergeordneten Behörde steht oder in eigener oder länderübergreifender Zuständigkeit betrieben wird, nicht Gegenstand dieses Gesetzes. Ausgenommen sind damit auch der BOS-Digitalfunk und dessen Kooperationsprodukte. In der Praxis besteht hier die Möglichkeit, z. B. für die Kommunikation der Richterinnen und Richter einen „Bypass-Anschluss“ einzurichten, der unter Umgehung der innerhalb des Verwaltungsnetzes notwendigen Sicherheitsvorkehrungen einen unmittelbaren Anschluss an das Internet oder andere öffentliche Telekommunikationsnetze ermöglicht.

Zu Absatz 7

Mit den Schnittstellen der Kommunikationstechnik des Landes sind die Übergänge beschrieben, an denen aus Gründen der Cybersicherheit eine Auswertung von Daten notwendig ist bzw. sein kann. Davon erfasst sind Übergänge zwischen den übergreifenden Kommunikationsnetzen der Landesverwaltung inklusive der Übergänge zwischen virtuellen Netzen oder zwischen unterschiedlichen Schutzzonen innerhalb eines Netzes sowie zwischen einzelnen internen Verwaltungsnetzen oder den Netzen einer Gruppe von öffentli-

chen sowie dem Internet und anderen nicht der Landesverwaltung zuzurechnenden Netzen. Ausgenommen hiervon ist ein Zugriff auf die Protokolldaten und Kommunikationsinhalte, die an den Komponenten der Netzwerkübergänge der in Absatz 2 genannten Stellen, des Landesamts für Verfassungsschutz, des Polizeivollzugsdienstes oder der Strafverfolgungsbehörden erzeugt bzw. gespeichert werden, soweit diese unter deren eigener Fachaufsicht oder unter der Fachaufsicht einer ihr übergeordneten Behörde stehen oder in eigener oder länderübergreifender Zuständigkeit betrieben werden. Ausgenommen sind damit auch die Netzübergänge des BOS-Digitalfunks und dessen Kooperationsprodukte.

Zu Absatz 8

Das Landesverwaltungsnetz im Sinne dieses Gesetzes ist eine Kommunikationstechnik im Sinne des Absatz 6, die eine gesicherte Verbindung zwischen den lokalen Netzen der damit verbundenen Stellen sowie zu Netzen anderer Verwaltungen ermöglicht und durch das Land oder im Auftrag des Landes betrieben wird. Konzeption und ressortübergreifende Verwaltung des Landesverwaltungsnetzes ist Aufgabe der BITBW nach Nr. 4.1.1 der Verwaltungsvorschrift des Innenministeriums über die Organisation und den Betrieb der Landesoberbehörde IT Baden-Württemberg (VwV BITBW) vom 27. Juli 2015 – Az.: 5-0272.1/2-1 – (GABl. 2015, S. 510).

Zu Absatz 9

Der Begriff der Informationssicherheit umfasst alle Maßnahmen zum Schutz von Informationen, soweit ein Bezug zur Informationstechnik besteht. Informationssicherheit ist besonders wichtig, weil sämtliche Aufgabenbereiche der Verwaltung auf informationsverarbeitenden Geschäftsprozessen basieren. Der Schutz dieser Geschäftsprozesse gegen die Bedrohungen der drei Schutzziele der Informationssicherheit – Vertraulichkeit, Integrität, Verfügbarkeit – ist entscheidend für die ordnungsgemäße Aufgabenerfüllung. Informationssicherheit ist damit die Planung, Umsetzung, Überprüfung und Aufrechterhaltung eines angemessenen Sicherheitsniveaus für die zu schützenden Geschäftsprozesse einschließlich der dabei verarbeiteten Informationen und hierfür erforderlichen Ressourcen unter Berücksichtigung von Wirtschaftlichkeits- und Machbarkeitsaspekten.

Der Begriff der Informationen ist dabei nicht auf digitale Daten beschränkt und erfasst im Unterschied zur Sicherheit in der Informationstechnik auch Informationen, die in Papierform vorliegen oder von Mensch zu Mensch mündlich weitergegeben werden. Umfasst sind Maßnahmen, welche die Vertraulichkeit sicherstellen, indem nur autorisierte Personen Zugriff auf bestimmte Informationen erhalten. Umfasst sind zudem Maßnahmen zum Schutz der Integrität der Informationen, indem sichergestellt wird, dass diese Informationen

nicht unbemerkt verändert werden. Auch sind Maßnahmen zur Sicherstellung der Verfügbarkeit von Informationen erfasst, welche den Zugriff auf Informationen in der zugesicherten Art und Weise ermöglichen und Systemausfälle verhindern sollen.

Zu Absatz 10

Der Cyberraum umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.

Zu Absatz 11

Der Begriff der Cybersicherheit umfasst alle Aspekte der Sicherheit in der Informationstechnik im Sinne des Absatzes 5 und den Schutz gesellschaftlich relevanter Prozesse im Cyberraum. Häufig wird bei der Betrachtung von Cybersicherheit ein spezieller Fokus auf Angriffe aus dem Cyberraum gelegt.

Zu Absatz 12 und 13

Gefahren für die Cybersicherheit gehen insbesondere von Schadprogrammen sowie von Sicherheitslücken in informationstechnischen Systemen aus, die in Absatz 12 und 13 definiert werden.

Die Definition von Schadprogrammen in Absatz 12 entspricht im Wesentlichen der in der Informationstechnik üblichen Terminologie. Maßgeblich ist, dass die Programme dem Zweck dienen, unbefugt unerwünschte Funktionen auszuführen. Nicht erfasst sind damit unbeabsichtigte Sicherheitslücken in normalen Programmen. Schadprogramme können typischerweise Schäden verursachen, dies ist aber keine zwingende Voraussetzung. Moderne Schadprogramme zeichnen sich gerade dadurch aus, dass sie möglichst unauffällig und klein sind. Schadfunktionen sind zunächst nicht enthalten, können aber ggf. nachgeladen werden. Auch der Versand von Spam, also die massenhafte Versendung unerwünschter E-Mails, oder sogenannte DoS-Angriffe (Denial of Service, Massenanfragen, insbesondere um Server durch Überlastung lahmzulegen) sind informationstechnische Routinen, die geeignet sind, unbefugt informationstechnische Prozesse zu beeinflussen.

Sicherheitslücken sind nach Absatz 13 hingegen unerwünschte Eigenschaften von informationstechnischen Systemen, insbesondere Computerprogrammen, die es dritten Personen erlauben, gegen den Willen der berechtigten Person dessen Informationstechnik zu beeinflussen. Eine Beeinflussung muss nicht zwingend darin bestehen, dass sich die angreifende Person Zugang zum System verschafft und dieses dann manipulieren kann. Es

genügt auch, dass die Funktionsweise in sonstiger Weise beeinträchtigt werden kann, z. B. durch ein ungewolltes Abschalten. Der Begriff ist notwendigerweise weit gefasst, da Sicherheitslücken in den unterschiedlichsten Zusammenhängen, oftmals abhängig von der Konfiguration oder Einsatzumgebung entstehen können.

Zu Absatz 14

Störungen, Fehlfunktionen von und Angriffe auf IT-Systeme können technisch oft durch eine Analyse der Protokolldaten erkannt werden. Protokolldaten sind in erster Linie die Steuerdaten, die bei jedem Datenpaket mit übertragen werden, um die Kommunikation zwischen sendender und empfangender Stelle technisch zu gewährleisten. Hinzu treten die Daten, die zwar nicht mitübertragen aber im Rahmen der Protokollierung von den Servern im Übertragungsprotokoll miterfasst werden, insbesondere Datum und Uhrzeit des Protokolleintrags und ggf. Absende- und Weiterleitungskennungen. Von besonderer Relevanz für die Erkennung und Abwehr von Cyberangriffen sind die Kopfdaten (sogenannte Header) der gängigen Kommunikationsprotokolle (IP, ICMP, TCP, UDP, DNS, HTTP und SMTP). Sofern die Datenübertragung zugleich einen Telekommunikationsvorgang darstellt (z. B. das Senden einer E-Mail), sind die Protokolldaten zugleich Verkehrsdaten im Sinne des Telekommunikationsgesetzes. Entsprechendes gilt hinsichtlich der Protokolldaten, die bei der Nutzung von Telemedien anfallen. Die eigentlichen Kommunikationsinhalte sind nicht Bestandteil der Protokolldaten.

Zu § 3 – Aufgaben

§ 3 zählt die gesetzlichen Aufgaben der Cybersicherheitsagentur auf, während die wichtigste Aufgabe – Zentrale Koordinierungs- und Meldestelle – in § 4 konkretisiert wird. Die Aufgabennormen des § 3 selbst enthalten keine Eingriffsbefugnisse der Cybersicherheitsagentur, vielmehr richtet sich der konkrete Umfang der Aufgabenwahrnehmung – soweit die Maßnahmen dem Gesetzesvorbehalt unterliegen – nach den Befugnisnormen des zweiten Teils.

Durch die Aufgabenfestlegung für die Cybersicherheitsagentur werden andere Stellen grundsätzlich nicht gehindert, im Rahmen ihrer Zuständigkeiten vergleichbare Aufgaben wahrzunehmen. Gleichwohl sind ineffiziente Parallelstrukturen auszuschließen. Die Feinabstimmung des Zusammenspiels der verschiedenen Beteiligten erfolgt durch eine Rechtsverordnung nach § 13 Nummer 5.

Zu Absatz 1

Zu Satz 1

Satz 1 legt umfassend fest, dass die Cybersicherheitsagentur die in § 2 Absatz 11 definierte Cybersicherheit fördert. Darunter ist jede Maßnahme mit dem Ziel der Erhöhung des Cybersicherheitsniveaus zu verstehen. Entsprechendes gilt für die mit der Cybersicherheit zusammenhängenden Aspekte der Informationssicherheit im Sinne des § 2 Absatz 9.

Zu Satz 2

Satz 2 konkretisiert die Generalklausel des Satzes 1 durch Aufzählung der Aufgabenbereiche. Dabei dienen die Wörter „wichtige im öffentlichen Interesse liegende Aufgaben“ lediglich der Klarstellung, dass die Aufgaben der Cybersicherheitsagentur wichtige im öffentlichen Interesse liegende Aufgaben darstellen (vgl. Artikel 6 Buchstabe e). Dies steht im Einklang mit dem Erwägungsgrund 49 der Verordnung (EU) 2016/679. Danach stellt die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams – CERT, beziehungsweise Computer Security Incident Response Teams – CSIRT), elektronischen Kommunikationsnetze und -dienste sowie Sicherheitstechnologien und -diensten in dem Maße ein berechtigtes Interesse der jeweiligen verantwortlichen Person dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Vertraulichkeit, Integrität und Verfügbarkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den unbefugten Zugang zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern durch sogenannte DoS-Angriffe und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren. Wegen der zunehmenden Vernetzung (Industrie 4.0, Internet-of-Things,…) und der damit einhergehenden vielfältigen Bedrohungen im Cyberraum, wie beispielsweise dem Betreiben von Botnetzen, dem unbefugten Zugang zu elektronischen Kommunikationsnetzwerken, der Weiterverbreitung von schädlichen Programmcodes oder Angriffen in Form der gezielten Überlastung von Servern durch sogenannte DoS-Angriffe, und des großen Schadenspotenzials dieser Bedrohungen, stellen die Aufgaben der Cybersicherheitsagentur wichtige im öffentlichen Interesse liegenden Aufgaben dar. Die Bedeutung der Sicherheit der Informationstechnik hat sich auch in Deutschland bereits mehrfach gezeigt, wie zum Beispiel beim Angriff von Botnetzen bestehend aus einer Vielzahl von „IoT“- Geräten („Internet-of-Things“), dem Ausfall

zahlreicher Router der Telekom oder dem Befall mehrerer Krankenhäuser mit Ransomware. Neben der unmittelbaren Gefahrenabwehr sind etwa auch das Sammeln, Auswerten und Untersuchen von Informationen über Sicherheitsrisiken oder -vorkehrungen und die gegenseitige Information, Beratung und Warnung von Staat, Wirtschaft oder Gesellschaft wesentliche Bestandteile des Schutzes der Cybersicherheitstechnik. Nur durch die Gesamtheit der Aufgaben der Cybersicherheitsagentur kann ein umfassender Schutz erreicht werden.

Zu Nummer 1

Grundsatzaufgabe der Cybersicherheitsagentur ist die Abwehr von Gefahren für die in § 2 Absatz 11 definierte Cybersicherheit. Damit ist der Cybersicherheitsagentur insbesondere die Aufgabe zugewiesen, die aktuellen und potenziellen Sicherheitsrisiken bei Anwendung der Informationstechnik allgemein zu untersuchen. Dies ist auch deshalb erforderlich, weil bei den herstellenden und anwendenden Personen von Informationstechnik bisher vor allem die allgemeinen Leistungsmerkmale im Vordergrund stehen. Zugleich erhält das Land mit der neuen Cybersicherheitsagentur eine kompetente Stelle, auf deren Sachverstand es sich zum Beispiel bei Gesetzesvorhaben stützen kann. Die Ergebnisse der Untersuchungen der Cybersicherheitsagentur sollen vor allem Eingang finden in die Entwicklung von Sicherheitsvorkehrungen, aber etwa auch in die Entwicklung von Prüfwerkzeugen sowie in die allgemeine Beratung der herstellenden, vertreibenden und anwendenden Personen von Informationstechnik. Die Entwicklung von informationstechnischen Verfahren und Geräten erstreckt sich nur auf Grundmuster oder Prototypen; die industrielle Entwicklung und Serienfertigung obliegt allein der Wirtschaft. Zu entwickeln und weiterzuentwickeln sind insbesondere kryptologische und mathematische Sicherungsverfahren, Kryptogeräte und -komponenten, Authentisierungsverfahren – etwa zur „digitalen Unterschrift“ – Zugriffskontrollverfahren und Vorkehrungen zur Unterbindung der kompromittierenden Abstrahlung bei Geräten. Soweit Endprodukte mit informationstechnischen Sicherheitsvorkehrungen der Cybersicherheitsagentur kommerziell vertrieben werden dürfen, d. h. wenn ihre Verwendung nicht ausschließlich auf den (Verschlusssache-) Bereich des Landes beschränkt ist, hat die herstellende Person der Endprodukte die bei der Cybersicherheitsagentur angefallenen Entwicklungskosten aufgrund vertraglicher Vereinbarung zu erstatten. Die Cybersicherheitsagentur soll sowohl Sicherheitsvorkehrungen in informationstechnischen Systemen oder Komponenten entwickeln als auch Sicherheitsvorkehrungen bei Anwendung der Informationstechnik aufzeigen (zum Beispiel Maßnahmen baulicher oder organisatorischer Art, welche die Sicherheitsvorkehrungen in informationstechnischen Systemen oder Komponenten ergänzen oder ersetzen). Die Aufgaben in Nummer 1 ergeben sich aus den eigenen Sicherheitsinteressen des Landes. Sie sind bereits durch die allgemeine Verwaltungskompetenz für seinen Bereich abgedeckt und bedürften keiner gesetzlichen Regelung. Da die dabei erzielten Ergebnisse im Interesse des Landes Baden-Württemberg jedoch auch

anderen sensitiven Bereichen zur Verfügung gestellt werden sollen und teilweise auch Voraussetzung für die sachgerechte Wahrnehmung der nachfolgenden Aufgaben sind, werden sie gleichwohl aufgeführt.

