LANDTAG DES SAARLANDES
16. Wahlperiode **Drucksache 16/761**
06.03.2019

GESETZENTWURF

der Regierung des Saarlandes

betr.: Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (Informationssicherheitsgesetz Saarland – IT-SiG SL) sowie zur Änderung weiterer Vorschriften

A. Problem und Ziel

Zu Artikel 1:

Die Digitalisierung in Staat, Wirtschaft und Gesellschaft hat Deutschland in nur wenigen Jahren grundlegend verändert. Neue Möglichkeiten der Kommunikation, des Wissenszuganges und der innovativen Gestaltung führen zu mehr sozialer Interaktion, neuen Geschäftsmodellen und neuen Feldern für Forschung und Entwicklung. Die Digitalisierung eröffnet Chancen, birgt aber auch Risiken und braucht daher Vertrauen. Sicherheit, insbesondere im Hinblick auf Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität, ist hierbei ein wesentlicher Aspekt. Das Saarland reagiert mit diesem Gesetz auf die Risiken, die sich aus der Digitalisierung ergeben. Dort, wo digitale Verwaltung stattfindet und Daten, insbesondere personenbezogene Daten, elektronisch gespeichert oder übermittelt werden, wird der Schutz der informationstechnischen Systeme zu einer fundamentalen Anforderung, um die Funktionsfähigkeit und vor allem die Verlässlichkeit der Verwaltung sicherzustellen.

Diverse Angriffs- und Kompromittierungsversuche zeigen, dass Systeme lahmgelegt oder infiziert werden und Informationen in die falschen Hände gelangen können. Dem gilt es wirksam zu begegnen, da in der öffentlichen Verwaltung – neben dem Gebot der Aufrechterhaltung der Funktionsfähigkeit – Daten von Bürgerinnen und Bürgern, Unternehmen und Verbänden, eigenen Mitarbeiterinnen und Mitarbeitern vorhanden sind, die im höchsten Maße sensibel sind und daher eines angemessenen und umfassenden Schutzes bedürfen. Daher gehört es zu den allgemeinen behördenübergreifenden Pflichten, die Sicherheit der informationstechnischen Systeme nach dem Stand der Technik sowie im Rahmen der Verhältnismäßigkeit sicherzustellen und wird in Artikel 1 § 3 des Gesetzentwurfs nach dem Vorbild der bayerischen Regelung allen Behörden auferlegt.

Des Weiteren hat der IT-Planungsrat im März 2015 die Anschlussbedingungen für das Verbindungsnetz (kurz: DOI-Anschlussbedingungen; DOI = Deutschland Online Infrastruktur; jetzt: Netze des Bundes = NdB) definiert. Diese Anschlussbedingungen sollten von den Ländern bis zum 31.12.2017 erfüllt und bis zum 31.12.2019 zertifiziert werden. Eine der hierzu umzusetzenden Maßnahmen ist die Einführung von Angriffserkennungssystemen (Intrusion Detection System = IDS).

Ausgegeben: 06.03.2019

Ein im Auftrag des IT-Planungsrates von der Universität Hannover 2016 erstelltes Gutachten kommt zu dem Ergebnis, dass es für die Installation eines Intrusion Detection Systems im Hinblick auf Artikel 10 GG (Fernmeldegeheimnis) in den Ländern einer Rechtsgrundlage bedarf. Bestehende Gesetze wie datenschutzrechtliche Regelungen, Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG) werden hierfür nicht als ausreichend angesehen. Für den Bund besteht diese Problematik angesichts expliziter Regelungen im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) nicht. Die im vorliegenden Gesetzentwurf vorgesehenen Regelungen orientieren sich hieran.

Zu Artikel 2:

Für Bund und Länder (einschließlich Kommunen) besteht die Verpflichtung, die Vorgaben der Richtlinie 2014/55/EU über die elektronische Rechnungsstellung im öffentlichen Auftragswesen in nationales Recht umzusetzen (für die obersten Bundesbehörden bis zum 27. November 2018, für alle anderen bis zum 18. April 2020). Die für das Saarland vorgesehene Regelung umfasst dabei auch die Verpflichtung unterhalb der EU-Schwellenwerte, da ansonsten eine wirtschaftliche und organisatorisch handhabbare Umsetzung sowohl in der Verwaltung als auch in den Unternehmen schwer darstellbar erscheint.

Um die künftige Weiterentwicklung des E-Governments zu erleichtern, soll außerdem eine Experimentierklausel für Pilotprojekte zur Einführung neuer E-Government-Anwendungen geschaffen werden.

Zu Artikel 3:

Zur Koordinierung und Steuerung der Aufgaben im Zusammenhang mit der Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur der Landesverwaltung bedarf es der Funktion eines Landesbeauftragten für Informationssicherheit (Chief Information Security Officer, CISO). Die Einrichtung einer derartigen Funktion entspricht auch den Vorgaben des IT-Planungsrates von Bund und Ländern in seiner verbindlichen Leitlinie für Informationssicherheit in der öffentlichen Verwaltung.

Im Saarland ist diese Aufgabe dem Direktor des Landesamtes für Zentrale Dienste zusätzlich zu seinen mit der Leitung des Amtes obliegenden Aufgaben übertragen worden.

B. Lösung

Mit Artikel 1 dieses Gesetzes werden alle Behörden verpflichtet, in einem angemessenen Umfang die Sicherheit der informationstechnischen Systeme zu gewährleisten. Gleichzeitig wird der zentrale IT-Dienstleister, soweit informationstechnische Systeme mit dem Landesdatennetz verbunden sind, ermächtigt, neben den etablierten technischen Verfahren wie portbasierten Firewalls, Virenscannern und Proxy-Servern weitergehende Maßnahmen durchzuführen, die das allgemeine Persönlichkeitsrecht in Artikel 2 Absatz 1 in Verbindung mit Artikel 1 GG sowie das Fernmeldegeheimnis in Artikel 10 GG und Artikel 17 der Verfassung des Saarlandes berühren bzw. einschränken. Der Bedeutung der Grundrechtsrelevanz entsprechend ist ein mehrstufiges Verfahren vorgesehen.

Rein vorsorglich wird diese Ermächtigung ergänzend allen Behörden für ihre lokalen Netze eingeräumt.

Der Gesetzentwurf befindet sich im Einklang mit der Verordnung (EU) 2016/679 (EU-DSGVO). Er ist sogar die logische Konsequenz aus Artikel 32 EU-DSGVO, der die Sicherheit der Verarbeitung personenbezogener Daten durch geeignete technische und organisatorische Maßnahmen fordert.

Artikel 1 des Gesetzentwurfs orientiert sich in seinem materiellen Regelungsgehalt an vorhandenen Vorschriften im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885), sowie am Gesetz zur Errichtung des Landesamtes für Sicherheit in der Informationstechnik vom 27. November 2017 des Landes Bayern (GVBl. S. 518) und an Referentenentwürfen zum Thema Informationssicherheit anderer Bundesländer.

Artikel 2 setzt die Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen um. Öffentliche saarländische Auftraggeber europaweiter Vergabeverfahren werden durch die EU-Vorgaben verpflichtet, elektronische Rechnungen zu geschlossenen Verträgen über Lieferungen und Leistungen spätestens ab dem 18. April 2020 empfangen und verarbeiten zu können. Der hierfür ursprünglich vorgesehene Termin war der 27. November 2019. Aufgrund der erst am 17. Oktober 2017 verspätet erfolgten Veröffentlichung der europäischen Norm für die elektronische Rechnungsstellung (s. Artikel 3 E-Rechnungsrichtlinie) im Amtsblatt der Europäischen Union hat sich dieser Termin verschoben. Diese verlängerte Frist wird in Anspruch genommen.

Die Verpflichtung zum Empfang und zur Verarbeitung elektronischer Rechnungen wird in diesem Gesetzentwurf auch auf den sogenannten unterschwelligen Bereich, also für Vergaben und Auftragshöhen unterhalb der jeweils maßgeblichen EU-Schwellenwerte ausgedehnt, um eine Vereinfachung und Standardisierung des Rechnungsstellungverfahrens insgesamt zu gewährleisten, die Möglichkeit der Interoperabilität zwischen verschiedenen Rechnungsstellungs- und Rechnungsbearbeitungssystemen zu schaffen und letztlich das elektronische Rechnungswesen überhaupt wirtschaftlich zu machen.

Um die künftige Weiterentwicklung des E-Governments zu erleichtern, soll außerdem eine Experimentierklausel für Pilotprojekte zur Einführung neuer E-Government-Anwendungen geschaffen werden.

Artikel 3 trägt Rechnung, dass es zur Koordinierung und Steuerung der Aufgaben im Zusammenhang mit der Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur der Landesverwaltung der Funktion eines Landesbeauftragten für Informationssicherheit (Chief Information Security Officer, CISO) bedarf. Die Einrichtung einer derartigen Funktion entspricht auch den Vorgaben des IT-Planungsrates von Bund und Ländern in seiner verbindlichen Leitlinie für Informationssicherheit in der öffentlichen Verwaltung.

Im Saarland ist diese Aufgabe dem Direktor des Landesamtes für Zentrale Dienste zusätzlich zu seinen mit der Leitung des Amtes obliegenden Aufgaben übertragen worden.

Wegen der Bedeutung, des Aufwandes und der mit der zusätzlichen Aufgabe verbundenen landesweiten Verantwortung wird daher in der Besoldungsgruppe B 5 ein weiteres Amt für den Direktor des Landesamtes für Zentrale Dienste ausgebracht. Durch die Ausbringung eines Funktionszusatzes wird geregelt, dass dieses Amt ausschließlich Leitern des Landesamtes für Zentrale Dienste vorbehalten ist, denen neben der Leitung des Landesamtes die Funktion des Landesbeauftragten für Informationssicherheit übertragen wurde.

C. Alternativen

Keine.

D. Finanzielle Auswirkungen

1. Haushaltsausgaben ohne Vollzugsaufwand

Keine.

2. Vollzugsaufwand

Zu Artikel 1:

Um die mit elektronischem Verwaltungshandeln verbundenen Risiken hinsichtlich der in der öffentlichen Verwaltung vorhandenen sensiblen Daten von Bürgerinnen, Bürgern und Unternehmen aber auch hinsichtlich der jederzeitigen Handlungsfähigkeit der Verwaltung selbst auf ein unumgängliches Maß zu beschränken, sind neue Techniken und Handlungsweisen notwendig.

Die Ermittlung der finanziellen Auswirkungen gestaltet sich schwierig. Zur Gewährleistung einer ausreichenden Informationssicherheit sind auch ohne den vorliegenden Gesetzentwurf zusätzliche Anstrengungen erforderlich und Kosten zu erwarten. Durch die Schaffung eines klaren rechtlichen Rahmens werden Standards und Strukturen vorgegeben, die insgesamt zu einer Kostendämpfung beitragen. Bei den behördenübergreifenden Pflichten nach § 3 Absatz 1 sind Verhältnismäßigkeit und Angemessenheit zu berücksichtigen. Soweit die kommunale Ebene betroffen ist, wird hierdurch keine Konnexität ausgelöst. Als Anschubfinanzierung werden für die Erstellung von Informationssicherheitskonzepten in Absprache mit der kommunalen Ebene Bedarfszuweisungen durch das Ministerium für Inneres, Bauen und Sport (MIBS) gewährt. Die Einbindung der kommunalen Ebene in das CERT nach § 3 Absatz 2 führt nicht zu nennenswerten Mehrkosten. Einzelheiten sind in der Begründung zu Artikel 1 § 3 des Gesetzentwurfs ausgeführt. Die dem zentralen IT-Dienstleister in Artikel 1 §§ 4 bis 7 zugewiesenen Aufgaben beinhalten zum einen die Installation der technischen Komponenten sowie zum anderen die für die Auswertungen notwendigen Mitarbeiterinnen/Mitarbeiter mit entsprechender Qualifikation.

Die rein vorsorgliche Ermächtigung für alle Behörden im Artikel 1 § 11 des Gesetzentwurfs führt nicht unmittelbar zu finanziellen Folgen, sondern erst wenn von dieser Ermächtigung Gebrauch gemacht wird. Eine Verpflichtung besteht nur, soweit ein unmittelbarer Anschluss an die Netze des Bundes (NdB, früher: Deutschland Online Infrastruktur, DOI) besteht und die Vorgaben des IT-Planungsrates zu erfüllen sind.

