Landtag von Baden-Württemberg **Drucksache 16 / 9490**

16. Wahlperiode **08. 12. 2020**

Gesetzentwurf

der Landesregierung

Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften

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.

Eingegangen: 08. 12. 2020 / Ausgegeben: 07. 01. 2021

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 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 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 ein geringfügiger Erfüllungsaufwand, wenn Hersteller oder Inverkehrbringer vor Veröffentlichung einer Warnung nach Artikel 1 § 8 angehört werden.

E.3 Erfüllungsaufwand für die Verwaltung

Bei der Verwaltung entsteht insgesamt ein einmaliger Erfüllungsaufwand in Höhe von 2 036 128 Euro. Dabei handelt es sich bei 261 128 Euro um Personalaufwand und bei 1 775 000 Euro um Sachaufwand. Zudem entsteht ein jährlicher Erfüllungsaufwand in Höhe von 8 311 104 Euro. Davon sind 6 898 104 Euro Personalaufwand und 1 413 000 Euro Sachaufwand.

Nachrichtlich wird darauf hingewiesen, dass – abweichend von der bisherigen Methode – der Erfüllungsaufwand durch Gesetze zukünftig gemäß Beschluss des Ministerialdirektorenausschusses für Bürokratieabbau vom 4. November 2020 und der darin vorgesehenen länderspezifischen Anpassung der Folgekostenberechnung darzustellen sein wird. Danach wäre ein Erfüllungsaufwand für die Verwaltung durch dieses Gesetz in Höhe von einmalig 15 200 Euro und jährlich 12 200 Euro zu prognostizieren. Weitere Folgekosten sind bereits in den Angaben

zu den Auswirkungen auf den Landeshaushalt ausgewiesen, weshalb ein darüber hinausgehendes Transparenzinteresse entfällt.

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.

Staatsministerium
Baden-Württemberg
Ministerpräsident

Stuttgart, 8. Dezember 2020

An die
Präsidentin des Landtags
von Baden-Württemberg

Sehr geehrte Frau Landtagspräsidentin,

als Anlage übersende ich Ihnen gemäß Artikel 59 Absatz 1 der Verfassung des Landes Baden-Württemberg den von der Landesregierung beschlossenen Entwurf eines Gesetzes zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften. Ich bitte Sie, die Beschlussfassung des Landtags herbeizuführen. Die Zuständigkeit liegt beim Ministerium für Inneres, Digitalisierung und Migration.

Mit freundlichen Grüßen

Kretschmann
Ministerpräsident

Der Landtag wolle beschließen,

dem nachstehenden Gesetzentwurf seine Zustimmung zu erteilen:

Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften

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 Landratsämter als untere Verwaltungsbehörden und 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 Kommunikationsvorgangs 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. zentrale 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 nach § 20 Absatz 1 des E-Government-Gesetzes Baden-Württemberg eingerichteten 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 behindert 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. Mai 2016, S. 1, zuletzt ber. ABl. L 127 vom 23. Mai 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 dem Hersteller 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. Bei Maßnahmen der Cybersicherheitsagentur nach § 6 haben 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 des Herstellers 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 dem Hersteller 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 vor 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 des Herstellers oder Inverkehrbringers 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 den Hersteller oder Inverkehrbringer 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 den Hersteller oder Inverkehrbringer 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 zugrunde liegenden Umstände als unrichtig wiedergegeben heraus, so ist dies unverzüglich zu veröffentlichen. 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.

(6) Die Informationen nach Absatz 1 sind einschließlich zusätzlicher Informationen nach Absatz 5 sechs Monate nach der Veröffentlichung nach Absatz 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, einer oder einem Bediensteten der Cybersicherheitsagentur mit Befähigung zum Richteramt sowie der oder dem behördlichen Datenschutzbeauftragten der Cybersicherheitsagentur 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. Satz 1 bis 3 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 4 sowie 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 Errichtungsgesetzes BITBW

In § 2 Absatz 1 Nummer 2 des Errichtungsgesetzes BITBW vom 12. Mai 2015 (GBl. S. 326), das durch Artikel 3 des Gesetzes vom 15. Oktober 2020 (GBl. S. 912, 913) 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 E-Government-Gesetzes Baden-Württemberg

Das E-Government-Gesetz Baden-Württemberg vom 17. Dezember 2015 (GBl. S. 1191), das zuletzt durch Artikel 3 des Gesetzes vom 15. Oktober 2020 (GBl. S. 913) 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 oder einer Gleichstellung nach § 2 Absatz 3 des Neunten Buches Sozialgesetzbuch das 58. Lebensjahr, vollendet hat oder

   b) einen dienstunfallrechtlich festgestellten Grad der Schädigungsfolgen (GdS) von mindestens 50 vom Hundert vorweist 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 einem Betreuungsangebot lebt, 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 61. Lebensjahr, im Falle einer Schwerbehinderung im Sinne des § 2 Absatz 2 des Neunten Buches Sozialgesetzbuch oder einer Gleichstellung nach § 2 Absatz 3 des Neunten Buches Sozialgesetzbuch das 58. 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. Als Voraussetzung nach Absatz 1 Satz 1 Nummer 1 Buchstabe b gilt eine Minderung der Erwerbsfähigkeit um mindestens 50 vom Hundert im Sinne des § 56 Absatz 2 des Siebten Buches Sozialgesetzbuch oder eine Erwerbsminderung im Sinne des § 43 des Sechsten Buches Sozialgesetzbuch.

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, die Beamtinnen und Beamten im höheren Dienst vergleichbar sind, 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 (...) vom (...) (GBl. S. ...) 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), die zuletzt durch Artikel 22 des Gesetzes vom 21. Mai 2019 (GBl. 161, 188) geändert worden ist, 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 3 a eingefügt:

   „(3 a) 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 3 a 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.

Begründung

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 Regelun-

gen 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 des Herstellers oder des Inverkehrbringers 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 ein Erfüllungsaufwand, wenn Hersteller oder Inverkehrbringer vor Veröffentlichung einer Warnung nach Artikel 1 § 8 angehört werden.

c) Erfüllungsaufwand für die Verwaltung

Bei der Verwaltung entsteht insgesamt ein einmaliger Erfüllungsaufwand in Höhe von 2 036 128 Euro. Dabei handelt es sich bei 261 128 Euro um Personalaufwand und bei 1 775 000 Euro um Sachaufwand. Zudem entsteht ein jährlicher Erfüllungsaufwand in Höhe von 8 311 104 Euro. Davon sind 6 898 104 Euro Personalaufwand und 1 413 000 Euro Sachaufwand.

Der einmalige Erfüllungsaufwand wird maßgeblich durch die Kosten für die bauliche Ertüchtigung und die Einrichtung der von der Cybersicherheitsagentur genutzten Räumlichkeiten bestimmt. Der einmalige Sachaufwand, insbesondere für bauliche Maßnahmen inklusive Nebenkosten, beträgt 1 775 000 Euro. In diesem Zusammenhang wird für die Projektsteuerung ein einmaliger Personalaufwand in Höhe von 42 600 Euro geschätzt. Diesem Wert liegt die Annahme zugrunde, dass für diese Tätigkeit ca. 3 % des oben genannten Sachaufwandes (abzüglich der Nebenkosten von 20 % des Gesamtwertes) zu veranschlagen sind (1 775 000 Euro x 80 % x 3 %).

Die Personalrekrutierung für die Cybersicherheitsagentur führt im Jahr 2020 zu einem einmaligen Personalaufwand in Höhe von 72 787 Euro (je eine Person des höheren Dienstes [933 Std. x 60,5 Euro pro Std.] sowie des gehobenen Dienstes [400 Std. x 40,8 Euro pro Std.]. Beide Personen sind erst im Verlauf des Jahres 2020 tätig geworden).

Der jährliche Erfüllungsaufwand bei der Cybersicherheitsagentur selbst setzt sich zusammen aus einem Personalaufwand in Höhe von 6 875 360 Euro sowie einem Sachaufwand in Höhe von 1 413 000 Euro.

Der Personalaufwand wird abweichend vom haushaltsrechtlichen Ansatz mit der Methodik und den Lohnsätzen aus dem „Leitfaden zur Ermittlung und Darstellung des Erfüllungsaufwands“ des Bundes bewertet. Die zugrundeliegende Anzahl der Stellen stimmt bei beiden Ansätzen überein. Es handelt sich hierbei um 51 Stellen im höheren Dienst, 22 Stellen im gehobenen Dienst sowie 10 Stellen im mittleren Dienst. Daraus ergibt sich der Personalaufwand in Höhe von 6 875 360 Euro ([(51 x 60,50 Euro pro Std.) + (22 x 40,80 Euro pro Std.) + (10 x 31,40 Euro pro Std.)] x 1 600 Std.).

Für den Sachaufwand werden entsprechend dem Haushaltsansatz 1 413 000 Euro pro Jahr veranschlagt. Berücksichtigt sind hier insbesondere Ausgaben für Geschäftsbedarf sowie Geräte, Ausstattungs- und Ausrüstungsgegenstände und sonstige Gebrauchsgegenstände, Veröffentlichungen und sonstige Öffentlichkeitsarbeit, Veranstaltungen, Konferenzen, Bewirtungskosten, Fortbildung.

Insgesamt ergibt sich damit für den laufenden Betrieb bei der Cybersicherheitsagentur selbst ein Erfüllungsaufwand in Höhe von 8 288 360 Euro.

Nachfolgend werden die Vorgaben aufgeführt, bei denen unabhängig von den obigen Ausführungen nennenswerte Belastungen bei anderen Verwaltungseinrichtungen prognostiziert werden:

Beim Innenministerium Baden-Württemberg entsteht für die Ausübung der Dienst- und Fachaufsicht über die Cybersicherheitsagentur nach Artikel 1 § 1 Absatz 3 ein jährlicher Personalaufwand in Höhe von rund 10 588 Euro (175 Std. x 60,50 Euro pro Std.). Dies entspricht 175 Stunden im höheren Dienst.

Nach Artikel 1 § 2 Absatz 2 wird die Cybersicherheitsagentur mit den obersten Landesbehörden (z. B. die oder der Landesdatenschutzbeauftragte, der Rechnungshof, das Ministerium für Finanzen) für sich bzw. deren nachgeordnete Stellen mit Sonderstatus gesonderte Vereinbarungen zur Zusammenarbeit treffen. Es wird von 6 Vereinbarungen insgesamt ausgegangen. Bei einem Zeitauf-

wand von 40 Stunden pro Vereinbarung bei den obersten Landesbehörden entsteht ein einmaliger Personalaufwand in Höhe von 12 156 Euro (6 x [(20 Std. x 60,50 Euro pro Std.) + (20 Std. x 40,80 Euro pro Std.)]).

Nach Artikel 1 § 4 Absatz 1 wird die Cybersicherheitsagentur die zentrale Koordinierungs- und Meldestelle für die Zusammenarbeit der öffentlichen Stellen in Angelegenheiten der Cybersicherheit in Baden-Württemberg sein. Die durch das Regelungsvorhaben notwendig werdenden Anpassungen werden hauptsächlich die 4 Rechenzentren im Land, nicht jedoch die einzelnen Stellen in der Verwaltung betreffen. In den Rechenzentren ist ein einmaliger Umstellungsaufwand in Höhe von 0,5 Vollzeitäquivalenten des gehobenen Dienstes für jeweils 1 Jahr zu erwarten. Dies führt zu einem einmaligen Personalaufwand in Höhe von 130 560 Euro (4 x 800 Std. x 40,80 Euro pro Std.). Diesem Aufwand steht eine qualitative Erhöhung des Sicherheitsniveaus gegenüber.

Die Cybersicherheitsagentur kann entsprechend Artikel 1 § 7 Absatz 1 die Sicherheit der Informationstechnik der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen untersuchen und bewerten. Durch die Mitwirkung entsteht bei diesen Stellen ein Personalaufwand. Zielgröße ab dem Jahr 2022 sind ca. 6 Untersuchungen und Bewertungen pro Jahr. Bei einem Zeitaufwand von 40 Stunden pro Stelle für die Mitwirkung entsteht ein jährlicher Personalaufwand in Höhe von 12 156 Euro (6 x [(20 Std. x 60,50 Euro pro Std.) + (20 Std. x 40,80 Euro pro Std.)]).

Nach Artikel 9 sind die Auswirkungen dieses Gesetzes nach drei Jahren durch die Landesregierung unter Mitwirkung der kommunalen Landesverbände, der oder des Landesbeauftragten für den Datenschutz und gegebenenfalls weiterer sachverständiger Personen zu überprüfen. Bei den ungefähr 5 mitwirkenden Stellen ist jeweils ein Zeitaufwand in Höhe von ca. 10 Stunden zu erwarten. Dies führt zu einem einmaligen Personalaufwand in Höhe von 3 025 Euro (5 x 10 Std. x 60,50 pro Std.).

Nachrichtlich wird darauf hingewiesen, dass – abweichend von der bisherigen Methode – der Erfüllungsaufwand durch Gesetze zukünftig gemäß Beschluss des Ministerialdirektorenausschusses für Bürokratieabbau vom 4. November 2020 und der darin vorgesehenen länderspezifischen Anpassung der Folgekostenberechnung darzustellen sein wird. Danach wäre ein Erfüllungsaufwand für die Verwaltung durch dieses Gesetz in Höhe von einmalig 15 200 Euro und jährlich 12 200 Euro zu prognostizieren. Weitere Folgekosten sind bereits in den Angaben zu den Auswirkungen auf den Landeshaushalt ausgewiesen, weshalb ein darüberhinausgehendes Transparenzinteresse entfällt.

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 einerseits die Stellen des Landes sowie andererseits die 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 die sonstigen juristischen Personen des öffentlichen Rechts.

Stellen des Landes sind nur unmittelbar staatliche Stellen wie der Landtag, Gerichte und Staatsanwaltschaften, die obersten Landesbehörden, Landesoberbehörden, Regierungspräsidien und besondere Verwaltungsbehörden im Sinne der §§ 23 ff. des Landesverwaltungsgesetzes.

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. Mai 2016, S. 1; L 314 vom 22. November 2016, S. 72; L 127 vom 23. Mai 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.

Die Formulierung der „sonstigen Stellen des Landes“ nimmt Bezug auf die bereits in Absatz 1 verwendete Kategorie der „Stelle des Landes“. Nicht erfasst sind damit die ebenfalls in Absatz 1 daneben genannten „Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts“.

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 geregelt werden.

Zu Absatz 3

Absatz 3 nimmt die Landratsämter als untere Verwaltungsbehörden von den Regelungen aus, die ausschließlich für Stellen des Landes gelten. Sie werden wie die sonstigen öffentlichen Stellen, insbesondere die Stellen der Gemeinden und Gemeindeverbände, behandelt, um das Landratsamt in seiner Doppelfunktion nicht unterschiedlichen Regelungssystemen zu unterstellen.

Um der besonderen Situation von Beliehenen gerecht zu werden, sind auf diese die für die öffentlichen Stellen des Landes geltenden Regelungen nicht anzuwenden.

Im Übrigen ergibt sich die Zuordnung der öffentlichen Stellen zum Land aus den allgemeinen Regelungen.

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 öffentlichen 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 weiter-

gegeben 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 (Verschlusssachen-)Bereich des Landes beschränkt ist, hat der Hersteller 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), die aus den Informationssicherheitsbeauftragten der Ressorts gebildet ist, 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 des IT-Rates Baden-Württemberg (AK-IT, § 22 E-Government-Gesetz Baden-Württemberg). 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 Planungsrat für die IT-Zusammenarbeit der öffentlichen Verwaltung zwischen Bund und Ländern (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 Verfassungs-

schutz 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 Cybersicherheitsvorfällen 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 weitergegeben 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 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 Schadeneintritts 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, WebProxys 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, sodass 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 Übermittlung 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, sodass 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 Informationssicherheit 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 bereit erklärt 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 Hersteller 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 der Hersteller des jeweilige Produkts schnell und nachhaltig zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit beitragen – etwa durch das zeitnahe Bereitstellen eines Sicherheitspatches.

Aus Gründen der Verhältnismäßigkeit darf der Hersteller nicht zur kostenlosen Mitwirkung herangezogen werden, wenn die ersuchende Stelle Soft- oder Hardware einsetzt, deren Supportzeitraum bereits abgelaufen ist, und der Hersteller das Ende des Supportzeitraumes rechtzeitig angekündigt hat. Die Mitwirkungspflicht des Herstellers bleibt davon unberührt. Im Falle einer Weigerung des Herstellers 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 kleine Einrichtungen, deren besondere politische, wirtschaftliche oder gesellschaftliche Bedeutung im Fall eines erheblichen Angriffs ein Eingreifen der Cybersicherheitsagentur erforderlich erscheinen lässt. Insbesondere in ländlichen Gebieten kann selbst eine einzelne Apotheke oder Arztpraxis eine solche Bedeutung haben.

Zu Satz 2

Nach Satz 2 kann – abweichend von Absatz 4 in Verbindung mit § 5 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 informationstech-

nischen 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 Herstellern 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 des Herstellers 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 dem Hersteller zuvor die Gelegenheit zu einer Stellungnahme einzuräumen. Wenn der Hersteller 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 des Herstellers oder des Inverkehrbringers 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 einem bestimmten Hersteller oder Inverkehrbringer 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 des Herstellers oder Inverkehrbringers 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 Hersteller oder Inverkehrbringer zu berücksichtigen.

Satz 3 berücksichtigt das in der IT-Wirtschaft geübte Prinzip der verantwortungsvollen Weitergabe („responsible disclosure“). Danach werden in der Regel zunächst die Hersteller oder Inverkehrbringer 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 Hersteller oder Inverkehrbringer 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 Herstellern und Inverkehrbringern 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), sodass 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 des Herstellers oder Inverkehrbringers weitgehend kompensiert. Ausnahmsweise bestehende Entschädigungsansprüche richten sich nach den allgemeinen Regelungen.

Zu Absatz 6

Die gesetzliche Löschungsfrist für Informationen 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. Mai 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: 1. Mai 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 Vier-Augen-Prinzip 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 Ermächtigungsgrundlage 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 Möglichkeit 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 4 sowie 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, 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 Errichtungsgesetzes BITBW

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 E-Government-Gesetzes 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 3 a 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.

C. Wesentliches Ergebnis der Anhörung

Folgende Verbände und Institutionen haben Stellungnahmen abgegeben:

- Arbeitsgemeinschaft der Schwerbehindertenvertretungen der obersten Landesbehörden Baden-Württemberg (AGSV BW)
- Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.
- Arbeitsgemeinschaft der Vorsitzenden der Hauptpersonalräte des Landes Baden-Württemberg (ARGE-HPR)
- Architektenkammer Baden-Württemberg
- Baden-Württembergischer Handwerkstag e. V.
- Baden-Württembergischer Industrie- und Handelskammertag e. V.
- BBW Beamtenbund Tarifunion
- Beauftragte der Landesregierung für die Belange von Menschen mit Behinderungen
- Chaos Computer Club Stuttgart
- EnBW Energie Baden-Württemberg AG
- evalag (Evaluationsagentur Baden-Württemberg)
- Hauptpersonalrat beim Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg
- Hauptschwerbehindertenvertretung der Polizei
- Hochschule Karlsruhe – Technik und Wirtschaft
- Karlsruher Institut für Technologie (KIT)

– Kommunale Landesverbände (Gemeindetag Baden-Württemberg, Städtetag Baden-Württemberg und Landkreistag Baden-Württemberg)
– Landesbeauftragter für den Datenschutz und die Informationsfreiheit
– Landesrektorenkonferenz Baden-Württemberg
– Landesstudierendenvertretung Baden-Württemberg
– Landesverband Baden-Württemberg der Deutschen Polizeigewerkschaft (DPolG)
– Landesverband Baden-Württemberg des Bundes Deutscher Kriminalbeamter
– Normenprüfungsausschuss
– Rechnungshof Baden-Württemberg
– Rechtsanwaltskammern Freiburg, Karlsruhe, Stuttgart und Tübingen
– Steuerkreis zur Informationssicherheit der Universitäten und Hochschulen des Landes Baden-Württemberg
– Universitätsklinikum Tübingen
– Universitätsklinikum Ulm

1. Allgemein

a) Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Der Anwaltsverband habe Verständnis für das politische Anliegen, auf die fortschreitende Digitalisierung vieler Prozesse in der Landesverwaltung, der Wirtschaft, aber auch bei Verbraucherhandeln und damit auf deren Gefährdung durch digitale Angriffe, wie Schadsoftware o. ä. mit der Errichtung einer Cybersicherheitsagentur für Baden-Württemberg (bei einem ganzheitlichen Ansatz) zu reagieren. Er erkenne dabei – wegen des Ziels, sich jeweils ein Lagebild in diesem Bereich zu verschaffen – Ähnlichkeiten zum Landesverfassungsschutz, aber hinsichtlich der geplanten Beratungs- und Prüfaufgaben zum Bundesamt für Sicherheit in der Informationstechnik (BSI). Aufgrund der beabsichtigten Befugnisse komme der geplanten Cybersicherheitsagentur auch der Charakter einer speziellen Polizeibehörde zu, die sowohl präventiv zur Gefahrenabwehr, aber auch repressiv ermittelnd im strafrechtlichen Sinn tätig werden solle. Dies werde letztlich auch durch die Einbindung in den Geschäftsbereich des Innenministeriums sowie die besoldungsrechtliche Einstufung des zukünftigen Behördenleiters (Präsidenten) ähnlich einem Polizeipräsidenten zum Ausdruck gebracht.

Haltung der Landesregierung

Die Cybersicherheitsagentur soll nicht repressiv ermittelnd im strafrechtlichen Sinne tätig werden. Sie verfügt über keine dementsprechenden Befugnisse.

Die Befugnisse der geplanten Cybersicherheitsagentur würden also weit mehr umfassen als beispielsweise die des BSI.

Der Anwaltsverband sei deswegen skeptisch, ob eine klare Aufgabentrennung zu den Zuständigkeitsbereichen anderer Einrichtungen, etwa dem LfV, der BITBW oder dem BSI, gelingen könne. So betreibe beispielsweise schon das BSI die Entwicklung von Standards und Sicherheitsvorkehrungen und biete Information und Beratung für Unternehmen und Verbraucher an.

Es sei richtig, eine primäre Zuständigkeit für Landesbehörden und ihnen nachgeordnete öffentliche Stellen vorzusehen, aber die gewonnenen Erkenntnisse auch Unternehmen und Privatpersonen zur Verfügung zu stellen. So könne ein Mehrwert der für die Aufgabenerfüllung eingesetzten Steuermittel generiert werden.

Haltung der Landesregierung

Die ressortübergreifende Organisation im Bereich der Cyber- und Informationssicherheit soll durch eine Rechtsverordnung nach § 13 Nummer 5 CSG konkretisiert werden.

In der Gesetzesbegründung werde für den Laien zu viel fachspezifisches Wissen vorausgesetzt. So wäre es wünschenswert, die jeweils beteiligten Kreise, wie IT-Rat BW[1], BIT BW (Landesoberbehörde IT Baden-Württemberg im Geschäftsbereich des Innenministeriums), AK-IT[2], KG InfoSic[3], IT-Planungsrat[4] oder KoSt KRITIS[5] , deren Zusammensetzung und Kompetenzen, kurz zu erläutern, damit der Bürger erkennen könne, wozu deren Stellung hier jeweils hilfreich sein könne. Die Begründung eines Gesetzes soll nicht lediglich den mit der Materie in der Regel vertrauten Abgeordneten des Landtags Sinn und Zweck der Normen erschließen, sondern auch dem Bürger die nötige Transparenz vermitteln und so die Akzeptanz erhöhen. Überdies sei nicht auszuschließen, dass sich Zusammensetzung und Kompetenzen der in Bezug genommenen Gremien/Institutionen im Laufe der Zeit ändern, so wie das z. B. beim IT-Planungsrat geschehen sei. Dann sollten sich aber auch mögliche Auswirkungen auf die Arbeit der Cybersicherheitsagentur bzw. den hiesigen Gesetzestext erkennen lassen.

Haltung der Landesregierung

In Wortlaut zu § 5 Absatz 1 Satz 3 CSG wurde der Hinweis auf die Einrichtung des IT-Rates Baden-Württemberg nach § 20 Absatz 1 des E-Government-Gesetzes Baden-Württemberg ergänzt. Im Übrigen wurden Erläuterungen bei der ersten Verwendung in der Gesetzesbegründung ergänzt.

