Stand: 04.02.2026 12:22:47

Vorgangsmappe für die Drucksache 19/2591

"Gesetzentwurf der Staatsregierung zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung"

Vorgangsverlauf:

1. Initiativdrucksache 19/2591 vom 25.06.2024
2. Plenarprotokoll Nr. 24 vom 03.07.2024
3. Beschlussempfehlung mit Bericht 19/2966 des WI vom 11.07.2024
4. Beschluss des Plenums 19/3420 vom 26.09.2024
5. Plenarprotokoll Nr. 28 vom 26.09.2024
6. Gesetz- und Verordnungsblatt vom 15.10.2024

Bayerischer Landtag

19. Wahlperiode 25.06.2024 **Drucksache 19/2591**

Gesetzentwurf

der Staatsregierung

zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung

A) Problem

1. Änderung des Bayerischen Digitalgesetzes

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 Bayerische Digitalgesetz anzupassen.

2. Änderung des Gesetzes über die Bayerische Landesstiftung

Sitzungen des Stiftungsrats im Wege der Video- und Telefonkonferenz oder in einem hybriden Format sind derzeit weder im Gesetz über die Bayerische Landesstiftung (BayLStG) noch in der Satzung der Bayerischen Landesstiftung ausdrücklich vorgesehen. Ferner sind Beschlussfassungen des Stiftungsrats im Umlaufverfahren nicht möglich.

Die Regelung in Art. 10 Abs. 3 Halbsatz 1 BayLStG, wonach die Bayerische Landesstiftung innerhalb von sechs Monaten nach Ablauf des Geschäftsjahres Rechnung zu legen hat, entspricht nicht mehr den aktuellen Vorschriften im Bayerischen Stiftungsgesetz (BayStG). Nach Art. 14 Abs. 1 Satz 4 BayStG ist innerhalb von neun Monaten nach Ablauf des Geschäftsjahres Rechnung zu legen.

B) Lösung

1. Änderung des Bayerischen Digitalgesetzes

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 Bayerischen Digitalgesetzes (IT-Sicherheit) erfolgen. Als zuständige Behörde (Aufsichtsbehörde) und CSIRT wird das LSI benannt und mit entsprechenden Aufgaben und Befugnissen ausgestattet.

2. Änderung des Gesetzes über die Bayerische Landesstiftung

Neben dem Regelfall von Präsenzsitzungen sollen die Voraussetzungen für die Durchführung von Sitzungen im Wege der Video- und Telefonkonferenz oder in einem hybriden Format sowie von schriftlichen und elektronischen Umlaufverfahren ausdrücklich in der Satzung der Bayerischen Landesstiftung geregelt werden. Die Ermächtigung hierzu enthält Art. 11 Satz 1 BayLStG, der bestimmt, dass die nähere Ausgestaltung der Stiftung durch eine Satzung geregelt werden soll. Um eine ausdrückliche Regelung in der Satzung der Bayerischen Landesstiftung zu ermöglichen, ist es aus Gründen der Rechtssicherheit und -klarheit beabsichtigt und erforderlich, dass Art. 8 Abs. 8 Satz 2 BayLStG aufgehoben wird.

Die Einführung der Möglichkeit der Beschlussfassung im Wege der elektronischen Kommunikation sowie im Umlaufverfahren für den Stiftungsrat in der Satzung der

Bayerischen Landesstiftung kann nur durch Änderung des Gesetzes über die Bayerische Landesstiftung und damit im Wege einer Gesetzesänderung umgesetzt werden.

Die Regelung zur Rechnungslegungsfrist in Art. 10 Abs. 3 Halbsatz 1 BayLStG wird ersatzlos gestrichen. Über den Verweis in Art. 14 BayLStG zur sinngemäßen Geltung der Bestimmungen des Bayerischen Stiftungsgesetzes gilt die Vorlagefrist von neun Monaten gemäß Art. 14 Abs. 1 Satz 4 BayStG.

C) Alternativen

Keine

D) Kosten

1. Änderung des Bayerischen Digitalgesetzes

1.1. 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 die in ihren 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.

1.2. Bürger und Wirtschaft

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

2. Änderung des Gesetzes über die Bayerische Landesstiftung

Es entstehen keine Kosten.

Bayerischer Landtag
19. Wahlperiode
Drucksache 19/**2591**
25.06.2024

Gesetzentwurf

zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung[1]

§ 1
Änderung des Bayerischen Digitalgesetzes

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,

      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 Mitgliedstaaten 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.

[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).

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, Ermittlung, 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 bearbeitet 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
Änderung des Gesetzes über die Bayerische Landesstiftung

Das Gesetz über die Bayerische Landesstiftung (BayLStG) in der in der Bayerischen Rechtssammlung (BayRS 282-2-10-F) veröffentlichten bereinigten Fassung, das zuletzt durch § 1 Abs. 54 der Verordnung vom 4. Juni 2024 (GVBl. S. 98) geändert worden ist, wird wie folgt geändert:

1. Art. 8 Abs. 8 wird wie folgt geändert:
   a) Satz 2 wird aufgehoben.

b) Satz 3 wird Satz 2.

2. In Art. 10 Abs. 3 Halbsatz 1 werden die Wörter „innerhalb von sechs Monaten“ gestrichen.

§ 3

Inkrafttreten

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

Begründung:

A) Allgemein

1. Änderung des Bayerischen Digitalgesetzes

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 kritische 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 − GG). 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 des Bayerischen Digitalgesetzes − 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 angeschlossener 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 Bayerischen Digitalgesetzes bleiben.

2. Änderung des Gesetzes über die Bayerische Landesstiftung

Vor dem Hintergrund der insbesondere in den letzten Jahren während der Coronapandemie gesammelten positiven Erfahrungen mit digitalen und elektronischen Kommunikationsformaten und der fortschreitenden Digitalisierung soll die Möglichkeit der virtuellen Kommunikation für den Stiftungsrat eine dauerhafte Regelung erhalten. Sitzungen des Stiftungsrats im Wege der Video- und Telefonkonferenz oder in einem hybriden Format sind derzeit weder im Gesetz über die Bayerische Landesstiftung (BayLStG) noch in der Satzung der Bayerischen Landesstiftung (BayLStS) ausdrücklich vorgesehen. Ferner sind Beschlussfassungen des Stiftungsrats im Umlaufverfahren nicht möglich.

Zur Erleichterung der Teilnahme an Sitzungen des Stiftungsrats sowie zur Vereinfachung von Beschlussfassungen sollen die Voraussetzungen für die Durchführung von Sitzungen im Wege der Video- und Telefonkonferenz oder in einem hybriden Format sowie von schriftlichen und elektronischen Umlaufverfahren ausdrücklich in der Satzung der Bayerischen Landesstiftung geregelt werden. Die Ermächtigung hierzu enthält Art. 11 Satz 1 BayLStG, der bestimmt, dass die nähere Ausgestaltung der Stiftung durch eine Satzung geregelt werden soll. Um eine ausdrückliche Regelung in der Satzung der Bayerischen Landesstiftung zu ermöglichen, ist es aus Gründen der Rechtssicherheit und -klarheit beabsichtigt und erforderlich, dass Art. 8 Abs. 8 Satz 2 BayLStG aufgehoben wird.

Künftig können die Voraussetzungen für die Beschlussfähigkeit des Stiftungsrats mitsamt der Möglichkeit der Beschlussfassung im Wege der elektronischen Kommunikation einheitlich in der Satzung geregelt werden.

Nach Art. 10 Abs. 3 Halbsatz 1 BayLStG hat die Landesstiftung innerhalb von sechs Monaten nach Ablauf des Geschäftsjahres Rechnung zu legen. Gemäß Art. 14 Abs. 1 Satz 4 des Bayerischen Stiftungsgesetzes (BayStG) haben Stiftungen gegenüber der Stiftungsbehörde innerhalb von neun Monaten Rechnung zu legen.

Die Bestimmungen des Bayerischen Stiftungsgesetzes gelten für die Landesstiftung sinngemäß (Art. 14 BayLStG).

Zur Anpassung der Rechnungslegungsfrist der Landesstiftung an die jeweils aktuellen Regelungen des Bayerischen Stiftungsgesetzes werden die Wörter „innerhalb von sechs Monaten“ in Art. 10 Abs. 3 Halbsatz 1 BayLStG gestrichen.

B) Zwingende Notwendigkeit einer normativen Regelung

1. Änderung des Bayerischen Digitalgesetzes

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).

2. Änderung des Gesetzes über die Bayerische Landesstiftung

Das Gesetz über die Bayerische Landessstiftung regelt die Aufgaben, die Struktur und Zusammensetzung der Organe sowie den im Übrigen für die Stiftung maßgeblichen Rechtsrahmen. Art. 8 Abs. 8 Satz 2 BayLStG bestimmt bisher, dass zur Beschlussfähigkeit die „Anwesenheit“ der Stiftungsratsmitglieder erforderlich ist. Durch die dargelegte Änderung des Art. 8 Abs. 8 Satz 2 BayLStG kann die Ausgestaltung der Beschlussfähigkeit des Stiftungsrats mitsamt der Möglichkeit von Beschlussfassungen im Wege der elektronischen Kommunikation einheitlich in der Satzung geregelt werden. Eine Erweiterung des Normbestandes des Gesetzes über die Bayerische Landesstiftung kann hierdurch vermieden werden. Art. 8 Abs. 8 Satz 2 BayLStG ist daher zwingend zu ändern.

Art. 10 Abs. 3 Halbsatz 1 BayLStG bestimmt bislang, dass die Rechnungslegung innerhalb von sechs Monaten nach Ablauf des Geschäftsjahres zu erfolgen hat. Durch die dargelegte Änderung des Art. 10 Abs. 3 Halbsatz 1 BayLStG gilt über den Verweis in Art. 14 BayLStG die jeweils aktuelle Regelung des Bayerischen Stiftungsgesetzes.

C) Einzelbegründung

1. Änderung des Bayerischen Digitalgesetzes

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 Mitgliedstaat 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-Verordnung) 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 der Datenschutz-Grundverordnung (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 Abs. 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 zugrunde 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 Bundesamt für Sicherheit in der Informationstechnik (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 Bayerischen Digitalgesetzes (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 Abs. 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 2 der Verfassung des Freistaates Bayern − BV − sowie Art. 28 Abs. 2 GG) 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 Bayerischen Digitalgesetzes 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 den Datenschutz zusätzlich Art. 33a Abs. 3 BV). 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 wird 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 angeschlossener 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 Richtlinie (EU) 2022/2555 umgesetzt. EBB 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 setzt 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 Datenschutz-Grundverordnung, 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 GG 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.

2. Änderung des Gesetzes über die Bayerische Landesstiftung

Zu § 2 Nr. 1 (Art. 8 Abs. 8 BayLStG)

Die Voraussetzungen für die Durchführung von Sitzungen im Wege der Video- und Telefonkonferenz oder in einem hybriden Format sowie von schriftlichen und elektronischen Umlaufverfahren sollen ausdrücklich in der Satzung der Bayerischen Landesstiftung geregelt werden. Die Ermächtigung hierzu enthält Art. 11 Satz 1 BayLStG, wonach die nähere Ausgestaltung der Stiftung durch eine Satzung geregelt werden soll. Um

eine ausdrückliche Regelung in der Satzung der Bayerischen Landesstiftung vorzusehen, bedarf es aus Gründen der Rechtssicherheit und -klarheit einer Aufhebung des Art. 8 Abs. 8 Satz 2 BayLStG.

Zu § 2 Nr. 2 (Art. 10 Abs. 3 BayLStG)

Bislang hat die Bayerische Landesstiftung nach Art. 10 Abs. 3 Halbsatz 1 BayLStG innerhalb von sechs Monaten nach Ablauf des Geschäftsjahres Rechnung zu legen. Damit besteht eine Diskrepanz zu der seit 1. August 2023 geltenden Regelung in Art. 14 Abs. 1 Satz 4 BayStG, der eine Rechnungslegungsfrist von neun Monaten vorsieht. Künftig kann durch den Verweis in Art. 14 BayStG auf die sinngemäße Anwendung des Bayerischen Stiftungsgesetzes die jeweils aktuelle Rechnungslegungsfrist zur Anwendung kommen.

Zu § 3

§ 3 regelt das Inkrafttreten des Gesetzes.

Redner zu nachfolgendem Tagesordnungspunkt

Erster Vizepräsident Tobias Reiß
Staatsminister Albert Füracker
Abg. Florian Köhler
Abg. Dr. Stefan Ebner
Abg. Benjamin Adjei
Abg. Tobias Beck
Abg. Florian von Brunn
Abg. Andreas Jurca

Erster Vizepräsident Tobias Reiß: Ich rufe **Tagesordnungspunkt 1 b** auf:

Gesetzentwurf der Staatsregierung
zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung (Drs. 19/2591)
- Erste Lesung -

Begründung und Aussprache werden miteinander verbunden. Die Staatsregierung hat 14 Minuten Redezeit. Zugleich eröffne ich die Aussprache. Die Gesamtredezeit der Fraktionen beträgt 29 Minuten. – Ich erteile Herrn Staatsminister Albert Füracker das Wort.

Staatsminister Albert Füracker (Finanzen und Heimat): Lieber Herr Präsident, sehr geehrte Damen und Herren, Kolleginnen und Kollegen! Es geht um die sichere IT-Infrastruktur und die Cyberabwehr. Das sind große Themen für unsere staatliche Verwaltung sowie für die Strafverfolgung, die Kommunen und die Unternehmen. In Bayern haben wir einen hohen Digitalisierungsgrad in unserer Verwaltung. Deswegen haben wir uns schon längst entschlossen, einen besonderen Weg zu gehen. Bayern hat als erstes Bundesland eine eigene Fachbehörde eingerichtet.

Schon im Jahr 2017 wurde das Landesamt für Sicherheit in der Informationstechnik eingerichtet. Das kommt uns heute zugute. Das LSI arbeitet sehr erfolgreich. Mittlerweile hat es 150 Mitarbeiterinnen und Mitarbeiter. Das LSI hat die Aufgabe, staatliche Behörden vor Cyberangriffen zu schützen. Wir treten auch als hoch kompetente Unterstützer und Berater für die Kommunen und Betreiber kritischer Infrastrukturen auf. Das LSI ist gleichsam das Pendant zum BSI, dem Bundesamt für Sicherheit in der Informationstechnik. Mittlerweile hat es sich in Bayern etabliert. Ich bin sehr froh, dass wir es haben.

Im Übrigen gibt es viel zu tun. Das LSI analysiert im Sicherheitsmonitoring täglich 2,5 Milliarden Datensätze. Täglich werden 1,4 Millionen E-Mails mit Schadcode gefiltert. Das LSI hat bereits Ende 2023 mit den Angeboten rund 94 % der Kommunen er-

reicht. Warum ist es jetzt so bedeutsam? – Durch die Neuerung, die jetzt in eine gesetzliche Form gebracht werden muss, müssen wir nicht bei null beginnen. Stattdessen kommen wir mit einer Ergänzung des Digitalgesetzes zurecht. Es geht um die Umsetzung der sogenannten NIS-2-Richtlinie. Das ist natürlich etwas für Feinschmecker. Es handelt sich um eine Richtlinie der Europäischen Union, die nichts anderes zum Ziel hat, als das gemeinsame Cybersicherheitsniveau in der EU zu stärken. Diese Richtlinie betrifft vor allen Dingen Unternehmen und muss vorrangig durch den Bund umgesetzt werden. Das ist wahr. Der Bund führt jedoch im Rahmen der Gesetzgebung eine Länder- und Verbändeanhörung durch. Die zeitliche Perspektive ist unklar. Für uns ist das – das sage ich in aller Offenheit – nicht entscheidend. Wir müssen in jedem Fall, wie jedes andere Bundesland auch, unsere eigene Gesetzgebung anpassen.

In den Anwendungsbereich der Richtlinie fallen auch die öffentlichen Verwaltungen. Im Übrigen hat der Bund für die bayerischen Behörden keine Gesetzgebungskompetenz. Deswegen machen wir uns unabhängig von der Zeitschiene des Bundes auf den Weg und setzen die NIS-2-Richtlinie in Landesrecht um. Die Notwendigkeit einer gesetzlichen Regelung besteht. Wir passen bereits bestehende Vorschriften zur IT-Sicherheit einfach an. Es besteht eine hohe Übereinstimmung. Im Hinblick auf die NIS-2-Richtlinie besteht anders als bei vielen anderen EU-Richtlinien kein Anlass, in großes Geschrei zu verfallen. Die Regelung ist nicht ideal und sehr auf Unternehmen zugeschnitten. Unser Gesetzentwurf befasst sich mit der Umsetzung insbesondere für die Verwaltungen.

Wir machen eine Eins-zu-eins-Umsetzung. Wir praktizieren kein Gold Plating von EU-Recht, wie es der Bund so gerne betreibt. Das kann man dem Gesetzentwurf nicht nachsagen. Wir sind gut aufgestellt. Ich sprach es an. Wir müssen aber die EU-Vorgaben erfüllen. Die EU verlangt, in Zukunft in jedem Land ein Computer Security Incident Response Team einzurichten. Meine Damen und Herren, das hört sich toll an, das haben wir aber schon längst. Früher hieß das bei uns Bayern-CERT, jetzt heißt es LSI.

