Referentenentwurf

des Bayerischen Staatsministeriums für Digitales

Entwurf eines Gesetzes über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – BayDiG)

A) Problem

Die fortschreitende Digitalisierung aller Lebens-, Gesellschafts- und Wirtschaftsbereiche stellt den Freistaat Bayern vor eine der wohl größten Herausforderungen der letzten Jahrzehnte. „Digitalisierung“ kann nach einer gängigen Definition als ein Prozess beschrieben werden, der auf der intelligenten Vernetzung von Prozessketten und einer durchgängigen Erfassung, Aufbereitung, Analyse und Kommunikation von Daten beruht. Auf Grundlage der nahezu kontinuierlichen informationstechnischen Erreichbarkeit von Personen (Smartphone), Maschinen (Industrie 4.0.), Objekten (Internet of Things) sowie Diensten (Internet of Services), Daten (Big Data) und Rechenleistung (Cloud Computing), haben sich, wie *Marco Brunzel* konstatiert, in den letzten beiden Jahrzehnten neue Formen der Kommunikation (Social Media) der Produktion und des Handels (e-Commerce) sowie der kollektiven Nutzung von Gütern und Dienstleistungen (Sharing, Streaming) entwickelt und etabliert. Gerade die aktuelle Corona-Krise hat ein besonderes Schlaglicht nicht nur auf die Potentiale der Digitalisierung, sondern auch auf bestehende Defizite geworfen. Digitalisierung kann und sollte aber nicht auf ihre Rolle bei der Bewältigung aktueller Krisen reduziert werden. Sie steht für einen langfristigen und grundlegenden Transformationsprozess von Gesellschaft und Wirtschaft, Staat und Verwaltung. Bis zum Jahr 2025 werden – noch beschleunigt durch die aktuellen Entwicklungen – weltweit nach Schätzungen bis zu 75 Milliarden Geräte vernetzt sein. Die in diesen Kontexten übermittelten, ausgetauschten und (über Algorithmen, KI) aufbereiteten Daten werden als „Rohstoff einer neuen Ökonomie“ begriffen, deren Potentiale es zu erschließen gilt.

Der Freistaat Bayern hat auf die Chancen und Herausforderungen der Digitalisierung bereits frühzeitig mit der Entwicklung übergreifender Digitalisierungsprogramme reagiert (BAYERN DIGITAL I und II, High-Tech-Agenda). Als konsequenter nächster Schritt ist nunmehr auch die Verankerung zielgerichteter, entwicklungsoffen gestalteter rechtlicher Leitplanken für die Digitalisierung von Gesellschaft und Wirtschaft, Staat und Verwaltung im Freistaat Bayern erforderlich. In dem Maße, in dem die Digitalisierung aller Lebensbereiche voranschreitet, müssen in einem demokratischen Rechtsstaat die digitalen Rechte der Bürgerinnen und Bürger und Unternehmen konsequent weiterentwickelt und ausgebaut werden. Im Zuge der Digitalisierung verändern sich auch Aufgaben und Verantwortlichkeiten des Staates. Der Siegeszug globaler Plattformtechnologien schafft neue Abhängigkeiten und erfordert die Entwicklung von Strategien zur Gewährleistung der digitalen Souveränität staatlichen Handelns, aber auch zur Sicherung der autonomen digitalen Handlungs- und Entscheidungsfähigkeit von

Bürgern, Unternehmen und Kommunen. Hierzu gehören auch zielgerichtete Maßnahmen zur Förderung digitaler Spitzentechnologien.

Die konsequente Förderung von digitalen Technologien und Geschäftsmodellen ist ein Schlüsselfaktor der Zukunftsfähigkeit des Wirtschafts- und Technologiestandorts Bayern. Unter den Bedingungen von Digitalisierung ändern sich private Kommunikationswege ebenso wie die Arbeitsabläufe, Geschäfts- und Entwicklungsprozesse in Organisationen (z. B. mobiles und agiles Arbeiten). Digitalisierung bietet auch neue Chancen für nachhaltige Entwicklungen. Erhebliche Potentiale bestehen bei der Erleichterung des Zugangs von Menschen mit Behinderung zum gesellschaftlichen und beruflichen Leben, beim Klimaschutz durch den Einsatz umweltfreundlicher Technologien (Clean IT), aber auch bei der Umsetzung flexibler und klimaförderlicher Arbeitszeitmodelle, z. B. durch den Einsatz von Home- oder Mobile Office Technologien.

Der Freistaat Bayern versteht sich nicht nur als aktiver Mitgestalter der Digitalisierung in Gesellschaft und Wirtschaft, sondern sieht in der Digitalisierung auch eine Chance für die weitere Modernisierung von Staat und Verwaltung. Für den Freistaat relevante Rahmenbedingungen ergeben sich hier nicht nur aus dem Onlinezugangsgesetzes (OZG), dass Anfang 2023 in seiner ersten Ausbauphase umgesetzt sein soll, sondern auch aus unionsrechtlichen Vorgaben, wie etwa der Single Digital Gateway Verordnung (EU) Nr. 2018/1724. Diese Regelungen haben gemeinsam, dass sie nicht nur auf ebenenübergreifende Wirkungen, sondern auch auf die Vernetzung der digitalen Verwaltungsangebote von Bund, Ländern, Kommunen und sonstigen öffentlich-rechtlichen Körperschaften gerichtet sind. Dies erfordert eine noch engere Abstimmung aller staatlichen und nichtstaatlichen Verwaltungsebenen, insbesondere einen weiteren Ausbau der engen Kooperation zwischen Freistaat und den bayerischen Kommunen.

Die Digitalpolitik des Freistaates bewegt sich in einem rasch wandelnden Kontext, der durch eine zunehmende Konzentration technologischer, wirtschaftlicher und gesellschaftlicher Macht bei vergleichsweise wenigen global agierenden Technologieplattformen geprägt ist. Diese Entwicklung hat sich unter anderem in der Diskussion um die Bedingungen „digitaler Souveränität“ niedergeschlagen. Für den Gesetzgeber ist hiermit die Aufgabe verbunden, wirksame, zugleich aber hinreichend entwicklungsoffene rechtliche Leitplanken zur Sicherung der eigenständigen digitalen Entscheidungs- und Handlungsfähigkeit des Freistaates Bayern und seiner Gebietskörperschaften zu schaffen. Hierzu zählen unter anderem gesetzliche Regelungen zu staatlich verfügbaren Cloud Services und zur strategischen Autonomie des Freistaates beim Zugang und bei der Verfügbarkeit und Datensicherheit staatlicher Netze.

B) Lösung

Die bisherigen Maßnahmen zur Förderung und Gestaltung der Digitalisierung sollen durch einen einheitlichen und übergreifenden rechtlichen Rahmen abgesichert, flankiert und verstärkt werden. Mit dem vorliegenden Entwurf eines Bayerischen Digitalgesetzes soll ein umfassender, allgemeiner Rechtsrahmen für die Digitalisierung von

Gesellschaft und Wirtschaft, Staat und Verwaltung geschaffen werden – ein Novum auch auf Bundes- und EU-Ebene.

Bisher wird das gesellschaftliche Schlüsselthema der Digitalisierung durch Maßnahmen der Exekutive auf den Ebenen der Europäischen Union, des Bundes und der Länder dominiert. Die Digitalisierung hat aber mittlerweile eine gesamtgesellschaftliche Bedeutung erlangt, die das Tätigwerden des Gesetzgebers zur Festlegung der „wesentlichen“ Grundsätze staatlicher Digitalpolitik erfordern. Der vorliegende Entwurf für ein Bayerisches Digitalgesetz trägt bundesweit erstmals dem Erfordernis einer gesetzgeberischen Regelung Rechnung. Ziel des Bayerischen Digitalgesetzes ist daher auch eine nachhaltige Stärkung der gestaltenden Rolle der Legislative gerade bei Fragen der gesellschaftlichen Zukunftsgestaltung.

Das Bayerische Digitalgesetz stellt den Menschen in den Mittelpunkt der Digitalisierung. Das Digitalgesetz definiert hierzu bundesweit erstmals einen umfassenden Katalog digitaler Rechte von Bürgerinnen, Bürgern und Unternehmen. Ziel des allgemeinen Teils ist es auch, die allgemeinen Grundsätze des Rechts der Digitalisierung in Bayern für die Bürger erkennbar und nachvollziehbar in einem einheitlichen Regelwerk „vor die Klammer“ zu ziehen. Daher enthält der allgemeine Teil des Gesetzes unter anderem auch allgemeine Regelungen zur Barrierefreiheit sowie Regelungen zu den Grundsätzen des „offenen Datenzugangs“ (Open Data).

In seinen besonderen Teilen knüpft das Gesetz in den Bereichen „Digitale Verwaltung“ und „IT-Sicherheit“ inhaltlich an das bestehende E-Government-Gesetz an, ersetzt dieses jedoch durch ein grundlegend neu konzipiertes, umfassend angelegtes Regelwerk. Bewährte Regelungen etwa zu digitalen Zugangs- und Verfahrensrechten, zu elektronischen Verwaltungsverfahren oder zur IT-Sicherheit werden übernommen und inhaltlich weiterentwickelt. Hinzukommen neue Regelungen zum Aufbau eines bayerischen Portalverbunds, zur Volldigitalisierung der bayerischen Staatsverwaltung und zur Umsetzung des 12-Punkte Plans der Staatsregierung. Weiter werden auch Themen der Nachhaltigkeit und Umweltfreundlichkeit adressiert.

Die wesentlichen Ziele des Gesetzes sind:

- die Förderung der Digitalisierung im Freistaat Bayern, insbesondere in den Bereichen Wirtschaft und Technologie, Planen und Bauen, Bildung, Forschung und Wissenschaft, Mobilität, Medizin, Gesundheit und Pflege sowie öffentliche Verwaltung,
- die Verankerung digitaler Rechte der Bürgerinnen und Bürger und der Unternehmen im Freistaat Bayern,
- der Schutz der eigenständigen digitalen Entscheidungs- und Handlungsfähigkeit des Freistaates Bayern und der Gemeindeverbände und Gemeinden,

- die Stärkung der strategischen Autonomie des Freistaates Bayern in Bezug auf staatlich verfügbare Netze und Verbesserung ihrer Bereitstellung und Verfügbarkeit,
- die Förderung der Entwicklung und des Einsatzes innovativer digitaler Geschäftsmodelle am Digitalstandort Bayern und die Förderung des gleichberechtigten Zugangs zu Digitalberufen,
- der Ausbau der Digitalen Daseinsvorsorge im Freistaat Bayern, einschließlich der Bereitstellung und Sicherung digitaler Netze und Infrastrukturen,
- die Förderung von Informationssicherheit und Datenschutz in der digitalen Gesellschaft,
- die Digitalisierung der Verwaltung und der Ausbau digitaler Verwaltungsangebote,
- die vollständige Digitalisierung aller geeigneten Prozesse und der Einsatz innovativer digitaler Lösungen in Staat und Verwaltung im Freistaat Bayern,
- die Umsetzung des Onlinezugangsgesetzes und die Implementierung eines Bayerischen Portalverbunds mit einem zentralen Nutzerkonto zur Inanspruchnahme aller digitalen Verwaltungsleistungen,
- der Ausbau und die Weiterentwicklung nutzerfreundlicher, insbesondere auch mobiler und personalisierter Verwaltungsangebote und die Einführung des digitalen Verfahrens als Regelverfahren im Freistaat Bayern,
- der Ausbau der digitalen Verwaltung für die Wirtschaft und der Aufbau und Betrieb eines Organisationskonto zur Bündelung wirtschafts- und organisationsbezogener Verwaltungsleistungen,
- die Förderung und der weitere Ausbau nachhaltiger, barrierefreier und umweltfreundlicher digitaler Verwaltungsprozesse sowie der Ausbau von Experimentierräumen für innovative, digitale öffentliche Dienste,
- die Mitwirkung des Freistaates Bayern an Aufbau und Entwicklung des Portalverbunds von Bund und Ländern und beim Aufbau und Betrieb des „Single Digital Gateway“ der Europäischen Union,
- die Mitwirkung des Freistaates Bayern bei weiteren Maßnahmen zur Digitalisierung der Verwaltung auf den Ebenen von Ländern, Bund und Europäischer Union.

C) Alternativen

Keine.

D) Kosten

1) Staat

Die vorgesehenen Maßnahmen dienen der Gestaltung und Förderung der Digitalisierung im Freistaat Bayern. Die mit dem Gesetz verbundenen Zielsetzungen und Maßnahmen erfordern erhebliche Investitionen und binden zumindest temporär weiteres Personal in der Verwaltung. Auch unter Berücksichtigung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit (Art. 7 BayHO) werden bei der Umsetzung daher zusätzliche Aufwände entstehen, denen allerdings auch erhebliche Einsparpotentiale gegenüberstehen.

Die Umsetzung und Finanzierung erfolgen im Rahmen fachlicher Priorisierungen und Schwerpunktsetzungen der Ressorts und vorbehaltlich der jeweils bei den Ressorts verfügbaren Stellen und Mittel. Für die Umsetzung der in diesem Gesetz vorgesehenen ressortübergreifenden Maßnahmen im Bereich der digitalen Verwaltung ist mit Gesamtkosten in der ersten Phase von insgesamt rd. 61,6 Mio. € zu rechnen. Der Personalbedarf für die ressortübergreifende Koordinierung der Maßnahmen liegt bei rd. 50 Stellen. Zur Umsetzung der Fördermaßnahmen des Gesetzes (vgl. Art. 2) sind weitere Mittel in allen Ressorts erforderlich, die durch den Landtag festzulegen sind. Die in den Ressorts im Übrigen anfallenden Kosten und Stellen können nicht abschließend quantifiziert werden. Ihre zielgerichtete Steuerung und Begrenzung ist über die im Gesetz vorgesehenen Ausführungsvorschriften möglich (vgl. Art. 53). Im Übrigen ist eine nähere Quantifizierung der Umsetzungskosten im Rahmen des Digitalplans der Staatsregierung vorgesehen (vgl. Art. 15).

Das Gesetz berücksichtigt die aktuellen haushalterischen Unwägbarkeiten und enthält daher eine Vielzahl von Stellschrauben, etwa in Form von Verordnungs- oder Planungsvorbehalten, um die anfallenden Kosten für den Freistaat Bayern flexibel zu steuern und ggfs. situationsorientiert zu begrenzen.

Den (steuerbaren) Kosten stehen bei vollständiger Umsetzung der Maßnahmen des Gesetzes erhebliche Effizienz- und Effektivitätsgewinne gegenüber. Allein im staatlichen Bereich ist bei vollständiger Umsetzung der Maßnahmen dieses Gesetzes mit mittel- und langfristigen Einsparungen von mindestens 1 Mrd. € p.a. zu rechnen (vgl. Normenkontrollrat 2012, 2015, 2017). Der Normenkontrollrat (NKR) geht bei der Digitalisierung der Verwaltung von einem Einsparpotential gegenüber dem Ist-Stand von gut 30 % aus. Allein bezogen auf die 60 wichtigsten Verwaltungsleistungen entspricht dies laut NKR einem bundesweiten Einsparpotential von 700 Mio. € p.a. (NKR 2015). Da im Freistaat insgesamt eine deutlich höhere Zahl von Verwaltungsleistungen zu digitalisieren ist, liegt das Einsparpotential entsprechend höher. Hinzu kommen Einsparpotentiale bei internen Prozessen im Zuge der Registermodernisierung. Hier wird ein bundesweites Einsparpotential für die Verwaltung von 3,9 Mrd. € geschätzt (NKR 2017, 2020), was übertragen auf Bayern (entsprechend Königsteiner Schlüssel) einer Einsparung von rd. 600 Mio. € p.a. entspricht.

Unbeschadet der damit grundsätzlich im Bereich der digitalen Verwaltung bestehenden Einsparpotentiale ist allerdings zu berücksichtigen, dass derartige Einsparungen erst mit zum Teil erheblicher zeitlicher Versetzung zur digitalen Umsetzung eintreten. Darüber hinaus wird bei Aufwendungen und Einsparungen zwischen dem Kernbereich

der digitalen Verwaltung und anderen Teilbereichen der Digitalisierung zu unterscheiden sein: Von Einsparpotentialen kann daher besonders im Bereich der Verwaltungsdigitalisierung gesprochen werden, soweit Effizienzgewinne nicht bereits durch Verfahren zur elektronischen Sachbearbeitung realisiert wurden. In anderen staatlichen Verantwortungsbereichen, insbesondere auch in Bildung, Wissenschaft und Kulturpflege, führt die infolge der Corona Pandemie nochmals beschleunigte Digitalisierung zu Mehraufwendungen, denen zwar Leistungsverbesserungen und Qualitätsgewinne, aber keine wesentlichen Einsparungen gegenüberstehen. Angesichts wachsender Bedrohungen steigen auch die Kosten für Maßnahmen zur Gewährleistung der Informationssicherheit stetig an, deren Nutzen in der Vermeidung materieller und immaterieller Schäden, nicht in einer Verringerung von Aufwänden besteht.

2) Kommunen

Bei der Gestaltung und Förderung der Digitalisierung kommt den Kommunen eine Schlüsselfunktion zu. Das Bayerische Digitalgesetz stellt die Kooperation zwischen Freistaat und Kommunen im Bereich der Digitalisierung daher auch in Hinblick auf die Kosten auf eine neue Grundlage. Das Gesetz enthält zunächst Verpflichtungen der Kommunen, die teilweise über den bisherigen Rechtstand hinausgehen. Die damit verbundenen Mehrausgaben auf kommunaler Ebene lassen sich angesichts der Dynamik der technischen Entwicklungen im Bereich der Digitalisierung ebenso wenig abschließend kalkulieren, wie die ebenfalls zu erwartenden Einsparpotentiale, etwa durch Beschleunigung und Automatisierung von Verwaltungsprozessen. Im Rahmen einer Gesamtbilanz der bei den Kommunen entstehenden Kosten ist auch zu berücksichtigen, dass zentrale Rechtsvorschriften des Gesetzes auf Kommunen nur eingeschränkt Anwendung finden (vgl. z. B. elektronische Verwaltungsverfahren und elektronische Aktenführung), dass eine Reihe von Pflichten der Kommunen erst durch Ausführungsbestimmungen konkretisiert werden müssen (vgl. z. B. mobile digitale Dienste) und dass das Gesetz auch umfassende neue Unterstützungsmaßnahmen zu Gunsten der Kommunen vorsieht (vgl. z. B. Digitale Daseinsvorsorge, Digitale Qualifizierung). Die Gesamtkonzeption des Gesetzes zielt bei den Kommunen darauf, deren neue rechtlichen Verpflichtungen im Rahmen der Digitalisierung durch ein abgestimmtes Bündel technischer, organisatorischer, finanzieller und personeller Unterstützungsmaßnahmen angemessen zum Ausgleich zu bringen. Ebenso wie im staatlichen Bereich wird eine genauere Quantifizierung der bei den Kommunen entstehenden Kosten und der hier zu erwartenden Entlastungen erst auf Grundlage der Festlegungen des Digitalplans der Staatsregierung möglich ein (vgl. Art. 15).

3) Wirtschaft und Bürger

Unmittelbare Kosten für die Wirtschaft oder den Bürger entstehen durch das Gesetz nicht. Die Maßnahmen zur Stärkung des Digitalstandorts Bayern und zur Förderung digitaler Technologien werden zu positiven volkswirtschaftlichen Effekten führen. Darüber hinaus wird die Digitalisierung der Verwaltung für Bürger und Unternehmen zu

erheblichen Kosteneinsparungen bei der Abwicklung von Verwaltungskontakten führen.

Die Einführung eines Bürger- und Organisationskontos bewirkt eine Reduzierung des Zeitaufwandes zur Erfüllung bestehender Verwaltungspflichten für Bürger und Wirtschaft. Weitere Effizienzgewinne ergeben sich aus dem massiven Ausbau digitaler Verwaltungsangebote, dem Abbau von Formvorschriften, der Erleichterung des E-Payment und durch die Einführung der digitalen Rechnung in der Verwaltung.

Mit dem Ausbau von digitalen Verwaltungsangeboten und -lösungen werden Unternehmen und Bürgern neue und vereinfachte Möglichkeiten der Kommunikation, des Datenzugriffs, der Antragstellung, der Nachweisführung, der Bürgerbeteiligung und der Bezahlung über das Internet zur Verfügung stehen. Durch digitale Identifizierungsmöglichkeiten beispielsweise mittels des ELSTER-Verfahrens können diese Angebote auch genutzt werden, wenn ein Schriftformerfordernis besteht. Ebenso reduzieren sich durch die Nutzung der neuen E-Government-Angebote Wege- und Wartezeiten erheblich. Schätzungen des Normenkontrollrats gehen bundesweit von jährlichen Einsparpotentialen für Wirtschaft und Bürger in Milliardenhöhe aus.

206-1-D

Gesetz über die Digitalisierung im Freistaat Bayern

(Bayerisches Digitalgesetz – BayDiG)

Teil 1
Allgemeiner Teil

Kapitel 1
Allgemeines, Digitalstandort, Digitale Technologien

Art. 1
Anwendungsbereich

(1) [1]Dieses Gesetz gilt für den Freistaat Bayern, die Gemeindeverbände und Gemeinden und die sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts. [2]Für die staatlichen Landratsämter, die Verwaltungsgemeinschaften und Zweckverbände gelten die Rechtsvorschriften für Gemeindeverbände und Gemeinden entsprechend.