Angesichts des ehrgeizigen Zeitplans für den Aufbau der Cybersicherheitsagentur noch in 2020 bzw. 2021 fragt der Anwaltsverband, ob überhaupt ausreichend Fachkräfte zur Verfügung stehen würden.

Haltung der Landesregierung

Insbesondere im Hinblick auf die aktuell unsichere wirtschaftliche Lage konnten bereits viele Personen aus der Privatwirtschaft oder nach dem Studium eingestellt werden.

Der Anwaltsverband bemängelt, dass für die in § 5 CSG geregelten Befugnisse der Cybersicherheitsagentur im Rahmen der Gefahrenabwehr – abgesehen von der Datenerhebung und -verarbeitung – in der Gesetzesbegründung keinerlei Beispiele genannt seien, an welche Anordnungen und Maßnahmen hier gedacht werde. Zwar sei das Verfahren mit Fristsetzung und Verhältnismäßigkeitsanforderungen näher beschrieben, aber nicht, was die Betroffenen erwarten könne.

Nachdem es nun schon einige Jahre Erfahrungen mit empfehlenswerten Maßnahmen gebe, z. B. seitens des BSI, könne erwartet werden, dass solche Maßnahmen auch beispielhaft in der Gesetzesbegründung aufgeführt würden.

---

[1] Der IT-Rat Baden-Württemberg setze sich zusammen aus dem CIO (Beauftragter der Landesregierung für Informationstechnologie) als Vorsitzendem, den Amtschefinnen und Amtschefs der Ministerien sowie weiteren beratenden Mitgliedern. Er sei damit ressortübergreifend.

[2] Arbeitskreis Informationstechnik des IT-Rates Baden-Württemberg.

[3] Koordinierungsgruppe Informationssicherheit des Landes Baden-Württemberg.

[4] Der IT-Planungsrat sei das zentrale Gremium für die föderale Zusammenarbeit in der Informationstechnik. Der Vorsitz im IT-Planungsrat wechsele seit 2010 jährlich zwischen Bund und Ländern, wobei die Länder in alphabetischer Reihenfolge den Vorsitz übernehmen würden.

[5] Koordinierungsstelle kritische Infrastrukturen beim Innenministerium BW.

Haltung der Landesregierung

Auf Beispiele, die technisch schnell nicht mehr aktuell sind, wurde in der Gesetzesbegründung verzichtet.

b) Architektenkammer Baden-Württemberg

Die Architektenkammer befürwortet und unterstützt die Landesregierung darin, mit der Einrichtung einer Cybersicherheitsagentur in Baden-Württemberg die Cybersicherheit zu verbessern.

c) Baden-Württembergischer Handwerkstag e. V.

Das Handwerk begrüßt die Vorkehrungen des Landes, zur Verbesserungen der Cybersicherheit. Als Körperschaften des öffentlichen Rechts seien viele Handwerksorganisationen unmittelbar von der Einführung der Cybersicherheitsagentur betroffen. Die Handwerkskammern, Innungen und Kreishandwerkerschaften seien somit nach § 2 Absatz 1 Satz 1 CSG „öffentliche Stelle“ im Sinne des Gesetzesentwurfs. Durch die Vorgaben unterständen die Handwerksorganisationen unmittelbar dem Wirkungskreis der Cybersicherheitsagentur. Zu bedenken bleibe, dass sich damit nicht nur die Schutzwirkung entfalte, sondern auch bürokratische Anforderungen und Meldepflichten auf die Organisationen zukomme. Über die Ausgestaltung der auf die Organisationen zukommenden Verpflichtungen könne noch keine Aussage getroffen werden, da diese bisher nicht bekannt seien. Zu bedenken bei der Umsetzung der neuen Aufgaben der Cybersicherheitsagentur sei, dass in den Kreishandwerkerschaften und Innungen die Personal- und Finanzausstattung oft wenig Spielraum gebe, deshalb müssen die künftig entstehenden Anforderungen an die Cybersicherheit und Meldepflichten bei Cybervorfällen so bürokratiearm und kostenneutral wie möglich ausgestaltet werden. Es wird darum gebeten, die vorgebrachten Bedenken beim Aufbau der Strukturen der Cybersicherheitsagentur zu berücksichtigen.

Haltung der Landesregierung

Verpflichtungen nach diesem Gesetz sind für Stellen des Landes und unmittelbar an das Landesverwaltungsnetz angeschlossene Stellen vorgesehen. Die berufsständischen Kammern sind aber keine Stellen des Landes, weil in § 2 Absatz 1 Satz 1 zwischen „Stellen des Landes“ und „Gemeinden und Gemeindeverbänden“ sowie den „sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts“ differenziert wird.

d) Baden-Württembergischer Industrie- und Handelskammertag e. V.

Die Sicherheit der Informationstechnik in Baden-Württemberg sei ein wichtiges Anliegen der Wirtschaft und Wissenschaft. Entsprechend fänden sich im Land eine Vielzahl von Unternehmen, Forschungseinrichtungen und Initiativen in diesem Feld.

Die Bündelung von Wissen, Infrastruktur und Fachkräften in einer zentralen Behörde könne dazu beitragen, im Krisenfall die Funktionsfähigkeit der öffentlichen Verwaltung sicherzustellen. Ebenso könne eine zentrale Stelle nach Vorbild der Bundesbehörde BSI auch die Bürgerinnen, die Bürger und die Wirtschaft in vorbeugender Weise unterstützen, etwa durch Sensibilisierung und Informationsbereitstellung.

Die baden-württembergischen Industrie- und Handelskammern (IHKs) begrüßen daher die Einrichtung einer Cybersicherheitsagentur grundsätzlich.

e) BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Der BBW weist ausdrücklich darauf hin, dass sich ihm nicht erschließe, weshalb statt der Einrichtung einer neuen Cybersicherheitsagentur nicht die schon be-

stehende Struktur gestrafft und an der gemeinsamen Schnittstelle, dem Landeskriminalamt, gebündelt werde. Dies erfolge auch vor dem Hintergrund, dass die Zuständigkeiten auf Bundes- und Länderebene nicht zersplittert werden sollten. Die Struktur der Cybersicherheit müsse in die vorhandenen Landes- und Bundesstrukturen integriert werden. Es wird daher angeregt, auf eine neue Landesoberbehörde zu verzichten und die mit dem Gesetz erhofften Mehrwerte beim Landeskriminalamt zu konzentrieren.

Von der BBW und seiner Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg, wird ausdrücklich begrüßt, dass die Landesregierung der Cybersicherheit in Baden-Württemberg eine höhere Bedeutung beimessen wolle. Allerdings sei der mit diesem Gesetzesentwurf eingeschlagenen Weg nicht optimal. Es sei zu erwarten, dass Aufbau und Wirkbetrieb der mit diesem Gesetzesentwurf begründeten Cybersicherheitsagentur lange Zeit in Anspruch nehmen würden. Dem Vernehmen nach sollten bis zum Wirkbetrieb mindestens 12 bis 18 Monate vergehen. Selbst dann dürfte der Aufbau andauern, bis vollwirksame personelle und technische Strukturen erreicht seien.

Hierauf könne nicht gewartet werden. Statt dem Aufbau neuer Strukturen und dem Aufbau einer neuen Cybersicherheitsarchitektur sollte daher die bestehende Struktur gestrafft und an der gemeinsamen Schnittstelle, dem Landeskriminalamt, gebündelt werden. Damit wäre in schnellstmöglicher Zeit eine effiziente Optimierung erreicht.

Haltung der Landesregierung

Parallel zum Gesetzgebungsverfahren sind schon wesentliche Vorarbeiten durchgeführt worden, um mit dem Betrieb der Cybersicherheitsagentur baldmöglichst zu beginnen.

Eine Bündelung aller Aufgaben beim Landeskriminalamt kommt nicht in Betracht, weil die Cybersicherheitsagentur auch nicht polizeiliche Aufgaben wie die Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen übernehmen soll. Überdies kann die Gewährleistung der Cybersicherheit nicht alleine von der Polizei geschultert werden. Im Bereich der Cyberkriminalität ist von einem hohen Dunkelfeld auszugehen, weil die betroffenen Opfer gar keine Anzeige erstatten. Vor diesem Hintergrund sind die bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme gewonnenen Erkenntnisse im Rahmen eines ganzheitlichen Ansatzes zur Verbesserung der Cybersicherheit erforderlich.

Stattdessen dürfte die Einrichtung einer neuen Landesoberbehörde zwangsläufig dazu führen, dass bestehende Strukturen durch Personalwechsel geschwächt würden, ohne dass im Gegenzug die neue Stelle diesen Personalabgang und den damit verbundenen Leistungsabfall sofort kompensieren könne. Ein aus seiner Sicht relevantes Sicherheitsdelta wäre die Folge. Bei der aktuellen und weiter steigenden Bedrohungslage im Bereich Cybercrime und hybride Bedrohungen sollte dies unbedingt vermieden werden.

Um es in einem Bild auszudrücken: Wir befänden uns in schwerer See. Statt aber die bestehenden Rettungsschiffe zu verstärken und einer zentralen Steuerung zu unterstellen, würden wir deren Personal abziehen und ließen diese in der Werft ein neues Rettungsschiff bauen, das Jahre brauchen werde, bis es in See stechen würde. Doch in der Zwischenzeit schlügen die Wellen weiter über uns herein. Angesichts der begrenzten Zuständigkeit, der ohnehin über die Corona-Maßnahmen erheblichen Neuverschuldung des Landes und insbesondere der Notwendigkeit sofort und schlagkräftig zu reagieren, wird daher anregt, auf die Einrichtung einer neuen Landesoberbehörde zu verzichten und die mit diesem Gesetz erhofften Mehrwerte beim Landeskriminalamt zu konzentrieren.

Haltung der Landesregierung

Inwieweit etwaige Personalwechsel zur Schwächung der bestehenden Strukturen führen, ist eine Frage des Einzelfalls. Angestrebt werden Vorteile für die wechselnden Personen, die abgebenden und die aufnehmenden Dienststellen. Wech-

selnde Personen tragen sich häufig mit dem Gedanken der Veränderung und daher bietet eine neue Tätigkeit häufig eine größere Motivation aufgrund einer Personalentwicklungsperspektive innerhalb der Landesverwaltung sowie eine starke Bindung zum Land als Dienstherrn. Eine solche Personalentwicklung kann damit die Abwanderung in die besser bezahlende freie Wirtschaft vermeiden. Die Vorteile der abgebenden und der aufnehmenden Dienststellen liegen in den Netzwerken zu den bisherigen Kolleginnen und Kollegen, die in beide Richtungen weiter genutzt werden können. Darüber hinaus bietet die angedachte Struktur allen Akteuren die Möglichkeit, sich ihren jeweiligen Kernaufgaben zu widmen und sich nicht mit neuen Aufgabenfeldern, die ggf. eine andere Zielrichtung haben, zu belasten. Darüber hinaus wird der Expertenpool der Landesverwaltung durch zeitlich befristete Abordnungen mit dadurch erfolgender Weiterqualifizierung der Beschäftigten insgesamt stetig anwachsen und so auch andere Dienststellen unterstützen. Auch wurden bislang lediglich zwei von insgesamt 25 Personen aus Bereichen der Landesverwaltung rekrutiert, die bislang mit der Cybersicherheit beschäftigt waren (Stand: 1. November 2020). Der größte Teil der Neueinstellungen kommt nicht aus der Landesverwaltung, sondern aus der freien Wirtschaft. Insbesondere im Hinblick auf die unsichere wirtschaftliche Lage konnten viele Personen aus der Privatwirtschaft oder nach dem Studium eingestellt werden.

Die Cybersicherheitsagentur soll ein Leuchtturm (= zentrale Koordinierungs- und Meldestelle nach § 4 CSG) werden, um den sichersten Weg aufzuzeigen, und sie soll auch die beschädigten Schiffe wieder flottmachen. Gemeinsam mit den bestehenden Rettungsschiffen und den zukünftigen Schnellbooten der Cybersicherheitsagentur (Mobile Incident Response Teams nach § 6 CSG) soll die Sicherheit im Cyberraum verbessert werden.

Darüber hinaus ließe dieser Gesetzesentwurf außer Acht, dass es weitere schlagkräftige Organisationen in der Bundesverwaltung gäbe, deren Expertise und Know-how sich bedient werden sollte. Beispielsweise sei ZETIS genannt, die mit hoher personeller und finanzieller Kompetenz Aufgaben durchführten, die nunmehr auch die Cybersicherheitsagentur für sich reklamiere. Statt Parallelstrukturen in einem weltweiten Bedrohungsszenario aufzubauen müssten stattdessen Kompetenzen zentralisiert werden. Das betreffe Landes- wie Bundesstrukturen gleichermaßen. Die Cybersicherheitsagentur führe zweifelsfrei zu einer weiteren Zerklüftung der Strukturen im Bereich Cybercrime, weil nun ein zusätzlicher Akteur eintreten solle, ohne dass die bisherigen entfielen. Es sei weitaus effektiver die Koordination unter den bisherigen Akteuren zu verbessern und bündeln.

Haltung der Landesregierung

Mit der Bundesverwaltung sind – im Rahmen des nach dem Föderalismusprinzip Zulässigen – Kooperationen geplant. Ausgehend davon, dass in dem Beispiel ZITiS statt ZETIS gemeint ist, hat ZITiS nach § 2 Absatz 1 Satz 1 des Erlasses über die Errichtung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich vom 6. April 2017 (GMBl. Seite 274) die „Aufgabe, Behörden des Bundes mit Sicherheitsaufgaben im Hinblick auf informationstechnische Fähigkeiten zu unterstützen und zu beraten.“ Die Cybersicherheitsagentur wird nicht für den Bund tätig, die ZITiS nicht für die Stellen des Landes Baden-Württemberg.

f) Beauftragte der Landesregierung für die Belange von Menschen mit Behinderungen

Mit Blick auf die fortschreitende Digitalisierung in allen Arbeits- und Lebensbereichen sei die notwendige strukturelle und qualitative Stärkung der Cybersicherheit vollumfänglich nachvollziehbar. Als Kompetenzzentrum zur Verbesserung der Cybersicherheit sollten im Kern die Landesoberbehörde Cybersicherheitsagentur Baden-Württemberg errichtet sowie deren Aufgaben und Befugnisse geregelt werden.

Genauso wichtig wie die Erhöhung der Effektivität und Effizienz staatlicher Aufgabenwahrnehmung im Bereich der Cybersicherheit sei bei der Schaffung der neuen Struktur und der damit verbundenen personalwirtschaftlichen Maßnahmen die Frage, wie dabei die spezifischen Belange der von einer Schwerbehin-

derung bzw. Gleichstellung betroffenen Mitarbeiterinnen und Mitarbeiter diskriminierungsfrei in dem Prozess der notwendigen räumlichen, organisatorischen und personellen Veränderungen berücksichtigt würden. Dabei sei in besonderer Weise die Verpflichtung aus der UN-Konvention über die Rechte von Menschen mit Behinderungen (UN-Behindertenrechtskonvention) mit Blick auf das Treffen sogenannter „angemessener Vorkehrungen" nach Artikel 2 der Konvention bei der Ausgestaltung der gesetzlichen Rahmenbedingungen für die Gestaltung des Personalübergangs zu berücksichtigen. Angemessene Vorkehrungen im Sinne der UN-Behindertenrechtskonvention seien notwendige und geeignete Änderungen und Anpassungen, die keine unverhältnismäßige oder unbillige Belastung darstellten und die in einem bestimmten Fall erforderlich seien um zu gewährleisten, dass Menschen mit Behinderungen gleichberechtigt mit anderen alle Menschenrechte und Grundfreiheiten genießen oder ausüben könnten. Dabei gehe die UN-Behindertenrechtskonvention in Artikel 2 zugleich davon aus, dass die Versagung „angemessener Vorkehrungen" eine Form der menschenrechtlich nicht zulässigen Diskriminierung darstelle.

Vor diesem Hintergrund begrüße sie grundsätzlich, dass zur sozialverträglichen Umsetzung der Gründung bzw. Einrichtung der neuen Landesoberbehörde Cybersicherheitsagentur Baden-Württemberg zur Abmilderung von besonderen Härtefällen bei Versetzungen im Zusammenhang mit dem Vollzug des geplanten Gesetzes auf Antrag zeitlich befristet von der Zusage der Umzugskostenvergütung abgesehen werde. In diesem Zusammenhang bittet sie darum, dass die betroffenen Beamtinnen und Beamten sowie Tarifbeschäftigten zu gegebener Zeit in geeigneter Weise hierauf hingewiesen würden.

g) Chaos Computer Club Stuttgart

Grundsätzlich bewertet der Chaos Computer Club Stuttgart die Ziele, welche die Landesregierung mit diesem Gesetzentwurf erreichen wolle, positiv. Im Folgenden werden Kritik bzw. Verbesserungsvorschläge bei den jeweiligen Gesetzespassagen erläutert.

h) EnBW Energie Baden-Württemberg AG

Die EnBW begrüßt die geplante Einrichtung der Cybersicherheitsagentur (CSBW) Baden-Württemberg, mit der der Einsatz der Ressourcen und bisher dezentraler Zuständigkeiten für die Cybersicherheit effizient an zentraler Stelle gebündelt werden solle. Damit übernehme Baden-Württemberg im Vergleich zu den Entwicklungen in den anderen Bundesländern eine Führungsrolle.

Mit dem Cybersicherheitsgesetz würden die Rahmenbedingungen für die Errichtung der CSBW und deren Aufgaben und Befugnisse geregelt. Primär solle die CSBW die öffentlichen Stellen als Ergänzung zu den bereits bestehenden Strukturen im Bereich der Informationssicherheit unterstützen. Die Rolle der CSBW sei damit zunächst die einer „Cyber Defence Einheit" für die Landesbehörden.

Zu den hierzu getroffenen Regelungen im Cybersicherheitsgesetz hätte sie im Prinzip keine Anmerkungen.

Allerdings hätte sie auf Grundlage der Ergebnisse und Informationen aus dem Fachbeirat zur CSBW – in dem EnBW auch mitarbeite – den Eindruck, dass das Zielbild für die Ausgestaltung der CSBW ursprünglich ein umfassenderes gewesen sei. Die CSBW sollte neben der Verbesserung der behördlichen Zusammenarbeit in Baden-Württemberg auch die Zusammenarbeit mit den weiteren „Kunden" der CSBW, also Kommunen, KMU, KRITIS Unternehmen, Bürgerinnen und Bürgern mehr in den Fokus nehmen. Dahingehende Regelungen seien im Gesetz nun aber im Wesentlichen noch nicht enthalten.

Haltung der Landesregierung

Die Cybersicherheitsagentur verfolgt einen ganzheitlichen Ansatz unter Berücksichtigung auch der Kommunen, KMU, KRITIS-Unternehmen sowie Bürgerinnen und Bürgern, hat sich aber in der Gründungsphase bei ihren Leistungen auf die Landesverwaltung zu fokussieren.

i) evalag

Die Zielsetzung sei als sinnvoll anzusehen. Die evalag befürwortet die Bündelung von sicherheitstechnischen IT-Kompetenzen an einer zentralen Stelle als Ansprechpartner im Land.

Strukturen und Prozesse der Kommunikation zwischen der Cybersicherheitsagentur und den öffentlichen Einrichtungen seien für den Erfolg wichtig. Dabei sei die Rolle der Cybersicherheitsagentur gegenüber den Einrichtungen näher zu definieren.

Unklar sei für sie, ob und ggf. welche IT-Sicherheitsstandards die öffentlichen Einrichtungen nutzen sollen und ob dadurch weitere Investitionen in IT-Infrastruktur entstünden.

Haltung der Landesregierung

Die von der evalag aufgeworfenen Detailfragen sollen nach Inkrafttreten des Gesetzes durch Rechtsverordnung aufgrund § 13 CSG geregelt werden.

j) Hauptschwerbehindertenvertretung der Polizei

Aus schwerbehindertenrechtlicher Sicht bestünden keine Bedenken.

k) Hochschule Karlsruhe – Technik und Wirtschaft

Die Hochschule Karlsruhe schließt sich der Stellungnahme des Steuerkreises zur Informationssicherheit der Universitäten und Hochschulen des Landes an und freut sich, dass sich die Cybersicherheitsagentur in den ersten Gesprächen mit dem Steuerkreis/Kernteam Informationssicherheit der Universitäten und Hochschulen des Landes bisher sehr aufgeschlossen gezeigt habe. Die Hochschulen und Universitäten würden die kooperativen Ansätze mit der Cybersicherheitsagentur befürworten, wenn die hochschulspezifischen Anforderungen im IT-Grundschutz vor allem über das Kernteam Informationssicherheit wie auch über die standortspezifische IT-Struktur berücksichtigt würden.

l) Karlsruher Institut für Technologie (KIT)

Das KIT begrüßt ausdrücklich die vielfältigen Anstrengungen des Landes zur Verbesserung der Cyber- und Informationssicherheit, wenngleich der Gesetzentwurf „nicht als angemessen für wissenschaftliche Einrichtungen“ bewertet werde, weil durch eine Vereinbarung zwischen der Cybersicherheitsagentur und der fachlich zuständigen obersten Landesbehörde in die Autonomie der Hochschulen eingegriffen werden könne.

Haltung der Landesregierung

Den Hochschulen werden keine Pflichten auferlegt, welche ihre verfassungsrechtlich garantierte Unabhängigkeit beeinträchtigen. In den sonstigen Stellungnahmen aus dem Hochschulbereich (Hochschule Karlsruhe – Technik und Wirtschaft, Landesrektorenkonferenz, der Steuerkreis zur Informationssicherheit der Universitäten und Hochschulen des Landes und die Landesstudierendenvertretung) wurden keine solchen Bedenken geäußert. Bei der Gesetzesanwendung sind die verfassungsrechtliche Unabhängigkeit der Hochschulen zu beachten, was insbesondere bei einer etwaigen einvernehmlichen Vereinbarung nach § 2 Absatz 2 Satz 2 zwischen der Cybersicherheitsagentur und der fachlich zuständigen obersten Landesbehörde gilt.

m) Kommunale Landesverbände (Gemeindetag Baden-Württemberg, Städtetag Baden-Württemberg und Landkreistag Baden-Württemberg)

Die Kommunalen Landesverbände würden die konstruktive Zusammenarbeit schätzen, die bisher zwischen dem Innenministerium und den Kommunalen Landesverbänden stattgefunden habe, und möchten auch künftig dazu beitragen, diese beizubehalten und weiter fortzuführen. Bei der Ausgestaltung der Cybersicherheitsagentur und deren künftiger Zusammenarbeit mit der kommunalen Seite seien sie gerne bereit, kommunale Expertise, auch über die Hinzuziehung von Fachexperten aus den Kreisen der Mitglieder, einzubringen.

Auf die Zusammenarbeit der neuen Cybersicherheitsagentur mit der kommunalen Seite sei insofern ein besonderer Fokus zu legen. So sei es erforderlich, dass im Verlauf der weiteren Zusammenarbeit gemeinsam definiert werde, welche Rolle der kommunale IT-Dienstleister Komm.ONE in den Bereichen der Zusammenarbeit mit der Zentralen Koordinierungs- und Meldestelle nach § 4, der Abwehr von Gefahren nach § 5 sowie den Befugnissen nach § 6 des Gesetzes zur Verbesserung der Cybersicherheit aber auch grundsätzlich die baden-württembergischen Gemeinden, Städte und Landkreise einnehmen würden und die sich daraus ergebenen Rechte und Pflichten unter Wahrung der Prinzipien der kommunalen Selbstverwaltung abzugrenzen. Eine unmittelbare und auch eine mittelbare Auswirkung etwaiger Regelungen auf die kommunale Ebene sollte sich nur auf Grundlage einer gemeinsamen Verabredung des Landes mit den Kommunalen Landesverbänden ergeben.