Für Bürgerinnen und Bürger sowie Unternehmen bleibt Artikel 1 ohne finanzielle Auswirkungen.

Zu Artikel 2:

Artikel 2 erfordert auf Seiten der Verwaltung ein IT-Verfahren, das E-Rechnungen zu geschlossenen Verträgen über Lieferungen und Leistungen entgegennehmen und mindestens visualisieren kann (Webportal/E-Poststelle und Ablage für E-Rechnungen), das im Idealfall auch einen Workflow zur Rechnungsbearbeitung beinhaltet.

Konnexitätsaspekte kommen durch die Verpflichtung der kommunalen Ebene im EU-unterschwelligen Bereich nicht zum Tragen. Zwar gibt es hierzu keine gesetzliche Verpflichtung einer höheren Ebene, sodass das Land insoweit einen eigenen Gestaltungsspielraum nutzt.

Nach Artikel 120 der Verfassung des Saarlandes können nur durch förmliches Gesetz den Gemeinden und Gemeindeverbänden staatliche Aufgaben zur Durchführung übertragen und die Erfüllung von Selbstverwaltungsaufgaben zur Pflicht gemacht werden, wenn dabei gleichzeitig Bestimmungen über die Deckung der Kosten getroffen werden. Allerdings handelt es sich bei der durch dieses Gesetz bzw. der aufgrund dieses Gesetzes in der noch zu erlassenden Rechtsverordnung geregelten Entgegennahme und Behandlung elektronischer Rechnungen nicht um die Übertragung einer neuen Aufgabe, sondern als Ausgestaltung der kommunalen Haushalts- und Rechnungsführung um rein organisatorische Vorgaben, bei denen die Anwendung des Konnexitätsprinzips ausgeschlossen ist. Hinzu kommt, dass die Vorgaben zum elektronischen Rechnungsempfang bei Erreichen der EU-Schwellenwerte durch EU-Recht ohnehin vorgegeben sind und eine Differenzierung je nach Rechnungshöhe auch bei den Kommunen zu einem wirtschaftlichen und organisatorischen Mehraufwand führen würde.

Eine solide Kostenschätzung ist derzeit nicht möglich und hängt davon ab, welches konkrete IT-Verfahren gewählt wird, ob eine Ein- oder Anbindung in bzw. zu bereits vorhandenen Verfahren möglich ist und inwieweit Ebenen übergreifende Lösungen möglich sind. Nähere Angaben zu den Kosten sind daher erst im Zusammenhang mit der nach Artikel 2 § 10a Absatz 3 zu erlassenden Rechtsverordnung und nach Abstimmung einer anzustrebenden gemeinsamen Lösung mit der kommunalen Ebene im IT-Kooperationsrat möglich.

Mit der Einführung der E-Rechnung sind aber auch erhebliche Einsparungen zu erwarten, wenn die vollständige Rechnungsbearbeitung in der Verwaltung elektronisch durchgeführt wird.

Dies gilt eingeschränkt auch für Unternehmen, die bis zum heutigen Tage die Rechnungserstellung regelmäßig bereits auf elektronischer Basis realisiert haben, jedoch ggf. Aufwände für die zu nutzende Übertragungstechnik erbringen müssen.

Für Bürgerinnen und Bürger bleibt Artikel 2 ohne finanzielle Auswirkungen.

Zu Artikel 3:

Es muss keine separate B4-Stelle für einen IT-Sicherheitsbeauftragten mehr vorgehalten werden.

E. Sonstige Kosten

Keine.

F. Auswirkungen von frauenpolitischer Bedeutung

Nach Überprüfung der für die Gleichstellungsverträglichkeit von Kabinettsvorlagen entwickelten Kriterien und Kernfragen sind unterschiedliche Auswirkungen des Gesetzentwurfs auf die unterschiedliche Lebenssituation von Frauen und Männern nicht zu erwarten.

G. Federführende Zuständigkeit

Ministerium für Finanzen und Europa.

G e s e t z

**zur Abwehr von Gefahren
für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes
(Informationssicherheitsgesetz Saarland – IT-SiG SL)**

sowie zur Änderung weiterer Vorschriften

Vom

Der Landtag wolle beschließen:

Artikel 1

**Gesetz zur Abwehr von Gefahren
für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes
(Informationssicherheitsgesetz Saarland – IT-SiG SL)**

Inhaltsübersicht

§ 1
Zweck und Geltungsbereich

Dieses Gesetz dient der Informationssicherheit des Landesdatennetzes, der informationstechnischen Systeme, der genutzten Anwendungen und der darüber verarbeiteten Informationen der Behörden des Saarlandes. Dieses Gesetz gilt für die Verwaltungstätigkeit der Behörden des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Verwaltungstätigkeit im Sinne dieses Gesetzes umfasst die öffentlichrechtliche Verwaltungstätigkeit und rechtsgeschäftliche oder tatsächliche Tätigkeiten im allgemeinen privatrechtlichen Rechtsverkehr einschließlich der fiskalischen Hilfsgeschäfte. Behörde im Sinne dieses Gesetzes ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt. Die Vorschriften dieses Gesetzes gelten entsprechend für die Gerichte und Staatsanwaltschaften.

§ 2
Begriffsbestimmungen

Im Sinne dieses Gesetzes sind:

1. Informationssicherheit:
   die Gewährleistung der Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Informationen durch Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen,

2. Schadprogramme:
   Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten auszuspähen, zu manipulieren, zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken,

3. das Landesdatennetz:
   eine Kommunikationsinfrastruktur, die eine gesicherte Verbindung zwischen den lokalen Netzen der damit verbundenen Behörden sowie zu Netzen anderer Verwaltungen ermöglicht und durch das Land oder im Auftrag des Landes betrieben wird,

4. informationstechnische Systeme mit dem Landesdatennetz verbunden:
   wenn sie direkt, über ein behördeneigenes Subnetz oder über einen IT-Dienstleister technisch angeschlossen sind,

5. Angriffe:
   Versuche, die Informationssicherheit eines Computersystems unbefugt zu beeinflussen,

6. Sicherheitslücken:
   Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Unbefugte Zugang zu informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können,

7. Protokolldaten:
   Steuerungsdaten und Ereignisprotokolle einer informationstechnischen Datenverarbeitung oder eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt einer Datenverarbeitung gespeichert oder unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 30 des Telekommunikationsgesetzes und Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes enthalten,

8. Inhaltsdaten:
   Informationen, die den Inhalt einer Datenverarbeitung oder eines Telekommunikationsvorgangs betreffen und die keine Protokolldaten sind,

9. Informationstechnik:
   Alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen,

10. Informationstechnik des Landes:
    Informationstechnik, die von einer oder mehreren Landesbehörden oder im Auftrag einer oder mehrerer Landesbehörden betrieben wird.

§ 3
Behördenübergreifende Pflichten

(1) Die Sicherheit der informationstechnischen Systeme der Behörden ist nach dem Stand der Technik im Rahmen der Verhältnismäßigkeit und unter Beachtung der Vorschriften der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) sowie des Saarländischen Datenschutzgesetzes vom 16. Mai 2018 (Amtsbl. I S. 254) sicherzustellen. Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen und erstellen die hierzu erforderlichen Informationssicherheitskonzepte.

(2) Werden Behörden Informationen bekannt, die zur Abwehr von Gefahren für die Informationssicherheit von Bedeutung sind, unterrichten diese den zentralen IT-Dienstleister des Landes unverzüglich hierüber, soweit andere Vorschriften oder Vereinbarungen mit Dritten nicht entgegenstehen, Meldepflichten aufgrund gesetzlicher Vorschriften bestehen oder sie einem Meldesystem innerhalb eines anderen deutschen CERT-Verbundes angeschlossen sind.

§ 4
Abwehr von Gefahren für die Informationssicherheit

(1) Der zentrale IT-Dienstleister kann nach Maßgabe dieser und der nachfolgenden Regelungen die zur Erfüllung seiner Aufgaben als Betreiber des Landesdatennetzes und Auftragsverarbeiter nach dem Gesetz zur Errichtung eines Landesamtes für IT-Dienstleistungen vom 02. Dezember 2015 (Amtsbl. I S. 967), geändert durch Gesetz vom 24. Oktober 2017 (Amtsbl. I S. 1005), in der jeweils geltenden Fassung, notwendigen und angemessenen Maßnahmen ergreifen, um Gefahren für die Informationssicherheit des Landesdatennetzes, aller daran angeschlossenen und mit ihm und miteinander verbundenen informationstechnischen Systeme (IT-Systeme), der genutzten Anwendungen und der darüber verarbeiteten Informationen zu erkennen, einzugrenzen und abzuwehren. Dies umfasst die Ermächtigung zur Verarbeitung personenbezogener Daten, soweit die Verarbeitung zur Erfüllung der nach diesem Gesetz übertragenen Befugnisse erforderlich ist.

(2) Der zentrale IT-Dienstleister kann zum in Absatz 1 genannten Zweck, soweit dies erforderlich ist, die beim Betrieb von Informationstechnik des Landes sowie die an den Schnittstellen des Landesdatennetzes und anderen Netzen und innerhalb des Landesdatennetzes anfallenden Protokolldaten und Inhaltsdaten erheben und automatisiert auswerten.

(3) Zur Ermöglichung einer automatisierten Auswertung nach Absatz 2 können die an das Landesdatennetz angeschlossenen Stellen dem zentralen IT-Dienstleister die bei ihnen gespeicherten Protokolldaten auf Anfrage zur Verfügung stellen.

(4) Sofern nicht die nachfolgenden Vorschriften eine weitere Verwendung gestatten, muss eine automatisierte Auswertung der Daten unverzüglich erfolgen und müssen die Daten nach erfolgtem Abgleich sofort und spurlos gelöscht werden. Die Speicherung und sonstige Verarbeitung nach dem ursprünglichen Verwendungszweck bleiben hiervon unberührt. Daten, die weder dem Fernmeldegeheimnis unterliegen noch Personenbezug aufweisen, sind von den Verwendungsbeschränkungen dieser Vorschrift ausgenommen.

(5) Personenbezogene Daten, die zum Zweck der Gewährleistung der Informationssicherheit nach diesem Gesetz ausgewertet werden dürfen, dürfen nicht für andere Zwecke, insbesondere nicht zur Verhaltens- und Leistungskontrolle, verarbeitet werden.

§ 5
Auswertung von Protokolldaten

(1) Bestehen tatsächliche Anhaltspunkte für das Vorliegen einer Gefahr für die Informationssicherheit, dürfen Protokolldaten über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus gespeichert und automatisiert ausgewertet werden, soweit und solange dies zur weiteren Eingrenzung und Abwehr dieser Gefahr erforderlich ist. Entsprechendes gilt, wenn diese Daten zur Verfolgung damit zusammenhängender Straftaten erforderlich sein können.

(2) Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach Absatz 1 gespeicherten Daten nur automatisiert erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist.

(3) Sofern im Rahmen der automatisierten Auswertung ein Verdachtsfall auf eine Gefährdung der Informationssicherheit entdeckt wird und für die weitere Analyse die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch die Leitung des zentralen IT-Dienstleisters angeordnet werden. Die Entscheidung ist zu dokumentieren. Eine nicht automatisierte Auswertung oder eine personenbezogene Verwendung ist nur nach Maßgabe der nachfolgenden Vorschriften zulässig.

§ 6
Auswertung von Inhaltsdaten

(1) Für die Datenverarbeitung von Inhaltsdaten gilt § 5 mit der Maßgabe, dass eine Speicherung für höchstens zwei Monate zulässig ist, die Speicherung und Auswertung von der Leitung des zentralen IT-Dienstleisters und von einer oder einem Bediensteten des für die Fachaufsicht über den zentralen IT-Dienstleister zuständigen Ministeriums mit der Befähigung zum Richteramt angeordnet sind und dies zum Schutz der technischen Systeme unerlässlich ist. Die Entscheidung ist zu dokumentieren.

(2) Die Anordnung gilt längstens für zwei Monate und kann höchstens um einen weiteren Monat verlängert werden.