Das ist also kein Problem. Die Fachbehörde LSI existiert. Wir werden die Aufgaben dieser Aufsichtsbehörde im LSI bündeln, wie es die Richtlinie fordert. Durch unser bereits hohes Sicherheitsniveau werden wir zusätzliche Bürokratie auch in Grenzen halten können. Eine gute Zusammenarbeit zwischen dem LSI und dem BayernServer ist vorhanden.

Wir haben vor, die europarechtlich vorgegebenen Aufsichts- und Durchsetzungsbefugnisse gegenüber allen erfassten Behörden im LSI zu bündeln. Fazit: Die Entscheidung, das LSI zu gründen, war eine wirklich wichtige und zukunftsweisende Entscheidung. Somit ist die Umsetzung der Richtlinie keine große Herausforderung für uns. Wir haben eine gewisse Vorreiterfunktion. Im Hinblick auf die IT-Sicherheit sage ich immer: Es geht nicht darum, dass sich jemand als zuständiger Minister hinstellt.

(Toni Schuberl (GRÜNE): Wo ist der Digitalminister?)

Wenn man für die IT-Sicherheit des Freistaats Bayern Verantwortung trägt, stellt sich jeden Tag die Frage: Was kann man machen, damit die IT-Sicherheit intensiver gewährleistet ist? Insoweit ist die Zuständigkeit in meinem Geschäftsbereich für das Landesamt für Sicherheit und Informationstechnik von jeher gegeben. Diese werden wir auch wahrnehmen. Wir können zusagen, alles Menschenmögliche zu tun, aber zu versprechen, dass niemandem irgendetwas passieren könnte, wäre vermessen. Das mache ich sicher nicht. Aber ich kann zusagen, dass wir das aus unserer Sicht Menschenmögliche tun, um die IT-Sicherheit bei uns zu gewährleisten.

Wir habe noch ein Update für die Bayerische Landesstiftung an dieses Gesetz angehängt. Dabei geht es darum – ich würde sagen, dass das mehr eine Formalie ist –, dass die Bayerische Landesstiftung, wie es auch während der Pandemie der Fall war, in Sitzungen in Form von Video- und Telefonkonferenzen handeln und Beschlussfassungen im Umlaufverfahren durchführen kann. Während der COVID-Pandemie sind gute Erfahrungen damit gemacht worden. Deswegen besteht der Wunsch, dass man das Ganze in Gesetzesform fixiert. Das können wir gerne machen.

Es gibt eine weitere Änderung, und zwar für die Rechnungslegung der Bayerischen Landesstiftung: Es gilt künftig eine Frist von 9 statt bisher 6 Monaten. Das gilt auch für alle anderen Stiftungen in Bayern.

Diese Änderungen machen die Bayerische Landesstiftung agiler, schaffen überflüssige Sonderregelungen ab und entbürokratisieren gleichsam. Es ist daher aus meiner Sicht kein Problem, sowohl der Änderung des Digitalgesetzes als auch der Regelung zur Landesstiftung zuzustimmen. Das Ganze kommt jetzt dann in die Ausschüsse. Ich bitte um eine positive Beratung, eine positive Beschlussfassung und somit Zustimmung zum Gesetzentwurf.

(Beifall bei der CSU und den FREIEN WÄHLERN)

Erster Vizepräsident Tobias Reiß: Danke, Herr Staatsminister. – Der nächste Redner ist der Kollege Florian Köhler.

(Beifall bei der AfD)

Florian Köhler (AfD): Sehr geehrter Herr Vizepräsident, sehr geehrte Kollegen, sehr geehrte Damen und Herren auf der Besuchertribüne! Das Ziel des vorgelegten Gesetzes ist es, ein hohes Cybersicherheitsniveau in der EU und ihren Mitgliedstaaten zu gewährleisten. Im Wesentlichen wird die NIS-2-Richtlinie der Europäischen Union auf Landesebene umgesetzt. Bayern hat bei der Umsetzung tatsächlich einen sehr geringen Umsetzungsspielraum. Der Freistaat hat mit dem Landesamt für Sicherheit in der Informationstechnik – LSI – bereits den Grundstein gelegt, das wurde eben schon angesprochen. Der Freistaat hat bereits eine entsprechende Behörde gegründet. Diese wird nun in einigen Fällen – ich sage mal – mit mehr Befugnissen ausgestattet. Wobei ich sagen muss, dass diese Ausdrucksweise ein bisschen zu hoch gegriffen ist. Im Wesentlichen sorgt die Novellierung erst mal für mehr Klarheit, um angemessene Reaktionen auf Angriffe sicherzustellen. Neben deutlicheren Formulierungen bei Rechtsbegriffen und neben ein paar redaktionellen Änderungen gibt es zusätzliche sprachli-

che Angleichungen. Wir sind immer ein Freund von klaren, bestimmten und unmissverständlichen Formulierungen.

Im Fokus steht auch das bereits angesprochene Computer Security Incident Response Team. Auch das wurde bereits vom Freistaat eingerichtet und untersteht dem LSI. Eine wesentliche Änderung bezieht sich auf die Speicherfrist von Protokolldaten, die das LSI erhebt: Diese soll von 12 auf 18 Monate verlängert werden – aber auch darüber kann man diskutieren. Auf der einen Seite sehen wir durch die Verlängerung der Speicherfristen von Protokolldaten eine gewisse Praktikabilität, aber auf der anderen Seite könnte das auch zu einem Datenschutzproblem führen, insbesondere im Hinblick auf personenbezogene Daten.

Wir müssen uns noch ein finales Urteil über das dreistufige Meldeverfahren bilden; denn die Einführung neuer Melde- und Berichtspflichten könnte den Verwaltungsaufwand erheblich erhöhen, ohne dass klare Mehrwerte entstehen.

Im Gegensatz zur Staatsregierung sehen wir durchaus, dass die EU-Richtlinie am Ende des Tages wahrscheinlich für einen erhöhten Verwaltungsaufwand insgesamt sorgen wird, ganz zu schweigen davon, was auf die Unternehmen zukommen wird. Dafür ist – das ist bereits angesprochen worden – der Bund, also die Ampel zuständig. Vermutlich wird das also noch schlechter gemacht für Unternehmen.

Die noch nicht verabschiedeten Rahmenbedingungen auf Bundesebene könnten zu weiteren notwendigen Anpassungen und möglicher Rechtsunsicherheit führen. Aber wie der Herr Minister gerade schon gesagt hat, müssen wir abwarten und Tee trinken, und anschließend können wir entsprechend reagieren.

Die Regelungen des Stiftungsgesetzes sind an sich sehr praxisorientiert. Ich nenne nur als Beispiel die Ermöglichung von Umlaufbeschlüssen. Das ist durchaus sinnvoll.

Zum Schluss bleibt noch die Kostenfrage: Obwohl die Änderungen als kostenneutral dargestellt werden, werden versteckte Kosten gerade beim LSI bzw. den anderen Ver-

waltungsbehörden durch notwendige Schulungen und Infrastrukturmaßnahmen entstehen. Das ist einfach so. Wir werden die Argumente im Ausschuss genau analysieren und uns dann eine abschließende Meinung bilden.

(Beifall bei der AfD)

Erster Vizepräsident Tobias Reiß: Vielen Dank. – Der nächste Redner ist der Kollege Dr. Stefan Ebner.

Dr. Stefan Ebner (CSU): Herr Präsident, meine sehr verehrten Kolleginnen und Kollegen, sehr geehrte Damen und Herren! Ich möchte meine Rede heute mit etwas Positivem beginnen, weil wir heute Bayern sicherer machen können. Wir können heute Bayern cybersicherer machen. Das ist wichtig, weil die Cyberkriminalität jedes Jahr weiter zunimmt. Jedes dritte Unternehmen in Deutschland ist in den letzten zwei Jahren Opfer von Cyberattacken geworden. Der wirtschaftliche Schaden ist enorm: Er liegt bei 150 Milliarden Euro pro Jahr. Deswegen müssen wir in unserer digitalen Welt verteidigungs- und wehrfähiger werden. Bayern wird täglich angegriffen. Bayern muss sich täglich verteidigen, aber nicht nur Bayern, sondern auch Deutschland und Europa. Deswegen haben der Europäische Rat und das Europäische Parlament richtig entschieden, die Cybersecurity in unserem Heimatkontinent auf ein neues, höheres Niveau zu heben.

Meine Damen und Herren, die Menschen und die Unternehmen erwarten zu Recht, dass sie vor Einbruch, Diebstahl, Sabotage und Erpressung geschützt werden. Sie erwarten das nicht nur in der analogen Welt, sondern auch in der digitalen Welt. Ich will betonen, dass die Europäische Volkspartei – die EVP – unter dem Vorsitz von Manfred Weber dieses Thema federführend vorangetrieben hat, damit Europa stärker vor Cyberangriffen geschützt wird.

Wir sehen im Übrigen auch, dass die Thematik ein gutes Beispiel dafür ist, wie wichtig europäische Zusammenarbeit ist. Ich will eine Randbemerkung in die rechte Richtung machen, zu Ihrem Freund Björn Höcke. Dieser sagt, dieses Europa muss sterben.

(Zuruf von der AfD: Die EU! Mein Gott!)

Nein, dieses Europa wird nicht sterben, ganz im Gegenteil. Auf europäischer Ebene müssen wir dafür sorgen, dass wir die Menschen noch stärker schützen. Gerade solch große Probleme und Herausforderungen sind europäisch zu lösen; sie können nur europäisch gelöst werden.

Ich komme nun zurück zur Mitte Europas, zurück nach Bayern. Unser Staatsverständnis ist klar, unser Staatsverständnis heißt: Sicherheit und Ordnung für die Bürger herstellen. Bayern ist exzellent aufgestellt – der Minister hat das ausführlich dargestellt – mit IT-Spezialistinnen und -Spezialisten, bei der Polizei, beim Verfassungsschutz, bei der Justiz und beim Landesamt für Sicherheit in der Informationstechnik. Dieses Landesamt macht seit sechs Jahren einen ganz tollen Job bei der Abwehr von Cybergefahren. Ich möchte das Ganze konkret machen: Im Jahr 2022 sind 4.000 Angriffe auf das Bayerische Behördennetz unternommen worden. Das sind im Durchschnitt 11 Angriffe pro Tag. Wir werden heute lange tagen, wahrscheinlich bis 23 Uhr. Das heißt, bis zum Ende unserer Sitzung werden wahrscheinlich 5 Angriffe auf das Bayerische Behördennetz erfolgen. Das Gute dabei ist, dass es bei den Angriffen wahrscheinlich genauso sein wird wie bei den letzten 4.000 Mal, dass kein einziger dieser Angriffe durchkommen wird.

Deswegen möchte ich an dieser Stelle den 150 IT-Sicherheitsexpertinnen und -experten am Landesamt für Sicherheit in der Informationstechnik, die Bayerns IT schützen, ein herzliches Dankeschön aussprechen. Auf dem Cyberschlachtfeld sind sie die Cyberarmee des Freistaates.

(Beifall bei der CSU)

Ja, so ist es: Bayern nimmt eine Vorreiterrolle beim Thema Cybersecurity ein. Das ist das bayerische Staatsverständnis von Ordnung und Sicherheit. Das gilt analog, und das gilt digital.

Meine Damen und Herren, diese Art von Politik ist deswegen so wichtig, weil wir uns nicht sicher sein können, dass wir alle in der Politik an einem gemeinsamen Strang ziehen. Ich schaue wieder zu Ihnen nach rechts, meine Damen und Herren von der AfD. Mit Ihnen ist kein glaubwürdiger Kampf gegen die Cyberkriminalität zu führen. Bei Ihnen weiß man nicht, auf welcher Seite Sie stehen. Die Mehrheit der Cyberangriffe kommt aus China, Russland, Nordkorea und dem Iran. Das heißt, ein Drittel der Cyberangriffe kommt aus Staaten, die gegen den Westen gerichtet sind. Ich frage Sie: Wie soll denn eine politische Partei glaubwürdig im Kampf gegen Cyberangriffe aus China und Russland sein, wenn einige Leute seit Monaten im Verdacht stehen, sich genau von diesen Ländern schmieren zu lassen?Ich frage mich schon ernsthaft, wie so eine Partei in ihrem Namen behaupten kann, sie sei für Deutschland.

(Florian von Brunn (SPD): Abstieg für Deutschland: AfD!)

Meine Damen und Herren, so wenig, wie Sie eine Alternative sind, so wenig sind Sie offenbar für Deutschland. Meine Damen und Herren, aber unabhängig davon ist es die ureigenste Aufgabe politischer Verantwortungsträger, enge Verbindungen ins Ausland aufzubauen, Verbindungen zu pflegen oder auszubauen.

(Florian von Brunn (SPD): Alles andere, aber nicht für Deutschland! – Widerspruch bei der AfD)

Das müssen dann Verbindungen im Interesse des eigenen Landes und nicht im Interesse der anderen sein. Im globalen Cyberkampf braucht es Soldaten und keine Söldner, meine Damen und Herren.

Wir sprechen aber über den Kampf gegen Cyberkriminalität. Da würde man sich auch ein bisschen mehr Engagement vom linken Rand des Parlaments wünschen. Nehmen wir die GRÜNEN: Ähnlich wie bei vielen anderen Themen sind die GRÜNEN manchmal zu naiv, ein bisschen zu zurückhaltend, ein bisschen zu bürokratisch, ein bisschen zu langsam. Man sieht es auch: Das Gesetz muss bis zum 17. Oktober 2024 in natio-

nales Recht umgesetzt werden. Auf Bundesebene ist in dem Bereich immer noch nichts entstanden.

(Florian von Brunn (SPD): Das stimmt doch überhaupt nicht! Sie sind nur nicht informiert! Das ist das Problem!)

Wären manche Grüne im Kampf gegen Cyberattacken engagierter, könnte man Viren und Trojaner zu einer Tüte drehen, meine Damen und Herren.

(Florian von Brunn (SPD): Meine Güte!)

Aber Hacker lösen sich nicht in Rauch auf. Hackern muss man das Handwerk legen, meine Damen und Herren.

Lassen Sie mich zum Schluss kommen: Mit der heutigen Debatte und der Ersten Lesung beschließen wir noch mehr Sicherheit für Bayern. Wir setzen eine EU-Richtlinie um. Wir setzten sie eins zu eins um, das heißt, ohne ein Mehr an Bürokratie und ohne Extras. Der Freistaat rüstet sich und präpariert sich, und das alles unter dem Dach des Staatsministers der Finanzen und für Heimat Albert Füracker. Bei ihm ist das Thema Cyberkriminalität in besten Händen. Ich bitte Sie, diesen Gesetzentwurf zu unterstützen.

(Beifall bei der CSU – Zuruf des Abgeordneten Martin Böhm (AfD))

Erster Vizepräsident Tobias Reiß: Vielen Dank, Herr Kollege. – Als Nächstem erteile ich dem Kollegen Benjamin Adjei das Wort.

Benjamin Adjei (GRÜNE): Herr Präsident, liebe Kolleginnen und Kollegen! Beim Finanzminister ist das Thema Cyberkriminalität in besten Händen – nur ärgerlich, dass wir einen Digitalminister haben. Lieber Fabian, ich bin mir aber sicher: Du versuchst auch irgendwie dein Bestes, in internen Gesprächsrunden bei der Digitalisierung mal etwas bewegen zu können; denn die Digitalisierung in Bayern und in Deutschland schreitet immer weiter voran. Wir wollen, wie ihr in der Staatsregierung es euch auf die

Fahnen geschrieben habt, unsere Staatsverwaltung modernisieren und digitalisieren. Dann müssen wir natürlich dafür sorgen, dass die Verwaltung am Ende resilient gegenüber Angriffen von außerhalb ist und ihnen standhalten kann, um die Staatsverwaltung zu sichern, aber auch die Bürgerinnen und Bürger zu schützen.

Gerade ist schon ausgeführt worden: Die Zahl der Angriffe nimmt zu. Das BSI hat für das letzte Jahr eine Steigerung der Zahl der Angriffe um 28 % gemessen, vor allem aus dem Ausland. Die Angriffe kommen weniger von innen heraus, sondern mehr aus dem Ausland, insbesondere aus China und Russland. Da ist es wichtig und richtig, dass die EU sich jetzt auf den Weg macht, das Thema Cybersecurity mit der NIS-2-Richtlinie zu stärken. Die EU möchte flächendeckend hohe Standards ansetzen. Dabei muss sie die verschiedenen Regelungen in den Mitgliedstaaten der Europäischen Union harmonisieren; denn ich glaube, auch mit Blick auf Unternehmen ist es ganz essenziell, dass es nicht in jedem Land andere, sondern einheitliche, gleiche und gute Regeln gibt. Hier ist der Bund auf dem Weg. Er ist etwas verspätet, das stimmt, aber er ist auf dem Weg, das umzusetzen. Die Bayerische Staatsregierung setzt auf Landesebene das um, was hier umzusetzen ist.