Haltung der Landesregierung

Die konstruktive Zusammenarbeit mit den Kommunalen Landesverbänden soll fortgesetzt werden. Eine Vereinbarung mit den Kommunalen Landesverbänden – wie etwa beim 2019 vom Land und den Kommunalen Landesverbänden geschlossenen E-Government-Pakt – wird angestrebt.

n) Landesrektorenkonferenz Baden-Württemberg

Die Landesrektorenkonferenz schließt sich der Stellungnahme des Steuerkreises zur Informationssicherheit der Universitäten und Hochschulen des Landes an. Überdies freut sie sich über die Aufgeschlossenheit in den ersten Gesprächen. Die Universitäten und Hochschulen seien gerne bereit, kooperative Ansätze mit der Cybersicherheitsagentur auf- und auszubauen, soweit sichergestellt sei, dass spezifischen Anforderungen im IT-Grundschutz vor allem über das Kernteam Informationssicherheit wie auch über die standortspezifischen IT-Strukturen abgebildet würden.

Haltung der Landesregierung

Die Kooperation mit Hochschulen als Stellen des Landes mit Sonderstatus kann durch Vereinbarungen nach § 2 Absatz 2 Satz 2 CSG ausgestaltet werden.

o) Landesverband Baden-Württemberg des Bundes Deutscher Kriminalbeamter

Durch die Einrichtung der Cybersicherheitsagentur entstehe eine Landesoberbehörde mit einer erstaunlichen personellen Ausstattung in der Anfangsphase. So seien 83 Neu-Stellen im Haushalt 2020/21 veranschlagt. Mit Blick auf die Kernaufgaben der Polizei Baden-Württemberg im Bereich der Repression und Prävention würden derartige konsequente Schritte für die Kriminalpolizei gewünscht. So bestünde die im LKA 2012 eingerichtete Abteilung Cybercrime/Digitale Spuren anfangs aus einem Personalkörper von unter 70 Personen – zudem seien diese ohne Neustellen aus dem Bestand der Polizei generiert worden und bis zur Reform 2014 hätte auf Landesebene in der Polizei zudem keine regionale Struktur an polizeilichen Einheiten mit ähnlichen Aufgaben bestanden, wie im LKA. Mit der personellen Ausstattung einer neuen Oberbehörde Cybersicherheitsagentur müsse dringend eine personelle und landesweite Stärkung der Polizeistruktur im Bereich Cybercrime/Digitale Spuren einhergehen. Hier bedürfe es eines neuen Sonderprogrammes.

Neben dem Bereich der Politisch Motivierten Kriminalität (PMK) sei es die Digitalisierung des gesamten Lebens, die perspektivisch neue Kriminalitätsfelder, -phänomene und Fallzahlen sowie Herausforderungen für die Gesellschaft und damit auch für die Polizei generiere, wie dies ausführlich in den Unterlagen dargestellt sei. Für den Doppelhaushalt 2020/21 bzw. dem Nachtragshaushalt seien weder eine gezielte personelle Stärkung der polizeilichen Zentralstellen noch der Regionalpräsidien in den Bereichen der kriminalpolizeilich elementaren Felder der PMK oder der Cybercrime-Bekämpfung vorgesehen. Das wird in Anbetracht der polizeilichen Lage für höchst kritisch bewertet. Deswegen sei es zwingend erforderlich, ein landesweites Gesamtkonzept für Sachmittel und Personal im Themenkomplex Cyber zu erstellen, das sämtliche Aspekte des Tätigwerdens umfasse und sowohl bestehende Strukturen berücksichtige, wie neu einzurichtende.

Haltung der Landesregierung

Zusammen mit der Freigabe des Gesetzentwurfes zur Anhörung wurden Eckpunkte für eine Cybersicherheitsstrategie beschlossen. Darauf aufbauend soll eine Cybersicherheitsstrategie entwickelt werden.

Der Landesverband habe große Bedenken, dass die künftigen Schnittstellen der Cybersicherheitsagentur zur bestehenden Struktur der Akteure, namentlich auch der Polizei Baden-Württemberg, nicht ausreichend beschrieben und berücksichtigt worden seien. Er stünde einer sinnvollen Ergänzung offen gegenüber, würde aber die Gefahr von Konkurrenzen sehen in der Aufgabenwahrnehmung, die anstelle zusätzliche Ressourcen zu schaffen und Themenfelder neu zu erschließen, bestehende Ressourcen der aktuellen Akteure binde. Innerhalb der Kriminalpolizei stünden im Themenfeld Cybercrime und Digitale Spuren dafür keine Ressourcen zur Verfügung.

Haltung der Landesregierung

Mit der Verbesserung der Cybersicherheit durch die Cybersicherheitsagentur könnte bei den bestehenden Akteuren ggf. ein geringfügiger Erfüllungsaufwand entstehen (siehe oben Begründung A. 5.). Im Übrigen soll mit der Rechtsverordnung nach § 13 Nummer 5 eine effiziente Zusammenarbeit sichergestellt werden.

Zudem wird zu Bedenken gegeben, dass die Cybersicherheitsagentur nach Inkrafttreten entsprechender gesetzlicher Vorschriften unmittelbar in der Lage sein müsse, die Vorgaben auch umzusetzen. Ob eine Behörde, die in der allgemeinen Verwaltungsstruktur aufgebaut werde und am Anfang stehe, dazu in der Lage sein werde, daran würden gewisse Zweifel geäußert. Ein besserer Weg wäre die Cybersicherheitsagentur zunächst mit Kompetenzen in den Bereichen Prävention/ Information, Grundlagen/Forschung und Vernetzung der Akteure auszustatten und nicht mit operativen, polizeilichen Befugnissen.

Haltung der Landesregierung

Parallel zum Gesetzgebungsverfahren sind schon wesentliche Vorarbeiten durchgeführt worden, um mit dem Betrieb der Cybersicherheitsagentur baldmöglichst zu beginnen.

p) Landesstudierendenvertretung Baden-Württemberg

Die Zielsetzung und der wesentliche Inhalt des Gesetzentwurfs werden grundsätzlich begrüßt.

q) Rechnungshof Baden-Württemberg

Stärkere Anstrengungen im Bereich der Cybersicherheit seien – nicht zuletzt vor dem Hintergrund der Sicherheitsvorfälle bei Landesbehörden – erforderlich. Der Rechnungshof unterstützt das Ziel, hierzu eine kompetente und schlagkräftige

Struktur zu schaffen und wendet sich nicht grundsätzlich gegen das Vorhaben, die künftigen Aufgaben organisatorisch in einer Landesoberbehörde anzusiedeln. Bei der Entscheidung über die organisatorischen Strukturen sei neben fachlichen Fragen auch der Aspekt der Wirtschaftlichkeit zu berücksichtigen. Dabei sei jene Organisationsform zu wählen, mit der das verfolgte Ziel mit dem geringsten Ressourceneinsatz erreicht werden könne. Fachlich und wirtschaftlich tragfähig könne eine Lösung nur dann sein, wenn die Aufgaben klar abgegrenzt seien und parallele Strukturen vermieden würden.

1. Alternative Organisationsformen und Wirtschaftlichkeitsbetrachtung

Die übersandten Unterlagen zur Wirtschaftlichkeitsbetrachtung und zum Haushaltscontrolling beschäftigten sich ausschließlich mit der Frage der Wirtschaftlichkeit der Aufgabenwahrnehmung an sich, nicht aber mit Fragen zur wirtschaftlichsten Organisationsform und dem Personalbedarf. So werde im Vorblatt zum Gesetzentwurf als Alternativen zur Gründung einer neuen Landesoberbehörde die „vollständige Übertragung der … Aufgaben an private Unternehmen“ und die „Beibehaltung der bisherigen Regelung“ genannt.

Beide Alternativen seien mit Blick auf das gegebene Ziel von vornherein unrealistisch. Näherliegende Alternativen würden hingegen nicht dargestellt, obwohl in der Gesetzesbegründung angeführt werde, dass verschiedene Rechtsformen geprüft worden seien, „sowohl privatrechtliche … als auch rechtsfähige und nicht rechtsfähige Anstalten des öffentlichen Rechts sowie die Form einer Behörde“.

Angesichts der mittlerweile vorgesehenen Fokussierung der Aufgaben auf den öffentlichen Bereich und der damit verbundenen „Binnenorientierung“ hätte dabei auch eine Aufgabenwahrnehmung durch die – ebenfalls vorrangig nach innen wirkende – BITBW in den Blick geraten können, ebenso eine Weiterführung der Aufgabenwahrnehmung durch das Innenministerium. So könne bei einer vollständigen Angliederung der Aufgaben an eine bestehende Institution auf die Schaffung eigener Stellen für Querschnittsaufgaben verzichtet werden.

Haltung der Landesregierung

Der Staat muss Sicherheit, Recht und Freiheit in unserem Land auch im Cyberraum gewährleisten. Hierzu bedarf es einer zeitgemäßen Cybersicherheitsarchitektur, die die verschiedenen Akteure wirksam verzahnt. Die Cyber-Sicherheitsstrategie der Bundesregierung aus dem Jahr 2016 stellte bereits fest, dass für ein sicheres und selbstbestimmtes Handeln in einer zunehmend digitalisierten Umgebung ein gesamtgesellschaftlicher Ansatz erforderlich ist.

Eine zukünftige Aufgabenerledigung durch das Innenministerium, wie vom Rechnungshof vorgeschlagen, kommt aus grundsätzlichen Erwägungen nicht in Betracht, denn es ist generell sicherzustellen, dass in obersten Landesbehörden grundsätzlich nur ministerielle Aufgaben wahrgenommen werden. Ministerien sollen Vollzugsaufgaben nur in begründeten Einzelfällen wahrnehmen (vgl. Rechnungshöfe des Bundes und der Länder, Grundsätze der Verwaltungsorganisation, 5. Dezember 2016; abrufbar auf der Internetseite des Rechnungshofs). Dass ein solcher Einzelfall hier vorliegen könnte, ist nicht erkennbar. Die Cybersicherheitsagentur wird mit ihren Aufgabenbereichen – dem Betrieb der Leitstelle und Bereitstellung eines Lagebildes sowie eines Warn- und Informationsdienstes, der Sensibilisierung und Schulung der Beschäftigten der Landesverwaltung sowie der Beratung und Unterstützung bei Cybersicherheitsvorfällen – umfangreiche operative und keine ministeriellen Aufgaben wahrnehmen.

Anders als der Rechnungshof meint, sind sowohl in der Gesetzesbegründung als auch in der Kabinettsvorlage die Gründe, die zur Entscheidung für eine eigene Landesoberbehörde und damit gegen eine Angliederung der Aufgaben an die BITBW geführt haben, benannt und erläutert. So wird im Allgemeinen Teil der Gesetzesbegründung ausgeführt (vgl. Allgemeiner Teil der Begründung, 1. b]):

> „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."

Diese Aufgabenstellung geht damit weit über die bestehende Aufgabe der BITBW hinaus, die nach § 2 Absatz 1 BITBWG insbesondere folgende Aufgaben hat: Bereitstellung, Betrieb und Ausbau der zentralen informationstechnischen Infrastruktur des Landes (Nummer 1) und Beschaffung von nicht fachspezifischen Geräten, Programmen und Lizenzen der Informationstechnik für die Landesverwaltung (Nummer 3), und damit weder sektorenübergreifende Aufgaben übernehmen noch die nunmehr auf die Cybersicherheitsagentur übertragenen Aufgaben der Gefahrenabwehr erfüllen kann.

Dabei ist die BITBW auch ein Landesbetrieb (§ 1 Absatz 2 BITBWG). In der Rolle als Landesbetrieb hat die BITBW eine Abwägung zwischen möglichst geringem Ressourceneinsatz für Sicherheitsmaßnahme bei gleichzeitig möglichst hohem Schutzlevel zu treffen. Bei der Wahrnehmung der Aufgaben einer Cybersicherheitsagentur bestünde der Konflikt bei dem Ressourceneinsatz, ob die Ressourcen für die von der BITBW eingesetzte Infrastruktur verwendet werden oder für die anderen öffentlichen Stellen, die ebenfalls den Gefahren aus dem Cyberraum ausgesetzt sind.

Selbst in dem aktuell favorisierten Modell einer neuen Landesbehörde wäre eine wirtschaftlichere Erledigung von Querschnittsaufgaben möglich, wenn Aufgaben wie Personalverwaltung oder Haushalt im Sinne eines „shared service" beispielsweise durch die Querschnittsabteilung des Innenministeriums oder einer anderen bestehenden Behörde wahrgenommen würden. Nach Kenntnis des Rechnungshofs sei ein solches Modell – wie es auch vom Rechnungshof mit seinen nachgeordneten Staatlichen Rechnungsprüfungsämtern praktiziert werde – im Vorfeld durchaus in der Diskussion gewesen. Die Gründe, warum eine Auseinandersetzung mit diesen Lösungsansätzen nicht erfolge, seien für den Rechnungshof nicht erkennbar.

Haltung der Landesregierung

Soweit der Rechnungshof für das gewählte Modell einer weiteren Landesbehörde weitergehend darauf hinweist, dass eine wirtschaftlichere Erledigung von Querschnittsaufgaben durch deren Wahrnehmung durch andere Behörden (genannt werden das Innenministerium und die BITBW) möglich sei, ist dies nicht zutreffend.

Richtig ist, dass, sofern und soweit sich Wirtschaftlichkeitsvorteile ergeben, Querschnittsaufgaben über Behördengrenzen hinweg gebündelt werden sollen („shared service"). Für den Bereich der Personalverwaltung ist deshalb bereits zum Teil eine Bündelung von Aufgaben beim Innenministerium vorgesehen: Die Zuständigkeit für die Personalverwaltung und Stellenbewirtschaftung liegt bei der Cybersicherheitsagentur und beim Innenministerium. Die Zuständigkeit ist entsprechend der Handhabung in der Innenverwaltung in abgestuftem Umfang den nachgeordneten Dienststellen übertragen. Im höheren Dienst verbleibt die Zuständigkeit für die Stellenbewirtschaftung und einzelne Personalmaßnahmen beim Innenministerium. Für Beamtinnen und Beamte des mittleren und gehobenen Dienstes und vergleichbare Tarifbeschäftigte ist die Zuständigkeit in Personalsachen vollständig auf die nachgeordneten Behörden übertragen.

Eine weitergehende Übernahme auch dieser Aufgaben der Personalverwaltung durch das Innenministerium oder die BITBW würde dagegen zu keinen weiteren Wirtschaftlichkeitsvorteilen führen. Vielmehr ist davon auszugehen, dass durch eine weitergehende Bündelung vielfache Reibungsverluste und Mehraufwände entstehen würden.

Die Cybersicherheitsagentur wird ihren Sitz in Stuttgart in einer Liegenschaft des Landes und damit räumlich getrennt vom Innenministerium haben. Schon aufgrund der räumlichen Trennung ist eine effiziente Aufgabenwahrnehmung vor Ort durch das Innenministerium nicht sachgerecht möglich, da viele der genannten Aufgaben insbesondere den persönlichen Kontakt zwischen der Personalverwaltung und den anderen Beteiligten voraussetzen.

Personalvertretungsrechtlich besteht die Gefahr, dass die umfassende Übertragung von Befugnissen der Cybersicherheitsagentur in personeller, sozialer, organisatorischer und innerdienstlicher Hinsicht auf das Innenministerium zu einer Schwächung der Stellung des Örtlichen Personalrats bei der Cybersicherheitsagentur und damit zu einer Beeinträchtigung des Grundsatzes der vertrauensvollen und partnerschaftlichen Zusammenarbeit zwischen Dienststelle und Personalvertretung führen könnte.

Als Landesoberbehörde ist die Cybersicherheitsagentur nach § 3 Absatz 1 BITBWG verpflichtet, die Leistungen der BITBW zu nutzen. Es ist überdies davon auszugehen, dass gerade beim Thema „Steigerung der Cybersicherheit“ auch in Sachen IT besondere Anforderungen formuliert werden und Spezialwissen auch für einen laufenden Betrieb gefordert sein wird, das über das hinausgeht, was in der Querschnittsabteilung eines Ministeriums aktuell vorhanden ist.

Hinsichtlich der Aufgaben des inneren Dienstes stellt es sich entsprechend dar, dass diese vor allem Tätigkeiten umfassen, die mit der Örtlichkeit verbunden sind und dementsprechend vor Ort erfolgen müssen. Hierzu gehören im Wesentlichen Gebäudetechnik, Materialausgabe, Mediathek, Registratur, Botendienste und Veranstaltungsdienst. Für den Bereich der Cybersicherheitsagentur können diese Aufgaben auch nur in den Örtlichkeiten der Cybersicherheitsagentur erbracht werden. Der Innere Dienst des Innenministeriums stößt derzeit schon an die Grenzen seiner Leistungsfähigkeit und müsste in diesem Fall aufgestockt werden und zwar im Umfang der zusätzlich zu leistenden Tätigkeiten inklusive zusätzlicher Wegezeiten. Insgesamt wäre also ein größerer Personalkörper aufzubauen als durch eine getrennte Aufgabenwahrnehmung benötigt würde. Eine Aufgabenwahrnehmung durch den Inneren Dienst des Innenministeriums außerhalb des eigenen Gebäudes ist deshalb aus unserer Sicht unwirtschaftlich und generiert keinen fachlichen Mehrwert.

Das für die Betreuung notwendige Personal müsste im Übrigen auch in der Querschnittsabteilung des Innenministeriums geschaffen werden. Das Innenministerium wäre für solche Zusatzaufgaben nicht auskömmlich aufgestellt. Zudem wurde der Personalzuwachs im Innenministerium der vergangenen Jahre durch den Inneren Dienst des Innenministeriums bisher ohne Zuwachs an eigenem Personal gestemmt. Dies hat dauerhaft zu erheblichen Mehrbelastungen geführt.

2. Bündelung und Abgrenzung von Aufgaben

Nach den Ausführungen in der Gesetzesbegründung wie auch in der Kabinettsvorlage diene die Cybersicherheitsagentur primär der Unterstützung öffentlicher Stellen „als Ergänzung zu den bereits bestehenden Strukturen“. Sie solle „die bislang überwiegend dezentral wahrgenommenen Aufgaben bündeln bzw. in angemessener Form koordinieren“.

Nach Auffassung des Rechnungshofs bleibe das Verhältnis von „Bündelung dezentral wahrgenommener Aufgaben“ und „Ergänzung bestehender Strukturen“ weitgehend offen.

In den vergangenen Jahren habe der Haushaltsgesetzgeber insgesamt 120 Stellen für Informationssicherheitsbeauftragte geschaffen, die dezentral in den Einzelplänen veranschlagt seien. Die Informationssicherheitsbeauftragten seien vor Ort in den Behörden des Landes eingesetzt. Weitere Aufgaben der Informationssicherheit nehme das bislang bei der BITBW angesiedelte Computer Emergency Response Team (CERT BWL) wahr. Mit Blick auf die spezifischen Sicherheitsbelange der Steuerverwaltung sei zudem 2019 ein eigenes Sicherheitszentrum IT in der Finanzverwaltung Baden-Württemberg (SITiF BW) bei der Oberfinanzdirektion Karlsruhe gebildet worden.

In den Unterlagen zum Haushaltscontrolling hieße es, durch die konsequente Bündelung aller nicht fachspezifischen Aufgaben der Cybersicherheit bei der Cybersicherheitsagentur seien Synergieeffekte zu erwarten. Der Rechnungshof

verstehe unter „Bündelung“, dass bislang dezentral wahrgenommene Aufgaben künftig von der Cybersicherheitsagentur wahrgenommen würden. Bei den dezentralen Einheiten müsste es folglich zu einem Aufgabenabbau kommen.

Näher ausgeführt würden die vorgesehenen Änderungen in der Aufgabenwahrnehmung und die erwarteten oder erhofften Synergieeffekte jedoch nur ansatzweise. Nachvollziehbar, aber nicht quantifiziert seien Synergieeffekte aus der Übertragung der bislang vom CERT BWL in der BITBW wahrgenommenen Aufgaben auf die Cybersicherheitsagentur. Hier folgten die Personalressourcen der Aufgabe. Allerdings verliere die BITBW hier auch Sachverstand, der für den operativen Betrieb notwendig sei.

Mit Blick auf die weiteren mit Aufgaben der Informationssicherheit befassten Stellen hieße es hingegen in der Gesetzesbegründung, dass „die bisherigen Strukturen … weitestgehend in der bisherigen Form bestehen bleiben“. Insbesondere seien die Funktionen eines übergeordneten Informationssicherheitsbeauftragten (Chief Information Security Officer – „CISO“), der Ressort-CISO, der Dienststellen-CISO und der Sicherheitsbeauftragten vor Ort in den Behörden „beizubehalten und mit angemessenen Ressourcen auszustatten“.

Gleiches gelte für die SITiF. Hinsichtlich der Aufgabenabgrenzung zu diesen weiterbestehenden, ebenfalls mit IT-Sicherheit befassten Stellen bleibe der Gesetzentwurf vage. So hieße es, durch die Aufgabenfestlegung für die Cybersicherheitsagentur würden „andere Stellen grundsätzlich nicht gehindert, im Rahmen ihrer Zuständigkeiten vergleichbare Aufgaben wahrzunehmen“. Die „Feinabstimmung des Zusammenspiels der verschiedenen Beteiligten“ solle durch eine Rechtsverordnung erfolgen.

Diese Formulierungen ließen befürchten, dass zwischen den verschiedenen mit Aufgaben der IT-Sicherheit befassten Stellen noch kein gemeinsames Verständnis über die künftige Aufgaben- und Kompetenzverteilung bestehe. Weder mit Blick auf die Informationssicherheitsbeauftragten noch hinsichtlich der für die Steuerverwaltung zuständigen Einheit SITiF scheine die Aufgaben- und Kompetenzabgrenzung zur Cybersicherheitsagentur geklärt. Aus Sicht des Rechnungshofs bestehe hier das Risiko, dass künftig an mehreren Stellen und unabhängig voneinander an denselben Aufgaben der IT-Sicherheit gearbeitet werde und auf diese Weise Parallelstrukturen entstünden. Daran ändere auch der Hinweis in der Gesetzesbegründung nichts, dass „ineffiziente Parallelstrukturen auszuschließen“ seien.

Auch und gerade in Fragen der IT-Sicherheit sei ein koordiniertes und zielgerichtetes Handeln erforderlich. Vor diesem Hintergrund hält der Rechnungshof die Schaffung einer neuen Behörde ohne vorherige, von allen Beteiligten getragene Klärung der künftigen Aufgaben- und Kompetenzabgrenzung für risikobehaftet und nicht zielführend.

Haltung der Landesregierung

Die Anstrengungen für die Verbesserung der Cybersicherheit müssen im Hinblick auf die fortschreitende Digitalisierung erhöht werden. Immer mehr sensible Prozesse der Verwaltung werden digitalisiert und sind damit das potenzielle Ziel von Cyberangriffen. Dies gilt insbesondere im Hinblick auf die 575 bis Ende des Jahres 2022 umzusetzenden Prozesse nach dem Onlinezugangsgesetz (OZG), die digitale Kommunikation mit Bürgerinnen und Bürgern sowie der Wirtschaft, Digitalisierung der Verwaltungsprozesse, die eAkte und die Arbeit von außerhalb des Dienstgebäudes, die eine sichere Anbindung an das Landesverwaltungsnetz erfordert. Trotz der angeführten Synergien wächst der Ressourcenbedarf für die Cybersicherheit stetig. Durch die zentrale Cybersicherheitsagentur kann der Anstieg des Ressourcenbedarfs verlangsamt werden.

Ein gemeinsames Verständnis über Herausforderungen und Lösungswege sowie die künftige Aufgaben- und Kompetenzverteilung wächst nicht von alleine. Bereits der Abstimmungsprozess hat hierzu einen wichtigen Beitrag geleistet.