(2) [1]Soweit nichts anderes bestimmt ist, gelten Teil 2 und 3 dieses Gesetzes für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden der in Abs. 1 genannten juristischen Personen. [2]Teil 2 und 4 dieses Gesetzes gelten nicht für

1. die Tätigkeiten der Schulen, Krankenhäuser, des Landesamtes für Verfassungsschutz und Beliehener,
2. die Tätigkeit der Finanzbehörden nach der Abgabenordnung (AO),
3. die in Art. 2 Abs. 1, 2 Nr. 2, 3, 5 und 6 des Bayerischen Verwaltungsverfahrensgesetzes (BayVwVfG) genannten Bereiche,
4. die Tätigkeit der Behörden im Rahmen des Prüfungsverfahrens und
5. die Tätigkeit der Gerichtsverwaltungen und der Behörden der Justizverwaltung, soweit sie nicht der Nachprüfung durch die Gerichte der Verwaltungsgerichtsbarkeit oder durch die in verwaltungsrechtlichen Anwalts- und Notarsachen zuständigen Gerichte unterliegt oder soweit Teil 2 Kapitel 3 die Einbeziehung von Justizleistungen nicht ausdrücklich regelt.

(3) Dieses Gesetz gilt nicht für die Verwaltungstätigkeit nach dem Zweiten Buch Sozialgesetzbuch (SGB II), soweit sie von gemeinsamen Einrichtungen nach § 44b SGB II vollzogen wird.

(4) Das E-Government-Gesetz findet nur beim Vollzug von Bundesrecht im Auftrag des Bundes Anwendung.

Art. 2
Förderung der Digitalisierung

[1]Der Freistaat Bayern gestaltet und fördert die Digitalisierung im Interesse von Bürgern, Gesellschaft und Wirtschaft. [2]Die Maßnahmen des Freistaates Bayern zielen insbesondere auf

1. die Förderung digitaler Technologien am Digitalstandort Bayern,
2. den Ausbau allgemeiner digitaler Bildungs-, Weiterbildungs- und Informationsangebote,
3. die Förderung der digitalen Daseinsvorsorge, insbesondere leistungsfähiger digitaler Infrastrukturen,
4. eine stärkere Nutzung der Möglichkeiten der Digitalisierung im Mobilitätsbereich,
5. die Digitalisierung in Gesundheit und Pflege,
6. die Stärkung der Digitalisierung in der Wissenschaft,
7. die Stärkung digitaler Grundkompetenzen in Gesellschaft, Wirtschaft und Verwaltung,
8. den digitalen Verbraucherschutz und die Stärkung digitaler Kompetenzen der Verbraucher,
9. die Förderung digitaler Geschäftsmodelle,
10. die Förderung des gleichberechtigten Zugangs zu Digitalberufen,
11. die Stärkung der IT-Sicherheit in Staat, Verwaltung und Wirtschaft,
12. die Digitalisierung der Verwaltung und den Ausbau digitaler Verwaltungsangebote,
13. die Vereinfachung und nutzerfreundliche Gestaltung von Verwaltungsverfahren,
14. die Bereitstellung offener Daten der Verwaltung und
15. die digitale Barrierefreiheit öffentlicher Dienste.

Art. 3
Digitale Entscheidungsfähigkeit des Freistaates Bayern

(1) [1]Die eigenständige digitale Entscheidungs- und Handlungsfähigkeit des Freistaates Bayern ist durch geeignete Maßnahmen zu sichern. [2]Der Freistaat Bayern unterhält hierfür staatliche Rechenzentren und staatlich verfügbare Netze, geeignete Cloud-Dienste und weitere geeignete Technologien und Anwendungen.

(2) Der Freistaat Bayern schützt die Funktionsfähigkeit und den Zugang zu kritischen staatlichen Infrastrukturen und Netzen.

(3) Der Freistaat Bayern, die Gemeindeverbände und Gemeinden treffen nach Maßgabe dieses Gesetzes angemessene Maßnahmen zur Abwehr von Gefahren für die Sicherheit ihrer informationstechnischen Systeme.

(4) [1]Die Behörden des Freistaates Bayern sollen bei Neuanschaffungen offene Software verwenden und offene Austauschstandards nutzen, soweit dies wirtschaftlich und zweckmäßig ist. [2]Den Gemeindeverbänden und Gemeinden wird die Verwendung offener Software im Sinne von Satz 1 empfohlen.

Art. 4
Digitale Daseinsvorsorge

(1) Der Freistaat Bayern, die Gemeindeverbände und Gemeinden und sonstige unter der Aufsicht des Freistaates Bayern stehende juristische Personen des öffentlichen Rechts stellen ihre hierfür geeigneten öffentlichen Dienste im Rahmen ihrer Zuständigkeiten nach Maßgabe dieses Gesetzes auch digital über öffentlich zugängliche Netze bereit.

(2) Der Freistaat Bayern, die Gemeindeverbände und Gemeinden stellen zur inhaltlichen Vermittlung und zur Förderung der Akzeptanz ihrer digitalen Angebote qualifizierte Ansprechpartner bereit.

(3) [1]Der Freistaat Bayern unterstützt die Gemeindeverbände und Gemeinden beim Angebot digitaler öffentlicher Dienste im Sinne der Abs. 1 und 2. [2]Der Freistaat Bayern stellt hierzu insbesondere Basisdienste und zentrale Dienste bereit und fördert die Qualifizierung von digitalen Ansprechpartnern. [3]Die Aufgaben, Zuständigkeiten und Verantwortlichkeiten der Gemeindeverbände und Gemeinden bleiben unberührt.

Art. 5
Digitalisierung von Staat und Verwaltung

(1) Geeignete staatliche Prozesse der Verwaltung des Freistaates Bayern sollen vollständig digitalisiert und bereits digitalisierte Prozesse in einem Verbesserungsprozess fortentwickelt werden.

(2) Bei Verwaltungsverfahren, die vollständig durch automatische Einrichtungen durchgeführt werden, sind die eingesetzten Einrichtungen regelmäßig auf Ihre Zweckmäßigkeit, Objektivität und Wirtschaftlichkeit hin zu überprüfen.

(3) [1]Die Digitalisierung der Verwaltung zur Umsetzung des Onlinezugangsgesetzes (OZG) wird im Freistaat Bayern vom Staatsministerium für Digitales gesteuert. [2]Die Zuständigkeiten der Staatsministerien sowie die Themenfeldverantwortung und Themenfeldbetreuung nach dem Onlinezugangsgesetz bleiben unberührt.

Art. 6
Nachhaltigkeit

Im Rahmen der Wirtschaftlichkeit und Zweckmäßigkeit sind staatliche Behörden verpflichtet, bei ihrer digitalen Aufgabenerfüllung Aspekte der Ökologie und der Nachhaltigkeit zu berücksichtigen, insbesondere

1. bei der Beschaffung der IT-Infrastruktur auf eine Wiederverwertbarkeit der Rohstoffe, auf hohe Energieeffizienz sowie auf umweltgerechtes Verpackungsmaterial zu achten,
2. bei der Server-Betreuung und beim Server-Betrieb auf Energieeffizienz und -sparsamkeit zu achten,
3. für eine umweltgerechte Entsorgung der IT-Infrastruktur Sorge zu tragen,
4. bei Beschaffung, Entwicklung und Einsatz von Software und mobilen Applikationen auf Energieeffizienz hinzuwirken,
5. nach Möglichkeit auf Dienstreisen zu verzichten und sie durch digitale Formen der Zusammenarbeit zu ersetzen,
6. die Einrichtung von Telearbeitsplätzen zu fördern.

Art. 7
Personal und Qualifizierung

(1) [1]Der Freistaat Bayern fördert die digitale Qualifizierung der Beschäftigten der öffentlichen Verwaltung. [2]Der Freistaat Bayern trifft geeignete Maßnahmen zur Gewinnung, Bindung und Entwicklung von IT-Fachkräften in der bayerischen Staatsverwaltung.

(2) Bei der Einführung neuer digitaler Verfahren sowie bei wesentlichen Erweiterungen oder sonstigen Änderungen bestehender Verfahren sind die hiervon betroffenen staatlichen Bediensteten angemessen fort- und weiterzubilden.

Kapitel 2
Digitale Rechte und Gewährleistungen

Art. 8
Freier Zugang zum Internet

[1]Jeder hat das Recht auf freien Zugang zum Internet über allgemein zugängliche Netze. [2]Der Zugang zum Internet kann nur durch oder aufgrund Gesetzes beschränkt werden. [3]Allgemeine staatliche Internetzugangsblockaden sind unzulässig.

Art. 9
Digitale Handlungsfähigkeit

Der Freistaat Bayern stellt digitale Dienste bereit, die insbesondere die Möglichkeiten zur digitalen Ausübung der Rechts- und Geschäftsfähigkeit, der Beteiligten- und

Handlungsfähigkeit im Verwaltungsverfahren, der elterlichen Sorge, der Vormundschaft, der Betreuung, der Bevollmächtigung, der Pflegschaft und der Rechtsnachfolge im Erbfall im Rahmen der Kommunikation mit den Behörden verbessern.

Art. 10
Digitale Selbstbestimmung

(1) [1]Der Freistaat Bayern fördert die digitale Selbstbestimmung der Bürger und stellt hierzu nutzerfreundliche und barrierefreie digitale Dienste bereit. [2]Die Nutzer sollen in die Entwicklung neuer digitaler Angebote des Freistaates Bayern einbezogen werden.

(2) [1]Der Freistaat Bayern fördert geeignete Maßnahmen zur Stärkung der digitalen Grundkompetenzen von Bürgern und Unternehmen. [2]Der Freistaat Bayern fördert geeignete Qualifizierungsmaßnahmen zur digitalen Barrierefreiheit.

Art. 11
Digitale Identität

(1) [1]Jede natürliche Person hat das Recht auf eine eigene digitale Identität nach Maßgabe dieses Artikels. [2]Dies umfasst die Bereitstellung digitaler Identitätsdienste zur sicheren Abwicklung digitaler Kontakte mit den Behörden, zur Inanspruchnahme digitaler öffentlicher Dienste, zur Durchführung von Verwaltungsverfahren und zum Empfang, zur Vorlage und Archivierung von Belegen und Nachweisen.

(2) [1]Hierzu stellt der Freistaat Bayern den Berechtigten unentgeltlich Nutzerkonten und weitere erforderliche digitale Dienste nach Maßgabe der Art. 29 bis 31 zur Verfügung. [2]Die digitalen Identitätsdienste werden über einen sicheren Identitätsnachweis im Sinne von Art. 31 Abs. 2 beantragt.

(3) [1]Die Einrichtung und Nutzung der digitalen Identität ist freiwillig. [2]Ihr Inhaber hat das jederzeitige Zugriffs- und Löschungsrecht für die digitale Identität als solche und all ihrer Inhalte. [3]Die datenschutzrechtliche Aufsicht über die bereitstellende Stelle erfolgt durch den Landesbeauftragten für den Datenschutz.

(4) [1]Die in der digitalen Identität gespeicherten amtlichen Dokumente sind der Sphäre des Inhabers zuzurechnen, dauerhaft zu sichern und gegen den unbefugten Zugriff Dritter zu schützen. [2]Ein Zugriff auf die im Rahmen der digitalen Identität gespeicherten digitalen Dokumente ist ohne Einwilligung des Inhabers nur unter den Voraussetzungen der §§ 94, 95, 97 und 98 der Strafprozessordnung (StPO) zulässig. [3]Besondere gesetzliche Befugnisse bleiben unberührt.

Art. 12
Rechte in der digitalen Verwaltung

(1) [1]Jeder hat das Recht nach Maßgabe der Art. 16 bis 18 digital über das Internet mit den Behörden zu kommunizieren und ihre Dienste in Anspruch zu nehmen. [2]Er

kann verlangen, dass Verwaltungsverfahren nach Maßgabe des Art. 19 ihm gegenüber digital durchgeführt werden. [3]Die Möglichkeit, Verwaltungsverfahren auch nichtdigital zu erledigen, bleibt unberührt.

(2) [1]Die zuständigen Behörden sollen den Beteiligten in digitalen Verfahren eine nichtdigitale Beratung, Auskunft und Anhörung anbieten. [2]Die Kontaktdaten für die persönliche Beratung, Auskunft und Anhörung sollen für die Beteiligten leicht erkennbar, erreichbar und ständig verfügbar sein. [3]Der sofortige Vollzug vollständig automatisiert erlassener Entscheidungen ist nur aufgrund ausdrücklicher gesetzlicher Ermächtigung zulässig.

Art. 13
Mobile Dienste

(1) Jeder hat nach Maßgabe dieses Artikels das Recht auf mobile Bereitstellung öffentlicher digitaler Dienste.

(2) [1]Der Freistaat Bayern stellt geeignete öffentliche digitale Dienste auch mobil über allgemein zugängliche Netze bereit. [2]Der Freistaat Bayern unterstützt die Gemeindeverbände und Gemeinden bei der mobilen Bereitstellung digitaler öffentlicher Dienste durch geeignete Basisdienste oder zentrale Dienste.

Art. 14
Offene Daten

[1]Die Nutzbarkeit offener Datenbestände der öffentlichen Verwaltung wird gewährleistet. [2]Die staatlichen Behörden sind zur zielgruppenorientierten und nutzerfreundlichen Aufbereitung öffentlich zugänglicher Daten verpflichtet. [3]Das Nähere zu Voraussetzungen und Grenzen des offenen Datenzugangs wird durch oder aufgrund Gesetzes bestimmt.

Art. 15
Digitalplan, Digitalbericht

(1) Zur Umsetzung der Ziele dieses Gesetzes beschließt die Staatsregierung auf Vorschlag des Staatsministeriums für Digitales im Einvernehmen mit den Ressorts einen Digitalplan und schreibt diesen regelmäßig fort.

(2) Die Staatsregierung berichtet auf Basis des Digitalplanes dem Landtag regelmäßig, spätestens drei Jahre nach Inkrafttreten dieses Gesetzes, über den Stand der Digitalisierung in Bayern und die Umsetzung der nach diesem Gesetz vorgesehenen Maßnahmen.

Teil 2
Digitale Verwaltung

Kapitel 1
Digitale Kommunikation und Dienste

Art. 16
Digitale Kommunikation

[1]Jede Behörde ist verpflichtet, einen Zugang für die Übermittlung digitaler sowie im Sinne des Art. 3a Abs. 2 BayVwVfG schriftformersetzender Dokumente zu eröffnen. [2]Die Übermittlung digitaler Dokumente durch Behörden ist zulässig, soweit und solange der Empfänger hierfür einen Zugang eröffnet. [3]Die Behörden stellen geeignete sichere Verfahren für die Kommunikation mit dem Nutzer bereit. [4]Soweit nichts anderes bestimmt ist, entscheidet die Behörde über die Art und Weise der Übermittlungsmöglichkeit.

Art. 17
Digitale öffentliche Dienste

(1) [1]Die Behörden sollen ihre hierfür geeigneten Dienste auch digital anbieten. [2]Die Behörden sollen dabei zugleich die Informationen bereitstellen, die ihre sachgerechte und nutzerfreundliche digitale Inanspruchnahme ermöglichen.

(2) Für die Nutzung des digitalen Weges werden vorbehaltlich anderer Rechtsvorschriften keine zusätzlichen Kosten erhoben.

(3) [1]Veröffentlichungspflichtige Mitteilungen und amtliche Verkündungsblätter sollen auch digital bekannt gemacht werden. [2]Vorbehaltlich entgegenstehender rechtlicher Vorgaben kann die Bekanntmachung ausschließlich digital erfolgen, wenn eine Veränderung der veröffentlichten Inhalte ausgeschlossen ist und die Einsichtnahme auch unmittelbar bei der die Veröffentlichung veranlassenden Stelle auf Dauer gewährleistet wird. [3]Das Nähere regelt die Staatsregierung für ihren Bereich durch Bekanntmachung.

Art. 18
Digitale Zahlungsabwicklung und Rechnungen

(1) [1]Geldansprüche öffentlicher Kassen können unbar beglichen werden, solange kein sofortiges anderes Vollstreckungsinteresse besteht. [2]Die Behörden bieten hierfür integrierte digitale Zahlungsmöglichkeiten an, soweit dies wirtschaftlich und zweckmäßig ist.

(2) [1]Alle Auftraggeber im Sinne von § 98 des Gesetzes gegen Wettbewerbsbeschränkungen stellen den Empfang und die Verarbeitung digitaler Rechnungen sicher, soweit

1. für sie eine Vergabekammer des Freistaates Bayern zuständig ist,

2. sie im Rahmen der Organleihe für den Bund tätig werden oder

3. dies durch Rechtsverordnung der Staatsregierung vorgesehen ist.

[2]Eine Rechnung ist digital, wenn sie in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen werden kann, das ihre automatische und elektronische Verarbeitung ermöglicht.

Kapitel 2
Digitales Verwaltungsverfahren

Art. 19
Digitale Verfahren

(1) Behörden sind auf Verlangen eines Beteiligten verpflichtet, Verwaltungsverfahren oder abtrennbare Teile davon ihm gegenüber elektronisch durchzuführen, soweit dies wirtschaftlich und zweckmäßig ist.

(2) [1]Behördliche Formulare, die zur Verwendung durch Beteiligte dienen, sollen über das Internet auch elektronisch abrufbar sein. [2]Ist aufgrund einer Rechtsvorschrift ein bestimmtes Formular zwingend zu verwenden, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform bewirkt.

(3) Die Behörden sind verpflichtet, in digitalen Verwaltungsverfahren, in denen sie die Identität einer Person aufgrund einer Rechtsvorschrift festzustellen haben oder aus anderen Gründen eine Identifizierung für notwendig erachten, die Identifizierung über einen digitalen Identitätsnachweis anzubieten:

1. nach § 18 des Personalausweisgesetzes (PAuswG),
2. nach § 78 Abs. 5 des Aufenthaltsgesetzes (AufenthG),
3. nach § 12 des eID-Karte-Gesetzes (eIDKG) oder
4. durch ein anderes sicheres Verfahren, das gesetzlich oder durch Rechtsverordnung der Staatsregierung als Identifizierungs- oder Authentifizierungsmittel oder zum Ersatz der Schriftform zugelassen ist.

Art. 20
Digitale Verfahren als Regelfall

(1) [1]Staatliche Behörden sollen geeignete Verwaltungsverfahren oder Teile hiervon in der Regel digital durchführen. [2]Digital durchgeführte Verfahren sind von den staatlichen Behörden nutzerfreundlich im Sinne des Art. 10 zu gestalten. [3]Art. 12 bleibt unberührt.

(2) [1]Verwaltungsleistungen, die über ein Organisationskonto im Sinne des Art. 29 Abs. 2 Satz 2 abgewickelt werden, können auch ausschließlich digital angeboten werden. [2]Zur Vermeidung unbilliger Härten ist auf eine digitale Abwicklung auf Antrag des Beteiligten zu verzichten, wenn diese persönlich oder wirtschaftlich unzumutbar ist.

(3) Der Freistaat Bayern, die Gemeindeverbände und die Gemeinden können Verwaltungsdienstleistungen im Bereich der Personalverwaltung und Personalwirtschaft gegenüber ihren Beschäftigten ausschließlich digital anbieten und erbringen.

Art. 21
Digitale Assistenzdienste

(1) [1]Die Staatsministerien können beim Angebot digitaler Verwaltungsleistungen den Einsatz digitaler Assistenzdienste gewerblicher Anbieter durch Bekanntmachung zulassen. [2]In der Bekanntmachung sind für die jeweilige Verwaltungsleistung die amtlichen Datensätze und amtlichen Schnittstellen zu bezeichnen.

(2) [1]Bei der elektronischen Übermittlung von amtlich vorgeschriebenen Datensätzen an die zuständigen Behörden hat der Anbieter gewerblicher Assistenzdienste die hierfür amtlich bestimmten Schnittstellen ordnungsgemäß zu bedienen. [2]Die amtlich bestimmten Schnittstellen werden über das Internet zur Verfügung gestellt.

Art. 22
Zustimmung im digitalen Verfahren

(1) [1]Die Durchführung digitaler Verwaltungsverfahren erfolgt mit Zustimmung des oder der Beteiligten, soweit gesetzlich nichts anderes bestimmt ist. [2]Die Zustimmung kann für einzelne Verfahren oder generell erteilt werden. [3]Sie kann die Weitergabe personenbezogener Daten an andere digitale Anwendungen und Verfahren umfassen.

(2) [1]Die generelle Zustimmung im digitalen Verwaltungsverfahren soll digital über das Nutzerkonto gemäß Art. 29 erteilt werden. [2]Die Zustimmung ist im Nutzerkonto zu dokumentieren und kann mit Wirkung für die Zukunft widerrufen werden.

Art. 23
Digitale Nachweise, Direktabruf von Belegen

(1) [1]Die Beteiligten können benötigte Nachweise und Unterlagen digital einreichen, soweit durch Rechtsvorschrift nichts anderes bestimmt ist. [2]Die Behörde kann für bestimmte Verfahren oder im Einzelfall die Vorlage eines Originals oder amtlich beglaubigter Kopien verlangen.

(2) [1]Von einer zuständigen inländischen Behörde zur Vorlage verlangte Informationen sollen mit Zustimmung der betroffenen Person von der Behörde selbst eingeholt werden, wenn die Informationen von der Behörde in digitaler Form aus Registern abgerufen werden können. [2]Für den Abruf nach Satz 1 werden Kosten nach Maßgabe des Kostengesetzes erhoben. [3]Die betroffene Person ist über die Kosten des Abrufs vorab zu informieren. [4]Sonstige gesetzliche Regelungen bleiben unberührt.

Art. 24
Bekanntgabe über Portale

(1) [1]Mit Einwilligung des Beteiligten können Verwaltungsakte bekannt gegeben werden, indem sie dem Beteiligten oder einem von ihm benannten Dritten zum Datenabruf durch Datenfernübertragung bereitgestellt werden. [2]Für den Abruf hat sich die abrufberechtigte Person zu authentifizieren.