§ 7
Weitergehende Auswertungen

(1) Eine über die in den §§ 5 und 6 hinausgehende Verarbeitung der Protokoll- und Inhaltsdaten ist nur zulässig,

1. wenn bestimmte Tatsachen den hinreichenden Verdacht begründen, dass die Daten Hinweise auf Gefahren für die Informationssicherheit, etwa durch Schadprogramme oder Sicherheitslücken, Angriffe oder unbefugten Datenzugriff enthalten und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen
   oder
2. wenn sich der Verdacht nach Nummer 1 bestätigt und dies zur Abwehr von Gefahren für die Informationssicherheit erforderlich ist.

   Werden Daten, welche die richterliche Unabhängigkeit berühren, nach dieser Vorschrift verarbeitet, ist der jeweils zuständigen obersten Dienstbehörde unverzüglich zu berichten. Berührt die Datenverarbeitung die Aufgabenwahrnehmung anderer unabhängiger Stellen oder ein Berufs- oder besonderes Amtsgeheimnis, ist die betroffene Stelle unverzüglich zu unterrichten. Die jeweiligen Stellen nach Satz 2 und 3 können vom zentralen IT-Dienstleister Auskunft über die Verarbeitung von Daten nach dieser Vorschrift verlangen.

(2) Soweit möglich, ist bei der Datenverarbeitung technisch und organisatorisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Dies gilt auch in Zweifelsfällen.

§ 8
Sicherheitskonzept

(1) Von den Ermächtigungen nach den §§ 4 bis 7 darf nur Gebrauch gemacht werden, wenn hierfür durch den zentralen IT-Dienstleister ein Sicherheitskonzept erstellt wurde und die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen in einem Steuerungssystem dokumentiert, überwacht und fortgeschrieben wird. Das Sicherheitskonzept ist vor jeder Veränderung der eingesetzten technischen Systeme zu aktualisieren. Für jede Veränderung des Sicherheitskonzeptes gilt Satz 1 entsprechend.

(2) Das Sicherheitskonzept nach Absatz 1 bedarf in Bezug auf den Umgang mit der Verarbeitung personenbezogener Daten im Sinne des § 4 sowie von Protokoll- und Inhaltsdaten im Sinne der §§ 5 bis 7, soweit es sich um Daten der Landesmedienanstalt Saarland (LMS) oder privater Rundfunkveranstalter und Telemedienanbieter bei der LMS handelt, der Zustimmung der Landesmedienanstalt Saarland.

§ 9
Benachrichtigung der Betroffenen

(1) Die von Maßnahmen nach § 7 Betroffenen und betroffenen Behörden sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von sonstigen Gefahren zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist. Die Benachrichtigung kann unterbleiben, solange hierdurch der Ermittlungszweck eines Straf- oder Disziplinarverfahrens oder die Informationssicherheit gefährdet würde.

(2) Sofern die Benachrichtigung nach Absatz 1 Sätzen 2 und 3 unterbleiben soll, ist dies durch eine Bedienstete oder einen Bediensteten des für die Fachaufsicht über den zentralen IT-Dienstleister zuständigen Ministeriums mit der Befähigung zum Richteramt anzuordnen und zu dokumentieren.

§ 10
Übermittlung personenbezogener Daten

(1) Der zentrale IT-Dienstleister soll personenbezogene Daten nach den §§ 6 und 7 unverzüglich übermitteln

1. an die Polizeibehörden des Bundes und der Länder zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht,
2. an die Polizeibehörden des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,
3. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100 a Absatz 2 der Strafprozessordnung bezeichneten Straftat,
4. an die Verfassungsschutzbehörde zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen.

(2) Die Übermittlung nach Absatz 1 Nummern 2 und 3 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Absatz 1 Nummern 2 und 3 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die Übermittlung nach Absatz 1 Nummer 4 bedarf der vorherigen Zustimmung eines Bediensteten oder einer Bediensteten des für die Fachaufsicht über den zentralen IT-Dienstleister zuständigen Ministeriums mit der Befähigung zum Richteramt. Die Entscheidung ist zu dokumentieren.

§ 11
Befugnisse bei lokalen Netzen

Die §§ 4 bis 10 gelten für jede Behörde entsprechend bezüglich ihrer lokalen Netze. Der nach § 5 Absatz 3 erforderliche Leitungsvorbehalt sowie die in § 6 Absatz 1, § 9 Absatz 2 und § 10 Absatz 2 Satz 3 erforderlichen Zustimmungserfordernisse werden insoweit durch die jeweilige Behördenleitung bzw. ihre Vertretung wahrgenommen.

§ 12
Datenschutzrechtliche Kontrolle

(1) Der oder dem Landesbeauftragten für Datenschutz ist vom zentralen IT-Dienstleister einmal im Jahr eine Aufstellung über die nach § 5 Absatz 3, § 6, § 7 und § 10 erfolgten Verarbeitungen vorzulegen.

(2) Die nach diesem Gesetz anzufertigenden Dokumentationen dürfen ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie sind zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich sind, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 13
Einschränkung von Grundrechten

Das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes und Artikel 17 der Verfassung des Saarlandes wird durch die §§ 4 bis 7, § 10 und § 11 eingeschränkt.

Artikel 2

Änderung des E-Government-Gesetzes Saarland

Das Gesetz zur Förderung der elektronischen Verwaltung im Saarland vom 15. November 2017 (Amtsbl. I S. 1007), zuletzt geändert durch Gesetz vom 16. Mai 2018 (Amtsbl. I S. 254), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Nach der Angabe zu § 10 wird folgende Angabe eingefügt:

      „§ 10a Elektronischer Rechnungsempfang; Verordnungsermächtigung“.

   b) Nach der Angabe zu § 20 wird folgende Angabe angefügt:

      „§ 21 Experimentierklausel“.

2. Nach § 10 wird folgender § 10a eingefügt:

„§ 10a
Elektronischer Rechnungsempfang, Verordnungsermächtigung

(1) Elektronische Rechnungen, die nach Erfüllung von öffentlichen Aufträgen und Aufträgen sowie zu Konzessionen von Stellen im Sinne von § 98 des Gesetzes gegen Wettbewerbsbeschränkungen in der Fassung vom 26.Juni 2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Artikel 10 des Gesetzes vom 12. Juli 2018 (BGBl. I S. 1151), in der jeweils geltenden Fassung mit Sitz im Saarland ausgestellt wurden, sind nach Maßgabe einer Rechtsverordnung nach Absatz 3 zu empfangen und zu verarbeiten. Diese Verpflichtung gilt unabhängig von dem Geltungsbereich gemäß § 1 und unabhängig davon, ob der Wert des vergebenen öffentlichen Auftrags, des vergebenen Auftrags oder der Vertragswert der vergebenen Konzession den gemäß § 106 des Gesetzes gegen Wettbewerbsbeschränkungen jeweils maßgeblichen Schwellenwert erreicht oder überschreitet. Vertragliche Regelungen, die die elektronische Rechnungsstellung vorschreiben, bleiben unberührt.

(2) Eine Rechnung ist elektronisch, wenn

1. sie in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird
   und
2. das Format die automatische und elektronische Verarbeitung der Rechnung ermöglicht.

(3) Die Landesregierung wird ermächtigt, durch Rechtsverordnung besondere Vorschriften zur Ausgestaltung des elektronischen Rechnungsverkehrs zu erlassen. Diese Vorschriften können sich beziehen auf

1. die Art und Weise der Verarbeitung der elektronischen Rechnung, insbesondere auf die elektronische Verarbeitung,
2. die Anforderungen an die elektronische Rechnungsstellung und zwar insbesondere auf die von den elektronischen Rechnungen zu erfüllenden Voraussetzungen, den Schutz personenbezogener Daten, das zu verwendende Rechnungsdatenmodell sowie auf die Verbindlichkeit der elektronischen Form,

3. die Befugnis von öffentlichen Auftraggebern, Sektorenauftraggebern und Konzessionsgebern, in Ausschreibungsbedingungen die Erteilung elektronischer Rechnungen vorzusehen sowie
4. Ausnahmen für sicherheitsspezifische Aufträge.“

3. Nach § 20 wird folgender § 21 angefügt:

„§ 21
Experimentierklausel

Die Landesregierung wird ermächtigt, zur Einführung und Fortentwicklung elektronischer Verwaltungsstrukturen durch Rechtsverordnung sachlich und räumlich begrenzte Abweichungen von folgenden Vorschriften vorzusehen:

1. Zuständigkeits- und Formvorschriften nach den §§ 3, 3a, 27a, 33, 34, 37 Absatz 2 bis 5, 41, 57, 64, 69 Absatz 2 des Saarländischen Verwaltungsverfahrensgesetzes vom 15. Dezember 1976 (Amtsbl. S. 1151), zuletzt geändert durch Gesetz vom 25. Juni 2014 (Amtsbl. I S. 306),

2. § 1 Absatz 2 des Saarländischen Verwaltungszustellungsgesetzes vom 13. Dezember 2005 (Amtsbl. 2006, S. 214) in Verbindung mit § 5 Absatz 4 bis 7, § 5a und § 10 Absatz 2 des Verwaltungszustellungsgesetzes vom 12. August 2005 (BGBl. I S. 2354), zuletzt geändert durch Artikel 11 Absatz 3 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745), und

3. sonstigen landesgesetzlichen Zuständigkeits- und Formvorschriften, soweit dies zur Erprobung neuer elektronischer Formen des Schriftformersatzes, der Übermittlung und Bekanntgabe von Dokumenten und Erklärungen, der Vorlage von Nachweisen, der Erhebung, Verarbeitung, Nutzung oder Weitergabe von Daten oder für die Erprobung der Dienste von zentralen Portalen erforderlich ist.

Die Rechtsverordnung ist auf höchstens drei Jahre zu befristen.“

Artikel 3

Änderung des Saarländischen Besoldungsgesetzes

In der Besoldungsordnung B in der Anlage des Saarländischen Besoldungsgesetzes in der Fassung der Bekanntmachung vom 10. Januar 1989 (Amtsbl. S. 301), zuletzt geändert durch Gesetz vom 13. Juni 2018 (Amtsbl. I S. 358), wird in der Besoldungsgruppe B 5 vor der Amtsbezeichnung „Direktor der Landesmedienanstalt Saarland“ die Amtsbezeichnung „Direktor des Landesamtes für Zentrale Dienste“ mit dem Funktionszusatz „- als Leiter des Landesamtes für Zentrale Dienste und Landesbeauftragter für Informationssicherheit“ eingefügt.

Artikel 4

Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach seiner Verkündung in Kraft.

(2) Artikel 2 Nummer 2 § 10a Absätze 1 und 2 treten am 18. April 2020 in Kraft.

B e g r ü n d u n g :

A. Allgemeines

1. Ziel und Gegenstand des Gesetzentwurfes

Die Digitalisierung in Staat, Wirtschaft und Gesellschaft hat Deutschland in nur wenigen Jahren grundlegend verändert. Neue Möglichkeiten der Kommunikation, des Wissenszuganges und der innovativen Gestaltung führen zu mehr sozialer Interaktion, neuen Geschäftsmodellen und neuen Feldern für Forschung und Entwicklung. Die Digitalisierung eröffnet Chancen, birgt aber auch Risiken und braucht daher Vertrauen. Sicherheit, insbesondere im Hinblick auf Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität, ist hierbei ein wesentlicher Aspekt. Das Saarland reagiert mit diesem Gesetz auf die Risiken, die sich aus der Digitalisierung ergeben. Dort, wo digitale Verwaltung stattfindet und Daten, insbesondere personenbezogene Daten, elektronisch gespeichert oder übermittelt werden, wird der Schutz der informationstechnischen Systeme zu einer fundamentalen Anforderung, um die Funktionsfähigkeit und vor allem die Verlässlichkeit der Verwaltung sicherzustellen.

Diverse Angriffs- und Kompromittierungsversuche zeigen, dass Systeme lahmgelegt oder infiziert werden und Informationen in die falschen Hände gelangen können. Dem gilt es wirksam zu begegnen, da in der öffentlichen Verwaltung – neben dem Gebot der Aufrechterhaltung der Funktionsfähigkeit – Daten von Bürgerinnen und Bürgern, Unternehmen und Verbänden, eigenen Mitarbeiterinnen und Mitarbeitern vorhanden sind, die im höchsten Maße sensibel sind und daher eines angemessenen und umfassenden Schutzes bedürfen.