Eine weitere „Feinabstimmung des Zusammenspiels der verschiedenen Beteiligten“ soll durch Rechtsverordnung erfolgen, weil im Hinblick auf die sich ändernden Vorgaben der EU und des Bundes, auf die sich ändernden Zuständigkeiten der Beteiligten und auf die dynamische Entwicklung im Bereich der eingesetzten Soft- und Hardware mit einem regelmäßigen Anpassungsbedarf zu rechnen ist.

r) Rechtsanwaltskammern Freiburg, Karlsruhe, Stuttgart und Tübingen

Der Gesetzentwurf sehe die Einrichtung einer Landesbehörde mit dem Namen „Agentur für Cybersicherheit“ vor. Die Cybersicherheitsagentur solle für die Cybersicherheit in Baden-Württemberg zuständig sein. Die Fach- und Dienstaufsicht solle das Innenministerium führen. Die Aufgaben und Befugnisse der Cybersicherheitsagentur dienten insbesondere der Abwehr von Gefahren im Bereich der Sicherheitstechnik der öffentlichen Stellen des Landes.

s) Steuerkreis zur Informationssicherheit der Universitäten und Hochschulen des Landes Baden-Württemberg

Die eingeleiteten Maßnahmen werden begrüßt, sowohl zur Stärkung der Schwerpunkte der Cybersicherheit im Land Baden-Württemberg als auch im Hinblick auf die sich anbahnende direkte Zusammenarbeit mit der Cybersicherheitsagentur.

t) Universitätsklinikum Tübingen

Das Universitätsklinikum Tübingen geht davon aus, dass es vom Gesetz und den darin enthaltenen Forderungen nicht betroffen seien, da das Universitätsklinikum Tübingen nicht am Landesnetz angeschlossen sei, sondern an das Hochschulnetz BELWÜ.

Das Universitätsklinikum Tübingen begrüßt die Bemühungen des Landes, die Cybersicherheit im Land grundsätzlich zu erhöhen.

Haltung der Landesregierung

Für Hochschulen ist in § 2 Absatz 2 CSG eine Sonderregelung enthalten.

2. Zum Vorblatt

a) BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Richtigerweise werde im Vorblatt die Notwendigkeit postuliert, die vorhandenen Landesressourcen für die Cybersicherheit an einer zentralen Stelle zu bündeln. Allerdings widerspreche es der unter Abschnitt B geforderten Effektivität und Effizienz hierzu eine neue Landesoberbehörde zu schaffen. Fakt sei, dass im Land Baden-Württemberg bereits eine Vielzahl von Akteuren seien, die an ihrer jeweiligen Stelle eine unterschiedlich ausgeprägte Kompetenz und Schlagkraft im Bereich Cybersicherheit vorweisen könnten. Eine einfache Darstellung der bestehenden Beziehungsgeflechte zwischen diesen Organisationen zeige offenkundig, dass zwar nicht jede dieser Organisationen mit allen anderen in Beziehung stehe, jedoch alle mit dem Landeskriminalamt. Diese bestehende Struktur zu verstetigen und eine Cybersicherheitsagentur beim LKA BW einzurichten, statt eine neue Landesoberbehörde mit enormen personellen und finanziellem Aufwand zu schaffen, wäre daher die effizientere und damit wirtschaftlichere und schlagkräftigere Alternative. Entsprechende Vorschläge des LKA lägen dem Innenministerium vor. Zudem sei der ehemalige Leiter der Abteilung Cybercrime im Landeskriminalamt im Aufbaustab der Cybersicherheitsagentur tätig. Es erschließe sich nicht, warum dieser naheliegende Weg nicht beschritten und noch nicht einmal unter Ziffer C – Alternativen aufgeführt sei.

Haltung der Landesregierung

Eine Bündelung aller Aufgaben beim Landeskriminalamt kommt nicht in Betracht, weil die Cybersicherheitsagentur auch nicht polizeiliche Aufgaben wie die Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen übernehmen soll. Überdies kann die Gewährleistung der Cybersicherheit nicht alleine von der Polizei geschultert werden. Im Bereich der Cyberkriminalität ist von einem hohen Dunkelfeld auszuge-

hen, weil die betroffenen Opfer gar keine Anzeige erstatten. Vor diesem Hintergrund sind die bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme gewonnenen Erkenntnisse im Rahmen eines ganzheitlichen Ansatzes zur Verbesserung der Cybersicherheit erforderlich.

Ziffer D. beziffere die Kosten zum Aufbau einer Cybersicherheitsarchitektur (nicht Agentur) mit 13 Mio. Euro und stelle darüber hinaus fest, dass mit bedeutenden Einnahmen nicht zu rechnen sei. Hier würden Architektur und Agentur fälschlicherweise miteinander vermengt. Tatsächlich bestehe bereits heute eine Cybersicherheitsarchitektur. Andernfalls hätte sich das Land bislang diesem Bedrohungsszenario gegenüber bloßgestellt, was nicht der Fall sei. Daher wird angenommen, dass es bei den hier aufgeführten Kosten im Wesentlichen um die Kosten für den Aufbau dieser Landesoberbehörde gehe, die dann wiederum einer neuen Cybersicherheitsarchitektur bedürfe, um diese in die bestehenden Prozesse einzubinden. Dass dies unnötig erscheine, hätten sie bereits oben dargestellt.

Haltung der Landesregierung

Im Staatshaushaltsplan 2020/2021 wurden die Haushaltsmittel für die Cybersicherheitsarchitektur veranschlagt, weil die Cybersicherheitsagentur noch nicht eingerichtet war.

b) EnBW Energie Baden-Württemberg AG

In der Vorbemerkung zum Gesetz sei geregelt, dass die Cybersicherheitsagentur in Einzelfällen auch nichtöffentliche Stellen beraten und bei Sicherheitsvorfällen unterstützen könne und außerdem auch Bürgerinnen und Bürger zu Themen der Cybersicherheit sensibilisieren solle. Der Anspruch eine zentrale Koordinationsstelle im Land auch für die Wirtschaft bzw. KRITIS-Unternehmen in Richtung aller Security Behörden in Deutschland aber auch EU-weit und international zu werden, sei vor diesem Hintergrund aber noch in weiter Ferne. Dies wäre für sie aber ein echter Mehrwert, da die Anzahl der zuständigen Behörden und die Komplexität der Thematik immer weiter zunehme. Daher brauche es auch eine weitere Entwicklung in der Wirtschaft zu mehr Cyber-Security-Kompetenz im Sinne einer Förderung von Unternehmen, Forschung und Entwicklung.

Haltung der Landesregierung

Die Cybersicherheitsagentur verfolgt einen ganzheitlichen Ansatz unter Berücksichtigung auch der Wirtschaft, gleichzeitig fokussiert sie sich in der Gründungsphase auf die Landesverwaltung.

3. Zu Artikel 1 – § 1 CSG

a) Zu § 1 Absatz 1 Satz 2 CSG

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

§ 1 Absatz 1 Satz 2 definiere, dass die Cybersicherheitsagentur zuständig sei für die Cybersicherheit in Baden-Württemberg. Tatsächlich sei deren Zuständigkeit jedoch weitaus geringer und umfasse, wie im Vorblatt aufgeführt sei, lediglich die Zuständigkeit für die Cybersicherheit öffentlicher Stellen. Auch im weiteren Gesetzestext fänden sich keine Handlungsbefugnisse gegenüber Privaten. § 1 Absatz 1 Satz 2 sei daher irreführend und solle konkretisiert werden.

Haltung der Landesregierung

Zwar liegt der Schwerpunkt der Tätigkeit der Cybersicherheitsagentur im Bereich der öffentlichen Stellen, allerdings kann die Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

nach § 6 auch bei privaten Stellen erfolgen. Überdies bezieht sich die Befugnis zur Warnung nach § 8 an die Öffentlichkeit auch auf Produkte von Privaten. Insbesondere spiegelt sich die gesamtheitliche Zuständigkeit der Agentur für die Cybersicherheit in Baden-Württemberg in ihrer Funktion als zentrale Koordinierungs- und Meldestelle gemäß § 4 wider.

b) Zu § 1 Absatz 2 CSG

Baden-Württembergischer Industrie- und Handelskammertag e. V.

Befürwortet werde die Aufgabe der Agentur, die Cybersicherheit in Baden-Württemberg zentral und landesweit von Stuttgart aus zu betreuen. Diesbezüglich werde jedoch angeregt, auch Außenstellen in den Regionen zu prüfen und eine Vernetzung mit den regionalen Sicherheitsakteuren anzustreben. Dadurch könnten die Dienstleistungen der Agentur unter Einbeziehung regionaler IT-Sicherheits-Kompetenzträger direkt vor Ort verfügbar gemacht werden.

Haltung der Landesregierung

Die Erwägungen werden genauer geprüft und bei den näheren Regelungen zur Organisation der Cybersicherheitsagentur durch Erlass von Verwaltungsvorschriften nach § 14 dann dementsprechend berücksichtigt.

c) Zu § 1 Absatz 3 CSG

Chaos Computer Club Stuttgart

Um den unzweideutigen Auftrag („Verbesserung der Cybersicherheit“) ohne Interessenkonflikt folgen zu können, dürfe die Cybersicherheitsagentur nicht dem Innenministerium unterstellt werden, vielmehr solle sie einen unzweifelhaften Status als unabhängige Landesbehörde erhalten. Sollte die Cybersicherheitsagentur Baden-Württemberg dem Innenministerium unterstehen, könne diese ihren Auftrag nicht kompromisslos gerecht werden, weil demselben Ministerium unterstellten Behörden konträre Interessen verfolgen (z. B. Nutzung von Sicherheitslücken zur Quellen-TKÜ). Eine solche Unabhängigkeit habe sich beispielsweise beim LfDI deutlich positiv bemerkbar gemacht und das Vertrauen von Bürgern und Unternehmen in die Institution gestärkt.

Landesstudierendenvertretung Baden-Württemberg

Aus Sicht der Landesstudierendenvertretung sei die geplante Unterstellung der Cybersicherheitsagentur unter die Dienst- und Fachaufsicht des Innenministeriums kritisch zu hinterfragen. Hinsichtlich der geplanten Aufgaben, bzw. eines Teilspektrums derer (untersuchen, bewerten, berichten), lasse die künftige Cybersicherheitsagentur Parallelen zu denen des Rechnungshofs erkennen und bedinge daher eine Unabhängigkeit von einem Ministerium. Durch die gleichzeitige Eigenschaft als Aufsichtsbehörde des Landesamts für Verfassungsschutz sowie als zuständige Behörde für Polizei und Strafverfolgung seien Interessenkonflikte denkbar. Die Cybersicherheitsagentur sollte daher den Rang einer obersten Landesbehörde erhalten.

Haltung der Landesregierung

Das angeführte Beispiel der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit zeigt, dass in einigen Fällen konträre Interessen wie der Datenschutz und die Informationsfreiheit in einer Behörde angemessen miteinander abgewogen werden können. Die Unabhängigkeit des Landesbeauftragten beruht auf der Vorgabe der Artikeln 51 ff. der Verordnung (EU) 2016/679. Die Unabhängigkeit der Mitglieder des Rechnungshofs beruht auf Artikel 83 Absatz 2 Satz 2 der Landesverfassung. Im Übrigen ist nach deutschem und baden-württembergischem Verfassungsrecht eine Unabhängigkeit von Behörden nur schwer mit dem Demokratieprinzip in Einklang zu bringen. „Verfassungsrechtlich wird der notwendige Zurechnungszusammenhang zwischen Volk und staatlicher Herr-

schaft vor allem durch die Wahl des Parlaments, durch die von ihm beschlossenen Gesetze als Maßstab der vollziehenden Gewalt, durch den parlamentarischen Einfluss auf die Politik der Regierung sowie durch die grundsätzliche Weisungsgebundenheit der Verwaltung gegenüber der Regierung hergestellt (vgl. BVerfGE 83, 60 <72>; 136, 194 <261 f. Rn. 168>; stRspr). Ein Amtsträger ist personell uneingeschränkt legitimiert, wenn er sein Amt im Wege einer Wahl durch das Volk oder das Parlament oder durch einen seinerseits personell legitimierten Amtsträger oder mit dessen Zustimmung erhalten hat. Sachlich-inhaltliche Legitimation wird durch die Bindung an das Gesetz sowie durch Aufsicht und Weisung übergeordneter staatlicher Stellen vermittelt“ (Bundesverfassungsgericht Urteil des Zweiten Senats vom 30. Juli 2019 – 2 BvR 1685/14 –, – 2 BvR 2631/14 –, Randnummer 129). „Eine Absenkung des demokratischen Legitimationsniveaus ist jedoch nicht unbegrenzt zulässig und bedarf zudem der Rechtfertigung“ (Bundesverfassungsgericht, ebenda, Randnummer 131). Ein vermeintlicher Interessenskonflikt zwischen mehreren der Aufsichtsbehörde unterstellten Behörden kann die Absenkung des demokratischen Legitimationsniveaus der Cybersicherheitsagentur durch Trennung von der Aufsicht durch das demokratisch legitimierte Innenministerium nicht rechtfertigen, vielmehr kann die gemeinsame Aufsichtsbehörde einen Interessenausgleich bewirken.

4. Zu Artikel 1 – § 2 CSG

a) Überschrift

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Es wird angeregt, diesen Paragrafen umzubenennen in „Begriffsbestimmungen und Zuständigkeitsbegrenzungen“. Es würde deutlich, dass zur ohnehin bereits eingeschränkten Zuständigkeit der Cybersicherheitsagentur auf Landesbehörden und andere öffentlichen Stellen eine weitere Zuständigkeitsbeschränkung vorgenommen würde.

Haltung der Landesregierung

Eine Umbenennung von § 2 ist nicht erforderlich, weil Begriffsbestimmungen immer insoweit die Zuständigkeit der Behörde begrenzen, als die Zuständigkeit der Behörde nur im Rahmen der Reichweite der für die Umschreibung der Zuständigkeit verwendeten Begriffe besteht.

b) Zu § 2 Absatz 1 Satz 1 CSG

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Es erscheine kaum zielführend, im Rahmen der Begriffsbestimmungen mit Pleonasmen zu arbeiten.

Nach § 2 Absatz 1 Satz 1 sei unter einer öffentlichen Stelle eine Stelle zu verstehen, die einer bestimmten Gebietskörperschaft angehört oder unter der Aufsicht des Landes steht. Auch natürliche oder juristische Personen des Privatrechts sollten – die Wahrnehmung bestimmter Aufgaben vorausgesetzt, hierunter fallen. Der Begriff „Stelle“ werde bei genauer Betrachtung gerade nicht definiert. Während etwa der Behördenbegriff in § 1 Absatz 2 des Landesverwaltungsverfahrensgesetzes (LVwVfG) durch die Aufgabenwahrnehmung der dort genannten Stelle konkretisiert werde, bediene sich der vorliegende Entwurf eines Pleonasmus. Dies sei nicht nur unbefriedigend, sondern berge auch das Risiko von Missverständnissen. Wenn natürliche Personen – mithin Einzelpersonen – unter bestimmten Voraussetzungen als „Stelle“ anzusehen sein sollten, stelle sich die Frage, ob auch einzelne Behördenbedienstete „öffentliche Stelle“ in diesem Sinn sein könnten. Vorzugswürdig erscheine es deshalb, den Begriff der Stelle genauer zu definieren. Zu denken sei etwa an eine Organisationseinheit. Eine solche könne im privatrechtlichen Bereich durchaus durch eine Einzelperson verkörpert werden, während es im öffentlich-rechtlichen Bereich sicherlich einer organisatorischen Einheit

innerhalb des hierarchischen Aufbaus bedürfe, um die angesprochenen Aufgaben wahrnehmen zu können.

Haltung der Landesregierung

Die Argumentation ist nicht nachvollziehbar, da auch in § 1 Absatz 2 des Landesverwaltungsgesetzes der dort verwendete Begriff der „Stelle“ nicht definiert ist, sondern lediglich der Behördenbegriff anhand der Funktion der „Stelle“ definiert wird. Der vorgeschlagene Begriff der „Organisationseinheit“ wird in der Gesetzessprache üblicherweise als Teil einer Behörde verstanden (so etwa in § 98 Absatz 5 und 6 des Agrarstatistikgesetzes), was hier allerdings gerade nicht gemeint ist.

Überdies falle auf, dass an Gebietskörperschaften, denen die „öffentlichen Stellen“ zugeordnet oder angehören sollten, nur das Land sowie Gemeinden und Gemeindeverbände genannt seien. Zu fragen sei deshalb, weshalb Landkreise und Verbände wie etwa der Verband Region Stuttgart u. Ä. oder sonstige Zusammenschlüsse wie Zweckverbände o. Ä. nicht erwähnt werden. Es bedürfe wohl keiner Vertiefung, dass auch diese vornehmlich Aufgaben der Daseinsvorsorge wahrnähmen. Weshalb ihnen ein Sonderstatus gemäß § 2 Absatz 2 Nummer 8 zuzubilligen sein sollte, erschließe sich nicht, zumal es sich insoweit wohl nicht um Stellen des Landes i. S. der Gesetzesbegründung handele.

Haltung der Landesregierung

Die angeführten Beispiele bedurften keiner ausdrücklichen Erwähnung in § 2 Absatz 1 Satz 1. Die Landkreise sind nach § 1 Absatz 2, § 51 der Landkreisordnung Körperschaften des öffentlichen Rechts unter der Rechtsaufsicht des Innenministeriums, die Regionalverbände sind nach § 32 Satz 1 des Landesplanungsgesetzes Körperschaften des öffentlichen Rechts unter der Aufsicht des Landes und die Zweckverbände sind nach § 3 Satz 1 und § 28 des Gesetzes über kommunale Zusammenarbeit Körperschaften des öffentlichen Rechts unter staatlicher Aufsicht. Die drei angeführten Beispiele sind mithin „der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts“ im Sinne des Satz 1, und damit allerdings keine „Stellen des Landes“ im Sinne des § 2 Absatz 2 Satz 1 Nummer 8.

c) Zu § 2 Absatz 2 CSG

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Die explizite Berücksichtigung der verfassungsrechtlich oder einfachgesetzlich garantierten Unabhängigkeit weiterer öffentlicher Stellen als „Sonderstatus“ (§ 2 Absatz 2) wird ausdrücklich begrüßt.

d) Zu § 2 Absatz 2 Satz 1 CSG

Baden-Württembergischer Industrie- und Handelskammertag e. V.

Die Industrie- und Handelskammern seien gemäß § 2 Absatz 1 Satz 1 „öffentliche Stelle“. Dadurch seien die IHKs im Land unmittelbar von dem Wirkungskreis der Cybersicherheitsagentur erfasst. Die Ausgestaltung der Aufgaben der Cybersicherheitsagentur müsse daher den verschiedenen „öffentlichen Stellen“ Rechnung tragen. Dabei müsse sichergestellt werden, dass Organisationen nicht zum Aufbau von Doppelstrukturen gezwungen würden, sofern sie ein bereits funktionierendes Cybersicherheitssystem nachweisen könnten. Das bedeutet auch, dass gegebenenfalls bestehende Meldepflichten und Anforderungen an die Cybersicherheit verzahnt werden sollten, um den bürokratischen wie kostentechnischen Aufwand so gering wie möglich zu halten. Denn es sei wichtig, dass für die Wirtschaft weder mittelbar noch unmittelbar ein Erfüllungsaufwand entstehe.

Haltung der Landesregierung

Verpflichtungen nach diesem Gesetz sind für Stellen des Landes und unmittelbar an das Landesverwaltungsnetz angeschlossene Stellen vorgesehen. Die berufsständischen Kammern sind aber keine Stellen des Landes, weil in § 2 Absatz 1 Satz 1 zwischen „Stellen des Landes“ und „Gemeinden und Gemeindeverbänden“ sowie den „sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts“ differenziert wird.

Im Übrigen wird die Übertragbarkeit der Erwägungen auf öffentliche Stellen des Landes genauer geprüft und bei der Regelung durch Rechtsverordnung nach § 13 dann dementsprechend berücksichtigt.

e) Zu § 2 Absatz 2 Satz 1 Nummer 3 CSG

Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Zu Recht werde in § 2 Absatz 2 Satz 1 Nummer 3 der aus der europarechtlich begründeten und gewährleisteten völligen Unabhängigkeit des Landesbeauftragten für den Datenschutz (LfDI) Rechnung getragen. Nach dem Wortlaut der Bestimmung gelte der Vorbehalt gesonderter Vereinbarungen für „Verpflichtungen nach diesem Gesetz“. Eine solche ausdrückliche gesetzliche Verpflichtung ergebe sich aus § 5 Absatz 2 Satz 4 (Unterstützungspflicht und Pflicht, Zugang zu internen Protokolldaten sowie Schnittstellendaten sicherzustellen). Soweit § 4 Absatz 3 eine Meldeverpflichtung regele, falle (u. a.) der LfDI nach seinem Verständnis unter die spezielle Ausnahmeregelung des § 4 Absatz 4. Weitere gesetzliche Verpflichtungen seien nicht ersichtlich. Soweit es nicht um Maßnahmen nach diesem Gesetz, sondern um solche aufgrund dieses Gesetzes gehe (Anordnungen gemäß § 5 Absatz 1 Satz 1), sehe § 5 Absatz 12 eine Sonderregelung zugunsten (u. a.) des LfDI vor. Insgesamt sehe der LfDI von daher die völlige Unabhängigkeit des LfDI gewährleistet.

f) Zu § 2 Absatz 2 Satz 2 CSG

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Absatz 2 benenne Stellen, für deren angestrebte Einbindung es gesonderter Vereinbarungen bedürfe, wobei nicht klar sein dürfte, dass diese in jedem Fall erreicht werden könne. Damit sei beispielsweise ein wesentlicher und hoch brisanter Bereich für Cyberangriffe, nämlich die Hochschulen des Landes, von der angestrebten Zielsetzung des Gesetzes, nämlich die „Cybersicherheit zu verbessern“ und die „Abwehr von Gefahren für die Cybersicherheit … zu professionalisieren“ nicht umfasst. Es seien doch gerade die Hochschulen, die in Träger der wichtigsten Ressource des Wohlstands, nämlich das Know-how, sind.

Haltung der Landesregierung

Mithilfe gesonderter Vereinbarungen kann den verfassungsrechtlichen und sich dynamisch ändernden technischen Besonderheiten der Stellen des Landes mit Sonderstatus besser Rechnung getragen werden als durch eine gesetzliche Pauschalregelung.

Karlsruher Institut für Technologie (KIT)

Der Gesetzentwurf finde Anwendung für das KIT als Universität, sofern nicht die verfassungsrechtliche Unabhängigkeit als Wissenschaftseinrichtung beeinträchtigt werde, und dürfe vor diesem Hintergrund nicht in die Freiheit von Forschung und Lehre eingreifen.

Der Gesetzentwurf statuiere Regelungen, die tief in die Aufgaben und Befugnisse der Universitäten eingreifen würden:

– *Meldepflicht nach § 4 Absatz 3*

– *Anordnungen und Maßnahmen zur Gefahrenabwehr durch die Cybersicherheitsagentur nach § 5 und Unterstützung der Cybersicherheitsagentur bei der automatisierten Auswertung von Protokolldaten aus dem Betrieb von Kommunikationstechnik nach § 5 Absatz 2*

  • *Der Umfang der Ausnahmen/Regelungsmöglichkeit nach Abs. 12 sei unklar*

– *Möglichkeit der Cybersicherheitsagentur nach § 7 im Bereich Cyber- bzw. Informationssicherheit Untersuchungen und Bewertungen durchzuführen*

– *Empfehlungen der Cybersicherheitsagentur nach § 8 bestimmte Sicherheitsprodukte einzusetzen*

– *Nähere Regelung der Aufgaben und Befugnisse sowie der Standards für Cyber- und Informationssicherheit durch Rechtsverordnungen nach § 13*

Mögliche Konsequenzen hieraus für die Universitäten könnten unter anderem sein:

– *Die erhebliche Anpassung von Prozessen und/oder der IT-Infrastruktur*

– *Die Beteiligung/Anhörung der Universitäten sei unklar*

– *Die Zusammenarbeit mit Forschungspartnern/Industrie kann wegen konkurrierender Vorgaben erschwert werden*

Daher werde der Gesetzentwurf in dieser Form nicht als angemessen für wissenschaftliche Einrichtungen bewertet, insbesondere Forschungsuniversitäten, da die Agentur durch mehrere Paragrafen, insbesondere § 5 Absatz 1, mit weitgehenden Befugnissen ausgestattet werde bzw. Einrichtungen Pflichten auferlegen könne, die die Entscheidungsbefugnisse der Universitätsrektorate und -präsidien massiv einschränken könnten. Auch blieben durch die noch vorzulegenden Rechtsverordnungen weitere Auswirkungen des Gesetzes aktuell unklar.