(2) [1]Der Verwaltungsakt gilt am dritten Tag, nachdem die digitale Benachrichtigung über die Bereitstellung des Verwaltungsakts zum Abruf an die abrufberechtigte Person abgesendet wurde, als bekannt gegeben. [2]Dies gilt nicht, wenn die digitale Benachrichtigung nicht oder zu einem späteren Zeitpunkt zugegangen ist. [3]Im Zweifel hat die Behörde den Zugang der digitalen Benachrichtigung nachzuweisen. [4]Gelingt ihr der Nachweis nicht, gilt der Verwaltungsakt in dem Zeitpunkt als bekannt gegeben, in dem die abrufberechtigte Person den Datenabruf durchgeführt hat.

(3) Die Übermittlung der Benachrichtigung, der Tag der Bereitstellung zum Abruf und des Versands der Benachrichtigung sowie der Abruf durch die abrufberechtigte Person sind zu protokollieren und in den Akten zu vermerken.

Art. 25
Zustellung über Portale

[1]Ein elektronisches Dokument kann, unbeschadet des Art. 5 Abs. 4 bis 6 des Bayerischen Verwaltungszustellungs- und Vollstreckungsgesetzes (VwZVG), auch durch Bereitstellung zum Datenabruf gemäß Art. 24 zugestellt werden. [2]Die Zustellung setzt voraus, dass der Beteiligte ausdrücklich in die Zustellung durch Bereitstellung zum Datenabruf einwilligt. [3]Der Beteiligte ist vor der Einwilligung unter ausdrücklichem Hinweis auf diese Rechtsvorschrift über die Rechtsfolgen der Zustellung zu informieren.

Kapitel 3
Portalverbund Bayern

Art. 26
Portalverbund Bayern

(1) [1]Der Freistaat Bayern errichtet und betreibt den Portalverbund Bayern. [2]Der Portalverbund Bayern umfasst das Bayernportal und das Organisationsportal Bayern. [3]Der Portalverbund Bayern stellt sicher, dass Nutzer einen barriere- und medienbruchfreien Zugang zu elektronischen Verwaltungsleistungen der Behörden in Bayern erhalten. [4]Der Portalverbund Bayern ist auch das Verwaltungsportal des Freistaates Bayern im Sinne des § 1 Abs. 2 OZG.

(2) Über den Portalverbund Bayern werden von den Behörden

1. aktuelle Informationen über Verwaltungsleistungen, Anschrift, Geschäftszeiten sowie postalische, telefonische und digitale Erreichbarkeiten zur Verfügung gestellt,

2. die Rechte aus den Art. 11 bis 13 gewährleistet,

3. der digitale Zugang zur Verwaltung nach Art. 16 eröffnet,
4. digitale Behördendienste nach Art. 17 bereitgestellt,
5. der digitale Zahlungsverkehr nach Art. 18 ermöglicht,
6. Verwaltungsverfahren nach Maßgabe der Art. 19 bis 25 abgewickelt,
7. Verwaltungsverfahren bereitgestellt, die über den Einheitlichen Ansprechpartner oder über die einheitliche Stelle abgewickelt werden können,
8. die Identifizierung mit einem digitalen Identitätsnachweis nach Art. 19 Abs. 3 ermöglicht,
9. Nutzerkonten nach den Art. 29 bis 32 bereitgestellt und
10. die Pflichten der Behörden aus dem Onlinezugangsgesetz und aus der Verordnung (EU) 2018/1724 erfüllt.

Art. 27
Bayernportal

[1]Das Bayernportal ist das allgemeine Verwaltungsportal des Freistaates Bayern. [2]Über das Bayernportal stellt der Freistaat Bayern Funktionen bereit, um insbesondere

1. eine elektronische Suche nach Verwaltungsleistungen anzubieten der Behörden des Freistaates Bayern und der Gemeindeverbände und Gemeinden anzubieten,
2. die Identifizierung und Authentifizierung über das Bürgerkonto gemäß Art. 29 Abs. 2 Satz 1 zu ermöglichen,
3. Online-Antragsformulare für die elektronische Beantragung von Verwaltungs- und Justizleistungen der Behörden des Freistaates Bayern und der Gemeindeverbände und Gemeinden bereitzustellen, und
4. einen sicheren elektronischen Übermittlungsweg für die Behörden zu eröffnen, der es ihnen ermöglicht Bescheide und sonstige Dokumente elektronisch an das Postfach im Bürgerkonto des Antragsstellers zu übermitteln, soweit der Antragssteller diesen Kommunikationskanal gewählt hat.

Art. 28
Organisationsportal Bayern

(1) Der Freistaat Bayern errichtet und betreibt ein elektronisches, über allgemein zugängliche Netze aufrufbares Verwaltungsportal, das die landesweite, elektronische Abwicklung von Verwaltungs- und Justizleistungen ermöglicht, die über das Organisationskonto im Sinne von Art. 29 Abs. 2 Satz 2 in Anspruch genommen werden können (Organisationsportal).

(2) Über das Organisationsportal werden alle Verwaltungsverfahren bereitgestellt, die über das „einheitliche digitale Zugangstor“ im Sinne der Verordnung (EU) Nr. 2018/1724 abgewickelt werden.

(3) Die Behörden sind zur elektronischen Abwicklung der im Organisationsportal bereitgestellten Verwaltungsleistungen verpflichtet, die der Nutzer über das Portal einleitet oder anfordert.

(4) [1]Die Behörden müssen die für die Abwicklung erforderlichen technischen und organisatorischen Voraussetzungen schaffen. [2]Sie sollen der effizienten Verfahrensgestaltung dienende technische Einrichtungen, technische Kommunikationsstandards und Möglichkeiten zur medienbruchfreien Datenübermittlung nutzen.

Art. 29
Nutzerkonto, Postfach

(1) [1]Der Freistaat Bayern stellt im Portalverbund Bayern Nutzerkonten bereit, über die sich Nutzer für die im Portalverbund angebotenen Verwaltungs- und Justizleistungen einheitlich identifizieren und authentisieren können. [2]Das Nutzerkonto umfasst auch ein Postfach, das die Bekanntgabe und Zustellung von Verwaltungsakten und die Übermittlung sonstiger elektronischer Dokumente und Informationen von den Behörden, Gerichten oder Staatsanwaltschaften ermöglicht. [3]Nutzerkonten werden als jeweils eigenständige Bürger- und Organisationskonten angeboten.

(2) [1]Ein Bürgerkonto ist ein Nutzerkonto, das natürlichen Personen für ihre privaten, nicht wirtschaftlichen Verwaltungskontakte zur Verfügung steht. [2]Ein Organisationskonto ist ein Nutzerkonto, das juristischen Personen, Vereinigungen, denen ein Recht zustehen kann, natürlichen Personen, die beruflich oder wirtschaftlich tätig sind oder wirtschaftliche Fördermaßnahmen in Anspruch nehmen, Land- und Forstwirten sowie Behörden zur Verfügung steht.

(3) [1]Über das Organisationskonto können sich Nutzer für die im Organisationsportal des Freistaates Bayern verfügbaren digitalen Verwaltungsleistungen einheitlich über ein nach § 87a Abs. 6 Satz 1 AO in der Steuerverwaltung eingesetztes sicheres Verfahren identifizieren und authentifizieren. [2]Das schließt den Einsatz von Identifizierungsmitteln für natürliche Personen als Vertreter von Organisationen nicht aus.

(4)[1]Die Behörden haben die Nutzerkonten im Rahmen ihrer Online-Dienste anzubinden. [2]Dies gilt nicht für Online-Dienste, die über rein verwaltungsinterne Portale angeboten werden.

Art. 30
Funktionsumfang des Nutzerkontos, Datenschutz

(1) [1]Im Nutzerkonto werden die zur Identifizierung des Nutzers gespeicherten Daten und die in das Postfach übermittelten elektronischen Dokumente so aufgeführt, dass sie für ihn nach vorheriger Authentifizierung jederzeit einsehbar sind. [2]Der Nutzer

hat die Möglichkeit über ihn im Nutzerkonto gespeicherte Daten, im Postfach gespeicherte Dokumente oder auch das gesamte Nutzerkonto zu löschen. [3]Die Sicherheit des Nutzerkontos wird nach dem Stand der Technik gewährleistet.

(2) [1]Das Nutzerkonto ist mit einer Funktion zu verknüpfen, die es dem Nutzer ermöglicht, sich über aktive Zustimmungen und die auf dieser Grundlage derzeit übermittelten Daten zu informieren, Zustimmungen zu erteilen sowie jederzeit zu widerrufen. [2]Daten aus dem Nutzerkonto können mit Zustimmung des Nutzers automatisiert in die zur Antragstellung bereitgestellten Formulare übernommen werden.

(3) [1]Das Nutzerkonto umfasst eine sichere Archivierungsfunktion für digitale amtliche Dokumente des Nutzers. [2]Die im Nutzerkonto gespeicherten Dokumente sind vor unberechtigten Zugriffen und Veränderungen zu schützen. [3]Sie sind zum Datenabruf durch den Nutzer auch zur mobilen Vorlage bereitzustellen. [4]Von den zuständigen Behörden in das Postfach übermittelte digitale Dokumente können zur Erfüllung von Nachweispflichten auch digital als Nachweis vorgelegt werden.

(4) Die Datenverarbeitungsvorgänge, die im Zusammenhang mit der Antragsstellung über das Nutzerkonto stehen, sind in digital abrufbarer Form im Nutzerkonto zu speichern.

Art. 31
Identifizierung am Nutzerkonto, Schriftformersatz

(1) [1]Der Nachweis der Identität eines Nutzers kann durch unterschiedliche Identifizierungsmittel erfolgen. [2]Vor jeder Verwendung muss der Nutzer die Zustimmung zur Verarbeitung seiner Identitätsdaten für die konkrete digitale Verwaltungs- und Justizleistung erteilen. [3]Der Nutzer kann die Zustimmung zur Verarbeitung seiner Identitätsdaten auch generell für alle Verwaltungs- und Justizleistungen erteilen. [4]In den Fällen des Satzes 3 ist der Nutzer bei der Zustimmung über deren rechtliche Folgen zu informieren. [5]Die Zustimmung ist zu protokollieren und kann jederzeit widerrufen werden.

(2) [1]In Verwaltungsverfahren kann sich jeder Nutzer unter Inanspruchnahme des Nutzerkontos identifizieren

1. durch einen Identitätsnachweis nach § 18 PAuswG, nach § 78 Abs. 5 AufenthG oder nach § 12 eIDKG,

2. durch ein sicheres Verfahren nach § 87a Abs. 6 Satz 1 AO oder

3. durch ein anderes sicheres Verfahren, das gesetzlich oder durch Rechtsverordnung der Staatsregierung als Identifizierungs- oder Authentifizierungsmittel oder zum Ersatz der Schriftform zugelassen ist.

[2]Die zuständige Behörde kann von einer Identifizierung durch ein Verfahren im Sinne von Satz 1 für einzelne Verwaltungsverfahren absehen, soweit Sicherheitsbedenken nicht entgegenstehen. [3]Satz 1 Nr. 2 und 3 sowie Satz 2 gelten nicht, soweit durch gesetzliche Vorschrift ein Identitätsnachweis nach § 18 PAuswG, nach § 78 Abs. 5

AufenthG oder nach § 12 eIDKG genutzt wird. [4]In begründeten Ausnahmefällen kann die Behörde ein Verfahren im Sinne des Satzes 3 auch für weitere Verwaltungsverfahren vorsehen.

(3) [1]Das nach § 87a Abs. 6 Satz 1 AO eingesetzte sichere Verfahren ersetzt im Falle der Identifizierung und Authentifizierung am Nutzerkonto auch eine durch Rechtsvorschrift angeordnete Schriftform. [2]Gleiches gilt für Dienste anderer Mitgliedstaaten, die nach Maßgabe der Verordnung (EU) Nr. 910/2014 auf dem Vertrauensniveau „hoch“ notifiziert worden sind.

Art. 32
Rechtsgrundlage der Datenverarbeitung

(1) [1]Zur Feststellung der Identität des Nutzers dürfen bei Registrierung und Nutzung eines Nutzerkontos die zur Identitätsfeststellung erforderlichen Daten natürlicher und juristischer Personen verarbeitet werden. [2]Gleiches gilt für Daten, die zum bestimmungsgemäßen Betrieb des Nutzerkontos und zur Abwicklung von Verwaltungsverfahren über das Nutzerkonto erforderlich sind. [3]Bei Einsatz des Nutzerkontos dürfen die zur Durchführung des Verwaltungsverfahrens oder zur Inanspruchnahme sonstiger Leistungen der öffentlichen Verwaltung erforderlichen Daten verarbeitet werden.

(2) Daten im Sinne des Abs. 1 dürfen auch zwischen den Nutzerkonten von Bund und Ländern ausgetauscht und an weitere öffentliche Stellen weitergegeben werden, soweit dies zur Durchführung eines Verwaltungsverfahrens oder zur Inanspruchnahme eines Dienstes erforderlich ist.

(3) [1]Daten im Sinne des Abs. 1 sind im Nutzerkonto zu speichern und können automatisiert aktualisiert werden, soweit die Daten für den Betrieb des Nutzerkontos oder die Abwicklung von Verwaltungsverfahren über das Nutzerkonto erforderlich sind. [2]Sie können zur Abwicklung von Verwaltungsverfahren genutzt und in die hierfür bereitgestellten Verfahren und Formulare automatisiert übertragen werden.

Kapitel 4
Digitale Akten und Register

Art. 33
Digitale Akten

(1) [1]Die staatlichen Behörden sollen, Landratsämter und sonstige Behörden können, ihre Akten digital führen. [2]Die Grundsätze ordnungsgemäßer Aktenführung sind zu wahren. [3]Die verarbeiteten Daten sind vor Informationsverlust sowie unberechtigten Zugriffen und Veränderungen zu schützen.

(2) Nutzt eine Behörde die digitale Aktenführung, soll sie Akten, Vorgänge und Dokumente gegenüber anderen Behörden unter Einhaltung der datenschutzrechtlichen Bestimmungen digital übermitteln.

(3) [1]Papierdokumente sollen in ein digitales Format übertragen und gespeichert werden. [2]Sie können anschließend vernichtet werden, soweit keine entgegenstehenden Pflichten zur Rückgabe oder Aufbewahrung bestehen. [3]Bei der Übertragung ist nach dem Stand der Technik sicherzustellen, dass die digitale Fassung mit dem Papierdokument übereinstimmt.

(4) Die Verfahren zur elektronischen Vorgangsbearbeitung und Aktenführung sind schrittweise technisch so zu gestalten, dass sie auch von Menschen mit Behinderung grundsätzlich uneingeschränkt genutzt werden können.

Art. 34
Einsicht in die digitale Akte

[1]Die Einsicht in digital geführte Akten ist in nutzerfreundlicher Form sicherzustellen. [2]Soweit ein Recht auf Akteneinsicht besteht, können die Behörden, die Akten digital führen, Akteneinsicht dadurch gewähren, dass sie

1. einen Aktenausdruck zur Verfügung stellen,
2. die digitalen Dokumente auf einem Bildschirm wiedergeben,
3. digitale Dokumente übermitteln oder
4. den digitalen Zugriff auf den Inhalt der Akten gestatten.

Art. 35
Digitale Register

[1]Die staatlichen Behörden sollen ihre Register digital führen. [2]Landratsämter und sonstige Behörden können ihre Register digital führen.

Kapitel 5
Behördenzusammenarbeit, Rechenzentren

Art. 36
Behördliche Zusammenarbeit

[1]Die Behörden unterhalten die zur Erfüllung ihrer Aufgaben erforderlichen digitalen Verwaltungsinfrastrukturen. [2]Sie gewährleisten deren Sicherheit und fördern deren gegenseitige technische Abstimmung und Barrierefreiheit. [3]Die Behörden können bei Entwicklung, Einrichtung und Betrieb von digitalen Verwaltungsinfrastrukturen zusammenwirken und sich diese wechselseitig zur öffentlichen Aufgabenerfüllung überlassen.

Art. 37
Basisdienste und zentrale Dienste

(1) [1]Der Freistaat Bayern soll digitale Verwaltungsinfrastrukturen zur behördenübergreifenden Nutzung bereitstellen (Basisdienste). [2]Die datenschutzrechtliche Ver-

antwortung für die Nutzung liegt bei der nutzenden Stelle. [3]Die Möglichkeit einer gemeinsamen Verantwortung gemäß Art. 26 der Verordnung (EU) 2016/679 (Datenschutz–Grundverordnung – DSGVO) bleibt hiervon unberührt.

(2) [1]Der Freistaat Bayern soll den Behörden digitale Verwaltungsinfrastrukturen des Staatsministeriums für Digitales oder des Staatsministeriums der Finanzen und für Heimat bereitstellen (zentrale Dienste). [2]Die datenschutzrechtliche Verantwortung liegt beim bereitstellenden Staatsministerium. [3]Personenbezogene Daten können mit Zustimmung des Nutzers an angeschlossene Behörden übermittelt werden. [4]Diese personenbezogenen Daten dürfen ausschließlich für die Zwecke der zentralen Dienste verarbeitet werden.

(3) [1]Behördenübergreifende Dienste werden in der Regel als Basisdienste angeboten. [2]Die Bereitstellung als zentraler Dienst ist von der bereitstellenden Behörde ausdrücklich festzulegen.

(4) [1]Der Freistaat Bayern stellt den Behörden Dienste im Sinne des Abs. 1 und 2 zur Aufgabenerfüllung zur Verfügung, soweit dies wirtschaftlich und zweckmäßig ist. [2]Die Behörden können ihre Verpflichtungen gemäß den Art. 16 bis 25 auch durch den Anschluss an Dienste im Sinne der Abs. 1 und 2 erfüllen.

(5) Die Bereitstellung von Diensten im Sinne des Abs. 1 Satz 1 erfolgt durch das Staatsministerium für Digitales im Einvernehmen mit dem Staatsministerium der Finanzen und für Heimat.

Art. 38
Auftragsverarbeitung durch staatliche Stellen

(1) [1]Unabhängig vom Anwendungsbereich dieses Gesetzes erfolgt die datenschutzrechtliche Auftragsverarbeitung durch staatliche Stellen für öffentliche Stellen auf Grundlage eines Vertrages im Sinne des Art. 28 Abs. 3 Satz 1 Alternative 1 DSGVO oder § 62 Abs. 5 Satz 1 Alternative 1 des Bundesdatenschutzgesetzes und mit dem Vertragsinhalt, wie er nach Maßgabe dieses Artikels bestimmt wird, wenn und soweit die Auftragsverarbeitung nicht anderweitig gesetzlich geregelt ist. [2]Zur Begründung eines Auftragsverarbeitungsverhältnisses durch Vertrag teilt der Verantwortliche dem Auftragsverarbeiter in Textform mit:

1. Gegenstand und Dauer der Verarbeitung,
2. Art und Zweck der Verarbeitung,
3. die Art der personenbezogenen Daten und
4. die Kategorien betroffener Personen.

(2) [1]Bereits bestehende Auftragsverarbeitungsverhältnisse im Sinne des Abs. 1 Satz 1 werden zum Ablauf des dritten auf das Inkrafttreten des Gesetzes folgenden

Kalenderjahres ungültig, soweit nicht rechtzeitig vor diesem Zeitpunkt der Verantwortliche oder der Auftragsverarbeiter ein bestehendes Auftragsverarbeitungsverhältnis in Textform bestätigt und der jeweils andere Vertragspartner zustimmt. [2]Die allgemeinen Nutzungsbedingungen zur datenschutzrechtlichen Auftragsverarbeitung werden in der jeweils geltenden Fassung, die durch Bekanntmachung der Staatsregierung im Bayerischen Ministerialblatt festgelegt werden, Bestandteil des Vertrages im Sinne des Abs. 1 Satz 1, soweit Verantwortlicher und Auftragsverarbeiter nicht eine abweichende individualvertragliche Vereinbarung treffen. [3]Die allgemeinen Nutzungsbedingungen zur datenschutzrechtlichen Auftragsverarbeitung können auch Regelungen zur Begründung von weiteren Auftragsverarbeitungsverhältnissen enthalten.

Art. 39
Bayernserver

(1) Die für die Digitalisierung der staatlichen öffentlichen Verwaltung erforderlichen Infrastrukturen, insbesondere Leitungen, Server und Programme, sind nach Stand der Technik und der angemessenen Verfügbarkeit einzurichten und vorzuhalten.

(2) [1]Die staatliche öffentliche Verwaltung betreibt im Geschäftsbereich des Staatsministeriums der Finanzen und für Heimat sowohl ein zentrales Rechenzentrum als Dienstleister für den IT-Betrieb der Staatsverwaltung und der Fachgerichte als auch ein spezialisiertes Rechenzentrum für den IT-Betrieb im Bereich der Steuerverwaltung und für die Gerichte und Staatsanwaltschaften (Bayernserver). [2]Den Rechenzentren obliegt auch der Betrieb von bestimmten Diensten und Anwendungen im Sinne der Art. 26 bis 29 und von bestimmten Basisdiensten und zentralen Diensten im Sinne des Art. 37. [3]Das Staatsministerium der Finanzen und für Heimat steuert die beiden vorgenannten staatlichen Rechenzentren. [4]Die Befugnisse der Gerichtsbarkeiten bleiben hiervon unberührt. [5]Polizeiliche Fachanwendungen werden in einem spezialisierten Rechenzentrum im Geschäftsbereich des Staatsministeriums des Innern, für Sport und Integration betrieben. [6]Es stimmt sich hinsichtlich Aufbau und Betrieb der Rechenzentrumsflächen mit dem Staatsministerium der Finanzen und für Heimat ab.