Lieber Albert Füracker, ich habe es bei der Haushaltsdebatte schon gesagt: Natürlich lobe ich auch das, was in Bayern gut läuft. Damals habe ich auch das LSI hervorgehoben. Das ist eine Errungenschaft des Freistaates, die es in keinem anderen Bundesland gibt. Jetzt hat es sich wieder bewährt, weil viele der Regelungen, die eingeführt werden müssen, sehr einfach durch kleine Gesetzesänderungen ohne das Einführen neuer Behörden und Strukturen umgesetzt werden können. Ich habe selber schon das Bayern-CERT am LSI besucht. Das ist wirklich eine sehr gute Institution. Entsprechend gut ist es, das weiterzuführen und auszubauen.

Bei allem Lob gibt es aber natürlich auch ein bisschen Kritik: Die richtet sich nicht rein an die Bayerische Staatsregierung, sondern eigentlich an den IT-Planungsrat insgesamt. Die Bundesländer haben sich nämlich entschieden, nicht alles aus der NIS-2-Richtlinie umzusetzen, insbesondere die Kommunen nicht mit aufzunehmen. Das

halte ich für einen großen Fehler. Die Kommunen sind das Rückgrat unserer Staatsverwaltung. Insbesondere, wenn es um die Digitalisierung der Kommunal- oder der Staatsverwaltung geht, wird sehr viel von den Kommunen umgesetzt werden müssen. Gleichzeitig nehmen die Angriffe auf Kommunen massiv statt.

(Bernhard Pohl (FREIE WÄHLER): Zu!)

– Sie nehmen massiv zu. Das BSI hat letztes Jahr 27 Angriffe auf Kommunalverwaltungen gemessen. 6 Millionen Menschen in Deutschland leben in diesen betroffenen Kommunen. Das ist die Hälfte der bayerischen Bevölkerung. Das muss man sich wirklich mal vorstellen, wie viele Menschen allein im letzten Jahr betroffen waren. Ich schaue mir die Steigerungsraten an: Die werden in den nächsten Jahren massiv zunehmen. Ich glaube, es wäre insbesondere mit Blick auf die Daseinsvorsorge fatal, hier die Kommunen jetzt komplett rauszunehmen und zu sagen: Nein, wir geben euch nicht die hohen Sicherheitsstandards und die Auflagen und natürlich dann, damit verbunden, auch nicht die Unterstützung bei der Umsetzung.

Ich selber stamme aus dem Landkreis Miesbach. Vielleicht kennt der eine oder andere das Krankenhaus Agatharied. Das arbeitet nämlich im Moment analog, offline. Warum arbeitet es analog und offline? – Weil es vor zwei Wochen Opfer eines großen Cyberangriffs geworden ist. Es ist das einzige Kreiskrankenhaus in dem Landkreis und auch noch Mitversorgungskrankenhaus für die benachbarten Landkreise. Die müssen im Moment alles analog machen, weil alle Systeme, übrigens inklusive der Schrankensteuerung an den Zuwegen zu dem Krankenhaus, wegen des Angriffs abgeschaltet werden mussten. Ich glaube, das zeigt ganz deutlich, wie wichtig es ist, die Kommunen in der IT-Sicherheit stärker mit in die Pflicht zu nehmen, aber auch entsprechend zu unterstützen. Da hätte ich mir vom Freistaat Bayern mehr Drive gewünscht.

Die anderen Bundesländer haben gesagt, sie halten die Kommunen da auch raus. Sonst sagt Bayern eigentlich auch immer: Es ist uns doch egal, was die anderen Bundesländer sagen. Wir gehen voran. Wir machen mehr. Wir gehen weiter. – Das würde

ich mir in dem Fall auch wünschen. Vielleicht kommt da noch ein Änderungsvorschlag, vielleicht von den FREIEN WÄHLERN, die die Themen des modernen Staates und der Kommunen für sich so hoch proklamieren.

(Felix Locke (FREIE WÄHLER): Von euch kommt da wohl nichts, oder?)

– Vielleicht kommt da von euch noch etwas. Darüber würde ich mich freuen.

(Beifall bei den GRÜNEN)

Erster Vizepräsident Tobias Reiß: Nächster Redner ist der Kollege Tobias Beck.

Tobias Beck (FREIE WÄHLER): Sehr geehrter Herr Präsident, werte Kolleginnen und Kollegen, liebe Besucherinnen und Besucher! Täglich erreichen uns Berichte über Cyberangriffe in verschiedenen Sektoren, sei es in der Wirtschaft, den Finanzen, den Immobilien oder im Gesundheitswesen. All dies sind Angriffe auf unseren täglichen Alltag und den unserer Bürgerinnen und Bürger. Zudem müssen bei den täglich wachsenden Angriffsmöglichkeiten auch Gesetze der Situation entsprechend angepasst und erweitert werden, um auch weiterhin die Cybersicherheit im privaten, wirtschaftlichen und staatlichen Sektor zu erhalten.

Hier sei gesagt: Hundertprozentige Sicherheit gibt es nicht; aber der Staat hat die Aufgabe, die Rahmenbedingungen so zu setzen, dass das Risiko minimiert und eine Rekapitulation der Ereignisse möglich ist. Deshalb gibt es für die Neufassung der NIS-2-Richtlinie, welche von den Mitgliedstaaten bis Oktober dieses Jahres umzusetzen ist, Ansätze, um Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Europäischen Union in nationales Recht umzusetzen.

Die Bayerische Staatsregierung hat mit der Errichtung des Landesamts für Sicherheit in der Informationstechnik und der gesetzlichen Verpflichtung der Behörden zu angemessener Informationssicherheit mit dem Bayerischen Digitalgesetz sowie der Einführung von Managementsystemen für Informationssicherheit in den staatlichen Behörden bereits Maßnahmen zur IT-Sicherheit für Verwaltungsbehörden in Bayern

ergriffen, die den Zielsetzungen der Richtlinie sehr nahekommen. Insbesondere besteht gemäß der Richtlinie das Cybersecurity Incidence Response Team bereits als Bayern-CERT im LSI. Zudem verfügt das LSI in seiner Funktion als Behörde zur Gefahrenabwehr bereits über Befugnisse, unter anderem zur Untersuchung der Sicherheit in der Informationstechnik staatlicher und an das Behördennetz angeschlossener Stellen. Gleichwohl bedürfen die sehr detaillierten Vorgaben der EU-Richtlinie der Umsetzung ergänzender Regelungen im Landesrecht. Dies betrifft etwa das dreistufige Verfahren für Einrichtungen im Anwendungsbereich der Richtlinie zur Meldung erheblicher Sicherheitsvorfälle an das LSI.

Aufgrund der sich erst noch abzeichnenden bundesrechtlichen Regelungen sind die nationalen Rahmenbedingungen zwar weiterhin offen; gleichwohl ist zur Wahrung der Umsetzungsfrist das Bayerische Digitalgesetz bereits jetzt anzupassen. Vor allem die Entwicklung der Bedrohungslage macht die Notwendigkeit einer engeren Zusammenarbeit zwischen BSI und LSI deutlich.

Wie die Cybervorfälle gerade in jüngster Vergangenheit gezeigt haben, geht besondere Gefahr von hochspezialisierten Cyberangriffen aus, sogenannten Advanced Persistent Threats oder APTs. Angreifer versuchen dabei, vorsichtig und verdeckt vorzugehen, sodass zwischen dem erfolgreichen Hack der Kommunikationstechnik und der Aufdeckung des Angriffes in der Regel große Zeiträume liegen. Hier wird in aller Regel nur mitgehört und protokolliert, was im System passiert. Aufgrund dieser Infiltrierung können weitere Angriffe sehr detailliert geplant und teils erfolgreich umgesetzt werden.

Um das Ganze etwas einfacher und verständlicher zu machen: Wenn heute jemand ein Auto stehlen will, wird dies dadurch einfacher, wenn man weiß, um welchen Autotyp es sich handelt, welches Baujahr das Auto hat und welcher Serie es zugehört. Genau so erfolgen die Angriffe auf die IT-Systeme. Mit APTs wird versucht, die Gerätehersteller und Firmwarestände herauszufinden, um so einen höheren Grad an erfolgreichen Attacken zu erreichen.

An diesem Punkt setzt die NIS-2-Richtlinie an: Die Protokollspeicherdauer wird auf 18 Monate erhöht. Das verbessert die Möglichkeit der Reaktion auf Angriffe und gewährleistet unserer Ansicht nach zugleich einen angemessenen Schutz von personenbezogenen Daten.

Der letzte Punkt ist die Änderung des Gesetzes über die Bayerische Landesstiftung. Dazu ist schon einiges gesagt worden. Es geht hauptsächlich darum, dass die Landesstiftung auch digital tagen kann und dass Umlaufverfahren auch elektronisch durchgeführt werden können. Das ist unserer Meinung nach eine sehr gute und wichtige Änderung.

Zum Schluss möchte ich noch einmal darauf hinweisen: Die Sicherheit der Informationstechnik staatlicher und sonstiger an das Behördennetz angeschlossener Stellen muss auch in Zukunft im Fokus des Bayerischen Digitalgesetzes bleiben. Deshalb bitte ich um Ihre Zustimmung.

(Beifall bei der CSU)

Erster Vizepräsident Tobias Reiß: Vielen Dank. – Nächster Redner ist der Fraktionsvorsitzende der SPD, Florian von Brunn.

Florian von Brunn (SPD): Sehr geehrter Herr Vizepräsident, sehr geehrte Damen und Herren! Gut, dass sich die Europäische Union um die Themen Cyberkriminalität und Schutz vor Hackerangriffen kümmert. Die Richtlinie muss jetzt umgesetzt werden. Der Freistaat Bayern macht das jetzt, der Bund ist intensiv bei der Umsetzung. Es gibt dort schon Referentenentwürfe. Insofern sollte man hier nicht mit irgendwelchen falschen Behauptungen den Eindruck erzeugen, auf Bundesebene geschehe nichts. Zumal wir dort mit dem Bundesamt für Sicherheit in der Informationstechnik eine sehr gut aufgestellte Behörde haben.

Das Gleiche gilt natürlich auch für das Landesamt für Sicherheit in der Informationstechnik hier in Bayern. Es ist notwendig, dass wir diese Behörde haben. Ich halte es

auch für dringend notwendig, dass wir jetzt die mit der europäischen Richtlinie kommenden Veränderungen umsetzen. Es ist auf jeden Fall richtig und wichtig, dass wir zum Beispiel auch den Zeitraum für die Protokollierung verändern, damit man auf einer Firewall und einem Serversystem nachschauen kann, wann der Angriff erfolgt ist, welche Techniken dabei genutzt worden sind usw. Es geht dabei um Angriffe aus China, es geht um Angriffe aus Russland. Dabei wundert es mich nicht, dass die AfD-Fraktion Probleme damit hat, dass wir hier gegen Cyberkriminalität klare Kante zeigen, da es um ihre Freunde aus Russland und China geht.

Es geht auch um global agierende Kriminelle. Allein an dem, was der Bitkom in seiner Studie im letzten Jahr festgestellt hat, sieht man, um welche Dimensionen es geht: Nur in einem Jahr 206 Milliarden Euro Schäden für Unternehmen durch IT-Diebstahl, durch Spionage und Sabotage. Nicht mitgezählt wurden dabei die Angriffe auf Krankenhäuser, auf Schulen und Kommunen usw.

Es wäre gut, im Zusammenhang mit der Beratung dieses Gesetzes auch darüber zu reden, wie wir unsere Kommunen in Bayern noch besser unterstützen können, wie wir Krankenhausverbünde noch besser unterstützen können, wie wir andere öffentliche Einrichtungen oder Wohlfahrtsverbände beim Thema IT-Sicherheit noch besser unterstützen können.

Herr Kollege Adjei hat schon das Krankenhaus Agathariedangesprochen: Es gab in den letzten zwei Jahren eine ganze Reihe von Vorfällen, zum Beispiel der Angriff auf das Medienzentrum München im Oktober 2022. Davon waren 55 Schulen im Landkreis München betroffen sowie 20 Grund- und Hauptschulen im Landkreis Berchtesgaden. Wahrscheinlich sind die Daten nicht in fremde Hände gelangt.

Im November 2023 wurden im Landkreis Neu-Ulm mehrere Kommunen von Hackern lahmgelegt. Davon waren Bürgerbüros betroffen, sodass Passanträge nicht bearbeitet werden konnten. Die Friedhofsverwaltungen hatten plötzlich keinen Zugriff mehr auf Programme, weil durch Ransomware die Daten verschlüsselt waren. In diesem Januar

– und nun reden wir über gravierende Vorfälle – flossen bei der Bezirksklinik Mittelfranken Personaldaten, Patientendaten, unternehmensinterne Dokumente plötzlich ab. Die Kliniken im Verbund waren aufgrund dieses Angriffes nur noch telefonisch erreichbar. Im Klinikum am Europakanal in Erlangen konnte gar nicht mehr telefoniert werden. Im Mai 2024 sind bei der IT-Infrastruktur der Katholischen Jugendfürsorge Augsburg offenbar massenhaft sensible Daten in die Hände von Kriminellen oder ausländischen Diensten gelangt: Patientendaten, Personaldaten, Finanzdaten.

Das dürfen wir nicht länger zulassen, und deswegen ist es wichtig und richtig, dass wir alles unternehmen, um die IT-Sicherheit in Bayern zu gewährleisten und um Cyberkriminellen das Handwerk zu legen. Wir werden uns deshalb als SPD auch intensiv an den Beratungen beteiligen. – Vielen Dank für Ihre Aufmerksamkeit.

(Beifall bei der SPD)

Erster Vizepräsident Tobias Reiß: Herr von Brunn, bleiben Sie bitte am Rednerpult. Es liegt eine Meldung zu einer Zwischenbemerkung des Herrn Kollegen Andreas Jurca vor.

Andreas Jurca (AfD): Werter Kollege von Brunn!

Florian von Brunn (SPD): Ich bin nicht Ihr Kollege. Ich bitte darum, den Begriff zu vermeiden.

(Beifall bei der SPD – Widerspruch bei der AfD)

Andreas Jurca (AfD): Wir sitzen zusammen hier im Landtag, soweit ich weiß. – Sie werden hier nicht müde, uns wegen unserer Freundschaften zu China und Russland zu kritisieren. Wenn ich mich recht erinnere, war der Bundeskanzler Scholz von der SPD im April für zwei Tage in China. Haben Sie ihn auch schon kritisiert, oder wie stehen Sie dazu? Distanzieren Sie sich von Ihrem Bundeskanzler?

Florian von Brunn (SPD): Wissen Sie, was der Unterschied zwischen Sozialdemokraten, zwischen dem Bundeskanzler Olaf Scholz und Leuten wie Ihnen ist? – Von uns fährt niemand nach Russland, um dort zu bestätigen, dass Putin demokratische Wahlen durchgeführt hat.

(Widerspruch und Lachen bei der AfD)

Das zeigt doch schon, in welchem geistigen Zustand Sie sich befinden. Mehr muss man dazu nicht mehr sagen.

(Beifall bei der SPD)

Erster Vizepräsident Tobias Reiß: Vielen Dank. – Damit ist die Aussprache geschlossen, und ich schlage vor, den Gesetzentwurf dem Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung als federführendem Ausschuss zu überweisen. Erhebt sich Widerspruch? – Das ist nicht der Fall. Dann ist das so beschlossen.

Bayerischer Landtag

19. Wahlperiode 11.07.2024 **Drucksache** 19/**2966**

Beschlussempfehlung und Bericht

des Ausschusses für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung

Gesetzentwurf der Staatsregierung zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung
Drs. 19/**2591**

I. Beschlussempfehlung:

Zustimmung

Berichterstatter: **Dr. Stefan Ebner**
Mitberichterstatterin: **Christiane Feichtmeier**

II. Bericht:

1. Der Gesetzentwurf wurde dem Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung federführend zugewiesen.
   Der Ausschuss für Verfassung, Recht, Parlamentsfragen und Integration hat den Gesetzentwurf endberaten.
2. Der federführende Ausschuss hat den Gesetzentwurf in seiner 13. Sitzung am 11. Juli 2024 beraten und mit folgendem Stimmergebnis:
   CSU: Zustimmung
   FREIE WÄHLER: Zustimmung
   AfD: Enthaltung
   B90/GRÜ: Zustimmung
   SPD: Zustimmung
   Zustimmung empfohlen.
3. Der Ausschuss für Verfassung, Recht, Parlamentsfragen und Integration hat den Gesetzentwurf in seiner 12. Sitzung am 11. Juli 2024 endberaten und mit folgendem Stimmergebnis:
   CSU: Zustimmung
   FREIE WÄHLER: Zustimmung
   AfD: Ablehnung
   B90/GRÜ: Zustimmung
   SPD: Enthaltung
   Zustimmung empfohlen mit der Maßgabe, dass folgende Änderungen durchgeführt werden:

   1. Im Einleitungssatz von § 1 sind die Wörter „das durch Art. 57b des Gesetzes vom 22. Juli 2022 (GVBl. S. 374) geändert worden ist“ durch die Wörter „das zuletzt durch Art. 10 des Gesetzes vom 21. Juni 2024 (GVBl. S. 114) geändert worden ist“ zu ersetzen.