Ein Schwerpunkt der Cybersicherheitsagentur wird der Schutz des Landesverwaltungsnetzes in Kooperation mit der BITBW sein, das täglich tausenden von Angriffen ausgesetzt ist. Zentrale Bedeutung hat hier die Überwachung des zentralen Internetübergangs, dem größten Einfallstor für Angriffe aus dem Internet. Der Cybersicherheitsagentur stehen hierzu die Befugnisse des zweiten Teiles zur Verfügung.

Zu Nummer 2

Nummer 2 hebt hervor, dass der Schutz gesellschaftlicher Prozesse vor Angriffen im Cyberraum ein besonders wichtiger, neuer Aspekt im Rahmen der neuen Cybersicherheitsarchitektur ist. Insbesondere sollen die Bürgerinnen und Bürger vor Angriffen im Zusammenhang mit Wahlen geschützt werden.

Zu Nummer 3

Durch Nummer 3 wird der Cybersicherheitsagentur die Aufgabe zugewiesen, an der Entwicklung und Setzung von Standards für die Cybersicherheit mitzuwirken und die Einhaltung der verbindlichen Standards zu überprüfen. Die Sicherheit des Landesverwaltungsnetzes hängt sowohl von den innerhalb des Netzes umgesetzten Sicherheitsvorkehrungen als auch von den Sicherheitsmaßnahmen der diese Netze nutzenden Stellen ab. Sicherheitslücken bei einzelnen Stellen können dabei die Gesamtsicherheit des Landesverwaltungsnetzes und damit aller anderen angeschlossenen Stellen gefährden.

Zur Erhöhung des Sicherheitsniveaus kann die Cybersicherheitsagentur an der Entwicklung und Setzung von Mindeststandards mitwirken. Die Entwicklung von Standards für die Cybersicherheit wird durch die Koordinierungsgruppe Informationssicherheit der Landesverwaltung Baden-Württemberg (KG InfoSic) orchestriert und die Festlegung erfolgt durch Rechtsverordnung des Innenministeriums im Einvernehmen mit dem IT-Rat Baden-Württemberg gemäß § 13 Nummer 2 nach Vorberatung im Arbeitskreis Informationstechnik (AK-IT). Bei der Entwicklung und Setzung von Standards für spezielle Fachverfahren, wie beispielsweise für den Digitalfunk BOS, hat die sachnähere Stelle die Federführung und eine Beteiligung der Cybersicherheitsagentur beschränkt sich auf eine wechselseitige Information über bestehende oder geplante Sicherheitsstandards.

Vom IT-Planungsrat verbindlich beschlossene fachunabhängige und fachübergreifende IT-Sicherheitsstandards nach § 1 Absatz 1 Satz 1 Nummer 2 und § 3 des Vertrages über die

Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (GBl. 2010, S. 314, 315) sind nach § 17 des Gesetzes zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg (E-Government-Gesetz Baden-Württemberg – EGovG BW) nach Ablauf der jeweils im Beschluss des IT-Planungsrats festgelegten Frist durch die Behörden bei den von ihnen eingesetzten informationstechnischen Systemen einzuhalten.

Auf Bundesebene regelt § 8 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) die Befugnis des BSI, allgemeine technische Mindeststandards für die IT-Sicherheit zu entwickeln.

Alle Dienststellen und Einrichtungen der Landesverwaltung Baden-Württemberg setzen nach Nummer 3.1 der Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit) vom 7. April 2017 – 5-0275.0/25 – (GABl. 2017, S. 214) die Informationssicherheit nach IT-Grundschutz um. Dieser bei Inkrafttreten des Gesetzes geltende Standard gilt weiter, bis die VwV Informationssicherheit außer Kraft getreten sein wird. Neue Standards für die Cybersicherheit sollen zukünftig durch Rechtsverordnung des Innenministeriums nach § 13 Nummer 2 im Einvernehmen mit dem IT-Rat Baden-Württemberg für grundsätzlich verbindlich erklärt werden, aber für die in § 2 Absatz 2 genannten Stellen haben die Vorgaben lediglich empfehlenden Charakter.

Wichtig für ein der informationstechnischen Verwaltungsinfrastruktur angemessenes Sicherheitsniveau ist, dass die gesetzten Mindeststandards eingehalten werden. Die Cybersicherheitsagentur prüft, ob die eingesetzten informationstechnischen Systeme, Komponenten, Prozesse und IT-Sicherheitskonzepte der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen die sicherheitstechnischen Mindeststandards erfüllen. Bei Nichteinhaltung dieser Mindeststandards kommen Anordnungen nach § 5 Absatz 1 in Betracht.

Zu Nummer 4

Die Aufgaben der zentralen Koordinierungs- und Meldestelle werden in § 4 konkretisiert.

Zu Nummer 5

Die Cybersicherheitsagentur übernimmt die Aufgabe als zentrale Kontaktstelle zu § 8b Absatz 2 Nummer 4 Buchstabe c BSIG. Die vom BSI erhaltenen Informationen gibt sie an die Aufsichtsbehörden, die obersten Landesbehörden und die im Innenministerium angesiedelte Koordinierungsstelle Kritische Infrastrukturen (KoSt KRITIS) weiter. Ziel ist es, die

Meldungen zu kanalisieren und dadurch die Gesamtsicherheitslage besser zu überblicken. Auch können die Informationen für andere Behörden, die zunächst nicht unmittelbar betroffen zu sein scheinen, von Nutzen sein. Je nach Komplexität der Meldung bereitet die Cybersicherheitsagentur die Informationen des BSI für die Behörden derart auf, dass auch technische Laien die Kritikalität der Informationen beurteilen können.

In Einzelfällen kann eine unverzügliche Weitergabe notwendig sein.

Zu Nummer 6

Für die Cybersicherheit im Land kommt der Information und Beratung durch die Cybersicherheitsagentur nach Nummer 6 eine große Bedeutung zu.

Soweit die Cybersicherheitsagentur bei der Information zur Cybersicherheit in Rechte von dritten Personen eingreift, dürfen Warnungen, Empfehlungen und Hinweise nur nach Maßgabe der Befugnisnorm des § 8 erfolgen.

Die Aufgabe der Cybersicherheitsagentur, allgemein zu beraten, umfasst insbesondere das Aufzeigen von Risiken bei Anwendung der Informationstechnik sowie geeigneter Sicherheitsvorkehrungen. Die Cybersicherheitsagentur erfüllt die Aufgabe beispielsweise durch die Veröffentlichung von Informationsbroschüren und -schriften, die Durchführung von Lehrgängen, Seminaren oder Kolloquien. Die Wahrnehmung der Aufgabe setzt voraus, dass der Wissensstand der Cybersicherheitsagentur dem Stand von Wissenschaft und Technik entspricht. Sie gebietet auch eine Mitarbeit in den einschlägigen Normungsgremien (vgl. Nummer 3). Ein erheblicher Beratungsbedarf der öffentlichen Stellen besteht, um folgende gravierende Sicherheitsmängel zu beseitigen:

- das Fehlen von Risikoanalysen und Sicherheitskonzepten,
- unzureichende Vorbereitung auf Sicherheitsvorfälle: keine Erprobung des Wiederanlaufs mittels Programm- und Datenkopien in einem Ausweichrechenzentrum, keine Überprüfung der Vollständigkeit von Datenträgern im Sicherheitsarchiv,
- unzureichende Zugangs- und Ausweiskontrolle für den Zutritt zum Rechenzentrum; Umgehung von bestehenden Kontrollen,
- unzureichende organisatorische Begleitmaßnahmen hinsichtlich des Sicherheitsprogramms, das Daten, Programme und technische Einrichtungen vor unberechtigtem Zugriff schützen soll: unvollständige Erfassung der Anwendungsprogramme, keine Auswertung und keine Reaktion auf Meldungen des Sicherheitsprogramms über unberechtigte Zugriffsversuche.

Zu Nummer 7

Über die Information und Beratung nach Nummer 6 hinaus hat die Cybersicherheitsagentur auch die Aufgabe ein Kompetenzzentrum für Sensibilisierungen und Schulungen zu betreiben. Durch die frühzeitige Sensibilisierung und Schulung zu Themen der Cybersicherheit können nämlich eine Vielzahl von Personen erreicht werden, um sie besser auf den Umgang mit Gefahren für die Cybersicherheit vorzubereiten.

Zu Absatz 2

Absatz 2 staffelt die Priorität der Unterstützungsleistungen der Cybersicherheitsagentur nach den Ersuchenden: Nach Satz 5 sind öffentliche Stellen des Landes bei ihrer Abwehr von Gefahren für die Cybersicherheit zu unterstützen. Nach Satz 2 sollen die Polizei, Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz bei der Wahrnehmung ihrer gesetzlichen Aufgaben technisch unterstützt werden. Schließlich können nach Satz 1 auch sonstige Stellen auf Ersuchen unterstützt werden.

Zu Satz 1

Nach Satz 1 kann die Cybersicherheitsagentur auf Ersuchen bei der Abwehr von Gefahren für die Cybersicherheit unterstützen oder auf qualifizierte sicherheitsdienstleistende Personen verweisen. Damit wird klargestellt, dass die Cybersicherheitsagentur erst auf Ersuchen tätig wird und ihr ein Ermessen eingeräumt ist. Im Rahmen der pflichtgemäßen Ermessensausübung kann die Cybersicherheitsagentur auch auf qualifizierte sicherheitsdienstleistende Personen verweisen.

Die Aufgabe der Cybersicherheitsagentur beschränkt sich auf die reine Unterstützung. Die Verantwortlichkeit für die Sicherheit der Informationstechnik geht nicht auf die Cybersicherheitsagentur über.

Die Vorschrift ist aufgrund der schnelllebigen Entwicklung der Informationstechnologie bewusst weit gefasst, um neben der Amtshilfe nach §§ 4 ff. des Landesverwaltungsverfahrensgesetzes die Unterstützung in möglichst vielen und auch zukünftig neuen Bereichen zuzulassen.

Als Unterstützung kann die Cybersicherheitsagentur beispielsweise einzelne Hard- und Softwarekomponenten (etwa Betriebssysteme, Textverarbeitungsprogramme oder Netzwerkkomponenten) auf Sicherheitsrisiken überprüfen (dazu § 7). Damit entlastet sie die einzelnen Stellen, die bereits geprüfte Produkte nicht erneut auf Einsatztauglichkeit in ihrem Bereich untersuchen müssen. Auch entfallen unnötige Mehrfachprüfungen, da Standardprodukte an einer zentralen Stelle geprüft werden.

Im Fall eines Angriffs kann ein Eingreif- und Reaktionsteam – eventuell sogar durch Vor-Ort-Service – bei der Abwehr mit seiner Fachexpertise behilflich sein (dazu § 6).

Bei IT-Sicherheitskonzepten, wie sie beispielsweise bei einer Zertifizierung nach ISO 27001 in der Ausprägung BSI IT-Grundschutz benötigt werden, soll die Cybersicherheitsagentur etwa durch das Erstellen von Vorlagen oder die Übernahme der Projektleitung unterstützen. Eine weitere Unterstützung kann in der Erteilung von Sicherheitszertifikaten liegen. Mit Genehmigung der originär ausstellenden Personen des Sicherheitszertifikats, dass die Cybersicherheitsagentur nach Vorliegen der Voraussetzungen hierzu befugt, kann sie ein Zertifikat (beispielsweise Zertifizierung nach ISO 27001 in der Ausprägung BSI IT-Grundschutz) verleihen. Möglich ist es auch eigene Zertifikate der Cybersicherheitsagentur zu verleihen, die die Einhaltung von Sicherheitsrichtlinien oder bestimmten Standards bestätigen. Auch die Aufstellung eines eigenen Anforderungskatalogs ist denkbar.

Darüber hinaus kann die Cybersicherheitsagentur als zentrale Stelle für Cybersicherheit in der Verwaltung Verfahren und Geräte entwickeln, bereitstellen und betreiben, die öffentlichen und an das Landesverwaltungsnetz angeschlossenen Stellen zur Verfügung gestellt werden. In erster Linie wird es sich dabei um Krypto- und Sicherheitsmanagementsysteme handeln, die behördenübergreifend zum Einsatz kommen. Solche Systeme verschlüsseln u. a. die staatliche Kommunikation gegen einen Angriff. Die Cybersicherheitsagentur kann Schlüssel vergeben und Public Key Infrastructures (PKI) zur Verteilung der Schlüssel betreiben.

Zu Satz 2 bis 4

Mit Satz 2 wird der Tatsache Rechnung getragen, dass die Polizei, Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz mit der Abwehr von Gefahren für die Cybersicherheit befasst sind oder sein können, ohne immer über den speziellen technischen Sachverstand oder die erforderlichen Geräte zu verfügen. Die Cybersicherheitsagentur kann die zuständigen öffentlichen Stellen auf ihr Ersuchen mit technischer Expertise – etwa im Bereich Forensik, Kryptoanalyse oder Big Data – oder Ausrüstung unterstützen.

Es handelt sich insoweit um einen spezialgesetzlich geregelten Fall der Amtshilfe, bei dem die Cybersicherheitsagentur ihre technische Expertise und Geräte bei der Bewältigung ihrer gesetzlichen Aufgaben zur Verfügung stellt. Ergänzend finden die §§ 4 ff. des Landesverwaltungsverfahrensgesetzes Anwendung, soweit nicht durch die Sätze 3 und 4 Sonderregelungen getroffen wurden.

Zu Satz 5

Im Übrigen hat die Cybersicherheitsagentur die öffentlichen Stellen des Landes auf deren Ersuchen bei der Abwehr von Gefahren für die Cybersicherheit uneingeschränkt zu unterstützen.

Zu Absatz 3

Nach Absatz 3 bleiben die Regelungen des Errichtungsgesetzes BITBW und dort insbesondere der § 1 Absatz 5 und § 2 Absatz 1 Nummer 2 durch die Aufgabenzuweisung an die Cybersicherheitsagentur unberührt. Die Landesoberbehörde IT Baden-Württemberg (BITBW) kann für ihren Zuständigkeitsbereich, der im Errichtungsgesetz BITBW beschrieben ist, für die Verarbeitung oder Übertragung von Informationen eigene informationstechnische Sicherheitsvorkehrungen ergreifen, Systeme, Dienste, Komponenten oder Prozesse entwickeln, prüfen, bewerten und zulassen, Schlüsseldaten herstellen und Krypto- und Sicherheitsmanagementsysteme betreiben sowie eigene Maßnahmen zur Abwehr von Gefahren für ihre Informations- und Kommunikationstechnik ergreifen.

