Gesetzentwurf
der Staatsregierung

Gesetz zur Änderung des Bayerischen Digitalgesetzes

A) Problem

Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27. Dezember 2022, S. 80 – NIS-2-Richtlinie) enthält rechtliche Maßnahmen zur Steigerung des Gesamtniveaus der Cybersicherheit in der EU. Sie ist von den Mitgliedstaaten bis 17. Oktober 2024 umzusetzen.

Die Richtlinie (EU) 2022/2555 zielt auf einen weiten Anwendungsbereich. Sie gilt im Grundsatz nach ihrem Art. 2 Abs. 1 gesamtheitlich für öffentliche und private Einrichtungen, sodass eine Unterscheidung zwischen dem öffentlichen und dem privaten Sektor aus Sicht der Richtlinie grundsätzlich obsolet ist. Entscheidend sind andere Kriterien: Zum einen die Zuordnung zu einem Sektor, der in Anhang I und II der Richtlinie genannten Art, der die Kritikalität zum maßgeblichen Faktor erklärt, zum anderen die Unternehmensgröße.

Soweit Regelungsadressat der Richtlinie (EU) 2022/2555 Unternehmen in einem europarechtlich weit verstandenen Sinne sind, besteht eine konkurrierende Gesetzgebungskompetenz des Bundes zur Umsetzung gemäß Art. 74 Abs. 1 Nr. 11 des Grundgesetzes (Recht der Wirtschaft). Eine bundesrechtliche Regelung zur Umsetzung der NIS-2-Richtlinie ist noch nicht verabschiedet. Es ist jedoch davon auszugehen, dass der Bund, wie bereits bei der Umsetzung der Richtlinie (EU) 2016/1148 (sog. NIS-Richtlinie), von seiner konkurrierenden Gesetzgebungskompetenz Gebrauch machen wird.

Soweit darüber hinaus Regelungsadressat der Richtlinie (EU) 2022/2555 auch „Einrichtungen der öffentlichen Verwaltung“ auf Landesebene sind, hat eine Umsetzung der Richtlinie durch Landesrecht zu erfolgen, da dem Bund insoweit die Gesetzgebungskompetenz fehlt.

Mit der Errichtung des Landesamtes für Sicherheit in der Informationstechnik (LSI) und der gesetzlichen Verpflichtung der Behörden zu angemessener Informationssicherheit gemäß Art. 43 Abs. 1 des Bayerischen Digitalgesetzes (BayDiG) sowie der Einführung von Informationssicherheitsmanagementsystemen in den staatlichen Behörden wurden bereits Maßnahmen zur IT-Sicherheit für Verwaltungsbehörden in Bayern ergriffen, die den Zielsetzungen der Richtlinie (EU) 2022/2555 entsprechen. Insbesondere besteht das gemäß der Richtlinie (EU) 2022/2555 einzurichtende Computer Security Incident Response Team (CSIRT) bereits als Bayern-CERT im LSI. Zudem verfügt das LSI in seiner Funktion als Gefahrenabwehrbehörde bereits über Befugnisse, u.a. zur Untersuchung der Sicherheit in der Informationstechnik staatlicher und an das Behördennetz angeschlossener Stellen. Gleichwohl bedürfen die sehr detaillierten Vorgaben der Richtlinie (EU) 2022/2555 einer Umsetzung ergänzender Regelungen im Landesrecht. Dies betrifft etwa das nach der Richtlinie vorzusehende dreistufige Meldeverfahren, mit dem Einrichtungen im Anwendungsbereich der Richtlinie erhebliche Sicherheitsvorfälle an das LSI melden, oder die von der Richtlinie vorgesehen Aufsichts- und Durchsetzungsmaßnahmen gegenüber den vom Anwendungsbereich der Richtlinie erfassten Einrichtungen.

Aufgrund der sich erst noch abzeichnenden bundesrechtlichen Regelungen sind die nationalen Rahmenbedingungen weiterhin offen. Es ist nicht auszuschließen, dass nach Abschluss der Richtlinienumsetzung auf Bundesebene weitere punktuelle Anpassungen im Landesrecht erforderlich werden könnten. Zur Wahrung der Umsetzungsfrist ist gleichwohl bereits jetzt das BayDiG anzupassen.

B) Lösung

Für Bayern erfolgt in Bezug auf die von der Richtlinie (EU) 2022/2555 adressierten Einrichtungen der öffentlichen Verwaltung auf Landesebene (in diesem Gesetz als „Einrichtungen mit Bedeutung für den Binnenmarkt“, kurz „EBB“ bezeichnet) eine Umsetzung der Richtlinie „Eins-zu-eins“. Die detaillierten Vorgaben der Richtlinie lassen nur geringen Umsetzungsspielraum zu.

Ergänzend zur Umsetzung der Richtlinie (EU) 2022/2555 soll die Speicherfrist von Protokolldaten, die das LSI erhebt, von 12 auf 18 Monate verlängert werden und somit

an die derzeitige Rechtslage auf Bundesebene angeglichen werden. Mit dieser Verlängerung der Speicherfrist können nachträglich Angriffe auf das Behördennetz besser erkannt werden.

Die Umsetzung der Richtlinie (EU) 2022/2555 soll in einem eigenen Kapitel 4 im Teil 3 des BayDiG (IT-Sicherheit) erfolgen. Als zuständige Behörde (Aufsichtsbehörde) und CSIRT wird das LSI benannt und mit entsprechenden Aufgaben und Befugnissen ausgestattet.

C) Alternativen

Keine.

D) Kosten

1. Staat und Kommunen

Aufgrund der bereits ergriffenen Maßnahmen zur Stärkung der Sicherheit der Informationstechnik staatlicher Behörden ist hinsichtlich der Umsetzung der Richtlinie (EU) 2022/2555 mit einem geringen Erfüllungsaufwand zu rechnen. Die Umsetzung erfolgt im Rahmen der zur Verfügung stehenden Mittel und Stellen.

Nach dem vom IT-Planungsrat am 3. November 2023 beschlossenen sogenannten Identifizierungskonzept, das eine bundesweit einheitliche Auslegung des Anwendungsbereichs der Richtlinie (EU) 2022/2555 in Bezug auf in die seinen Anwendungsbereich fallenden Einrichtungen der öffentlichen Verwaltung auf Landesebene gewährleisten soll, ist von einer geringen Zahl betroffener bayerischer Behörden auszugehen. Diese Behörden haben gegenüber dem bisher praktizierten Informationssicherheitsmanagement voraussichtlich geringfügig erweiterte Risikomanagementmaßnahmen zu beachten, wenngleich der konkrete Umfang derzeit nicht absehbar ist. Zudem entstehen punktuelle Aufwände für das erweiterte, aufgrund von Art. 23 der Richtlinie (EU) 2022/2555 vorzusehende, Meldeverfahren an das LSI. Für die Schulung der Leitungsebene der staatlichen Behörden entstehen diesen keine Kosten, da entsprechende Angebote des LSI vorgesehen sind.

Die aufgrund der Umsetzung der Richtlinie (EU) 2022/2555 erforderlich werdenden neuen Aufgaben des LSI als Aufsichtsbehörde und CSIRT haben hohen Überschneidungsgrad mit bisherigen Tätigkeiten des LSI und wachsenden Anforderungen an die Behörde. Gleiches gilt für die Bereitstellung von Schulungsangeboten. Bisherige Maßnahmen, wie die Erhöhung der zeitlichen Reaktionsfähigkeit und ein Ausbau operativer Kapazitäten im Lagezentrum, werden aufgrund der europarechtlichen Vorgaben der Richtlinie (EU) 2022/2555 nunmehr rechtsverbindlich.

Den von der Richtlinienumsetzung nicht betroffenen Kommunen entstehen keine Kosten.

2. Bürger und Wirtschaft

Bürger und Wirtschaft sind durch dieses Gesetz nicht unmittelbar betroffen. Es entstehen für sie keine Be- und Entlastungen.