(3) [1]Der Bayernserver stellt im Benehmen mit der Staatskanzlei und den Staatsministerien staatliche Informationstechnik zur Verfügung. [2]Die Aufgaben des zentralen Rechenzentrums umfassen insbesondere

1. die Beobachtung der Entwicklungen in der Informationstechnik,
2. das Bereitstellen und den Betrieb von IT-Infrastruktursystemen für die Informationstechnik der staatlichen öffentlichen Verwaltung,
3. die Entwicklung und den Betrieb ressortübergreifender digitaler Verwaltungsverfahren unter Berücksichtigung der Regelungen des Datenschutzes und der Datensicherheit,

4. den Auf- und Ausbau sowie die Förderung des Datenaustausches mit Dritten auf der Basis standardisierter Prozesse und Techniken,

5. die Beratung der staatlichen öffentlichen Verwaltung bei Planung, Entwicklung und Einsatz digitaler Verwaltungsverfahren und

6. die Übernahme von Entwicklungen und des Betriebs der von der Staatskanzlei oder einem Staatsministerium beauftragten digitalen Verwaltungsverfahren nach Maßgabe des Staatshaushaltes.

[3]Die Rechenzentren im Sinne des Abs. 2 können im Einvernehmen mit den betroffenen obersten Dienstbehörden Dritte mit der Durchführung der ihnen obliegenden Aufgaben betrauen. [4]Auf der Basis von Vereinbarungen oder öffentlich-rechtlichen Verträgen können auch der Landtag, Kommunen oder sonstige Personen des öffentlichen Rechts die Dienste der Rechenzentren im Sinne des Abs. 2 im Einvernehmen mit den betroffenen obersten Dienstbehörden in Anspruch nehmen. [5]Im Rahmen der Umsetzung des Onlinezugangsgesetzes und von IT-Kooperationen ist auch eine Aufgabenübernahme für Behörden außerhalb Bayerns möglich.

Art. 40
Staatlich verfügbare Netze

(1) Der Freistaat Bayern unterhält staatlich verfügbare Netze für die behördeninterne Kommunikation.

(2) Zur Festigung seiner strategischen Autonomie in den staatlich verfügbaren Netzen, kann der Freistaat Bayern zukünftig seine Fertigungstiefe in Bezug auf die eigene Netzinfrastruktur erhöhen.

Teil 3
IT-Sicherheit

Kapitel 1
Allgemeine Vorschriften

Art. 41
Landesamt für Sicherheit in der Informationstechnik

[1]Es besteht ein Landesamt für Sicherheit in der Informationstechnik (Landesamt). [2]Es ist dem Staatsministerium der Finanzen und für Heimat unmittelbar nachgeordnet.

Art. 42
Aufgaben

(1) Das Landesamt hat

1. Gefahren für die Sicherheit der Informationstechnik an den Schnittstellen zwischen Behördennetz und anderen Netzen abzuwehren,

2. die staatlichen und die sonstigen an das Behördennetz angeschlossenen Stellen bei der Abwehr von Gefahren für die Sicherheit in der Informationstechnik zu unterstützen,

3. sicherheitstechnische Mindeststandards an die Informationstechnik für die staatlichen und die sonstigen an das Behördennetz angeschlossenen Stellen zu entwickeln,

4. die Einhaltung der Mindeststandards nach Nr. 3 zu prüfen,

5. alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen zu sammeln und auszuwerten sowie die staatlichen und sonstigen an das Behördennetz angeschlossenen Stellen unverzüglich über die sie betreffenden Informationen zu unterrichten und

6. die zuständigen Aufsichtsbehörden über Informationen, die es als Kontaktstelle im Rahmen des Verfahrens zu § 8b des BSI-Gesetzes erhalten hat, zu unterrichten.

(2) Auf Ersuchen kann das Landesamt staatliche und kommunale Stellen, öffentliche Unternehmen, Betreiber kritischer Infrastrukturen und weitere Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen beraten und unterstützen.

(3) Auf Ersuchen kann das Landesamt die Polizei, die Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz bei der Wahrnehmung ihrer gesetzlichen Aufgaben technisch unterstützen, insbesondere bei der Durchführung von technischen Untersuchungen oder der Datenverarbeitung.

(4) Für die Kommunikationstechnik des Landtags, der Gerichte, des Obersten Rechnungshofs und des Landesbeauftragten für den Datenschutz ist das Landesamt nur zuständig, soweit sie an das Behördennetz angeschlossen sind oder Dienste im Sinne des Art. 37 nutzen.

Art. 43
Behördenübergreifende Pflichten

(1) [1]Die Sicherheit der informationstechnischen Systeme der Behörden ist im Rahmen der Verhältnismäßigkeit sicherzustellen. [2]Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen im Sinn von Art. 32 DSGVO und Art. 32 des Bayerischen Datenschutzgesetzes und erstellen die hierzu erforderlichen Informationssicherheitskonzepte.

(2) Werden staatlichen oder sonstigen an das Behördennetz angeschlossenen Stellen Informationen bekannt, die zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Bedeutung sind, unterrichten diese das Landesamt und ihre jeweilige oberste Dienstbehörde unverzüglich hierüber, soweit andere Vorschriften oder Vereinbarungen mit Dritten nicht entgegenstehen.

(3) Die staatlichen und die sonstigen an das Behördennetz angeschlossenen Stellen unterstützen das Landesamt bei Maßnahmen nach Art. 42 Abs. 1 Nr. 1, 2, 4 und 5, soweit keine Vorschriften entgegenstehen.

(4) Bei der Planung und Umsetzung von maßgeblichen neuen Digitalisierungsvorhaben des Landes ist das Landesamt zur Gewährleistung der Sicherheit in der Informationstechnik durch die jeweils zuständige Stelle frühzeitig zu beteiligen und es ist ihm die Gelegenheit zur Stellungnahme zu geben.

Kapitel 2
Befugnisse

Art. 44
Abwehr von Gefahren für die Informationstechnik

(1) [1]Das Landesamt kann zur Erfüllung seiner Aufgaben gegenüber staatlichen und an das Behördennetz angeschlossenen Stellen die nötigen Anordnungen treffen oder Maßnahmen ergreifen, um Gefahren für die Informationstechnik etwa durch Schadprogramme, programmtechnische Sicherheitslücken oder unbefugte Datenverarbeitung zu erkennen und abzuwehren. [2]Das umfasst insbesondere auch die dazu nötige Datenverarbeitung gemäß Abs. 2. [3]Die Sätze 1 und 2 gelten nicht für die vom Behördennetz getrennte Informationstechnik des Landesamts für Verfassungsschutz.

(2) Das Landesamt kann hierzu, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist,

1. Protokolldaten erheben und automatisiert auswerten, die beim Betrieb von Informationstechnik des Landes oder der an das Behördennetz angeschlossenen Stellen anfallen,

2. Daten erheben und automatisiert auswerten, die an den Schnittstellen zwischen dem Behördennetz und anderen Netzen und an vergleichbaren Schnittstellen innerhalb des Behördennetzes anfallen,

3. Daten aus öffentlich zugänglichen Quellen, die Informationen mit Auswirkungen auf die Sicherheit der Informationstechnik des Landes oder der an das Behördennetz angeschlossenen Stellen haben können, erheben und automatisiert auswerten und

4. bei der Untersuchung von Informationstechnik des Landes oder der an das Behördennetz angeschlossenen Stellen, soweit ein Angriff auf die Informationstechnik anzunehmen ist, zur Bearbeitung des Angriffs die dort gespeicherten Daten verarbeiten.

(3) Soweit das Landesamt zur Erfüllung seiner Aufgaben nach Art. 42 Abs. 2 gegenüber kommunalen Stellen, öffentlichen Unternehmen, Betreibern kritischer Infrastrukturen und weiteren Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen personenbezogene Daten verarbeitet, handelt das Landesamt als Auftragsverarbeiter der für die Daten verantwortlichen Stelle nach Art. 28 DSGVO.

Art. 45
Untersuchung der Sicherheit in der Informationstechnik

(1) [1]Das Landesamt kann zur Erfüllung seiner Aufgaben nach Art. 42 Abs. 1 Nr. 1 und 4 die Sicherheit der Informationstechnik staatlicher und an das Behördennetz angeschlossener Stellen untersuchen und bewerten. [2]Über das Ergebnis erstellt das Landesamt einen Bericht, der der untersuchten Stelle zur Verfügung gestellt wird.

(2) [1]Das Landesamt kann auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen und bewerten. [2]Die Bewertung kann vom Landesamt an die an das Behördennetz angeschlossenen Stellen und im Einzelfall an die in Art. 42 Abs. 2 genannten öffentlichen Stellen weitergegeben werden.

Art. 46
Mindeststandards

[1]Das Landesamt erarbeitet Mindeststandards für die Sicherheit der Informationstechnik. [2]Das Staatsministerium der Finanzen und für Heimat kann im Einvernehmen mit den weiteren Staatsministerien und der Staatskanzlei diese Mindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften erlassen. [3]Für Landratsämter und die an das Behördennetz angeschlossenen nicht staatlichen Stellen gelten die Mindeststandards für die Teilnahme am Behördennetz.

Art. 47
Warnungen

(1) Das Landesamt kann Warnungen zu Gefahren für die Sicherheit in der Informationstechnik, insbesondere zu Sicherheitslücken, Schadprogrammen oder unbefugten Datenzugriffen aussprechen und Sicherheitsmaßnahmen empfehlen.

(2) [1]Stellen sich die von der Behörde an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch oder die zu Grunde liegenden Umstände als unrichtig wiedergegeben heraus, so ist dies unverzüglich öffentlich bekannt zu machen, sofern der betroffene Wirtschaftsbeteiligte dies beantragt oder dies zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist. [2]Diese Bekanntmachung soll in derselben Weise erfolgen, in der die Information der Öffentlichkeit ergangen ist.

Kapitel 3
Datenschutz

Art. 48
Datenspeicherung und -auswertung

(1) [1]Sofern nicht die nachfolgenden Absätze eine weitere Verarbeitung gestatten, muss eine automatisierte Auswertung der Daten durch das Landesamt unverzüglich erfolgen und müssen die Daten nach erfolgtem Abgleich sofort und spurlos gelöscht

werden. [2]Daten, die weder dem Fernmeldegeheimnis unterliegen noch Personenbezug aufweisen, sind von den Verarbeitungseinschränkungen dieser Vorschrift ausgenommen.

(2) [1]Protokolldaten nach Art. 44 Abs. 2 Nr. 1 dürfen über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus, längstens jedoch für zwölf Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass die Daten erforderlich sein können

1. für den Fall der Bestätigung eines Verdachts nach Abs. 4 Satz 1 Nr. 2 zur Abwehr von Gefahren für die Informationstechnik oder

2. zur Verhütung, Unterbindung oder Verfolgung damit zusammenhängender Straftaten.

[2]Die Daten sind im Gebiet der Europäischen Union zu speichern. [3]Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt. [4]Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. [5]Eine nicht automatisierte Auswertung oder eine personenbezogene Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. [6]Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch die Behördenleitung angeordnet werden. [7]Die Entscheidung ist zu dokumentieren.

(3) [1]Für die Datenverarbeitung von Inhaltsdaten gilt Abs. 2 mit der Maßgabe, dass eine Speicherung für höchstens zwei Monate zulässig ist, die Speicherung und Auswertung von der Behördenleitung und einem weiteren Bediensteten des Landesamts mit der Befähigung zum Richteramt angeordnet sind und dies zum Schutz der technischen Systeme unerlässlich ist. [2]Die Anordnung gilt längstens für zwei Monate; sie kann verlängert werden.

(4) [1]Eine über die Abs. 2 und 3 hinausgehende Verarbeitung der Daten ist nur zulässig,

1. wenn bestimmte Tatsachen den Verdacht begründen, dass die Daten Gefahren für die Informationstechnik, etwa durch Schadprogramme, programmtechnische Sicherheitslücken oder unbefugte Datenverarbeitung, enthalten oder Hinweise auf solche Gefahren geben können und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen,

2. wenn sich der Verdacht nach Nr. 1 bestätigt und soweit dies zur Abwehr von Gefahren für die Informationstechnik erforderlich ist oder

3. wenn bei einer Verarbeitung der Daten ein nach Art. 49 Abs. 2 zu übermittelndes Datum festgestellt wird.

[2]Werden Daten, welche die richterliche Unabhängigkeit berühren, nach diesem Absatz verarbeitet, ist dies der jeweils zuständigen obersten Dienstbehörde unverzüglich zu berichten. [3]Berührt die Datenverarbeitung die Aufgabenwahrnehmung anderer unabhängiger Stellen oder ein Berufs- oder besonderes Amtsgeheimnis, ist die betroffene Stelle unverzüglich zu unterrichten. [4]Die jeweiligen Stellen nach den Sätzen 2 und 3 können vom Landesamt Auskunft über die Verarbeitung von Daten nach diesem Absatz verlangen.

(5) [1]Soweit möglich, ist bei der Datenverarbeitung technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. [2]Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwendet werden und sind unverzüglich zu löschen. [3]Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. [4]Dies gilt auch in Zweifelsfällen.

Art. 49
Datenübermittlung

(1) Das Landesamt übermittelt Daten nach Art. 48 Abs. 2 bis 4 an die für den Betrieb der Informations- und Kommunikationstechnik verantwortlichen Stellen, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren für die Vertraulichkeit, Verfügbarkeit und Integrität der Daten in der Informations- und Kommunikationsinfrastruktur erforderlich ist.

(2) [1]Das Landesamt soll Daten nach Art. 48 Abs. 2 bis 4 unverzüglich übermitteln

1. an die Polizei und sonstigen Sicherheitsbehörden zur Verhütung und Unterbindung von in Nr. 2 genannten Straftaten sowie zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person; Art. 24 des Bayerischen Verfassungsschutzgesetzes bleibt unberührt; und
2. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat,
   a) soweit die Tatsachen, aus denen sich eine Gefahr für die Informationstechnik oder der diesbezügliche Verdacht ergibt, den Verdacht einer Straftat begründen oder
   b) soweit bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat.

[2]Näheres regeln Verwaltungsvorschriften, die das Staatsministerium der Finanzen und für Heimat im Einvernehmen mit dem Staatsministerium des Innern, für Sport und Integration und dem Staatsministerium der Justiz festlegt.

Teil 4
Organisation

Art. 50
Kommunaler Digitalpakt

(1) Der Kommunale Digitalpakt ist das gemeinsame Gremium für die verwaltungsträgerübergreifende Zusammenarbeit zwischen dem Freistaat Bayern und den Gemeindeverbänden und Gemeinden im Bereich der Digitalisierung.

(2) [1]Dem Kommunalen Digitalpakt gehören als ständige Mitglieder an:

1. ein Vertreter des Staatsministeriums für Digitales, das den Vorsitz führt,
2. je ein Vertreter des Staatsministeriums der Finanzen und für Heimat, des Staatsministeriums des Innern für Sport und Integration und des Staatsministeriums für Wirtschaft, Landesentwicklung und Energie und
3. je ein Vertreter der kommunalen Spitzenverbände.

[2]Bei Bedarf kann der Kommunale Digitalpakt weitere Dritte als beratende Mitglieder hinzuziehen. [3]Beratende Mitglieder sind nicht stimmberechtigt.

(3) Der Kommunale Digitalpakt ist über Beschlüsse des IT-Planungsrats, Maßnahmen zur Umsetzung des Onlinezugangsgesetzes und der Verordnung (EU) 2018/1724 sowie sonstige für die Gemeindeverbände und Gemeinden relevante Rechtssetzungsvorhaben, Planungen und Maßnahmen der Europäischen Union, des IT-Planungsrats, anderer Gremien auf Bund-Länderebene und des Freistaates Bayern im Bereich der Digitalisierung zu informieren.

(4) Der Kommunale Digitalpakt kann einstimmig Empfehlungen aussprechen insbesondere

1. zu den im IT-Planungsrat behandelten Themen und den Beschlussvorschlägen des IT-Planungsrats sowie zu relevanten Rechtssetzungsvorhaben, Planungen und Maßnahmen nach Maßgabe des Abs. 3,
2. zur Umsetzung von Standardisierungsbeschlüssen nach Art. 51 soweit sie für die Gemeindeverbände und Gemeinden relevant sind,
3. zur Weiterentwicklung der Digital-Strategie des Freistaates Bayern, soweit sie alle Teilnehmer des Kommunalen Digitalpakts betrifft,
4. zu den im Freistaat Bayern vom Land und von Gemeindeverbänden und Gemeinden gegenseitig überlassenen oder gemeinsam genutzten Verwaltungsinfrastrukturen,
5. zur Förderung des Angebots digitaler öffentlicher Dienste und von anforderungsgerechten Qualifizierungsmaßnahmen,

6. zum Anschluss der Landratsämter und Gemeinden an das sichere Behördennetz des Freistaates Bayern,

7. zu landesspezifischen IT-Interoperabilitäts- und IT-Sicherheitsstandards für die ebenenübergreifende Kooperation der im Freistaat Bayern eingesetzten informationstechnischen Systeme und

8. zu digitalen Kommunikations- und Zahlungsverfahren.

(5) [1]Das Staatsministerium für Digitales berichtet dem Landesbeauftragten für den Datenschutz regelmäßig über datenschutzrelevante Themen im Sinne des Abs. 1. [2]Der Landesbeauftragte für den Datenschutz wird zu datenschutzrechtlich relevanten Empfehlungen des Kommunalen Digitalpakts angehört.

(6) [1]Der Kommunale Digitalpakt wird durch eine Geschäftsstelle beim Staatsministerium für Digitales unterstützt. [2]Der Kommunale Digitalpakt gibt sich eine Geschäftsordnung.

Art. 51
Standardisierungsbeschlüsse

(1) [1]Das Staatsministerium für Digitales legt nach Anhörung des Kommunalen Digitalpakts im Einvernehmen mit dem Staatsministerium der Finanzen und für Heimat, im Einvernehmen mit den fachlich zuständigen Ressorts und unter Beachtung der sicherheitstechnischen Mindeststandards nach Art. 42 Abs. 1 Nr. 3 IT-Standards für die im Freistaat Bayern übergreifend eingesetzten informationstechnischen Systeme fest. [2]Das Landesamt für Sicherheit in der Informationstechnik ist bei Sicherheitsfragen anzuhören.

(2) [1]Vom IT-Planungsrat gemäß § 1 Abs. 1 Satz 1 Nr. 2 und § 3 des IT-Staatsvertrages beschlossene fachunabhängige und fachübergreifende IT-Interoperabilitäts- oder IT-Sicherheitsstandards gelten für die Behörden im Sinne des Art. 1 Abs. 2. [2]Das Staatsministerium für Digitales kann nach Beteiligung des Kommunalen Digitalpakts und im Einvernehmen mit den fachlich zuständigen Staatsministerien Ausführungsbestimmungen erlassen.

Teil 5
Übergangs- und Schlussbestimmungen

Art. 52
Experimentierklausel

[1]Zur Einführung und Fortentwicklung digitaler Verwaltungsinfrastrukturen kann das Staatsministerium für Digitales im Einvernehmen mit der Staatskanzlei und den fachlich betroffenen Ressorts durch Rechtsverordnung sachlich und räumlich begrenzte Abweichungen von folgenden Vorschriften zulassen

1. Zuständigkeits- und Formvorschriften nach den Art. 3, 3a, 27a, 33, 34, 37 Abs. 2 bis 5, Art. 41, 57, 64 und 69 Abs. 2 BayVwVfG,

2. Art. 5 Abs. 4 bis 7, Art. 6 und 15 Abs. 2 VwZVG und

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

[2]Die Ausnahmegenehmigungen sind auf höchstens drei Jahre zu befristen und können verlängert werden.

Art. 53
Verordnungsermächtigungen

(1) Die Staatsregierung wird ermächtigt, durch Rechtsverordnung

1. Maßnahmen zur Gewährleistung der Barrierefreiheit in der digitalen Verwaltung im Zusammenhang mit den Förderzielen aus Art. 2 und den Aufgaben nach Art. 10 zu bestimmen,

2. ausführende Maßnahmen zum Schutz des freien Zugangs zum Internet im Sinne von Art. 8 zu treffen, insbesondere in Bezug auf die Freiheit und Pluralität der Medien, den Jugendschutz, den Schutz des unternehmerischen Wettbewerbs im Internet und die Förderung kleinerer und mittlerer Unternehmen,

3. das Nähere zum Vollzug des Art. 18, insbesondere Vorschriften, die sich auf die Ausgestaltung des elektronischen Rechnungsverkehrs, insbesondere auf die Verbindlichkeit der elektronischen Form beziehen, festzulegen,

4. Ausführungsbestimmungen zu digitalen Verwaltungsverfahren oder Teilen hiervon im Sinne des Art. 19 Abs. 1, einschließlich Mindeststandards, Übergangsvorschriften und Ausnahmen festzulegen,

5. im Rahmen von Art. 19 festzulegen, dass Verwaltungsverfahren auch über vom Freistaat Bayern festgelegte einheitliche digitale Formulare oder Online-Verfahren erreichbar sein müssen,

6. im Rahmen von Art. 19 zu bestimmen, dass für bestimmte Verwaltungsleistungen der Behörden Zugangstor-Dienste im Sinne der Art. 4 bis 7 der Verordnung (EU) Nr. 2018/1724 anzubieten oder Anforderungen im Sinne der Art. 9 bis 16 der Verordnung (EU) Nr. 2018/1724 einzuhalten sind,

7. im Rahmen von Art. 21 nähere Bestimmungen zum Einsatz digitaler Assistenzdienste gewerblicher Anbieter zu treffen, insbesondere im Hinblick auf Zuverlässigkeit und technischen Betrieb,

8. zur Umsetzung der Art. 26 bis 31 weitere Anforderungen an den Portalverbund Bayern und die Nutzerkonten, insbesondere Standards zur Nutzerfreundlichkeit,

zur Kommunikation zwischen den im Portalverbund Bayern genutzten informationstechnischen Systemen, zu Anforderungen und Standards im Sinne des Abs. 3, zur Gewährleistung von IT-Sicherheit sowie zu Art, Umfang und Aktualisierung veröffentlichungspflichtiger Informationen festzulegen, soweit nicht Zuständigkeiten aus Abs. 4 Nr. 1 und 2 bestehen,

9. im Rahmen von Art. 28 und 29 Abs. 3 Anforderungen für Verwaltungsleistungen festzulegen, die über das Organisationsportal bereitzustellen und über das Organisationskonto abzuwickeln sind,

10. weitere Identifizierungs- und Authentifizierungsmittel im Sinne von Art. 31 Abs. 2 zuzulassen,

11. Einzelheiten zu den Datenverarbeitungstatbeständen im Nutzerkonto gemäß Art. 30 Abs. 4 und für die Feststellung der Identität des Nutzers und die Kommunikation im Portalverbund Bayern im Rahmen von Art. 32 festzulegen und

12. im Rahmen von Art. 36 Einzelheiten zu Planung, Errichtung, Betrieb, Bereitstellung, Nutzung, Sicherheit und technischen Standards digitaler Verwaltungsinfrastrukturen sowie die damit zusammenhängenden Aufgaben und datenschutzrechtlichen Befugnisse der Behörden festzulegen; dies gilt für die Kommunen nur für die Behördenzusammenarbeit im Sinne von Art. 36 Satz 3.