Zu § 4 – Zentrale Koordinierungs- und Meldestelle

Zu Absatz 1

Absatz 1 betont die Funktion der Cybersicherheitsagentur als zentrale Koordinierungs- und Meldestelle für Cybersicherheit in Baden-Württemberg: Die Cybersicherheitsagentur soll Informationen zu Sicherheitslücken, Schadprogrammen und Cybersicherheitsvorfällen zentral und strukturiert sammeln und auswerten sowie die Maßnahmen der verschiedenen Akteurinnen und Akteure zur Abwehr der Gefahren für die Cybersicherheit unter Berücksichtigung der etablierten Strukturen in der Gefahrenabwehr und im Krisenmanagement koordinieren.

Denn es ist erforderlich, Kommunikationsstrukturen zur Prävention und Bewältigung von Sicherheitsvorfällen vorzuhalten und sich gegenseitig zu informieren. Der Cybersicherheitsagentur kommen in diesem Zusammenhang besondere Koordinierungsaufgaben zu, die gesetzlich abgesichert und hervorgehoben werden sollen. Dabei beschäftigt sie sich nicht nur mit aktuellen Ereignissen, auch Informationen über Zukunftstechnologien in der Branche werden untersucht und erprobt. Die Erkenntnisse stellt sie den öffentlichen Stellen zur Verfügung. In Betracht kommen insbesondere kommunale Stellen, aber auch nationale oder internationale Einrichtungen wie das BSI (dazu speziell auch § 3 Absatz 1 Nummer 5), das European Cybercrime Center oder die European Union Agency for Cybersecurity (ENISA).

Schnelle Reaktionszeiten sind bei der Abwehr von Gefahren für die Cybersicherheit unabdingbar. Über aktuelle Bedrohungen hat die Cybersicherheitsagentur daher unverzüglich nach Absatz 2 Nummer 2 die betroffenen öffentlichen Stellen zu unterrichten. Damit soll sichergestellt werden, dass diese Stellen rechtzeitig Abwehrmaßnahmen gegen neue oder bevorstehende Bedrohungen ergreifen können.

Zu Absatz 2

Für die Abwehr von Gefahren für die Cybersicherheit ist es zentral, dass die Cybersicherheitsagentur nach Nummer 1 die erforderlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Cybersicherheit und der dabei beobachteten Vorgehensweise strukturiert sammelt und auswertet.

Sind Informationen für andere öffentliche Stellen von Interesse, weil diese etwa bestimmte Software einsetzen, die von neu entdeckten Sicherheitslücken betroffen ist, informiert nach Nummer 2 die Cybersicherheitsagentur diese unverzüglich. Insbesondere sind die öffentlichen Stellen über die Erkenntnisse aufgrund einer bei ihr durchgeführten Erhebung von Daten nach § 5 Absatz 2 bis 11, einer Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 6 und einer Untersuchung der Sicherheit in der Informationstechnik nach § 7 zu informieren.

Schließlich kommt der Cybersicherheitsagentur nach Nummer 3 die Aufgabe zu, die Maßnahmen der öffentlichen Stellen des Landes für die Abwehr der Gefahren für die Cybersicherheit zu koordinieren. Für die effektive und effiziente Gefahrenabwehr ist es wichtig, dass die verschiedenen Akteure koordiniert zusammenarbeiten. Eine Koordinierung durch die Cybersicherheitsagentur ist nur soweit möglich, wie dieser keine anderen gesetzlichen Vorschriften entgegenstehen. Demgemäß kann eine Koordinierung durch die Cybersicherheitsagentur insbesondere insoweit nicht in Betracht kommen, als dadurch in die gesetzlich geregelten Zuständigkeiten und Koordinierungsaufgaben des Bundesamtes für Verfassungsschutz nach § 5 Absatz 3 BVerfSchG eingegriffen würde.

Zu Absatz 3

Damit die Cybersicherheitsagentur ihre Aufgabe nach Absatz 2 Nummer 1 erfüllen und ihrer Informationspflicht nach Absatz 2 Nummer 2 nachkommen kann, müssen nach Absatz 3 die anderen öffentlichen Stellen des Landes und die unmittelbar an das Landesverwaltungsnetz angeschlossenen Stellen die Cybersicherheitsagentur unterrichten, wenn dort Erkenntnisse etwa zu neuen Schadprogrammen, neuen Angriffsmustern oder Cybersicher-

heitsvorfällen gewonnen werden. Nicht unmittelbar an das Landesverwaltungsnetz angeschlossen sind beispielsweise Gemeinden und Gemeindeverbände, die über das kommunale Netz nur mittelbar an das Landesverwaltungsnetz angeschlossen sind.

Die Einzelheiten dieses Meldeverfahrens nach Absatz 3, insbesondere hinsichtlich der Frage, welche Informationen für die Arbeit der Cybersicherheitsagentur relevant sind, werden in einer Rechtsverordnung nach § 13 Nummer 3 festgelegt. Damit die Rechtsverordnung des Innenministeriums rechtzeitig fertiggestellt werden kann und die öffentlichen Stellen des Landes und die unmittelbar an das Landesverwaltungsnetz angeschlossenen Stellen sich rechtzeitig auf die Meldepflichten einstellen können, findet die Meldepflicht nach Absatz 3 frühestens ab dem 1. Januar 2022 Anwendung. Das Instrument der Rechtsverordnung wurde hier gewählt, um flexibel genug für die technischen Fortentwicklungen zu sein. Dabei wird die Ressorthoheit gewahrt, indem mit geeigneten Regelungen die jeweiligen in den Ressorts zuständigen Stellen zwingend in den Meldeweg eingebunden werden.

Zu Absatz 4

Nach Absatz 4 sind Stellen, denen kraft Verfassung oder Gesetzes eine besondere Unabhängigkeit zukommt, von der Unterrichtungspflicht nach Absatz 3 ausgenommen, wenn eine Übermittlung im Widerspruch zu deren Unabhängigkeit stehen würde. Eine Unterrichtungspflicht besteht ebenso nicht, wenn die Informationen aufgrund von Regelungen zum Geheimschutz, Weitergabevorbehalte der Herausgeberinnen oder Herausgeber oder Vereinbarungen mit dritten Personen nicht weitergeben werden dürfen. Die Übermittlung und Weitergabe von eingestuften Informationen an die Cybersicherheitsagentur durch das Landesamt für Verfassungsschutz richtet sich nach dem Landesverfassungsschutzgesetz (LVSG). Dort bestehende Übermittlungsvorschriften können einer Übermittlung von Informationen an die Cybersicherheitsagentur entgegenstehen.

Zu Absatz 5

Die im Rahmen von § 4 übermittelten Informationen sind üblicherweise rein technischer Natur und haben keinen Personenbezug. Sollte im Einzelfall ein Personenbezug gegeben sein, stellt Absatz 5 klar, dass die Vorschriften zum Schutz personenbezogener Daten (Teil 3 dieses Gesetzes) unberührt bleiben.

Zu Teil 2 – Befugnisse

Bei der Wahrnehmung ihrer in Teil 2 geregelten Befugnisse hat die Cybersicherheitsagentur die Vorgaben des EU-Rechts (insbesondere die Datenschutz-Grundverordnung) sowie des Bundesrechts (insbesondere zum Schutz des geistigen Eigentums) zu beachten.

Zu § 5 – Abwehr von Gefahren für die Cybersicherheit

§ 5 ist die zentrale Befugnisnorm, um Gefahren für die Cybersicherheit effektiv und effizient abzuwehren. Effektive Gefahrenabwehr kann nur durch ein einheitlich hohes Schutzniveau gewährleistet werden. Das beste Cybersicherheitskonzept der einen öffentlichen Stelle ist nutzlos, wenn der Angriff an anderer Stelle durch nicht ausreichend gesicherte Kanäle ermöglicht wird. Dies gilt es mit den nach Absatz 1 gegebenen Möglichkeiten zu verhindern, die in datenschutzrechtlicher Hinsicht durch Absatz 2 bis 7 konkretisiert und durch den Teil 3 flankiert werden.

Zu Absatz 1

Zu Satz 1

Um die die öffentlichen Stellen und das Landesverwaltungsnetz gegen Cyberangriffe zu stärken, darf die Cybersicherheitsagentur nach Absatz 1 zur Gefahrenabwehr gegenüber öffentlichen Stellen des Landes und an das Landesverwaltungsnetz angeschlossenen Stellen die nötigen Anordnungen treffen oder Maßnahmen ergreifen. Nur so kann ein homogenes Schutzniveau im Landesverwaltungsnetz gegen Cyberangriffe gewährleistet werden.

Bei den zu ergreifenden Maßnahmen ist der Verhältnismäßigkeitsgrundsatz zu beachten, insbesondere ist stets das mildeste Mittel zur Erreichung des Zwecks zu wählen.

Zu Satz 2

Den Verhältnismäßigkeitsgrundsatz konkretisiert Satz 2 insoweit, als ein mindestens zweistufiges Verfahren zu wählen ist. Insbesondere können so die finanziellen, technischen und organisatorischen Folgen von Anordnungen und Maßnahmen der Cybersicherheitsbehörden besser eingeschätzt und bewertet werden. Die Dauer der Frist bemisst sich dabei nach der Dringlichkeit, dem Schweregrad des Schadenseintritts und dessen Eintrittswahrscheinlichkeit; eine Mindest- oder Höchstdauer kann somit gesetzlich nicht verbindlich vorgegeben werden.

Zu Satz 3

Die Befugnis der Cybersicherheitsagentur für Anordnungen und Maßnahmen setzt nach Satz 3 grundsätzlich das Einvernehmen mit der jeweils fachlich zuständigen obersten Landesbehörde oder im Einzelfall einen Beschluss des IT-Rates Baden-Württemberg voraus. Das Einvernehmenserfordernis berücksichtigt, dass bei der fachlich zuständigen obersten Landesbehörde spezielle Expertise für die Informationstechnik im jeweiligen Geschäftsbereich vorhanden ist. Die zweite Alternative stellt darauf ab, dass der IT-Rat Baden-Württemberg das ressortübergreifende Gremium im Bereich des E-Governments und der Informationstechnik ist.

Zu Satz 4

Ausnahmsweise kann nach Satz 4 die Cybersicherheitsagentur ohne Beteiligung der jeweils fachlich zuständigen obersten Landesbehörde oder des IT-Rates Baden-Württemberg agieren, wenn zur Gefahrenabwehr sofortiges Handeln erforderlich ist.

Zu Satz 5

In den Fällen des Satzes 4 ist nach Satz 5 eine Anordnung durch die Präsidentin oder den Präsidenten erforderlich, damit sie oder er die Verantwortung für dieses Vorgehen übernimmt.

Zu Satz 6

Die Pflicht zur Protokollierung ermöglicht eine nachträgliche Kontrolle, ob die Voraussetzung für die Entscheidung der Präsidentin oder des Präsidenten gegeben waren.

Zu Satz 7

Satz 7 räumt der betroffenen obersten Landesbehörde ein Antragsrecht bei dem IT-Rat Baden-Württemberg für die Überprüfung der Entscheidung der Präsidentin oder des Präsidenten der Cybersicherheitsagentur ein.

Zu Satz 8

Die in Absatz 1 geregelte Befugnis erstreckt sich nicht auf die Informationstechnik des Landesamts für Verfassungsschutz, des Polizeivollzugsdienstes oder der Strafverfolgungsbehörden, soweit sie in deren eigener oder länderübergreifender Zuständigkeit betrieben wird. Ausgenommen nach Satz 2 sind insbesondere der BOS-Digitalfunk und dessen Kooperationsprodukte.

Zu Absatz 2

Absatz 2 gibt der Cybersicherheitsagentur, den anderen öffentlichen Stellen des Landes sowie den an das Landesverwaltungsnetz angeschlossenen Stellen die Befugnis, zur Abwehr von Gefahren für die Kommunikationstechnik, die in Absatz 2 aufgezählten Daten zu erheben und automatisiert auszuwerten, etwa hinsichtlich des Datenvolumens oder durch das automatisierte „Absurfen“ von aus dem Landesverwaltungsnetz heraus aufgerufenen Uniform Resource Locator (URL), um sogenannte Phishingseiten zu identifizieren.

Zu Satz 1

Nach Nummer 1 kann die Cybersicherheitsagentur Protokolldaten, die beim Betrieb der Kommunikationstechnik des Landes anfallen, erheben und automatisiert auswerten, soweit dies zur Abwehr von Gefahren für die Cybersicherheit erforderlich ist. Die Erforderlichkeit stellt dabei eine Relevanzgrenze dar. Informationen – z. B. Zugriffe auf Verzeichnisdienste oder Zugriffsprotokolldaten der Polizei – die für eine effiziente Abwehr von Schadprogrammen oder anderen Angriffen nicht von Bedeutung sind, dürfen nicht erhoben und ausgewertet werden. Für den unwahrscheinlichen Fall, dass ein Zugriff durch die Cybersicherheitsagentur auf solche sensiblen Systeme unabdingbar wird und es sich hierbei um Verschlusssachen im Sinne des § 4 des Landessicherheitsüberprüfungsgesetzes handelt, sind die Beschäftigten einer Sicherheitsüberprüfung nach den Vorgaben des Landessicherheitsüberprüfungsgesetzes zu unterziehen, die Zugriffe zu protokollieren und der Bericht bzw. die Akte als Verschlusssache gemäß § 4 Absatz 2 des Landessicherheitsüberprüfungsgesetzes in Verbindung mit der VS-Anweisung zu deklarieren und zu behandeln. Auch ist eine personenbezogene Verwendung der Protokolldaten zu anderen Zwecken, insbesondere zur Erstellung von Kommunikationsprofilen oder der Verhaltens- und Leistungskontrolle von Beschäftigten, ausgeschlossen.