Entwurf

Gesetz zur Änderung des Bayerischen Digitalgesetzes[1]

vom [*Ausfertigungsdatum*]

§ 1

Das Bayerische Digitalgesetz (BayDiG) vom 22. Juli 2022 (GVBl. S. 374, BayRS 206-1-D), das durch Art. 57b des Gesetzes vom 22. Juli 2022 (GVBl. S. 374) geändert worden ist, wird wie folgt geändert:

1. Dem Art. 41 wird folgender Satz 3 angefügt:

   „[3]Das Landesamt ist zuständige Behörde im Sinne des Art. 8 der Richtlinie (EU) 2022/2555."

2. Art. 42 wird wie folgt geändert:

   a) Abs. 1 wird wie folgt geändert:

      aa) In Nr. 5 werden nach dem Wort „Informationstechnik" die Wörter „ , die Erkennung von Sicherheitsrisiken und die Bewertung von Sicherheitsvorkehrungen" eingefügt.

      bb) In Nr. 6 wird der Punkt am Ende durch ein Komma ersetzt.

      cc) Die folgenden Nrn. 7 bis 10 werden angefügt:

         „7. als Computer-Notfallteam (CSIRT) im Sinne von Art. 10 der Richtlinie (EU) 2022/2555 die Aufgaben nach Art. 11 Abs. 3 der Richtlinie (EU) 2022/2555 wahrzunehmen,

---

[1] Dieses Gesetz dient der Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27. 12. 2022, S. 80).

8. an Peer Reviews nach Art. 19 der Richtlinie (EU) 2022/2555 mitzuwirken,

9. der Leitungsebene und den Beschäftigten von Behörden Schulungen im Bereich Cybersicherheit anzubieten,

10. Meldungen nach Art. 43 Abs. 3 Satz 3 und Art. 49b Abs. 5 sowie Informationen nach Art. 49a Abs. 3 an die nationale zentrale Anlaufstelle im Sinne des Art. 8 Abs. 3 der Richtlinie (EU) 2022/2555 zu übermitteln."

b) Folgender Abs. 5 wird angefügt:

„(5) Das Landesamt arbeitet mit dem Bundesamt für Sicherheit in der Informationstechnik, den für IT-Sicherheit in den Ländern und in den Mitgliedsstaaten zuständigen Stellen, der Agentur der Europäischen Union für Cybersicherheit und den gemäß der Verordnung (EU) 2022/2554 und der Richtlinie (EU) 2022/2557 jeweils zuständigen Behörden zusammen."

3. Art. 43 wird wie folgt geändert:

a) In Abs. 1 Satz 2 wird nach dem Wort „technische" das Wort „ , operative" eingefügt und die Wörter „im Sinn von Art. 32 DSGVO und Art. 32 des Bayerischen Datenschutzgesetzes" werden gestrichen.

b) Nach Abs. 1 wird folgender Abs. 2 eingefügt:

„(2) Die obersten Dienstbehörden stellen in ihrem Geschäftsbereich sicher, dass die Leitungsebene staatlicher Behörden über ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie zu Risikomanagementpraktiken im Bereich Cybersicherheit verfügt."

c) Der bisherige Abs. 2 wird Abs. 3 und wird wie folgt geändert:

aa) Der Wortlaut wird Satz 1.

bb) Die folgenden Sätze 2 bis 4 werden angefügt:

„[2]Andere Stellen können erhebliche Sicherheitsvorfälle im Sinne des Art. 49b Abs. 2 Satz 2, Cyberbedrohungen im Sinne des Art. 2 Nr. 8 der Verordnung (EU) 2019/881 und Beinahe-Vorfälle im Sinne des

Art. 6 Nr. 5 der Richtlinie (EU) 2022/2555 an das Landesamt melden. [3]Soweit erforderlich übermittelt das Landesamt der nationalen zentralen Anlaufstelle im Sinne des Art. 8 Abs. 3 der Richtlinie (EU) 2022/2555 die Informationen über die gemäß diesem Absatz eingegangenen Meldungen, wobei es die Vertraulichkeit und den angemessenen Schutz der von der meldenden Stelle übermittelten Informationen sicherstellt. [4]Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten dürfen Meldungen nach Satz 2 nicht dazu führen, dass der meldenden Stelle zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte."

d) Die bisherigen Abs. 3 und 4 werden die Abs. 4 und 5.

4. In Art. 48 Abs. 2 Satz 1 Satzteil vor Nr. 1 wird das Wort „zwölf" durch die Angabe „18" ersetzt.

5. Nach Art. 49 wird folgendes Kapitel 4 eingefügt:

„Kapitel 4

Besondere Vorschriften für Einrichtungen mit Bedeutung für den Binnenmarkt

Art. 49a

Einrichtung mit Bedeutung für den Binnenmarkt

(1) [1]In Bezug auf Einrichtungen mit Bedeutung für den Binnenmarkt gelten ergänzend zu den Art. 41 bis 49 die Bestimmungen dieses Kapitels. [2]Die Art. 41 bis 49 bleiben unberührt.

(2) [1]Einrichtungen mit Bedeutung für den Binnenmarkt sind staatliche Behörden, die nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte. [2]Satz 1 gilt nicht für den Landtag, den Landesbeauftragten für den Datenschutz, den Obersten Rechnungshof, die Justiz sowie Behörden, die ausschließlich in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermitt-

lung, Aufdeckung und Verfolgung von Straftaten, tätig werden. [3]Werden Behörden nur teilweise in den Bereichen des Satzes 2 tätig, finden die Vorschriften dieses Kapitels insoweit keine Anwendung.

(3) [1]Das Landesamt ermittelt unter Einbindung der obersten Dienstbehörden erstmalig bis zum 17. April 2025 alle Einrichtungen mit Bedeutung für den Binnenmarkt. [2]Dabei sind die in Art. 27 Abs. 2 der Richtlinie (EU) 2022/2555 genannten Informationen zu erfassen. [3]Einrichtungen mit Bedeutung für den Binnenmarkt teilen Änderungen der erfassten Informationen unverzüglich dem Landesamt mit. [4]Das Landesamt überprüft die erfassten Informationen regelmäßig, spätestens jedoch alle zwei Jahre. [5]Die ermittelten Einrichtungen mit Bedeutung für den Binnenmarkt und die erfassten Informationen übermittelt das Landesamt der nationalen zentralen Anlaufstelle im Sinne des Art. 8 Abs. 3 der Richtlinie (EU) 2022/2555 erstmals zum 17. April 2025 und danach alle zwei Jahre, im Fall von Änderungen unverzüglich.

(4) [1]Für Einrichtungen mit Bedeutung für den Binnenmarkt gelten als Mindestsicherheitsniveau die durch und aufgrund von Art. 21 der Richtlinie (EU) 2022/2555 festgelegten Standards. [2]Art. 45 Abs. 1 findet in Bezug auf die Anforderungen nach Satz 1 entsprechend Anwendung.

(5) Die in diesem Kapitel festgelegten Verpflichtungen umfassen nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde.

Art. 49b

Besonderes Meldeverfahren

(1) Einrichtungen mit Bedeutung für den Binnenmarkt übermitteln dem Landesamt über eine eingerichtete Meldemöglichkeit

1. unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Frühwarnung, in der

angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte,

2. unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntniserlangung des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall, in der die in Nr. 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden,

3. auf Ersuchen des Landesamtes einen Zwischenbericht über relevante Statusaktualisierungen und

4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nr. 2, vorbehaltlich des Abs. 3, einen Abschlussbericht, der Folgendes enthält:

   a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen,

   b) Angaben zur Art der Bedrohung sowie zur zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat,

   c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen und

   d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

(2) [1]Ein Sicherheitsvorfall liegt vor, wenn ein Ereignis die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder die Dienste, die über informationstechnische Systeme, Komponenten oder Prozesse angeboten werden oder zugänglich sind, beeinträchtigt. [2]Ein Sicherheitsvorfall gilt als erheblich, wenn dieser

1. schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann,

2. andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann oder

3. in einem Durchführungsrechtsakt der Europäischen Kommission gemäß Art. 23 Abs. 11 Unterabs. 2 der Richtlinie (EU) 2022/2555 als erheblich bezeichnet ist.