(2) Das Staatsministerium für Digitales wird im Einvernehmen mit der Staatskanzlei ermächtigt, durch Rechtsverordnung

1. Voraussetzungen für die Bereitstellung und den Funktionsumfang der digitalen Identität sowie die Zuständigkeiten für deren Bereitstellung gemäß Art. 11 im Benehmen mit dem Staatsministerium des Innern für Sport und Integration festzulegen und

2. die technischen Voraussetzungen der Verpflichtung nach Art. 13 Abs. 2 einschließlich Übergangsfristen zu regeln.

(3) Das Staatsministerium für Digitales wird im Einvernehmen mit den fachlich zuständigen Staatsministerien ermächtigt, durch Rechtsverordnung

1. zur Ausführung von Art. 26 für Behörden der in Art. 1 Abs. 1 genannten juristischen Personen verbindliche IT-Interoperabilitätsstandards oder die Nutzung von Basisdiensten festzulegen und

2. im Rahmen von Art. 26 Mindestkataloge von Verwaltungsleistungen festzulegen, die von den zuständigen Behörden über den Portalverbund Bayern bereitgestellt werden und Standards für die einheitliche Bereitstellung dieser Leistungen über den Portalverbund festzulegen.

(4) Das Staatsministerium für Digitales wird ermächtigt, durch Rechtsverordnung

1. Einzelheiten zur Errichtung, Betrieb und Nutzung des Organisationsportals und des Organisationskontos im Sinne von Art. 28 und 29 festzulegen,

2. zur Ausführung von Art. 29 und 30 die Nutzungsbedingungen des Nutzerkontos, die technischen Anforderungen an Nutzerkonto und Postfach, insbesondere die zugelassenen Identifizierungsmittel und Schnittstellen, sowie den Zeitpunkt der Freischaltung des Nutzerkontos und seiner Funktionen festzulegen,

3. im Rahmen von Art. 32 Verfahren zur Änderung personenbezogener Daten und der Rechtsnachfolge festzulegen.

(5) Jedes Staatsministerium wird ermächtigt, in den Angelegenheiten seines Geschäftsbereichs durch Rechtsverordnung im Einvernehmen mit dem Staatsministerium der Finanzen und für Heimat juristischen Personen des öffentlichen Rechts, die der Aufsicht des Freistaates Bayern unterstehen, die Erbringung von IT-Dienstleistungen im Zusammenhang mit der Bereitstellung digitaler öffentlicher Dienste im Sinne von Art. 17, der Errichtung und dem Betrieb des Portalverbundes Bayern im Sinne von Art. 26, des Bayernportals im Sinne von Art. 27, des Organisationsportals Bayern im Sinne von Art. 28 sowie der Bereitstellung von Nutzerkonten im Sinne von Art. 29 zu übertragen.

(6) Das Staatsministerium für Umwelt und Verbraucherschutz wird ermächtigt, beim Betrieb von Flächenmanagement-Datenbanken durch Gemeinden durch Rechtsverordnung Regelungen der hierzu erforderlichen Verarbeitung, Verwendung und Einbeziehung personen- und grundstücksbezogener Daten zu treffen.

Art. 53a
Änderung weiterer Rechtsvorschriften

(1) Das Kostengesetz (KG) vom 20. Februar 1998 (GVBl. S. 43, BayRS 2013-1-1-F), das zuletzt durch § 2 des Gesetzes vom 19. März 2020 (GVBl. S. 153) geändert worden ist, wird wie folgt geändert:

1. Dem Art. 5 Abs. 2 werden die folgenden Sätze 4 und 5 angefügt:

   „[4]Ist für eine Amtshandlung ein digitales Verfahren eröffnet, kann für die Gebühr, die im Kostenverzeichnis festgelegt wird, eine Ermäßigung vorgesehen werden, wenn sich der Verwaltungsaufwand durch das digitale Verfahren verringert. [5]Die Ermäßigung darf 100 € nicht überschreiten.“

2. Art. 21 Abs. 3 Satz 1 Halbsatz 2 wird wie folgt gefasst:

   „Art. 5 Abs. 2 Satz 4 und 5, Abs. 3, 5 und 6 gilt entsprechend.“

(2) Die Gemeindeordnung (GO) in der Fassung der Bekanntmachung vom 22. August 1998 (GVBl. S. 796, BayRS 2020-1-1-I), die zuletzt durch § 1 des Gesetzes vom 9. März 2021 (GVBl. S. 74) geändert worden ist, wird wie folgt geändert:

1. Art. 26 Abs. 2 Satz 2 wird wie folgt geändert:

a) In Halbsatz 1 wird das Wort „anderen“ gestrichen.

b) In Halbsatz 2 werden nach dem Wort „Niederlegung“ die Wörter „digital über das Internet,“ eingefügt.

2. Dem Art. 38 Abs. 2 wird folgender Satz 4 angefügt:

„[4]Bei der Vergabe von öffentlichen Aufträgen und Konzessionen genügt die Textform, soweit eine andere Rechtsvorschrift nichts Abweichendes bestimmt.“

(3) Dem § 35 Abs. 2 der Landkreisordnung (LKrO) in der Fassung der Bekanntmachung vom 22. August 1998 (GVBl. S. 826, BayRS 2020-3-1-I), die zuletzt durch § 2 des Gesetzes vom 9. März 2021 (GVBl. S. 74) geändert worden ist, wird folgender Satz 4 angefügt:

„[4]Bei der Vergabe von öffentlichen Aufträgen und Konzessionen genügt die Textform, soweit eine andere Rechtsvorschrift nichts Abweichendes bestimmt.“

(4) Dem Art. 33a Abs. 2 der Bezirksordnung (BezO) in der Fassung der Bekanntmachung vom 22. August 1998 (GVBl. S. 850, BayRS 2020-4-2-I), die zuletzt durch § 3 des Gesetzes vom 9. März 2021 (GVBl. S. 74) geändert worden ist, wird folgender Satz 4 angefügt:

„[4]Bei der Vergabe von öffentlichen Aufträgen und Konzessionen genügt die Textform, soweit eine andere Rechtsvorschrift nichts Abweichendes bestimmt.“

(5) Art. 37 des Gesetzes über die kommunale Zusammenarbeit (KommZG) in der Fassung der Bekanntmachung vom 20. Juni 1994 (GVBl. S. 555, 1995 S. 98, BayRS 2020-6-1-I), das zuletzt durch § 4 des Gesetzes vom 9. März 2021 (GVBl. S. 74) geändert worden ist, wird wie folgt geändert:

1. Abs. 1 wird wie folgt geändert:

a) Die Absatzbezeichnung „(1)“ wird gestrichen.

b) In Satz 1 werden die Wörter „oder müssen in elektronischer Form mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur versehen sein“ durch die Wörter „ ; das gilt nicht für ständig wiederkehrende Geschäfte des täglichen Lebens, die finanziell von unerheblicher Bedeutung sind“ ersetzt.

c) Folgender Satz 4 wird angefügt:

„[4]Bei der Vergabe von öffentlichen Aufträgen und Konzessionen genügt die Textform, soweit eine andere Rechtsvorschrift nichts Abweichendes bestimmt.“

2. Abs. 2 wird aufgehoben.

(6) In Art. 15 Abs. 2a Satz 1 des Bayerischen Besoldungsgesetzes (BayBesG) vom 5. August 2010 (GVBl. S. 410, 764, BayRS 2032-1-1-F), das zuletzt durch Art. 9

und Art. 10 des Gesetzes vom 9. April 2021 (GVBl. S. 150) geändert worden ist, werden die Wörter „mit Zustimmung des Beamten oder der Beamtin“ gestrichen.

Art. 53b
Änderung des Bayerischen Digitalgesetzes

Art. 19 Abs. 1 und 2 des Bayerischen Digitalgesetzes (BayDiG) vom [DATUM] (GVBl. XXX, BayRS 206-1-D) wird wie folgt gefasst:

„(1) [1]Die Behörden bieten geeignete Verwaltungsverfahren oder geeignete abtrennbare Teile eines Verwaltungsverfahrens auch digital an. [2]Die Gemeindeverbände und die Gemeinden sollen in Angelegenheiten des eigenen Wirkungskreises geeignete Verwaltungsleistungen auch digital anbieten.

(2) [1]Behördliche Formulare, die zur Verwendung durch Beteiligte dienen, sind in digital ausfüllbarer Form zum Abruf und zur sicheren Datenübermittlung an die Behörden bereitzustellen. [2]Dies gilt nicht, soweit Verwaltungsleistungen gemäß Abs. 1 vollständig digital angeboten werden. [3]Ist aufgrund einer Rechtsvorschrift ein bestimmtes Formular zwingend zu verwenden, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform bewirkt.“

Art. 54
Einschränkung von Grundrechten

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

Art. 55
Inkrafttreten, Außerkrafttreten

(1) [1]Dieses Gesetz tritt am ….. in Kraft. [2]Abweichend von Satz 1 tritt Art. 53b am 1. Januar 2023 in Kraft.

(2) Art. 53a tritt am 1. Januar 2023 außer Kraft.

(3) Art. 53b tritt mit Ablauf des 31. Dezember 2023 außer Kraft.

(4) Das Bayerische E-Government-Gesetz (BayEGovG) vom 22. Dezember 2015 (GVBl. S. 458, BayRS 206-1-D), das zuletzt durch § 1 Abs. 138 der Verordnung vom 26. März 2019 (GVBl. S. 98) geändert worden ist, tritt mit Ablauf des … (einsetzen: Tag vor Inkrafttreten nach Abs. 1 Satz 1) … außer Kraft.

Begründung

A. Allgemeines

Die fortschreitende Digitalisierung aller Lebensverhältnisse stellt Staat und Gesellschaft vor grundlegende Herausforderungen. Die Europäische Union, Bund und Länder haben auf die mit der Digitalisierung einhergehenden tiefgreifenden gesellschaftlichen Transformationsprozesse, die Potentiale, aber auch die Risiken des Siegeszugs digitaler Technologien, frühzeitig mit der Entwicklung umfassend angelegter Digitalisierungsstrategien reagiert. Der Freistaat Bayern hat hier mit den Programmen Bayern Digital I und II und jüngst wieder der High-Tech Agenda besondere Akzente gesetzt.

Neben diesen primär auf Förderung ausgelegten Maßnahmen und Initiativen wirft der heutige Stand der Digitalisierung aber auch grundlegende Fragen nach der Neujustierung der allgemeinen politischen und rechtlichen Leitplanken für das digitale Zeitalter auf. So hat die Erkenntnis der Abhängigkeiten von Bürgerinnen und Bürgern und Unternehmen, aber auch von Staat und Verwaltung von global agierenden digitalen Plattformanbietern zu einer Diskussion um die Gewährleistung eigenständiger autonomer Entscheidungs- und Handlungsfähigkeit unter Bedingungen von Digitalisierung („Digitale Souveränität“) geführt.

Die faktische Abhängigkeit der Ausübung nahezu aller grundlegenden Freiheits- und Gleichheitsrechte vom Zugriff auf digitale Technologien, Plattformen und Netze wirft die Frage nach einer entsprechenden Weiterentwicklung der subjektiven Rechte der Bürgerinnen und Bürger und der Unternehmen im digitalen Zeitalter auf. Angesichts der notwendigen „Technik- und Infrastrukturabhängigkeit“ von digitalen subjektiven Rechten trifft den Staat eine besondere Verantwortung zur Gewährleistung der technischen und infrastrukturellen Voraussetzungen sowie ihrer praktischen Wirksamkeit.

Der Freistaat Bayern hat im Bereich der „digitalen Verwaltung“ bereits frühzeitig auch rechtlich auf die Herausforderungen der Digitalisierung reagiert. Mit dem Gesetz über die digitale Verwaltung in Bayern (BayEGovG) vom 22.12.2015 (GVBl. S. 458) lieferte der Freistaat Bayern erstmals einen einheitlichen und zusammenhängenden Rechtsrahmen für die digitale Verwaltungstätigkeit der Behörden des Freistaates Bayern, der Gemeindeverbände und Gemeinden und der sonstigen unter der Aufsicht des Freistaates stehenden juristischen Personen des öffentlichen Rechts. Darüber hinaus hat der Freistaat auch in einer Vielzahl von Fachgesetzen die Digitalisierung der Verwaltung konsequent vorangetrieben – sei es durch die Anpassung bestehender oder die Schaffung neuer gesetzlicher Regelungen.

Was bisher allerdings fehlt, ist ein übergreifender rechtlicher Ordnungsrahmen, der allgemeine, entwicklungsoffene rechtliche Leitplanken für die Digitalisierung von Gesellschaft und Wirtschaft, Staat und Verwaltung definiert, insbesondere

- die Ziele des Freistaates Bayern unter Bedingungen der Digitalisierung weiterentwickelt,

- die digitalen Freiheits- und Teilhaberechte der Bürgerinnen und Bürger und der Unternehmen in Bayern konsequent weiterentwickelt,
- die damit verbundenen Gewährleistungsverantwortungen des Freistaates definiert und
- die Grundlagen der Zusammenarbeit der öffentlichen Einrichtungen im Freistaat, insbesondere die enge Zusammenarbeit von Freistaat und Kommunen festschreibt.

Bei der Schaffung eines allgemeinen gesetzlichen Regelungsrahmens für die Digitalisierung in Bayern kann an bereits bestehende Regelungen des BayEGovG im Bereich der Digitalisierung der Verwaltung angeknüpft werden, die in den neuen, deutlich weiter gefassten gesetzlichen Rahmen integriert werden können.

Darüber hinaus sollten auch die erforderlichen gesetzlichen Regelungen geschaffen werden, um auf die grundlegenden Veränderungen im Bundesrecht in diesem Bereich zu reagieren. Mit dem Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz, OZG) v. 14. 8. 2017 (BGBl. I S. 3122, 3138) hat der Bundesgesetzgeber den zeitgleich neu geschaffenen Regelungsauftrag des Art. 91 c Abs. 5 GG aufgegriffen. Hauptziel des Gesetzes ist es, den digitalen Gang zur Behörde unkompliziert und sicher zu gestalten. Im Kern verpflichtet das OZG Bund und Länder

- jeweils eigene Verwaltungsportale auf Bundes- und Landesebene auf- und auszubauen und
- zu einem Portalverbund zusammenzuschließen sowie
- im Portalverbund Nutzerkonten einzurichten.

Bürgerinnen, Bürger und Unternehmen sollen von einem beliebigen Verwaltungsportal aus auf alle onlinefähigen Verwaltungsleistungen zugreifen können. Zu diesem Zweck regelt das Gesetz, dass die bislang heterogenen IT-Strukturen bei Verwaltungsleistungen von Bund und Ländern sukzessive interoperabel gestaltet werden (vgl. BT-Drs. 18/11135 v. 10. 2. 2017, S. 5, 91 ff.).

Im Landesrecht sind nunmehr korrespondierende Regelungen zu einem Bayerischen Portalverbund zu schaffen, der zu den geänderten bundesrechtlichen Rahmenbedingungen kompatibel ist, zugleich aber auch im Bund-Länder Kontext neue, weitergehende Impulse setzt.

Mit dem vorliegenden Gesetz legt der Freistaat bundesweit erstmalig ein eigenes Digitalgesetz vor, welches den Anspruch erhebt, die Rahmenbedingungen für die Digitalisierung von Staat und Verwaltung, Wirtschaft und Gesellschaft in Bayern nicht nur wie bisher in den „E-Government-Gesetzen“ punktuell, sondern von den Zielsetzungen her deutlich umfassender zu regeln, da Digitalisierung eine umfassende, alle Lebensbereiche, Staat, Verwaltung, Wirtschaft und Gesellschaft umfassende Herausforderung und Chance darstellt.

Der umfassenden Herausforderung der Digitalisierung für Staat, Wirtschaft und Gesellschaft trägt das neue Bayerische Digitalgesetz mit seinem „Allgemeinen Teil“ Rechnung. In diesem Teil werden die Gewährleistung digitaler Souveränität des Freistaates, die Entwicklung einer staatlichen Cloud Strategie sowie die Förderung des Digitalstandorts Bayern als staatliche Zielsetzungen festgeschrieben. Diese staatlichen Zielbestimmungen werden flankiert durch die deutschlandweit erstmalige gesetzliche Verankerung einer „Charta Digitaler Rechte und Gewährleistungen“ (u. a. Recht auf Zugang zu schnellem Internet, Recht auf digitale Identität, Recht auf digitale Teilhabe, Gewährleistung der digitalen Daseinsvorsorge).

Die Verankerung von Zielbestimmungen und subjektiv öffentlichen Rechten auf einfachgesetzlicher Ebene ist dem öffentlichen Recht generell nicht fremd (Recht auf Akteneinsicht in Verwaltungsverfahren, vgl. auch Bayerisches Naturschutzgesetz, Bayerisches Klimaschutzgesetz). Eine zunächst einfachgesetzliche Normierung digitaler Ziele, Rechte und Gewährleistungen wird auch der besonderen Dynamik des Sachbereichs „Digitalisierung“ gerecht, dessen weitere faktische Entwicklung und der daraus resultierende Normierungsbedarf sich derzeit nur eingeschränkt abschätzen lässt.

Mit der Entscheidung für eine zunächst einfachgesetzliche Normierung wird eine spätere verfassungsrechtliche Verankerung „digitaler Staatsziele“ oder „digitaler Grundrechte“ keineswegs ausgeschlossen. Ziel der Staatsregierung ist es aber, in einem ersten Schritt einen ergebnisoffenen Prozess der Verrechtlichung der digitalen Gesellschaft in Bayern einzuleiten, der perspektivisch auch in verfassungsrechtliche Regelungen in Bayern münden kann. Damit stößt der Gesetzentwurf zielgerichtet einen Entwicklungsprozess an, wie er sich z. B. auch im Datenschutz- und Naturschutzrecht bewährt hat, in denen jeweils die einfachgesetzliche Normierung einer späteren „Konstitutionalisierung“ zeitlich zum Teil deutlich vorangegangen ist.

Mit dem allgemeinen Teil zieht das Bayerische Digitalgesetz allgemeine Zielbestimmungen und rechtliche Gewährleistungen „vor die Klammer“, die der weiteren einfachgesetzlichen Konkretisierung bedürfen. Hierzu dienen die besonderen Teile des Gesetzes, die eine Reihe von Schlüsselthemen der Digitalisierung von Staat und Verwaltung im Einzelnen regeln. Hierzu zählen die Regelungen

- zur „Digitalen Verwaltung“, einschließlich Aufbau eines Bayerischen Portalverbunds,
- zur IT-Sicherheit, einschließlich der Aufgaben und Befugnisse des Landesamts für Sicherheit in der Informationstechnik sowie
- zu den Organisations- und Kooperationsstrukturen im Freistaat Bayern im Bereich der Digitalisierung.

Das Regelungskonzept des Bayerischen Digitalgesetzes muss der Dynamik des Sachbereichs Rechnung tragen. In einigen Bereichen wurde daher zum jetzigen Zeitpunkt bewusst auf Detailregelungen verzichtet, um Raum für noch laufende erforderliche Diskussionsprozesse zu belassen. So bedarf etwa die allgemeine Gewährleistung des

„Zugangs zu den Datenbeständen der Behörden“ (vgl. Art 14) der weiteren gesetzlichen Konkretisierung, bei der auch neue EU-rechtliche Vorgaben zu berücksichtigen sind (z. B. Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors und die Richtlinie 2013/37/EU zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors). Da die erforderlichen Vorarbeiten hierzu noch nicht abgeschlossen sind, wurde auch eine nähere Regelung des Themas „Open Data“ zum jetzigen Zeitpunkt verzichtet.

Besondere Herausforderungen für den Gesetzgeber sind zudem mit dem Aufbau und Betrieb eines Portalverbunds von Bund und Ländern nach Maßgabe des Onlinezugangsgesetzes (Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen - OZG) verbunden, der Anfang 2023 in seiner ersten Ausbauphase umgesetzt sein soll. Hinzu treten unionsrechtliche Anforderungen, insbesondere aus der Single-Digital-Gateway-Verordnung (SDG-VO). Die Regelungen des OZG und ergänzend der SDG-VO haben gemeinsam, dass sie nicht nur auf ebenenübergreifende Wirkungen für alle Verwaltungsebenen, sondern auch auf die übergreifende Verknüpfung der digitalen Verwaltungsangebote von Bund, Ländern, Kommunen und sonstigen öffentlich-rechtlichen Körperschaften gerichtet sind.