Mit diesem Gesetz werden daher alle Behörden verpflichtet in einem angemessenen Umfang die Sicherheit der informationstechnischen Systeme zu gewährleisten. Gleichzeitig wird der zentrale IT-Dienstleister, soweit informationstechnische Systeme mit dem Landesdatennetz verbunden sind, ermächtigt, neben den etablierten technischen Verfahren wie portbasierten Firewalls, Virenscannern und Proxy-Servern – weitergehende Maßnahmen durchzuführen, die das allgemeine Persönlichkeitsrecht in Artikel 2 Absatz 1 in Verbindung mit Artikel 1 GG sowie das Fernmeldegeheimnis in Artikel 10 GG und Artikel 17 der Verfassung des Saarlandes berühren bzw. einschränken. Der Bedeutung der Grundrechtsrelevanz entsprechend ist ein mehrstufiges Verfahren vorgesehen.

Rein vorsorglich wird diese Ermächtigung ergänzend allen Behörden für ihre lokalen Netze eingeräumt.

Der Gesetzentwurf befindet sich im Einklang mit der Verordnung (EU) 2016/679 (EU-DSGVO). Er ist sogar die logische Konsequenz aus Artikel 32 EU-DSGVO, der die Sicherheit der Verarbeitung personenbezogener Daten durch geeignete technische und organisatorische Maßnahmen fordert.

Artikel 1 des Gesetzentwurfs orientiert sich in seinem materiellen Regelungsgehalt an vorhandenen Vorschriften im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885), sowie am Gesetz zur Errichtung des Landesamtes für Sicherheit in der Informationstechnik vom 27. November 2017 des Landes Bayern (GVBl. S. 518) und an Referentenentwürfen zum Thema Informationssicherheit anderer Bundesländer.

Artikel 2 setzt die Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen um. Öffentliche saarländische Auftraggeber europaweiter Vergabeverfahren werden durch die EU-Vorgaben verpflichtet, elektronische Rechnungen zu geschlossenen Verträgen über Lieferungen und Leistungen spätestens ab dem 18. April 2020 empfangen und verarbeiten zu können. Die Verpflichtung zum Empfang und zur Verarbeitung elektronischer Rechnungen wird in diesem Gesetzentwurf auch auf den sogenannten unterschwelligen Bereich, also für Vergaben und Auftragshöhen unterhalb der jeweils maßgeblichen EU-Schwellenwerte ausgedehnt, um eine Vereinfachung und Standardisierung des Rechnungsstellungverfahrens insgesamt zu gewährleisten, die Möglichkeit der Interoperabilität zwischen verschiedenen Rechnungsstellungs- und Rechnungsbearbeitungssystemen zu schaffen und letztlich das elektronische Rechnungswesen überhaupt wirtschaftlich zu machen.

Um die künftige Weiterentwicklung des E-Governments zu erleichtern, soll außerdem eine Experimentierklausel für Pilotprojekte zur Einführung neuer E-Government-Anwendungen geschaffen werden.

Artikel 3 (Änderung des Saarländischen Besoldungsgesetzes) wurde aufgrund organisationsrechtlicher Veränderungen aufgenommen.

2. Finanzielle Auswirkungen

Die bereits erfolgte und weiterhin fortschreitende Digitalisierung der Gesellschaft und damit auch der Verwaltung führt einerseits zu vielen neuen Möglichkeiten, birgt gleichzeitig aber auch neue Risiken beispielsweise durch Schadprogramme oder Hackerangriffe. Die Verwaltung kann und will sich der Fortentwicklung aber schon aufgrund der dadurch entstehenden Möglichkeiten zur Rationalisierung und Beschleunigung des Verwaltungshandels sowie des damit verbundenen Komfortgewinns für Bürgerinnen, Bürger und Unternehmen aber auch für ihre Beschäftigten nicht verschließen. Entsprechende Ziele hat die saarländische Landesregierung bereits im Koalitionsvertrag und der Digitalisierungsstrategie dargelegt. Diese Ziele sind nur unter Einsatz neuer Techniken erreichbar und bedürfen angesichts ständig wachsender Bedrohungen in der digitalen Welt zunehmend sicherheitstechnischer Vorkehrungen zu deren Gewährleistung. Sowohl zur Erreichung der Ziele als auch zum sicheren Betrieb sind auf Verwaltungsseite zusätzliche finanzielle und personelle Aufwände erforderlich.

2.1. Finanzielle Auswirkungen für Bürgerinnen, Bürger und Wirtschaft

Artikel 1 bleibt gegenüber Bürgerinnen, Bürgern, Unternehmen und Verbänden ohne unmittelbare Auswirkungen und erzeugt dort keinerlei Handlungsbedarf. Artikel 1 bleibt für diese ohne finanzielle Auswirkungen.

Artikel 2 setzt die verpflichtende Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen um. Schon in der Entstehung der EU-Richtlinie wurde davon ausgegangen, dass die medienbruchfreie elektronische Rechnungslegung sowohl auf Seiten der Verwaltung, aber vor allem auch auf Seiten der unternehmerisch Tätigen erhebliche Rationalisierungs- und Einsparpotenziale bietet, die vorlaufende Investitionen sehr schnell amortisieren.

Bürgerinnen und Bürger, die gegenüber der Verwaltung nicht unternehmerisch tätig sind, sind von Artikel 2 nicht betroffen.

2.2. Finanzielle Auswirkungen für die öffentlichen Haushalte

Um die mit elektronischem Verwaltungshandeln verbundenen Risiken hinsichtlich der in der öffentlichen Verwaltung vorhandenen sensiblen Daten von Bürgerinnen, Bürgern und Unternehmen aber auch hinsichtlich der jederzeitigen Handlungsfähigkeit der Verwaltung selbst auf ein unumgängliches Maß zu beschränken, sind neue Techniken und Handlungsweisen notwendig.

Die Ermittlung der finanziellen Auswirkungen gestaltet sich schwierig. Zur Gewährleistung einer ausreichenden Informationssicherheit sind auch ohne den vorliegenden Gesetzentwurf zusätzliche Anstrengungen erforderlich und Kosten zu erwarten. Durch die Schaffung eines klaren rechtlichen Rahmens werden Standards und Strukturen vorgegeben, die insgesamt zu einer Kostendämpfung beitragen. Bei den behördenübergreifenden Pflichten nach § 3 Absatz 1 sind Verhältnismäßigkeit und Angemessenheit zu berücksichtigen. Soweit die kommunale Ebene betroffen ist, wird hierdurch keine Konnexität ausgelöst. Als Anschubfinanzierung werden für die Erstellung von Informationssicherheitskonzepten in Absprache mit der kommunalen Ebene Bedarfszuweisungen durch das Ministerium für Inneres, Bauen und Sport gewährt. Die Einbindung der kommunalen Ebene in das CERT nach § 3 Absatz 2 führt nicht zu nennenswerten Mehrkosten. Einzelheiten sind in der Begründung zu Artikel 1 § 3 Absatz 2 ausgeführt. Die dem zentralen IT-Dienstleister in Artikel 1 §§ 4 bis 7 zugewiesenen Aufgaben beinhalten zum einen die Installation der technischen Komponenten sowie zum anderen die für die Auswertungen notwendigen Mitarbeiterinnen/Mitarbeiter mit entsprechender Qualifikation.

Die rein vorsorgliche Ermächtigung für alle Behörden im Artikel 1 § 11 des Gesetzentwurfs führt nicht unmittelbar zu finanziellen Folgen, sondern erst wenn von dieser Ermächtigung Gebrauch gemacht wird. Eine Verpflichtung besteht nur, soweit ein unmittelbarer Anschluss an die Netze des Bundes (NdB, früher: Deutschland Online Infrastruktur, DOI) besteht und die Vorgaben des IT-Planungsrates zu erfüllen sind.

Artikel 2 erfordert auf Seiten der Verwaltung ein IT-Verfahren, das E-Rechnungen zu geschlossenen Verträgen über Lieferungen und Leistungen entgegennehmen und mindestens visualisieren kann (Webportal/E-Poststelle und Ablage für E-Rechnungen), das im Idealfall auch einen Workflow zur Rechnungsbearbeitung beinhaltet.

Konnexitätsaspekte kommen durch die Verpflichtung der kommunalen Ebene im EU-unterschwelligen Bereich nicht zum Tragen. Zwar gibt es hierzu keine gesetzliche Verpflichtung einer höheren Ebene, sodass das Land insoweit einen eigenen Gestaltungsspielraum nutzt.

Nach Artikel 120 der Verfassung des Saarlandes können nur durch förmliches Gesetz den Gemeinden und Gemeindeverbänden staatliche Aufgaben zur Durchführung übertragen und die Erfüllung von Selbstverwaltungsaufgaben zur Pflicht gemacht werden, wenn dabei gleichzeitig Bestimmungen über die Deckung der Kosten getroffen werden. Allerdings handelt es sich bei der durch dieses Gesetz bzw. der aufgrund dieses Gesetzes in der noch zu erlassenden Rechtsverordnung geregelten Entgegennahme und Behandlung elektronischer Rechnungen nicht um die Übertragung einer neuen Aufgabe, sondern als Ausgestaltung der kommunalen Haushalts- und Rechnungsführung um rein organisatorische Vorgaben, bei denen die Anwendung des Konnexitätsprinzips ausgeschlossen ist. Hinzu kommt, dass die Vorgaben zum elektronischen Rechnungsempfang bei Erreichen der EU-Schwellenwerte durch EU-Recht ohnehin vorgegeben sind und eine Differenzierung je nach Rechnungshöhe auch bei den Kommunen zu einem wirtschaftlichen und organisatorischen Mehraufwand führen würde.

Eine solide Kostenschätzung ist derzeit nicht möglich und hängt davon ab, welches konkrete IT-Verfahren gewählt wird, ob eine Ein- oder Anbindung zu bereits vorhandenen Verfahren möglich ist und inwieweit Ebenen übergreifende Lösungen möglich sind. Nähere Angaben zu den Kosten sind daher erst im Zusammenhang mit der nach Artikel 2 § 10a Absatz 3 zu erlassenden Rechtsverordnung und nach Abstimmung einer anzustrebenden gemeinsamen Lösung mit der kommunalen Ebene im IT-Kooperationsrat möglich.

Mit der Einführung der E-Rechnung sind aber auch erhebliche Einsparungen zu erwarten, wenn die vollständige Rechnungsbearbeitung in der Verwaltung elektronisch durchgeführt wird.

Artikel 3 führt im Ergebnis zu einer Ersparnis in Höhe von 93.000 € jährlich, da die Funktionen des Leiters des Landesamtes für Zentrale Dienste und des Leiters der Stabsstelle Informationssicherheitsmanagement und IT-Recht mit der dort verorteten Funktion des Landesinformationssicherheitsbeauftragten bisher jeweils von Beamten in der Besoldungsgruppe B 4 wahrgenommen wurden und nunmehr verbunden werden.

B. Im Einzelnen

Zu Artikel 1:

Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsstruktur des Landes (Informationssicherheitsgesetz Saarland – IT-SiG SL)

Zu § 1: Zweck und Geltungsbereich

Die Vorschrift beschreibt als Gesetzeszweck die Gewährleistung der Informationssicherheit in den Behörden des Saarlandes, wobei der Begriff der Informationssicherheit in den Legaldefinitionen in § 2 beschrieben wird.

Geschützt werden sollen alle in den saarländischen Verwaltungen vorhandenen Infrastrukturen, Geräte, genutzte Anwendungen und darüber verarbeitete Informationen, um auch die Daten der Bürgerinnen, Bürger und Unternehmen entsprechend zu sichern.

In den Sätzen 2 bis 4 wird der Geltungsbereich definiert. Dieser erfasst dabei über den Geltungsbereich des Saarländischen Verwaltungsverfahrensgesetzes (SVwVfG) hinaus auch die privatrechtlichen Tätigkeiten der Behörden.

In Satz 5 wird klargestellt, dass der Anwendungsbereich auch die Gerichte und Staatsanwaltschaften umfasst, soweit die Voraussetzungen von Satz 1 vorliegen.