Bei Protokolldaten handelt es sich um sogenannte Logfiles von Servern, Firewalls, Web-Proxys etc. Diese Logfiles protokollieren sogenannte Events, also Ereignisse über Anfragen von anderen Systemen, Softwareänderungen, Fehlermeldungen etc. Sie enthalten keine Inhaltsdaten. Setzt man Protokolldaten verschiedener Systeme in Korrelation und wertet diese aus, so können Unregelmäßigkeiten und damit potenzielle Bedrohungen erkannt werden. Protokolldateien, die für die Abwehr von Gefahren interessant sind, können unter anderem sein:

- Protokolldateien von Firewall-Systemen einschließlich Erhebungszeitpunkt, IP-Adresse und Port sowie vollständigem Domänennamen von ein- und ausgehenden Verbindungen sowie die durch die Firewall durchgeführte Aktion;
- Protokolldateien von Systemen zur Erkennung und Beseitigung von Schadsoftware einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen

des betroffenen Systems, ausgegebener Meldung sowie Informationen über die Schadsoftware und die als Schadprogramm erkannten Daten;

- Protokolldateien von Systemen zur Erkennung von unerwünschten E-Mails einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen von ein- und ausgehenden Verbindungen, E-Mail-Adressen einer Nachricht, deren Größe und eindeutiger Identifikationsnummer sowie Fehler- und sonstige Statusmeldungen und die als Schadprogramm erkannten Daten;
- Protokolldateien von Datenbankservern einschließlich Erhebungszeitpunkt, Anmeldename, IP-Adresse und vollständigem Domänennamen von Verbindungen und die Identifikationsnummer der ausgegebenen Meldung und deren Klartext;
- Protokolldateien von Web- und Proxyservern einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen von ein- und ausgehenden Verbindungen sowie dem einheitlichen Ressourcenzeiger (URL) und Kopfdaten (sogenannte Header) der gängigen Kommunikationsprotokolle (etwa IP, ICMP, TCP, UDP, DNS, HTTP und SMTP) und
- Protokolldateien der Betriebssoftware von Computersystemen einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen des betroffenen Computersystems, Namen des Programms oder Systemdiensts sowie dessen Typ, die Identifikationsnummer der ausgegebenen Meldung und deren Klartext.

Nach Nummer 2 kann die Cybersicherheitsagentur die an den Schnittstellen der Kommunikationstechnik des Landes anfallenden Daten erheben und automatisiert auswerten. Die Begrenzung auf beim Betrieb der Kommunikationstechnik des Landes anfallende Protokolldaten stellt klar, dass keine Datenerhebung bei dritten Personen von der Regelung erfasst wird. Die behördeninterne Kommunikation ist ebenfalls nicht erfasst. Die Vorschrift erlaubt lediglich eine sofortige Analyse des in das Landesverwaltungsnetz eindringenden Datenverkehrs. Damit sollen Schadprogramme bereits am Übergang vom Internet zum Landesverwaltungsnetz erkannt und abgewehrt werden. Davon umfasst ist auch der Zugriff auf (technische) Telekommunikationsinhalte. Nur so können gefährliche Dateianhänge oder Links zu Internetseiten, die ihrerseits Schadsoftware einzuschleusen versuchen, analysiert und abgewehrt werden. Dies ermöglicht auch den Einsatz von Virenscannern und ähnlichen Detektionstools, der bislang nur mit Einwilligung der betroffenen Personen zulässig ist. Die automatisierte Auswertung gestattet nicht die Speicherung der Inhalte über den für die technische Abwicklung des Kommunikations- und Erkennungsvorgangs ohnehin notwendigen Umfang hinaus.

Zu Satz 2

Satz 2 räumt auch den anderen öffentlichen Stellen des Landes und den an das Landesverwaltungsnetz angeschlossenen Stellen innerhalb ihres jeweiligen Zuständigkeitsbereichs die gleichen Befugnisse entsprechend Satz 1 wie der Cybersicherheitsagentur ein. Dies ist erforderlich, denn nur wenn diese Stellen entsprechende Daten rechtmäßig erhoben haben, kann die Cybersicherheitsagentur Daten bei den betroffenen Stellen – etwa durch Überlassung einer Kopie der gespeicherten Daten – rechtmäßig erheben und auswerten.

Zu Satz 3

Satz 3 verlangt, dass die nach Satz 1 und 2 erhobenen Daten sofort nach der Auswertung spurenlos zu löschen sind, so dass ein weitergehender Zugriff auf die Daten nicht mehr möglich ist (vgl. BVerfG vom 11. März 2008, 1 BvR 2074/05, 1 BvR 1254/07), soweit nicht eine Weiterverarbeitung nach den nachfolgenden Absätzen ausnahmsweise zulässig ist, insbesondere weil sich ein konkreter Verdacht ergibt.

Zu Satz 4

Satz 4 verpflichtet die öffentlichen Stellen des Landes zur Mitwirkung, denn nur mit deren Mithilfe kann die Cybersicherheitsagentur ihren Auftrag zur zentralen Abwehr und Detektion von Angriffen auf die informationstechnischen Systeme des Landes erfüllen, wenn das zentrale Monitoring des Landesverwaltungsnetzes ausgebaut wird, wofür auch die Protokolldaten aus den internen Systemen der öffentlichen Stellen des Landes benötigt werden.

Zu Absatz 3

Schadprogramme können regelmäßig erst mit einem zeitlichen Verzug von mehreren Tagen oder Wochen (abhängig von deren Verbreitung) detektiert werden. Wenn ein neues Schadprogramm gefunden wurde, besteht daher die Notwendigkeit, auch rückwirkend zu untersuchen, ob dieses bereits zuvor innerhalb der Landesverwaltung verbreitet wurde, um hierdurch verursachte Schäden zu erkennen, zu vermeiden oder zu begrenzen.

Einzig zu diesem Zweck dürfen nach Absatz 3 die insoweit relevanten Protokolldaten im Sinne des Absatzes 2 Satz 1 Nummer 1 und Satz 2 auch länger gespeichert und im Falle eines bei Abgleich der Daten bestätigten Fundes oder anderer Hinweise auf neue Schadprogramme automatisiert auf weitere Verdachtsfälle ausgewertet werden.

Die Dauer der Speicherung ist abhängig von der technischen Entwicklung und richtet sich danach, innerhalb welchen Zeitraums eine Rückschau auf bereits stattgefundene Angriffe

verhältnismäßig ist. Sobald die Cybersicherheitsagentur einen neuartigen Angriff unter Verwendung von Schadprogrammen entdeckt, werden die Protokolldaten nach Bezügen zu diesem neuen Angriff untersucht. Dies führt regelmäßig zur Entdeckung von ähnlichen Angriffen, die bereits stattgefunden haben. Aufgrund dieser Erkenntnisse werden die betroffenen öffentlichen Stellen informiert, um die notwendigen Maßnahmen zur Verhinderung von Schäden und zur Abwehr weiterer Angriffe treffen zu können. Die Speicherdauer von maximal drei Monaten ist auch angemessen: Nach den bisherigen Erfahrungen wird der größte Teil (ca. 80 Prozent) der Angriffe innerhalb der ersten drei Monate entdeckt, womit lediglich etwa 20 Prozent der Angriffe noch entdeckt würden, wenn die Daten länger als drei Monate gespeichert werden könnten.

Unter Berücksichtigung des Schutzbedarfs der öffentlichen Stellen wird deshalb die maximale Speicherdauer der zur Erkennung von Schadprogrammen relevanten Protokolldaten auf drei Monate festgelegt. Nach Ablauf dieser Zeitspanne sind die Protokolldaten spurenlos zu löschen.

Im Trefferfall erfolgt die Weiterverarbeitung der trefferrelevanten Daten nach Absatz 5.

Die Vorgaben des Absatzes 3 sind auch durch organisatorische und technische Maßnahmen sicherzustellen.

Zu Absatz 4

Die Verarbeitungsbeschränkungen nach Absatz 2 und 3 gelten nach Absatz 4 nicht für Daten, die weder personenbezogene noch dem Fernmeldegeheimnis unterfallende Daten enthalten (z. B. Angaben zur Serverlast). Diese Daten genießen nämlich keinen Grundrechtsschutz.

Zu Absatz 5

Wenn, insbesondere aufgrund der Maßnahmen nach Absatz 2, ein konkreter Verdacht auf das Vorliegen eines Schadprogramms besteht, sind nach Absatz 5 weitergehende Maßnahmen möglich. In einem ersten Schritt sind die Untersuchungen zulässig, die nötig sind, um den konkreten Verdacht zu bestätigen oder zu widerlegen. Im Falle eines Fehlalarms ist die betroffene öffentliche Stelle beziehungsweise sind deren Beschäftigte, soweit feststellbar, hiervon zu unterrichten.

Die Daten sind dann, gegebenenfalls nach Weiterleitung an den ursprünglichen Adressaten, wieder zu löschen. Im Falle der Bestätigung können die Daten zum Zweck der Abwehr des Schadprogramms oder ähnlicher Schadprogramme, etwa durch Untersuchung der

Funktionsweise des Schadprogramms oder durch Aufnahme der Virensignatur verwendet werden. Dabei sind personenbezogene Daten nach dem Grundsatz der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 soweit möglich zu anonymisieren oder zu pseudonymisieren.

Außerdem kann ein durch das Schadprogramm ausgelöster ungewollter Datenstrom detektiert und ggf. unterbunden werden. Auch hiervon ist die betroffene Person oder Stelle zu unterrichten. Die Unterrichtung der absendenden Person des Schadprogramms dürfte im Regelfall nicht möglich sein, weil diese Person bereits technisch, etwa aufgrund von gefälschten Adressen, nicht ermittelbar ist. Die Unterrichtung unterbleibt ferner, wenn dieser Unterrichtung schutzwürdige Belange von dritten Personen entgegenstehen. Werden die Daten aufgrund der Befugnisse nach Absatz 6 oder 7 für ein Strafverfahren oder für Zwecke der Verfassungsschutzbehörden weiterverwendet, erfolgt die Benachrichtigung durch die insoweit zuständigen Behörden nach Maßgabe der für diese geltenden Vorschriften der Strafprozessordnung, des Polizeigesetzes oder des LVSG.

Dass die Ermessensausübung zur nicht automatisierten Verwendung personenbezogener Daten nach Satz 3 nur durch Bedienstete mit Befähigung zum Richteramt erfolgen darf, bietet eine interne Kontrolle.

Zu Absatz 6

Angriffe auf die Informationstechnik des Landes mittels Schadprogrammen stellen zugleich auch Straftaten oder eine Gefahr für die öffentliche Sicherheit dar. Absatz 6 Satz 1 verpflichtet die Cybersicherheitsagentur daher, die Daten unverzüglich an die insoweit zuständigen Behörden zu übermitteln, sofern dies zur Verfolgung einer der abschließend aufgezählten Straftaten erforderlich ist.

Die Datenübermittlung an das Landesamt für Verfassungsschutz richtet sich nach § 9 LVSG; mithin ist sie vorliegend nicht regelungsbedürftig. Demnach haben Behörden wie die Cybersicherheitsagentur, die ihnen bekannt gewordenen personenbezogenen Daten und sonstigen Informationen auch ohne vorheriges Ersuchen des Landesamts für Verfassungsschutz zu übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass diese Informationen zur Wahrnehmung von Aufgaben nach § 3 Absatz 2 LVSG erforderlich sind.

Zu Absatz 7

Eine zweckändernde Übermittlung möglicher Zufallsfunde an die Strafverfolgungsbehörden hat unter den engen Voraussetzungen des Absatzes 7 unverzüglich zu erfolgen. Die Über-

mittlung von Zufallsfunden soll höheren Schranken unterworfen sein als die zweckbewahrende Übermittlung bei Schadprogrammfunden nach Absatz 6. Absatz 7 sieht daher zusätzliche Schranken, insbesondere einen – nur bei besonderer Eilbedürftigkeit entfallenden – Richtervorbehalt, vor.

Außerdem hat die Cybersicherheitsagentur Daten zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- und Vermögenswerte unverzüglich an die Polizei zu übermitteln. Wegen der typischerweise bestehenden Eilbedürftigkeit wurde insoweit auf einen Richtervorbehalt verzichtet.

Zu Absatz 8

Eine darüberhinausgehende Nutzung oder Verarbeitung von Telekommunikationsinhalten, insbesondere des semantischen Inhalts, ist untersagt. Insbesondere sind daneben auch noch der Schutz des Kernbereichs privater Lebensgestaltung nach § 10 und der Schutz von Zeugnisverweigerungsrechten nach § 11 zu beachten.

Zu Absatz 9

Die Befugnisse nach § 5 erlauben eine Erhebung und Verarbeitung von personenbezogenen Daten mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen, so dass nach Satz 1 die Cybersicherheitsagentur vor Aufnahme der Datenverarbeitung eine Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 mit vorheriger Konsultation nach Artikel 36 der Verordnung (EU) 2016/679 durchzuführen hat. Für die sonstigen in Absatz 2 genannten Stellen ist im Einzelfall zu prüfen, ob eine Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 mit vorheriger Konsultation nach Artikel 36 der Verordnung (EU) 2016/679 durchzuführen ist.

Nach Satz 2 soll die Cybersicherheitsagentur – aufgrund der hohen Verantwortung der Ressorts gegenüber der Vertraulichkeit der Kommunikation der Mitarbeiterinnen und Mitarbeiter – das Ergebnis der Konsultation dem IT-Rat Baden-Württemberg übermitteln.

Zu Absatz 10

Absatz 10 sieht zusätzliche Kontrollmöglichkeiten vor, indem eine Unterrichtungspflicht über die Zahl der zweckändernden Übermittlungen nach Nummer 1 und der Fehltreffer („false positives“) nach Nummer 2 gegenüber der oder dem Landesbeauftragten für den Datenschutz geschaffen wird.

Zu Absatz 11

Außerdem hat die Cybersicherheitsagentur nach Absatz 11 jährlich dem Innenausschuss des Landtags umfänglich über ihre Umsetzung dieser Vorschrift, insbesondere die Bedrohungslage und die technische Entwicklung, zu unterrichten. Die Unterrichtung nach Absatz 11 enthält auch die Zahlen nach Absatz 10.

Zu Absatz 12

Absatz 12 nimmt die Informationstechnik der Stellen des Landes mit Sonderstatus im Sinne des § 2 Absatz 2 von den Regelungen des § 5 aus, um Wertungswidersprüche zu verfassungsrechtlichen Vorgaben (insbesondere Gewaltenteilung) oder gesetzlichen Regelungen zu vermeiden.

Zu § 6 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

Mit § 6 werden Maßnahmen durch sogenannte Mobile Incident Response Teams (MIRTs) geregelt. Mit den MIRTs soll die Cybersicherheitsagentur andere Stellen bei der Wiederherstellung ihrer IT-Systeme bei Cyberangriffen unterstützen. Die Sicherheit informationstechnischer Systeme von öffentlichen Stellen gehört zu dem Aufgabenkreis der Abwehr von Gefahren für die Cybersicherheit (§ 3 Absatz 1 Satz 2 Nummer 1). Mit dem § 6 wird die rechtliche Grundlage näher konkretisiert, auf der die Cybersicherheitsagentur die erforderlichen Maßnahmen zur Unterstützung und Wiederherstellung der Sicherheit oder Funktionsfähigkeit der von Cyberangriffen betroffenen informationstechnischen Systeme von öffentlichen Stellen sowie (in begründeten Einzelfällen) von anderen Stellen mit wichtiger Bedeutung für das öffentliche Gemeinwesen mit MIRTs treffen kann.