   2. „§ 1 Nr. 2 Buchst. a wird wie folgt geändert:“
      a) In Doppelbuchst. aa wird der Punkt am Ende durch die Wörter ‚und das Wort „und“ am Ende wird durch ein Komma ersetzt.‘ ersetzt.

b) In Doppelbuchst. cc wird in der neu angefügten Nr. 9 das Komma am Ende durch das Wort „und“ ersetzt.

3. Als Datum des Inkrafttretens ist in den Platzhalter von § 3 der „18. Oktober 2024“ einzusetzen.

Stephanie Schuhknecht
Vorsitzende

Bayerischer Landtag

19. Wahlperiode 26.09.2024 **Drucksache** 19/**3420**

Beschluss

des Bayerischen Landtags

Der Landtag hat in seiner heutigen öffentlichen Sitzung beraten und beschlossen:

Gesetzentwurf der Staatsregierung
Drs. 19/**2591**, 19/**2966**

Gesetz zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung[1]

§ 1
Änderung des Bayerischen Digitalgesetzes

Das Bayerische Digitalgesetz (BayDiG) vom 22. Juli 2022 (GVBl. S. 374, BayRS 206-1-D), das zuletzt durch Art. 10 des Gesetzes vom 21. Juni 2024 (GVBl. S. 114) 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 und das Wort „und" am Ende wird durch ein Komma ersetzt.

      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,

         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 und

[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).

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 Mitgliedstaaten 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, Ermittlung, 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 bearbeitet 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

Änderung des Gesetzes über die Bayerische Landesstiftung

Das Gesetz über die Bayerische Landesstiftung (BayLStG) in der in der Bayerischen Rechtssammlung (BayRS 282-2-10-F) veröffentlichten bereinigten Fassung, das zuletzt durch § 1 Abs. 54 der Verordnung vom 4. Juni 2024 (GVBl. S. 98) geändert worden ist, wird wie folgt geändert:

1. Art. 8 Abs. 8 wird wie folgt geändert:
   a) Satz 2 wird aufgehoben.
   b) Satz 3 wird Satz 2.
2. In Art. 10 Abs. 3 Halbsatz 1 werden die Wörter „innerhalb von sechs Monaten“ gestrichen.

§ 3

Inkrafttreten

Dieses Gesetz tritt am 18. Oktober 2024 in Kraft.

Die Präsidentin

I.V.

Ludwig Hartmann

IV. Vizepräsident

Redner zu nachfolgendem Tagesordnungspunkt

Fünfter Vizepräsident Markus Rinderspacher
Abg. Dr. Stefan Ebner
Abg. Florian Köhler
Abg. Tobias Beck
Abg. Benjamin Adjei
Abg. Florian von Brunn
Abg. Prof. Dr. Ingo Hahn
Staatssekretär Martin Schöffel

Fünfter Vizepräsident Markus Rinderspacher: Ich rufe den **Tagesordnungspunkt 7** auf:

Gesetzentwurf der Staatsregierung
zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung (Drs. 19/2591)
- Zweite Lesung -

Die Gesamtredezeit der Fraktionen beträgt 29 Minuten. Die Redezeit der Staatsregierung orientiert sich dabei an der Redezeit der stärksten Fraktion. Ich eröffne die Aussprache. Erster Redner ist der Kollege Dr. Stefan Ebner von der CSU-Fraktion. – Herr Dr. Ebner, bitte sehr.

Dr. Stefan Ebner (CSU): Herr Präsident, meine verehrten Kolleginnen und Kollegen, sehr geehrte Damen und Herren! Bayern ist das Land der Sicherheit. Bayern ist dank unseres Innenministers Joachim Herrmann das Land der inneren Sicherheit; Bayern ist aber auch das Land der Cybersicherheit. Sie ist dank unseres Finanz- und Heimatministers Albert Füracker das zentrale Feld bei der modernen Gefahrenabwehr.

Wir kennen die aktuelle Bedrohungslage. Die geopolitischen Entwicklungen, der Angriffskrieg Russlands auf die Ukraine, verschärfen die dynamische Bedrohungslage; aber auch unser Staat, unsere Wirtschaft, unsere Gesellschaft stehen vor großen Herausforderungen. Neben all diesen physischen Angriffen erleben wir mittlerweile eine ganz starke, intensive Cyberkriminalität und Cyberspionage. Zusätzlich hat sich eine neue Dimension des Hacktivismus entwickelt, also des Angriffs auf Behördennetze, auf Webseiten mit einer ideologischen, einer politischen Zielsetzung.

Meine Damen und Herren, im nächsten Jahr finden die Bundestagswahlen statt. Da müssen wir uns auf allerlei Schmutzeleien einstellen, vor allem aus Russland, aus China, von all denen, die die Feinde unserer freiheitlichen Gesellschaft, unseres Way of Life, unseres Wohlstands sind. Denen werden wir uns entgegenstellen. Bayern ist gerüstet, bereit und vorbereitet, meine Damen und Herren. Wir haben beste Organisa-

tionseinheiten für den Kampf gegen diese Bedrohungen. Wir sind bei der Polizei, beim Verfassungsschutz, bei der Justiz, bei den Datenschutzaufsichtsbehörden und, ganz entscheidend, beim Landesamt für Sicherheit in der Informationstechnik, kurz LSI, bestens aufgestellt.

Dieses Amt gibt es seit 2017. Das ist die erste Landesbehörde dieser Art bei der Cybergefahrenabwehr. Sie arbeitet intensiv und erfolgreich mit Bund und Ländern zusammen. Sie beschäftigt mittlerweile 150 Mitarbeiterinnen und Mitarbeiter, alles hervorragende IT-Experten, und bald werden es 200 sein. Das LSI schützt staatliche Behörden vor Cyberangriffen und unterstützt als Berater die Kommunen und Betreiber kritischer Infrastruktur. Man kann sagen: Auf dem Cyberschlachtfeld ist das LSI die Cyberarmee des Freistaats, meine Damen und Herren.

Im Übrigen gibt es viel zu tun. Das LSI analysiert im Sicherheitsmonitoring täglich 2,5 Milliarden Datensätze. Täglich werden 1,5 Millionen E-Mails mit Schadcodes gefiltert. Das LSI hat auch 94 % unserer bayerischen Kommunen bei der Abwehr von Cyberkriminalität unterstützt. Das ist wichtig; denn Bayern steht unter Dauerbeschuss. Im Jahr 2022 hat das LSI über 4.000 Angriffsversuche auf das bayerische Behördennetz registriert. 1.500 davon wären sehr schwerwiegend gewesen. Kein einziger dieser Angriffsversuche, null, zero, ist durchgekommen. Das LSI hat alles abgewehrt.

Worum geht es heute? – Das Europäische Parlament und der Europäische Rat haben Ende 2022 eine neue Richtlinie verabschiedet, die NIS-2-Richtlinie. Sie enthält Maßnahmen, die das Gesamtniveau der Cybersicherheit in der EU heben sollen. Sie gilt für private und für öffentliche Einrichtungen gleichermaßen. Sie betrifft also Unternehmen und Behörden. Betroffen sind vor allem Unternehmen der kritischen Infrastruktur. Sie sollen mit vorausschauenden Risikoanalysen und strengen Berichtspflichten einen größeren Beitrag zur Cybersicherheit in unserem Land leisten.

Diese NIS-2-Richtlinie folgt einer NIS-Richtlinie aus dem Jahr 2016. Damals herrschte noch eine andere Situation. Seinerzeit wurden in Deutschland 2.000 Unternehmen als

kritische Infrastruktur klassifiziert. Heute fallen 30.000 Unternehmen unter diese neue Regelung, weil die Gesamtsituation komplexer geworden ist. Heute werden Registrierungs-, Nachweis- und Meldepflichten eingeführt, um die Cybersicherheit zu gewährleisten. Die EU-Mitgliedstaaten sind bis zum 17. Oktober dieses Jahres verpflichtet, diese Maßnahmen umzusetzen. Vorrangig muss der Bund diese Richtlinie umsetzen.

Soweit die Richtlinie Behörden des Landes betrifft, müssen die Länder – also auch wir in Bayern – tätig werden und diese Richtlinie in Landesrecht umsetzen. Das bedeutet, genau wie jedes andere Bundesland müssen wir eine eigene Gesetzgebung vorlegen. Das Erfreuliche ist: Das LSI muss dafür in Bayern nicht bei null anfangen. In Bayern ist alles vorhanden. Dank dieser Vorarbeit genügt es in Bayern, das bestehende Digitalgesetz einfach zu ändern. Wir passen die bereits bestehenden Vorschriften zur IT-Sicherheit an. Bereits jetzt besteht eine hohe Übereinstimmung. Der Gesetzentwurf, der jetzt vorliegt, befasst sich besonders mit der Umsetzung für unsere bayerische Verwaltung.

Ein weiterer wichtiger Inhalt dieses Gesetzes ist die Verlängerung der Speicherfrist von Protokolldaten, die das LSI erhebt, von 12 auf 18 Monate. Das ist deswegen sinnvoll, weil dadurch nachträgliche Angriffe auf das Behördennetz besser erkannt werden können. Zudem wird dadurch eine Angleichung auf Bundesebene erreicht.

Wir machen uns, unabhängig von der Zeitschiene der Ampel, auf den Weg und setzen die NIS-2-Richtlinie in Landesrecht um. Die Ampel wird dagegen die vorgegebene Zeitschiene nicht erreichen. Das Bundesinnenministerium rechnet mit einem Inkrafttreten im Frühjahr 2025.

Bei der Umsetzung dieses Gesetzes stellt sich natürlich die Frage, wie es mit der Bürokratie aussieht. Im Sinne der Philosophie dieser Landesregierung sagen wir: keine zusätzliche Bürokratie. Deswegen setzen wir dieses Gesetz eins zu eins um. Wir wollen keine Bürokratie, keine zusätzliche Gängelung und keinen zusätzlichen Aufwand. Was tut die Ampel? – In den Fachmedien ist zu diesem Thema zu lesen, dass sich

andere Länder sehr eng am Text orientieren, nicht aber die Ampel. Dort gibt es eine zusätzliche und aufwendige Ausregulierung.

Apropos Ampel: Vor einer Woche hat der Bundesrechnungshof in seinem Bericht dargelegt, wie die Ampel bei der Umsetzung dieser NIS-2-Richtlinie vorankommt. In diesem Bericht, der an die Vorsitzenden des Haushaltsausschusses und des Innenausschusses des Deutschen Bundestags weitergegeben wurde, heißt es: Die Rechnungsprüfer sehen die Sicherheit in Deutschland gefährdet. – Laut dem Bundesrechnungshof läuft die Regierung sogar Gefahr, ihr Ziel, die Informations- und Cybersicherheit zu verbessern, zu verfehlen. Auch der Entwurf der Bundesinnenministerin Nancy Faeser bleibt nach Meinung des Bundesrechnungshofs in zentralen Punkten hinter den selbstgesteckten Zielen zurück. Ich zitiere:

> "Wichtige Regelungen sollen nicht für die gesamte Bundesverwaltung in einheitlicher Weise verbindlich sein. Die Folge wäre ein ‚Flickenteppich', der die Informations- und Cybersicherheit aller Beteiligten gefährden kann."

Der Rechnungshof zeigt zahlreiche weitere Kritikpunkte auf. Meine Redezeit ist begrenzt, deshalb belasse ich es dabei. Das Scheitern ist auf den 44 Seiten des Berichtes dokumentiert. Liebe Ampel-Vertreter, ich muss schon sagen: Nicht einmal das kriegen Sie hin. Sie scheitern bei der Migration, Sie scheitern bei der Wirtschaft, Sie scheitern beim Bürgergeld, Sie scheitern bei der inneren Sicherheit, und Sie scheitern im Haushalt. Als Ampel scheitern Sie sogar daran, eine EU-Richtlinie in ein Bundesgesetz umzusetzen. Das ist ein Zeichen dafür: Sie können es nicht.

(Beifall bei der CSU)

Deswegen ist es gut, dass Berlin von Bayern sehr weit weg ist. Gut, dass wir einen Finanzminister und einen Finanzstaatssekretär haben, die sich um die digitale Sicherheit in Bayern mit Weitsicht kümmern.

Nach der Ersten Lesung wurde dieses Gesetz in den Ausschüssen beraten. Der federführende Wirtschaftsausschuss hat bei Stimmenthaltung der AfD empfohlen, dem Gesetzentwurf zuzustimmen. Der endberatende Verfassungsausschuss hat mit den Stimmen der CSU, der FREIEN WÄHLER und der GRÜNEN gegen die Stimmen der AfD bei Stimmenthaltung der SPD dem Gesetzentwurf zugestimmt. Die kommunalen Spitzenverbände wurden ebenfalls angehört und haben innerhalb der Anhörungsfrist keine Stellungnahme abgegeben. Insofern können wir alle diesem Gesetz zustimmen. – Herzlichen Dank für Ihre Aufmerksamkeit.

(Beifall bei der CSU und den FREIEN WÄHLERN)

Fünfter Vizepräsident Markus Rinderspacher: Vielen Dank, Herr Dr. Ebner. – Der nächste Redner ist Herr Abgeordneter Köhler für die AfD-Fraktion.

(Beifall bei der AfD)

Florian Köhler (AfD): Sehr geehrter Herr Vizepräsident, sehr geehrte Kollegen, sehr geehrte Damen und Herren! Wir sind heute in der Zweiten Lesung zum Digitalgesetz. Die vorliegenden Änderungsanträge zum Bayerischen Digitalgesetz enthalten im Wesentlichen redaktionelle Änderungen, die für Rechtsklarheit sorgen sollen. Diese Änderungen kann man beschließen, aber man müsste das nicht tun. Ein Punkt, den ich bereits in der Ersten Lesung und dann im Ausschuss angesprochen habe, wird aber leider nicht angefasst, nämlich das dreistufige Meldeverfahren. Einerseits will die Staatsregierung Bürokratie abschaffen, aber auf der anderen Seite führt sie neue Meldeverfahren mit Berichtspflichten ein. Genau das führt zu mehr Verwaltungsaufwand, ohne dass klare Mehrwerte entstehen.Auch bei diesem Gesetz gilt: Wir machen diesen Spuk nur mit, weil uns Brüssel mit einer EU-Richtlinie knebelt und wir dazu verpflichtet sind. Meistens tritt eben genau das ein, was man aus Brüssel gewohnt ist: Man produziert viel Papier und verwaltet sich selbst, ohne viel Mehrwert.

(Zuruf von den GRÜNEN)

Darauf, was auf unsere Unternehmen zukommt, möchte ich eigentlich gar nicht eingehen, aber ich muss es trotzdem, weil der Bund da zuständig ist, was Bürger und Unternehmen angeht. Aber Sie sind eher mit sich selbst beschäftigt. Das ist aber vielleicht auch nicht ganz verkehrt. Dann kommt die Ampel wenigstens nicht auf noch dümmere Ideen, als sie eh schon tagtäglich hat.

Herr Ebner, das stimmt nicht so ganz. Nicht nur die Ampel zerfleddert EU-Richtlinien, die in ihrem Wesen manchmal gar nicht so schlecht sind. Das muss ich in aller Ehrlichkeit sagen. Auch unter CSU-Beteiligung an Bundesregierungen haben es zum Beispiel im Verkehrssektor tatsächlich bessere Richtlinien nicht so in die Umsetzung geschafft, sondern die Bundesregierung hat alles zerfleddert und zerstückelt. Am Ende haben wir jetzt den Salat. Sie lesen ja sicherlich Zeitung. VW macht zu, und andere machen zu wegen der ganzen Grenzwerte. Aber das nur am Rande.

Die noch nicht verabschiedeten Rahmenbedingungen auf Bundesebene, die eben angesprochen worden sind, könnten also zu weiteren notwendigen Anpassungen führen. Wir werden uns hier enthalten. Wir sehen aber, dass die Regierung dieses heiße Eisen mit dem Meldeverfahren nicht anfassen will.

(Beifall bei der AfD)

Fünfter Vizepräsident Markus Rinderspacher: Nächster Redner ist der Kollege Tobias Beck für die FREIEN WÄHLER

Tobias Beck (FREIE WÄHLER): Sehr geehrter Herr Vizepräsident, werte Kolleginnen und Kollegen, liebe Besucher auf der Besuchertribüne! Auch in der Zweiten Lesung zu diesem Gesetz möchte ich von Anfang an betonen, dass es um die Sicherheit von Informationstechnik und kritischer Infrastruktur geht. Deshalb kann und darf es keine Diskussion darüber geben, ob eine Unterstützung erfolgen muss oder nicht, sondern es geht weiterhin lediglich um das Wie.