Aufgrund dieser weitergehenden, über die engere Zielsetzung der E-Government-Gesetze hinausgehenden Regelungswirkung sowie der eigenständigen grundgesetzlichen Kompetenzgrundlage hat sich der Bundesgesetzgeber entschlossen, die verfassungspolitische Zielsetzung des Art. 91c Abs. 5 GG nicht im E-Government-Gesetz des Bundes, sondern vielmehr gesondert im Onlinezugangsgesetz einfachgesetzlich auszugestalten. Der Freistaat berücksichtigt die weitergehende Zielsetzung des Portalverbunds dagegen im Rahmen eines neuen, weitergefassten Regelungsansatzes des Bayerischen Digitalgesetzes.

Der umfassende Regelungsanspruch des Gesetzes kommt schließlich auch in besonderen Bestimmungen zu Nachhaltigkeit, Clean IT, Open Source, neuen Kooperationsgremien wie dem Kommunalen Digitalpakt, digitalen Qualifizierungsprogrammen oder der bayerischen Cloud Strategie zum Ausdruck.

Neben neuen Herausforderungen im Freistaat adressiert der Gesetzentwurf schließlich auch das gewandelte verfassungsrechtliche und einfachgesetzliche Umfeld, in das die Digitalisierung des Freistaates eingebettet ist. Mit der Einführung des Art 91 c GG und der zeitlichen einfachgesetzlichen Normierung des Onlinezugangsgesetzes haben sich die Rahmenbedingungen für Ausbau und Weiterentwicklung der digitalen Verwaltung in Deutschland und damit auch in Bayern deutlich verändert. Der Bund verfügt über deutlich weiterreichende Rechtssetzungskompetenzen, zugleich hat der wechselseitige Kooperationsbedarf zwischen Bund und Ländern drastisch zugenommen. Gleiches gilt entsprechend, wenn auch mit etwas weniger weitreichenden Folgen, für die Ebene der Europäischen Union.

Angesichts dieser Ausgangslage war es erforderlich, nicht nur die Kooperationsstrukturen innerhalb des Freistaates weiterzuentwickeln, sondern die Handlungsfähigkeit

des Freistaates insbesondere auf Bund-Länder Ebene deutlich zu erhöhen und die hierfür erforderlichen Organisationsstrukturen auch gesetzlich besonders zu regeln.

Der vorliegende Gesetzesentwurf geht mithin deutlich über eine einfache Anpassung des Bayerischen E-Government-Gesetzes oder die bloße landesrechtliche „Umsetzung“ neuer unions- oder bundesrechtlicher Vorgaben hinaus. Aus diesem Grund war eine bloße Überarbeitung des BayEGovG nicht sinnvoll. Es musste vielmehr ein inhaltlich und systematisch neues, sachlich deutlich weiter angelegtes Gesetz erarbeitet werden. Bewährte Regelungen des BayEGovG, etwa zu digitalen Zugangs- und Verfahrensrechten, zu digitalen Verwaltungsverfahren oder zur IT-Sicherheit wurden jedoch übernommen und inhaltlich weiterentwickelt. Die neuen Aufgaben des Aufbaus eines bayerischen Portalverbunds, der Volldigitalisierung der bayerischen Staatsverwaltung, die Umsetzung des 12-Punkte Plans der Staatsregierung zur Digitalisierung der Verwaltung vom Februar 2020, aber auch Themen wie Nachhaltigkeit und Umweltfreundlichkeit erforderten aber eine inhaltliche und systematische Neukonzeption.

Das vorliegende Gesetz ist im Prinzip ein in Gesetzesform gegossenes, umfassendes Verwaltungsmodernisierungsprogramm, weshalb auch konsequenter Weise ein laufendes Monitoring unter Mitwirkung aller Ressorts, eine wissenschaftliche Begleitung der Umsetzung ab Inkrafttreten sowie eine zeitnahe Evaluierung erforderlich sind.

Folgende Hauptziele werden mit der Gesetzesnovelle verfolgt:

- Förderung der Digitalisierung im Freistaat Bayern in den Schlüsselbereichen, Technologie, Wirtschaft, Wissenschaft, Bildung, Gesundheit und Verwaltung
- Implementierung einer Charta digitaler Rechte und Gewährleistungen
- Bereitstellung einer sicheren und datenschutzkonformen digitalen Identität für alle Bürger und Unternehmen in Bayern
- Gewährleistung der digitalen Handlungs- und Entscheidungsfähigkeit des Freistaates Bayerns (Digitale Autonomie) einschließlich der Bereitstellung und Sicherung digitale Netze und Infrastrukturen
- Ausbau der digitalen Daseinsvorsorge im Freistaat und den bayerischen Kommunen
- Unterstützung der Gemeindeverbände und Gemeinden bei der Digitalisierung
- die Digitalisierung der Verwaltung und den Ausbau digitaler Verwaltungsangebote
- Ausbau der digitalen Verwaltung für die Wirtschaft und Schaffung eines einheitlichen Online-Zugangs für Unternehmen (Single Point of Contact)
- Übernahme und Weiterentwicklung der bisherigen Rechtsvorschriften des BayEGovG zur digitalen Verwaltung und IT-Sicherheit
- Schaffung eines nutzerfreundlichen Portalverbunds Bayern
- Zulassung von ELSTER als Authentifizierungslösung und Schriftformersatz
- Bereitstellung rechtlich verbindlicher „Bayernstandards“
- Möglichkeit zum Direktabruf von Belegen
- Errichtung eines „Digital Wallets“

- Förderung und weiterer Ausbau nachhaltiger und umweltfreundlicher digitaler Verwaltungsprozesse
- Stärkung der digitalen Aus- und Weiterbildung der Beschäftigten der öffentlichen Verwaltung
- Schaffung von Experimentierräumen

Die Regelungen des BayEGovG werden grundsätzlich unverändert übernommen, allerdings in die neue Systematik des Digitalgesetzes integriert, zum Teil in dessen „Allgemeinen Teil“, überwiegend in die neuen „Besonderen Teile“ (vgl. Teil 2 „Digitale Verwaltung“, Kapitel 1 und 2 bzw. Teil 3 „IT-Sicherheit“).

Wesentliche Regelungsschwerpunkte im Einzelnen:

Gewährleistung der digitalen Souveränität Bayerns:

Grundlage und Voraussetzung für die aktive Gestaltung der Digitalisierung durch den Freistaat ist die Gewährleistung einer möglichst umfassenden autonomen digitalen Handlungsfähigkeit (Digitale Souveränität). Das Gesetz schreibt die Digitale Souveränität als Zielbestimmung des Freistaates fest und regelt die Entwicklung von Strategien und Umsetzungsmaßnahmen in wichtigen Teilbereichen, wie insbesondere im Bereich von Cloud-Lösungen für die digitale Verwaltung (vgl. Art. 3).

Charta digitaler Rechte:

Das Gesetz sieht erstmal eine Charta Digitaler Rechte vor. Als Basisrecht einer digitalen Gesellschaft wird zunächst das Recht auf freien Zugang zum Internet verankert (Art. 8), das allgemeine staatliche Internetzugangsblockaden ausschließt. Weiter werden Rechte auf Bereitstellung digitaler Identitätsdienste und auf Bereitstellung digitaler Verwaltungsleistungen, auch in mobiler Form, verankert (Art. 11 bis 13).

Fördermaßnahmen der Digitalpolitik:

Das Gesetz verankert anknüpfend an die Programme Bayern Digital I und II und die High Tech Agenda thematische Schwerpunkte für Fördermaßnahmen der bayerischen Digitalpolitik. Hierzu zählen unter anderem der Ausbau digitaler Bildungsangebote, die Stärkung digitaler Grundkompetenzen in Gesellschaft, Wirtschaft und Verwaltung, die Förderung des Digitalstandorts Bayern, die Stärkung digitaler Disziplinen in der Wissenschaft, die Implementierung intelligenter digitaler Mobilitätskonzepte und die Digitalisierung von Medizin und Pflege (siehe Art. 2).

Digitale Daseinsvorsorge:

Digitalisierung ist kein Prozess, der sich allein auf die private Kommunikation, die Wirtschaft und die digitale Durchführung von Verwaltungsverfahren beschränkt. Vielmehr erwächst dem Staat und den Kommunen eine neue Form der öffentlichen Daseinsvor-

sorgeverantwortung. Diese beschränkt sich nicht allein darauf, bisher „analog“ angebotene staatliche Leistungen (von der Kita-Anmeldung bis zum Baubescheid) auch oder vorrangig digital anzubieten. Vielmehr gilt es auch, die Potentiale digitaler Technologien zu nutzen, um öffentliche Versorgungs- und Netzdienstleistungen zu modernisieren und effizienter auszugestalten.

Digitalisierung aller geeigneten Prozesse in Staat und Verwaltung:

Bisher beschränkt sich das Recht der digitalen Verwaltung (OZG, BayEGovG) bundesweit darauf, dass Verwaltungsleistungen „auch“ digital angeboten werden („Digitale Option“). Was bisher fehlt, sind rechtliche Regelungen zum digitalen Verfahren als „Regelfall“ (Digital First). Diese Lücke soll mit dem vorliegenden Gesetz geschlossen werden, wobei natürlich die Anforderungen des Datenschutzes und der IT-Sicherheit gewahrt werden müssen (siehe Art. 5). Schon aus Gründen der Rechtsstaatlichkeit ist sicherzustellen, dass auch Bürger, die nicht über die notwendigen Voraussetzungen verfügen, weiterhin einen effektiven Verwaltungszugang erhalten. Daher wird die Verpflichtung der Behörden zum „digitalen Regelfall“ durch ein Recht des Bürgers auf nichtdigitale Antragstellung (als Ausnahmefall) flankiert, vgl. Art. 20 Abs. 1.

Vollständig automatisierte Verfahrensabwicklung:

Ein wichtiges Zukunftsthema der digitalen Verwaltung ist das vollständig automatisierte Verfahren. Verfassungsrechtliche Grenzen ergeben sich allerdings aus dem Rechtsstaatsprinzip. Ausgehend von diesen Prämissen normiert das BayDiG eine Reihe von besonderen einfachgesetzlichen Anforderungen an die vollständig automatisierte Verfahrensabwicklung. Automatisierte Verfahren müssen regelmäßig auf ihre Zweckmäßigkeit, Objektivität und Wirtschaftlichkeit hin überprüft werden (Art. 5 Abs. 4). Weiter ist der sofortige Vollzug von vollständig automatisiert erlassenen Entscheidungen nur zulässig, wenn dies spezialgesetzlich besonders zugelassen wird (Art. 12 Abs. 2 Satz 4).

Schaffung eines nutzerfreundlichen Portalverbunds Bayern:

Das Gesetz zielt auf die Schaffung eines Bayerischen Portalverbunds. Ziel ist es alle Behörden und deren Leistungen in den Portalverbund Bayern einzubinden und es allen Bürgern und Unternehmen zu ermöglichen, diese Verwaltungsleistungen nutzerfreundlich in Anspruch zu nehmen. Um alle Prozesse möglichst nutzerfreundlich zu gestalten, sollen rechtlich verbindliche „Bayernstandards“ für alle Behörden definiert werden können, vgl. Art. 26. Umgekehrt wird die digitale Selbstbestimmung gefördert durch hohen Datenschutz in staatlichen Angeboten („Privacy by Design“), digitale Kompetenzvermittlung in Schulen und für besondere Gruppen, wie z. B. Senioren.

Zulassung digitaler Assistenzdienste für mehr Nutzerfreundlichkeit:

Zudem sieht das Gesetz bundesweit erstmals außerhalb der Steuerverwaltung die Möglichkeit vor, digitale Assistenzdienste von privaten Drittanbietern zur nutzerfreundlichen Verfahrensabwicklung zuzulassen (Art. 21). Dieses Verfahren hat sich in der

Steuer bewährt. Hier legt die Verwaltung Schnittstellen offen, über die private Steuersoftwareanbieter ihre Dienste zur Erleichterung der elektronischen Steuererklärung anbieten.

Möglichkeit zum Direktabruf von Belegen:

Zur Nutzerfreundlichkeit zählt auch die Möglichkeit, Belege direkt abzurufen. Bisher müssen die Bürger erforderliche Belege (z. B. Geburtsurkunden) selbst bei der ausstellenden Behörde (z. B. am Geburtsort) einholen und dann bei der einfordernden Behörde vorlegen. In digitalen Verfahren sollen künftig die Behörden, die Belege fordern, diese (auf Antrag des Bürgers) direkt einholen, wenn die Informationen von der Behörde in digitaler Form aus Registern abgerufen werden können, vgl. Art. 23 Abs. 2.

Mobile Government und Digital Wallet:

Mittelfristig sollen alle Online-Dienste für Bürger (nach dem Grundsatz “Mobile-First”) und alle geeigneten Online-Dienste für Unternehmen auch an Mobilgeräten durchgeführt werden können. Um eine ausreichende Übergangszeit und eine Anpassung an technologische Entwicklungen zu gewährleisten, wird hinsichtlich der Voraussetzungen des Anspruchs auf eine Verordnungsermächtigung verwiesen.

Um den Mehrwert der digitalen Verwaltung weiter hervorzuheben, soll das Unternehmenskonto auch über ein Digital Wallet (Datensafe) verfügen.

„Once Only“:

Weiter soll es möglich sein, in Formularen Datensätze automatisch zu übernehmen und so zur Verwirklichung des „Once Only“ Prinzips beizutragen (vgl. Art. 30 Abs. 2 S. 2). Hierdurch müssen beispielsweise die im Melderegister enthaltenden Standardinformationen nur noch einmal eingegeben werden, für alle weiteren Formulare werden die Datensätze dann automatisch übernommen.

Zulassung von ELSTER-Zertifikaten auch außerhalb der Steuer:

Ein Schlüsselfaktor erfolgreichen E-Governments sind einfache, in der Fläche verfügbare Identifizierungs- und Authentifizierungsmittel. Die größte Verbreitung in Deutschland hat aktuell das ELSTER-Zertifikat (rd. 8 Millionen Zertifikate). Parallel zu den aktuell auf Bundesebene anstehenden Rechtsänderungen in der Abgabenordnung soll in Bayern auf landesrechtlicher Ebene das ELSTER-Verfahren auch außerhalb der Steuer als Authentifizierungsmittel und zusätzlich auch als Schriftformersatz zugelassen werden.

Digitale Verwaltung für die Wirtschaft: Organisationskonto auf ELSTER-Basis:

Die Digitalisierung der Verwaltung ist für Unternehmen schon aufgrund der hohen Zahl von Verwaltungskontakten von Bedeutung. Unternehmen stellen aber auch besondere

Anforderungen an die digitale Kommunikation mit Behörden, etwa in Form der Maschine-zu-Maschine-Kommunikation. Diesen Besonderheiten trägt das Gesetz mit Regelungen an ein Organisationskonto bundesweit erstmals Rechnung. Die rechtlichen Rahmenregelungen erlauben den Rückgriff von Unternehmen auf die in der Steuer bewährten digitalen Dienste der ELSTER-Technologie. Unter anderem sollen ELSTER-Zertifikate erstmals außerhalb der Steuer genutzt werden können, darüber hinaus aber auch die sicheren und hochverfügbaren technischen Infrastrukturen der Steuerverwaltung auch für nichtsteuerliche Verwaltungsleistungen zur Verfügung gestellt werden. Mit den rechtlichen Regelungen zum Organisationskonto rückt der „Single Point of Contact“ für Unternehmen auch faktisch näher. Die gesetzlichen Rahmenbedingungen für das Organisationsportal und das Organisationskonto werden in den Art. 27 und 28 verankert.

Förderung und weiterer Ausbau nachhaltiger und umweltfreundlicher digitaler Verwaltungsprozesse:

Das Gesetz adressiert in Art. 6 das Thema „Nachhaltiges E-Government“. Die Beschaffung, der Betrieb, der Ersatz und die Entsorgung der staatlichen IT-Infrastruktur soll möglichst umwelt- und klimaschonend erfolgen. Digitale Technologien sollen aber auch für die Umsetzung von flexiblen und zugleich klimafreundlichen Beschäftigungsmodellen genutzt werden, z. B. im Rahmen von Telearbeit und Homeoffice. Staatliche Behörden sollen auch angehalten werden, verstärkt freie Software (open source) oder eigenentwickelte Software zu nutzen.

Datenschutz und Auftragsverarbeitung:

Auch ist es ein Anliegen des vorliegenden Gesetzesentwurfs mit Art. 38 Auftragsverarbeitungen in der öffentlichen Verwaltung einer Neukonzeption zuzuführen. Am 27. April 2016 hat das Europäische Parlament und der Rat mit der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 – DSGVO) einen zentralen Rechtsakt zur Reform des europäischen Datenschutzrechts verabschiedet. Die Regelungen der DSGVO gelten seit dem 25. Mai 2018 in allen Mitgliedstaaten der EU mit unmittelbarer Wirkung. Bereits seit dem 5. Mai 2016 ist die Datenschutz-Richtlinie für den Bereich Polizei und Justiz (Richtlinie (EU) 2016/680 – JI-RL) in Kraft getreten, welche in Bayern durch die Art. 28 ff. des Bayerischen Datenschutzgesetzes sowie auf Bundesebene durch die diesen in weiten Bereichen vorrangigen bundesrechtlichen Regelungen des BDSG, der StPO und des OWiG umgesetzt worden ist.

Nach Art. 28 Abs. 3 DSGVO (i.V.m. Art. 28 BayDSG bzw. gemäß § 500 StPO, § 62 Abs. 5 BDSG ggfs. i.V.m. § 46 OwiG für den Bereich der JI-RL) hat die Verarbeitung von personenbezogenen Daten durch einen Auftragsverarbeiter entweder auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet, zu erfolgen.

Zu beachten ist hierbei, dass aus datenschutzrechtlicher Sicht jede einzelne öffentliche Stelle – und nicht der Freistaat Bayern als Gebietskörperschaft – verantwortlich im Sinne des Art. 4 Nr. 7 DSGVO ist, respektive gemäß Art. 4 Nr. 8 DSGVO (jeweils i.V.m. Art. 28 BayDSG bzw. gemäß § 500 StPO, § 62 Abs.5 BDSG ggfs. i.V.m. § 46 OwiG für den Bereich der JI-RL) Auftragsverarbeiter sein kann.

Konkret führt dies dazu, dass staatliche Stellen, die personenbezogene Daten im Auftrag für andere öffentliche Stellen verarbeiten, ein Auftragsverarbeitungsverhältnis eingehen und hierzu einen Vertrag schließen müssen sofern nicht ein anderes Regelungsinstrument greift.

IT-Verfahren und sonstige informationstechnische Dienstleistungen werden heutzutage durch die bayerischen Rechenzentren, die Mittelbehörden oder die obersten Dienstbehörden zentral für den nachgeordneten Bereich zur Verfügung gestellt. Der Abschluss von Einzelverträgen im Rahmen von Auftragsverarbeitungsverhältnissen ist in diesem Zusammenhang mit hohem bürokratischem Aufwand verbunden, da die Anzahl der zu schließenden Auftragsverarbeitungsvereinbarungen auf weit über 3.000 geschätzt wird. Dies soll mit der Regelung des Art. 38 erleichtert werden.

Schaffung von Experimentierräumen:

Das Gesetz sieht erweitere Experimentierräume für neue und innovative E-Government-Lösungen vor. Durch VO kann von bestimmten Zuständigkeits- und Formvorschriften abgesehen werden, um die nötige Flexibilität zu schaffen, um so neue technische Entwicklungen zu testen, vgl. Art. 52.

Unterstützung der kommunalen Gebietskörperschaften, Verwaltungsgemeinschaften und Zweckverbände bei der Digitalisierung:

Das Gesetz sieht Maßnahmen zur Förderung der Digitalisierung (auch) auf kommunaler Ebene vor (vgl. Art. 4 Abs. 3). Die Rahmenregelungen des Digitalgesetzes wahren die Befugnisse des Haushaltsgesetzgebers, ermöglichen aber zugleich eine flexible Anpassung von Fördermaßnahmen an die Bedarfe der Kommunen.

Änderungen der Gemeindeordnung:

Darüber hinaus soll im Zuge des Gesetzgebungsverfahren auch die Gemeindeordnung geändert werden.

Insbesondere soll Art. 26 Abs. 2 GO geändert werden, um eine ausschließliche elektronische Bekanntmachung von Verkündungen der Gemeinden und Verwaltungsgemeinschaften zu ermöglichen, auch wenn sie Satzungen beinhalten. In Folge ist die Verordnung über die amtliche Bekanntmachung gemeindlicher Satzungen und von Rechtsvorschriften der Verwaltungsgemeinschaften (BekV) des Staatsministeriums des Innern vom 19. Januar 1983 um Regelungen zu ergänzen, die eine ausschließli-

che elektronische Bekanntmachung gemeindlicher Satzungen und von Rechtsvorschriften der Verwaltungsgemeinschaften zulassen, um die Vorteile der Digitalisierung auch in diesem Zusammenhang zu nutzen. Weiterhin soll klargestellt werden, dass Gemeindetafeln auch in Form digitaler Bildschirme unterhalten werden können. Eine dementsprechende Änderung der BekV wird vom Staatsministerium des Innern, für Sport und Integration gesondert vorgenommen werden.

Um eine elektronische Kommunikation einfacher zu ermöglichen, soll bei der Vergabe von öffentlichen Aufträgen und Konzessionen in Zukunft die Textform (§ 126b BGB) genügen. Die Verpflichtung zur Schriftform dient zwar dem Schutz der Kommunen vor unbedachten und übereilten Verpflichtungserklärungen. Für den Zuschlag als Abschluss eines Vergabeverfahrens wird die Textform nach § 126b BGB dieser Funktion aber ausreichend gerecht. Dem Zuschlag geht ein zu dokumentierendes, oberhalb der Schwellenwerte stark formalisiertes Verfahren zur Wertung der Angebote voraus, das eine unbedachte Zuschlagserteilung in der Regel ausschließt. Bei Direktvergaben ist eine Warnfunktion aufgrund der geringen Auftragshöhe entbehrlich.