Zwar kann die Cybersicherheitsagentur im Rahmen ihrer zugewiesenen Aufgaben (vergleiche insbesondere § 3 Absatz 1 Satz 2 Nummer 1) auf Einwilligungsbasis und im Rahmen der Regelungen zum Datenschutz in Teil 3 dieses Gesetzes bereits von Cyberattacken betroffene Stellen mit MIRTs vor Ort unterstützen und beraten. Es können im Rahmen einer Maßnahme der MIRTs aber auch Maßnahmen erforderlich werden, die nicht von einer Einwilligung der betroffenen Einrichtung abgedeckt werden, da sie mit Eingriffen in das Fernmeldegeheimnis verbunden sind. Dies ist etwa der Fall, wenn zur Wiederherstellung der betroffenen Systeme der Netzwerkverkehr der betroffenen Stellen analysiert werden muss. Hierfür ist zum einen eine ausdrückliche rechtliche Grundlage erforderlich; zum anderen sind die entsprechenden Eingriffsschwellen und der Schutz personenbezogener Daten ausdrücklich zu regeln, um eine klare Rechtsgrundlage für die Maßnahmen der MIRTs zu schaffen.

Zu Absatz 1

Nach Absatz 1 soll die Cybersicherheitsagentur mit MIRTs auch operative Unterstützung bei der Bewältigung von Sicherheitsvorfällen bei öffentlichen Stellen leisten. Voraussetzung ist, dass es sich um einen herausgehobenen Fall handelt. Dabei wird die Cybersicherheitsagentur nur auf Ersuchen der betroffenen Stelle tätig, da die MIRTs primär der Unterstützung der betroffenen Stelle dienen. Deshalb soll der betroffenen Stelle die Entscheidung überlassen werden, ob sie die Dienste der Cybersicherheitsagentur in Anspruch nimmt.

Aufgabe der MIRTs ist dabei zunächst die kurzfristige Unterstützung der betroffenen Stelle bei der Schadensbegrenzung und der Sicherstellung eines Notbetriebes vor Ort. Danach sollen die betroffenen Stellen aber auch bei der forensischen Untersuchung des Vorfalles, der Beseitigung der Ursachen und damit der Wiederherstellung des Normalbetriebes unterstützt werden dürfen. Dies kann vor Ort oder aber z. B. auch in der Cybersicherheitsagentur erfolgen. Insbesondere forensische Arbeiten werden im Regelfall in der Cybersicherheitsagentur selbst erfolgen. Die Möglichkeit eines Einsatzes der MIRTs der Cybersicherheitsagentur entbindet die um Unterstützung ersuchenden Stellen jedoch nicht von der Pflicht, sich eigenständig auf Sicherheitsvorfälle vorzubereiten. Insbesondere werden die MIRTs nur dann tätig, wenn die betroffenen Stellen nicht mit eigenen Mitteln in der Lage sind, die Vorfälle zu bewältigen. Die Ausgestaltung als „Soll-Regelung“ stellt klar, dass eine Pflicht der Cybersicherheitsagentur zum Tätigwerden im Regelfall besteht. Hieraus folgt, dass eine ersuchende Stelle keinen Anspruch auf ein Tätigwerden der Cybersicherheitsagentur hat, sondern der Cybersicherheitsagentur ein eingeschränkter Ermessensspielraum zusteht. Die von der Cybersicherheitsagentur zu ergreifenden Maßnahmen können unterschiedlicher Natur sein. Neben Analysen der betroffenen informationstechnischen Systeme und des Netzwerkverkehrs können dazu insbesondere auch aktive Sicherungsmaßnahmen gehören, wie etwa das Blockieren der Netzwerkverbindungen zu den Quellen der Gefährdung (z. B. zu den Kontrollservern der angreifenden Person oder zu den Ausgangspunkten von verteilten Netzwerkangriffen (sogenannte Distributed Denial of Service – DDoS-Angriffen)).

Zu Absatz 2

In Absatz 2 wird festgelegt, wann ein herausgehobener Fall vorliegt, bei dem um Unterstützung durch die MIRTs der Cybersicherheitsagentur ersucht werden kann. Ein herausgehobener Fall liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems im besonderen öffentlichen

Interesse ist. Angriffe besonderer Qualität liegen etwa dann vor, wenn zumindest der Verdacht auf sogenannte Advanced Persistent Threats besteht, die sich dadurch auszeichnen, dass Standardsicherheitsmaßnahmen zur Abwehr nicht ausreichen. Eine besondere Qualität kann auch sogenannten DDoS-Angriffen zugeschrieben werden, sofern sie mit einer außergewöhnlichen Bandbreite oder Technik ausgeführt werden. Wird zum Beispiel ein Verschlüsselungstrojaner eingesetzt, kann es sein, dass der erste Angriff als außergewöhnlich einzustufen ist; diese Einstufung würde aber für spätere Fälle nicht mehr gelten, wenn in diesen Fällen keine neuen Techniken verwendet wurden und Anleitungen zum Umgang mit den Vorfällen bereits verfügbar sind.

Ein besonderes öffentliches Interesse an der zügigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems wird immer dann anzunehmen sein, wenn dessen Ausfall oder Beeinträchtigung spürbare Auswirkungen auf das Gemeinwohl zum Beispiel im Sinne der Versorgung der Allgemeinheit mit kritischen Dienstleistungen, auf die Sicherheit oder auf die Arbeitsfähigkeit von öffentlichen Stellen haben kann oder diese aus einem anderen Grund ein gegenwärtiges Anliegen der Allgemeinheit darstellen. Dies ist z. B. dann der Fall, wenn IT-Systeme des Landes durch Angriffe kompromittiert sind und dadurch die Funktionsfähigkeit und Vertraulichkeit ihres Handelns nicht mehr sichergestellt sind.

Zu Absatz 3

In Absatz 3 ist der Umgang mit den personen- und kommunikationsbezogenen Daten geregelt, die die Cybersicherheitsagentur bei ihrer Unterstützung verarbeiten muss. Zur Analyse eines Cyberangriffes müssen Logdaten der betroffenen Systeme und Netze analysiert werden, um den Angriff und die Aktivitäten der kriminellen Person nachvollziehen zu können. Üblicherweise verbleiben kriminelle Personen nicht nur auf einem IT-System, sondern versuchen, sich im Netz der angegriffenen Stelle auszubreiten. Die Aufklärung eines solchen Angriffs und die Bereinigung der infizierten Systeme können nur mittels umfassender Analyse der Log- und Kommunikationsdaten ermöglicht werden. Die personen- und kommunikationsbezogenen Daten, die die Cybersicherheitsagentur erhoben hat, sind nach Beendigung der Unterstützung zu löschen. Ausnahmen gelten nur dann, wenn die Daten mit Einwilligung der betroffenen Stelle oder entsprechend § 5 Absatz 6 oder 7 an eine andere Stelle zur Erfüllung ihrer gesetzlichen Aufgaben weitergegeben worden sind. Dies ist im Hinblick auf die Abstimmung der Cybersicherheitsagentur mit den Sicherheitsbehörden notwendig, die ebenfalls entsprechende Vor-Ort-Teams aufbauen werden. Das in § 5 Absatz 8 in Verbindung mit dem Teil 3 dieses Gesetzes vorgesehene hohe Datenschutzniveau wird auf § 6 übertragen. Im Übrigen gelten zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten die Vorgaben des Landesdatenschutzgesetzes

und der Verordnung (EU) 2016/679. Für die Unterstützungsleistungen der Cybersicherheitsagentur stellt § 6 eine Sondernorm dar, die sonstigen landesrechtlichen Regelungen vorgeht.

Zu Absatz 4

Nach Absatz 4 dürfen Informationen, von denen die Cybersicherheitsagentur Kenntnis erlangt, von dieser nur mit Einwilligung der ersuchenden Stelle übermittelt werden, es sei denn, die weiterzugebenden Informationen lassen keine Rückschlüsse auf die Identität der ersuchenden Stelle zu oder die Informationen sind entsprechend § 5 Absatz 6 und 7 zu übermitteln. Diese Regelung dient dem Schutz der Interessen der ersuchenden Stelle. Sofern die Ergebnisse und Fakten bekannt würden, die bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit der informationstechnischen Systeme erarbeitet wurden, könnten angreifende Personen daraus wertvolle Informationen für neue Angriffe auf die Sicherheit dieser Systeme erhalten. Außerdem setzt die Einschaltung der Cybersicherheitsagentur das Zutrauen der zu unterstützenden Stellen in die vertrauliche Behandlung des Vorfalles voraus. Da sich allerdings aus den Daten auch für die Strafverfolgungsbehörden, die Polizei und das Landesamt für Verfassungsschutz wichtige Erkenntnisse für ihre Aufgabenwahrnehmung ergeben können, werden zur Übermittlung dieser Daten die Verfahren nach § 5 Absatz 6 und 7 übernommen. In diesem Zusammenhang begründen Angriffe, die eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer öffentlichen Stelle des Landes oder einer Stelle im Sinne des Absatzes 7 nach sich ziehen, in der Regel zugleich auch den Anfangsverdacht der Begehung von Straftaten oder eine Gefahr für die öffentliche Sicherheit. Satz 3 regelt ferner, dass zum Schutz des öffentlichen Interesses an der Bewältigung der hier in Rede stehenden Sicherheitsvorfälle, der hierfür zu treffenden Maßnahmen sowie der schutzwürdigen Interessen der ersuchenden Stelle ein Zugang für dritte Personen (beispielsweise auf Grundlage des Landesinformationsfreiheitsgesetzes) zu den Akten von Verfahren nach § 6 Absatz 1 ausgeschlossen wird. Soweit die Cybersicherheitsagentur andere informationspflichtige Stellen im Sinne des § 3 Nummer 2 des Landesinformationsfreiheitsgesetzes unterstützt, bleibt das Recht auf Informationszugang gegenüber diesen Stellen unberührt.

Zu Absatz 5

Absatz 5 stellt klar, dass die Cybersicherheitsagentur nicht nur mit eigenen Mitteln unterstützen kann, sondern mit Zustimmung der ersuchenden Person und auf deren Kosten auch auf externe Unterstützung zurückgreifen darf, soweit dies nicht aufgrund gesetzlicher Vorschriften ausgeschlossen ist. Die Cybersicherheitsagentur verpflichtet die qualifizierten dritten Personen zur vertraulichen Behandlung von Informationen, zur Einhaltung der Infor-

mationssicherheit und zum Datenschutz. Soweit die dritte Person personenbezogene Daten im Auftrag verarbeitet, ist sie sorgfältig auszuwählen. Sie muss insbesondere die Gewähr dafür bieten, dass die dritte Person in der Lage ist, die für eine datenschutzgerechte Datenverarbeitung erforderlichen technischen und organisatorischen Maßnahmen zu treffen. Die Cybersicherheitsagentur und die dritte Person schließen eine Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag ab (Artikel 28 der Datenschutz-Grundverordnung).

Die Einbindung dritter Personen durch die Cybersicherheitsagentur kann in verschiedenen Formen geschehen. Zum einen kann die Cybersicherheitsagentur selbst externe Personen mit der Wahrnehmung bestimmter Tätigkeiten beauftragen. Zum anderen kann sie aber auch dritte Personen einbinden, die von der ersuchenden Stelle bestimmt wurden. Sie kann mit den dritten Personen auch Daten austauschen. Hierbei sind die Vorgaben des Absatzes 3 einzuhalten. Unter den Begriff der dritten Personen fallen auch natürliche und juristische Personen, die sich im Rahmen einer IT-Sicherheitskooperation mit dem Land Baden-Württemberg bereiterklärt haben, in Notfällen zu helfen, obwohl sie hierzu nicht verpflichtet sind. Dies werden in der Regel Spezialistinnen und Spezialisten anderer Unternehmen sein, die diese im Wege der gegenseitigen Hilfe und Unterstützung entsenden. Mit dieser Möglichkeit zur Einbindung freiwillig helfender Personen aus der Mitte der Wirtschaft wird der Gedanke von der Cybersicherheit als gesamtgesellschaftlicher Aufgabe auch legislativ mit Leben gefüllt. Anders als bei § 3 Absatz 2 bezieht sich die Regelung in § 6 Absatz 5 explizit nicht nur auf dritte Personen, die IT-Sicherheitsdienstleistungen anbieten, sondern generell auf qualifizierte Personen. Dies trägt der Tatsache Rechnung, dass das Ziel der Unterstützung nicht nur die reine Absicherung ist, sondern die Wiederherstellung des sicheren (Regel-)Betriebs des informationstechnischen Systems. Dies gilt insbesondere bei Vorfällen mit Spezial-IT, zu der in der Cybersicherheitsagentur keine ausreichenden Ressourcen für eine rasche Unterstützung vorliegen.

Gleichzeitig fehlt der betroffenen Stelle im akuten Notfall die Zeit für eine Marktsichtung. Daher besteht die Erwartung, dass die Cybersicherheitsagentur zumindest eine Auswahl geeigneter dienstleistender oder sonstiger qualifizierter Personen benennen kann. Die Auswahl der dritten Personen obliegt der betroffenen Stelle selbst.

Zu Absatz 6

Absatz 6 sieht vor, dass die Cybersicherheitsagentur die herstellenden Personen der betroffenen informationstechnischen Systeme auffordern kann, bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken. Insbesondere wenn die Cybersicherheit durch eine Sicherheitslücke in der verwendeten Hard- oder Software gefährdet wird, kann in erster Linie die das jeweilige Produkt herstellende Person schnell und

nachhaltig zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit beitragen – etwa durch das zeitnahe Bereitstellen eines Sicherheitspatches.

Aus Gründen der Verhältnismäßigkeit darf die herstellende Person nicht zur kostenlosen Mitwirkung herangezogen werden, wenn die ersuchende Stelle Soft- oder Hardware einsetzt, deren Supportzeitraum bereits abgelaufen ist, und die herstellende Person das Ende des Supportzeitraumes rechtzeitig angekündigt hat. Die Mitwirkungspflicht der herstellenden Person bleibt davon unberührt. Im Falle einer Weigerung der herstellenden Person gelten die allgemeinen Regelungen des Verwaltungszwangs.