Die weltweite Entwicklung der Bedrohungslage macht die Notwendigkeit einer engeren Zusammenarbeit zwischen dem Bundesamt für Sicherheit in der Informationstechnik – BSI – und dem Landesamt für Sicherheit in der Informationstechnik – LSI – umso dringlicher. Wir sind mit immer raffinierteren und gezielteren Angriffen auf unsere digitalen Systeme konfrontiert. Cyberangriffe, die hochspezialisiert sind, haben das Potenzial, immense Schäden anzurichten und die ganze Gesellschaft vorübergehend lahmzulegen. Ob es sich dabei um Regierungsbehörden, Unternehmen oder sogar Privatpersonen handelt – niemand ist vor den Auswirkungen solcher Angriffe sicher. Wir sehen uns einer unsichtbaren Bedrohung gegenüber, die nicht nur schwer zu erkennen, sondern oftmals auch schwierig zu bekämpfen ist. Deshalb muss jetzt gehandelt werden.

Die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit – NIS-2 – muss bis 17. Oktober 2024 in nationales Recht umgesetzt werden. Dabei geht es um definierte Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der EU und um den Ausbau nationaler Kapazitäten für die Cybersicherheit. Ebenso geht es um die Meldepflicht für kritische Infrastruktur. Durch die NIS 2 sollen die Befugnisse des BSI weiter gestärkt werden und die Zusammenarbeit beim Thema IT-Sicherheit in Kooperation zwischen Staat und Wirtschaft ausgebaut werden.

Das Gesetz müsste eigentlich am 17. Oktober 2024, wie ich zuvor schon erwähnt habe, in nationales Recht umgesetzt werden. Aktuell ist es aber nicht absehbar, dass die Bundesregierung die von der EU gesetzten Umsetzungsfristen einhalten wird und einhalten kann. Vonseiten des Bundes wird sogar um Verständnis gebeten, dass keine Auskunft erteilt werden kann. Der Kollege Ebner hat das Frühjahr 2025 genannt.

Ich möchte hier aber kein Ampel-Bashing betreiben, sondern nur sagen, dass die Opposition in Bayern immer fordert, sich auf bayerische Themen zu konzentrieren. Wir haben wieder mal gezeigt, dass genau das bei uns funktioniert. Wie selbstverständlich werden wir unsere Aufgaben termingerecht erledigen.

(Beifall bei den FREIEN WÄHLERN)

Das Bayerische Digitalgesetz ist nicht nur ein Gesetzestext, sondern auch ein Schlüssel zur digitalen Transformation. Es soll Innovation fördern, Bürokratie abbauen und den Menschen die Chancen und Herausforderungen der digitalen Welt näherbringen. Unser Bayerisches Staatsministerium für Digitales ist deshalb auch federführend an den Ausarbeitungen beteiligt gewesen.

Ein weiterer Punkt im Gesetzentwurf betrifft das Gesetz über die Bayerische Landesstiftung. Hier möchten wir der Digitalisierung mit den getroffenen Maßnahmen mehr Anschub verleihen. Dieses Thema liegt klar beim Finanz- und Heimatminister Albert Füracker, der das Gesetz in Erster Lesung vorgestellt hat.

Wie Herr Adjei zuvor erwähnt hat: Der Digitalminister ist nicht da. Aber das liegt daran, dass es bei uns kein großes Hickhack um Zuständigkeiten gibt wie anderswo. Darauf möchte ich ausdrücklich hinweisen. Die Bayerische Staatsregierung ist auf allen Ebenen handlungsfähig.

(Beifall bei den FREIEN WÄHLERN sowie Abgeordneten der CSU)

Wir haben die Möglichkeit, Bayern zu einem Vorreiter in Sachen Digitalisierung zu machen und unseren Bürgerinnen und Bürgern eine moderne und zukunftsorientierte und vor allen Dingen sichere Infrastruktur zu bieten. Wir dürfen dabei nicht vergessen, dass mit der Digitalisierung auch Verantwortung und ethische Fragen einhergehen. Datenschutz, IT-Sicherheit und der Schutz der Privatsphäre müssen auch in der digitalen Welt gewahrt bleiben.

Uns liegt daran, dass die Chancen der Digitalisierung genutzt und gleichzeitig die Risiken minimiert werden. Wir wollen als Freistaat Bayern die Unternehmen mit den Problemen, die sie in den betroffenen Bereichen wie der Energieversorgung, dem Gesundheitswesen, Verkehr und Transporten sowie den digitalen Infrastrukturen haben,

nicht alleine lassen. Wir müssen doch ein großes Interesse daran haben, unsere kritische Infrastruktur und Unternehmen vor Cyberangriffen zu schützen.

Insgesamt wird die NIS-2-Richtlinie in Bayern sowohl von staatlicher Seite als auch von privaten Akteuren als Anstoß gesehen, die Cyberresilienz zu verbessern und sicherzustellen, dass die bayerische Wirtschaft und Verwaltung vor wachsenden Bedrohungen im digitalen Raum bestmöglich geschützt wird. Deshalb bitten wir auch hier um Zustimmung. Der Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung hat dem Gesetz bereits mehrheitlich zugestimmt. Ich bitte Sie, auch hier zuzustimmen.

(Beifall bei den FREIEN WÄHLERN und der CSU)

Fünfter Vizepräsident Markus Rinderspacher: Vielen Dank, Herr Kollege Beck. – Nächster Redner ist Herr Kollege Benjamin Adjei für BÜNDNIS 90/DIE GRÜNEN.

Benjamin Adjei (GRÜNE): Herr Präsident, liebe Kolleginnen und Kollegen! Ich habe gerade, als ich hergekommen bin, dem Digitalminister die Klinke in die Hand gegeben. Er geht, ich komme. Da merkt man, dass das Thema Digitalisierung hier im Plenum wieder auf der Tagesordnung steht, weil auch dieses Mal nicht das Digitalministerium, sondern das Finanzministerium federführend zuständig ist.

Egal, wie bei Ihnen in der Koalition das Kompetenzwirrwarr fortschreitet – gleichzeitig schreitet auch die Digitalisierung im Freistaat massiv voran. In der Wirtschaft, der Gesellschaft und der Verwaltung geschieht einiges. Wir werden immer digitaler, unabhängig davon, ob wir uns proaktiv dafür einsetzen oder ob man wie manche weiterhin versucht, das zu verhindern. Die Digitalisierung lässt sich nicht verhindern, sondern wir müssen sie jetzt begleiten und die notwendigen Rahmenbedingungen aufbauen, um insbesondere unseren Staat resilient zu gestalten und den Herausforderungen, die die Digitalisierung mit sich bringt, entsprechend zu begegnen. Da geht es um den Schutz von Bürgerinnen und Bürgern, um den Schutz unserer Unternehmen und natürlich den Schutz unserer Demokratie und unseres Staates.

Das ist gerade schon ausgeführt worden: Die Angriffe auf Unternehmen, aber auch auf Kommunen, auf die Verwaltung, nehmen massiv zu. Die Zunahme basiert dabei nicht vor allem auf inländischen, sondern vor allem auf ausländischen Akteuren, vor allem China und Russland. Das ist schon erwähnt worden. Mich wundert übrigens nicht, dass die AfD da kein Interesse daran hat. Als Putin-Unterstützer wollen Sie natürlich, dass die russischen Angriffe auf Deutschland stärker werden.

(Martin Huber (AfD): So ein Schmarrn! Jetzt hör auf! Was soll das?)

Umso wichtiger ist es, dass wir in Europa genau hier das Thema Cyber Security vorantreiben und uns um eine europäische einheitliche, harmonisierte Lösung kümmern.Und da ist die NIS-2-Richtlinie der EU genau der richtige Weg, um gleiche Rahmenbedingungen zu setzen, einen hohen Schutzstandard zu fordern und dann natürlich die entsprechende Infrastruktur zu schaffen und auszubauen. Bayern setzt jetzt das um, was umzusetzen ist. Leider nicht mehr. Es wäre noch mehr möglich. Man kann schon zusammenfassend sagen, dass Bayern relativ weit ist. Das ist gerade schon gesagt worden, und ich bin jemand, der das lobt, was gut läuft, und ja, in Bayern läuft es gut, beispielsweise mit dem LSI. Es ist, wie erwähnt, das erste Landesamt seiner Art in Deutschland und treibt mit dem Bayern-CERT sehr erfolgreich die Stärkung der IT-Sicherheit in Bayern voran.

Vorgestern haben wir im Cyber-Sicherheitsbericht des Innenministers erfahren, dass diese Einrichtung gut funktioniert und dass sie das bayerische Behördennetz und die bayerischen Behörden sehr gut schützt. Es ist entsprechend richtig, das LSI fortzuführen und auszubauen. Wo aber Sonne ist, ist auch Schatten. Auf das bayerische Behördennetz sind im letzten Jahr 5.200 Angriffe ausgeführt worden. Diese waren alle erfolglos. Es war eine gute Arbeit des LSI. Das Problem ist, dass das Behördennetz nicht alle Behörden und nicht alle Kommunen umfasst. Insbesondere die bayerischen Kommunen sind das Ziel starker Angriffe. Wir haben im letzten Jahr deutschlandweit 27 Kommunen gehabt, auf die erfolgreiche Angriffe ausgeführt worden sind. Sechs Millionen Bürgerinnen und Bürger sind davon betroffen gewesen. Das muss man sich

wirklich einmal überlegen: Das ist jetzt nur der Anfang, das wird noch massiv vorangehen. Umso schlimmer ist es, dass Sie ausgerechnet den Handlungsspielraum, den Sie bei der Umsetzung hatten, nicht ausnutzen, und sagen, Sie wollen die Kommunen eben nicht in diese strukturellen Umbauten einbeziehen. Sie wollen keinen verpflichtenden Schutz für die Kommunen sicherstellen. Das ist fahrlässig; denn die Kommunen sind am Ende das Rückgrat unserer Staatsverwaltung.

Wir merken das immer wieder: Ich komme aus dem Landkreis Miesbach. Das Krankenhaus Agatharied, das vor wenigen Monaten wochenlang offline war und nicht richtig arbeiten konnte, musste analog arbeiten, weil es Opfer eines Cyberangriffs wurde. Das wird in Zukunft zunehmen. Umso wichtiger ist es, die Kommunen bei dieser wichtigen Herausforderung zu unterstützen. Entsprechend wünsche ich mir, oder ich hoffe, dass Sie das nachbessern und bei zukünftigen Änderungen die Kommunen mit in das IT-Sicherheitssystem des Freistaats Bayern einbauen. Ansonsten werden wir in Zukunft bei den Kommunen riesige Probleme bei der IT-Sicherheit haben.

(Beifall bei den GRÜNEN)

Fünfter Vizepräsident Markus Rinderspacher: Vielen Dank, Herr Kollege Adjei. – Nächster Redner ist Herr Kollege Florian von Brunn für die SPD-Fraktion.

Florian von Brunn (SPD): Sehr geehrte Damen und Herren, es ist richtig und wichtig, dass Bayern die NIS-2-Richtlinie umsetzt. Wir haben im letzten Jahr ungefähr 200 bis 300 Milliarden Euro an Schäden durch Cyberangriffe und Hackerangriffe gehabt. Für die öffentliche Hand wurden die Schäden auch auf mehrere Milliarden Euro geschätzt. Deswegen ist es so wichtig, dass man in Europa auf Bundes-, aber auch auf Länderebene einheitlich dafür sorgt, dass es Regelungen gibt, dass man solche Angriffe auch protokolliert, dass man aufklärt, woher sie kommen, zum Beispiel aus Russland – von dort kommt auch im Übrigen Desinformation –, und dass man dagegen etwas unternimmt, also die öffentliche Verwaltung stärkt und schützt.

Deswegen werden wir dem Gesetzentwurf zustimmen, wobei wir kritisch anmerken, dass man die Kommunen, die Städte und Gemeinden in Bayern, die für 80 % der Verwaltungsdienstleistungen zuständig sind, stärker unterstützen muss. Wir haben es in vielen Fällen in Bayern schon erlebt, egal ob es im Regierungsbezirk Schwaben, in Oberbayern oder Mittelfranken war, dass Krankenhäuser, Schulen und die öffentliche Verwaltung von solchen Hackerangriffen und einem Verlust von Daten betroffen waren. Es sind Daten von Bürgerinnen und Bürgern, von Patientinnen und Patienten an irgendwelche Kriminelle abgeflossen. Dazu kommt natürlich auch, dass es zum Teil nicht mehr möglich war, wichtige Verwaltungsdienstleistungen zu erbringen. Die Verwaltung hat nicht mehr funktioniert, zum Beispiel die Friedhofsverwaltung oder die Beantragung von Reisepässen. All das muss man verhindern.

Vielleicht darf ich an dieser Stelle noch etwas sagen, weil Herr Ebner soeben sehr breitbeinig aufgetreten ist. Es gibt schon Defizite im kommunalen Bereich in Bayern. Wenn Sie mit den Bürgermeisterinnen und Bürgermeistern reden, dann sagen diese: Wir haben immer mehr Aufgaben, auch in der IT-Sicherheit, aber wir bekommen dafür nicht die entsprechenden Mittel. Wir haben auch große Probleme, Fachkräfte zu finden. Das, was das LSI, das Landesamt für Sicherheit in der Informationstechnik, selbst auf seiner Webseite schreibt, ist, dass zwar die Kreisverwaltungsbehörden, zum Beispiel die Landratsämter, sich an das bayerische Behördennetz anschließen lassen und Subnetze bilden können, nämlich kommunale Behördennetze. Daran können sich die eigenen Gemeinden beteiligen, was bei Weitem aber nicht alle Städte und Gemeinden machen. Das heißt: Wir haben Städte und Gemeinden, die durch dieses bayerische Behördennetz nicht geschützt sind. Da stellt sich mir die Frage: Was tut man dafür, dass diese auch unter den Schutzschirm kommen?

Es gibt also noch einige Aufgaben, die wir anpacken sollten. Nichtsdestoweniger stimmen wir zu. Wir halten es für den richtigen Weg. Der Check, ob wir bei der IT-Sicherheit in Bayern wirklich gut aufgestellt sind, findet in der Praxis statt. Wir werden in den nächsten Monaten beobachten, wie es in Bayern weitergeht: ob Kommunen, ob Kran-

kenhäuser, ob Schulen Opfer von Cyberattacken werden, oder ob es erfolgreich verhindert werden kann. Das ist der Lackmustest für den Erfolg Ihrer Sicherheitspolitik in diesem Bereich.

(Beifall bei der SPD)

Fünfter Vizepräsident Markus Rinderspacher: Es gibt eine Zwischenbemerkung von Herrn Abgeordneten Prof. Hahn von der AfD-Fraktion.

(Beifall bei der AfD)

Prof. Dr. Ingo Hahn (AfD): Geschätzter Herr von Brunn von der SPD, Sie haben sich gerade beschwert, dass der Kollege Ebner hier sehr breitbeinig auftritt. Das machen Sie jetzt vielleicht nicht mehr.

(Heiterkeit bei der AfD)

In der Vergangenheit war es ja so, dass Sie für Ihre Äußerungen, nicht nur gegenüber der AfD, Ordnungsrufe erhalten haben. Meine Frage ist jetzt, ob Sie die Ehre dieses Hohen Hauses noch wertschätzen. Sie treten hier ans Podium, begrüßen die Damen und Herren, aber nicht den Vizepräsidenten. Ist das der neue Stil von Ihnen, oder ist Ihnen das Hohe Haus nicht mehr wertvoll genug?

Florian von Brunn (SPD): Also Herr Hahn, Ihre Frage hat überhaupt nichts mit der Sache zu tun. Trotzdem möchte ich Sie beantworten. Ich habe den Herrn Rinderspacher heute schon persönlich begrüßt, und ich glaube, die einzige Fraktion, die hier nicht über Anstand und Stil in diesem Haus reden muss, das ist die AfD, die sich wirklich in diesem Landtag schon so aufgeführt hat, dass man als normaler Parlamentarier nur noch verwundert die Schultern zucken kann. Wenn man gerade sieht, was im Landtag in Thüringen geschieht, mit Nazi-Sprüchen, mit der Blockade der Parlamentsarbeit durch Ihre AfD-Genossen dort, dann muss ich ganz ehrlich sagen: Sie sind eine Schande für unsere Demokratie und nichts anderes.

(Beifall bei der SPD und den FREIEN WÄHLERN)

Fünfter Vizepräsident Markus Rinderspacher: Für die Staatsregierung hat Herr Staatssekretär Martin Schöffel das Wort.

Staatssekretär Martin Schöffel (Finanzen und Heimat): Sehr geehrter Herr Vizepräsident,

(Heiterkeit bei der AfD)

liebe Kolleginnen und Kollegen! Ich kann nur an das anschließen, was der Kollege Stefan Ebner schon ausgeführt hat. Bayern ist das Land der Sicherheit. Datensicherheit wird großgeschrieben, und das Finanzministerium ist übrigens auch das Ministerium für IT-Sicherheit.