(3) Dauert der Sicherheitsvorfall im Zeitpunkt des Abs. 1 Nr. 4 noch an, legt die betreffende Einrichtung statt eines Abschlussberichtes zu diesem Zeitpunkt einen Fortschrittsbericht und binnen eines Monats nach Abschluss der Bearbeitung des Sicherheitsvorfalls einen Abschlussbericht vor.

(4) [1]Soweit die Europäische Kommission einen Durchführungsrechtsakt gemäß Art. 23 Abs. 11 Unterabs. 1 der Richtlinie (EU) 2022/2555 erlässt, in dem die Art der Angaben, das Format oder das Verfahren der Meldungen festgelegt ist, sind diese Vorgaben einzuhalten. [2]Das Landesamt kann die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte im Einvernehmen mit dem Staatsministerium der Finanzen und für Heimat festlegen, soweit dies Durchführungsrechtsakten der Europäischen Kommission nicht widerspricht.

(5) Das Landesamt unterrichtet die nationale zentrale Anlaufstelle im Sinne des Art. 8 Abs. 3 der Richtlinie (EU) 2022/2555 unverzüglich über eingegangene Meldungen nach diesem Artikel.

(6) [1]Das Landesamt übermittelt der meldenden Einrichtung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Eingang der Frühwarnung eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operative Beratung für die Durchführung möglicher Abhilfemaßnahmen. [2]Das Landesamt leistet auf Ersuchen der meldenden Einrichtung zusätzliche technische Unterstützung. [3]Wird bei dem erheblichen Sicherheitsvorfall ein krimineller Hintergrund vermutet, gibt das Landesamt ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden. [4]Das Landesamt bear-

beitet auch sonstige Meldungen gemäß Art. 43 Abs. 3 Satz 2 nach dem in diesem Absatz vorgesehenen Verfahren und kann der meldenden Stelle auf Ersuchen entsprechende Unterstützung leisten.

(7) [1]Einrichtungen mit Bedeutung für den Binnenmarkt können darüber hinaus auf freiwilliger Basis Sicherheitsvorfälle im Sinne des Abs. 2 Satz 1, Cyberbedrohungen im Sinne des Art. 2 Nr. 8 der Verordnung (EU) 2019/881 und Beinahe-Vorfälle im Sinne des Art. 6 Nr. 5 der Richtlinie (EU) 2022/2555 an das Landesamt melden. [2]Abs. 6 Satz 4 und Art. 43 Abs. 3 Satz 3 und 4 gelten entsprechend.

Art. 49c

Aufsicht und Durchsetzung

(1) [1]Das Landesamt überwacht bei Einrichtungen mit Bedeutung für den Binnenmarkt die Einhaltung der Verpflichtungen nach Art. 43 Abs. 1, Art. 46, 49a Abs. 3 Satz 3, Abs. 4 und Art. 49b nach Maßgabe des Art. 33 der Richtlinie (EU) 2022/2555. [2]Rechtfertigen Tatsachen die Annahme, dass eine Einrichtung mit Bedeutung für den Binnenmarkt einer Verpflichtung nach Satz 1 nicht nachkommt, so kann das Landesamt, soweit dies zur Erfüllung seiner Aufgabe nach Satz 1 erforderlich ist, im Einvernehmen mit der zuständigen obersten Dienstbehörde

1. bei der betreffenden Einrichtung Vor-Ort-Kontrollen, externe nachträgliche Aufsichtsmaßnahmen, gezielte Sicherheitsprüfungen oder Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls auch in Zusammenarbeit mit der betreffenden Einrichtung, durchführen oder unabhängige Stellen mit der Durchführung einer gezielten Sicherheitsüberprüfung beauftragen,

2. von der betreffenden Einrichtung Informationen zur nachträglichen Bewertung der ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit, einschließlich dokumentierter Cybersicherheitskonzepte oder zur Einhaltung der Verpflichtungen nach Art. 49a Abs. 3 Satz 3 anfordern,

3. bei der betreffenden Einrichtung den Zugang zu Daten, Dokumenten oder sonstigen Informationen anfordern oder

4. von der betreffenden Einrichtung Nachweise für die Umsetzung der Cybersicherheitskonzepte anfordern.

[3]Das Landesamt kann, soweit dies zur Behebung festgestellter Verstöße einer Einrichtung mit Bedeutung für den Binnenmarkt gegen Verpflichtungen nach Satz 1 erforderlich ist, im Einvernehmen mit der zuständigen obersten Dienstbehörde

1. die betreffende Einrichtung anweisen oder ihr gegenüber anordnen, die festgestellten Mängel oder Verstöße gegen die Verpflichtungen nach Satz 1 zu beheben,

2. die betreffende Einrichtung anweisen, das gegen die Verpflichtungen nach Satz 1 verstoßende Verhalten einzustellen und von Wiederholungen abzusehen,

3. die betreffende Einrichtung anweisen, entsprechend bestimmter Vorgaben und innerhalb einer bestimmten Frist die Erfüllung der Verpflichtungen nach Satz 1 sicherzustellen oder

4. die betreffende Einrichtung anweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen.

[4]Anweisungen nach Satz 3 sind zu begründen. [5]Der anzuweisenden Einrichtung mit Bedeutung für den Binnenmarkt ist vorab mit angemessener Frist Gelegenheit zur Stellungnahme zu geben, es sei denn, dies würde die Wirksamkeit von sofortigen Maßnahmen zur Verhütung von Sicherheitsvorfällen oder zur Reaktion auf Sicherheitsvorfälle beeinträchtigen.

(2) Stellt das Landesamt fest, dass der Verstoß einer Einrichtung mit Bedeutung für den Binnenmarkt gegen Verpflichtungen aus Art. 43 Abs. 1, Art. 46, 49a Abs. 4 oder Art. 49b eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO zur Folge haben kann, die gemäß Art. 33 DSGVO zu melden ist, unterrichtet es im Einvernehmen mit der zuständigen

obersten Dienstbehörde unverzüglich den Landesbeauftragten für den Datenschutz.

(3) [1]Das Landesamt kann, soweit erforderlich, im Einvernehmen mit der zuständigen obersten Dienstbehörde die Öffentlichkeit oder von einem Sicherheitsvorfall betroffene Dritte über erhebliche Sicherheitsvorfälle bei Einrichtungen mit Bedeutung für den Binnenmarkt sowie mögliche Abwehr- oder Abhilfemaßnahmen informieren oder Einrichtungen mit Bedeutung für den Binnenmarkt anweisen, dies zu tun. [2]Zudem kann es diese im Einvernehmen mit der zuständigen obersten Dienstbehörde anweisen, Informationen zu Verstößen gegen die Verpflichtungen nach Abs. 1 Satz 1 nach bestimmten Vorgaben öffentlich bekannt zu machen oder selbst Warnungen über Verstöße gegen diese Verpflichtungen durch Einrichtungen mit Bedeutung für den Binnenmarkt herausgeben, soweit dies erforderlich ist.“

6. Art. 57b wird Art. 57a.

7. Art. 58 wird wie folgt gefasst:

„Art. 58

Einschränkung von Grundrechten

Die Art. 44, 48, 49 und 49c schränken das Fernmeldegeheimnis (Art. 10 des Grundgesetzes, Art. 112 der Verfassung) ein.“

8. Art. 59 wird wie folgt geändert:

a) Abs. 1 wird wie folgt geändert:

aa) In Satz 1 wird die Satznummerierung „[1]“ gestrichen.

bb) Satz 2 wird aufgehoben.

b) Abs. 2 wird aufgehoben.

c) Der bisherige Abs. 3 wird Abs. 2 und die Angabe „57b“ wird durch die Angabe „57a“ ersetzt.

d) Abs. 4 wird aufgehoben.