Zu Absatz 7

Zu Satz 1

In Absatz 7 wird der Cybersicherheitsagentur die Möglichkeit eingeräumt, in begründeten Einzelfällen auch nichtöffentliche Stellen auf deren Ersuchen bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit ihrer informationstechnischen Systeme zu unterstützen. Ein begründeter Einzelfall liegt dann vor, wenn (neben den sonstigen Voraussetzungen des Absatzes 1) ein vergleichbares öffentliches Interesse an der Behebung des Sicherheitsvorfalls besteht, auch wenn die betroffene Einrichtung nicht zu dem Adressatenkreis des Absatzes 1 zählt. Zwar soll der Einsatz der MIRTs primär auf den Adressatenkreis des Absatzes 1 beschränkt bleiben. Der Cybersicherheitsagentur soll aber die Möglichkeit eröffnet werden, ausnahmsweise auch in anderen Fallkonstellationen tätig werden zu können. Dies kann etwa dann der Fall sein, wenn Anlagen oder Systeme von Unternehmen, welche sich in der staatlichen Geheimschutzbetreuung befinden, angegriffen werden oder Anlagen oder Systeme von Organisationen betroffen sind, deren Ausfall oder Beeinträchtigung weitreichende Auswirkungen hätte. Solche Auswirkungen können etwa bei erfolgreichen Angriffen auf Unternehmen mit besonderem Sicherheitsbezug oder besonderem Gefahrenpotenzial (z. B. Unternehmen der chemischen Industrie) oder auf große Konzerne sowie deren Zulieferer eintreten. Durch die starke Vernetzung und moderne Just-in-Time-Lieferungen wirken sich erfolgreiche Angriffe nicht nur auf das unmittelbar angegriffene, sondern auf viele assoziierte Unternehmen aus. Aufgrund der erheblich schädigenden Auswirkungen von Betriebsausfällen auf die Wertschöpfung in Baden-Württemberg und des drohenden Verlusts vieler Arbeitsplätze wäre das Gemeinwohl in ähnlich starkem Ausmaß gefährdet. In Betracht kommen aber auch Einrichtungen, deren besondere politische, wirtschaftliche oder gesellschaftliche Bedeutung im Fall eines erheblichen Angriffs ein Eingreifen der Cybersicherheitsagentur erforderlich erscheinen lässt.

Zu Satz 2

Nach Satz 2 kann – abweichend von Absatz 4 in Verbindung mit § 6 Absatz 6 und 7 – eine Übermittlung im Einzelfall bei einem geltend gemachten schutzwürdigen Interesse der ersuchenden Stelle unterbleiben. Das im Einzelfall geltend gemachte schutzwürdige Interesse setzt eine dementsprechende Erklärung der betroffenen Stelle für den konkreten Sicherheitsvorfall voraus.

Zu Absatz 8

Mit dem Absatz 8 wird eine angemessene Berücksichtigung von Aspekten der nuklearen Sicherheit durch die Einbeziehung der Aufsichtsbehörden gewährleistet. Eine Regelung ist notwendig, um die besonderen Belange im Atomrecht sowie der damit verbundenen Gewährleistung der nuklearen Sicherheit und nuklearen Sicherung von kerntechnischen Anlagen und Tätigkeiten sowie des Geheimschutzes zu berücksichtigen. Daher ist insbesondere in Fällen der Absätze 1, 4, 5 und 7 vor Tätigwerden der Cybersicherheitsagentur das Benehmen mit den zuständigen atomrechtlichen Aufsichtsbehörden des Bundes und des Landes Baden-Württemberg herzustellen, da unmittelbare Auswirkungen auf Sicherungsmaßnahmen nach dem Atomgesetz möglich sind. Da Sicherungsmaßnahmen auf Grundlage des Atomgesetzes in der Regel auch dem Geheimschutz unterliegen, ist auch aus diesem Grund das Benehmen mit den atomrechtlich zuständigen Aufsichtsbehörden herzustellen. Hierdurch soll eine gegenseitige Beeinflussung von jeweils in unterschiedlichen Rechtsgebieten zuständigen Behörden vermieden werden.

Zu Absatz 9

Wegen des zunehmenden Bedrohungspotenzials und des damit verbundenen herausragenden öffentlichen Interesses an der Sicherheit der von § 6 erfassten betroffenen Stellen, sind nach Satz 1 erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort nicht kostenpflichtig. Hierdurch wird gewährleistet, dass von einem Hilfeersuchen nicht aus Kostengründen abgesehen wird. Denn angesichts des zunehmenden Bedrohungspotenzials durch Cyberangriffe besteht ein herausragendes öffentliches Interesse an der Cybersicherheit auch dieser Stellen. Die Unterstützung der Cybersicherheitsagentur dient alleine der schnellen Wiederherstellung der Sicherheit der betroffenen informationstechnischen Systeme und soll keine günstige Alternative zur Beauftragung kommerzieller IT-Dienstleistungsunternehmen darstellen.

Nach Satz 2 hat die betroffene Einrichtung die Kosten für den Einsatz qualifizierter dritter Personen selbst zu tragen. Darüber hinaus gilt das Landesgebührengesetz und die Gebührenverordnung Innenministerium.

Zu § 7 – Untersuchung der Sicherheit in der Informationstechnik

Im Rahmen der Analyse und Wiederherstellung der Sicherheit und Funktionsfähigkeit informationstechnischer Systeme nach § 6 muss die Cybersicherheitsagentur auch die Möglichkeit haben, diese Systeme vollständig zu untersuchen, erforderlichenfalls auch mittels Reverse-Engineering. Um Auslegungsfragen zur Reichweite der bestehenden Regelung vorzubeugen, wird dies mit § 7 Absatz 1 Satz 1 bezüglich der Informationstechnik der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen und mit § 7 Absatz 2 Satz 1 bezüglich informationstechnischer Produkte und Systeme klargestellt. Ergänzend dazu werden jeweils Regelungen zum Umgang mit den gewonnenen Erkenntnissen getroffen.

Dabei sind die bundesrechtlichen Vorgaben (insbesondere zum Schutz des geistigen Eigentums) zu beachten.

Zu Absatz 1

Zu Satz 1

Die Cybersicherheitsagentur kann nach Satz 1 die Sicherheit der Informationstechnik der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen im Einvernehmen mit der jeweils fachlich zuständigen obersten Landesbehörde untersuchen und bewerten, mithin hat sie ein Recht zur Prüfung einzelner Systemkomponenten bis hin zur Auditierung der gesamten IT-Infrastruktur. Damit wird sichergestellt, dass alle Stellen des Landesverwaltungsnetzes das erforderliche Sicherheitsniveau erfüllen. Die Cybersicherheitsagentur muss für eine Beurteilung der IT-Sicherheit Zugang zu den Systemen haben. Dieser kann u. U. nur eingeschränkt gewährt werden, wenn beispielsweise Vorschriften des Geheimschutzes dem entgegenstehen. Vorab ist zu prüfen, ob eine Sicherheitsüberprüfung der prüfenden Beschäftigten der Cybersicherheitsagentur Abhilfe schaffen kann. Werden bei der Prüfung Gefahren für die Informationstechnik des Landes entdeckt, kann die Cybersicherheitsagentur nach § 5 Absatz 1 die nötigen Anordnungen treffen oder entsprechende Maßnahmen zur Abwehr der Gefahren ergreifen.

Zu Satz 2

Die in Satz 1 geregelte Befugnis erstreckt sich nach Satz 2 nicht auf die Informationstechnik des Landesamts für Verfassungsschutz, des Polizeivollzugsdienstes oder der Strafverfolgungsbehörden, soweit sie in deren eigener oder länderübergreifender Zuständigkeit betrieben wird. Ausgenommen nach Satz 2 sind insbesondere der BOS-Digitalfunk und dessen Kooperationsprodukte.

Zu Satz 3

Über die gewonnenen Erkenntnisse aus der Prüfung erstellt die Cybersicherheitsagentur nach Satz 3 einen Bericht, den sie der untersuchten Stelle zur Verfügung stellt, damit diese Stelle das Sicherheitsniveau ihrer Informationstechnik verbessern kann.

Zu Absatz 2

Absatz 2 Satz 1 dient dazu, Rechtssicherheit für umfassende Untersuchungen von IT-Produkten (zum Beispiel mittels Reverse-Engineering) und IT-Systemen durch die Cybersicherheitsagentur zur Erfüllung ihrer Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 6 herzustellen. Die gesetzliche Befugnis führt dazu, dass die Beschaffung von Daten und Informationen über den Aufbau und die Funktionsweise der Untersuchungsgegenstände durch die Cybersicherheitsagentur nicht als unbefugt im Sinne von § 202a des Strafgesetzbuches (StGB) anzusehen ist. Auch geht Absatz 2 als eine öffentlich-rechtliche Vorschrift nach § 1 Absatz 2 des Gesetzes zum Schutz von Geschäftsgeheimnissen den sonstigen Regelungen des Gesetzes zum Schutz von Geschäftsgeheimnissen vor.

Auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene Untersuchungsgegenstände sind solche, die für einen Erwerb durch die Cybersicherheitsagentur verfügbar sind. Die Formulierung „auf dem Markt bereitgestellte Produkte“ ist angelehnt an das Gesetz über die Bereitstellung von Produkten auf dem Markt (Produktsicherheitsgesetz – ProdSG). Durch die Formulierung „zur Bereitstellung auf dem Markt vorgesehene“ Untersuchungsgegenstände wird klargestellt, dass die Untersuchungsbefugnis auch solche Produkte und Systeme erfasst, die zwar von den herstellenden Personen bereits angekündigt wurden, aber noch nicht allgemein am Markt verfügbar sind. Untersuchungsrechte der Cybersicherheitsagentur bei herstellenden, anbietenden und sonstigen Einrichtungen werden durch Satz 1 nicht begründet. Bei der Auswahl der dritten Personen, die von der Cybersicherheitsagentur nach Satz 2 mit der Untersuchung beauftragt werden können, hat die Cybersicherheitsagentur die schutzwürdigen Interessen der herstellenden Person zu berücksichtigen. Hierzu gehört auch, dass die Cybersicherheitsagentur die beauftragten dritten Personen zur Wahrung einer entsprechenden Vertraulichkeit verpflichtet. Die Beauftragung von direkt konkurrierenden Personen ist in diesem Zusammenhang ausgeschlossen.

Satz 3 bis 5 enthalten eine Zweckbindung für die aus der Untersuchung nach Satz 1 gewonnenen Erkenntnisse. Soweit erforderlich, ist zudem eine Weitergabe und Veröffentlichung dieser Erkenntnisse durch die Cybersicherheitsagentur zulässig. In diesem Fall ist der herstellenden Person zuvor die Gelegenheit zu einer Stellungnahme einzuräumen.

Wenn die herstellende Person Abhilfe schafft, ist eine zusätzliche Veröffentlichung der Erkenntnisse durch die Cybersicherheitsagentur nicht erforderlich.

Zu § 8 – Warnungen, Empfehlungen und Hinweise

Die Vorschrift regelt die genauen Umstände, unter denen die Cybersicherheitsagentur aufgrund von gewonnenen Erkenntnissen bei Gefahren für die Cybersicherheit die Öffentlichkeit oder betroffene Kreise informieren darf. Damit wurde insoweit eine Spezialvorschrift zur Information der Öffentlichkeit oder der betroffenen Kreise geschaffen, die einen Rückgriff auf die allgemeinen Regelungen im Teil 3 dieses Gesetzes zur Verarbeitung personenbezogener Daten ausschließt. Für die Information von Landesbehörden enthält § 4 eine Spezialvorschrift zu § 8. Soweit sich die Warnungen, Empfehlungen und Hinweise an Verbraucherinnen und Verbraucher richten, erfolgt dies in Kooperation mit dem für Verbraucherschutz zuständigen Ministerium.

Zu Absatz 1

Mit Warnungen und Empfehlungen kann ein nicht unerheblicher Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb einhergehen. Insbesondere bei Nennung der herstellenden oder inverkehrbringenden Person liegt ein Eingriff in deren Grundrechte vor. Andererseits kann eine Warnung oder Empfehlung zur Reduzierung der Gefahr für die Cybersicherheit bzw. Schadenseingrenzung bei Verlust von oder eines unerlaubten Zugriffs auf Daten erforderlich und angemessen sein.

Unter den in Satz 1 genannten Voraussetzungen hat die Cybersicherheitsagentur ein Ermessen darüber zu entscheiden, ob sie Warnungen oder Empfehlungen ausspricht, soweit kein konkreter Bezug zu einer bestimmten herstellenden oder inverkehrbringenden Person vorliegt. Dabei ist in Satz 1 klargestellt, dass die Cybersicherheitsagentur nach § 8 auch in Fällen tätig werden kann, in denen nicht die Warnung vor einem Schadprogramm oder einer Sicherheitslücke im Vordergrund steht, sondern vielmehr die Bewältigung eines bereits erfolgten Verlustes von oder Zugriffs auf Daten. Zur Schadenseingrenzung wird die Cybersicherheitsagentur im Regelfall frühzeitig eine Warnung aussprechen und die Bürgerinnen und Bürger informieren, es sei denn, dieses Vorgehen würde zu erheblichen Sicherheitsrisiken führen.

Nach Satz 2 dürfen Warnungen und Empfehlungen die Bezeichnung der herstellenden oder inverkehrbringenden Person nur enthalten, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Cybersicherheit von dem Produkt oder Dienst ausgehen. Bei der Ermessensausübung sind insbesondere die Schwere des Eingriffs in die Grundrechte der herstellenden oder inverkehrbringenden Personen zu berücksichtigen.

Satz 3 berücksichtigt das in der IT-Wirtschaft geübte Prinzip der verantwortungsvollen Weitergabe („responsible disclosure“). Danach werden in der Regel zunächst die herstellenden oder inverkehrbringenden Personen betroffener Produkte über entdeckte Sicherheitslücken informiert, um diesen Gelegenheit zu geben, Sicherheits-Updates zu entwickeln und ihren Kundinnen und Kunden zur Verfügung zu stellen. Eine Vorabinformation dritter Personen, insbesondere der Öffentlichkeit, ist allerdings dann geboten, wenn der Zweck der Maßnahme sonst nicht erreicht würde.

Satz 4 stellt als Ausfluss des Verhältnismäßigkeitsprinzips klar, dass auf berechtigte Interessen der betroffenen Stellen Rücksicht zu nehmen ist.

Zu Absatz 2

Durch das allgemeine Bekanntwerden entdeckter Sicherheitslücken oder Schadprogramme könnten kriminelle Personen Möglichkeiten für Begehung von Straftaten erfahren oder Vertraulichkeitsbeziehungen zwischen der Cybersicherheitsagentur und dritten Personen (d.h. natürlichen oder juristischen Personen des öffentlichen oder des privaten Rechts) gestört werden. Dementsprechend kann die Cybersicherheitsagentur den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken. In Betracht kommen insbesondere die öffentlichen Stellen oder Stellen mit wichtiger Bedeutung für das öffentliche Gemeinwesen wegen deren besonderen Gefährdung und/oder der besonderen Zuverlässigkeit.

Zu Absatz 3

Absatz 3 ermöglicht, über eigene Warnungen, Empfehlungen und Hinweise an die Öffentlichkeit auch auf Informationen der herstellenden oder inverkehrbringenden Personen oder anderer öffentlicher Stellen hinzuweisen, um Gefahren für die Cybersicherheit durch schnelle Verbreitung dieser Informationen abzuwehren.

Zu Absatz 4

Die Regelung ermöglicht bei Warnungen, Empfehlungen oder Hinweisen Personen außerhalb der Cybersicherheitsagentur als Informationsintermediäre einzubeziehen, sofern dies für eine wirksame und rechtzeitige Information erforderlich ist, insbesondere um die betroffenen Personen schnellstmöglich zu erreichen. Diese Regelung eröffnet aber keine Möglichkeit, zusätzliche personenbezogene Daten bei diesen Personen zu erheben. Informationsintermediäre können insbesondere die von den Kundinnen und Kunden genutzten

diensteanbietenden Stellen sein. Oftmals wird die Cybersicherheitsagentur gerade abhandengekommene Daten nicht direkt einer betroffenen Person zuordnen oder diese nicht ohne weiteres selbst unterrichten können.