Darüber hinaus besteht folgendes Problem im bayerischen Kommunalrecht: Zwar können amtliche Verkündungen bereits nach Art. 4 BayEGovG elektronisch bekannt gemacht werden, jedoch trifft Art. 26 Abs. 2 Satz 2 Halbsatz 2 Gemeindeordnung (GO) bisher eine entgegenstehende Regelung. Verpflichtungserklärungen der Kommunen und kommunalen Zweckverbände bedürfen derzeit der Schriftform. Nach geltendem Recht sind Kommunen allerdings verpflichtet, in einem Verfahren zur Vergabe von Aufträgen oder Konzessionen vollständig elektronisch zu kommunizieren, wenn der Auftragswert die EU-Schwellenwerte erreicht oder überschreitet. Damit muss auch der Zuschlag auf das wirtschaftlichste Angebot als Verpflichtungserklärung der Kommune elektronisch erteilt werden. Nach § 126 Abs. 3 i. V. m. § 126a BGB ist für solche Fälle wegen der in den Kommunalgesetzen festgelegten Schriftform eine qualifizierte elektronische Signatur erforderlich. In der Praxis hat sich gezeigt, dass viele Kommunen die qualifizierte elektronische Signatur als unpraktikabel empfinden und daher nicht vorhalten. Die alternativen Lösungen in Art. 3a BayVwVfG sind auf zivilrechtliche Verpflichtungserklärungen der Gemeinden nicht anwendbar.

B. Gesetzgebungskompetenzen

Die Gesetzgebungskompetenzen des Freistaates Bayern für die im Rahmen des Bayerischen Digitalgesetzes vorgesehenen Maßnahmen ergeben sich aus den Art. 30 Abs. 1, 70 Abs. 1 und 83 bis 85 GG. Soweit Maßnahmen zum Recht der Wirtschaft vorgesehen sind, hat der Bund seine diesbezüglichen Kompetenzen nicht voll ausgeschöpft. Die vorgesehenen Regelungen zum Aufbau eines Portalverbunds Bayern steht Art. 91 c GG nicht entgegen, da sie sich auf erforderliche Umsetzungsmaßnahmen im Freistaat Bayern beschränken. Regelungen zum Telekommunikationsrecht werden im Gesetz nicht getroffen.

C. Zu den einzelnen Vorschriften

Teil 1. Allgemeiner Teil

Kapitel 1. Allgemeines

Zu Art. 1 Anwendungsbereich:

In Art. 1 wurden die Vorschriften aus Art. 1 BayEGovG modifiziert übernommen.

Zu Abs. 1

Zu Satz 1

Nach Art. 1 Abs. 1 Satz 1 ist das Gesetz auf den Freistaat Bayern, die Gemeinden und Gemeindeverbände und sonstige unter Aufsicht des Freistaates Bayern stehende juristische Personen des öffentlichen Rechts anwendbar. Im Gegensatz z. B. zum BayVwVfG und zum bisherigen Anwendungsbereich des BayEGovG setzt das BayDiG damit nicht bei den Behörden, sondern bei den Gebietskörperschaften und sonstigen juristischen Personen des öffentlichen Rechts als Behördenträgern an. Mit der Verlagerung des Anwendungsbereichs trägt Art. 1 dem vom Verwaltungsverfahrensrecht abweichenden gesetzlichen Regelungsgehalt der Teile 1 und 4 des Gesetzes Rechnung, die gerade nicht konkrete Aufgaben, Befugnisse oder Rechtspflichten einzelner Behörden, sondern vielmehr Aufgaben und Befugnisse der Gebietskörperschaften regeln, wie z. B. Förderpflichten, Schutzpflichten oder Gewährleistungen. In den Teilen 1 und 4 werden damit einzelne behördenbezogene Pflichten nur begründet, wenn dies in einer Einzelvorschrift explizit vorgesehen ist.

Zu Satz 2

Satz 2 stellt klar, dass für die staatlichen Landratsämter und die Verwaltungsgemeinschaften und Zweckverbände die Vorschriften des Gesetzes über Gemeindeverbände und Gemeinden anwendbar sind. Damit wird u.a. der Doppelnatur der Landratsämter Rechnung getragen. Die Vorschriften für die Landratsämter gelten auch für die Schulämter, da diese regelmäßig an die Infrastruktur der Landratsämter und kreisfreien Städte gebunden sind (vgl. Art. 48 BaySchFG).

Zu Abs. 2

Abweichend von Abs. 1 Satz 1 definiert Abs. 2 Satz 1 den Anwendungsbereich der Teile 2 und 3 behördenbezogen. Die Vorschrift trägt damit insbesondere dem verwaltungsverfahrensrechtlichen Regelungsgehalt des Teils 2 und – mit Abstrichen des – Teil 3 Rechnung. Absatz 2 S. 1 knüpft dabei an die Regelung des Art. 1 Abs. 1 BayVwVfG zum Anwendungsbereich des Bayerischen Verwaltungsverfahrensgesetzes an. Hierdurch wird für den verfahrensrechtlichen Teil des BayDiG die prinzipielle Übereinstimmung des Anwendungsbereichs des BayDiG mit dem BayVwVfG gewährleistet. Durch Absatz 2 S. 1 wird sichergestellt, dass das Gesetz grundsätzlich auf die

gesamte öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Freistaates Bayern, der Gemeindeverbände und Gemeinden und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts Anwendung findet.
Für das Landesrecht stellt Art. 1 Abs. 2 S. 1 zudem das Verhältnis der Teile 2 und 3 des BayDiG zum sonstigen Verwaltungsrecht klar. Das BayDiG ist gegenüber dem BayVwVfG als allgemeinem Verwaltungsverfahrensgesetz spezieller, gegenüber inhaltsgleichen oder entgegenstehenden Regelungen des besonderen Verwaltungsrechts dagegen nachrangig. So gehen z. B. auch das Verwaltungszustellungs- und Vollstreckungsgesetz (VwZVG) oder das Kommunalabgabengesetz (KAG) dem BayDiG vor.
Das BayVwVfG bleibt anwendbar, wenn und soweit das BayDiG keine inhaltsgleichen oder entgegenstehenden Regelungen enthält (z. B. bei Art. 3a Abs. 2 und 3 BayVwVfG). Uneingeschränkt anwendbar ist das BayVwVfG zudem auf jene Behörden, die gemäß Art. 1 Abs. 2 S. 2 vom Anwendungsbereich des BayDiG ausgenommen sind.
Ebenso wie das BayVwVfG ist das BayDiG damit in seinen verfahrensrechtlichen Teilen grundsätzlich auf die gesamte Verwaltungstätigkeit im Freistaat und damit umfassend auf den Vollzug von Bundes-, Landes- und Kommunalrecht anwendbar. Dieses Gesetz gilt auch für Verfassungsorgane, wenn und soweit diese als Behörden Verwaltungstätigkeiten ausüben. Die Vorschriften dieses Gesetzes gelten daher für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird. Ebenso gilt das Gesetz für den Bayerischen Landesbeauftragten für den Datenschutz sowie den Obersten Rechnungshof und seine nachgeordneten Prüfungsämter, soweit diese als Verwaltungsbehörde tätig werden. Werden der Landtag als Legislativorgan, der Oberste Rechnungshof und seine Prüfungsämter als Organ der externen Finanzkontrolle und der Bayerische Landesbaufragte für den Datenschutz als unabhängige Aufsichts- und Kontrollinstanz tätig, üben sie dagegen keine Verwaltungstätigkeit aus.

Absatz 2 S. 1 normiert keinen generellen Nachrang des BayDiG zum besonderen Verfahrens- und Fachrecht des Freistaates, sondern begrenzt diesen auf inhaltsgleiche oder entgegenstehende (hierzu zählen auch weitergehende) Regelungen zum digitalen Verwaltungsrecht. Das Gesetz tritt daher nur zurück, soweit Vorschriften des Fachrechts inhaltlich mit den Vorschriften des BayDiG vergleichbar sind, also z. B. den digitalen Zugang, die digitale Identifizierung, den digitalen Schriftformersatz, das digitale Verwaltungsverfahren oder die digitale Akten- und Registerführung regeln.

Das BayDiG tritt in diesen Fällen zunächst bei „inhaltsgleichen“ Vorschriften des Fachrechts zurück, wenn also im Fachrecht gleichlautende Regelungen zu einzelnen Vorschriften des BayDiG getroffen werden. Das BayDiG tritt aber auch dann zurück, wenn das Fachrecht „entgegenstehende“ Vorschriften enthält. Dies ist insbesondere dann der Fall, wenn das Fachrecht die Anwendung des BayDiG ausdrücklich ausschließt, wenn das Fachrecht abschließende vom BayDiG abweichende Regelungen enthält oder wenn das Fachrecht abschließende weitergehende Regelungen enthält (wenn

z. B. in bestimmten Verfahren eine ausschließlich digitale Abwicklung angeordnet wird).

Das BayDiG und das Fachrecht sind dagegen nebeneinander anwendbar, soweit das Fachrecht keine dem BayDiG inhaltlich vergleichbaren, sondern vielmehr hierzu komplementären Regelungen mit besonderer rechtlicher Zielsetzung enthält. Daher sind zum Beispiel die Bestimmungen des BayDiG und die Vorschriften über die digitale Verwaltung im BayDSG, im Bayerischen Behindertengleichstellungsgesetz oder in der BayEGovV kumulativ anwendbar. Das BayDiG lässt die Anwendung des Datenschutzrechts unberührt. Die datenschutzrechtlichen Anforderungen der DSGVO, des BayDSG und des BDSG sowie des jeweils einschlägigen Fachrechts sind von den Behörden daher auch im Anwendungsbereich des BayDiG zu beachten.

Seine Anwendungsgrenzen findet das BayDiG nach allgemeinen kompetenzrechtlichen Regelungen in Bereichen, die vom Bundesgesetzgeber abschließend geregelt wurden. Dies gilt insbesondere für das Sozialrecht und das Sozialversicherungsrecht. Grundsätzlich unterfallen das Sozialrecht und das Sozialversicherungsrecht der konkurrierenden Gesetzgebung gemäß Art. 74 Abs. 1 Nr. 7 bzw. Nr. 12 GG, sodass auch die Länder auf diesem Sektor tätig werden können. Dies gilt aber gemäß Art. 72 Abs. 1 GG nur solange und soweit der Bund von seiner Gesetzgebungszuständigkeit nicht durch Gesetz Gebrauch gemacht hat. Der Bund hat mit §§ 8 ff. SGB X bereits allgemeine Vorschriften über das Verwaltungsverfahren im Sozialrecht erlassen, insofern besteht kein Spielraum für landesgesetzliche Reglungen.

Insbesondere im Recht der gesetzlichen Krankenversicherung (SGB V) und des Vertragsarztrechts hat der Bundesgesetzgeber seine konkurrierende Gesetzgebungskompetenz bereits weitestgehend ausgeschöpft. Das durch das SGB V, durch untergesetzliche Normen (z. B. Zulassungsverordnung für Ärzte – Ärzte-ZV) sowie durch Regelungen der gemeinsamen Selbstverwaltung (z. B. Bundesmantelvertrag – BMV-Ä, samt Anlagen) geregelte Krankenversicherungs- und Vertragsarztrecht ist daher vom Anwendungsbereich des BayDiG insoweit ausgenommen. Auf Krankenhäuser, die nicht allgemeiner Bestandteil der öffentlichen Verwaltung sind, als eigenverantwortlich wirtschaftende Unternehmen sind die Teile 2 und 4 des Gesetzes ohnehin schon wegen der Ausnahmeregelung des Art. 1 Abs. 2 Satz 2 Nr. 1 nicht anwendbar (siehe bereits oben). Generell nicht anwendbar ist das Gesetz auch auf gemeinsame Einrichtungen gem. § 44b Abs. 4 Satz 1 SGB II (siehe unten zu Abs. 3).

Der Freistaat weicht mit dem BayDiG weder von den Verfahrensvorschriften der Sozialgesetzbücher ab, noch hat er hinsichtlich der übrigen Normen der Sozialgesetzbücher eine Abweichungskompetenz. Dies gilt insbesondere auch für den Sozialdatenschutz. Eventuell entgegenstehende Bestimmungen des BayDiG treten daher hinter den Rechtsvorschriften der SGB zurück. Das gilt insbesondere für die Sondervorschriften zur Verantwortlichkeit wie § 67 Abs. 4 S. 2 SGB X.

Das Gesetz gilt nur für die öffentlich-rechtliche Tätigkeit der erfassten Behörden. Ebenso wie das EGovG des Bundes und das BayVwVfG ist damit auch das BayDiG nicht auf das fiskalische Handeln des Staates anwendbar. Ausnahmen hiervon greifen gemäß Art. 18 für den digitalen Zahlungsverkehr und digitale Rechnungen.
Absatz 2 Satz 2 regelt für den verwaltungsverfahrensrechtlich ausgerichteten Teil des Gesetzes (Teil 2) sowie für den organisatonsrechtlichen Teil (Teil 4) die Ausnahmen vom Anwendungsbereich des Gesetzes. Die Regelungen orientieren sich im Grundsatz an den Ausnahmeregelungen des Art. 2 BayVwVfG, die allerdings modifiziert werden. Auch hierdurch wird der prinzipielle Gleichklang des Anwendungsbereichs des BayDiG mit dem BayVwVfG sichergestellt, zugleich aber auch den Besonderheiten des E-Government Rechnung getragen. Klar zu stellen ist in diesem Zusammenhang auch, dass für diejenigen, für die Teil 2 und 3 des Gesetzes nicht gilt, sich auch aus Teil 1 keine anspruchsbegründenden Sachzusammenhänge ergeben.

Gemäß Abs. 2 Satz 2 Nummer 1 werden Schulen und Krankenhäuser, das Landesamt für Verfassungsschutz und Beliehene vom Anwendungsbereich des 2. Teils ausgenommen, da die besonderen Aufgaben dieser Einrichtungen sondergesetzliche Regelungen auch zur Digitalisierung nahelegen. Aufgrund des in Art. 7 Abs. 1 des Grundgesetzes und Art. 130 Abs. 1, Art. 131 der Verfassung verankerten staatlichen Bildungs- und Erziehungsauftrags unterscheiden sich auch die Schulen wesentlich von anderen staatlichen Behörden. Dies gilt auch, soweit Leistungen anderer staatlicher Behörden gegenüber den Schulen betroffen sind (z. B. die staatliche Genehmigung oder Anerkennung von Ersatzschulen). Den Schulen gleichgestellt sind die Bildungseinrichtungen nach Art. 120 und 121 BayEUG. Gemeint sind in diesem Zusammenhang bei Nummer 1 nur die Tätigkeit der Schulen als Behörden, nicht die Beschäftigten an Schulen.
Im Bereich des Krankenhausbetriebs bestehen ebenfalls grundsätzliche Unterschiede zur klassischen behördenmäßigen Organisation. Anwendbar ist das BayDiG dagegen auf die behördenmäßig verfassten staatlichen Gesundheitsämter. Das Landesamt für Verfassungsschutz ist dagegen aufgrund seiner besonderen Funktionen ebenfalls vom Anwendungsbereich des Gesetzes ausgenommen. Beliehene, wie z. B. Bezirksschornsteinfeger oder Luftsicherheitsbeauftragte mit Kontrollfunktionen an den Flughäfen, nehmen im Freistaat verschiedenste öffentliche Aufgaben wahr. Die Regelungen des BayDiG sind auf die Besonderheiten dieser Tätigkeiten nicht zugeschnitten. Daher erscheint die Anwendung des BayDiG auf Beliehene als nicht zweckmäßig.

Nummer 2 nimmt die Tätigkeit der Finanzbehörden nach der Abgabenordnung vom Anwendungsbereich des Teils 2 des Gesetzes aus. Die Arbeitsabläufe in den Finanzämtern werden von eigens entwickelten, bundeseinheitlichen IT- und E-Government-Verfahren unterstützt (z. B. ELSTER), für die bundeseinheitliche Regelungen gelten (z. B. AO, StDÜV).

Gemäß Nummer 3 gilt Teil 2 des Gesetzes über die Verweisungskette ins BayVwVfG nicht für die Tätigkeit der Kirchen, der Religionsgemeinschaften und der weltanschaulichen Gemeinschaften sowie ihrer Verbände und Einrichtungen sowie ebenfalls nicht für die Anstalt des öffentlichen Rechts „Bayerischer Rundfunk“. Das Gesetz gilt ferner nicht für die Strafverfolgung, die Verfolgung und Ahndung von Ordnungswidrigkeiten, die Rechtshilfe für das Ausland in Straf- und Zivilsachen und, unbeschadet des Art. 80 Abs. 4 BayVwVfG, für Maßnahmen des Richterdienstrechts.

Nummer 4 nimmt das Prüfungsverfahren aufgrund seines speziellen Charakters vom Anwendungsbereich des Teils 2 aus.

Nummer 5 stellt klar, dass Teil 2 dieses Gesetzes für die Tätigkeit der Gerichtsverwaltungen und der Behörden der Justizverwaltung nur gelten, soweit die Tätigkeit der Nachprüfung durch die Gerichte der Verwaltungsgerichtsbarkeit oder durch die in verwaltungsrechtlichen Anwalts- und Notarsachen zuständigen Gerichte unterliegt.

Die zuvor erläuterteten Ausnahmen gelten auch für den organisationsrechtlichen Teil 4 des Gesetzes. Daraus folgt, dass die Aufgaben und Befugnisse der dort genannten Gremien (wie z.B. des Kommunalen Digitalpakts) und die dort genannten Standardisierungsbefugnisse auf die in Art. 1 Abs. 2 Satz 2 genannten Tätigkeitsbereiche (wie etwa die Schulen, das Landesamt für Verfassungsschutz etc) keine Anwendung finden.

Zu Abs. 3

Abs. 3 Satz 1 sieht eine Ausnahme für gemeinsame Einrichtungen (gE) vor. Bei gE handelt es sich um Mischverwaltungsbehörden. Die Hoheit über die verwendete Informationstechnologie obliegt gem. § 50 Abs. 3 SGB II der Bundesagentur für Arbeit (BA). Das bedeutet, dass auch Leistungen im Zuständigkeitsbereich des kommunalen Trägers im Rahmen der von der BA verantworteten IT angeboten werden. Der kommunale Träger hat es also nicht in der Hand, seine Leistungen und Dienste eigens online anzubieten. Für die Verwaltungstätigkeit der zugelassenen kommunalen Träger nach § 6a SGB II sowie für die Verwaltungstätigkeit, die aufgrund einer Delegation nach § 44b Abs. 4 Satz 1 SGB II durch kommunale Träger außerhalb von gemeinsamen Einrichtungen wahrgenommen wird, verbleibt es beim uneingeschränkten Anwendungsbereich des Gesetzes. Denn insoweit handelt es sich um keine Form der Mischverwaltung, sondern um kommunale Verwaltung unter Nutzung kommunaler Informationstechnologie und unter Aufsicht des Landes.

Zu Abs. 4

Bayern nutzt mit Art. 1 Abs. 4 die Möglichkeit der Abweichungsgesetzgebung nach Art. 84 Abs. 1 Satz 2 des Grundgesetzes (GG). Danach können die Länder von einer bundesrechtlichen Norm zur Regelung der Einrichtung der Behörden und des Verwaltungsverfahrens abweichen. Mit dem E-Government-Gesetz vom 25. Juli 2013 (BGBl

I S. 2749) hat der Bundesgesetzgeber das digitale Verwaltungsverfahren bei der Ausführung von Bundesgesetzen auch mit Wirkung für Behörden der Länder und Kommunen und Behörden der Gerichtsverwaltung geregelt (vgl. § 1 Abs. 2 und 3 EGovG). Für bayerische Behörden soll künftig grundsätzlich das Bayerische Digitalgesetz (BayDiG) zur Anwendung kommen, unabhängig davon, ob die Behörden landes- oder bundesrechtliche Regelungen vollziehen. Auch für die Gerichtsverwaltungen und die Behörden der Justizverwaltung einschließlich der unter ihrer Aufsicht unterstehenden Körperschaften des öffentlichen Rechts soll von den Vorschriften des EGovG des Bundes abgewichen werden und das BayDiG in dem in Art. 1 Abs. 1 und 2 BayDiG in Verbindung mit Art. 2 BayVwVfG vorgesehenen Bereich gelten.
Dies stellt Art. 1 Abs. 4 BayDiG sicher. Diese Vorschrift dient der Einheitlichkeit des Verwaltungsvollzugs und gewährleistet, dass die Behörden im Freistaat im Wesentlichen aufgrund eines einzigen Normregimes tätig werden können. Die Tätigkeit der Verwaltungen wird dadurch erleichtert, der Verwaltungsvollzug vereinfacht und Parallelstrukturen werden vermieden. Mit Art. 1 Abs. 4 BayDiG weicht der Landesgesetzgeber von den § 1 Abs. 2 und Abs. 3 des E-Government-Gesetz des Bundes ab. Nur in den Fällen, in denen die Behörden des Freistaates im Rahmen der Bundesauftragsverwaltung tätig werden, kommt notwendigerweise das E-Government-Gesetz des Bundes zur Anwendung (vgl. Art. 85 GG), da dem Land insoweit keine Abweichungskompetenz nach Art. 84 GG zusteht. Die Abweichung vom Bundesrecht beschränkt sich auf das E-Government-Gesetz des Bundes (Stammgesetz). Die Anwendung von Regelungen über die digitale Verwaltung im übrigen Fachrecht des Bundes bleibt daher unberührt.
Anwendbar ist das E-Government-Gesetz des Bundes damit auf die
– Bundeswehrverwaltung, Art. 87b Abs. 2 GG
– Verwaltung bei Erzeugung und Nutzung der Kernenergie, Art. 87c GG
– Luftverkehrsverwaltung, Art. 87d Abs. 2 GG
– Eisenbahnverkehrsverwaltung, Art. 87e Abs. 1 Satz 2 GG
– Verwaltung der Bundeswasserstraßen, Art. 89 Abs. 2 GG
– Verwaltung der Bundesfernstraßen durch Länder bzw. Gemeinden, die Träger der Straßenbaulast für die Ortsdurchfahrten im Zuge von Bundesstraßen sind, Art. 90 Abs. 3 GG
– Ausgabenverteilung, Finanzhilfe des Bundes, Art. 104a Abs. 3 Satz 2 GG
– Landesfinanzverwaltung, Art. 108 Abs. 3 GG
– Durchführung des Lastenausgleichs, Art. 120a Abs. 2 GG
– weitere Gebiete wie etwa den Vollzug des BAföG.