§ 2

Dieses Gesetz tritt am ***…[einzusetzen: Datum des Inkrafttretens – aber vor dem 1. Januar 2025]*** in Kraft.

Begründung:

A) Allgemein

Die am 16. Januar 2023 in Kraft getretene Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27. Dezember 2022, S. 80 (sogenannte NIS-2-Richtlinie) ist von den Mitgliedstaaten bis 17. Oktober 2024 in nationales Recht umzusetzen. Sie löst die bisherige Richtlinie (EU) 2016/1148 (sogenannte NIS-Richtlinie) ab und erweitert das bestehende Regelwerk, um das Cybersicherheitsniveau in der gesamten EU zu steigern und somit eine höhere Resilienz gegen Cyberangriffe im europäischen Binnenmarkt zu schaffen.

Die Richtlinie zielt auf einen weiten Anwendungsbereich, um das Ziel eines hohen gemeinsamen Cybersicherheitsniveaus für den Binnenmarkt zu erreichen (vgl. Art. 1 Abs. 1 der Richtlinie (EU) 2022/2555). Sie gilt daher im Grundsatz nach ihrem Art. 2 Abs. 1 gesamtheitlich für öffentliche und private Einrichtungen, sodass schon an dieser Stelle eine Unterscheidung zwischen dem öffentlichen und dem privaten Sektor aus Sicht der Richtlinie grundsätzlich obsolet ist. Entscheidend sind andere Kriterien. Zum einen die Zuordnung zu einem Sektor, der in Anhang I und II der Richtlinie genannten Art, der die Kritikalität zum maßgeblichen Faktor erklärt. Zum anderen die Unternehmensgröße. Gleichwohl werden in Art. 2 Abs. 2 „Einrichtungen“ aufgezählt, die unabhängig von der Größe wiederum in den Anwendungsbereich der Richtlinie eingeschlossen werden sollen. Dazu gehören gem. Art. 2 Abs. 2 Buchst. f der Richtlinie (EU) 2022/2555 auch „Einrichtungen der öffentlichen Verwaltung“, sowohl auf Ebene der Zentralregierung (Ziffer i), als auch solche auf regionaler Ebene, soweit sie nach einer risikobasierten Bewertung kritische Dienste erbringen (Ziffer ii). Der Sektor „öffentliche Verwaltung“ ist in diesem Zusammenhang nach Anhang I Nr. 10 der Richtlinie (EU) 2022/2555 ein solcher von hoher Kritikalität.

Die Richtlinie (EU) 2022/2555 verpflichtet die von ihrem Anwendungsbereich erfassten Einrichtungen angemessene Sicherheitsmaßnahmen zu implementieren und Sicherheitsvorfälle zu melden. Die Richtlinie sieht auch die Einrichtung von Computer Security Incident Response Teams (CSIRTs) vor. Die Mitgliedstaaten sollen zudem

nationale Cybersicherheitsbehörden (eine oder mehrere zuständige Behörden und eine nationale zentrale Anlaufstelle) benennen oder errichten und eine nationale Cybersicherheitsstrategie erstellen. Im Grundsatz zielt die Richtlinie (EU) 2022/2555 darauf ab, die Zusammenarbeit zwischen den Mitgliedstaaten in Bezug auf Cybersicherheit zu verbessern und das Schutzniveau für digitale Dienste und kritischen Infrastrukturen zu verbessern.

Die Maßnahmen aus der Richtlinie (EU) 2022/2555 bewahren Einrichtungen nicht vollumfänglich vor Cyberangriffen, sie sollen jedoch dafür sorgen, dass eine Vielzahl von Angriffen durch geschützte Netz- und Informationssicherheitssysteme auf ein Minimum reduziert werden kann.

Die Richtlinie (EU) 2022/2555 ist im Hinblick auf die überwiegend dem Anwendungsbereich unterfallenden wirtschaftlich tätigen Einrichtungen grundsätzlich vom Bund umzusetzen (Recht der Wirtschaft, konkurrierende Gesetzgebungskompetenz des Bundes gem. Art. 74 Abs. 1 Nr. 11 des Grundgesetzes). Soweit jedoch auch Landesbehörden von der Richtlinie als sogenannte Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene erfasst sind, ist eine landesrechtliche Umsetzung erforderlich.

Die Ziele der Richtlinie (EU) 2022/2555 stehen grundsätzlich mit den bisherigen Regelungen zur Informationssicherheit von Behörden im derzeitigen Teil 3 BayDiG (IT-Sicherheit) in Einklang. Gleichwohl sind Anpassungen am Bayerischen Digitalgesetz erforderlich, u.a. weil die bestehenden landesrechtlichen Regelungen zwar die Voraussetzung für eine wirksame Abwehr von Gefahren für die Informationstechnik staatlicher und sonstiger an das Behördennetz angeschlossenen Stellen schaffen und das Landesamt für Sicherheit in der Informationstechnik (LSI) mit entsprechenden Aufgaben und Befugnissen ausstatten, bisher jedoch nicht die primär auf Unternehmen zugeschnittenen Meldewege und Aufsichtsmaßnahmen sowie weitere Standards abbilden, welche die Richtlinie (EU) 2022/2555 vorsieht. Die Vorgaben der Richtlinie (EU) 2022/2555 werden insbesondere in einem separaten Kapitel 4 in Teil 3 (Art. 49a bis 49c) des Bayerischen Digitalgesetzes umgesetzt. Soweit die Richtlinie (EU) 2022/2555 die Option eröffnet ihren Anwendungsbereich auch auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken wird hiervon gemäß Beschluss des IT-Planungsrats vom 3. November 2023 (Beschluss 2023/39) kein Gebrauch gemacht.

Unabhängig von der Umsetzung der Richtlinie (EU) 2022/2555 muss die Sicherheit der Informationstechnik staatlicher und sonstiger an das Behördennetz angeschlossener Stellen im Fokus des Teil 3 des BayDiG bleiben.

B) Zwingende Notwendigkeit einer normativen Regelung

Die Umsetzung der Richtlinie (EU) 2022/2555 erfordert auf Landesebene eine gesetzliche Regelung. Bei Nichtumsetzung besteht ein erhebliches Risiko eines Vertragsverletzungsverfahrens, an dessen Ende finanzielle Sanktionen stehen können. Diese Sanktionen werden ggf. nach dem Verursacherprinzip vom Bund an die Länder weitergereicht (siehe hierzu auch Gesetz zur Lastentragung im Bund-Länder-Verhältnis bei Verletzung von supranationalen oder völkerrechtlichen Verpflichtungen).

C) Einzelbegründung

Zu § 1 Nr. 1 (Art. 41 Satz 3 BayDiG)

Die Norm dient der Umsetzung von Art. 8 der Richtlinie (EU) 2022/2555. Danach benennen die Mitgliedstaaten eine oder mehrere zuständige Behörden oder richten diese ein. Diese Behörden überwachen die Anwendung der Richtlinie (EU) 2022/2555 auf nationaler Ebene. Satz 3 legt fest, dass das LSI eine zuständige Behörde im Sinne der Richtlinie (EU) 2022/2555 ist. Die örtliche und sachliche Zuständigkeit des LSI als zuständige Stelle ergibt sich aus den weiteren mit diesem Gesetz verbundenen Änderungen, insbesondere durch die in den Art. 49a bis 49c BayDiG geregelten Aufgaben und Befugnissen.