Ich danke für das ganze Lob, welches das LSI erhalten hat. Uns ist das wirklich wichtig, denn umgekehrt sind wir als bayerische Finanzverwaltung auch verantwortlich für das deutschlandweit erfolgreichste E-Government-Programm. Das ist unser ELSTER, das wir im Konsensverbund in Bayern programmieren und allen anderen Bundesländern zur Verfügung stellen. Wir haben in diesem Bereich bereits rund 22 Millionen Nutzer in Deutschland. Diese haben im vergangenen Jahr über ihre Nutzeradressen über 60 Millionen Steuererklärungen eingereicht. Das ist uns auch sehr wichtig, dass wir für den Steuerpflichtigen mit ELSTER ein einfacheres Angebot machen.

Da wird auch noch viel kommen an einfacherer Programmierung. Umgekehrt entlasten wir auch unsere Mitarbeiter in den Finanzämtern. Es ist ein Riesenunterschied, ob die Daten online vorliegen und der Finanzbeamte selbst entscheiden kann, welche Belege er einsehen und anklicken will, oder ob alles Mögliche in Papierform ankommt.Deswegen ist IT-Sicherheit für uns sehr wichtig, weil wir die Nutzung entsprechend ausweiten wollen.

Über das heutige Thema, die NIS-2-Richtlinie der Europäischen Union, die das gemeinsame Cybersicherheitsniveau in der EU entsprechend heben soll, ist bereits viel

gesprochen worden. Sie betrifft überwiegend Unternehmen, rund 30.000 Unternehmen der kritischen Infrastruktur, und muss vorrangig vom Bund umgesetzt werden. Das wurde bereits gesagt. Ich möchte noch einmal betonen: Der Gesetzentwurf der Staatsregierung ergänzt das, was in der Hoheit des Landesgesetzgebers liegt. Wir setzen die Richtlinie eins zu eins um. Wir weiten die Regelung auf wichtige Behörden aus, die von der neuen Richtlinie betroffen und angesprochen sind. Es findet kein Gold-Plating statt. Wir machen keine erhebliche Bürokratie aus der ganzen Geschichte, aber es geht natürlich immer auch darum, zu sensibilisieren und zur Vorsicht aufzurufen; denn IT-Sicherheit ist wie gesagt ein sehr, sehr wichtiges Thema.

Bayern nimmt das ernst. Wir haben in Bayern unsere Hausaufgaben ohnehin erledigt. Das wurde bereits angesprochen. Mit dem LSI haben wir eine Einheit gegründet, die deutschlandweit einmalig ist. Am 01.12.2017 hat der damalige Finanzminister Markus Söder das LSI weitblickend, kann man sagen, auf den Weg gebracht; denn die Problematik hat ja noch einmal deutlich zugenommen. Vorhin sind schon Zahlen genannt worden, was heute auch an Spam in unseren Netzen ankommt. Täglich müssen über 2 Milliarden Datensätze analysiert werden. Wir erhalten im Jahr – auch eine interessante Zahl – 470 Millionen E-Mails im öffentlichen Netz. Davon werden 340 Millionen E-Mails maschinell sofort geblockt und können die Sicherheitssperre nicht durchdringen. Dies zeigt, wie vorsichtig ein solches Netz ist. Vorhin wurde schon angesprochen, dass über 3.000 Cyberangriffe, die irgendwo im Netz angekommen sind, verhindert wurden, sodass kein Schaden entstanden ist, und dass wir, egal von welcher Seite die Angriffe erfolgen, zum Glück auch entsprechenden Schaden im staatlichen Netz verhindern konnten.

Die Ausweitung des LSI ist ein wichtiger Punkt. Derzeit arbeiten dort 150 Spezialistinnen und Spezialisten. Das Ziel ist 200. Jetzt geht es also um die IT-Sicherheit im gesamten Staatsapparat, auch in den Kommunen. Natürlich sind nach dem Digitalgesetz auch die Kommunen bereits jetzt umfasst und zur IT-Sicherheit verpflichtet. Dies ist der Inhalt des Gesetzes. Am Ende geht es aber vor allem darum, sie bei der Datensi-

cherheit zu unterstützen. Dafür steht das LSI zur Verfügung. Auch die bayerischen Kommunen arbeiten mehr und mehr digital. Die IT-Sicherheit muss dort mehr in den Fokus rücken. Durch die neue Richtlinie erhält das Thema noch einmal mehr Aufmerksamkeit.

Bayern unterstützt die Kommunen beim Thema IT-Sicherheit, und es war von Anfang an auch Bestandteil der LSI-Idee, die Kommunen bei diesem Thema zu unterstützen, und zwar kostenlos. Wir verleihen beispielsweise das Siegel "Kommunale IT-Sicherheit", wenn eine entsprechende Zusammenarbeit stattgefunden hat, und führen individuelle Beratung zu allen Fragen rund um die IT-Sicherheit durch. Es werden Arbeitshilfen und Schulungsveranstaltungen angeboten. Auch gibt es einen Warn- und Informationsdienst, der sich insbesondere an die Kommunen richtet, und natürlich unterstützt das LSI die Kommunen vor allem im Angriffsfall durch versierte Experten. Für alle ist es sehr interessant, jederzeit einmal das Einsatz- und Lagezentrum im LSI in Nürnberg zu besichtigen. Es ist sehr spannend, wie dort dann live nachvollzogen werden kann, wo möglicherweise Schadsoftware eingedrungen ist oder Probleme bestehen und wie dort dann auch schnell zugegriffen und geholfen werden kann.

Mit der Zukunftskommission "#Digitales Bayern 5.0", die ja von unserem Finanzminister Albert Füracker geführt wird, wird gerade an einer zukunftsfähigen Ausrichtung der kommunalen Digitalisierung gearbeitet. Dabei ist auch die IT-Sicherheit von zentraler Bedeutung. Unser Ziel ist es, die bayerischen Kommunen bestmöglich auf Cybervorfälle vorzubereiten und ihnen zur Seite zu stehen. Insbesondere geht es dabei um kommunale Unternehmen wie Krankenhäuser, Wasserversorgungen und vieles andere mehr. Trotzdem haben wir hier eine schlanke und bürokratiearme Regelung gewählt, die auch in der Gesetzgebungskompetenz des Bayerischen Landtags liegt und sehr gut zu unserem Credo passt. Ich danke dem Landtag für die zügige Beratung. Da in den Ausschüssen eine zügige Beratung stattfand, kann unsere Gesetzesänderung jetzt auch schnell in Kraft treten, damit wir bei diesem Thema gut vorankommen.

Die Entscheidung, das LSI zu gründen, war zukunftsweisend. Mit der fristgerechten Umsetzung der NIS-2-Richtlinie wird der Freistaat Bayern seiner Vorreiterrolle in Fragen der IT-Sicherheit erneut gerecht. Ich darf Sie auch um die Zustimmung zu diesem Gesetzentwurf bitten. Wir stellen dadurch Konformität mit dem Europarecht sicher. Wir eröffnen damit auch noch ein paar andere zukunftsfähige Möglichkeiten wie zum Beispiel Sitzungen per Videokonferenz bei der Bayerischen Landesstiftung und Ähnliches mehr und schaffen überflüssige Sonderregelungen in diesem Bereich ab. Bayern wird auch zukünftig das Thema IT-Sicherheit mit aller Kraft verfolgen und die besten Experten zusammenziehen, um das staatliche Netz, aber auch die Netze von Kommunen und kritischer Infrastruktur weiterhin zu schützen. Ich denke, auch der Bund und andere Länder können sich daran ein Beispiel nehmen. Wir sehen das auch an vielen Informationsbesuchen im LSI. Klar ist auch, wir müssen hier immer auf der Höhe der Zeit bleiben; denn wir müssen immer etwas besser und schneller sein als die, die uns angreifen wollen.

In diesem Sinne bitte ich um Zustimmung.

(Beifall bei der CSU und den FREIEN WÄHLERN)

Fünfter Vizepräsident Markus Rinderspacher: Vielen Dank, Herr Staatssekretär Schöffel. – Weitere Wortmeldungen liegen mir nicht vor. Die Aussprache ist geschlossen. Wir kommen zur Abstimmung. Der Abstimmung zugrunde liegen der Gesetzentwurf der Staatsregierung auf Drucksache 19/2591 und die Beschlussempfehlung mit Bericht des federführenden Ausschusses für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung auf Drucksache 19/2966. Der federführende Ausschuss empfiehlt Zustimmung zum Gesetzentwurf. Der endberatende Ausschuss für Verfassung, Recht, Parlamentsfragen und Integration empfiehlt Zustimmung mit der Maßgabe, dass mehrere Änderungen vorgenommen werden. Im Einzelnen verweise ich hierzu auf Drucksache 19/2966.

Wer dem Gesetzentwurf mit den empfohlenen Änderungen zustimmen will, den bitte ich um das Handzeichen. – CSU, FREIE WÄHLER, BÜNDNIS 90/DIE GRÜNEN und SPD. Gegenstimmen! – Keine Gegenstimmen. Stimmenthaltungen! – Bei Stimmenthaltung der AfD-Fraktion. Damit ist das Gesetz so beschlossen.

Da ein Antrag auf Dritte Lesung nicht gestellt wurde, führen wir gemäß § 56 der Geschäftsordnung sofort die Schlussabstimmung durch. Ich schlage vor, sie in einfacher Form durchzuführen. – Widerspruch erhebt sich nicht.

Wer dem Gesetzentwurf in der soeben beschlossenen Fassung seine Zustimmung geben will, den bitte ich, sich vom Platz zu erheben. – CSU, FREIE WÄHLER, BÜNDNIS 90/DIE GRÜNEN und SPD. Danke sehr. Gegenstimmen bitte ich auf die gleiche Weise anzuzeigen! – Keine Gegenstimmen. Stimmenthaltungen! – Damit ist das Gesetz bei Stimmenthaltung der AfD angenommen. Es hat den Titel: "Gesetz zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung".

Ich gebe nun die Ergebnisse der vorher durchgeführten Wahlen eines Vizepräsidenten des Bayerischen Landtags sowie einer Schriftführerin bekannt und komme zunächst zur Wahl eines Vizepräsidenten – Tagesordnungspunkt 5: Gewählt ist, wer mehr als die Hälfte der abgegebenen gültigen Stimmen erhält. Bei der Ermittlung der erforderlichen Mehrheit werden Enthaltungen nicht berücksichtigt. An der Wahl haben 158 Abgeordnete teilgenommen. Es gab keine ungültigen Stimmen. Auf Herrn Abgeordneten Markus Walbrunn entfielen 26 Ja-Stimmen und 131 Nein-Stimmen. Es gab 1 Enthaltung. Damit hat Herr Abgeordneter Markus Walbrunn nicht die erforderliche Mehrheit der Stimmen erreicht.Nun gebe ich das Ergebnis der vorher durchgeführten Wahl einer Schriftführerin des Bayerischen Landtags, Tagesordnungspunkt 6, bekannt. Auch hier ist gewählt, wer mehr als die Hälfte der abgegebenen gültigen Stimmen erhält. Bei der Ermittlung der erforderlichen Mehrheit werden Enthaltungen nicht berücksichtigt. An der Wahl haben 157 Abgeordnete teilgenommen. Es gab keine ungültigen Stimmen. Auf Frau Abgeordnete Roon entfielen 25 Ja-Stimmen und 130 Nein-Stim-

men. Der Stimme enthalten haben sich 2 Abgeordnete. Damit hat Frau Abgeordnete Roon nicht die erforderliche Mehrheit der Stimmen erreicht.

B 1612
473

Bayerisches Gesetz- und Verordnungsblatt

Nr. 19 **München, den 15. Oktober** **2024**

Datum	Inhalt	Seite
8.10.2024	**Gesetz zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung** 206-1-D, 282-2-10-F	474
13.9.2024	Verordnung zur Änderung der Verordnung über die Bayerische Landesanstalt für Landwirtschaft und der Verordnung zur Ausführung des Bayerischen Fischereigesetzes 7801-9-L, 793-3-L	479
23.9.2024	Verordnung zur Änderung des Bayerischen Beamtengesetzes 2030-1-1-F	484
24.9.2024	Verordnung zur Änderung der StMB Zuständigkeitsverordnung Beamtenrecht 2030-3-2-1-I/B	485
27.9.2024	Verordnung zur Änderung der Bayerischen Digitalverordnung 206-1-1-D	486

206-1-D, 282-2-10-F

Gesetz zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung[1]

vom 8. Oktober 2024

Der Landtag des Freistaates Bayern hat das folgende Gesetz beschlossen, das hiermit bekannt gemacht wird:

§ 1

Änderung des Bayerischen Digitalgesetzes

Das Bayerische Digitalgesetz (BayDiG) vom 22. Juli 2022 (GVBl. S. 374, BayRS 206-1-D), das zuletzt durch Art. 10 des Gesetzes vom 21. Juni 2024 (GVBl. S. 114) 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 und das Wort „und“ am Ende wird durch ein Komma ersetzt.

      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,

      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 und

      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 Mitgliedstaaten 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

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).

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, Ermittlung, 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 bearbeitet 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

Änderung des Gesetzes über die Bayerische Landesstiftung

Das Gesetz über die Bayerische Landesstiftung (BayLStG) in der in der Bayerischen Rechtssammlung (BayRS 282-2-10-F) veröffentlichten bereinigten Fassung, das zuletzt durch § 1 Abs. 54 der Verordnung vom 4. Juni 2024 (GVBl. S. 98) geändert worden ist, wird wie folgt geändert:

1. Art. 8 Abs. 8 wird wie folgt geändert:

   a) Satz 2 wird aufgehoben.

   b) Satz 3 wird Satz 2.

2. In Art. 10 Abs. 3 Halbsatz 1 werden die Wörter „innerhalb von sechs Monaten“ gestrichen.

§ 3

Inkrafttreten

Dieses Gesetz tritt am 18. Oktober 2024 in Kraft.

München, den 8. Oktober 2024

Der Bayerische Ministerpräsident

Dr. Markus S ö d e r

7801-9-L, 793-3-L

Verordnung zur Änderung der Verordnung über die Bayerische Landesanstalt für Landwirtschaft und der Verordnung zur Ausführung des Bayerischen Fischereigesetzes

vom 13. September 2024

Auf Grund

– des § 2 Abs. 3 Satz 1 des Öko-Landbaugesetzes (ÖLG) vom 7. Dezember 2008 (BGBl. I S. 2358), das zuletzt durch Art. 1 des Gesetzes vom 17. August 2023 (BGBl. 2023 I Nr. 219) geändert worden ist, in Verbindung mit § 6 Nr. 11 der Delegationsverordnung (DelV) vom 28. Januar 2014 (GVBl. S. 22, BayRS 103-2-V), die zuletzt durch § 1 der Verordnung vom 25. Juni 2024 (GVBl. S. 208) und durch § 2 der Verordnung vom 2. Juli 2024 (GVBl. S. 210) geändert worden ist, und

– des Art. 53 Abs. 1 Satz 1 des Bayerischen Fischereigesetzes (BayFiG) in der Fassung der Bekanntmachung vom 10. Oktober 2008 (GVBl. S. 840, 2009 S. 6, BayRS 793-1-L), das zuletzt durch § 1 Abs. 94 der Verordnung vom 4. Juni 2024 (GVBl. S. 98) geändert worden ist,

verordnet das Bayerische Staatsministerium für Ernährung, Landwirtschaft, Forsten und Tourismus:

§ 1

Änderung der Verordnung über die Bayerische Landesanstalt für Landwirtschaft

Die Verordnung über die Bayerische Landesanstalt für Landwirtschaft (LfLV) vom 12. November 2002 (GVBl. S. 652, BayRS 7801-9-L), die zuletzt durch § 1 Abs. 60 der Verordnung vom 4. Juni 2024 (GVBl. S. 98) geändert worden ist, wird wie folgt geändert:

1. § 4 wird wie folgt geändert:

   a) Abs. 1 wird wie folgt gefasst:

      „(1) Privaten Kontrollstellen mit einer Zulassung für Bayern nach § 2 Abs. 2 Nr. 1 des Öko-Landbaugesetzes – ÖLG – (Kontrollstellen) überträgt die Landesanstalt auf Antrag die Aufgaben nach § 3 Abs. 1 Satz 1 ÖLG und beleiht sie mit der Aufgabe nach § 3 Abs. 1 Satz 2 Nr. 4 ÖLG.“

   b) Abs. 2 wird wie folgt geändert:

      aa) Satz 1 wird wie folgt gefasst:

      „[1]Die Aufgabenübertragung nach Abs. 1 umfasst alle dort genannten Bereiche und erfolgt widerruflich durch schriftlichen Bescheid.“

      bb) Satz 2 wird wie folgt geändert:

         aaa) In Halbsatz 1 wird das Semikolon am Ende durch einen Punkt ersetzt.

         bbb) Halbsatz 2 wird Satz 3 und die Wörter „die Erfüllung“ werden durch die Wörter „[3]Die Erfüllung“ ersetzt.

      cc) Der bisherige Satz 3 wird aufgehoben.

   c) In Abs. 3 wird das Wort „beliehenen“ gestrichen.