Zu § 2: Begriffsbestimmungen

In § 2 werden zentral die im Gesetz verwendeten Begriffe definiert.

Zu § 3: Behördenübergreifende Pflichten

Zu Absatz 1:

Absatz 1 enthält Basisregelungen zur effektiven Gewährleistung der Informationssicherheit im Interesse von Bürgerinnen, Bürgern, Unternehmen und Verwaltung. Er knüpft an die Regelung in § 2 Absatz 3 des E-Government-Gesetzes Saarland an und erweitert und konkretisiert die Aufgaben zur Gewährleistung der Informationssicherheit.

Mit Satz 1 wird die Gewährleistung von Informationssicherheit in der öffentlichen Verwaltung als öffentliche Aufgabe definiert. Die Norm verpflichtet die Behörden nach dem Stand der Technik sowie den Vorschriften der EU-DSGVO und des Saarländischen Datenschutzgesetzes (SDSG) im Rahmen der Verhältnismäßigkeit zur Gewährleistung von Informationssicherheit. Im Rahmen der Prüfung der Verhältnismäßigkeit sind Art und Ausmaß des Risikos, die Wahrscheinlichkeit des Risikoeintritts und die Kosten der Risikovermeidung abzuwägen. Unter dem Gesichtspunkt der Wirtschaftlichkeit kann auch die Leistungsfähigkeit der jeweiligen Behörde berücksichtigt werden, da diese nach wie vor in der Lage sein muss, ihre jeweiligen öffentlichen Aufgaben zu erfüllen.

Zur Umsetzung von Satz 1 verpflichtet Satz 2 1. Halbsatz die Behörden, die Sicherheit ihrer informationstechnischen Systeme durch angemessene technisch-organisatorische Maßnahmen sicherzustellen.

Satz 2 2. Halbsatz verpflichtet die Behörden, Informationssicherheitskonzepte zu erstellen. Die Regelung setzt die Verpflichtung des Saarlandes aufgrund des 10. IT-Planungsrat-Beschlusses 2013/01 um, der die Einführung von Informationssicherheitskonzepten für staatliche Behörden verbindlich vorschreibt und den Kommunen empfiehlt. Im Übrigen ergeben sich diese Verpflichtungen aus Artikel 32 der EU-Datenschutz-Grundverordnung und dem Grundsatz des rechtmäßigen Verwaltungshandelns insoweit auch unmittelbar für die kommunale Ebene. Als anerkannte Methoden kommen hierbei die ISO-Normen der 27000er-Reihe, der BSI-Grundschutz und für Kommunen mit bis zu 500 Mitarbeitern die ISIS12-Methodik in Betracht bzw. branchenspezifische rechtliche oder methodische Regelungen wie bspw. im Bereich der Sparkassen (z.B. KWG, MaRisk, BAIT, PSD II). Nach aktuellem Stand wird vom IT-Planungsrat für Kommunen mit bis zu 500 Mitarbeitern die ISIS12-Methodik anerkannt, im Übrigen die BSI-Standards in Verbindung mit dem BSI-Grundschutz. Der vorliegende Gesetzentwurf schreibt bewusst keine der anerkannten Methoden als einzig verbindlichen Standard vor, geht allerdings davon aus, dass sich die Praxis an den jeweils aktuellen Vorgaben und Empfehlungen des IT-Planungsrates orientiert.

Die finanziellen Auswirkungen sind im Einzelnen nicht abschätzbar, da zum einen durch die Koppelung der Informationssicherheit an das Verhältnismäßigkeitsgebot klargestellt wird, dass auch Sicherheitsmaßnahmen einer Aufwands-Nutzen-Betrachtung unterliegen, zum anderen in den einzelnen Behörden unterschiedliche Risiken zu bewerten sind und unterschiedliche Reifegrade bei der Gewährleistung der Informationssicherheit bereits erreicht sind. Zur Gewährleistung einer ausreichenden Informationssicherheit sind auch ohne den vorliegenden Gesetzentwurf zusätzliche Anstrengungen erforderlich und Kosten zu erwarten. Durch die Schaffung eines klaren rechtlichen Rahmens werden Standards und Strukturen vorgegeben, die insgesamt zu einer Kostendämpfung beitragen.

Im Bereich der Landesverwaltung wird der Prozess durch die Stabsstelle Informationssicherheitsmanagement und IT-Recht und das IT-Dienstleistungszentrum unterstützt. Mit der vorgesehenen fortschreitenden Migration und Zentralisierung der IT zum IT-Dienstleistungszentrum wird der Aufwand vor Ort sich weiter reduzieren.

Für den kommunalen Bereich wird durch die Regelung des Absatzes 1 keine Konnexität ausgelöst, da es sich nicht um die Übertragung einer neuen Aufgabe handelt, sondern lediglich um Anforderungen, die aus dem Betrieb der elektronischen Systeme erwachsen.

Bezüglich der Abschätzung der finanziellen Auswirkungen gelten die Ausführungen bezüglich der Landesverwaltung entsprechend.

Zur Anschubfinanzierung der Implementierung von Informationssicherheit nach der ISIS12-Methodik wird das Ministerium für Inneres, Bauen und Sport in Absprache mit der kommunalen Ebene Bedarfszuweisungen bis zu einer Höhe von 50 % der hierdurch entstehenden Kosten, maximal 15.000,- Euro, gewähren, als Ersteinstieg auch bei kommunalen Behörden mit mehr als 500 Mitarbeitern.

Zu Absatz 2:

Absatz 2 knüpft an das bestehende Computersicherheits-Ereignis und Reaktionsteam (CERT, Computer Emergency Response Team) an, das vom Saarland in Kooperation mit Rheinland-Pfalz betrieben wird und in das die kommunale Ebene im Saarland eingebunden ist. Als Bestandteil der Gewährleistung der Informationssicherheit löst die Einbindung der kommunalen Ebene in das CERT ebenfalls keine Konnexität aus. Die finanziellen Auswirkungen auf die kommunale Ebene sind gering. Im Rahmen der bestehenden Kooperation mit dem Landesbetrieb für Daten und Information (LDI) des Landes Rheinland-Pfalz wird dieses den Warn- und Informationsdienst für die kommunale Ebene im Rahmen einer Vereinbarung mit dem eGo-Saar für einen jährlichen Betrag unter 10.000,- Euro wahrnehmen. Die unmittelbaren Verpflichtungen der kommunalen Ebene beschränken sich dabei auf die Erstermittlung und Mitteilung vorhandener Hard- und Software an das LDI über den eGo-Saar, die Sichtung von über den eGo-Saar eingehenden Meldungen aus dem LDI, gegebenenfalls Informationsweitergabe innerhalb der Behörde sowie Meldung von etwaigen Sicherheitsvorfällen von allgemeiner Bedeutung an den CERT-Verbund. Zentrale Anlaufstelle im Saarland ist hierfür das Informationssicherheitsteam beim zentralen IT-Dienstleister des Landes. Die Regelung in Absatz 2 stellt klar, dass zum Funktionieren des CERT die zeitnahe Information über sicherheitsrelevante Vorfälle gehört und verpflichtet alle Behörden zu entsprechenden Meldungen.

Die Verpflichtung zur Meldung an das CERT der Landesverwaltung entfällt, wenn für die Behörde bereits eine Meldepflicht im Rahmen eines anderen deutschen CERT-Verbundes besteht, wie dies bspw. bei der Deutschen Rentenversicherung oder im Bereich der Sparkassen gegeben ist.

Zu § 4: Abwehr von Gefahren für die Informationssicherheit

Zu Absatz 1:

Absatz 1 stellt die zentrale Befugnisnorm für den zentralen IT-Dienstleister dar, um die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Behördennetzes etwa durch Schadprogramme oder programmtechnische Sicherheitslücken, unbefugte Datennutzung oder unbefugte Datennutzung durch Dritte effektiv und effizient mit technischen Mitteln zu ermöglichen.

Effektive Gefahrenabwehr kann nur durch ein einheitlich hohes Schutzniveau gewährleistet werden. Das beste Informationssicherheitskonzept einer Behörde ist nutzlos, wenn ein Angreifer durch nicht ausreichend gesicherte Kanäle einer anderen Behörde in das gesamte Netz eindringen kann.

Daher darf der zentrale IT-Dienstleister zur Gefahrenabwehr gegenüber allen Behörden, deren informationstechnische Systeme mit dem Landesdatennetz verbunden sind, die notwendigen und angemessenen Maßnahmen ergreifen. Nur so kann ein homogenes Qualitätsniveau der Informationssicherheit gewährleistet werden. Bei den zu ergreifenden Maßnahmen ist der Verhältnismäßigkeitsgrundsatz zu beachten, insbesondere ist stets das mildeste Mittel zur Erreichung des Zwecks zu wählen.

Ein informationstechnisches System gilt im Sinne dieses Gesetzes mit dem Landesdatennetz verbunden, wenn es direkt oder über ein behördeneigenes Subnetz (z.B. lokale Netze) technisch angeschlossen ist. Auch die Anbindung an das Landesdatennetz über einen Dritten, der auch ein IT-Dienstleister in einer Rechtsform des Privatrechts sein kann, ist vom Geltungsbereich erfasst. Mit der Realisierung des geplanten gemeinsamen Netzes von Land und kommunaler Ebene, ist auch diese vom Geltungsbereich des Gesetzes erfasst.

Nicht verbunden mit dem Landesdatennetz sind informationstechnische Systeme, die nur über das Internet erreichbar sind. Netze von Verwaltungen außerhalb des Saarlandes einschließlich des Verbindungsnetzes zwischen den Landesdatennetzen sind im Sinne dieses Gesetzes nicht mit dem Landesdatennetz verbunden.

Die datenschutzrechtliche Generalklausel des Satzes 2 dient dem legitimen Datenzugriff zur Gefahrenabwehr. Soweit der zentrale IT-Dienstleister auf Systeme zugreifen muss, um etwa Schadprogramme zu entfernen, könnte er hierbei auf personenbezogene Daten stoßen. Eine Einwilligung ist in diesen Fällen nicht immer oder nicht rechtzeitig wirksam einzuholen, wenn Gefahr in Verzug vorliegt. Wie sich aus Satz 1 ergibt, beschränkt sich die Datennutzung bzw. -verarbeitung auf das Notwendige.

Zu Absatz 2:

Absatz 2 konkretisiert die Generalbefugnis. Danach kann der zentrale IT-Dienstleister Protokolldaten und Inhaltsdaten, die beim Betrieb von Informationstechnik des Landes sowie an den Schnittstellen des Landesdatennetzes und anderen Netzen und innerhalb des Landesdatennetzes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Informationstechnik, von Angriffen auf die Informationstechnik, zur Abwehr von unbefugter Datennutzung oder -verarbeitung oder sonstigen Gefahren erforderlich ist.

Die Erforderlichkeit stellt dabei eine Relevanzgrenze dar. Informationen – beispielsweise Zugriffe auf Verzeichnisdienste oder Zugriffsprotokolldaten der Polizei – , die für eine effiziente Abwehr von Schadprogrammen oder anderen Angriffen nicht von Bedeutung sind, dürfen nicht erhoben und ausgewertet werden.

Bei Protokolldaten handelt es sich um sogenannte Logfiles von Servern, Firewalls, Web-Proxys etc. Diese Logfiles protokollieren sogenannte Events, also Ereignisse über Anfragen von anderen Systemen, Softwareänderungen, Fehlermeldungen etc.. Sie enthalten keine Inhaltsdaten.