Zu § 1 Nr. 2 Buchst. a Doppelbuchst. aa (Art. 42 Abs. 1 Nr. 5 BayDiG)

Die Norm dient der Umsetzung von Art. 8 Abs. 2 in Verbindung mit Art. 31 Abs. 1 und Art. 33 der Richtlinie (EU) 2022/2555 und ergänzt die Aufgaben des LSI um die in der Richtlinie (EU) 2022/2555 für zuständige Behörden vorgesehenen Aufgaben.

Zu § 1 Nr. 2 Buchst. a Doppelbuchst. bb (Art. 42 Abs. 1 Nr. 6 BayDiG)

Redaktionelle Änderung aufgrund des erweiterten Aufgabenbereichs des LSI.

Zu § 1 Nr. 2 Buchst. a Doppelbuchst. cc (Art. 42 Abs. 1 Nr. 7 bis 10 BayDiG)

Gemäß Art. 10 der Richtlinie (EU) 2022/2555 benennen oder richten die Mitgliedstaaten sogenannte CSIRTs ein. Das CSIRT ist gemäß der Richtlinie u.a. Meldestelle und für die Unterstützung der regulierten Einrichtungen zuständig. Diese können auch innerhalb einer zuständigen Behörde benannt oder eingerichtet werden. Die im Wesentlichen in Art. 11 der Richtlinie (EU) 2022/2555 beschriebenen Aufgaben eines CSIRT nimmt das LSI bereits im Rahmen seiner Aufgaben zur Abwehr von Gefahren für die Sicherheit der Informationstechnik wahr (sog. Bayern-CERT). Daher soll dem LSI mit Art. 42 Abs. 1 Nr. 7 BayDiG auch die entsprechende Funktion im Rahmen der Richtlinienumsetzung übertragen werden.

Art. 42 Abs. 1 Nr. 8 BayDiG dient der Umsetzung von Art. 10 Abs. 5 der Richtlinie (EU) 2022/2555, nach dem die CSIRTs an gemäß Art. 19 der Richtlinie (EU) 2022/2555 organisierten Peer Reviews teilnehmen.

Nachdem die Sensibilisierung der Mitarbeiter und Leitungsorgane von staatlichen (und kommunalen) Behörden eine wichtige Maßnahme zur Prävention von IT-Sicherheitsvorfällen ist, bietet das LSI bereits entsprechende zentrale Angebote für die Beschäftigten staatlicher Behörden (z.B. auf der Plattform BayLern) oder Informationsangebote für Kommunen an. Daher und zur Entlastung der Dienststellen wird das Angebot entsprechender Schulungen als zentrale Aufgabe des LSI in Art. 42 Abs. 1 Nr. 9 BayDiG normiert. Solche Schulungen zentral anzubieten, dient der Reduzierung des Vollzugsaufwandes und der Gewährleistung eines einheitlichen, hohen Informationsstandes. Das gesetzlich normierte Schulungsangebot des LSI schafft die Voraussetzung, dass die obersten Dienstbehörden ihrer Verpflichtung nachkommen können, sicherzustellen, dass die Leitungsebene staatlicher Behörden über ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie zu Risikomanagementpraktiken im Bereich Cybersicherheit verfügt. Auf die Ausführungen zu § 1 Nr. 3 Buchst. b wird verwiesen.

Die Richtlinie (EU) 2022/2555 legt ferner fest, dass die zuständigen Behörden bestimmte Meldungen und Informationen an eine nationale zentrale Anlaufstelle übermitteln, die jeder Mitgliedsstaat gemäß Art. 8 Abs. 3 der Richtlinie (EU) 2022/2555 einzurichten oder zu benennen hat. Die entsprechende Aufgabe wird dem LSI über Art. 42 Abs. 1 Nr. 10 BayDiG zugewiesen. Da noch kein Bundesgesetz zur Umsetzung der Richtlinie (EU) 2022/2555 vorliegt und bislang keine nationale zentrale Anlaufstelle benannt oder eingerichtet ist, muss die landesrechtliche Umsetzung insoweit abstrakt bleiben. Aufgrund der bestehenden Aufgabenzuweisungen ist damit zu rechnen, dass der Bundesgesetzgeber das Bundesamt für Sicherheit in der Informationstechnik zur nationalen zentralen Anlaufstelle bestimmt.

Zu § 1 Nr. 2 Buchst. b (Art. 42 Abs. 5 BayDiG)

Die Anfügung dient der Umsetzung des Kooperationsauftrags, dem die CSIRTs z.B. gemäß Art. 10 Abs. 6 ff. der Richtlinie (EU) 2022/2555 unterliegen. Dies schließt die Teilnahme am europäischen CSIRT-Netzwerk (Art. 15 der Richtlinie (EU) 2022/2555) ein. Außerdem muss das LSI gemäß Art. 32 Abs. 9 und 10 der Richtlinie (EU) 2022/2555 mit den zuständigen Behörden gemäß der Richtlinie (EU) 2022/2557 (sog. CER-Richtlinie) und gemäß der Verordnung (EU) 2022/2554 (sog. DORA-Ver-

ordnung) zusammenarbeiten. Dies umfasst ggf. auch die Entgegennahme von Meldungen im Sinne des Art. 19 Abs. 6 der Verordnung (EU) 2022/2554 von hierfür zuständigen Landesaufsichtsbehörden.

Zu § 1 Nr. 3 Buchst. a (Art. 43 Abs. 1 Satz 2 BayDiG)

Nach Art. 21 Abs. 1 der Richtlinie (EU) 2022/2555 ist sicherzustellen, dass die Einrichtungen im Anwendungsbereich der Richtlinie geeignete und verhältnismäßige, d.h. dem jeweiligen Einzelfall angemessene technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten. Diese allgemeine Vorgabe zur IT-Sicherheit besteht bereits nach Art. 43 Abs. 1 BayDiG. Die vollständige Umsetzung der europarechtlichen Vorgaben wird durch eine sprachliche Angleichung der bestehenden Regelung bzw. Streichung des rechtshistorisch begründeten Verweises auf das Datenschutzrecht in Art. 43 Abs. 1 Satz 2 BayDiG hergestellt.

Daraus ergibt sich keine Veränderung des bisherigen Regelungsgehalts. Insbesondere sind Art. 32 DSGVO und Art. 32 des Bayerischen Datenschutzgesetzes auch unabhängig von Art. 43 Abs. 1 Satz 2 BayDiG zu befolgen.

Die zusätzliche Erwähnung von operativen Maßnahmen, um die Sicherheit der informationstechnischen Systeme im Rahmen der Verhältnismäßigkeit sicherzustellen, trägt dem Wortlaut der Richtlinie (EU) 2022/2555 Rechnung und dient der Klarstellung, dass auch eine angemessene Reaktion auf Angriffe hinreichend sicherzustellen ist, sofern nicht bereits die technischen und organisatorischen Maßnahmen entsprechend ineinandergreifen.

Zu § 1 Nr. 3 Buchst. b (Art. 43 Abs. 2 BayDiG)

Der neue Absatz 2 trägt für den Bereich des Freistaates Bayern den in Art. 20 und 21 der Richtlinie (EU) 2022/2555 geregelten Verpflichtungen der Mitgliedstaaten unter Wahrung des verfassungsrechtlich gewährleisteten Ressortprinzips Rechnung, indem er die obersten Dienstbehörden verpflichtet, sicherzustellen, dass die Leitungsebene staatlicher Behörden über ausreichende Kenntnisse und Fähigkeiten zur Erkennung

und Bewertung von Risiken sowie zu Risikomanagementpraktiken im Bereich Cybersicherheit verfügt. Das kann insbesondere über entsprechende Schulungen erfolgen (siehe oben zu § 1 Nr. 2 Buchst. a Doppelbuchst. cc). Die in Art. 20 Abs. 1 der Richtlinie (EU) 2022/2555 ebenfalls vorgesehene Verpflichtung für Leitungsorgane, die ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und deren Umsetzung zu überwachen, folgt für den Bereich des Freistaates Bayern bereits aus der allgemeinen Leitungsverantwortung der Leitungsebene der staatlichen Behörden – wie sie dem Art. 43 Abs. 1 BayDiG bereits zu Grunde liegt – und muss damit im Rahmen der landesrechtlichen Umsetzung der europarechtlichen Vorgaben nicht gesondert normiert werden.