2. In der Überschrift des § 6 wird das Wort „In-Kraft-Treten“ durch das Wort „Inkrafttreten“ ersetzt.

§ 2

Änderung der Verordnung zur Ausführung des Bayerischen Fischereigesetzes

Die Anlage der Verordnung zur Ausführung des Bayerischen Fischereigesetzes (AVBayFiG) in der Fassung der Bekanntmachung vom 10. Mai 2004 (GVBl. S. 177, 270, BayRS 793-3-L), die zuletzt durch § 1 Abs. 95 der Verordnung vom 4. Juni 2024 (GVBl. S. 98) geändert worden ist, erhält die aus dem Anhang zu dieser Verordnung ersichtliche Fassung.

§ 3

Inkrafttreten

Diese Verordnung tritt am 1. Januar 2025 in Kraft.

München, den 13. September 2024

**Bayerisches Staatsministerium
für Ernährung, Landwirtschaft, Forsten
und Tourismus**

Michaela K a n i b e r , Staatsministerin

Anhang
(zu § 2)

Anlage
(zu den §§ 11, 14, 22, 27 und 32)

Schonzeiten, Schonmaße und räumlicher Geltungsbereich

Nr.	**Art**	**Schonzeit**	**Schonmaß** (in cm)	**Gültig in den sich aus der Karte über die Flussgebietseinheiten gemäß Anlage 2 zu § 7 Abs. 1 Satz 3 Wasserhaushaltsgesetz ergebenden Grenzen** von Donau (D), Elbe (E), Rhein (R), Weser (W)
1.	**Neunaugen**			
1.1	Bachneunauge, Lampetra planeri	ganzjährig	–	D/E/R/W
1.2	Donau-Neunauge, Eudontomyzon vladykovi	ganzjährig	–	D
1.3	Flussneunauge, Lampetra fluviatilis	ganzjährig	–	E/R/W
1.4	Meerneunauge, Petromyzon marinus	ganzjährig	–	E/R/W
2.	**Fische**			
	Ganzjährig geschonte Fische			
2.1	Ammersee-Kaulbarsch, Gymnocephalus ambriaelacus	ganzjährig	–	D
2.2	Ammersee-Kilch, Coregonus bavaricus	ganzjährig	–	D
2.3	Atlantischer Lachs, Salmo salar	ganzjährig	–	E/R/W
2.4	Atlantischer Stör, Acipenser sturio	ganzjährig	–	D/E/R/W
2.5	Balkan-Goldsteinbeißer, Sabanejewia balcanica	ganzjährig	–	D
2.6	Bitterling, Rhodeus amarus	ganzjährig	–	D/E/R/W
2.7	Bodensee-Kilch, Coregonus gutturosus	ganzjährig	–	R
2.8	Donau-Kaulbarsch, Gymnocephalus baloni	ganzjährig	–	D
2.9	Donau-Steinbeißer, Cobitis elongatoides	ganzjährig	–	D
2.10	Donau-Stromgründling, Romanogobio vladykovi	ganzjährig	–	D
2.11	Europäischer Schlammpeitzger, Misgurnus fossilis	ganzjährig	–	D/E/R/W
2.12	Frauennerfling, Rutilus virgo	ganzjährig	–	D
2.13	Karausche, Carassius carassius	ganzjährig	–	D/E/R/W
2.14	Maifisch, Alosa alosa	ganzjährig	–	E/R/W
2.15	Meerforelle, Salmo trutta forma trutta	ganzjährig	–	E/R/W
2.16	Neunstachliger Stichling, Pungitius pungitius	ganzjährig	–	E/R/W
2.17	Nordseeschnäpel, Coregonus oxyrinchus	ganzjährig	–	E/R/W
2.18	Perlfisch, Rutilus meidingeri	ganzjährig	–	D

Nr.	Art	Schonzeit	Schonmaß (in cm)	Gültig in den sich aus der Karte über die Flussgebietseinheiten gemäß Anlage 2 zu § 7 Abs. 1 Satz 3 Wasserhaushaltsgesetz ergebenden Grenzen von Donau (D), Elbe (E), Rhein (R), Weser (W)
2.19	Schneider, Alburnoides bipunctatus	ganzjährig	–	D/E/R/W
2.20	Schrätzer, Gymnocephalus schraetser	ganzjährig	–	D
2.21	Steinbeißer, Cobitis taenia	ganzjährig	–	D/E/R/W
2.22	Steingressling, Romanogobio uranoscopus	ganzjährig	–	D
2.23	Sterlet, Acipenser ruthenus	ganzjährig	–	D
2.24	Streber, Zingel streber	ganzjährig	–	D
2.25	Strömer, Telestes souffia	ganzjährig	–	D/R
2.26	Ziege, Pelecus cultratus	ganzjährig	–	D
2.27	Zingel, Zingel zingel	ganzjährig	–	D
2.28	Zobel, Ballerus sapa	ganzjährig	–	D
2.29	Zope, Ballerus ballerus	ganzjährig	–	D
	Fische mit Schonbestimmungen			
2.30	Aal, Anguilla anguilla	1. Oktober bis 31. Dezember	50	E/R/W
2.31	Äsche, Thymallus thymallus	1. Januar bis 30. April	35	D/E/R/W
2.32	Bachforelle, Salmo trutta forma fario	1. Oktober bis 15. März	26	D/E/R/W
2.33	Barbe, Barbus barbus	1. Mai bis 30. Juni	40	D/E/R/W
2.34	Elritze, Phoxinus phoxinus	1. Mai bis 30. Juni	–	D/E/R/W
2.35	Hasel, Leuciscus leuciscus	1. März bis 30. April	–	D/E/R/W
2.36	Hecht, Esox lucius	15. Februar bis 30. April	50	D/E/R/W
2.37	Huchen, Hucho hucho	15. Februar bis 30. Juni	90	D
2.38	Karpfen, Cyprinus carpio	–	35	D/E/R/W
2.39	Koppe, Cottus gobio	1. Februar bis 30. April	–	D/E/R/W
2.40	Mairenke, Alburnus mento	1. Mai bis 30. Juni	–	D
2.41	Nase, Chondrostoma nasus	1. März bis 30. April	30	D/E/R/W
2.42	Nerfling, Leuciscus idus	1. März bis 30. April	30	D/E/R/W
2.43	Regenbogenforelle, Oncorhynchus mykiss	15. Dezember bis 15. März	26	D/E/R/W
2.44	Renken/Felchen, Coregonus spp.	15. Oktober bis 31. Dezember	30	D/E/R/W
2.45	Rutte/Quappe/Trüsche, Lota lota	–	40	D/E/R/W
2.46	Schied/Rapfen, Leuciscus aspius	1. März bis 30. April	40	D/R
2.47	Schleie, Tinca tinca	1. Mai bis 30. Juni	26	D/E/R/W
2.48	Seeforelle, Salmo trutta forma lacustris	1. Oktober bis 15. März	60	D/R

Nr.	**Art**	**Schonzeit**	**Schonmaß** (in cm)	**Gültig in den sich aus der Karte über die Flussgebietseinheiten gemäß Anlage 2 zu § 7 Abs. 1 Satz 3 Wasserhaushaltsgesetz ergebenden Grenzen** von Donau (D), Elbe (E), Rhein (R), Weser (W)
2.49	Seesaiblinge, Salvelinus spp.	1. Oktober bis 31. Dezember	30	D
2.50	Zander, Sander lucioperca	15. Februar bis 30. April	50	D/E/R/W
	Fische ohne Schonbestimmungen			
2.51	Aitel/Döbel, Squalius cephalus	–	–	D/E/R/W
2.52	Bachsaibling, Salvelinus fontinalis	–	–	D/E/R/W
2.53	Bachschmerle, Barbatula barbatula	–	–	D/E/R/W
2.54	Brachse, Abramis brama	–	–	D/E/R/W
2.55	Dreistachliger Stichling, Gasterosteus aculeatus	–	–	E/R/W
2.56	Flussbarsch, Perca fluviatilis	–	–	D/E/R/W
2.57	Giebel, Carassius gibelio	–	–	D/E/R/W
2.58	Gründling, Gobio gobio	–	–	D/E/R/W
2.59	Güster, Blicca bjoerkna	–	–	D/E/R/W
2.60	Kaulbarsch, Gymnocephalus cernua	–	–	D/E/R/W
2.61	Laube, Alburnus alburnus	–	–	D/E/R/W
2.62	Moderlieschen, Leucaspius delineatus	–	–	E/R/W
2.63	Rotauge, Rutilus rutilus	–	–	D/E/R/W
2.64	Rotfeder, Scardinius erythrophthalmus	–	–	D/E/R/W
2.65	Wels, Silurus glanis	–	–	D
2.66	Zährte/Seerüssling, Vimba vimba	–	–	D/E/R/W
3.	**Krebse**			
3.1	Edelkrebs, Astacus astacus, männlich	–	12	D/E/R/W
	Edelkrebs, Astacus astacus, weiblich	1. Oktober bis 31. Juli	12	D/E/R/W
3.2	Steinkrebs, Austropotamobius torrentium	ganzjährig	–	D/E/R/W
4.	**Muscheln**			
4.1	Abgeplattete Teichmuschel, Pseudanodonta complanata	ganzjährig	–	D/E/R/W
4.2	Flussperlmuschel, Margaritifera margaritifera	ganzjährig	–	D/E/R/W
4.3	Gemeine Teichmuschel, Anodonta anatina	ganzjährig	–	D/E/R/W
4.4	Große Flussmuschel, Unio tumidus	ganzjährig	–	D/E/R/W
4.5	Große Teichmuschel, Anodonta cygnea	ganzjährig	–	D/E/R/W
4.6	Kleine Flussmuschel/Bachmuschel, Unio crassus	ganzjährig	–	D/E/R/W
4.7	Malermuschel, Unio pictorum	ganzjährig	–	D/E/R/W

2030-1-1-F

Verordnung zur Änderung des Bayerischen Beamtengesetzes

vom 23. September 2024

Auf Grund des Art. 96 Abs. 1 Satz 2 des Bayerischen Beamtengesetzes (BayBG) vom 29. Juli 2008 (GVBl. S. 500, BayRS 2030-1-1-F), das zuletzt durch Verordnung vom 4. Oktober 2023 (GVBl. S. 595) geändert worden ist, verordnet das Bayerische Staatsministerium der Finanzen und für Heimat:

§ 1

In Art. 96 Abs. 1 Satz 1 des Bayerischen Beamtengesetzes (BayBG) vom 29. Juli 2008 (GVBl. S. 500, BayRS 2030-1-1-F), das zuletzt durch Verordnung vom 4. Oktober 2023 (GVBl. S. 595) geändert worden ist, wird die Angabe „20 878 €“ durch die Angabe „21 832 €“ersetzt.

§ 2

Diese Verordnung tritt am 1. Januar 2025 in Kraft.

München, den 23. September 2024

Bayerisches Staatsministerium der Finanzen und für Heimat

Albert F ü r a c k e r , Staatsminister

2030-3-2-1-I/B

Verordnung zur Änderung der StMB Zuständigkeitsverordnung Beamtenrecht

vom 24. September 2024

Auf Grund des Art. 60a Abs. 5 und des Art. 68 Abs. 2 Satz 1 des Bayerischen Besoldungsgesetzes (BayBesG) vom 5. August 2010 (GVBl. S. 410, 764, BayRS 2032-1-1-F), das zuletzt durch § 1 Abs. 17 der Verordnung vom 4. Juni 2024 (GVBl. S. 98), Art. 12 des Gesetzes vom 21. Juni 2024 (GVBl. S. 114) sowie durch die §§ 1, 2, 3, 4 und 5 des Gesetzes vom 8. Juli 2024 (GVBl. S. 170) geändert worden ist, in Verbindung mit Art. 102 Satz 3 des Bayerischen Besoldungsgesetzes (BayBesG) vom 5. August 2010 (GVBl. S. 410, 764, BayRS 2032-1-1-F), das zuletzt durch § 1 Abs. 17 der Verordnung vom 4. Juni 2024 (GVBl. S. 98), Art. 12 des Gesetzes vom 21. Juni 2024 (GVBl. S. 114) sowie durch die §§ 1, 2, 3, 4 und 5 des Gesetzes vom 8. Juli 2024 (GVBl. S. 170) geändert worden ist, verordnet das Bayerische Staatsministerium für Wohnen, Bau und Verkehr im Einvernehmen mit dem Bayerischen Staatsministerium der Finanzen und für Heimat:

§ 1

§ 7 der StMB Zuständigkeitsverordnung Beamtenrecht (ZustV-BM) vom 24. Juli 2019 (GVBl. S. 544, BayRS 2030-3-2-1-I/B), die durch § 1 der Verordnung vom 30. November 2020 (GVBl. S. 705) geändert worden ist, wird wie folgt geändert:

1. Der Überschrift werden die Wörter „und Zuschläge zur Gewinnung von IT-Fachkräften“ angefügt.

2. Dem Wortlaut wird folgender Abs. 1 vorangestellt:

   „(1) [1]Die Entscheidung über die Gewährung von IT-Fachkräftegewinnungszuschlägen gemäß Art. 60a BayBesG wird den Leitungen der in § 1 genannten Behörden für die bei ihnen beschäftigten Beamten und Beamtinnen übertragen. [2]Bei abgeordneten Beamten und Beamtinnen entscheidet die Beschäftigungsdienststelle.“

3. Der bisherige Wortlaut wird Abs. 2.

§ 2

Diese Verordnung tritt am 1. November 2024 in Kraft.

München, den 24. September 2024

Bayerisches Staatsministerium für Wohnen, Bau und Verkehr

Christian B e r n r e i t e r , Staatsminister

206-1-1-D

Verordnung zur Änderung der Bayerischen Digitalverordnung

vom 27. September 2024

Es verordnet auf Grund

– des Art. 57 Abs. 4a Nr. 1 Buchst. a bis d des Bayerischen Digitalgesetzes (BayDiG) vom 22. Juli 2022 (GVBl. S. 374, BayRS 206-1-D), das zuletzt durch Art. 10 des Gesetzes vom 21. Juni 2024 (GVBl. S. 114) geändert worden ist,

das Bayerische Staatsministerium für Digitales im Einvernehmen mit den Bayerischen Staatsministerien des Innern, für Sport und Integration und der Finanzen und für Heimat sowie im Einvernehmen mit dem Bayerischen Bezirketag, dem Bayerischen Landkreistag, dem Bayerischen Städtetag und dem Bayerischen Gemeindetag und

– des Art. 57 Abs. 4a Nr. 2 des Bayerischen Digitalgesetzes (BayDiG) vom 22. Juli 2022 (GVBl. S. 374, BayRS 206-1-D), das zuletzt durch Art. 10 des Gesetzes vom 21. Juni 2024 (GVBl. S. 114) geändert worden ist,

das Bayerische Staatsministerium für Digitales im Einvernehmen mit den Bayerischen Staatsministerien des Innern, für Sport und Integration und der Finanzen und für Heimat:

§ 1

Änderung der Bayerischen Digitalverordnung

Die Bayerische Digitalverordnung (BayDiV) vom 11. Juli 2023 (GVBl. S. 464, BayRS 206-1-1-D) wird wie folgt geändert:

1. Nach § 7 wird folgender Teil 3a eingefügt:

‚Teil 3a

Gemeinsam finanzierte Dienste

§ 7a

Gemeinsam finanzierte Dienste

[1]Die nach Maßgabe von Art. 55a BayDiG gemeinsam finanzierten Dienste bestimmen sich nach der Anlage zu dieser Verordnung. [2]Soweit ein gemeinsam finanzierter Dienst abgrenzbare Verwaltungsleistungen enthält, die allein dem Freistaat Bayern zuzuordnen sind, trägt dieser die auf diese abgrenzbaren Verwaltungsleistungen entfallenden Kosten vollständig und eine gemeinsame Finanzierung erfolgt insoweit nicht. [3]Die Auswahl der gemeinsam finanzierten Dienste wird jährlich gemeinsam durch den Freistaat Bayern und die kommunalen Spitzenverbände evaluiert und bei Bedarf angepasst.

§ 7b

Berechnung und Erhebung des kommunalen Finanzierungsanteils

(1) Der kommunale Finanzierungsanteil im Sinne des Art. 55a Abs. 2 Satz 2 BayDiG berechnet sich durch Abzug des Anteils des Freistaates Bayern gemäß Art. 55a Abs. 2 Satz 1 Nr. 1 BayDiG von der Summe der Kosten der gemeinsam finanzierten Dienste.

(2) [1]Der kommunale Finanzierungsanteil teilt sich auf in die Kostenanteile der Ebenen der Bezirke, der Landkreise und der Gemeinden (Kostenanteile der kommunalen Ebenen). [2]Der Kostenanteil jeder kommunalen Ebene entspricht dem Anteil der Kosten der dieser Ebene gemäß Spalte 3 „Kommunale Ebene; ggf. Aufteilungsregel“ der Anlage zugeordneten Dienste an den Gesamtkosten der gemeinsam finanzierten Dienste. [3]In der Anlage können gemeinsam finanzierte Dienste auch anteilig mehreren kommunalen Ebenen zugewiesen werden, soweit sie von mehreren kommunalen Ebenen genutzt werden. [4]Es gilt:

1. jeder Bezirk trägt am Kostenanteil der Ebene der Bezirke einen Anteil in Höhe des Anteils seiner Einwohnerzahl an der Einwohnerzahl Bayerns,

2. jeder Landkreis trägt am Kostenanteil der Ebene der Landkreise einen Anteil in Höhe des Anteils seiner Einwohnerzahl an der Einwohnerzahl

Bayerns,

3. jede kreisfreie Stadt trägt an den Kostenanteilen der Ebene der Landkreise und der Ebene der Gemeinden einen Anteil in Höhe des Anteils ihrer Einwohnerzahl an der Einwohnerzahl Bayerns,

4. jede kreisangehörige Gemeinde trägt am Kostenanteil der Ebene der Gemeinden einen Anteil in Höhe des Anteils ihrer Einwohnerzahl an der Einwohnerzahl Bayerns.

[5]Die maßgeblichen Einwohnerzahlen entsprechen der nach § 1 Abs. 1 Satz 1 und 3 sowie Abs. 5 Satz 1 und 2 der Bayerischen Durchführungsverordnung Finanzausgleichsgesetz ermittelten Einwohnerzahl.

(3) [1]Die nach Abs. 2 bestimmten Einzelbeiträge der Gemeindeverbände und Gemeinden werden jährlich vom Landesamt für Statistik berechnet, auf volle Euro aufgerundet und sind bis zum 31. Oktober des jeweiligen Beitragsjahres festzusetzen. [2]Das Staatsministerium teilt dem Landesamt für Statistik die hierfür erforderlichen Daten jährlich bis spätestens 10. Oktober mit. [3]Eine Festsetzung unterbleibt, soweit für eine kommunale Ebene keine Dienste gemeinsam finanziert werden. [4]Für Gemeinden, die Mitglied einer Verwaltungsgemeinschaft sind, erfolgt die Festsetzung gegenüber der Verwaltungsgemeinschaft. [5]Die Beiträge werden mit der Auszahlung der Zuweisungen nach den Art. 7 und 15 des Bayerischen Finanzausgleichsgesetzes für das vierte Vierteljahr fällig und mit diesen verrechnet.

(4) [1]Die Veränderung der Kosten gemeinsam finanzierter Dienste zwischen dem Zeitpunkt der Festsetzung der Einzelbeträge und ihrer Verrechnung wirkt sich nicht auf die Verrechnung nach Abs. 3 aus. [2]Die resultierenden zu viel gezahlten Beiträge werden in der nächsten Abrechnungsperiode auf den kommunalen Finanzierungsanteil angerechnet. [3]Bei Erhöhung der Kosten gemeinsam finanzierter Dienste nach Festsetzung der Einzelbeträge erhöht sich der kommunale Finanzierungsanteil der nächsten Abrechnungsperiode um den ausstehenden Betrag.‘

2. Die aus dem Anhang zu dieser Verordnung ersichtliche Anlage wird angefügt.

§ 2

Weitere Änderung der Bayerischen Digitalverordnung

§ 7b Abs. 3 der Bayerischen Digitalverordnung (BayDiV) vom 11. Juli 2023 (GVBl. S. 464, BayRS 206-1-1-D), die zuletzt durch § 1 dieser Verordnung geändert worden ist, wird wie folgt geändert:

1. In Satz 1 wird die Angabe „31. Oktober“ durch die Angabe „30. April“ ersetzt.

2. In Satz 2 wird das Wort „Oktober“ durch das Wort „April“ ersetzt.

3. In Satz 5 wird das Wort „vierte“ durch das Wort „zweite“ ersetzt.

§ 3

Inkrafttreten

[1]Diese Verordnung tritt am 16. Oktober 2024 in Kraft. [2]Abweichend von Satz 1 tritt § 2 am 1. Januar 2025 in Kraft.

München, den 27.September 2024

Bayerisches Staatsministerium für Digitales

Dr. Fabian M e h r i n g , Staatsminister

Anhang
(zu § 1 Nr. 2)

Anlage
(zu den §§ 7a und 7b)

Gemeinsam finanzierte Dienste

Nr.	**Name des Dienstes / Dienstbündels** *(Beschreibung)*	**Kommunale Ebene;** **ggf. Aufteilungsregel**
1.	**EfA-Dienste**	
1.1.1	Geodigitalisierungskomponente *(In andere Dienste integrierbare Komponente, welche anhand einer graphischen Oberfläche und auf Basis amtlicher Geodaten die Erstellung von Lageskizzen ermöglicht)*	Alle Ebenen; zu gleichen Teilen
1.1.2	Breitband-Portal[1] *(Digitale und medienbruchfreie Beantragung und Bearbeitung von Verwaltungsleistungen im Rahmen der Verlegung und Änderung von Telekommunikationslinien gemäß dem Telekommunikationsgesetz)*	Alle Ebenen; zu gleichen Teilen
1.1.3	Bürgerbeteiligung und Information (kommunale Elemente)[2] *(Durchführung von Beteiligungsverfahren nach dem Baugesetzbuch, dem Raumordnungsgesetz und in der Planfeststellung, Einstellen von raumbezogenen Planwerken in das Internet)*	Ebenen der Gemeinden und Ebene der Landkreise; zu gleichen Teilen
1.2.1	Personalausweis[3] *(Annexleistungen zum Personalausweis: Antrag auf Befreiung von Ausweispflicht; Verlustmeldung)*	Ebene der Gemeinden
1.2.2	Reisepass *(Annexleistungen zum Reisepass: Meldung Fund/Diebstahl/ Verlust)*	Ebene der Gemeinden
1.2.3	Ummeldung[3] *(An- & Ummeldung, Adressänderung, Aktualisierung eID)*	Ebene der Gemeinden
1.3.1	Anlagengenehmigung und -zulassung[3] *(Anlagenbetreiber können ihre Anträge auf Erteilung einer immissionsschutzrechtlichen Genehmigung nach dem BImSchG medienbruchfrei erstellen und diese elektronisch und rechtsverbindlich an die zuständige Behörde übermitteln)*	Ebene der Landkreise
1.3.2	Aufenthaltstitel[4] (im Bündel mit Aufenthaltskarten und aufenthaltsrelevante Bescheinigungen und Beschäftigungserlaubnis) *(Anträge auf Ausstellung/Erteilung/Verlängerung von Aufenthaltstiteln in den Bereichen: „Erwerbstätigkeit“, „Familiäre Gründe“, „Ausbildung“, „Beschleunigtes Fachkräfteverfahren“, „Niederlassungserlaubnis“, „Aufenthaltstitel für Ukraine-Geflüchtete“; auch: Anträge auf Änderung von Nebenbestimmungen; auf Aufenthaltskarten und aufenthaltsrelevante Bescheinigungen; nicht erfasst: vor Ort nötige Identifizierung / Fingerabdruckerfassung / Unterschrifterfassung)*	Ebene der Landkreise
1.3.3	Aufstiegsfortbildungsförderung *(Antrag auf Förderung nach dem Aufstiegsfortbildungsförderungsgesetz – „Aufstiegs- bzw. Meister-BAföG“)*	Ebene der Landkreise

1.3.4	EMBE-Online *(Erfassung und Verwaltung von Emissionsmessberichterstattung sowie Übermittlung an Behörden)*	Ebene der Landkreise
1.3.5	eWaffe[3] *(Beantragung der grünen, gelben, roten Waffenbesitzkarte sowie der Erteilung einer Waffenbesitzkarte für Schießsportvereine)*	Ebene der Landkreise
1.3.6	Immissionsschutz-Online *(Erfüllung von Anzeige- und Auskunftspflichten nach dem Bundesimmissionsschutzgesetz)*	Ebene der Landkreise
1.3.7	Leistungen zum Infektionsschutz *(Belehrung nach dem Infektionsschutzgesetz sowie Ausstellung einer digitalen Bescheinigung)*	Ebene der Landkreise
1.3.8	Sozialplattform *(Anträge auf Aktivierung und berufliche Eingliederung, Leistungen für Bedarfe für Bildung und Teilhabe, Förderung der Aufnahme einer Erwerbstätigkeit, Grundsicherung im Alter und bei Erwerbsminderung, Hilfe zum Lebensunterhalt, Übernahme von Mietrückständen, Hilfe zur Überwindung besonderer sozialer Schwierigkeiten, Schuldnerberatung, Suchtberatung)*	Ebene der Landkreise
1.3.9	Trinkwasseranzeige *(Anzeige von Errichtung oder Änderungen im Betrieb von Wasserversorgungsanlagen und Nichttrinkwasseranlagen an das Gesundheitsamt)*	Ebene der Landkreise
1.3.10	Unterhaltsvorschuss[3] *(Abwicklung des Unterhaltsvorschuss-Erstantrags sowie der jährlichen Überprüfung der Anspruchsvoraussetzungen, inkl. digitaler Signatur und Upload aller Nachweise)*	Ebene der Landkreise
1.3.11	Verpflichtungserklärung[4] *(Abgabe von Verpflichtungserklärungen zur Absicherung der Kosten für den Lebensunterhalt von Drittstaatsangehörigen sowie Bezahlung per ePayment)*	Ebene der Landkreise
2.	**Nicht-EfA-Dienste** *(Digitale Meldeverfahren und Antragsverfahren für die Ausstellung von Urkunden/Bescheinigungen/Genehmigungen, soweit nicht anders angegeben)*	
2.1.1	Anschluss öffentliche Wasserversorgung	Ebene der Gemeinden
2.1.2	Ausnahmegenehmigung Veränderungssperre	Ebene der Gemeinden
2.1.3	Baumfällgenehmigung *(Ausnahmegenehmigung bei kommunalrechtlich/landesrechtlich geschützten Bäumen)*	Ebene der Gemeinden
2.1.4	Bewohnerparkausweis	Ebene der Gemeinden
2.1.5	Eheschließung	Ebene der Gemeinden
2.1.6	Eheurkunde	Ebene der Gemeinden
2.1.7	Fundsachen *(Statusabfrage, Herausgabe, Verwahrung, Versteigerung)*	Ebene der Gemeinden
2.1.8	Geburtsanzeige	Ebene der Gemeinden
2.1.9	Geburtsurkunde	Ebene der Gemeinden
2.1.10	Lebenspartnerschaftsurkunde	Ebene der Gemeinden
2.1.11	Marktfestsetzung	Ebene der Gemeinden
2.1.12	Meldebescheinigung *(Erteilung, Melderegisterauskunft, Lebensbescheinigung für Rentenversicherung)*	Ebene der Gemeinden

2.1.13	Parkplatzabsperrung	Ebene der Gemeinden
2.1.14	Schülerbeförderung *(Durchführung, Erstattung, Entlastung)*	Ebene der Gemeinden
2.1.15	Sterbefallanzeige *(Anzeige Sterbefall, Bescheinigung über Anzeige Todesfall, Sterbeurkunde im Rahmen der Sterbefallanzeige, Personenstandsregisterauszug im Rahmen der Sterbefallanzeige)*	Ebene der Gemeinden
2.1.16	Sterbefallanzeige (Erweiterung) *(Leichenschau, Bescheinigung über Anzeige eines Todesfalles, Beurkundung Sterbefall im Ausland)*	Ebene der Gemeinden
2.1.17	Sterbeurkunde	Ebene der Gemeinden
2.1.18	Übermittlungssperre	Ebene der Gemeinden
2.1.19	Veranstaltungserlaubnis	Ebene der Gemeinden
2.2.1	Antrag internationaler Führerschein	Ebene der Landkreise
2.2.2	Auskunft örtl. Fahrerlaubnisregister (Karteikartenabschrift)	Ebene der Landkreise
2.2.3	Ausnahmegenehmigung zum Parken für Betriebe	Ebene der Landkreise
2.2.4	Dienstfahrerlaubnis Katastrophenschutz Erteilung („Feuerwehrführerschein“)	Ebene der Landkreise
2.2.5	Fahrerlaubnis – Erstantrag	Ebene der Landkreise
2.2.6	Fahrerlaubnis – Verlängerung	Ebene der Landkreise
2.2.7	Fahrerqualifizierungsnachweis – Erstantrag	Ebene der Landkreise
2.2.8	Fahrlehrererlaubnis	Ebene der Landkreise
2.2.9	Fahrschulerlaubnis	Ebene der Landkreise
2.2.10	Führerschein Fahrgastbeförderung	Ebene der Landkreise
2.2.11	Führerschein Fahrgastbeförderung-Erweiterung um weitere Beförderungsart	Ebene der Landkreise
2.2.12	Führerschein Fahrgastbeförderung-Verlängerung	Ebene der Landkreise
2.2.13	Führerschein-Ersatz	Ebene der Landkreise
2.2.14	Führerschein-Erweiterung allg. Fahrerlaubnis	Ebene der Landkreise
2.2.15	Führerschein-Neuerteilung nach Entzug	Ebene der Landkreise
2.2.16	Führerschein-Umschreibung ausländischer Führerschein (EU/EWR-Führerschein und Drittstaaten)	Ebene der Landkreise
2.2.17	Führerschein-Umschreibung Dienstfahrerlaubnis in allg. Fahrerlaubnis	Ebene der Landkreise
2.2.18	Führerschein-Umtausch	Ebene der Landkreise
2.2.19	i-Kfz (Stufe 4) *(Zulassung, Um- und Abmeldung, Wiederzulassung und Außerbetriebsetzung – auch für juristische Personen)*	Ebene der Landkreise
2.2.20	Spielhallen-Erlaubnis	Ebene der Landkreise
2.2.21	Kfz-Zulassungsbescheinigung *(Ausstellung, Änderung, Ersatz, Statusabfrage)*	Ebene der Landkreise

[1] Wird für das Jahr 2024 aus dem FITKO-Budget und für das Jahr 2025 durch das Staatsministerium für Wohnen, Bau und Verkehr finanziert, es verbleiben lediglich die Kosten der Implementierung. Diese sind nicht Gegenstand dieser Verordnung.

[2] Wird für die Jahre 2024/2025 durch das Staatsministerium für Wohnen, Bau und Verkehr sowie das Staatsministerium für Wirtschaft, Landesentwicklung und Energie finanziert, es verbleiben lediglich die Kosten der Implementierung. Diese sind nicht Gegenstand dieser Verordnung.

[3] Wird für das Jahr 2024 aus dem FITKO-Budget finanziert, es verbleiben lediglich die Kosten der Implementierung. Diese sind nicht Gegenstand dieser Verordnung.

[4] Wird für das Jahr 2024 aus dem FITKO-Budget und für das Jahr 2025 durch das Staatsministerium des Innern, für Sport und Integration finanziert, es verbleiben lediglich die Kosten der Implementierung. Diese sind nicht Gegenstand dieser Verordnung.

Herausgeber/Redaktion: Bayerische Staatskanzlei, Franz-Josef-Strauß-Ring 1, 80539 München
Das Bayerische Gesetz- und Verordnungsblatt (GVBl.) wird nach Bedarf ausgegeben, in der Regel zweimal im Monat. Zur Herstellung des GVBl. wird Recycling-Papier verwendet.
Druck: Druckerei Reindl, Goethestr. 18, 85055 Ingolstadt.
Vertrieb: Verlag Bayerische Staatszeitung GmbH, Arnulfstraße 122, 80636 München
Tel. 0 89 / 29 01 42 - 59 / 69, Telefax 0 89 / 29 01 42 90.
Bezug: Die amtliche Fassung des GVBl. können Sie über den Verlag Bayerische Staatszeitung GmbH beziehen. Der Preis des Jahresabonnements für die amtliche Fassung des GVBl. beträgt ab dem 1. Januar 2019 **90,00 €** inkl. MwSt. und Versandkosten. Einzelausgaben können zum Preis von 3,50 € inkl. MwSt. zzgl. Versand beim Verlag angefordert werden. Für Abonnementkündigungen gilt eine Frist von vier Wochen zum nächsten Ersten eines Monats (bei Vorauszahlung zum Ende des verrechneten Bezugszeitraums).
Widerrufsrecht: Der Verlag räumt ein Widerrufsrecht von einer Woche ab Absendung der Bestellung ein.
Zur Wahrung der Frist genügt das rechtzeitige Absenden des Widerrufs (Poststempel) an:
Verlag Bayerische Staatszeitung GmbH, Vertrieb, Postfach 20 04 63, 80004 München
Bankverbindung: UniCredit Bank AG, IBAN: DE25 3022 0190 0036 9850 20
ISSN 0005-7134

Bayerisches Gesetz- und Verordnungsblatt
Verlag Bayerische Staatszeitung GmbH
Arnulfstraße 122, 80636 München
PVSt, Deutsche Post AG, Entgelt bezahlt, B 1612