Zu Absatz 5

Warnungen, Empfehlungen und Hinweise können erhebliche Grundrechtseingriffe gegenüber den herstellenden und inverkehrbringenden Personen darstellen. Aus diesem Grund sind Informationen, die sich im Nachhinein als falsch oder unrichtig wiedergegeben herausstellen, nach Satz 1 unverzüglich (d.h. ohne schuldhaftes Zögern) zu berichtigen.

Überdies können die Voraussetzungen nach Absatz 1 für eine Information entfallen (z.B. nach einem Update für ein Programm), so dass nach Satz 2 in diesem Fall die Öffentlichkeit oder die betroffenen Kreise unverzüglich darüber zu informieren sind.

Satz 3 legt fest, dass die Bekanntmachungen nach Satz 1 und 2 in derselben Weise erfolgen sollen, in der die Information nach Absatz 1 erfolgt ist. Dadurch wird der etwaige Eingriff in die Grundrechte der herstellenden oder inverkehrbringenden Personen weitgehend kompensiert. Ausnahmsweise bestehende Entschädigungsansprüche richten sich nach den allgemeinen Regelungen.

Die gesetzliche Löschungsfrist für Informationen nach Satz 4 berücksichtigt die Vorgaben des Bundesverfassungsgerichts (Beschl. vom 21. März 2018 – 1 BvF 1/13) zum staatlichen Informationshandeln. Nach Ablauf von sechs Monaten kann in der Regel davon ausgegangen werden, dass sich die Gefahr für die Cybersicherheit danach soweit vermindert hat, dass eine weiter andauernde Veröffentlichung der Gefahrverursacher nicht mehr angemessen erscheint.

Zu Teil 3 – Datenschutz

Die Datenverarbeitungsregeln des dritten Teils berücksichtigen insbesondere den Erwägungsgrund 49 der Verordnung (EU) 2016/679. Danach stellt die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams – CERT, beziehungsweise Computer Security Incident Response Teams – CSIRT), elektronische Kommunikationsnetze und -dienste sowie Sicherheitstechnologien und -dienste in dem Maße ein berechtigtes Interesse der jeweiligen verantwortlichen Person dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit

Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Vertraulichkeit, Integrität und Verfügbarkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den unbefugten Zugang zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern durch sogenannte DoS-Angriffe und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

Zu § 9 – Anwendbarkeit des Landesdatenschutzgesetzes

§ 9 stellt klar, dass neben diesem Gesetz auch das LDSG zur Anwendung kommt, soweit dieses Gesetz keine abschließende Regelung zum Datenschutz enthält. Die Verordnung (EU) 2016/679 gilt ohne Anordnung bereits kraft ihrer unmittelbaren Wirkung. Auch sind spezielle Regelungen zum Datenschutz wie etwa im Gesundheitsbereich zu beachten.

Ausnahmsweise findet die Verordnung (EU) 2016/679 nach deren Artikel 2 Absatz 2 Buchstabe d keine Anwendung auf die Datenverarbeitung „durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“ Komplementär dazu ist der Anwendungsbereich der 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) nach deren Artikel 1 Absatz 1 eröffnet.

Der Anwendungsbereich der Richtlinie (EU) 2016/680 ist nicht eröffnet, wenn die datenverarbeitende Behörde über keine Befugnisse zur repressiven Verfolgung von Straftaten oder Ordnungswidrigkeiten verfügt (Bäcker, in: BeckOK Datenschutzrecht, Wolff/Brink, 31. Edition, Stand: 01.05.2019, DS-GVO, Artikel 2 Sachlicher Anwendungsbereich, Randnummer 28; derselbe, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, S. 63 (65 ff.); Deutscher Bundestag, Wissenschaftliche Dienste, Datenverarbeitung durch Polizei und Sicherheitsbehörden, WD 3 - 3000 - 087/19, Seite 4; ebenfalls reine Ordnungsbehörden aus dem Anwendungsbereich ausnehmend Zerdick, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Artikel 2 Randnummer 12).

Da die Cybersicherheitsagentur über keine repressiven Befugnisse zur Verfolgung von Straftaten oder Ordnungswidrigkeiten verfügt, fällt deren Datenverarbeitung nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680, sondern in den Anwendungsbereich der Verordnung (EU) 2016/679.

Zu § 10 – Kernbereichsschutz

Dass der Cybersicherheitsagentur bei der Suche nach Gefahren für die Cybersicherheit kernbereichsrelevante Inhalte zur Kenntnis gelangen, ist extrem unwahrscheinlich. Auf eine Pflicht zur begleitenden Kernbereichskontrolle wurde verzichtet, da diese gegenüber der eigentlichen Maßnahme einen stärkeren Grundrechtseingriff darstellte: Die Inhaltsauswertung durch die Cybersicherheitsagentur beschränkt sich auf die Durchsicht der technischen Steuerbefehle. Semantische Inhalte können hierbei allenfalls als Zufallsfunde in Ausnahmefällen erkannt werden. Eine ständige Kontrolle auf Kernbereichsrelevanz würde hingegen die inhaltliche Auswertung auch der „menschlichen“ Kommunikationsanteile erforderlich machen.

Zu Satz 1 bis 4

Um den verfassungsrechtlichen Anforderungen zu genügen, ist bereits technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Um dennoch möglicherweise erfolgende Datenerhebungen möglichst bedeutungslos zu halten, dürfen diese Inhalte nach Satz 2 nicht verarbeitet werden. Dennoch erlangte Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind nach Satz 3 unverzüglich (d.h. ohne schuldhaftes Zögern) zu löschen. Diese Löschungsverpflichtung gilt nach Satz 4 auch dann, wenn Zweifel bestehen, ob die Inhalte kernbereichsrelevant sind oder nicht.

Zu Satz 5 und 6

Daten, die aus dem Kernbereich privater Lebensgestaltung stammen könnten, sind nach Satz 5 der oder dem behördlichen Datenschutzbeauftragten sowie einer oder einem weiteren Bediensteten vorzulegen, damit diese überprüfen können, ob eine Löschung vorzunehmen ist. Kommt eine der beiden Personen zu dem Ergebnis, dass Daten aus dem Kernbereich privater Lebensgestaltung stammen, sind diese Daten nach Satz 6 zu löschen. Dieses Vieraugenprinzip gewährleistet einen effektiven Grundrechtsschutz.

Zu Satz 7 bis 9

Die Tatsache der Erlangung solcher Daten und deren Löschung ist nach Satz 7 aktenkundig zu machen und diese Dokumentation dient nach Satz 8 ausschließlich der Datenschutzkontrolle. Dementsprechend ist sie nach Satz 9 spätestens am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt, zu löschen.

Zu § 11 – Schutz von Zeugnisverweigerungsrechten

Satz 1 regelt ein Verwertungsverbot für Erkenntnisse, die vom Zeugnisverweigerungsrecht der in § 53 Absatz 1 Satz 1 und § 53a Absatz 1 Satz 1 StPO genannten Personen übermittelt worden sind. Der privilegierte Personenkreis ist begrifflich durch Rechtsprechung und Lehre ausreichend konkretisiert. Vorbehaltlich der Verstrickungsregelung in Satz 4 ist der Schutz der Kommunikation mit den genannten Berufsgeheimnisträgern so umfassend ausgestaltet, als es der Landesgesetzgeber regeln kann, und hängt mithin nicht von Erwägungen zur Verhältnismäßigkeit im Einzelfall ab. Nach Satz 3 ist die Tatsache der Erlangung unter das Erhebungsverbot nach Satz 1 fallender Erkenntnisse sowie die Löschung dieser Erkenntnisse in geeigneter Form zu dokumentieren. Dies sichert zum einen die Einhaltung der Löschungspflicht, dient aber vor allem der späteren Nachvollziehbarkeit im Rahmen etwaiger Rechtsschutzbegehren der betroffenen Personen.

Satz 4 beinhaltet die sogenannte Verstrickungsregelung. Dies bedeutet, dass der von den Sätzen 1 bis 3 gewährleistete besondere Schutz des Zeugnisverweigerungsrechts nach Satz 4 dann endet, wenn die zeugnisverweigerungsberechtigte Person selbst für die Gefahr verantwortlich ist (vgl. §§ 6, 7 des Polizeigesetzes). Denn der Schutz der betroffenen Vertrauensverhältnisse oder der Institutionen an sich soll nicht zur Begründung von Geheimbereichen führen, in denen die Verursachung von Gefahren einer staatlichen Aufklärung schlechthin entzogen ist.

Zu § 12 – Verarbeitung personenbezogener Daten

Mit § 12 wird eine klare Rechtsgrundlage für die Cybersicherheitsagentur zur Verarbeitung von personenbezogenen Daten geschaffen. Die Cybersicherheitsagentur fördert die Cybersicherheit (§ 3 Absatz 1 Satz 1) und nimmt zu diesem Zweck die in § 3 Absatz 1 Satz 2 aufgeführten Aufgaben wahr. Zur Erfüllung dieser im wichtigen öffentlichen Interesse liegenden Aufgaben ist die Cybersicherheitsagentur auf datenschutzrechtliche Ermächtigungen zur Verarbeitung personenbezogener Daten angewiesen. Um sicherzustellen, dass die Cybersicherheitsagentur ihre gesetzlichen Aufgaben aus § 3 erfüllen kann und um eine auf die Erfordernisse der Cybersicherheitsagentur angepasste Datenverarbeitung zu ermöglichen, wird auf Basis von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e und Absatz 3 Satz 1 Buchstabe b der Verordnung (EU) 2016/679 der § 12 als datenschutzrechtliche Ermäch-

tigungsgrundlage geschaffen. § 12 Absatz 1 und 2 gilt nur für die Aufgaben und Tätigkeiten, die nicht unmittelbar durch die speziellen datenschutzrechtlichen Befugnisse in Teil 2 erfasst werden.

Zu Absatz 1

Durch Absatz 1 wird klargestellt, dass die Cybersicherheitsagentur zur Wahrnehmung ihrer Aufgaben personenbezogene Daten verarbeiten kann. Die Regelung beruht auf Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e der Verordnung (EU) 2016/679.

Zu Absatz 2

Absatz 2 ermöglicht die Weiterverarbeitung personenbezogener Daten über die Regelung in Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 und in § 5 LDSG hinaus. Die Regelung trägt dem Erfordernis Rechnung, dass die Cybersicherheitsagentur neben den speziellen Befugnissen zur Verarbeitung von Daten im zweiten Teil für die Erfüllung ihrer gesetzlichen Aufgaben eine datenschutzrechtliche Rechtsgrundlage benötigt, um personenbezogene Daten zum Zwecke der Sammlung, Auswertung und Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für den Cyberraum und zur Unterstützung, Beratung, Warnung, Empfehlung und zu Hinweisen in Fragen der Cybersicherheit zu verarbeiten. § 12 Absatz 2 stellt eine nach Artikel 6 Absatz 4 Variante 2 der Verordnung (EU) 2016/679 erforderliche Rechtsgrundlage für diese Weiterverarbeitungen dar. Die Cybersicherheitsagentur muss in der Lage sein, zur Erfüllung ihrer Aufgaben aus § 3 alle ihr aus öffentlichen, privaten, staatlichen, bekannten oder anonymen Quellen erlangten und zur Verfügung gestellten Daten auszuwerten, um vor möglichen Cybersicherheitsrisiken zu warnen und entsprechende Sicherheitsvorkehrungen, insbesondere zum Schutz des Landes, zu entwerfen oder zu etablieren, um die öffentliche Sicherheit sowie den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses sicherzustellen. Hierzu ist allerdings auch eine Interessenabwägung erforderlich. § 12 Absatz 2 bezieht sich nur auf Verarbeitungen außerhalb des Anwendungsbereiches von spezialgesetzlichen Regelungen. Soweit z. B. der Anwendungsbereich des § 5 eröffnet ist, gilt § 5 Absatz 5 als lex specialis.

Zu Absatz 3

In Absatz 3 wird die Verarbeitung besonderer Kategorien personenbezogener Daten geregelt. Grundsätzlich verarbeitet die Cybersicherheitsagentur keine besonderen Kategorien personenbezogener Daten. Es ist jedoch nicht auszuschließen, dass dies im Einzelfall vorkommt. Sofern für die Cybersicherheitsagentur im konkreten Einzelfall keine andere Mög-

lichkeit besteht, eine Aufgabe aus § 3 zu erfüllen, ermöglicht Absatz 3 der Cybersicherheitsagentur auf Grundlage des Artikels 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 die (Mit-) Verarbeitung dieser Daten. Zum Schutz besonderer Kategorien personenbezogener Daten ist hierfür ein erhebliches öffentliches Interesse erforderlich. Ein erhebliches öffentliches Interesse liegt insbesondere bei Hilfe-, Beratungs- und Unterstützungsleistungen eines Cybersicherheitsvorfalls in der Landesverwaltung vor. Im Einzelfall kann ein erhebliches öffentliches Interesse jedoch auch bei Schadens- oder Störfällen in anderen Bereichen nicht vollständig ausgeschlossen werden. Die Interessen der von der Verarbeitung betroffenen Person werden vor der Verarbeitung besonderer Kategorien personenbezogener Daten darüber hinaus durch das Erfordernis einer zusätzlichen Verhältnismäßigkeitsprüfung besonders geschützt. Erst wenn die Cybersicherheitsagentur im konkreten Einzelfall zu dem Ergebnis gelangt, dass die nicht zu vermeidende Verarbeitung der personenbezogenen Daten besonderer Kategorien keine unverhältnismäßige Beeinträchtigung der betroffenen Person darstellt, ist eine Datenverarbeitung zulässig.

Zu Absatz 4

Absatz 4 regelt, dass zum Schutz der betroffenen Person die Cybersicherheitsagentur angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person nach § 3 LDSG vorsieht. Hierzu zählt neben § 3 Absatz 1 Satz 2 Nummer 2 LDSG (Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind) und Nummer 5 (Pseudonymisierung personenbezogener Daten) auch die Anonymisierung personenbezogener Daten, soweit dies angemessen ist und die Aufgabenwahrnehmung nicht gefährdet.

Zu Teil 4 Schlussvorschriften

Zu § 13 – Rechtsverordnungen

§ 13 ermächtigt das Innenministerium im Einvernehmen mit dem IT-Rat Baden-Württemberg zum Erlass von konkretisierenden Rechtsverordnungen, weil in den Rechtsverordnungen ausschließlich Regelungen im Bereich der öffentlichen Sicherheit und Ordnung getroffen werden.

Nummer 1 ermächtigt Standards für die Informationssicherheit zu regeln. Dies ermöglicht insbesondere, die VwV Informationssicherheit zu aktualisieren und – der Erweiterung des Anwendungsbereichs auf Personen des Privatrechts nach § 2 Absatz 1 Satz 2 angepasst – durch Rechtsverordnung zu regeln.