Setzt man Protokolldaten verschiedener Systeme in Korrelation und wertet diese aus, so können Unregelmäßigkeiten und damit potentielle Bedrohungen erkannt werden. Protokolldateien, die für die Abwehr von Gefahren interessant sind, können unter anderem sein:

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

- Protokolldateien von Systemen zur Erkennung und Beseitigung von Schadsoftware einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen des betroffenen Systems, ausgegebener Meldung sowie Informationen über die Schadsoftware und die als Schadprogramm erkannten Daten;

- Protokolldateien von Systemen zur Erkennung von unerwünschten E-Mails einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen von ein- und ausgehenden Verbindungen, E-Mailadresse des Absenders und Empfängers einer Nachricht, deren Größe und eindeutiger Identifikationsnummer sowie Fehler- und sonstige Statusmeldungen und die als Schadprogramm erkannten Daten;

- Protokolldateien von Datenbankservern einschließlich Erhebungszeitpunkt, Anmeldename, IP-Adresse und vollständigem Domänennamen von Verbindungen und die Identifikationsnummer der ausgegebenen Meldung und deren Klartext;

- Protokolldateien von Web- und Proxyservern einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen von ein- und ausgehenden Verbindungen sowie dem einheitlichen Ressourcenbezeichner (Universal Resource Identifier = URI wie beispielsweise in Form eines Uniform Resource Locator = URL) und Kopfdaten und

- Protokolldateien der Betriebssoftware von Computersystemen einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen des betroffenen Computersystems, Namen des Programms oder Systemdiensts sowie dessen Typ, die Identifikationsnummer der ausgegebenen Meldung und deren Klartext.

Nach der Regelung kann der zentrale IT-Dienstleister auch die an den Schnittstellen zwischen dem Behördennetz und öffentlichen Netzen anfallenden Daten erheben und automatisiert auswerten. Die Vorschrift erlaubt eine sofortige Analyse des in das Landesdatennetz eindringenden Datenverkehrs. Damit sollen Schadprogramme bereits am Übergang vom Internet zum Behördennetz erkannt und abgewehrt werden. Davon umfasst ist auch der Zugriff auf (technische) Telekommunikationsinhalte. Nur so können gefährliche Dateianhänge oder Links zu Internetseiten, die ihrerseits Schadsoftware einzuschleusen versuchen, analysiert und abgewehrt werden. Die automatisierte Auswertung gestattet nicht die Speicherung der Inhalte über den für die technische Abwicklung des Kommunikations- und Erkennungsvorgangs ohnehin notwendigen Umfang hinaus.

Zu Absatz 3:

Absatz 3 stellt aus Datenschutzgründen klar, dass dem zentralen IT-Dienstleister auch Protokolldaten zur Verfügung gestellt werden können, die in lokalen Netzen gespeichert sind, soweit diese an das Landesdatennetz angeschlossen sind.

Zu Absatz 4:

Die Norm stellt klar, dass Daten, die Personenbezug aufweisen oder dem Fernmeldegeheimnis unterliegen, bei der automatisierten Auswertung nach Absatz 2 grundsätzlich nicht über die Dauer der automatisierten Auswertung hinaus gespeichert werden dürfen und sofort und spurlos zu löschen sind. Damit werden die Anforderungen des Bundesverfassungsgerichts aus dem Urteil zur automatisierten Erfassung von Kfz-Kennzeichen erfüllt (BVerfG in BVerfGE 120, 378 ff.). Die Speicherung und sonstige Verarbeitung nach dem ursprünglichen Verwendungszweck bleiben hiervon unberührt.

Zu Absatz 5:

Absatz 5 zeigt die strenge Zweckbindung auf und verbietet insbesondere, dass die Daten für Leistungskontrollen oder Ähnliches verwendet werden dürfen.

Zu § 5: Auswertung von Protokolldaten

Die Vorschrift regelt den Umgang mit Protokolldaten.

Zu Absatz 1:

Protokolldaten können für einen erforderlichen Zeitraum gespeichert werden. Voraussetzung ist, dass tatsächliche Anhaltspunkte bestehen, die für den Fall der Bestätigung eines Verdachts nach § 7 Absatz 1 Nummer 1 zur Abwehr von Gefahren für die Informationstechnik erforderlich sein können. Daher handelt es sich um das sogenannte Quick-Freeze-Verfahren, bei dem die Speicherung nicht anlasslos, sondern nur im Einzelfall und erst zu dem Zeitpunkt stattfindet, zu dem ein tatsächlicher Anhaltspunkt gegeben ist (vgl. BVerfG 1 BvR 256/08 in NJW 2010, 833, RNummer 208). Tatsächliche Anhaltspunkte liegen vor, wenn es möglich ist, dass die Protokolldaten zur Gefahrenabwehr erforderlich sein könnten. Der Begriff orientiert sich am Anfangsverdacht gemäß § 152 Absatz 2 StPO.

Die staatliche IT-Infrastruktur ist zu schützen. Zum einen können dort sensible Informationen wie Steuer- oder Gesundheitsdaten von Bürgern und Unternehmen abgegriffen werden. Zum anderen ist die IT für eine funktionierende Staatsverwaltung und damit für die Sicherheit des Staates von elementarer Bedeutung. Bereits heute würden bei einem Ausfall die überwiegende Anzahl von Verwaltungsverfahren nicht mehr bearbeitet werden können.

Das Prüfen der Protokolldaten ist geeignet, Angriffe zu erkennen und abzuwehren. Dies erfordert nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt lediglich, dass die Zweckerreichung gefördert wird (vgl. BVerfGE 1 BvR 256/08 in NJW 2010, 833, Rn 207 m.w.N.). Des Weiteren ist es das mildeste, weil zugleich das einzige Mittel, um gefährlichen Datenverkehr von außen an einem Eindringen in die Systeme zu hindern. Weniger einschneidende Mittel, die ebenso weitreichende Aufklärungsmaßnahmen ermöglichen, sind nicht ersichtlich.

Die Maßnahme ist auch verhältnismäßig im engeren Sinne, das heißt angemessen. Darüber hinaus wird das Recht auf informationelle Selbstbestimmung durch die Sicherstellung einer automatisierten Erkennung sowie einer Pseudonymisierung der Daten nach Absatz 2 geschützt.

Nach Absatz 1 Satz 2 ist eine Speicherung von Protokolldaten auch möglich, wenn die Daten zur Verfolgung damit zusammenhängender Straftaten erforderlich sein können. Die Regelung erlaubt die Speicherung von Daten, die beispielsweise bei einem versuchten Cyberangriff auf die IT-Infrastruktur angefallen sind. Nur so wird dem Land und anderen an das Landesdatennetz angeschlossenen Stellen als Geschädigtem die Möglichkeit gegeben, strafrechtliche Ermittlungen einleiten zu lassen.

Zu Absatz 2:

Absatz 2 regelt die Anforderungen an die Datensicherheit. Demnach müssen die organisatorischen und technischen Maßnahmen zur Sicherstellung einer automatisierten Auswertung zu jeder Zeit dem Stand der Technik entsprechen. Die einfachgesetzliche Rechtsfigur des Stands der Technik erfüllt die Vorgaben des Bundesverfassungsgerichts (vgl. BVerfG in NJW 2010, 833 ff., Rn. 224).

Im Hinblick auf mögliche weitergehende Befugnisse in den folgenden Vorschriften wird klargestellt, dass zunächst nur eine automatisierte Auswertung erfolgt und die Daten zu pseudonymisieren sind.

Zu Absatz 3:

Absatz 3 stellt klar, dass bei einem Verdachtsfall auf eine Gefährdung der Informationssicherheit und zur weiteren Analyse die Wiederherstellung des Personenbezugs der pseudonymisierten Daten die Entscheidung hierzu der Leitungsebene vorbehalten und zu dokumentieren ist. Bei Satz 3 handelt es sich um eine Rechtsgrundverweisung auf die nachfolgenden Vorschriften.

Zu § 6: Auswertung von Inhaltsdaten

Zu Absatz 1:

Absatz 1 regelt den Umgang mit Inhaltsdaten, die einer restriktiveren Regelung bedürfen. Dabei darf der Gesetzgeber bei der Entscheidung, wie weit solche Daten zu löschen oder zu speichern sind, einen Interessenausgleich vornehmen und die Belange staatlicher Aufgabenwahrnehmung berücksichtigen (vgl. BVerfGE 1 BvR 256/08 in NJW 2010, 833, Rn. 217). Eine Speicherung solcher Daten für zwei Monate ist zulässig und angemessen, da sie nur bei gesteigertem Risiko oder bei Vorliegen einer konkreten Gefahrenlage erfolgt (vgl. BVerfGE 120, 378).

Aufgrund der Sensibilität der Daten ist die Maßnahme durch die Behördenleitung und einen Bediensteten mit der Befähigung zum Richteramt anzuordnen. Das Vier-Augen-Prinzip und die Einschätzung eines Juristen soll die Wahrung der Verhältnismäßigkeit sicherstellen.

Zu Absatz 2:

Die Anordnung ist zeitlich beschränkt (vgl. EuGH C-293/12, RN. 59). Sie gilt längstens 2 Monate, kann aber erforderlichenfalls verlängert werden. Klarstellend wird angemerkt, dass sich ein Ablauf der Anordnung nicht auf die Speicherfrist auswirkt, d. h. die Daten sind unabhängig von ihrer Speicheranordnung max. 2 Monate speicherbar. Darüber hinaus ist eine Speicherung nur zulässig, wenn dies zum Schutz der technischen Systeme unerlässlich ist. Im Gegensatz zur Erforderlichkeit aus den §§ 4 und 5 ist die Hürde bei der Unerlässlichkeit nochmals erhöht.

Zu § 7: Weitergehende Auswertungen

Zu Absatz 1:

Liegt ein hinreichender Verdacht vor, so können weitere, auch nicht automatisierte Maßnahmen folgen. Dazu dürfen die Daten über die §§ 5 und 6 hinaus verarbeitet werden. Notwendige Untersuchungen der Daten sind zulässig, um einen Verdacht, dass die Daten eine Gefahr für die Informationssicherheit etwa durch ein Schadprogramm, Sicherheitslücken, Angriffe oder unbefugten Datenzugriff enthalten, zu bestätigen oder zu widerlegen.

Hat sich der Verdacht, dass die Daten Gefahren für die Informationstechnik enthalten bestätigt, so ist eine weitere Verarbeitung der Daten, etwa zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme zulässig, soweit dies erforderlich ist. Beispielsweise kann die Funktionsweise einer Schadsoftware untersucht oder ihre Signatur in Datenbanken von Anti-Viren-Software aufgenommen werden.

Ein hinreichender Verdacht liegt vor, wenn Anhaltspunkte gegeben sind, die das Szenario, dass die Daten durch einen Angriff oder ein Schadprogramm verursacht wurden oder sich aus ihnen entsprechende Hinweise ergeben, wahrscheinlicher erscheinen lässt als das Szenario, dass dies nicht der Fall ist. Der Begriff orientiert sich am hinreichenden Tatverdacht nach § 170 Absatz 1 StPO.

Während die §§ 5 und 6 lediglich eine automatisierte Auswertung und nicht personenbezogene Verwendung von Daten zulassen, kann sich § 7 auch auf die inhaltliche Prüfung von Dokumenten, beispielsweise nach Schadcode, beziehen. Zur Gewährleistung der richterlichen Unabhängigkeit ist daher, wenn Daten verarbeitet werden, welche die richterliche Unabhängigkeit berühren, nach Satz 2 der jeweils zuständigen obersten Dienstbehörde zu berichten. Darüber hinaus sind nach Satz 3 unabhängige Stellen wie die oder der Landesbeauftragte für Datenschutz und die auch anderweitig hervorgehobenen geschützten Träger von Berufs- oder besonderen Amtsgeheimnissen zu unterrichten, soweit deren Datenverarbeitung berührt ist.

Zu Absatz 2:

Die Vorschrift stellt besondere Anforderungen an den Datenschutz, auch um die Verhältnismäßigkeit der Norm zu wahren.

Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen, soweit möglich, nicht erhoben werden. Aus Artikel 1 Absatz 1 Grundgesetz ergibt sich, dass ein Kernbereich privater Lebensgestaltung als absolut unantastbar geschützt ist (vgl. BVerfG in BVerfGE 119, 1ff.). Selbst sehr schwerwiegende Interessen der Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen; eine Abwägung findet nicht statt (vgl. BVerfG in BVerfGE 34, 238 ff.). Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität (vgl. BVerfG in BVerfGE 109, 279 ff.).

Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung dennoch erlangt, dürfen diese nicht verwendet werden und sind sofort und spurlos zu löschen (vgl. BVerfG in BVerfGE 120, 378 ff.). Die Erlangung und Löschung sind zu dokumentieren.

Zu § 8: Sicherheitskonzept

Zu Absatz 1:

§ 8 Absatz 1 sieht vor der Nutzung der Ermächtigungen in den §§ 4 bis 7 die Vorlage eines Sicherheitskonzepts für das von dem zentralen IT-Dienstleister verwendete System zur Datenverarbeitung nach den §§ 4 bis 7 vor. Alle in diesem Sicherheitskonzept vorgesehenen technischen und organisatorischen Maßnahmen müssen in einem Steuerungssystem dokumentiert, überwacht und fortgeschrieben werden. Die jeweilige Umsetzung muss in den Akten vermerkt werden, damit sichergestellt ist, dass alle Schritte, die in dem Sicherheitskonzept vorgesehen sind, beachtet worden sind.

Nach Satz 2 muss das Sicherheitskonzept vor jeder Veränderung der genutzten technischen Systeme an die Veränderung angepasst werden. Auf diesem Wege ist gewährleistet, dass das Sicherheitskonzept und das technische System jederzeit übereinstimmen.

Satz 3 sieht weiterhin vor, dass auch jede Veränderung des Sicherheitskonzepts den Anforderungen aus Satz 1 gerecht werden muss, wonach diese und die Umsetzung der technischen und organisatorischen Maßnahmen entsprechend in den Akten vermerkt werden.

Zu Absatz 2:

Artikel 1 § 4 ff. ermöglicht weitreichende Zugriffsrechte des zentralen IT-Dienstleisters in Form der Erhebung und automatisierten Auswertung von Protokoll- und Inhaltsdaten auch bei der LMS. Im Hinblick auf die grundrechtliche Stellung der LMS wie auch ihre datenschutzrechtlichen Funktionen im Verhältnis zu Anbietern, die ihrerseits den besonderen Schutz des Artikel 5 Absatz 1 Satz 2 GG genießen, wurde mit dem Absatz 2 der LMS ein Zustimmungsvorbehalt eingeräumt. Diese Regelung wurde vorsorglich aufgenommen, da die LMS zum Zeitpunkt des Gesetzgebungsverfahrens zwar noch nicht an das Landesdatennetz angebunden ist, dies jedoch in der Überlegung steht.

Zu § 9: Benachrichtigung der Betroffenen

Zu Absatz 1:

Absatz 1 sieht grundsätzlich eine Benachrichtigung der Betroffenen vor, deren Inhaltsdaten personenbezogen und nicht automatisiert ausgewertet wurden. Betroffene sind natürliche Personen, deren personenbezogene Daten betroffen sind. Grund für die Regelung ist eine mögliche Kenntnisnahme der Inhaltsdaten. Jede oder jeder Betroffene soll insofern wissen, wer welche Daten über sie oder ihn kennt und die Möglichkeit haben, Maßnahmen einer Rechtmäßigkeitskontrolle unterziehen zu können oder sich an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz zu wenden. Eingeschränkt wird dieses Recht jedoch dadurch, dass die Betroffenen bekannt sein müssen oder eine Identifikation mit einem verhältnismäßigen Aufwand möglich ist. Eine Benachrichtigung kann sonst unterbleiben.

Eine weitergehende Benachrichtigungspflicht wurde aus verschiedenen Gründen nicht aufgenommen. Es bedeutet einen erheblichen Aufwand, sämtliche Personen zu benachrichtigen, bei denen beispielsweise eine IP-Adresse erhoben wurde. Diese ist nicht automatisch mit einer E-Mail-Adresse hinterlegt. Zudem würde eine generelle Benachrichtigungspflicht für sämtliche Personen, deren personenbezogene Daten erhoben wurden, dazu führen, dass auch die „Angreifer“ also diejenigen, die Schadsoftware an die Behörden senden, benachrichtigt werden müssten. Es wäre paradox, die „Angreifer“ zu informieren, insbesondere wäre für diese dann klar, dass Schadprogramme nunmehr auf anderem Wege zugestellt werden müssen. Insofern wurde die Benachrichtigungspflicht deutlich eingeschränkt.

Über die datenschutzrechtlichen Belange hinaus ist auch eine Benachrichtigung der betroffenen Behörden vorgesehen. Diese sollen über die Einsichtnahme in personenbeziehbare und sonstige vertrauliche Daten, die mit ihrem Geschäftsbetrieb zusammenhängen, informiert werden. Neben der eigentlichen Information soll ihnen damit insbesondere die Gelegenheit gegeben werden, auf Sicherheitsvorfälle zu reagieren und zur künftigen Vermeidung beitragen zu können.

Satz 2 sieht weiterhin eine Einschränkung vor, wonach die Benachrichtigung unterbleiben kann, wenn sie eine Gefahr für die Ermittlungen in Straf- und Disziplinarverfahren bedeutet oder dadurch die Informationssicherheit gefährdet ist.

Zu Absatz 2:

Absatz 2 sieht für den Fall, in dem eine Benachrichtigung unterbleiben soll, ein Anordnungserfordernis durch eine Juristin oder einen Juristen und deren Dokumentation vor.

Zu § 10: Übermittlung personenbezogener Daten

Zu Absatz 1

Ein Angriff auf die staatliche Informationstechnik stellt zumeist auch eine Straftat (z. B. nach §§ 202a ff., 303a f. StGB) dar. Mit Absatz 1 wird dem zentralen IT-Dienstleister die datenschutzrechtliche Möglichkeit zur Datenübermittlung an Sicherheitsbehörden, Polizei und Strafverfolgungsbehörden eingeräumt. Zu beachten ist jedoch, dass nicht sämtliche Fälle übermittelt werden dürfen bzw. sollen. Im Bereich der Prävention beschränkt sich die Übermittlungsbefugnis auf die Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, und die Abwehr von Gefahren für Leib, Leben oder Freiheit sowie zur Verhütung und Unterbindung von Straftaten. Im Bereich der Repression wiederum besteht eine Übermittlungsbefugnis nur, soweit die Tatsachen, aus denen sich die Gefahr für die Informationstechnik ergibt, den Verdacht einer Straftat begründen oder soweit bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 StPO bezeichnete Straftat begangen hat.

Aufgenommen wurde auch eine Übermittlungsbefugnis an die Verfassungsschutzbehörde zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen.

Die Vorschrift stellt die Übermittlung in ein gewisses Ermessen des IT-Dienstleisters. Eine generelle Regelübermittlung an die Strafverfolgungsbehörden würde bei mehreren tausend versuchten Angriffen pro Tag deren Kapazitäten unnötig belasten. Es sollen nur Angriffe mit einem gewissen Grad an Erheblichkeit gemeldet und folglich nur diese Daten übermittelt werden.

Zu Absatz 2:

Absatz 2 sieht für die Übermittlung von Daten nach Absatz 1 Nummer 4 die vorherige Zustimmung einer Juristin bzw. eines Juristen vor. Die Entscheidung ist zu dokumentieren. Für die Übermittlung von Daten nach Absatz 1 Nummern 2 und 3 ist eine vorherige gerichtliche Zustimmung vorgesehen.

Zu § 11: Befugnisse bei lokalen Netzen

In § 11 werden jeder Behörde die Befugnisse nach den §§ 4 bis 10 für ihre jeweiligen lokalen Netze eingeräumt. Der zentrale IT-Dienstleister hat diesbezügliche keine Befugnisse soweit ihm die Aufgabe nicht im Rahmen der Migration der IT nach dem IT-DLZ-Gesetz oder durch ausdrücklichen Auftrag der jeweiligen Behörde übertragen ist. Es handelt sich um eine rein vorsorgliche Ermächtigung, mit der bisher keine entsprechende Vorgabe durch den IT-Planungsrat korrespondiert, sofern kein unmittelbarer Anschluss an die Netze des Bundes besteht.

Gleichzeitig wird durch die Einräumung der Befugnisse der Tatsache Rechnung getragen, dass die Grenzen zwischen klassischen Firewall-Systemen, die fast überall zum Einsatz kommen, und Intrusion-Detection-Systemen zunehmend fließend sind.

Zu § 12: Datenschutzrechtliche Kontrolle

Zu Absatz 1

Absatz 1 verpflichtet den zentralen IT-Dienstleister zur jährlichen Berichterstattung an die oder den Landesbeauftragten für Datenschutz über die nach § 5 Absatz 3, § 6, § 7 und § 10 erfolgten Verarbeitungen, um eine datenschutzrechtliche Kontrolle zu ermöglichen. Die Behörden nach § 11 sind von dieser Verpflichtung nicht betroffen, unbeschadet der Befugnisse der/des Landesbeauftragten für Datenschutz nach dem Saarländischen Datenschutzgesetz.

Zu Absatz 2

Absatz 2 sieht eine zweckgebundene Verwendung und zeitlich befristete Aufbewahrung der nach diesem Gesetz anzufertigenden Dokumente vor.

Zu § 13: Einschränkung von Grundrechten

Das Fernmeldegeheimnis könnte verletzt werden, wenn durch den zentralen IT-Dienstleister bzw. eine Behörde im Rahmen des § 11 des Gesetzentwurfs Daten eines Telekommunikationsvorgangs zwischen einem Bürger und einer Behörde ausgewertet werden.

Nach Artikel 19 Absatz 1 Satz 2 i. V. m. Artikel 10 Grundgesetz dürfen Beschränkungen des Fernmeldegeheimnisses nur auf Grund eines Gesetzes angeordnet werden, das wiederum das Grundrecht unter Angabe des Artikels nennen muss.

Gleiches ergibt sich aus Artikel 17 der Verfassung des Saarlandes.

Zu Artikel 2:

Änderung des E-Government-Gesetzes Saarland

Zu Nummer 1:

In Nummer 1 wird die durch die Änderung des Gesetzestextes erforderliche Anpassung vorgenommen.

Zu Nummer 2:

Die neu einzufügende Vorschrift des § 10a regelt den Rechnungseingang bei Auftraggebern. Hierdurch werden die Vorgaben der E-Rechnungsrichtlinie (RL 2014/55/EU vom 16. April 2014) auf formell-gesetzlicher Grundlage in enger Anlehnung an die bundesgesetzlichen Regelungen des Gesetzes zur Umsetzung der Richtlinie 2014/55/EU über die elektronische Rechnungsstellung im öffentlichen Auftragswesen vom 04. April 2017 (BGBl. I S. 770) auch in saarländisches Recht umgesetzt.

Absatz 1 enthält die Grundverpflichtung zum Empfang elektronischer Rechnungen im Sinne der nach Absatz 2 verbindlichen Begriffsdefinition. Den vom Anwendungsbereich der Vorschrift erfassten Auftraggebern bleibt es jedoch unbenommen, weitergehende Details für die elektronische Rechnungsstellung bei der Vergabe öffentlicher Aufträge vertraglich, gegebenenfalls auch im Rahmen übergreifender Rahmenverträge, zu vereinbaren.

Die Richtlinie ist für alle öffentlichen Auftraggeber, insbesondere auch für Konzessionsgeber und Sektorenauftraggeber, umzusetzen. Aus diesem Grund wird auf die entsprechenden Vorschriften im Gesetz gegen Wettbewerbsbeschränkungen (GWB) abgestellt. Es wird zudem klargestellt, dass die Verpflichtung nur für saarländische Auftraggeber gilt, die als Aufraggeber nach § 98 GWB einzustufen sind.

Dabei sind sowohl Aufträge oberhalb als auch unterhalb der maßgeblichen EU-Schwellenwerte erfasst. Dieses Vorgehen setzt zum einen die Vorgaben der o.g. Richtlinie vollständig um, erweitert aber zum anderen auch den Bereich der Verpflichtung auf den sog. unterschwelligen Bereich, wie es auch auf Bundesebene umgesetzt wurde. Das wird in Absatz 1 Satz 2 auch ausdrücklich klargestellt. Andernfalls ließe sich das Ziel, die Rechnungskommunikation im Sinne des Bürokratieabbaus und der verwaltungsinternen Prozessoptimierung zu vereinfachen, zu standardisieren und interoperabel auszugestalten, nur unzureichend gewährleisten. Insbesondere ist es aus Sicht der rechnungsstellenden Unternehmen nicht praktikabel, die Form der Rechnungsstellung von einer vorherigen Prüfung des Auftragswertes abhängig zu machen. Eine solche Differenzierung der Rechnungsstellung nach oberschwelligen und unterschwelligen Aufträgen würde für eine Vielzahl der betroffenen Unternehmen eine Umgestaltung der internen Buchhaltungssysteme erforderlich machen und damit zu einem unverhältnismäßigen Mehraufwand an Prüfpflichten führen.

Durch die Vorgaben der E-Rechnungsrichtlinie nicht vorgeprägt sind im Übrigen die Fallgestaltungen, in denen die Ausschreibung eines Rahmenvertrages im oberschwelligen Vergabebereich erfolgt, die nachfolgenden Abrufe hingegen den Schwellenwert für sich betrachtet unterschreiten. Auch bei diesen Fallgestaltungen ist es aus Gründen der Rechtsklarheit und Praktikabilität angezeigt, den Anwendungsbereich der Richtlinie für die Umsetzung zu erweitern. Diese Erweiterung hilft entsprechend dem Sinn und Zweck der E-Rechnungsrichtlinie, den Rechnungsstellungsprozess insgesamt unbürokratisch und einfach handhabbar auszugestalten.

Absatz 2 des Gesetzentwurfs enthält eine Definition des Begriffs „elektronische Rechnung“. Der Begriff der elektronischen Rechnung ist aus technischer Sicht nicht eindeutig und wird im allgemeinen Sprachgebrauch sowohl auf rein bildhafte Darstellungen als auch auf ausschließlich strukturierte Datenformate umfassende Rechnungen bezogen.

Eine Rechnung ist demgemäß nicht bereits dann elektronisch, wenn sie im PDF-Format versendet wurde, obgleich dies nach dem allgemeinen Sprachgebrauch so verstanden werden könnte. Ein solches Vorgehen stellt jedoch keine elektronische Rechnung im Sinne dieses Gesetzes dar. Erforderlich ist vielmehr, dass es sich um ein strukturiertes elektronisches Format handelt und dieses die automatische und vollständige elektronische Verarbeitung der Rechnung ermöglicht, heute üblicherweise ein XML-Format. Insofern muss die elektronische Rechnung so ausgestaltet sein, dass eine vollständige elektronische Verarbeitung möglich ist, sofern in den Behörden die entsprechenden Strukturen und Schnittstellen vorhanden sind.

Absatz 3 des Gesetzentwurfs ermächtigt, Einzelheiten der elektronischen Rechnungsstellung in einer Rechtsverordnung zu regeln, also das Verfahren der Verarbeitung, die Verwendung von Standards und die Möglichkeit von Ausnahmen.

Dies ist u. a. erforderlich, weil sich der technische Standard der elektronischen Rechnung aufgrund der technischen Entwicklung verändern kann. Die Ausgestaltung der Datenverarbeitung hat entsprechend den Vorgaben der Datenschutz-Grundverordnung zu erfolgen.

In Satz 2 wird der Umfang der Verordnungsermächtigung konkretisiert.

Nach Nummer 1 kann die Art und Weise des Empfangs und der Verarbeitung elektronischer Rechnungen näher ausgestaltet werden. Hier können z. B. die bereitzustellenden Übertragungswege oder das Formatprüfungsverfahren normiert werden.

Nummer 2 ermächtigt dazu, Anforderungen an die elektronischen Rechnungen zu stellen. Nur wenn diese Anforderungen vom Rechnungssteller erfüllt werden, müssen die elektronischen Rechnungen entgegengenommen werden. Wichtigster Punkt ist die Festlegung des Rechnungsdatenmodells, das aufgrund der Richtlinie 2014/55/EU in bestimmten Rahmen vorgegeben wird.

Nummer 3 ermächtigt dazu, die Erteilung elektronischer Rechnungen verpflichtend vorzusehen.

Nummer 4 erlaubt, für sicherheitsspezifische Aufträge Ausnahmen von der elektronischen Rechnungsstellung vorzusehen.

Zu Nummer 3:

Die neu anzufügende Vorschrift des § 21 beinhaltet eine Experimentierklausel in Anlehnung an vergleichbare Klauseln in § 9 des schleswig-holsteinischen E-Government-Gesetzes, in § 20 des sächsischen E-Government-Gesetzes und Artikel 10 des bayerischen E-Government-Gesetzes. Unter einer Experimentierklausel versteht man eine gesetzliche Regelung, die die Verwaltung dazu ermächtigt, bei ihrer Tätigkeit von gewissen Bestimmungen des geltenden Rechts abzuweichen, um neue Vorgehensweisen zu erproben und daraus Erkenntnisse zu gewinnen. Auf Basis der gesammelten Erfahrungen können erprobte Verfahren später endgültig normiert, entsprechende Bestimmungen überarbeitet oder neue Gesetze geschaffen werden. Die Experimentierklausel geht speziell im E-Government von folgenden Überlegungen aus:

Der Einsatz von Informations- und Kommunikationstechnologie in der Verwaltung unterliegt technikbedingt einem raschen Wandel. Auch die rechtlichen Rahmenbedingungen des E-Government sind auf internationaler, europäischer und nationaler Ebene beständig Veränderungen unterworfen. Zugleich ist jedoch gerade die Durchführung von E-Government-Projekten mit weitreichenden Kosten- und Organisationsfolgen verbunden. Die Entwicklung von E-Government muss daher flexibel auf aktuelle Tendenzen reagieren und dabei die finanziellen und organisatorischen Risiken angemessen begrenzen können. Hierfür bietet es sich an, im Rahmen von Pilotprojekten in sachlich, räumlich und inhaltlich abgegrenzten Bereichen vertiefte Erkenntnisse zu einzelnen informationstechnischen Systemen und E-Government-Anwendungen zu gewinnen, ehe diese dauerhaft bzw. flächendeckend zum Einsatz kommen.

Die Umsetzung solcher Pilotprojekte wäre jedoch oft unzulässig, wenn dafür keine Ausnahmen von den Vorschriften des allgemeinen oder besonderen Verwaltungsverfahrensrechts erlaubt werden. Da diese allgemeinen Normen nach wie vor überwiegend anhand der Bedürfnisse einer noch nicht elektronisch unterstützten Verwaltung formuliert wurden, ergeben sich aus den in ihnen enthaltenen Form- und Zuständigkeitsvorschriften Hemmnisse für derartige Experimente im Bereich des E-Governments. Angesichts der Dynamik der technischen Entwicklungen kann sich zudem auch bei Regelungen, die bereits an die elektronische Verwaltung angepasst wurden, entsprechender Bedarf ergeben.

Gemäß Satz 1 Nummer 1 darf von den dort abschließend aufgezählten Zuständigkeits- und Formvorschriften des Saarländischen Verwaltungsverfahrensgesetzes (SVwVfG) abgewichen werden. Derartige Ausnahmen sind danach zulässig für die Vorschriften

- der örtlichen Zuständigkeit (§ 3 SVwVfG),
- zur elektronischen Kommunikation (§ 3a SVwVfG),
- zur zusätzlichen Internetveröffentlichung von öffentlichen oder ortsüblichen Bekanntmachungen (§ 27 a SVwVfG),
- zur Beglaubigung von Dokumenten (§ 33 SVwVfG),
- zur Beglaubigung von Unterschriften (§ 34 SVwVfG),
- zur Form des Verwaltungsaktes (§ 37 Absatz 2 bis 5 SVwVfG),
- zur Bekanntgabe des Verwaltungsaktes (§ 41 SVwVfG),
- zur Schriftform des öffentlich-rechtlichen Vertrags (§ 57 SVwVfG),
- zur Form des Antrags im förmlichen Verwaltungsverfahren (§ 64 SVwVfG) und
- zur Form der Entscheidung im förmlichen Verwaltungsverfahren (§ 69 Absatz 2 SVwVfG).

Nach Satz 1 Nummer 2 kann von den dort abschließend aufgezählten Zustellungsanforderungen abgewichen werden. Derartige Ausnahmen sind danach zulässig für die Vorschriften

- der elektronischen Zustellung (§ 1 Saarländisches Verwaltungszustellungsgesetz (SVwZG) i.V.m. § 5 Absatz 4 bis 7 Verwaltungszustellungsgesetz (VwZG) und § 5a VwZG) und

- zur Ausgestaltung der öffentlichen Zustellung (§ 1 SVwZG i.V.m. § 10 Absatz 2 VwZG).

Die Zuständigkeits- und Formvorschriften des Saarländischen Verwaltungsverfahrensgesetzes werden in den konkreten Fachverfahren des saarländischen Verwaltungsrechts teilweise durch spezielle Zuständigkeits- und/oder Formvorschriften des besonderen Verwaltungsrechts ergänzt oder modifiziert.

Für die effektive Erprobung neuer E-Government-Verfahren ist daher eine zeitlich befristete Abweichungsmöglichkeit von Regelungen des Saarländischen Verwaltungsverfahrensgesetzes allein in der Regel nicht ausreichend. Im Interesse der praktischen Wirksamkeit der Experimentierklausel erlaubt § 21 Satz 1 Nummer 3 daher ergänzend auch die Abweichung von sonstigen landesgesetzlichen Zuständigkeits- und Formvorschriften. Um den verfassungsrechtlichen Anforderungen des Rechtsstaats- und Demokratieprinzips, insbesondere dem Grundsatz vom Vorbehalt des Gesetzes und dem Bestimmtheitsgebot zu genügen, werden die technischen und rechtlichen Anwendungsfelder der Norm im Einzelnen abschließend festgelegt.

Gemäß § 21 Satz 2 ist die Verordnung aus der Natur des Experiments zeitlich zu befristen. Eine Dauer von drei Jahren wird insoweit als angemessen und ausreichend angesehen.

Zu Artikel 3

Änderung des Saarländischen Besoldungsgesetzes

Zur Koordinierung und Steuerung der Aufgaben im Zusammenhang mit der Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur der Landesverwaltung bedarf es der Funktion eines Landesbeauftragten für Informationssicherheit (Chief Information Security Officer, CISO). Die Einrichtung einer derartigen Funktion entspricht auch den Vorgaben des IT-Planungsrates von Bund und Ländern in seiner verbindlichen Leitlinie für Informationssicherheit in der öffentlichen Verwaltung.

Im Saarland ist diese Aufgabe dem Direktor des Landesamtes für Zentrale Dienste zusätzlich zu seinen mit der Leitung des Amtes obliegenden Aufgaben übertragen worden.

Wegen der Bedeutung, des Aufwandes und der mit der zusätzlichen Aufgabe verbundenen landesweiten Verantwortung wird daher in der Besoldungsgruppe B 5 ein weiteres Amt für den Direktor des Landesamtes für Zentrale Dienste ausgebracht.

Zu Artikel 4

Inkrafttreten

Zu Absatz 2:

Absatz 2 sieht das gemäß der E-Rechnungsrichtlinie (RL 2014/55/EU vom 16. April 2014) späteste verpflichtende Inkrafttreten am 18. April 2020 vor. Diese Inkrafttretens-Regelung korrespondiert mit Artikel 11 Absatz 2 Satz 2 der Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen. Artikel 11 Absatz 2 Satz 2 ermöglicht es den Mitgliedstaaten, die Anwendung in Bezug auf ihre subzentralen öffentlichen Auftraggeber um bis zu höchstens 30 Monate nach Veröffentlichung der europäischen Norm für die elektronische Rechnungsstellung im Amtsblatt der Europäischen Union aufzuschieben. Diese Norm wurde am 17. Oktober 2017 veröffentlicht. Von der Möglichkeit des Hinausschiebens für die subzentralen öffentlichen Auftraggeber im Sinne von § 5 Absatz 1 wird hier Gebrauch gemacht und damit den Betroffenen ausreichend Zeit für vorbereitende Maßnahmen eingeräumt.

Da sich der Absatz jedoch nur auf Artikel 2 Nummer 2 § 10a Absatz 1 und 2 bezieht, tritt Absatz 3 – die Ermächtigung zur Erstellung einer Rechtsverordnung zur Ausgestaltung des elektronischen Rechnungsverkehrs – unmittelbar in Kraft. Dies ist zwingend notwendig, da diese die technischen und organisatorischen Voraussetzungen zur Umsetzung der Absätze 1 und 2 bilden soll und mit ihrer Erarbeitung unmittelbar begonnen werden muss.