Trotz der „Ausnahmetatbestände“ nach § 2 Absatz 2 und § 5 Absatz 12 würden für die Universitäten erhebliche Berichts- und Informationspflichten entstehen, da diese insoweit nur einen begrenzten Sonderstatus bezüglich der Regelungen verliehen bekäme und durch Vereinbarungen zwischen der Cybersicherheitsagentur und dem Wissenschaftsministerium diese ergänzend geregelt werden können.

Damit bestehe ein erheblicher Eingriff in die Autonomie der Universitäten, da insbesondere IT-Systeme in der Regel von grundlegender Bedeutung für das Kerngeschäft Forschung und Lehre der Universitäten seien.

Weiterhin statte der Gesetzentwurf die Cybersicherheitsagentur mit § 7 mit weitreichenden, „aufsichtsbehördeähnlichen“ Rechten aus. Hierbei könne es zu einer Kollision der Kompetenzen und Zuständigkeiten zwischen der Aufsichtsbehörde für den Datenschutz sowie der Cybersicherheitsagentur kommen.

Haltung der Landesregierung

Den Hochschulen werden keine Pflichten auferlegt, welche ihre verfassungsrechtlich garantierte Unabhängigkeit beeinträchtigen. In den sonstigen Stellungnahmen aus dem Hochschulbereich (Hochschule Karlsruhe – Technik und Wirtschaft, Landesrektorenkonferenz, der Steuerkreis zur Informationssicherheit der Universitäten und Hochschulen des Landes und die Landesstudierendenvertretung) wurden keine solchen Bedenken geäußert. Bei der Gesetzesanwendung ist die verfassungsrechtliche Unabhängigkeit der Hochschulen zu beachten, was insbesondere bei einer etwaigen einvernehmlichen Vereinbarung nach § 2 Absatz 2 Satz 2 zwischen der Cybersicherheitsagentur und der fachlich zuständigen obersten Landesbehörde bedeutsam ist.

Landesstudierendenvertretung Baden-Württemberg

Die Tatsache, dass Hochschulen, soweit deren verfassungsrechtliche Unabhängigkeit reiche, im Sinne des Gesetzes Stellen des Landes mit Sonderstatus darstellen und daher ausgenommen seien hinsichtlich der Befugnisse der Cybersicherheitsagentur, stelle einen bedauerlichen Umstand dar. Die Landesstudierendenvertretung fordere in diesem Zusammenhang das Zustandekommen einer

gesonderten weitreichenden und einvernehmlichen Vereinbarung zwischen der Cybersicherheitsagentur und dem Wissenschaftsministerium als zuständige oberste Landesbehörde. Damit solle gewährleistet werden, dass die Agentur ihre Kompetenz auch auf den Schutz von wissenschaftlich genutzter Infrastruktur wie beispielsweise das Landeshochschulnetz BelWü und dessen Schnittstellen anwenden könne und dürfe. Darüber hinaus solle sichergestellt sein, dass mittels länderübergreifender und internationaler Kooperation in Sachen Cybersicherheit auch ein Beitrag zum Schutz von DFN, eduroam etc. geleistet werde.

Haltung der Landesregierung

Mit der Regelung wird der Hochschulfreiheit nach Artikel 20 der Landesverfassung Rechnung getragen.

Rechtsanwaltskammern Freiburg, Karlsruhe, Stuttgart und Tübingen

Die Agentur habe gemäß § 5 die Befugnis, Anordnungen gegenüber den öffentlichen Stellen des Landes zu treffen.

§ 2 Absatz 1 definiere den Begriff der öffentlichen Stelle: „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“.

Durch § 2 Absatz 2 werde bestimmten Stellen des Landes ein Sonderstatus im Hinblick auf deren verfassungsrechtliche Stellung oder andere gesetzliche Regelungen für diese Stellen zugewiesen. Hierunter fielen z. B. gemäß § 2 Absatz 2 Nummer 6 die Gerichte und Staatsanwaltschaften.

Völlig ausgenommen von der Geltung des beabsichtigten Gesetzes seien gemäß § 2 Absatz 3 die Beliehenen.

Die Rechtsanwaltskammern als Körperschaften des öffentlichen Rechts sei hingegen in den allgemeinen Geltungsbereich des Gesetzes gemäß § 2 Absatz 1 Satz 1 einbezogen. Dies werde der besonderen Stellung der Rechtsanwaltskammern, auch im Vergleich zu anderen juristischen Personen des öffentlichen Rechts, nicht gerecht.

Die Besonderheit der Rechtsanwaltskammern sei darin begründet, dass sie die unabhängigen Selbstverwaltungsorganisationen der Anwaltschaft seien; sie würden gewährleisten, dass alle Rechtsanwältinnen und Rechtsanwälte ihren Beruf unter dem Schutz, der Art. 9, 12 GG frei und als unabhängige Organe der Rechtspflege, § 1 BRAO, ausüben könnten. Die Rechtsanwaltskammern finanzierten sich aus den Beiträgen ihrer Mitglieder. Hinsichtlich der sachlichen, technischen und personellen Ausstattung seien sie ebenfalls unabhängig und frei. Aus diesem Grund bestehe auch lediglich eine Rechtsaufsicht des Justizministeriums.

Eine Befugnis der Agentur für Cybersicherheit, gegenüber den Rechtsanwaltskammern Anordnungen in Bezug auf die Sicherheitstechnik treffen zu dürfen, würde insoweit einen rechtswidrigen Eingriff in die anwaltliche Selbstverwaltung bedeuten.

Um dies zu vermeiden, genüge es nicht, den Rechtsanwaltskammern durch deren Aufnahme in den Katalog des § 2 Absatz 2 gleichfalls einen Sonderstatus zuzuweisen. § 2 Absatz 2 Satz 2 des Entwurfs sehe nämlich vor, dass dann für diese Stellen „einvernehmlich gesonderte Vereinbarungen zwischen der Cybersicherheitsbehörde und der jeweils zuständigen obersten Landesbehörde getroffen werden“. Zuständige oberste Landesbehörde für die Rechtsanwaltskammern sei das Landesjustizministerium. Diesem stehe zwar die Rechtsaufsicht über die Kammern zu, nicht aber die Befugnis, Vereinbarungen mit Dritten mit Wirkung für und gegen die Kammern zu schließen.

Aus diesem Grund bedürfe es einer (klarstellenden) Regelung im Gesetzentwurf, wonach die Rechtsanwaltskammern – ebenso wie die Beliehenen in § 2 Absatz 3 des Gesetzentwurfs –, nicht als öffentliche Stelle im Sinne des Gesetzes gelten würde. Folgende Formulierung des Absatz 3 werde vorgeschlagen:

„Nicht als öffentliche Stellen des Landes gelten die Rechtsanwaltskammern und die Beliehenen.“

Haltung der Landesregierung

In § 2 Absatz 1 Satz 1 wird zwischen den Kategorien „Stelle des Landes“, „Gemeinden und Gemeindeverbände“ sowie den „sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts“ unterschieden. Den „öffentlichen Stellen des Landes“ werden im Gesetz in einigen Regelungen Pflichten auferlegt oder der Cybersicherheitsagentur werden gegenüber „öffentlichen Stellen des Landes“ Befugnisse eingeräumt. Demgegenüber werden die „sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts“ nicht als verpflichtete „Stellen des Landes“ bewertet und sind auch keine der „sonstigen Stellen des Landes“ im Sinne des § 2 Absatz 2 Satz 1 Nummer 8. Dementsprechend kommt auch eine Vereinbarung nach § 2 Absatz 2 Satz 2 zwischen der Cybersicherheitsagentur und der zuständigen obersten Landesbehörde für die Rechtsanwaltskammer nicht in Betracht. Anders als bei Beliehenen, die in bestimmten Fällen als Teil der unmittelbaren Landesverwaltung angesehen werden könnten, kommt dies bei Rechtsanwaltskammern nicht in Betracht. Rechtsanwaltskammern sind eigenständige Körperschaften des öffentlichen Rechts, aber keine Stellen des Landes, sodass es in § 2 Absatz 2 keiner Regelung bedarf, um das Interesse der Rechtsanwaltskammer zur Wahrung ihrer Stellung als unabhängige Selbstverwaltungsorganisation der Anwaltschaft zu gewährleisten.

g) Zu § 2 Absatz 2 und Absatz 6 CSG

Hochschule Karlsruhe – Technik und Wirtschaft, Landesrektorenkonferenz Baden-Württemberg sowie Steuerkreis zur Informationssicherheit der Universitäten und Hochschulen des Landes Baden-Württemberg

Aus Absatz 2 sei klar abzuleiten, dass die im CSG genannten Regelungen die Hochschulen und Universitäten nicht unmittelbar betreffen: „für diese sollen einvernehmlich gesonderte Vereinbarungen zwischen der Cybersicherheitsagentur und der jeweils zuständigen obersten Landesbehörde getroffen werden“. Dieser Sachverhalt übertrage sich auch auf das Landeshochschulnetz Baden-Württemberg BelWü über § 2 Absatz 6 CSG: „die Kommunikationstechnik der in Absatz 2 genannten Stellen, … ist nicht Kommunikationstechnik des Landes (im Sinne dieses Gesetzes) …“.

h) Zu § 2 Absatz 3 CSG

Kommunale Landesverbände (Gemeindetag Baden-Württemberg, Städtetag Baden-Württemberg und Landkreistag Baden-Württemberg)

Hinsichtlich der Landratsämter werde gebeten, Folgendes zu berücksichtigen: Beim Landratsamt handele es sich ungeachtet seiner vielzitierten Janusköpfigkeit um eine Einheitsbehörde. Allein schon dieser organisationsrechtlichen Maßgabe widerspräche es, wenn die Landratsämter im Hinblick auf ihre staatlichen Aufgaben in den unmittelbaren Anwendungsbereich des Gesetzes einbezogen würden, hinsichtlich ihrer kreiskommunalen Aufgaben aber nicht. Vor allem liefe eine solche Differenzierung den IT-Realitäten in den Häusern zuwider: Die Landratsämter hätten eine einheitliche IT-Infrastruktur, die sich nicht künstlich in einen staatlichen und in einen kommunalen Teil auseinanderdividieren lasse. Es werde daher nachdrücklich darum gebeten, die ursprünglich vorgesehene Fassung – „Nicht als öffentliche Stellen des Landes im Sinne dieses Gesetzes gelten die Landratsämter als untere Verwaltungsbehörden und Beliehene.“ – wiederaufzunehmen.

Haltung der Landesregierung

Der gemeinsamen Stellungnahme der Kommunalen Landesverbände wird entsprochen; dementsprechend wird die Formulierung des § 2 Absatz 3 geändert und es wird auch die dazugehörige Begründung angepasst.

i) Zu § 2 Absatz 6 CSG

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Weiterhin sei gemäß Absatz 6 die Kommunikationstechnik bei LfV, Polizei und Justiz nicht von den Regelungen dieses Gesetzes umfasst. Gewertet würde dies als Konsequenz dessen, dass dort funktionierende Strukturen vorhanden seien. Auch dies spreche gegen die finanzielle Notwendigkeit des Aufbaus einer Cybersicherheitsarchitektur.

Haltung der Landesregierung

Absatz 6 berücksichtigt, dass in diesen Bereichen die Kommunikationstechnik der genannten Stellen bundesweit vereinheitlicht ist. Die geäußerte Schlussfolgerung in Bezug auf die „finanzielle Notwendigkeit“ ist nicht nachvollziehbar.

5. Zu Artikel 1 – § 3 CSG

a) Allgemein

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Zu den Aufgaben der Cybersicherheitsagentur solle – ausweislich der Gesetzesbegründung – u. a. die Einflussnahme auf die Entwicklung von Sicherheitsvorkehrungen und Prüfwerkzeugen gehören. Aber auch die Entwicklung von kryptologischen und mathematischen Sicherungsverfahren, Kryptogeräten und -komponenten, Authentifizierungsverfahren und Zugriffskontrollverfahren solle die Cybersicherheitsagentur vorantreiben. Soweit Endprodukte dann von Unternehmen kommerziell vertrieben werden, sollten diese dafür an den Entwicklungskosten beteiligt werden. Hier stelle sich die Frage, ob der Staat sich hier in nicht zulässiger Weise wirtschaftlich betätigen wolle. Politische Ziele lassen sich vielfach (direkter) über die regulative Ausgestaltung der Rahmenbedingungen und die Überwachung ihrer Einhaltung erreichen. Aus der wirtschaftlichen Tätigkeit des Staates könnten sich Wettbewerbsverzerrungen zu Lasten Privater ergeben. Ein Grund sei, dass staatliche Stellen weniger stark als private Unternehmen dem Druck der Kapitalmärkte ausgesetzt seien. Infolgedessen könnten effizientere und innovativere Wettbewerber aus dem Markt ausscheiden.

Staatliche Wirtschaftstätigkeit könne für die Bürger/Verbraucher mit unmittelbaren Kosten verbunden sein. Im Vergleich zu Privaten unterlägen öffentliche Stellen oftmals geringeren Anreizen für effizientes Wirtschaften und würden bisweilen haushaltspolitische Erwägungen in ihre Entscheidungen einbeziehen. Gerade auf Monopolmärkten – wie hier einer entstehen würde – könne dies zu überhöhten Endkundenpreisen führen.

Die in der Begründung des Gesetzentwurfs vorgenommene Begrenzung etwa „auf Grundmuster oder Prototypen“, während „die industrielle Entwicklung und Serienfertigung … allein der Wirtschaft“ zugewiesen werden solle, finde sich so nicht im Gesetzeswortlaut. Die vermeintlich einschränkende Begründung werde sogleich wieder aufgeweicht, wenn es dort heiße:

„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, … hat die herstellende Person der Endprodukte die bei der Cybersicherheitsagentur angefallenen Entwicklungskosten aufgrund vertraglicher Vereinbarung zu erstatten.“

Aus der Doppelrolle des Staates als Marktteilnehmer und Hoheitsträger ergebe sich ein erhöhtes Diskriminierungspotenzial gegenüber privaten Wettbewerbern. Aus den genannten Gründen sei es von entscheidender Bedeutung, dass die unter-

nehmerische Tätigkeit des Staates, soweit möglich, im Wettbewerb erbracht werde.

Die wirtschaftliche Betätigung des Staates sollte dort, wo auch private Unternehmen Leistungen erbringen könnten, stets hinterfragt werden. Sie bedürfe der besonderen Rechtfertigung. In den Entscheidungsprozessen über die wirtschaftliche Betätigung des Staates sollte der Gedanke der Subsidiarität stärker Berücksichtigung finden. Wenn die öffentliche Hand wirtschaftlich tätig werde, sollte sie ihre Beweggründe und die mit der wirtschaftlichen Betätigung verbundenen Vor- und Nachteile vor den Entscheidungen transparent und einer unabhängigen Überprüfung zugänglich machen.

Diese vorstehenden Ausführungen würden auch für den Bereich der Zertifizierungen gelten.

Haltung der Landesregierung

Dass bei etwaiger staatlicher Wirtschaftstätigkeit insbesondere die Vorgaben der EU und des Bundes sowie des Landeshaushaltsrechts zu beachten sind, bedarf keiner Erwähnung im Cybersicherheitsgesetz. Dort ist vielmehr nur die Zuständigkeit der Cybersicherheitsagentur zu regeln und diese hat dann im Einzelfall zu prüfen, ob ihre Tätigkeit im Einzelfall rechtlich zulässig und sinnvoll ist.

Architektenkammer Baden-Württemberg

Angeregt wird die Einfügung eines neuen Absatzes, wonach die Zweckbindung im Rahmen des Datenschutzrechts zu wahren sei, die Daten dürften nur für die Zwecke verwendet werden, für die sie erhoben wurden.

Haltung der Landesregierung

Der Grundsatz der Zweckbindung ist in Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 geregelt und in weiteren Regelungen des EU-Rechts und des Landesdatenschutzgesetzes konkretisiert, sodass eine weitere Regelung in § 3 nicht erforderlich ist.

Baden-Württembergischer Industrie- und Handelskammertag e. V.

Generell sei es richtig, den Fokus der Cybersicherheitsagentur auf öffentliche Stellen zu legen. Nach dem Vorbild des BSI seien entsprechend auch Eingriffsrechte in die IT-Systeme der staatlichen Verwaltung und Meldepflichten sinnvoll. Im Gesetzentwurf könnte jedoch noch deutlicher herausgearbeitet werden, dass keine zusätzlichen Pflichten dieser Art für die Wirtschaft und deren Selbstverwaltungssysteme einhergingen. Denn die IHK-Organisation verfügte bereits seit 2015 über ein internes Computer bzw. Cyber Emergency Response Team (CERT) in Dortmund, welches ein aktives Monitoring über Anomalien betreibe, die auf eine Kompromittierung von IT-Systemen hinweisen könnten, und Informationen zur Prävention für alle IHKs bündele. Dabei sei das CERT Team in Dortmund auch von der Carnegie Mellon University (CMU) in Pittsburgh bereits offiziell als Nutzer der Marke „CERT“ autorisiert worden. Die IHK-Organisation verfüge damit bereits deutschlandweit über klare Standards in diesem Bereich. Der Gesetzentwurf solle somit diese Systeme berücksichtigen, um Doppelstrukturen und doppelte Meldepflichten für die IHK-Organisation zu vermeiden.

Es müsse weiterhin deutlich werden, welche Rechte und Pflichten die Cybersicherheitsagentur gegenüber der Wirtschaft habe, insbesondere in Feldern, in welchen öffentliche Verwaltung und Privatwirtschaft eng kooperierten, z. B. im Bereich des E-Government.

Nach bisherigen Aussagen des Innenministeriums solle die Agentur nur in begrenzter Weise auch freiwillig nutzbare Services für die Wirtschaft bereithalten, etwa im Bereich Sensibilisierung, Vernetzung oder Information mittels Lagebildern (vgl. z. B. Minister Strobl beim Cybersicherheitsforum Stuttgart im März 2020; Behördenspiegel vom März 2020 und heise.de vom 21. September 2020).

Solche Angebote seien zu begrüßen und sollten im Gesetzentwurf als weitere Aufgaben konkret verankert werden.

Die Vielfältigkeit der IT-Sicherheitslandschaft in Baden-Württemberg sei zu beachten und zu wahren. Die Cybersicherheitsagentur sollte bestehende Angebote im privatwirtschaftlichen und wissenschaftlich-transferorientierten Bereich nicht verdrängen, sondern vielmehr mittels gegenseitiger Vernetzung unterstützen und vorhandene Lücken schließen. Beispielsweise sollten gewerbliche Anbieter von IT-Sicherheitsschulungen nicht durch kostenfreie öffentliche Angebote verdrängt werden.

Hinsichtlich der geplanten Aufgaben der Cybersicherheitsagentur würden teilweise noch beträchtliche Schnittmengen zu anderen öffentlichen Behörden im Bereich IT-Sicherheit gesehen. Dies betreffe insbesondere das BSI, die BITBW, den Verfassungsschutz, das LKA und den Landesdatenschutzbeauftragten. Es wird vorgeschlagen, im Gesetz eine genauere Abgrenzung zu formulieren, und damit Transparenz und Übersichtlichkeit sicherzustellen.

In diesem Zusammenhang solle auch die zukünftige Rolle der Cyberwehr mitgedacht werden. Es bleibe unklar, in welcher Weise Cybersicherheitsagentur und Cyberwehr interagieren. Ziel solle generell eine Verstetigung des Angebots der Cyberwehr sein. Hierfür seien die Schnittstellen zwischen Cybersicherheitsagentur und Cyberwehr im Sinne der Transparenz und Übersichtlichkeit zu definieren.

Haltung der Landesregierung

Befugnisse gegenüber privaten Stellen werden der Cybersicherheitsagentur nicht eingeräumt. Sie hat auf Ersuchen der betroffenen Stelle im Rahmen pflichtgemäßen Ermessens nach § 6 die erforderlichen Maßnahmen zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit eines beeinträchtigten informationstechnischen Systems zu treffen. Daneben wird sie im Rahmen von § 3 freiwillige Services für die Wirtschaft anbieten. Dabei soll das Zusammenspiel mit den anderen öffentlichen Stellen im Bereich der Cybersicherheit durch Rechtsverordnung nach § 13 Nummer 5 transparent geregelt werden.

Landesstudierendenvertretung

Hinsichtlich des Aufgabenspektrums der Cybersicherheitsagentur nach § 3 wäre für die Landesstudierendenvertretung zusätzlich die Aufnahme der Förderung von Forschung, Entwicklung sowie Innovation und Lehre bezüglich IT- und Cyber-Security an Hochschulen in Baden-Württemberg wünschenswert.

Haltung der Landesregierung

Zu den Themen können im Rahmen von § 2 Absatz 2 Satz 2 Vereinbarungen geschlossen werden, soweit dies nach dem Landeshaushaltsplan möglich ist.

Universitätsklinikum Ulm

Insofern die Cybersicherheitsagentur des Landes für die Universitätsklinika Zuständigkeit erlange, bestünden bei § 3 insgesamt Überlappungen zu den Aufgaben und Pflichten der Uniklinika gegenüber dem BSI. Die Uniklinika seien kritische Infrastruktur nach der KRITIS-Verordnung des BMI und kooperierten mit dem BSI.

b) Zu § 3 Absatz 1 CSG

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Sämtliche unter Absatz 1 aufgeführten Aufgaben würden bereits heute in der bestehenden Cybersicherheitsarchitektur des Landes wahrgenommen werden. Größtenteils würde dies durch das LKA oder durch BITBW, polizeiintern zudem durch das PTLSPol erfolgen. Darüber hinaus würden Standards verbindlich

durch das BSI definiert werden. Daher sei der Mehrwert der Cybersicherheitsagentur nicht zu erkennen.

Haltung der Landesregierung

Absatz 1 begründet eine umfassende Zuständigkeit der Cybersicherheitsagentur, die bislang nur in Teilbereichen wahrgenommen wird, insbesondere besteht bislang keine zentrale Koordinierungs- und Meldestelle, deren Einrichtung die Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg, (und infolge der Verweisung auf diese Stellungnahme auch der BBW) bei der Stellungnahme zu § 4 selbst unterstützt. Entgegen der Stellungnahme sind Standards des BSI nicht ohne Weiteres für die Landesverwaltung verbindlich. Überdies kann die Mitwirkung an der Entwicklung und Setzung von Sicherheitsstandards für speziell an die Bedürfnisse der Landesverwaltung angepasste Soft- oder Hardware erforderlich sein.

c) Zu § 3 Absatz 1 Satz 2 Nummer 1 CSG

Universitätsklinikum Tübingen

Dieser Punkt lasse eine aktive Rolle in der direkten Abwehr von Gefahren vermuten. Um eine solche aktive Abwehr zu ermöglichen, benötige es eine zentrale Zusammenführung von Informationen aus vielen Bereichen. Eine solche zentrale Zusammenführung berge ebenfalls Gefahren und sei technologisch als auch im Sinne des Datenschutzes und der Informationssicherheit kritisch einzustufen. Der Gesetzgeber möge bitte erläutern, ob dies in diesem Sinne gedacht gewesen sei.

Haltung der Landesregierung

Die Cybersicherheitsagentur soll eine aktive Rolle in der direkten Abwehr von Gefahren im Rahmen der §§ 5 ff. einnehmen. Dazu werden die Informationen zentral zusammengeführt, die für die Abwehr von Gefahren für die Cybersicherheit relevant sind, wie etwa Sicherheitslücken in Programmen oder Wirkungsweisen von Schadprogrammen.

Personenbezogene Daten sollen möglichst nicht zentral bei der Cybersicherheitsagentur gespeichert werden. Der Schutz der Informationen wird insbesondere durch Einhaltung der Verwaltungsvorschrift des Innenministeriums zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) vom 20. Dezember 2004 – Az.: 5-0214.3/77, zuletzt geändert durch Nr. 1 der Verwaltungsvorschrift vom 9. November 2018 (GABl. 2018, S. 714), und der VwV Informationssicherheit gewährleistet.

Universitätsklinikum Ulm

Die Universitätsklinika würden bisher dem BSI berichten, sodass eine weitere Koordinierungsstelle den Aufwand erhöhen würde.