Zu § 1 Nr. 3 Buchst. c Doppelbuchst. aa (Art. 43 Abs. 3 BayDiG)

Redaktionelle Folgeänderung aufgrund der Einfügung des Art. 43 Abs. 2 BayDiG. Der bisherige Wortlaut wird zu Abs. 3 Satz 1.

Zu § 1 Nr. 3 Buchst. c Doppelbuchst. bb (Art. 43 Abs. 3 BayDiG)

Die Vorschrift dient der Umsetzung von Art. 30 der Richtlinie (EU) 2022/2555. Nach diesem ist sicherzustellen, dass zusätzlich zu den Berichtspflichten nach Art. 23 der Richtlinie (EU) 2022/2555 den CSIRTs oder gegebenenfalls den zuständigen Behörden auch Meldungen auf freiwilliger Basis übermittelt werden können. Eine freiwillige Meldung muss aufgrund der europarechtlichen Vorgaben ohne nachteilige Folgen für die meldende natürliche oder juristische Person sein (vgl. Erwägungsgrund 62 der Richtlinie (EU) 2022/2555). Das LSI darf daher nicht veranlassen, dass der meldenden Stelle zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte. Diese Regelung schränkt die Befugnisse bzw. die Aufsichtstätigkeit anderer Behörden, insbesondere des unabhängigen Landesbeauftragten für den Datenschutz, nicht ein.

Zu § 1 Nr. 3 Buchst. c Doppelbuchst. cc (Art. 43 Abs. 4 und 5 BayDiG)

Redaktionelle Folgeanpassung aufgrund der Einfügung des Art. 43 Abs. 2 BayDiG.

Zu § 1 Nr. 4 (Art. 48 Abs. 2 Satz 1 BayDiG)

Die Möglichkeit zur Speicherung von Protokolldaten wird von 12 auf maximal 18 Monate erhöht. Mit der Erhöhung erfolgt eine Angleichung an die Rechtslage auf Bundesebene. Das BSI kann auf der Grundlage von § 5 Abs. 2 Satz 1 des BSI-Gesetzes Protokolldaten bis zu 18 Monate speichern. Im Zuge der Umsetzung der Richtlinie (EU) 2022/2555 wird sich die Zusammenarbeit zwischen BSI und LSI weiter verstärken. Um hier auf Augenhöhe agieren zu können, besteht bereits aus diesem Grund die fachliche Notwendigkeit einer Erhöhung der Speicherfrist. Aber auch die Entwicklung der Bedrohungslage macht die Notwendigkeit deutlich: Wie Cyber-Vorfälle gerade in der jüngeren Vergangenheit zeigen, geht besondere Gefahr von hochspezialisierten Cyberangriffen aus (sogenannte Advanced Persistent Threats – APTs), Kennzeichnend ist, dass Angreifer vorsichtig und verdeckt vorgehen, sodass zwischen der initialen Infektion der Kommunikationstechnik des Landes und der Aufdeckung des Angriffs in der Regel große Zeiträume liegen. Um solche Kompromittierungen erkennen und entfernen zu können, muss die Speicherdauer der Protokolldaten den Beginn des APT-Angriffs einschließen. Eine Speicherdauer von 18 Monaten verbessert die Möglichkeit der Reaktion auf Angriffe wesentlich und gewährleistet zugleich einen angemessenen Schutz von personenbezogenen Daten.

Das Prüfen der Protokolldaten ist geeignet, Angriffe zu erkennen und abzuwehren. Es ist auch aus datenschutzrechtlicher Sicht das mildeste, weil zugleich einzige Mittel, um gefährlichen Datenverkehr von außen an einem Eindringen in die Systeme zu hindern.

Zu § 1 Nr. 5 (Kapitel 4; Art. 49a bis 49c BayDiG)

Zu Art. 49a BayDiG:

Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene fallen aufgrund von Art. 2 Abs. 2 Buchst. f Ziffer ii der Richtlinie (EU) 2022/2555 in den Anwendungsbereich der Richtlinie (EU) 2022/2555, wenn sie nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte.

Im neuen Kapitel 4 von Teil 3 des BayDiG (Art. 49a ff. BayDiG) werden spezielle Regelungen für bayerische Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene zur Umsetzung der europarechtlichen Vorgaben geschaffen. Die Vorschriften der Art. 41 bis 49 BayDiG, die der weiterhin zu gewährleistenden Gefahrenabwehr für

das Behördennetz dienen, müssen davon unberührt bleiben und gelten neben den Vorschriften des neuen Kapitels 4 (vgl. Art. 49a Abs. 1 Satz 2 BayDiG).

Zur Umsetzung der Richtlinie wird in Art. 49a Absatz 2 Satz 1 BayDiG mit dem Begriff „Einrichtungen mit Bedeutung für den Binnenmarkt“ (EBB) ein eigenständiger Anwendungsbereich des neuen Kapitels 4 geschaffen. Die Begriffsdefinition orientiert sich am Begriff der Einrichtung der öffentlichen Verwaltung im Sinne des Art. 6 Nr. 35 Buchst. d der Richtlinie (EU) 2022/2555.

Die von der Richtlinie (EU) 2022/2555 abweichende Terminologie (dort: wesentliche und wichtige Einrichtungen) wurde gewählt, da die Richtlinie (EU) 2022/2555 im staatlichen Bereich nur Stellen mit spezifischen Funktionen erfasst und nicht alle Bereiche der Staatsverwaltung. Die Anwendung nur auf staatliche Behörden ergibt sich aus dem Wortlaut der Richtlinie, die in Art. 2 Abs. 2 Buchst. f Ziffer ii der Richtlinie (EU) 2022/2555 ausdrücklich Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene adressiert. Insoweit ist abzugrenzen von den Einrichtungen der Zentralregierung im Sinne des Art. 2 Abs. 2 Buchst. f Ziffer i der Richtlinie (EU) 2022/2555 (Bundesverwaltung) und den Einrichtungen der lokalen Ebene im Sinne des Art. 2 Abs. 5 Buchst. a der Richtlinie (EU) 2022/2555 (Kommunalverwaltung). Die Abgrenzung ist gemäß Art. 4 Abs. 2 Satz 1 des Vertrages über die Europäische Union unter Berücksichtigung des kommunalen Selbstverwaltungsrechts (Art. 11 Abs. 2 Satz der Verfassung des Freistaates Bayern sowie Art. 28 Abs. 2 des Grundgesetzes) vorzunehmen, sodass kommunale Behörden, einschließlich der Landratsämter, der lokalen Ebene zuzurechnen sind. Soweit die Richtlinie (EU) 2022/2555 die Option eröffnet, ihren Anwendungsbereich auch auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken, wird hiervon gemäß Beschluss des IT-Planungsrats vom 3. November 2023 (Beschluss 2023/33) kein Gebrauch gemacht.

Art. 49a Abs. 2 Satz 2 BayDiG bildet die Bereichsausnahmen des Art. 2 Abs. 7 der Richtlinie (EU) 2022/2555 unter Berücksichtigung der Behördendefinition in Art. 6 Nr. 35 der Richtlinie (EU) 2022/2555 ab. Daher sind insbesondere auch der Landtag (einschließlich des Landtagsamts) und die Justiz (einschließlich der Gerichtsverwaltungen) von den Vorschriften des neuen Kapitels 4 im Teil 3 des BayDiG ausgenommen. Der Oberste Rechnungshof sowie der Landesbeauftrage für den Datenschutz

sind aufgrund ihrer unabhängigen Stellung ebenfalls auszunehmen (vgl. Art. 6 Nr. 35 Buchst. c der Richtlinie (EU) 2022/2555 sowie für den Landesbeauftragten für Datenschutz zusätzlich Art. 33a Abs. 3 Verfassung des Freistaates Bayern). Ferner unterfallen Behörden, wie etwa der Verfassungsschutz, die ausschließlich in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung tätig sind, nicht den Vorschriften dieses Kapitels.