Bei Vollzug von Bundesrecht im Auftrag des Bundes (Bundesauftragsverwaltung gemäß Art. 85 GG) ist das EGovG des Bundes auch auf Behörden im Sinn von Art. 1 Abs. 1 BayDiG anwendbar. Die im Bundesgesetz für Behörden der Länder und Kommunen einschließlich der Gerichtsverwaltungen normierten Basisregelungen sollen jedoch auch in diesem Fall weitergehende landesrechtliche Regelungen regelmäßig gerade nicht vollständig ausschließen. Die Regelungen des BayDiG bleiben daher auch

bei der Ausführung von Bundesgesetzen im Auftrag des Bundes grundsätzlich anwendbar, soweit das BayDiG weitergehende Regelungen zum Beispiel zu digitalen Zugangs- und Verfahrensrechten, zur Zugangseröffnung, zur digitalen Identifizierung zum digitalen Verwaltungsverfahren oder zu digitalen Aktenführung enthält. Das BayDiG tritt gegenüber dem E-Government-Gesetz des Bundes im Bereich der Auftragsverwaltung allerdings dann zurück, wenn dieses inhaltsgleiche, entgegenstehende oder abschließende Regelungen enthält. Gleiches gilt, wenn das Fachrecht des Bundes abschließende Regelungen für die Bundesauftragsverwaltung normiert.
Sofern eine Landesbehörde für die Bundesverwaltung in Organleihe tätig wird, gilt das bundesrechtliche EGovG – vorbehaltlich anderer gesetzlicher oder sonstiger Regelungen (z.B. Organleihevereinbarung) – für die in Organleihe tätige Behörde.

Zu Art. 2 Förderung der Digitalisierung:

Art. 2 stellt die gesetzgeberischen „Metaziele“ der „Förderung“ und der (freiheits- und gemeinwohlorientierten) „Gestaltung“ der Digitalisierung nicht nur formal-systematisch, sondern auch materiell-inhaltlich an den „Anfang“ des Bayerischen Digitalgesetzes.

Zu Satz 1

Nach der Zielbestimmung in Satz 1 ist die Förderung der Digitalisierung durch den Freistaat nicht Selbstzweck, sondern Digitalisierung vielmehr im Interesse von Bürgerinnen und Bürgern und Unternehmen zielgerichtet zu gestalten. Mit dem Verweis auf die Interessen von Bürgern und Unternehmen hebt der Gesetzgeber die Selbstbestimmung der Bürgerinnen und Bürger und die konsequente Nutzung der Wachstumspotentiale der Digitalisierung als normative Kernzielsetzungen hervor.

Zu Satz 2

Auf Basis der allgemeinen Zielbestimmungen definiert Satz 2 – nicht abschließend – wesentliche Schwerpunktsetzungen für die Digitalisierungsmaßnahmen des Freistaates Bayern.

Die gesetzgeberischen Zielvorgaben definieren entwicklungsoffene gesetzliche Eckpunkte, die von der Staatsregierung und den Ressorts im Rahmen ihrer exekutiven Eigenverantwortung näher auszugestalten und umzusetzen sind. Als wesentliches Instrument sieht das Gesetz hierzu in Art. 15 den „Digitalplan“ der Staatsregierung vor.

Zum Digitalplan und zu den Berichtspflichten gegenüber dem Landtag siehe näher bei der Begründung zu Art. 15.

Zu Nr. 1

Die Norm schreibt das Ziel der Förderung digitaler Technologien am Digitalstandort Bayern fest. Wichtige Zukunftsfelder staatliche Fördermaßnahmen in Bayern sind aktuell u.a. Künstliche Intelligenz (KI), 5G-/ 6G-Mobilfunk, Autonomes Fahren, Cybersecurity, Robotik (KI, 5G, Autonomes Fahren, Cyber), Mikrosystemtechnik, 3D-Druck

und E-Health. Die Bayerische Staatsregierung hat gerade in diese Bereiche mit den Programmen Bayern Digital I und II und mit der High-Tech-Agenda massiv investiert. Diese Initiativen sind auf Basis der gesetzlichen Zielsetzung des Art. 2 S. 3 Nr. 1 konsequent weiterzuentwickeln, zu überprüfen und bei Bedarf neu zu konturieren.

Zu Nr. 2

Die Norm adressiert das Schlüsselthema digitale Bildung, dessen Bedeutung angesichts der Corona-Krise noch stärker in das öffentliche Bewusstsein getreten ist. Das Ziel digitaler Bildung ist es, Kinder, Jugendliche und Erwachsene zu einem eigenständigen, verantwortungsvollen und sachgemäßen Umgang mit der Digitalisierung zu befähigen. Sie bedient sich dazu geeigneter Soft- und Hardware, die Lehrkräfte in pädagogisch-didaktisch angemessener Weise zum Einsatz bringen. Digitale Bildung ist Aufgabe aller Schularten. Die praktische flächendeckende Umsetzung erfordert einen weiteren konsequenten Ausbau sowohl der technischen Infrastrukturen, als auch eine Weiterentwicklung von Organisationsstrukturen, Methodik und Inhalten. Zu den aktuellen Förderschwerpunkten zählen u.a. die Einführung digitaler Klassenzimmer an den Schulen, die Stärkung des Informatikunterrichts an den weiterführenden Schulen, eine Fortbildungsoffensive für Lehrkräfte und ein mehrjähriges Förderprogramm für die Sachaufwandsträger zur Verbesserung der IT-Ausstattung an den bayerischen Schulen. Diese Maßnahmen sind konsequent weiterzuentwickeln.

Doch darf auch nicht der Stellenwert der frühen Medienbildung außer Acht gelassen werden: Digitale Bildung und der Erwerb von Medienkompetenz beginnen jedoch viel früher. Bereits die Kindertagesbetreuung soll die Lebenswelt der Kinder aufgreifen und sie fit für die Herausforderungen der Gegenwart und Zukunft machen. Nur medienkompetente Kinder sind am besten vor Gefahren und Risiken geschützt und in der Lage, sinnvoll, kreativ und reflektiert Medien aller Art zu nutzen. Aus diesem Grund ist es unerlässlich, die Kinder bereits weit vor Schuleintritt in ihrer Medienkompetenz zu stärken. Ebenso wichtig ist es, die für die Kindertageseinrichtungen zuständigen Kommunen und Träger/Verbände analog der Schulsituation bei der Umsetzung ihres Bildungsauftrages aktiv zu unterstützen und auch ihnen die entsprechenden Ressourcen (insb. Hard- und Software) zur Verfügung zu stellen.

Zu Nr. 3

Die Zielbestimmung in Nr. 3 adressiert Digitalisierung als neue Aufgabe und Herausforderung für die öffentliche Daseinsvorsorge. Die Vorschrift hebt in Halbsatz 2 die Förderung leistungsfähiger digitaler Infrastrukturen exemplarisch hervor. Diese umfasst neben der Stärkung der mobilen und kabelgebundenen Breitbandnetze auch andere Formen digitaler Infrastrukturen, wie zum Beispiel digital gesteuerte Versorgungsinfrastrukturen, intelligente Energienetze, die Infrastrukturen von Smart City und Smart Region Angeboten, aber auch kritische digital gesteuerte Infrastrukturen. Die Staatsregierung hat hier unter anderem mit der Glasfaser-Initiative zur Schaffung einer gigabitfähigen Infrastruktur in ganz Bayern bis 2025, mit der Initiative Bay-

ernWLAN: 20.000 WLAN-Hotspots bis 2020, weitere 20.000 Hotspots an den bayerischen Schulen und mit der 5G-Initiative Akzente gesetzt. Der Begriff der digitalen Infrastrukturen ist nach dem Stand der Technik fortzuentwickeln. Die Maßnahmen sind an aktuelle Herausforderungen anzupassen.

Zu Nr. 4

Als weitere Aufgabe der digitalen Daseinsvorsorge hebt Nr. 4 die Implementierung intelligenter digitaler Mobilitätskonzepte hervor. Die Staatsregierung hat hier mit der Zukunftsinitiative „Autonomes Fahren“, der Digitalisierung der Straßeninfrastruktur und mit Programmen zur Vernetzung der Verkehrssysteme, z.B. zum Ausbau dynamischer Verkehrsinformationen oder zum eTicketing Akzente gesetzt. Auch dieser Begriff der Mobilitätskonzepte und die damit einhergehenden Förderaufgaben sind weit und entwicklungsoffen zu verstehen. Umfasst sind neben neuen Mobilitätstechnologien, wie etwa dem autonomen Fahren, auch intelligente Systeme der Mobilitäts- und Verkehrssteuerung auf kommunaler, regionaler und überregionaler Ebene.

Zu Nr. 5

Als dritten Schwerpunkt digitaler Daseinsvorsorge definiert Nr. 5 die Digitalisierung von Gesundheit und Pflege. Auch hier knüpft der Gesetzgeber an bestehende Schwerpunkte bayerischer Digitalpolitik an und schreibt diese entwicklungsoffen fort. Zu den aktuellen Maßnahmen zählen insbesondere die Zukunftsinitiative „Digitale Medizin“, z.B. der Wissenschaftsverbund der bayerischen Universitätskliniken im Bereich digitaler Medizin (Schwerpunkte München und Würzburg, Augsburg) und die Zukunftsinitiative „Hightech in der Pflege (u.a. Demonstrationsprojekte für den intelligenten Umbau einer Wohnung für das Leben daheim bis ins hohe Alter). Die Erfahrungen der Corona-Krise haben hier im letzten Jahr erhebliche Neujustierungen erforderlich gemacht, etwa wenn es um das Contact Tracing oder die digitale Abwicklung von Tests oder Impfungen geht. Diese neuen Impulse werden bei der Digitalplanung für den Gesundheitsbereich maßgeblich zu berücksichtigen sein.

Zu Nr. 6

Die rasanten Fortschritte der Digitalisierung wären ohne die Fortschritte digitalisierungsbezogener Disziplinen in Forschung und Wissenschaft undenkbar. Die Bayerische Staatsregierung hat hierauf u.a. mit der Hightech Agenda reagiert. Mit der High Tech Agenda hat Bayern eine Technologieoffensive mit Schwerpunkt digitale Technologien gestartet. Mit 2 Mrd. Euro, 1.000 neuen Professoren und 13.000 neuen Studienplätzen soll die Spitzenstellung des Freistaates gerade im Bereich der Digitalisierung gesichert und wenn möglich weiter ausgebaut werden.

Digitalisierung verändert aber auch – quer durch alle Disziplinen – die wissenschaftliche Kommunikation in Forschung und Lehre selbst. Dieser Transformationsprozess hat sich im Kontext der Corona-Krise noch einmal nachhaltig vertieft. Wissenschaftliche Kolloquien werden ebenso digital abgehalten, wie nahezu alle Lehrveranstaltun-

gen an Universitäten und Hochschulen in den „Corona-Semestern“. Auch das Prüfungswesen musste auf digitale Formate umgestellt werden, einschließlich der Anpassung der rechtlichen Grundlagen von Hochschulprüfungen (Bayerische Fernprüfungserprobungsverordnung – BayFEV vom 16. September 2020).

Art. 2 Satz 3 Nr. 6 verpflichtet den Freistaat die bisherigen Maßnahmen im Bereich der Digitalisierung der Wissenschaft im Lichte der Zielsetzungen des Art. 2 Satz 1 und 2 fortzuschreiben und weiterzuentwickeln.

Zu Nr. 7

Der Einsatz digitaler Technologien führt zu einer grundlegenden, globalen Veränderung von Kommunikationsmedien und Kommunikationsprozessen in Gesellschaft und Wirtschaft, in Staat und Verwaltung. Dieser Prozess setzt sich in rasanter Geschwindigkeit fort, ohne dass dessen Ausgang absehbar wäre. Damit gerät „Kommunikationskompetenz“ als grundlegende Sozialkompetenz unter Druck. Unter den Bedingungen von Digitalisierung kann praktisch jede erlernte Form von Kommunikation „fast über Nacht“ veralten. Bei mangelnder Kenntnis der neuen „Spielregeln“ digitale Kommunikation droht den Betroffenen „Anschlussverlust“ im privaten, wie im wirtschaftlichen, wie im politischen Bereich. Ins Positive gewendet ergibt sich hieraus ein Auftrag an den Freistaat, Bürgerinnen und Bürger, Akteure in der Zivilgesellschaft und Politik, die bayerische Wirtschaft, insbesondere kleine und mittlere Unternehmen beim Erwerb der erforderlichen digitalen Basiskompetenzen sowie die Beschäftigten in der öffentlichen Verwaltung beim Erwerb der erforderlichen digitalen Basis- und Fachkompetenzen zielgerichtet zu unterstützen. Den gesetzlichen Rahmen für die Förderverantwortung liefert Art. 2 Satz 3 Nr. 7.

Zu Nr. 8

Der primäre Treiber der Digitalisierung ist die digitale Wirtschaft, an der Spitze eine vergleichsweise kleine Zahl, miteinander gut vernetzter, weil weit ungewöhnlich marktmächtiger digitaler Plattformanbieter. Angesichts der wirtschaftszentrierten Dynamik der Digitalisierung werden die Bürgerinnen und Bürger im Freistaat Bayern mit den positiven, wie mit den negativen Folgen der Digitalisierung zwangsläufig gerade auch in ihrer Eigenschaft als Verbraucherinnen und Verbraucher konfrontiert. Entsprechend ist im Rahmen der Kompetenzen des Freistaates der Verbraucherschutz in der digitalen Wirtschaft eine Schlüsselaufgabe des Freistaates. Nr. 8 hebt die Vermittlung digitaler Grundkompetenzen an Verbraucher besonders hervor, damit diese aktiv, sicher und selbstbewusst auf dem digitalen Markt agieren können.

Zu Nr. 9

Der Freistaat Bayern versteht sich als digitales Gründerland. Hierzu unterstützt Bayern aktuell digitale Start-ups mit hoher Innovationskraft. Bayern trägt dadurch zur Schaffung von Arbeitsplätzen und zum wirtschaftlichen Wachstum bei. Gerade neugegründete Unternehmen helfen bei der Digitalisierung der bayerischen Wirtschaft. Daher unterstützt der Freistaat Bayern digitale Unternehmensgründungen in ganz Bayern,

u.a. durch den Aufbau Digitaler Gründerzentren und das Programm „BayStartup“. Um den Anspruch „Gründerland Nr. 1 zu werden“ (vgl. https://www.stmwi.bayern.de/digitalisierung/digitale-gruender/) auch im Bereich der Digitalwirtschaft einzulösen und weiter auszubauen, ist die konsequente Fortentwicklung von Maßnahmen zur Unterstützung digitaler Geschäftsmodelle erforderlich.

Zu Nr. 10

Die in Bayern rasch wachsende Digitalökonomie bietet neue attraktive Arbeitsplätze. Der Anteil von Frauen in Digitalberufen ist insgesamt aber nach wie vor eher gering. Daher setzt sich der Freistaat Bayern das Ziel, den gleichberechtigen Zugang zu Digitalberufen konsequent zu fördern. Der Freistaat Bayern hat hierzu u.a. die Initiative „BayFiD – Bayerns Frauen in Digitalberufen“ gestartet. Diese Maßnahmen sollen konsequent weiterentwickelt werden.

Zu Nr. 11

Zu den Herausforderungen und Schattenseiten fortschreitender digitaler Vernetzung nahezu aller gesellschaftlichen, wirtschaftlichen und administrativen Kommunikationsprozesse, zählt die damit einhergehende Gefahr für die Sicherheit, Integrität und Funktionsfähigkeit eben dieser digitalen Prozesse und der ihnen zu Grunde liegenden Infrastrukturen.

Der Freistaat Bayern hat das Thema „IT-Sicherheit“ sehr frühzeitig auch gesetzgeberisch adressiert. Bundesweit erstmalig hat Bayern im Rahmen des BayEGovG schon 2015 Regelungen zur Gewährleistung von IT-Sicherheit in der digitalen Verwaltung getroffen. Mit der Novelle des BayEGovG von 2017 wurde dieses Konzept weiterentwickelt.

Das Bayerische Digitalgesetz bildet die Rechtsgrundlage für die Einrichtung des Landesamts für Sicherheit in der Informationstechnik (LSI) mit bis zu 200 Mitarbeitern und für die Schaffung einer zentralen Kontaktstelle für die IT-Sicherheit kritischer Infrastrukturen, wie z.B. in Flughäfen.

Weitere Maßnahmen des Freistaates sind:

• Ausbau der Cybercrime-Bekämpfung, insbesondere der Zentralstelle Cybercrime in Bamberg und der Schwerpunktstaatsanwaltschaften sowie der spezialisierten Ermittlungseinheiten bei der Bayerischen Polizei.

• Ausstattung der Bayerischen Polizei mit modernster mobiler IT (z.B. Smartphones, Tablets und im Streifenwagen).

• Verstärkung der Forschung für die IT-Sicherheit (z.B. nationales Leistungszentrum „Sichere vernetzte Systeme“ von Fraunhofer in München; Forschungs- und Entwicklungs-Kooperationsprojekte für kritische Infrastrukturen privater Träger).

Die bisher vom Freistaat getroffenen Maßnahmen sind im Rahmen der gesetzlichen Zielvorgabe des Art. 2 Satz 3 Nr. 11 nunmehr anforderungsgerecht fortzuschreiben und auszubauen.

Zu den gesetzlichen Regelungen zur IT-Sicherheit im BayDiG siehe Art. 41 ff.

Zu Nr. 12

Gesamtgesellschaftliche Digitalisierung verändert auch das Koordinatensystem für die Digitalisierung der öffentlichen Verwaltung. Bis vor wenigen Jahren wurde der Einsatz von Informations- und Kommunikationstechnologien in der Verwaltung in erster Linie aus der „administrativen Binnenperspektive“ praktischer Effizienzprobleme der Verwaltung betrachtet. Hierfür steht auch der Begriff des „E-Government“. In jedem Maße, indem sich die gesamte gesellschaftliche Kommunikation auf digitale Prozesse umstellt, stellt sich Digitalisierung immer stärker als ein Prozess dar, der „von außen“ an die Verwaltung zwangsläufig herangetragen wird. Es geht nicht mehr allein um (optionale) Modernisierung, sondern um die (zwingend erforderliche) Anpassung der Verwaltungskommunikation an Veränderungen der gesellschaftlichen Kommunikation.

Art. 2 Satz 3 Nr. 12 trägt den veränderten digitalen Rahmenbedingungen des Verwaltungshandelns im Sinne einer allgemeinen gesetzlichen Zielbestimmung Rechnung. Der 1. Teil des Gesetzes (vgl. u.a. Art. 4 bis 7, Art. 9 bis 13), vor allem aber die Bestimmungen des 2. Teils des Gesetzes (Digitale Verwaltung) konkretisieren diese allgemeine Zielbestimmung. Im Vergleich zu den bisher geltenden Rechtsvorschriften des BayEGovG von 2015 trägt das DigitalG dem rasanten technischen Fortschritt, aber auch der grundlegenden Veränderungen der bundes- und unionsrechtlichen Rahmenbedingungen (insb. OZG, SDG-VO) der digitalen Verwaltung durch deutlich weitergehende gesetzliche Anforderungen an die Verwaltungsdigitalisierung Rechnung.

Zu Nr. 13

Die Potentiale der Digitalisierung der Verwaltung würden unterschätzt, wenn hierunter allein die mehr oder weniger schematische Übertragung analoger in digitale Prozesse verstanden würde. Vielmehr bietet die Digitalisierung gerade auch die Chance zu einer grundlegenden Verwaltungsmodernisierung, und dies nicht nur quantitativ (z.B. automatisierte digitale Masseverfahren), sondern gerade auch qualitativ (einfachere, nutzerfreundlicher Prozesse).

Zu Nr. 14

Offene Daten - "Open Data" – sollen für jedermann frei zugänglich sein und können aufgrund von offenen und diskriminierungsfreien Lizenzen frei wiederverwendet werden. Das Prinzip der offenen Daten - "Open Data" - bekommt weltweit eine immer größere Bedeutung. Die Verfügbarkeit von Daten wird zu einem immer bedeutenderen Wirtschaftsfaktor und ist Teil einer modernen Infrastruktur (vgl. BMI - Open Data - bund.de).

In Bayern hat das Thema „Open Data“ u.a. seinen Niederschlag im BayDSG (Allgemeiner Auskunftsanspruch) und im Fachrecht (z.B. BayUIG) gefunden. In Art. 2 Satz 3 Nr. 14 wird nunmehr die Förderung des Zugangs zu offenen Verwaltungsdaten als sachgebietsübergreifende gesetzliche Zielsetzung festgeschrieben. