Landtag von Baden-Württemberg **Drucksache 16 / 9723**

16. Wahlperiode

Gesetzesbeschluss

des Landtags

Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften

Der Landtag hat am 4. Februar 2021 das folgende Gesetz beschlossen:

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 Landesbe-

hörde 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 gel-

ten 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 öffent-

liche 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 Artikel 2 des Gesetzes 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.