Mit Art. 49a Abs. 2 Satz 3 BayDiG wird Art. 2 Abs. 8 der Richtlinie (EU) 2022/2555 umgesetzt.

Mit Art. 49a Abs. 3 BayDiG werden Art. 3 Abs. 3 und 4 der Richtlinie (EU) 2022/2555 umgesetzt. An die Stelle der dort, vornehmlich hinsichtlich der für die Aufsichtsbehörde nicht unmittelbar zugänglichen Unternehmen, vorgesehenen Registrierungspflicht tritt eine Ermittlung der EBB durch das LSI von Amts wegen. Dabei sind die jeweils zuständigen obersten Dienstbehörden einzubinden. Die Ermittlung der EBB erfolgt regelmäßig im Wege einer Abfrage betreffend der staatlichen Behörden im jeweiligen Zuständigkeitsbereich. Dieses Verfahren soll einen unbürokratischen und lückenlosen Vollzug gewährleisten, sowie Rechtsunsicherheit auf Seiten der Behörden vermeiden. Dabei findet das vom IT-Planungsrat am 3. November 2023 beschlossene Identifizierungskonzept Anwendung (Beschluss 2023/39).

Mit Art. 49a Abs. 4 BayDiG wird Art. 21 der Richtlinie (EU) 2022/2555 vollständig umgesetzt. Für die EBB gelten damit konkrete Vorgaben zu Risikomanagementmaßnahmen, die ggf. über die bisher von den Behörden praktizierten Maßnahmen zur Informationssicherheit hinausgehen, die sich am IT-Grundschutz orientieren (vgl. Beschluss 2019/04 des IT-Planungsrats). Soweit derzeit absehbar, werden mit dem IT-Grundschutz die Mindestanforderungen der Richtlinie (EU) 2022/2555 bereits weitgehend abgedeckt.

Mit Art. 49a Abs. 5 BayDiG wird schließlich Art. 2 Abs. 11 der Richtlinie (EU) 2022/2555 umgesetzt. Die Verpflichtungen des Kapitel 4 umfassen nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde. Die Vorschriften der Verschlusssachenanweisung für die Behörden des Freistaates Bayern bleiben unberührt.

Zu Art. 49b BayDiG:

Der neue Artikel dient der Umsetzung von Art. 23 der Richtlinie (EU) 2022/2555 und beschreibt ein dreistufiges Meldeverfahren, das bei erheblichen Sicherheitsvorfällen einzuhalten ist. Das von der Richtlinie vorgesehene Verfahren ist auf die Regulierung von Unternehmen zugeschnitten und soll deshalb getrennt von der bestehenden Meldepflicht nach Art. 43 Abs. 3 BayDiG normiert werden. Die bestehende Meldepflicht bleibt unberührt.

Das LSI ist unverzüglich nach Kenntnisnahme über einen in Art. 49b Abs. 2 BayDiG legaldefinierten erheblichen Sicherheitsvorfall, jedoch spätestens nach 24 Stunden (Frühwarnung) und spätestens nach 72 Stunden (Bewertung der Auswirkungen) zu kontaktieren. Einen Monat nach der Erstmeldung ist ein Abschlussbericht vorzulegen. Hinsichtlich der Ausführung dieser Vorschriften ist zu beachten, dass das LSI im Behördennetz entdeckte Sicherheitsvorfälle grundsätzlich federführend bearbeitet und zum Schutz der Informationstechnik staatlicher und sonstiger an das Behördennetz angeschlossenen Stellen eine unverzügliche und umfassende Information des LSI erforderlich ist (vgl. Art. 43 Abs. 3 BayDiG). Die Begriffsdefinitionen zum (erheblichen) Sicherheitsvorfall in Art. 49b Abs. 2 BayDiG setzen die europarechtlichen Vorgaben von Art. 23 und Art. 6 Nr. 6 der Richtlinie (EU) 2022/2555 um.

Erhebliche Sicherheitsvorfälle sind gemäß Art. 23 Abs. 9 der Richtlinie (EU) 2022/2555 von der zentralen Anlaufstelle (BSI) alle drei Monate der European Union Agency for Cybersecurity (ENISA) vorzulegen. Art. 49b Abs. 5 BayDiG regelt daher die Befugnis zur Weitergabe der beim LSI nach diesem Artikel eingegangenen Meldungen.

Mit Art. 49b Abs. 7 wird schließlich Art. 30 Abs. 1 Buchst. a der Richtline (EU) 2022/2555 umgesetzt. Einrichtungen mit Bedeutung für den Binnenmarkt können demnach auch freiwillige Meldung an das Landesamt übermitteln.

Zu Art. 49c BayDiG:

Die Norm dient der Umsetzung von Art. 33 der Richtlinie (EU) 2022/2555, der die Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wichtige Einrichtungen im Sinne

von Art. 3 Abs. 2 der Richtlinie konkretisiert. In der Richtlinie (EU) 2022/2555 findet eine Abgrenzung zwischen den Aufsichtssystemen für wesentliche und für wichtige Einrichtungen statt, um die Verpflichtungen für diese Einrichtungen und für die zuständigen Behörden ausgewogen zu gestalten. Während wesentliche Einrichtungen im Sinne der Richtlinie (EU) 2022/2555 einem umfassenden Ex-ante- und Ex-post-Aufsichtssystem unterliegen, unterliegen EBB als wichtige Einrichtungen im Sinne des Art. 3 Abs. 2 der Richtlinie (EU) 2022/2555 einem einfachen, ausschließlich nachträglichen Ex-post-Aufsichtskonzept (vgl. Erwägungsgrund 122 der Richtlinie (EU) 2022/2555). Aus diesem Grund werden in Art. 49c BayDiG allein die für wichtige Einrichtungen von Art. 33 der Richtlinie (EU) 2022/2555 vorgegebenen Aufsichts- und Durchsetzungsmaßnahmen landesrechtlich normiert. Die landesrechtliche Umsetzung erfolgt „Eins-zu-eins“ und unter Wahrung des Ressortprinzips; eine richtlinienüberschießende Umsetzung findet nicht statt.

Die in Art. 49c BayDiG normierten Befugnisse des LSI überschneiden sich mit den bestehenden Befugnissen aus Art. 44 und 45 BayDiG. Sie dienen jedoch nicht der IT-Sicherheit des Behördennetzes, sondern der Umsetzung der Vorgaben der Richtlinie (EU) 2022/2555. Daher ist es zur Rechtsklarheit angezeigt, das LSI in dem separaten Art. 49c BayDiG mit den notwendigen Befugnissen auf Grundlage der europarechtlichen Vorgaben auszustatten.

Bei EBB können Ex-post-Aufsichtsmaßnahmen nach Art. 49c Abs. 1 Satz 2 BayDiG dadurch ausgelöst werden, dass dem LSI Belege, Hinweise oder Informationen zur Kenntnis gebracht werden, die als Anzeichen für einen möglichen Verstoß gegen die in Art. 49c Abs. 1 Satz 1 BayDiG genannten Verpflichtungen der EBB gedeutet werden. Solche Belege, Hinweise oder Informationen könnten beispielsweise von anderen Behörden, Einrichtungen, Bürgern oder Medien zur Verfügung gestellt werden, aus anderen Quellen oder öffentlich zugänglichen Informationen herrühren oder sich aus anderen Tätigkeiten des LSI ergeben.