Haltung der Landesregierung

Sinn der Cybersicherheitsagentur ist den Koordinierungsaufwand für die anderen Stellen zu reduzieren. Dies soll insbesondere auch über die Bündelungsfunktion als Kontaktstelle zum BSI nach § 8b BSIG erreicht werden.

d) Zu § 3 Absatz 1 Satz 2 Nummer 2, 6 und 7 CSG

ARGE-HPR

Es sei sicherzustellen, dass ein Schulungskonzept für das betroffene Personal in den Ressorts erstellt werde und Mittel für Schulungen in den Ressorts zur Verfügung gestellt würden. Überdies wird angeregt, dass die zu errichtende Behörde

auch und verstärkt auf die Cybersicherheit der Lehrkräfte achte. In Zeiten verstärkter Bemühungen um eine schnellere Digitalisierung der Schulen, mehr Endgeräte, Software und verstärkter Internetanbindung und Bestrebungen, Elemente des Fernunterrichts zu verstetigen, sei es besonders geboten, Lehrkräfte und ihre Persönlichkeitsrechte zu schützen und den Datenschutz an Schulen konsequent durchzusetzen. Speziell Lehrkräfte seien von Cybermobbing betroffen und müssten wirksam davor geschützt werden. Deshalb rege der HPR Gymnasien auch die Erarbeitung einer umfassenden Broschüre zur Cybersicherheit und zum Cybermobbing an.

Haltung der Landesregierung

Innerhalb der Cybersicherheitsagentur ist die Einrichtung der Abteilung „Prävention und Innovationsmanagement“ geplant, um im Schwerpunkt die Aufgabe der Sensibilisierung und Schulung der Beschäftigten der Landesverwaltung zu erfüllen. Dort soll auch das erforderliche Informationsmaterial erarbeitet werden.

e) Zu § 3 Absatz 1 Satz 2 Nummer 3 CSG

Chaos Computer Club Stuttgart

Hier wird explizit empfohlen ein proaktives Monitoring der IT-Systeme im Zuständigkeitsbereich auf:

A. Zeitnahes Einspielen von Sicherheits-Updates

sofern noch kein Update zur Verfügung steht, die Lücke aber bereits öffentlich ist:

B. Die proaktive Überwachung der Implementierung von wirksamen Mitigations-Strategien.

Haltung der Landesregierung

Die Empfehlung wird bei dem Betrieb der Cybersicherheitsagentur berücksichtigt werden.

Universitätsklinikum Tübingen (in diesem Sinne auch das Universitätsklinikum Ulm)

Für die kritischen Infrastrukturen würde die Regelung eine weitere Überprüfung und damit Aufwand bedeuten, wenn es eine landeseigene Prüfung hierfür gäbe. Der Gesetzgeber möge bitte erläutern, ob er die Einhaltung geltender Standards bei kritischen Infrastrukturen so gestalte, dass die bereits gesetzlich geforderten Prüfungen anerkannt würden. Des Weiteren berge die Verbreitung von Prüfergebnissen an verschiedene Stellen immer die Gefahr mit sich, dass diese Informationen auch in Hände Dritter komme und gegen kritische Infrastrukturen ausgenutzt werden könne. Der Gesetzgeber möge bitte erläutern, wie er die Informationen schützt.

Haltung der Landesregierung

Bei dem Erlass der Rechtsverordnung nach § 13 Nummer 2 zu den Standards für die Cybersicherheit einschließlich der Verfahren zur Überprüfung von Standards wird das Innenministerium die Anerkennung bereits bundesgesetzlich geforderter Prüfungen berücksichtigen. Der Schutz der Informationen wird insbesondere durch Einhaltung der VS-Anweisung und der VwV Informationssicherheit gewährleistet.

f) Zu § 3 Absatz 1 Satz 2 Nummer 4 CSG

Chaos Computer Club Stuttgart

Durch die Gründung der Cybersicherheitsagentur bestehe die Gefahr die, ohnehin schon unübersichtliche, staatliche IT-Sicherheitsstruktur noch weiter zu verkomplizieren. Der Gesetzgeber sollte die Verantwortlichkeiten und Zuständigkeiten der Cybersicherheitsagentur Baden-Württemberg klar, für alle Beteiligten verständlich definieren und gegen die anderen Behörden des Landes (z. B. ZAC BW, CERT BWL) und des Bundes (z. B. BSI) abgrenzen. Betroffenen Behörden und Unternehmen müsse klar ersichtlich sein, welchen alleinigen Ansprechpartner diese jeweils haben und ein reibungsloser Informationsfluss zwischen allen Beteiligten muss zu jedem Zeitpunkt gewährleistet sein. Gerade bei zeitkritischen IT-Sicherheitsvorfällen unter massenhafter Ausnutzung von (ggf. bis dato unbekannten) Sicherheitslücken sei dies von entscheidender Bedeutung.

Haltung der Landesregierung

Die Meldepflichten sowie die ressortübergreifende Organisation im Bereich der Cyber- und Informationssicherheit soll durch Rechtsverordnung nach § 13 Nummer 3 beziehungsweise 5 geregelt werden.

g) Zu § 3 Absatz 1 Satz 2 Nummer 5 CSG

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Dass die geplante Cybersicherheitsagentur die Aufgaben der zentralen Kontaktstelle übernehme, entspreche § 8b BSIG.

Universitätsklinikum Tübingen

Eine Kontaktstelle im Sinne eines SPOC (= Single Points Of Contact) sei durchaus zu diskutieren, um Synergien zu ermöglichen. Auf der anderen Seite seien die kritischen Infrastrukturen bereits verpflichtet und hätten solche Meldewege eingerichtet. Ein Mehrwert für die kritische Infrastruktur sei nicht zu erkennen.

Auch hier sei die Weiterverbreitung der Informationen ein Sicherheitsrisiko und oftmals bei einem Sicherheitsvorfall nicht in allen Details erwünscht. Der Gesetzgeber werde gebeten zu erläutern, welchen Nutzen eine kritische Infrastruktur durch einen SPOC erhalten würde und wie die Informationssicherheit gewährleistet werden könne.

Universitätsklinikum Ulm

Die Universitätsklinika seien bereits mit dem BSI in Kontakt.

Haltung der Landesregierung

Mit der Regelung wird an die Meldewege des § 8b des BSI-Gesetzes angeknüpft. Die auf diesem bundesrechtlich geprägten Meldeweg erhaltenen Informationen können mit den Informationen, die die Cybersicherheitsagentur unabhängig von den KRITIS-Unternehmen gesammelt hat, zu einem umfassenderen Lagebild zusammengeführt werden. Dieser Informationsgewinn wird durch die Pflicht der Cybersicherheitsagentur zur Unterrichtung der öffentlichen Stellen über die sie betreffenden Informationen nach § 4 Absatz 2 Nummer 2 an die Betreiber von kritischen Infrastrukturen weitergegeben.

Der Schutz der Informationen wird insbesondere durch Einhaltung der VS-Anweisung und der VwV Informationssicherheit gewährleistet.

h) Zu § 3 Absatz 2 CSG

Universitätsklinikum Tübingen

Die adHoc-Hilfe bei der Abwehr von Gefahren sei nicht zielführend. Vielmehr sollte in diesem Punkt aufgenommen werden, dass in der Vorbereitung eines Sicherheitsvorfalls die Cybersicherheitsagentur den kritischen Infrastrukturen aktiv und mit Konzepten beratend zur Verfügung stehe und so eingebunden werde, dass die Spezialisten im Rahmen eines akuten Sicherheitsvorfalls 24/7 für eine Unterstützung in der Forensik, der Isolation und der Eindämmung zur Verfügung stehe. Dies würde einen Mehrwert für die kritischen Infrastrukturen, eine gleichartige Vorgehensweisen an den Standorten und Kosten für Rahmenverträge mit Externen für diese Leistung sparen. Der Gesetzgeber wird gebeten, diesen Abschnitt mindestens um die Beratung und Einbindung der Cybersicherheitsagentur in der Vorbereitung zu ergänzen.

Haltung der Landesregierung

Durch die vorgesehene Information und Beratung zur Cybersicherheit und das Kompetenzzentrum für Sensibilisierungen und Schulungen zur Cybersicherheit nach Absatz 1 Satz 2 Nummer 6 beziehungsweise 7 sollen Unterstützungen bei einem konkreten Sicherheitsvorfall erst gar nicht erforderlich werden. Diese präventiven Maßnahmen werden die Risiken aus dem Cyberraum verringern, nichtsdestoweniger bleiben Sicherheitsvorfällen, bei denen die Cybersicherheitsagentur unterstützen sollte, möglich.

i) Zu § 3 Absatz 2 Satz 1 CSG

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Dass die Unterstützungsleistungen der Cybersicherheitsagentur in Absatz 2 Satz 1 lediglich als Kann-Vorschrift und nicht als Verpflichtung aufgeführt seien, sei angesichts der Bedrohungslage und des mit der Einrichtung der Cybersicherheitsagentur verfolgten Ziels nicht verständlich.

Haltung der Landesregierung

Die Einräumung eines Ermessensspielraums für die Unterstützung berücksichtigt, dass in Ausnahmesituationen – wie etwa einem sich sehr schnell ausbreitenden Schadprogramm – die Unterstützungskapazitäten durch die Cybersicherheitsagentur nicht ausreichend sein können und in diesen Fällen eine Auswahl der zu unterstützenden Stellen nach sachgerechten Kriterien ermöglicht wird.

j) Zu § 3 Absatz 2 Satz 2 CSG

Architektenkammer Baden-Württemberg

Die Cybersicherheitsagentur solle bei Ersuchen der Sicherheitsbehörden diese unterstützen.

Die Klarstellung im Gesetzestext wird angeregt, dass sich die Cybersicherheitsagentur an die Vorschriften halten müsse, die für die anfragende Behörde gelten, und dass sie keine Daten, die ihr aus ihren umfassenden Zugriffsrechten auf Logdaten aus dem öffentlichen Dienst zur Verfügung stehen, unter Missachtung dieser Vorschriften verwenden dürfe.

Haltung der Landesregierung

Die Regelung zielt auf die technische Unterstützung der Sicherheitsbehörden und nicht auf die Verarbeitung von personenbezogenen Daten. Soweit bei einer Unterstützung durch die Cybersicherheitsagentur auch die Verarbeitung von personenbezogenen Daten durch die Cybersicherheitsagentur in Betracht kommt, sollte

eine Vereinbarung getroffen werden, insbesondere über eine Auftragsdatenverarbeitung nach Artikel 28 der Verordnung (EU) 2016/679.

6. Zu Artikel 1 – § 4 CSG

a) Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Mit der eingeführten Meldepflicht (ab 1. Januar 2022) sollten gleichwertige Informationsrechte der Meldepflichtigen korrespondieren. Wenn sie schon so in die Pflicht genommen würden, sollten sie auch von den dadurch gewonnenen Erkenntnissen unmittelbar und zeitnah profitieren können.

Haltung der Landesregierung

Nach § 4 Absatz 2 Nummer 2 sollen öffentliche Stellen unverzüglich über die sie betreffenden Informationen unterrichtet werden, sodass der Informationsgewinn über die nach § 4 Absatz 3 Meldepflichtigen hinaus geteilt wird.

b) Baden-Württembergischer Industrie- und Handelskammertag e. V.

Gegenseitige Informationspflichten zu IT-Sicherheitsvorfällen und entsprechende Warnhinweise seien mit dem IT-Sicherheitsgesetz auf Bundesebene für kritische Infrastrukturen bereits etabliert worden. Für Meldungen an eine Landesstelle sollte klar der Mehrwert dieses Ansatzes vermittelt werden (z. B. Warnung anderer Organisationen und ggf. Unternehmen, Beitrag zum Lagebild für eine qualifizierte Bewertung der Sicherheitslage und Ableitung präventiver Maßnahmen). Ebenfalls müsse eine effektive Arbeitsteilung und Kooperation mit den bestehenden Systemen der „öffentlichen Stellen“ sowie mit dem BSI und anderen Sicherheitsbehörden des Bundes und der Cybersicherheitsagentur sichergestellt sein.

Haltung der Landesregierung

Durch die Meldepflichten der öffentlichen Stellen des Landes und der unmittelbar an das Landesverwaltungsnetz angeschlossenen Stellen an die Cybersicherheitsagentur können weitere Informationen im Vergleich zu den dem BSI vorliegenden Informationen gewonnen werden. Umgekehrt ist die Cybersicherheitsagentur nach § 4 Absatz 2 Nummer 2 verpflichtet öffentliche Stellen ggf. unverzüglich über die sie betreffenden Informationen zu unterrichten. Eine entsprechende Pflicht des BSI gegenüber allen Stellen des Landes ist nicht ersichtlich. Eine effektive Arbeitsteilung und Kooperation mit den bestehenden öffentlichen Stellen des Landes soll mit der Rechtsverordnung nach § 13 Nummer 5 sichergestellt werden und im Übrigen finden Gespräche mit den Behörden des Bundes statt.

c) BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Unterstützt wird die Einrichtung einer zentralen Koordinierungs- und Meldestelle. Jedoch wird deren Ansiedlung aufgrund der bestehenden Strukturen und der bestehenden Architektur beim Landeskriminalamt gesehen. Dem Landeskriminalamt sei zudem gelungen, das Vertrauen der Privatwirtschaft in die Kompetenz und die Diskretion der dortigen Abteilung Cybercrime erheblich zu stärken, sodass dort neben den dann zugehenden Informationen aus der Landesverwaltung auch solche der Wirtschaft vorliegen und aggregiert werden könnten. Die Zentrale Ansprechstelle Cybercrime (ZAC) habe in den vergangenen Jahren die Anzahl der Beratungs- und Unterstützungsleistungen pro Jahr gegenüber dem jeweiligen Vorjahr verdoppelt.

Haltung der Landesregierung

Die Einrichtung einer zentralen Koordinierungs- und Meldestelle bei der Cybersicherheitsagentur erscheint deshalb besonders zweckmäßig, weil die Cyber-

sicherheitsagentur auch Erkenntnisse bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 6 gewinnen wird. Diese Aufgabe wird nicht vom Landeskriminalamt wahrgenommen und – als nichtpolizeiliche Aufgabe – wäre eine Übernahme der Aufgabe durch das Landeskriminalamt systemwidrig.

Zudem zeigen die Erfahrungen der Cyberwehr, dass in der Wirtschaft weiterhin erhebliche Vorbehalte bestehen, einen Cybersicherheitsvorfall an die Strafverfolgungsbehörden zu melden (aktuell dort nur in unter 10 % der bearbeiteten Vorfälle, obwohl in jedem Fall ausdrücklich auf eine entsprechende Möglichkeit hingewiesen wird). Die Angst vor Reputationsschäden ist gerade bei kleinen und mittleren Unternehmen weiterhin verbreitet. Gerade jene Fälle sind für die Erstellung eines ganzheitlichen Lagebildes für Baden-Württemberg essentiell, um das Cybersicherheitsniveau branchenübergreifend zu erhöhen.

d) Landesrektorenkonferenz Baden-Württemberg

Die Universitäten hoffen, dass die ab dem Jahr 2022 bestehenden Meldepflichten nach Maßgabe der aufgrund § 13 Nummer 3 des Gesetzentwurfs zu erlassenden Rechtsverordnung für sie keinen erheblichen bürokratischen Zusatzaufwand bedeuten werde.

Haltung der Landesregierung

Die Universitäten sind als Stellen mit Sonderstatus und rechtlich geregelter Unabhängigkeit nach Maßgabe von § 4 Absatz 4 von den Meldepflichten ausgenommen. Beim Erlass der Rechtsverordnung nach § 13 Nummer 3 wird auf die Vermeidung von Zusatzaufwand geachtet werden.

e) Universitätsklinikum Ulm

Die Uniklinika in Baden-Württemberg seien nicht am Landesverwaltungsnetz angeschlossen, vielmehr an das Hochschulnetz BELWÜ. Somit bestehe derzeit keine Meldepflicht für die Uniklinika. Sofern in Zukunft Kooperationen über das Landesverwaltungsnetz vorgesehen werden, könnten Meldungen an die Cybersicherheitsagentur des Landes versendet werden. Die Uniklinika berichteten bereits an das BSI.

7. Zu Artikel 1 – § 5 CSG

a) Zu § 5 Absatz 1 CSG

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Die Eingriffsbefugnisse sollten offenbar bewusst hinter denen der Polizei (§ 3 PolG) oder der Sonderordnungsbehörden (vgl. etwa § 47 Abs. 1 Satz 2 LBO) zurückbleiben. Dies dürfte dem Umstand geschuldet sein, dass die Cybersicherheitsagentur gegenüber anderen öffentlichen Stellen tätig werden solle. Gleichwohl werfe die Formulierung Fragen auf:

Vermisst werde die in den sonstigen Eingriffsbefugnissen enthaltene Vorgabe des pflichtgemäß auszuübenden Ermessens.

Haltung der Landesregierung

Bei der mit „kann“ formulierten Befugnisnorm hat die Cybersicherheitsagentur nach der allgemeinen Regel des § 40 LVwVfG ihr Ermessen entsprechend dem Zweck der Ermächtigung auszuüben und die gesetzlichen Grenzen des Ermessens einzuhalten.

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Die vorherige Fristsetzung erinnere an die Verwaltungsvollstreckung, nämlich an die Androhung einer Vollstreckungsmaßnahme; sie sei nämlich nicht wie eine Anhörung i. S. des § 28 LVwVfG formuliert.

Einerseits werde der Cybersicherheitsagentur die Befugnis eingeräumt, „die erforderlichen Anordnungen zu treffen und Maßnahmen“ zu ergreifen. Andererseits darf sie „Anordnungen treffen oder Maßnahmen vornehmen“ „nur im Einvernehmen mit der jeweils fachlich zuständigen obersten Landesbehörde oder im Einzelfall aufgrund Beschlusses des IT-Rates Baden-Württemberg“, und zwar auch dies nur nach vorheriger Fristsetzung. Dies erscheine zum einen kompliziert, zum anderen stelle sich die Frage, ob mit der Fristsetzung bereits die Erteilung des Einvernehmens für den Fall des fruchtlosen Verstreichens dieser Frist beantragt werden könne.

„Wenn zur Gefahrenabwehr sofortiges Handeln erforderlich ist“ – wenn also, polizeirechtlich gesprochen, Gefahr im Verzug sei –, solle die Präsidentin oder der Präsidenten der Cybersicherheitsagentur anordnen können, dass von der Einholung des Einvernehmens abgesehen werden könne.

Nicht geklärt sei damit strenggenommen, wer die Feststellung treffe, ob sofortiges Handeln erforderlich sei. Vor allem werde eine Vertretungsregelung für den Fall vermisst, dass die Präsidentin oder der Präsident der Cybersicherheitsagentur nicht erreichbar sei. Die oder der Vertreter(in) im Amt werde nicht erwähnt; eine Delegationsmöglichkeit sei nicht vorgesehen.

Haltung der Landesregierung

Die komplizierte Regelung ist erforderlich, weil für komplexe Gefährdungslagen adäquate Regelungen zu treffen sind. Für die Fälle, in denen Gefahr im Verzug vorliegt, müssen der Cybersicherheitsagentur weitreichende Sofortbefugnisse eingeräumt werden, wenn beispielsweise droht, dass ein mit einem Schadprogramm infiziertes System andere Systeme hochgradig gefährdet. Außerdem gibt es Fälle, in denen die Erhöhung des Schutzniveaus mit erheblichen Kosten verbunden ist. Die Risiko-Kosten-Abwägung hat auch unter Berücksichtigung der Haushaltssituation zu erfolgen, weshalb die jeweils fachlich zuständigen obersten Landesbehörden oder der IT-Rat Baden-Württemberg in den Entscheidungsprozess einbezogen werden.

Im Übrigen gelten die allgemeinen Regeln.

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Unklar sei, ob unterschiedliche Stellen gemeint seien, wenn einerseits von „der jeweils fachlich zuständigen obersten Landesbehörde“ gesprochen, deren vorherigen Einvernehmens etwaige Anordnungen und Maßnahmen bedürfte, andererseits aber von „der betroffenen obersten Landesbehörde“ die Rede sei, der die zu protokollierende Entscheidung über die Notwendigkeit sofortigen Handelns mitzuteilen sei.

Haltung der Landesregierung

Bevor eine Anordnung der Cybersicherheitsbehörde ergeht, ist grundsätzlich das Einvernehmen „mit der jeweils fachlich zuständigen obersten Landesbehörde“ herzustellen. Von einer Anordnung sind nur die obersten Landesbehörden betroffen, die als jeweils fachlich zuständige oberste Landesbehörde ihr Einvernehmen nicht erteilt haben. So kann etwa eine Anordnung Auswirkungen auf mehrere Organisationseinheiten haben, die unterschiedlichen Fachaufsichtsbehörden unterstehen, von denen eine oberste Landesbehörde ihr Einvernehmen erteilt hat und die andere oberste Landesbehörde nicht rechtzeitig erreichbar war. Nur der letzteren, betroffenen obersten Landesbehörde ist die Entscheidung nach Satz 6 unverzüglich mitzuteilen, da die andere oberste Landesbehörde die Entscheidung schon kennt. Nur der betroffenen obersten Landesbehörde steht nach Satz 7 das Antragsrecht zu, weil die andere oberste Landesbehörde ihr Einvernehmen erteilt hat.

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Fraglich sei außerdem, ob der Antrag der betroffenen obersten Landesbehörde auf Überprüfung dieser Entscheidung durch den IT-Rat Baden-Württemberg i. S. eines Rechtsbehelfs aufschiebende Wirkung entfalten oder sich nur um eine „nacheilende“ Rechtmäßigkeitskontrolle handeln solle. Ersteres würde erfordern, dass die Präsidentin oder der Präsident der Cybersicherheitsagentur ihre bzw. seine Entscheidung für sofort vollziehbar erkläre, weil anderenfalls die Gefahr nicht effektiv abgewehrt werden könnte.

Haltung der Landesregierung

Eine Überprüfung nach Satz 7 setzt notwendig eine bereits vorausgegangene Entscheidung der Cybersicherheitsagentur voraus. Auch aus dem Zusammenhang ergibt sich, dass es sich um eine nachträgliche Kontrolle handelt.

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Ungeklärt sei schließlich, welche Maßnahmen die Behörde auf wessen Kosten anordnen kann; die hiermit zusammenhängenden Fragen stellen sich insbesondere bei einem Tätigwerden gegenüber Privaten:

- *Soll dies Zutritts- und/oder Beschlagnahmerechte der Cybersicherheitsagentur umfassen?*
- *Soll sie berechtigt sein, ihrerseits Prüfsoftware auf die Server und Geräte der Betroffenen aufzuspielen?*
- *Soll die Cybersicherheitsbehörde „Stilllegungen“ ganzer IT-Systeme anordnen können und – bejahendenfalls – in welchem Umfang und für welche Zeiträume?*
- *Soll die Cybersicherheitsbehörde „Ersatzvornahmen“ durchführen können?*
- *Wie soll damit umgegangen werden, wenn die Cybersicherheitsagentur zu zögerlich handelt oder die falschen Maßnahmen ergreift? Mit anderen Worten: Haftet die Cybersicherheitsagentur für etwaige Versäumnisse?*

Richtig sei, dass die Cybersicherheitsagentur bei der Wahrnehmung der ihr eingeräumten Befugnisse auf den Verhältnismäßigkeitsgrundsatz, den Schutz personenbezogener Daten und den Schutz geistigen Eigentums Rücksicht nehmen müsse.

Haltung der Landesregierung

Unter Berücksichtigung der vom Anwaltsverband aufgezeigten Kriterien sind diese Fragen im jeweiligen Einzelfall zu beantworten.

Architektenkammer Baden-Württemberg

Um die öffentlichen Stellen vor Cybergefährdungen zu schützen, könne die Cybersicherheitsagentur erforderliche Anordnungen treffen und Maßnahmen ergreifen (Satz 1). Zuvor habe sie eine angemessene Frist zu setzen, um die Gefahr beseitigen zu lassen (Satz 2). Aus der Gesetzesbegründung werde ersichtlich, dass mit diesen Sätzen der Verhältnismäßigkeitsgrundsatz eingehalten werden solle.

Angeregt wird die explizite Aufnahme in § 5 Absatz 1 Satz 2, dass die Anordnungen und Maßnahmen nach dem Grundsatz der Verhältnismäßigkeit getroffen würden. Die gesetzgeberische Intention werde zwar in der Begründung ersichtlich, sei aber von solcher Bedeutung, dass sie unmittelbar in dem Gesetzestext aufzunehmen sei, um Rechtsklarheit an dieser Stelle zu gewährleisten.

Haltung der Landesregierung

Dass die explizite Aufnahme des Grundsatzes der Verhältnismäßigkeit in § 5 Absatz 1 Satz 2 die Rechtsklarheit erhöhen würde, ist nicht ersichtlich. Vielmehr ist der Grundsatz der Verhältnismäßigkeit stets im Verwaltungsrecht zu beachten und die Erwähnung nur in § 5 Absatz 1 Satz 2 würde die Frage aufkommen lassen, warum dieser Grundsatz beispielsweise nicht auch in den anderen Paragrafen erwähnt ist.

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Der Vollständigkeit halber werde hier nochmals erwähnt, dass § 5 Absatz 1 lediglich „die öffentlichen Stellen und das Landesverwaltungsnetz“ als Aufgabenbereich sähe und nicht wie in der Präambel dargestellt sei die Cybersicherheit des gesamten Landes.

Haltung der Landesregierung

Eine Präambel ist nicht vorgesehen. Über die vorgesehenen Befugnisse zum Schutz der öffentlichen Stellen und des Landesverwaltungsnetzes hinaus sind in dem Cybersicherheitsgesetz weitere Aufgaben und Befugnisse enthalten, um die Cybersicherheit im gesamten Land zu verbessern.

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Dringend wird angeraten, dass Maßnahmen der Gefahrenabwehr vor deren Ergreifen mit dem Landeskriminalamt abzustimmen seien. Dies vor allem vor dem Hintergrund, dass ansonsten möglicherweise wichtige Beweismittel eines Cyberangriffs unwiederbringlich verloren gehen könnten.

Haltung der Landesregierung

Eine Abstimmung von Maßnahmen der Gefahrenabwehr wird mit dem Landeskriminalamt nach Maßgabe der aufgrund § 13 Nummer 5 zu erlassenden Rechtsverordnung erfolgen.

Landesverband Baden-Württemberg des Bundes Deutscher Kriminalbeamter

Die Befugnisse aus § 5 des Gesetzesentwurfs stellten einen tiefen Eingriff insbesondere in die operative polizeiliche Infrastruktur des Landes dar. Das dürfte bei der Bearbeitung von Ereignissen ein Spannungsfeld verursachen – auch bei Gemengelagen der Gefahrenabwehr und Strafverfolgung (und solche Lagen sind die Regel).

Haltung der Landesregierung

Die operative polizeiliche Infrastruktur ist nach § 5 Absatz 1 Satz 8 ausgenommen.

b) Zu § 5 Absatz 2 CSG

Universitätsklinikum Tübingen und Universitätsklinikum Ulm

Die Herausgabe von Protokolldaten könnte möglicherweise mit Dienstvereinbarungen (zwischen Dienststelle und zuständigem Personalrat) kollidieren, die eine Herausgabe dieser personenbezogenen oder -beziehbaren Daten von Beschäftigten der öffentlichen Stelle einschränken. Soweit der Gesetzesverfasser nicht der Meinung sei, dass eine spezifische Regelung hierfür erforderlich sei, sollte zumin-

dest in der Gesetzesbegründung klargestellt werden, dass die gesetzliche Regelung materiellem Recht in Form von Dienstvereinbarungen bei Bedarf vorangehe.

Haltung der Landesregierung

Nach § 85 Absatz 1 Satz 1 des Landespersonalvertretungsgesetzes sind Dienstvereinbarungen nur zulässig, soweit eine gesetzliche oder tarifliche Regelung nicht besteht. Bereits nach allgemeinen Regeln folgt aus der Kollision einer Dienstvereinbarung mit höherrangigem Recht die Unwirksamkeit einer widersprechenden Regelung in einer Dienstvereinbarung (Hauck-Scholz, Rechtskontrolle von Dienstvereinbarungen, in: öAT – Zeitschrift für das öffentliche Arbeits- und Tarifrecht 2017, Seite 68, 70). Dementsprechend bedarf es keiner speziellen Regelung der Rechtsfolge im Cybersicherheitsgesetz, weil eine dem Cybersicherheitsgesetz widersprechende Regelung in einer Dienstvereinbarung nichtig wäre.

c) Zu § 5 Absatz 2, 3 und 5 CSG

Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Die von der Cybersicherheitsagentur gemäß § 5 Absatz 2 Satz 1 erhobenen Daten könnten Personenbezug aufweisen. Soweit dies der Fall sei, regelten die Absätze 3 und 5 bis 9 die weitere Verarbeitung. § 5 Absatz 2 Satz 1 in Verbindung mit Absatz 8 lege dabei den Verarbeitungszweck fest (Artikel 5 Absatz 1 Buchstabe b der Verordnung [EU] 2016/679). Die Verpflichtung zur Pseudonymisierung entspreche der Gewährleistung eines angemessenen Schutzniveaus (Artikel 32 Absatz 1 Buchstabe a der Verordnung [EU] 2016/679). Die Pflicht zur sofortigen Löschung (§ 5 Absatz 2 Satz 3) sowie die maximale Speicherdauer von drei Monaten Absatz 3 Satz 1) erschienen angemessen (Artikel 17 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679).

§ 5 Absatz 5 berechtige, abweichend von den in Absätzen 2 und 3 geregelten Verarbeitungsbeschränkungen, zu weitergehenden Verarbeitungen. Als Zweckbestimmung werde die Erforderlichkeit zur Bestätigung oder Widerlegung eines Schadprogramms sowie zum Ergreifen von Gegenmaßnahmen angegeben. Dies entspreche noch den Grundsätzen einer zulässigen Zweckänderung im Sinne der Artikel 5 Absatz 1 Buchstabe b und Artikel 6 Absatz 4 der Verordnung (EU) 2016/679. Woraus sich allerdings die in der Begründung zu § 5 Absatz 5 angeführte Pflicht zur Benachrichtigung der „betroffenen Person“ (Artikel 4 Nummer 1 der Verordnung [EU] 2016/679) sowie die Ausnahme hiervon ergeben solle, sei nicht ohne Weiteres nachvollziehbar.

Haltung der Landesregierung

In der Begründung wird davon ausgegangen, dass beispielsweise bei einer Übertragung eines Schadprogramms auch personenbezogene Daten mitübertragen werden können. Werden diese personenbezogenen Daten bei der Abwehr von Gefahren für die Cybersicherheit verarbeitet, besteht nach Artikel 13 oder 14 der Verordnung (EU) 2016/679 grundsätzlich eine Pflicht zur Information der betroffenen Person. Diese Pflicht entfällt beispielsweise nach Artikel 14 Absatz 5 Buchstabe b der Verordnung (EU) 2016/679 dann, wenn die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

d) Zu § 5 Absatz 6 und 7 CSG

Landesbeauftragter für den Datenschutz und die Informationsfreiheit

§ 5 Absatz 6 und 7 regelten die Zweckänderung in der Form der Datenübermittlung an Dritte (Artikel 4 Nummer 10 der Verordnung [EU] 2016/679). Die Voraussetzungen des Artikels 6 Absatz 3 Satz 3 und 3 der Verordnung (EU) 2016/679 sieht der Landesbeauftragte als erfüllt.

e) Zu § 5 Absatz 7 CSG

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Absatz 7 zeige das Dilemma der Informationsübermittlung an die Polizei, sofern diese Zentralstelle Cybersicherheitsagentur dort nicht angesiedelt sei.

Haltung der Landesregierung

Absatz 7 berücksichtigt, dass personenbezogene Daten tendenziell in einem größeren Umfang zu Zwecken der Gefahrenabwehr als zur Strafverfolgung verarbeitet werden dürfen.

Landesstudierendenvertretung Baden-Württemberg

Die Landesstudierendenvertretung erachtet den Regelungsgegenstand von § 5 Absatz 7 als problematisch. Dieser Absatz beschreibe den Umgang mit sogenannten Zufallsfunden (vgl. § 108 StPO „Beschlagnahme anderer Gegenstände"). Der Gesetzentwurf sehe hier vor, dass die Übermittlung solcher Zufallsfunde einem Richtervorbehalt unterliege, also richterlich genehmigt werden müsse. Dies gelte allerdings nicht, wenn die Übermittlung 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" geschehe. Dieser Sachverhalt wird von der Landesstudierendenvertretung kritisiert, da bei Gefahr im Verzug die richterliche Entscheidung in aller Regel ausreichend schnell eingeholt werden könne oder aber die Entscheidung nachgeholt werden könne. Falls die nachträgliche Genehmigung nicht richterlich erteilt werde, so sei die Übermittlung rückwirkend für rechtswidrig zu erklären und die übermittelten Daten seien zu löschen. Also auch für § 5 Absatz 7 Satz 1 Nummer 2 soll der Richtervorbehalt gelten. Der in der Gesetzesbegründung genannte Verzicht auf den Vorbehalt wegen der „typischerweise bestehenden Eilbedürftigkeit" werde insoweit als ungerechtfertigt erachtet.

Haltung der Landesregierung

Auch die Landesstudierendenvertretung erkennt, dass die richterliche Entscheidung „in aller Regel" ausreichend schnell eingeholt werden könne, was aber auch bedeutet, dass es Fälle gibt, in denen dies nicht der Fall ist. Für diese Fälle besteht kein Richtervorbehalt. Eine nachträgliche richterliche Kontrolle der Datenübermittlung ist nicht erforderlich, weil die Daten zur Gefahrenabwehr, aber nicht zur Strafverfolgung eingesetzt werden.

f) Zu § 5 Absatz 10 und 11 CSG

Chaos Computer Club Stuttgart

Im Sinne der Transparenz staatlichen Handelns sollten die dem LfDI und dem Innenausschuss vorgelegten Berichte zeitgleich der Öffentlichkeit zugänglich gemacht werden.

Haltung der Landesregierung

Dem Transparenzgedanken stehen Sicherheitsinteressen gegenüber, weshalb die vergleichbaren Berichte des BSI auch nicht veröffentlicht werden. Aus den in den Berichten aufgeführten Daten könnten nämlich Rückschlüsse auf Abwehrmaßnahmen/-strategien gezogen werden.

g) Zu § 5 Absatz 12 CSG

Universitätsklinikum Ulm

Die Aufgaben der Cybersicherheitsagentur seien gut beschrieben, Hinweise, auf die Kooperation mit dem BSI (Bund) und der ENISA (EU) wären überdies hilfreich.

8. Zu Artikel 1 – § 6 CSG

a) Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

§ 7 CSG-E – Untersuchung

Kritisch sieht der Anwaltsverband die Ausführungen in der Gesetzesbegründung, dass z. B. großen Konzernen und deren Zulieferern eher mit technischer Unterstützung geholfen werden soll als anderen Unternehmen oder gemeinnützigen Einrichtungen. Von solch großen Konzernen könne erwartet werden, dass sie durch das Vorhalten eigener ausreichender IT-Abteilungen und zeitgemäßer Fortbildung der dortigen Mitarbeiter selbst vorsorgen. Offensichtlich solle hier die Wettbewerbsfähigkeit von großen Unternehmen gestützt werden, wie man auch an dem Argument sehe, dass besonders auf ihre just-in-time-Organisation Rücksicht genommen werden solle. Gerade solche großen Unternehmen hätten aber auch die Möglichkeit, ihre Ressourcen anders zu verteilen und so IT-Sicherheitsanforderungen gerecht zu werden. Die aus Steuermitteln finanzierten Kapazitäten der Cybersicherheitsagentur in diesem Bereich sollten allen Unternehmen gleichermaßen offenstehen und gerade kleine und mittlere Unternehmen unterstützen.

Haltung der Landesregierung

Die vom Anwaltsverband unter der Überschrift § 7 CSG-E – Untersuchung angeführte Kritik bezieht sich wohl auf die Beispiele, die bei § 6 Absatz 7 für die Wiederherstellung durch die Cybersicherheitsagentur angeführten „Stellen mit wichtiger Bedeutung für das öffentliche Gemeinwesen“ genannt sind. Um keine Missverständnisse aufkommen zu lassen, werden als weitere Beispiele Apotheken und Arztpraxen genannt.

b) Landesbeauftragter für den Datenschutz und die Informationsfreiheit

§ 6 regele Fälle, in denen die Cybersicherheitsagentur andere öffentliche Stellen durch sogenannte Mobile Incident Response Teams (MIRTs) unterstütze. Werden im Rahmen dieser Unterstützung personenbezogene Daten verarbeitet, entspreche dies datenschutzrechtlich einer Auftragsverarbeitung im Sinne des Artikels 28 der Verordnung (EU) 2016/679. Zwar könnten die Grundlagen einer solchen Auftragsverarbeitung gemäß Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 grundsätzlich auch durch Gesetz geschaffen werden. Dies erfolge in § 6 Absatz 3 bis 5 allerdings nur rudimentär. Insoweit sei zu klären, ob es in den Fällen des § 6 Absatz 1 jeweils der ergänzenden Vereinbarung gemäß Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 bedürfe. Sollte sich das Innenministerium der Auffassung, dass es sich im gegebenen Zusammenhang um eine Auftragsverarbeitung handele, nicht anschließen, wäre zu klären, auf welcher Rechtsgrundlage die um Unterstützung ersuchende öffentliche Stelle berechtigt sei, der Cybersicherheitsagentur personenbezogene Daten offenzulegen; § 6 Absatz 1 Nummer 1 in Verbindung mit § 5 Absatz 1 LDSG erscheine auf den ersten Blick diesbezüglich nicht tragfähig. Und im Bereich der Richtlinie (EU) 216/680 bedürfte es wohl entsprechender Befugnisse im Polizeigesetz sowie im Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden (LDSG-JB) in Verbindung mit Teil 3 des Bundesdatenschutzgesetzes. Hierzu werde um Stellungnahme gebeten.

Haltung der Landesregierung

Wenn die Cybersicherheitsagentur andere Stellen durch MIRTs unterstützt und dabei personenbezogene Daten verarbeitet, liegt eine Auftragsdatenverarbeitung im Sinne des Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 vor. Dafür gibt § 6 lediglich einen Rahmen vor. Die Verarbeitung der personenbezogenen Daten durch die Cybersicherheitsagentur hat nach Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen.

c) BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Unklar sei, inwiefern die Cybersicherheitsagentur die fachliche und technische Kompetenz besitze, die in diesem Paragrafen dargestellten Aufgaben und Leistungen auszuführen. Deutlich würde dies durch die explizite Nennung einer „Hinzuziehung qualifizierter dritter Personen". In diesem Fall sei kein Mehrwert zur bestehenden Struktur zu erkennen.

Haltung der Landesregierung

Die Regelung berücksichtigt, dass die Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme bei selten verwendeter, spezieller Soft- oder Hardware teilweise nur durch Hinzuziehung besonderer Spezialisten möglich sein wird.

9. Zu Artikel 1 – § 7 CSG

Architektenkammer Baden-Württemberg

In § 7 Absatz 1 Satz 1 werde der Cybersicherheitsagentur eingeräumt, die jeweilige Informationstechnik der öffentlichen Stelle zu untersuchen und zu bewerten.

Hier wird die Ergänzung angeregt, dass auf Antrag der betroffenen Stellen der jeweilige eigene Datenschutzbeauftragte an der Untersuchung und Bewertung aktiv und vollständig eingebunden werde.

Haltung der Landesregierung

Soweit personenbezogene Daten betroffen sind, reichen die Regelungen in Artikel 38 und 39 der Verordnung (EU) 2016/679 aus, um die Einbeziehung der behördlichen Datenschutzbeauftragten sicherzustellen.

10. Zu Artikel 1 – § 8 CSG

a) Allgemein

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Die Cybersicherheitsagentur könne nach § 8 die Öffentlichkeit oder die betroffenen Kreise vor Gefahren für die Cybersicherheit – auch unter Angabe des Namens des Herstellers oder Inverkehrbringers – warnen. Hiermit seien regelmäßig Eingriffe in den eingerichteten und ausgeübten Gewerbebetriebe nach Art. 14 GG und in die Berufsfreiheit nach Art. 12 GG verbunden.

Zu begrüßen sei, dass die von der Rechtsprechung geforderte gesetzliche Ermächtigungsgrundlage für solche Warnungen geschaffen werde. Es bleibe zu hoffen, dass sie von den Verantwortlichen dann auch maßvoll angewendet werde, um nachhaltige Schäden bei Unternehmen zu vermeiden. Haftungsrechtliche Fragen stellten sich nicht nur, falls sich eine Warnung der Cybersicherheitsagentur im Nachhinein unzutreffend herausstelle, sondern auch wenn sie im Einzelfall unverhältnismäßig sei. Ob die zweifellos gebotene Richtigstellung in derselben Form in der die Warnung erfolgt sei, als weitgehende Kompensation verstanden wer-

den könne, erscheine indes mehr als fraglich. Der Schaden durch mit der Warnung erfolgten Imageverlust sei zu diesem Zeitpunkt bereits eingetreten. Als Anspruchsgrundlage kämen entgegen den Erläuterungen in der Begründung jedoch nicht nur Amtshaftungs- und Folgenbeseitigungsansprüche in Betracht, sondern auch Unterlassungsansprüche.

Der Anwaltsverband befürwortet auch die Normierung der Löschungsfrist; sie sei geboten, um ausweislich der Entscheidung BVerfG, Beschluss vom 21. März 2018 – 1 BvF 1/13 –, BVerfGE 148, 40, den Grundrechtsschutz der Betroffenen Rechnung zu tragen.

b) Zu § 8 Absatz 1 CSG

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Während der sonstige Gesetzestext lediglich auf Landesbehörden fokussiert sei, sei hier in Absatz 1 die gesamte Öffentlichkeit als Adressat von Warnungen der Cybersicherheitsagentur genannt. Solche Warnungen würden aktuell insbesondere ausgesprochen vom BSI, dem BKA und den Landeskriminalämtern. Ob eine zusätzliche Instanz einen Mehrwert erbringe, dürfe bezweifelt werden. Zumal hierdurch zusätzlicher Abstimmungsbedarf zu erwarten sei.

Haltung der Landesregierung

Ein Mehrwert besteht beispielsweise darin, dass die Cybersicherheitsagentur bei ihren Maßnahmen neue Erkenntnisse für eine Warnung gewinnen kann und ohne weitere Verzögerung warnen kann.

c) Zu § 8 Absatz 2 CSG

BBW und seine Mitgliedsgewerkschaft Deutsche Polizeigewerkschaft, Landesverband Baden-Württemberg

Absatz 2 spreche von der Warnung nicht allgemein bekannter Sicherheitslücken. Solche sogenannten Exploits würden nach dem Kenntnisstand der Polizeigewerkschaft gerade auch von den Sicherheitsbehörden zur Einbringung von Maßnahmen der Quellen-TKÜ und Onlinedurchsuchung genutzt. Es sei daher dringend geboten, dass derartige Warnungen nicht ohne Abstimmung mit den Sicherheitsbehörden kommuniziert werden dürfen. Ansonsten würde deren Erfolg vereitelt.

Haltung der Landesregierung

Absatz 2 ermöglicht eine Ermessensentscheidung, wobei alle relevanten Aspekte einschließlich Einbeziehung anderer Stellen zu berücksichtigen sind.

Chaos Computer Club Stuttgart

Die Cybersicherheitsagentur dürfe ausschließlich der Sicherheit von Computern und Netzen verpflichtet sein und Informationen über Sicherheitslücken ausschließlich zu deren Beseitigung anwenden. Bei Kenntnisnahme von öffentlich bisher unbekannten IT-Sicherheitslücken, seien diese unverzüglich an das BSI und den Hersteller zu melden. Die Sicherheitslücken sollten im Rahmen von sogenannten Coordinated/Responsible Disclosure-Verfahren behoben und veröffentlicht werden. Eine Geheimhaltung von Sicherheitslücken oder gar deren Weitergabe an andere staatliche Stellen (z. B. ZITiS), um diese ggf. gezielt auszunutzen, müsse ausgeschlossen sein.

Haltung der Landesregierung

In Absatz 2 wird entsprechend § 7 Absatz 1 Satz 4 BSIG geregelt, dass der Kreis der zu warnenden Personen eingeschränkt werden kann. Dies erfolgt nach pflicht-

gemäßen Ermessen. Damit wird keine Befugnis der Weitergabe von Informationen an andere staatliche Stellen geregelt.

11. Zu Artikel 1 – Teil 3

ARGE-HPR

Wichtig sei die Gewährleistung, dass schutzwürdige Daten der Personalvertretungen und der Schwerbehindertenvertretung nicht verarbeitet würden.

Haltung der Landesregierung

Die Regelungen zum Schutz der Daten der Personalvertretungen und Schwerbehindertenvertretung sind als Spezialregelungen zu berücksichtigen.

12. Zu Artikel 1 – § 9 CSG

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Gegen den Vorrang des CSG vor dem Landesdatenschutzgesetz bestünden mit Blick auf den Gesetzeszweck des CSG keine grundsätzlichen Bedenken.

13. Zu Artikel 1 – § 10 CSG

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Der Anwaltsverband begrüßt die Aufnahme expliziter Regeln zum Kernbereichsschutz in den Gesetzestext.

Zweifel wecke jedoch die konkrete Ausgestaltung, wenn Fälle, in denen sich die Frage stelle, ob Daten aus dem Kernbereich privater Lebensgestaltungen erhoben worden sei, der oder dem behördlichen Datenschutzbeauftragten der Cybersicherheitsagentur sowie einer oder einem weiteren Bediensteten der Cybersicherheitsagentur mit Befähigung zum Richteramt zur Kontrolle vorzulegen seien. Hier werde nicht deutlich, was die Aufgabe der oder des „weiteren Bediensteten der Cybersicherheitsagentur mit Befähigung zum Richteramt“ sein solle.

Zwar bestimme § 5 Absatz 5 Satz 4, dass, „die nicht automatisierte Verarbeitung der Daten nach den Sätzen 1 und 2 … nur durch Bedienstete mit der Befähigung zum Richteramt angeordnet werden“ dürfe. Zum einen sei dies die – soweit ersichtlich – einzige Norm die konkrete Befugnisse auf Bedienstete mit der Befähigung zum Richteramt beschränke; ob die dort angesprochenen personenbezogenen Daten zugleich zum Kernbereich privater Lebensführung zählten, sei damit noch nicht gesagt. Auch ergebe sich daraus nicht, dass die Entscheidung der Cybersicherheitsagentur zwingend von einer bzw. einem Bediensteten mit der Befähigung zum Richteramt zu treffen sei, was jedoch sinnvoll wäre.

Zum anderen lege die Formulierung, der zufolge ein(e) weitere(r) Bediensteter mit der Befähigung zum Richteramt hinzuziehen sei, nahe, dass es sich insoweit nicht um dieselbe Person handeln könne. Damit stelle sich aber die Frage, welche Befugnisse, diese(r) weitere Bedienstete haben solle.

Denn die Letztentscheidung treffe die oder der behördliche Datenschutzbeauftragte, wenn die Löschung nachzuholen sei, sofern sie oder er der Entscheidung der Cybersicherheitsagentur widerspreche. Oder solle – zum dritten – damit lediglich zum Ausdruck gebracht werden, dass die oder der Datenschutzbeauftragte der Cybersicherheitsagentur (ebenfalls) über die Befähigung zum Richteramt verfügen müsse? Dann sollte dies explizit geregelt werden.

Haltung der Landesregierung

Der Sinn und Zweck der Einbeziehung einer oder eines weiteren „Bediensteten der Cybersicherheitsagentur mit Befähigung zum Richteramt“ besteht in einem Vieraugenprinzip und der Einbeziehung qualifizierten juristischen Sachverstands. Diese Person und die oder der behördliche Datenschutzbeauftragte müssen überzeugt sein, dass der Kernbereich privater Lebensgestaltung durch die verarbeiten Daten nicht betroffen ist; ansonsten sind die Daten zu löschen. Die Anforderungen an die Qualifikation der oder des behördlichen Datenschutzbeauftragten ergeben sich aus Artikel 37 Absatz 5 der Verordnung (EU) 2016/679, wonach nicht zwingend die Befähigung zum Richteramt voraussetzt wird. Um keine Missverständnisse aufkommen zu lassen, dass ausreicht, wenn eine Person mit Befähigung zum Richteramt beteiligt wird, wird die Reihenfolge der Nennung in § 10 Satz 5 getauscht, sodass sich bereits aus dem Wortlaut ergibt, dass die oder der behördliche Datenschutzbeauftragte nicht auch die Befähigung zum Richteramt haben muss.

14. Zu Artikel 1 – § 11 CSG

a) Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Der Anwaltsverband begrüßt die Aufnahme des Verwertungsverbots von Erkenntnissen, die bei von den Zeugnisverweigerungsrechten nach §§ 53, 53a StPO geschützten Personen gewonnen werden.

Die konkrete Formulierung erscheine jedoch missverständlich. § 11 Satz 5 solle gewiss – insoweit § 9 a Absatz 4 PolG vergleichbar – eine Ausnahme zu § 11 Sätze 1 bis 4 darstellen, beziehe sich bei genauer Betrachtung jedoch nur auf den unmittelbar vorangegangenen Satz 4. Es erscheine deshalb vorzugswürdig entweder zu formulieren:

„Sätze 1 bis 4 gelten nicht …“

oder § 11 Sätze 1 bis 4 zu § 11 Abs. 1 zusammenzufassen und § 11 Satz 5 als § 11 Abs. 2 wie folgt zu fassen:

„Absatz 1 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.“

Haltung der Landesregierung

Wenngleich bereits aus Sinn und Zweck der Regelung sowie der Begründung deutlich wurde, dass sich ein Satzanfang mit „dies“ in § 11 Satz 5 auf alle vorstehenden vier Sätze beziehen sollte, soll dies im Wortlaut entsprechend dem ersten Vorschlag des Anwaltsverbands klargestellt werden.

b) Rechtsanwaltskammern Freiburg, Karlsruhe, Stuttgart und Tübingen

Die Rechtsanwaltskammern begrüßen ausdrücklich den in § 11 geregelten Schutz der Zeugnisverweigerungsberechtigten entsprechend der Regelung in § 53 Absatz 1 Satz 1 und § 53a StPO.

15. Zu Artikel 1 – § 11 und § 12 CSG

Universitätsklinikum Tübingen und Universitätsklinikum Ulm

Hier werde einerseits korrekterweise die Problematik der Zeugnisverweigerungsrechte z. B. von Ärzten behandelt. Es seien andererseits die erforderlichen datenschutzrechtlichen Erlaubnisse für eine befugte Verarbeitung personenbezogener Daten nach Artikel 6 der Verordnung (EU) 2016/679 und zur Verarbeitung be-

sonderer Kategorien personenbezogener Daten (wie Gesundheitsdaten, genetische Daten, biometrische Daten) enthalten. Unklar sei, ob damit auch eine Offenbarung/Offenlegung im Sinne von Schweige-/Geheimhaltungspflichten nach § 203 des Strafgesetzbuchs umfasst sei und die an Krankenhäusern Beschäftigten somit ihre Berufsgeheimnisse nicht verletzen. Sollte dies nicht hinreichend umfasst sein; sollte eine entsprechende Regelung aufgenommen werden.

Haltung der Landesregierung

Nur selten werden von der Cybersicherheitsagentur Daten verarbeitet werden, die durch Schweige-/Geheimhaltungspflichten nach § 203 des Strafgesetzbuchs geschützt sind. Ein Offenbaren im Verkehr mit externen Behörden ist dann gerechtfertigt, wenn dies durch eine rechtliche Vorgabe gebilligt wird (Weidemann, in: BeckOK StGB, 47. Ed. 1. August 2020, StGB § 203 Randnummer 55). Dies ist anzunehmen, soweit Datenverarbeitungsbefugnisse der Cybersicherheitsagentur bestehen.

16. Zu Artikel 1 – § 12 CSG

a) Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Unklar erscheine das Verhältnis des § 12 zu den Anforderungen des Landesdatenschutzgesetzes, insbesondere in Bezug auf den Grundsatz der Datensparsamkeit, der Zweckänderung u. ä.

Haltung der Landesregierung

An die Stelle des Grundsatzes der Datensparsamkeit nach nationalem Recht ist der Grundsatz der Datenminimierung in Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 getreten, der in allen Mitgliedstaaten der EU unmittelbar gilt. Der Grundsatz der Zweckbindung ist in Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 geregelt. Auf Basis von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e und Absatz 3 Satz 1 Buchstabe b der Verordnung (EU) 2019/679 wird § 12 als datenschutzrechtliche Ermächtigungsgrundlage geschaffen, womit insbesondere die Reichweite der Zweckbindung konkretisiert wird.

b) Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Die Datenerhebungsbefugnis nach § 12 Absatz 1 solle offenbar einen Auffangtatbestand bilden, soweit die spezielle Datenerhebungsbefugnis des § 5 Absatz 2 Satz 1 nicht ausreiche. Welche Aufgaben der Cybersicherheitsagentur aber neben der Abwehr von Gefahren für die Cybersicherheit obliegen, die nicht bereits durch die auf der Grundlage des § 5 Absatz 2 Satz 1 zu erhebenden Daten abgewehrt werden könnten, bleibe offen. Gleiches gelte für die in den Absätzen 2 und 3 geregelten Weiterverarbeitungsbefugnisse.

Haltung der Landesregierung

Über die speziellen Datenverarbeitungsbefugnisse der §§ 5 ff. hinaus sind die Auffangtatbestände des § 12 beispielsweise notwendig, um personenbezogene Daten im Vorfeld einer Warnung zu verarbeiten.

17. Zu Artikel 1 – § 15 CSG

Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Der Anwaltsverband hält eine Erweiterung der Berichtspflichten für geboten; so sollte die Pflicht zur jährlichen umfänglichen Unterrichtung über die Ausübung der eingeräumten Befugnisse, den Erkenntnissen zur Bedrohungslage und zu technischen Weiterentwicklungen auch gegenüber dem Innenausschuss des Landtags und gegenüber der bzw. dem Landesdatenschutzbeauftragten bestehen.

Wenn die bzw. der Landesdatenschutzbeauftragte aus zutreffenden Erwägungen bei der Evaluation zu beteiligen sei, gebiete es die Sachnähe, sie bzw. ihn bereits in die Berichtspflichten einzubeziehen.

Haltung der Landesregierung

Eine Einbeziehung des Innenausschusses sowie der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit ist nicht erforderlich, da auch sie oder er Teil der nach Absatz 2 zu informierenden Öffentlichkeit ist.

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

a) AGSV BW, ARGE-HPR und Hauptschwerbehindertenvertretung der Polizei

In Absatz 1 Satz 1 sei formuliert, dass von der Zusage der Umzugskostenvergütung abzusehen sei, wenn im Zeitpunkt der Versetzung

1. die Beamtin oder der Beamte … b) in der Erwerbsfähigkeit um mindestens 50 Prozent gemindert sei … Absatz 8 laute: „Bei Tarifbeschäftigten ist entsprechend zu verfahren.“

Im Dienstrecht des Landes Baden-Württemberg sei durch das Dienstrechtsreformgesetz 2010 im Landesbeamtenversorgungsgesetz der vormalige Begriff „Minderung der Erwerbsfähigkeit (MdE)“ ersetzt worden durch die Bezeichnung „Grad der Schädigungsfolgen (GdS)“ (siehe §§ 50 ff. LBeamtVGBW). Für bleibende Dienstunfallschädigungen werde seitdem nicht mehr eine MdE, sondern der GdS festgestellt. In der Beamtenschaft existierten zwar noch Altfälle mit dienstunfallrechtlich festgestellter MdE, in Bezug auf die Rechtsfolgenanwendung bestehen aber keine Unterschiede gegenüber einem festgestellten GdS in gleicher Höhe, was den Verwaltungen bekannt sei.

In der für tariflich Beschäftigte des Landes maßgeblichen gesetzlichen Unfallversicherung (SGB VII) finde die Begrifflichkeit „Minderung der Erwerbsfähigkeit“ hingegen nach wie vor Anwendung. In der gesetzlichen Rentenversicherung (SGB VI) werde außerdem nach „voller Erwerbsminderung“ und „teilweiser Erwerbsminderung“ unterschieden.

Um alle Varianten der Begrifflichkeiten zweifelsfrei abzubilden, werde folgende Formulierung vorgeschlagen:

Absatz 1 Satz 1 Nummer 1 Buchstabe b):

„einen dienstunfallrechtlich festgestellten Grad der Schädigungsfolgen (GdS) von mindestens 50 vorweist oder“

Absatz 8:

„Bei Tarifbeschäftigten ist entsprechend zu verfahren. Als Voraussetzung nach Abs. 1 Satz 1 Nr. 1 Buchst. b) dieses Artikels gilt eine Minderung der Erwerbsfähigkeit um mindestens 50 Prozent nach § 56 SGB VII oder eine Erwerbsminderung nach § 43 SGB VI.“

Haltung der Landesregierung

Der Wortlaut wird dementsprechend angepasst.

b) Beauftragte der Landesregierung für die Belange von Menschen mit Behinderungen

Bei der Regelung in Absatz 1 Ziffer 1 a) betr. Absehen von der Zusage der Umzugskostenvergütung bittet sie, neben schwerbehinderten Beamtinnen und Beamten auch diesen gleichgestellte Beamtinnen und Beamte einzubeziehen.

Ziffer 1 a) sei daher wie folgt zu fassen:

„1. die Beamtin oder der Beamte

a) das 61. Lebensjahr, im Falle einer Schwerbehinderung im Sinne des § 2 Absatz 2 oder einer Gleichstellung nach § 2 Absatz 3 des Neunten Buches Sozialgesetzbuch (SGB IX) das 58. Lebensjahr, vollendet hat oder“.

Bei der Formulierung des Tatbestands in Absatz 1 Ziffer 2 sei die Verwendung des Begriffs „Einrichtung“ mit Blick auf den tatsächlichen Aufenthalt bei langer schwerer Erkrankung bzw. dauernder Pflegebedürftigkeit nicht mehr zeitgemäß.

Ziffer 2 sei daher wie folgt zu fassen:

„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 einem Betreuungsangebot lebt untergebracht ist~~, das vom neuen Dienstort mindestens doppelt so weit entfernt ist als vom bisherigen Dienst- oder Wohnort oder“.

Absatz 4 sei zur Klarstellung wie folgt zu fassen:

(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 61., im Falle einer Schwerbehinderung im Sinne des § 2 Absatz 2 SGB IX oder einer Gleichstellung nach § 2 Absatz 3 SGB IX das 58. ~~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.

Im Übrigen gehe sie davon aus, dass im Sinne ihrer Ausführungen zum Treffen angemessener Vorkehrungen im Sinne der UN-Behindertenrechtskonvention im Einzelfall beim Verzicht auf die Zusage von Umzugskostenvergütung selbstverständlich auch die Fallkonstellationen berücksichtigt werde, die allgemein in § 12 Absatz 4 LUKG bzw. § 2 Absatz 2 LTGVO Niederschlag gefunden habe. Auch diese Regelungen führten dazu, dass ohne die Voraussetzungen der uneingeschränkten Umzugswilligkeit sowie des nachgewiesenen Wohnungsmangels während einer Übergangszeit Trennungsgeld gewährt werde. Ganz besonders denke sie hierbei an die Belange eines schwerbehinderten Kindes, welches eine Schul- oder Berufsausbildung absolviere.

Haltung der Landesregierung

Der Wortlaut wird dementsprechend angepasst und die Anregungen sollen bei der Umsetzung berücksichtigt werden.

19. Zu Artikel 5 – Personalverwaltung

Hauptpersonalrat beim Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg

Für den Hauptpersonalrat sei die geplanten Regelungen zur Zuständigkeit der Personalverwaltung nach § 2 nicht nachvollziehbar.

Haltung der Landesregierung

§ 2 wurde mit dem Hauptpersonalrat erörtert und danach vom Hauptpersonalrat akzeptiert.

20. Zu Artikel 9 – Überprüfung der Auswirkungen des Gesetzes

a) Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V.

Richtig sei es, eine Überprüfung der Auswirkungen des Cybersicherheitsgesetzes nach drei Jahren vorzusehen.

Der Einsatz der veranschlagten Haushaltsmittel und von mehr als 80 Personalstellen sollte auf seine Effektivität hin untersucht werden. Insbesondere sollte sich bis dahin zeigen, welche „Konkurrenzverhältnisse" zu bereits bestehenden Stellen bestehen, damit Doppelstrukturen abgebaut werden könnten. Es sollte auch untersucht werden, ob die geplanten Hilfestellungen für die mit diesem Gesetz Begünstigten tatsächlich eine wertvolle Unterstützung bei der Herstellung einer möglichst großen Cybersicherheit darstellen würden. Die Aufarbeitung digitaler Angriffe sei meist recht komplex und aufwendig. Es sollte geklärt werden, inwieweit eine solche Cybersicherheitsbehörde über ausreichend technische und personelle Kapazitäten verfüge, um die gewünschten Untersuchungen durchführen, die Funktionsfähigkeit informationstechnischer Systeme wiederherstellen zu können sowie Standards und Maßnahmen durchzusetzen.

Haltung der Landesregierung

Diese Aspekte sollen bei der Evaluierung berücksichtig werden.

b) Landesverband Baden-Württemberg des Bundes Deutscher Kriminalbeamter

Die Evaluation müsse zwingend die Landespolizei miteinbeziehen, beispielsweise in persona der Abteilungsleitung 3 des Innenministeriums.

Haltung der Landesregierung

Bei der Evaluation durch die Landesregierung werden alle Beteiligten der Landesregierung (also auch mittelbar die Abteilung 3 – Landespolizeipräsidium – des Innenministeriums) sowie die relevanten Stakeholder einbezogen.

21. Zu Artikel 10 – Änderung des ADV-Zusammenarbeitsgesetzes

Chaos Computer Club Stuttgart

Um die Vertraulichkeit der Sitzungen sicherzustellen, sollte das von Komm.ONE bereitgestellte System die Kommunikation mittels Ende-zu-Ende-Verschlüsselung absichern. Die verwendete Technologie müsse dem Stand der Technik entsprechen und der Quellcode der verwendeten Software öffentlich zugänglich sein, denn nur so könne dessen Vertrauenswürdigkeit und Sicherheit überprüft werden.

Haltung der Landesregierung

„Übertragung von Bild und Ton mittels geeigneter technischer Hilfsmittel" setzt voraus, dass die eingesetzten technischen Hilfsmittel dem Stand der Technik entsprechen. Dementsprechend hat der Vorstand auch „sicherzustellen, dass die technischen Anforderungen und die datenschutzrechtlichen Bestimmungen für eine ordnungsgemäße Durchführung der Sitzung einschließlich Beratung und Beschlussfassung eingehalten werden". Zu den technischen Anforderungen für eine ordnungsgemäße Durchführung der Sitzung gehören auch Sicherungsmaßnahmen zur Vertraulichkeit der Sitzung.

Baden-Württemberg

NORMENKONTROLLRAT BADEN-WÜRTTEMBERG

5. November 2020

Stellungnahme des Normenkontrollrats Baden-Württemberg gemäß Nr. 6.1 VwV NKR BW

Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften

NKR-Nummer 121/2020, Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg

Der Normenkontrollrat Baden-Württemberg hat den Entwurf des oben genannten Regelungsvorhabens geprüft.

I. Zusammenfassung

Bürgerinnen und Bürger
Keine Auswirkungen

Wirtschaft
Geringfügiger Erfüllungsaufwand

Verwaltung (Land/Kommunen)	
Jährlicher Erfüllungsaufwand:	8.311.200 Euro
• *davon Personalkosten:*	*6.898.200 Euro*
• *davon Sachkosten:*	*1.413.000 Euro*
Einmaliger Erfüllungsaufwand:	2.036.200 Euro
• *davon Personalkosten:*	*261.200 Euro*
• *davon Sachkosten:*	*1.775.000 Euro*

II. Im Einzelnen

Mit dem vorliegenden Regelungsvorhaben wird die Landesoberbehörde Cybersicherheitsagentur Baden-Württemberg errichtet sowie deren Aufgaben und Befugnisse geregelt. Die Cybersicherheitsagentur soll die öffentlichen Stellen im Bereich der Informationssicherheit unterstützen und bereits bestehende Strukturen ergänzen. Die Cybersicherheitsagentur kann in Einzelfällen auch nicht-öffentliche Stellen beraten und bei Sicherheitsvorfällen unterstützen sowie die Bürgerinnen und Bürger zu Themen der Cybersicherheit sensibilisieren. Durch das vorliegende Regelungsvorhaben wird es zudem der Komm.ONE ermöglicht, Verwaltungsratssitzungen unter bestimmten Voraussetzungen in digitaler Form durchzuführen.

II.1. Erfüllungsaufwand

II.1.1. Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht durch das Regelungsvorhaben kein Erfüllungsaufwand.

II.1.2. Wirtschaft

Nach dem Gesetzesentwurf kann die Cybersicherheitsagentur die Öffentlichkeit oder betroffene Kreise vor Gefahren für die Cybersicherheit warnen und Sicherheitsmaßnahmen empfehlen. Die Person, die das betroffene Produkt oder den betroffenen Dienst hergestellt bzw. in den Verkehr gebracht hat, darf hierbei unter bestimmten Umständen genannt werden, ist aber in der Regel zuvor anzuhören. Für die Wirtschaft entsteht durch die Anhörung lediglich ein geringfügiger Erfüllungsaufwand.

II.1.3. Verwaltung

Für die Verwaltung entstehen durch das vorliegende Regelungsvorhaben ein einmaliger Erfüllungsaufwand in Höhe von etwa 2.036.200 Euro sowie ein jährlicher Erfüllungsaufwand in Höhe von etwa 8.311.200 Euro. Der Erfüllungsaufwand setzt sich wie folgt zusammen:

Der einmalige Erfüllungsaufwand wird maßgeblich durch institutionelle Kosten für die Einrichtung der Cybersicherheitsagentur bestimmt (weitere Regelungskosten). Der einmalige Sachaufwand, insbesondere für bauliche Maßnahmen, beträgt 1.775.000 Euro. In diesem Zusammenhang wird für die Projektsteuerung ein einmaliger Personalaufwand in Höhe von etwa 42.600 Euro geschätzt. Diesem Wert liegt die Annahme zugrunde, dass für diese Tätigkeit circa drei Prozent des Sachaufwandes (abzüglich Nebenkosten) zu veranschlagen sind. Die Personalrekrutierung für die Cybersicherheitsagentur führt zu einem einmaligen Personalaufwand in Höhe von rund 72.800 Euro (je eine Person des höheren Dienstes (933 Stunden x 60,50 Euro) sowie des gehobenen Dienstes (400 Stunden x 40,80 Euro).

Da die Cybersicherheitsagentur die zentrale Koordinierungs- und Meldestelle für die Zusammenarbeit der öffentlichen Stellen in Angelegenheiten der Cybersicherheit in Baden-Württemberg sein wird, werden Anpassungen in den vier Rechenzentren im Land notwendig. In den Rechenzentren ist ein einmaliger Umstellungsaufwand in Höhe von 0,5 Vollzeitäquivalenten des gehobenen Dienstes für jeweils ein Jahr zu erwarten. Das führt zu einem einmaligen Personalaufwand (weitere Regelungskosten) in Höhe von etwa 130.600 Euro (4 x 800 Stunden x 40,80 Euro).

Die Cybersicherheitsagentur wird mit den obersten Landesbehörden (z.B. Landesdatenschutzbeauftragter und Rechnungshof) gesonderte Vereinbarungen zur Zusammenarbeit treffen. Es wird von sechs Vereinbarungen ausgegangen. Bei einem Zeitaufwand von 40 Stunden pro Vereinbarung bei den obersten Landesbehörden entsteht ein einmaliger Personalaufwand (Bürokratiekosten) in Höhe von rund 12.200 Euro (6 x ((20 Stunden x 60,50 Euro) + (20 Stunden x 40,80 Euro))).

Die Auswirkungen des vorliegenden Regelungsvorhabens sind nach drei Jahren durch die Landesregierung unter Mitwirkung der kommunalen Landesverbände, der oder des Landesbeauftragten für den Datenschutz und gegebenenfalls weiterer sachverständiger Personen zu überprüfen. Für die Mitwirkenden, die nicht der Landesregierung zuzurechnen sind, wird hierfür insgesamt von einmaligen Bürokratiekosten (Personalaufwand) in Höhe von 3.000 Euro ausgegangen.

Der jährliche Erfüllungsaufwand setzt sich zusammen aus einem Personalaufwand in Höhe von 6.898.200 Euro sowie einem Sachaufwand in Höhe von 1.413.000 Euro. Der Sachaufwand wird in Höhe des Haushaltsansatzes pro Jahr angenommen. Berücksichtigt hier u.a. Ausgaben für Geschäftsbedarf, Ausstattungs- und Ausrüstungsgegenstände, Öffentlichkeitsarbeit und Veranstaltungen sowie für Fortbildungen. Dem Personalaufwand zugrunde liegen 51 Stellen im höheren Dienst, 22 Stellen im gehobenen Dienst sowie zehn Stellen im mittleren Dienst (((51 x 60,50 Euro pro Stunde) + (22 x 40,80 Euro pro Stunde) + (10 x 31,40 Euro pro Stunde)) x 1.600 Stunden). Dadurch entstehen jährliche Personalkosten in Höhe von rund 6.875.400 Euro. Es handelt sich insgesamt um weitere Regelungskosten (institutionelle Kosten).

Beim Innenministerium Baden-Württemberg entsteht für die Ausübung der Dienst- und Fachaufsicht über die Cybersicherheitsagentur weiterer Erfüllungsaufwand (weitere Regelungskosten) in Form von jährlichem Personalaufwand in Höhe von rund 10.600 Euro (175 Stunden x 60,50 Euro).

Die Cybersicherheitsagentur kann die Sicherheit der Informationstechnik der öffentlichen Stellen des Landes und der an das Landesverwaltungsnetz angeschlossenen Stellen untersuchen und bewerten. Durch die Mitwirkung entstehen bei diesen Stellen Bürokratiekosten. Zielgröße ab dem Jahr 2022 sind sechs Untersuchungen und Bewertungen pro Jahr. Bei einem Zeitaufwand von 40 Stunden pro Stelle für die Mitwirkung entstehen somit jährliche Personalkosten in Höhe von rund 12.200 Euro (6 x ((20 Stunden x 60,50 Euro) + (20 Stunden x 40,80 Euro))).

II.2. Nachhaltigkeitscheck

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. Dadurch werden positive Auswirkungen auf die Zielbereiche ökologische und soziale Modernisierung der Wirtschaft sowie Verschuldung, leistungsfähige Verwaltung und Justiz erwartet.

III. Votum

Das Ressort hat die Auswirkungen des Regelungsvorhabens plausibel dargestellt.
Der Normenkontrollrat Baden-Württemberg erhebt im Rahmen seines Regierungsauftrags keine Einwände gegen die Darstellung der Regelungsfolgen. Der Normenkontrollrat weist jedoch darauf hin, dass der Erfüllungsaufwand, der durch die im Regelungsvorhaben angelegte Ermächtigung zu Rechtsverordnungen entstehen wird, bereits vollumfänglich bei der Folgekostenabschätzung dieses Gesetzesentwurfs zu berücksichtigen wäre. Da allerdings noch große Unsicherheiten bezüglich der Ausgestaltung der Verordnungen bestehen, wird ausnahmsweise darauf verzichtet. Der Erfüllungsaufwand ist daher zu berechnen, wenn weitere Verordnungen erlassen werden und dem Normenkontrollrat Baden-Württemberg vorzulegen. Bei der Ausgestaltung der weiteren untergesetzlichen Regelungen sollte besonders auf eine bürokratiearme Ausgestaltung geachtet werden. Dies betrifft vor allem mögliche Melde- und Informationspflichten.

Nach dem Beschluss des Ministerialdirektorenausschusses für Bürokratieabbau vom 4. November 2020 und der darin vorgesehenen länderspezifischen Anpassung der Folgekostenberechnung fallen einmalig 15.200 Euro und jährlich 12.200 Euro Verwaltungskosten an. Im Übrigen sind Folgekosten bereits in den Angaben zu den Auswirkungen auf den Landeshaushalt ausgewiesen, weshalb ein darüberhinausgehendes Transparenzinteresse entfällt.

Dr. Gisela Meister-Scheufelen	Prof. Dr. Gisela Färber
Vorsitzende und Berichterstatterin	stellvertretende Berichterstatterin

Verzeichnis der Abkürzungen

VwV NKR BW Verwaltungsvorschrift für den Normenkontrollrat Baden-Württemberg