Nummer 2 ermächtigt zum Erlass einer Rechtsverordnung, um darin das Nähere über die Standards für die Cybersicherheit nach § 3 Absatz 1 Nummer 3 einschließlich der Verfahren zur Überprüfung von Standards festzulegen. Dabei sind die nach § 17 des E-Government-Gesetzes Baden-Württemberg verbindlichen Standards zu beachten und Verfahren für deren Überprüfung zu regeln. Soweit vom BSI erarbeitete Sicherheitsstandards nicht bereits nach § 17 des E-Government-Gesetzes Baden-Württemberg für die Landesverwaltung verbindlich sind, können diese Standards durch Rechtsverordnung für verbindlich erklärt werden.

Nummer 3 ermächtigt das Nähere zu den Meldepflichten nach § 4 Absatz 3 zu regeln, weil davon auszugehen ist, dass infolge der Fortentwicklung der Technik unterschiedliche Ereignisse für die Cybersicherheit relevant sein werden. Mitumfasst ist die Regelung der Meldewege, die auch von der Entwicklung der technisch-organisatorischen Möglichkeiten der Cybersicherheitsagentur und der sonstigen Stellen des Landes abhängt.

Nummer 4 ermächtigt das Nähere zur Untersuchung der Sicherheit in der Informationstechnik nach § 7 zu regeln, um insbesondere das Verfahren der Cybersicherheitsagentur mit den betroffenen Stellen zu regeln.

Nummer 5 ermächtigt die ressortübergreifende Organisation im Bereich der Cyber- und Informationssicherheit zu regeln; insbesondere ist das Zusammenspiel der in Nummer 5 der VwV Informationssicherheit bereits geregelten Sicherheitsorganisation mit der neuen Cybersicherheitsagentur zu normieren.

Zu § 14 – Verwaltungsvorschriften

Das Innenministerium regelt die nähere Ausgestaltung zur Organisation und zum Betrieb der Cybersicherheitsagentur durch Verwaltungsvorschrift, weil die technische Fortentwicklung auch Anpassungen der Organisation und des Betriebs der Cybersicherheitsagentur erforderlich machen wird.

Zu § 15 – Berichtspflichten

Zu Absatz 1

Über die Berichtspflicht nach Absatz 1 wird sichergestellt, dass das Innenministerium als zuständige Aufsichtsbehörde der Cybersicherheitsagentur und der IT-Rat Baden-Württemberg über deren laufende Tätigkeit unterrichtet wird.

Zu Absatz 2

Die gesetzliche Verankerung einer Berichtspflicht und die vorgesehene Veröffentlichung eines Jahresberichts nach Absatz 2 dienen der Sensibilisierung der Öffentlichkeit für das Thema Cybersicherheit. Der Bericht ergänzt die fachlichen Informationsangebote der Cybersicherheitsagentur und trägt als Beitrag der Landesregierung zur Diskussion im politischen Raum bei. Da eine Vielzahl von Cyberangriffen bereits durch Basismaßnahmen abgewehrt werden könnte, spielt die Aufklärung und Sensibilisierung der Öffentlichkeit eine zentrale Rolle für die Erhöhung der Cybersicherheit in Baden-Württemberg. Dabei sind die Regelungen zu Warnungen, Empfehlungen und Hinweisen nach § 8 Absatz 1 Satz 3 und Absatz 2 entsprechend anzuwenden.

Zu § 16 – Einschränkung von Grundrechten

Durch die Befugnisse nach §§ 5, 6 und 7 wird in das Fernmeldegeheimnis aus Artikel 10 des Grundgesetzes eingegriffen. Durch § 16 wird dem Zitiergebot aus Artikel 19 Absatz 1 des Grundgesetzes Genüge getan.

Zu Artikel 2 bis 9 – Änderung anderer Vorschriften

Mit der Errichtung der Cybersicherheitsagentur als Landesoberbehörde sind auch die davon berührten Regelungen (Ernennungsgesetz, Landesbeamtengesetz, Landesbesoldungsgesetz Baden-Württemberg, E-Government-Gesetz Baden-Württemberg, Errichtungsgesetz BITBW, Unfallfürsorgezuständigkeitsverordnung und Bekanntmachung der Ministerien über die Vertretung des Landes in gerichtlichen Verfahren und förmlichen Verfahren vor den Verwaltungsbehörden) anzupassen.

Zu Artikel 2 – Änderung des BITBWG

Artikel 2 enthält eine Folgeänderung zu der durch Artikel 1 § 3 erfolgenden umfassenden Aufgabenzuweisung an die Cybersicherheitsagentur auf dem Gebiet der Cybersicherheit. Dementsprechend wird durch die Änderung von § 2 Absatz 1 Nummer 2 BITBWG die Aufgabe der BITBW zur Sicherstellung der Informationssicherheit, die bislang für die gesamte Landesverwaltung bestand, auf die von der BITBW betriebene zentrale informationstechnische Infrastruktur für die Landesverwaltung sowie auf die Erbringung der in § 2 Absatz 3 und 4 BITBWG geregelten Dienstleistungen beschränkt. Soweit die BITBW für diese Infrastruktur und diese Dienstleistungen zuständig ist, konzentriert sich die Zuständigkeit der

Cybersicherheitsagentur auf die Kontroll- und Unterstützungsfunktion im Einzelfall in Abstimmung mit der BITBW.

Zu Artikel 3 – Änderung des EGovG BW

Zu Nummer 1

In § 16 EGovG BW wird die Verweisung an die Paragrafenzählung des LDSG angepasst.

Zu Nummer 2 bis 4

Durch Nummer 2 bis 4 werden § 20 Absatz 4 Satz 1, § 22 Absatz 3 bzw. § 23 Absatz 2 Satz 3 Nummer 3 EGovG BW geändert, um die Cybersicherheitsagentur in die bestehende IT-Organisationsstruktur in Baden-Württemberg einzufügen. Die Cybersicherheitsagentur wird beratendes Mitglied im IT-Rat Baden-Württemberg und im Arbeitskreis Informationstechnik des IT-Rates Baden-Württemberg sowie stimmberechtigtes Mitglied des IT-Kooperationsrats Baden-Württemberg.

Zu Artikel 4 – Absehen von der Zusage der Umzugskostenvergütung in besonderen Härtefällen

Zur Abmilderung von besonderen Härtefällen bei Versetzungen im Zusammenhang mit dem Vollzug dieses Gesetzes wird auf Antrag zeitlich befristet von der Zusage der Umzugskostenvergütung abgesehen. Dies hat zur Folge, dass während einer Übergangszeit die Gewährung von Trennungsgeld noch nicht den Anforderungen unterliegt, die nach Zusage der Umzugskostenvergütung gestellt werden (uneingeschränkte Umzugswilligkeit, nachgewiesener Wohnungsmangel). Die Vorschrift entspricht inhaltlich beispielsweise dem Gesetz zur Umsetzung der Polizeistruktur 2020.

Zu Artikel 5 – Personalverwaltung

Der Cybersicherheitsagentur stehen für den mittleren und den gehobenen Dienst umfassend die in § 2 des Ernennungsgesetzes genannten Rechte zu.

Zu Artikel 6 – Änderung des Landesbesoldungsgesetzes Baden-Württemberg

Die besoldungsrechtliche Einstufung des Amtes der Präsidentin oder des Präsidenten der Cybersicherheitsagentur in der Besoldungsgruppe B 3 und der Vizepräsidentin oder des Vizepräsidenten der Cybersicherheitsagentur in der Besoldungsgruppe A 16 erfolgt entsprechend der Aufgabenstellung und Bedeutung der neu zu schaffenden Landesoberbehörde.

Zu Artikel 7 – Änderung der Unfallfürsorgezuständigkeitsverordnung

Ergänzung und Anpassung an die neuen Strukturen und Behördenbezeichnung.

Zu Artikel 8 – Änderung der Bekanntmachung der Ministerien über die Vertretung des Landes in gerichtlichen Verfahren und förmlichen Verfahren vor den Verwaltungsbehörden

Anpassung an die neue Bezeichnung bzw. Zuständigkeiten.

Zu Artikel 9 – Überprüfung der Auswirkungen des Gesetzes

Das Land errichtet erstmals eine zentrale Behörde für die Cybersicherheit in Baden-Württemberg. Vor einer Entscheidung darüber, ob und inwieweit sich dieses Gesetz in seiner Anwendung bewährt hat, sind die praktischen Erfahrungen auszuwerten.

Für eine Ex-post-Evaluation von Gesetzen wird eine Datenerhebung über einen Zeitraum von 3 bis 5 Jahren empfohlen (Ziekow/Debus/Piesker, Die Planung und Durchführung von Gesetzesevaluationen, 2013, S. 141).

Für eine verlässliche Datengrundlage ist eine Datenerhebung über einen Zeitraum von drei Jahren angezeigt.

Es wird zu prüfen sein, ob die Landesregierung mit der Durchführung eine Stelle des Landes oder ein externes Institut beauftragt.

Zu Artikel 10 – Änderung des ADV-Zusammenarbeitsgesetzes

Die Komm.ONE ist eine rechtsfähige Anstalt des öffentlichen Rechts (AöR) und beschafft, entwickelt und betreibt Verfahren der automatisierten Datenverarbeitung für kommunale

Körperschaften, deren Zusammenschlüsse und deren Unternehmen im Land. Träger der Komm.ONE AöR sind der Zweckverband 4IT und das Land, welches zu 12 Prozent am Stammkapital beteiligt ist. Organe der Komm.ONE sind der Vorstand sowie der Verwaltungsrat. Der Verwaltungsrat trifft seine Beschlüsse in Verwaltungsratssitzungen. § 5 Absatz 3 ADV-Zusammenarbeitsgesetz regelt die Beschlussfähigkeit des Verwaltungsrats. Die Anstaltssatzung enthält in § 8 darüber hinaus weitere Regelungen zum Geschäftsgang.

Die Anstaltssatzung darf nach § 2 Absatz 2 Satz 2 und Satz 4 ADV-Zusammenarbeitsgesetz mit Ausnahme des Anstaltsnamens inhaltlich nicht von den Regelungen des ADV-Zusammenarbeitsgesetzes abweichen.

Die Vorschriften des ADV-Zusammenarbeitsgesetz gehen von einer persönlichen Anwesenheit der Gremienmitglieder bei Beratung und Beschlussfassung aus. Es hat sich gezeigt, dass Situationen entstehen können, in denen eine Sitzung eines Verwaltungsgremiums mit persönlicher Anwesenheit der Gremienmitglieder aus schwerwiegenden Gründen nicht stattfinden kann, etwa bei einer Naturkatastrophe, einer Pandemie (wie aktuell die Corona-Pandemie) oder bei höherer Gewalt. Für diese Fälle soll nun durch eine Regelung im ADV-Zusammenarbeitsgesetz die Möglichkeit eröffnet werden, durch eine entsprechende Vorschrift in der Anstaltssatzung zu bestimmen, dass in diesen Fällen notwendige Sitzungen des Verwaltungsrats oder beschließender Ausschüsse ohne persönliche Anwesenheit der jeweiligen Mitglieder in Form einer Videokonferenz oder auf vergleichbare Weise durchgeführt werden können.

Diese Form der Durchführung von Sitzungen ist auf Ausnahmefälle zu beschränken und kann nicht die herkömmliche Arbeit des Verwaltungsrats in Form von Präsenzsitzungen ersetzen. Mit der Gesetzesänderung soll die dauerhafte Handlungsfähigkeit des Gremiums gewährleistet werden.

Die Erfüllung der für eine ordnungsgemäße Durchführung der Sitzung einschließlich Beratung und Beschlussfassung erforderlichen technischen Anforderungen und datenschutzrechtlichen Voraussetzungen ist sicherzustellen. Die für den Geschäftsgang von Sitzungen des Verwaltungsrats geltenden Regelungen bleiben unberührt. Insoweit ergeben sich im Vergleich zu der Durchführung von Gremiensitzungen in der herkömmlichen Form, d. h. mit persönlicher Anwesenheit der Mitglieder im Sitzungsraum, keine grundsätzlichen Änderungen. Allerdings dürfen in einer Sitzung nach Absatz 3a Satz 1 keine Wahlen im Sinne von Absatz 2 Satz 3 durchgeführt werden, da die grundsätzliche Möglichkeit offengehalten werden muss, diese Wahlen in geheimer Abstimmung durchzuführen, was bei Durchführung einer Sitzung per Videokonferenz oder auf vergleichbare Weise nicht gewährleistet werden kann.

Für den Fall, dass beschließende Ausschüsse nach § 5 Absatz 4 ADV-Zusammenarbeitsgesetz gebildet werden, soll die Regelung auf diese entsprechende Anwendung finden.

Durch die Gesetzesänderung entstehen für den Landeshaushalt unmittelbar keine Kosten. Technische Verfahren für eine Teilnahme der Vertreter des Landes an den Sitzungen des Verwaltungsrats der Komm.ONE sind in der Landesverwaltung bereits vorhanden.

Sofern die Komm.ONE von der Möglichkeit Gebrauch macht, Sitzungen in Form von Videokonferenzen oder vergleichbaren Verfahren durchzuführen, können der Komm.ONE insbesondere Kosten für die technische Umsetzung dieser Verfahren entstehen. Die erforderlichen Systeme sollten weitestgehend vorhanden sein.

Zu Nummer 1

Für schwerwiegende Ausnahmefälle soll gesetzlich die Möglichkeit eröffnet werden, durch Bestimmung in der Anstaltssatzung der Komm.ONE AöR zuzulassen, dass notwendige Sitzungen des Verwaltungsrats ohne persönliche Anwesenheit der Ratsmitglieder in Form einer Videokonferenz oder auf vergleichbare Weise durchgeführt werden können. Für eine Änderung der Anstaltssatzung sind ein übereinstimmender Beschluss der Anstaltsträger Land Baden-Württemberg und Zweckverband 4IT erforderlich.

Ein gegenseitiger Austausch der Verwaltungsratsmitglieder bei Beratung und Beschlussfassung durch Bildübertragung muss dabei gewährleistet sein. Eine die Mimik und Gestik einbeziehende Kommunikation trägt erheblich zu einem sachgerechten und qualifizierten Austausch bei. Eine Sitzung ohne Bildübertragung (etwa eine reine Telefonschaltkonferenz, bei der eine Identifikation der beteiligten Personen nicht zweifelsfrei möglich ist) soll daher nicht zulässig sein. Im Übrigen wird auf den Allgemeinen Teil der Begründung zu Artikel 10 verwiesen.

Zu Nummer 2

Die Regelung sorgt für die Möglichkeit einer entsprechenden Anwendung der Regelung nach Nummer 1 auf beschließende Ausschüsse.

Zu Artikel 11 – Inkrafttreten

Artikel 11 regelt das Inkrafttreten des Gesetzes.