Wahl und Einsatz der Aufsichtsmaßnahmen stehen im Ermessen des LSI und haben den Grundsatz der Verhältnismäßigkeit zu wahren. Entsprechend der europarechtlichen Vorgaben stellt das LSI dabei im Rahmen seiner Ermessensentscheidung sicher, dass die Umstände des Einzelfalls hinreichend berücksichtigt werden und die gewählte

Aufsichts- bzw. Durchsetzungsmaßnahme wirksam, verhältnismäßig und abschreckend ist (vgl. Art. 33 Abs. 1 der Richtlinie (EU) 2022/2555).

Die Aufsichtsbefugnis des LSI nach Art. 49c Abs. 1 Satz 2 BayDiG umfasst dabei sämtliche der in Art. 33 Abs. 2 der Richtlinie (EU) 2022/2555 genannten Maßnahmen.

Die in Art. 49c Abs. 1 Satz 2 Nr. 1 BayDiG genannten gezielten Sicherheitsüberprüfungen stützen sich auf Risikobewertungen, die vom LSI oder der geprüften Einrichtung durchgeführt wurden oder auf sonstige verfügbare risikobezogene Informationen. Die Ergebnisse gezielter Sicherheitsüberprüfungen sind dem LSI zur Verfügung zu stellen. Das LSI kann auch unabhängige Stellen mit der Durchführung gezielter Sicherheitsüberprüfungen beauftragen.

Bei der Ausübung von Befugnissen nach Art. 49 Abs. 1 Satz 2 Nr. 2 bis 4 BayDiG gibt das LSI den Zweck seiner Anfrage und die erbetenen Informationen an.

Kommen EBB den in Art. 43 Abs. 1, Art. 46, 49a Abs. 3 Satz 3, Abs. 4 und Art. 49b BayDiG genannten Verpflichtungen nicht nach, so kann das LSI im Rahmen des insoweit eingeräumten Ermessens die den EBB obliegenden Verpflichtungen mittels Maßnahmen gemäß Art. 49c Abs. 1 Satz 3, Abs. 3 BayDiG durchsetzen, um festgestellten Verstößen der EBB gegen die in Art. 49c Abs. 1 Satz 1 BayDiG genannten Verpflichtungen zu begegnen.

Wahl und Einsatz der Durchsetzungsmaßnahmen nach Art. 49c Abs. 1 Satz 3, Abs. 3 BayDiG stehen im Ermessen des LSI und haben den Grundsatz der Verhältnismäßigkeit zu wahren. Entsprechend der europarechtlichen Vorgaben des Art. 33 Abs. 5 der Richtlinie (EU) 2022/2555 stellt das LSI dabei im Rahmen seiner Ermessensentscheidung sicher, dass die Umstände des Einzelfalls und die in Art. 32 Abs. 7 Buchst. a bis h der Richtlinie (EU) 2022/2555 genannten Aspekte hinreichend berücksichtigt werden. Der Zugang zu Anwendungsdaten fällt zur Wahrung des Datenschutzes und des Steuergeheimnisses nicht unter den Begriff "Daten". Hierunter sind z.B. Dokumentationen oder LogDaten, zu verstehen, die zur Aufgabenerfüllung notwendig sind.

Die Befugnis zur Erteilung verbindlicher Anweisungen nach Art. 49c Abs. 1 Satz 3 BayDiG umfasst dabei insbesondere auch sämtliche der in Art. 33 Abs. 4 Buchst. b

bis d und Buchst. f der Richtlinie (EU) 2022/2555 genannten Maßnahmen. Die in Art. 49c Abs. 1 Satz 3 BayDiG verwendeten Begriffe „anweisen“ und „anordnen“ sind synonym zu verwenden; ein inhaltlicher Unterschied besteht nicht. Die Formulierung wurde klarstellend aus der Richtlinie (EU) 2022/2555 übernommen.

Die Nummerierung der Befugnisse in Art. 49c Abs. 1 BayDiG dient der Übersichtlichkeit und folgt der Systematik der Richtlinie (EU) 2022/2555. Eine Sortierung nach Intensität der Befugnis geht damit nicht einher. Verschiedene Befugnisse innerhalb einer Nummer schließen sich nicht gegenseitig aus, diese sind im Rahmen der Verhältnismäßigkeit grundsätzlich auch nebeneinander anwendbar.

Art. 49c Abs. 1 Satz 4 und 5 BayDiG setzen die Vorgaben der Art. 33 Abs. 5, Art. 32 Abs. 8 der Richtlinie (EU) 2022/2555 um. Das LSI hat Durchsetzungsmaßnahmen nach Art. 49c Abs. 1 Satz 3 BayDiG daher ausführlich zu begründen und den EBB – außer in besonders eilbedürftigen Fällen – vorab eine angemessene Frist zur Stellungnahme einzuräumen.

Art. 49c Abs. 2 BayDiG setzt die Vorgaben von Art. 35 der Richtlinie (EU) 2022/2555 um, nach dem eine Meldung des LSI an die zuständigen Datenschutzbehörden zu erfolgen hat, wenn ein Verstoß gegen bestimmte Vorgaben der Richtlinie (EU) 2022/2555 zugleich eine Verletzung des Schutzes personenbezogener Daten haben kann.

Art. 49c Abs. 3 BayDiG setzt die Vorgaben von Art. 23 Abs. 7 und Art. 33 Abs. 4 Buchst. a, e und g der Richtlinie (EU) 2022/2555 um.

Zu berücksichtigen ist, dass die obersten Dienstbehörden im Rahmen der staatlichen IT-Sicherheitsorganisation und des Ressortprinzips für die Sicherheit ihrer Informationstechnik ohnehin auch bereits selbst Sorge tragen. Sie haben u.a. für ihren Geschäftsbereich einen Informationssicherheitsbeauftragten bestellt, der für die Planung, Umsetzung, Prüfung und Verbesserung der Informationssicherheit verantwortlich ist und als Kontaktperson des LSI dient. Unbeschadet der Art. 44 und 45 BayDiG setzen Durchsetzungsmaßnahmen nach Art. 49c BayDiG daher im eng verzahnten IT-Betrieb staatlicher Behörden eine fortgeschrittene Eskalation des Sachverhalts voraus.

Die Vorgaben der DSGVO, insbesondere auch zu Art. 9 Abs. 1 DSGVO, bleiben unberührt.

Die Verhängung von Bußgeldern ist aufgrund von Art. 34 Abs. 7 der Richtlinie (EU) 2022/2555 nicht vorgesehen.

Zu § 1 Nr. 6 (Art. 57a BayDiG)

Die Umbenennung erfolgt lediglich zur Rechtsbereinigung.

Zu § 1 Nr. 7 (Art. 58 BayDiG)

Das Fernmeldegeheimnis könnte verletzt werden, wenn durch das LSI aufgrund der Befugnisse nach Art. 49c Daten eines Telekommunikationsvorgangs zwischen Bürgerinnen und Bürgern und einer staatlichen oder kommunalen Behörde ausgewertet werden. Nach Art. 19 Abs. 1 Satz 2 i. V. m. Art. 10 des Grundgesetzes dürfen Beschränkungen des Fernmeldegeheimnisses nur aufgrund eines Gesetzes angeordnet werden, das wiederum das Grundrecht unter Angabe des Artikels nennen muss. Zur Wahrung des Zitiergebots wird Art. 58 BayDiG vorsorglich neu gefasst.

Zu § 1 Nr. 8 (Art. 59 BayDiG)

Enthält Regelungen zum Inkraft- bzw. Außerkrafttreten. Die Streichung von Art. 59 Abs. 1 Satz 2 BayDiG und die Aufhebung von Art. 59 Abs. 2 und 4 BayDiG erfolgt lediglich zur Rechtsbereinigung, weil die dort genannten Änderungsbefehle jeweils wirksam geworden sind und die Vorschriften nunmehr nur noch eine gegenstandlos gewordene inhaltsleere Hülle darstellen. Daneben handelt es sich um redaktionelle Folgeänderungen aufgrund von § 1 Nr. 6.

Zu § 2

§ 2 regelt das Inkrafttreten des Gesetzes.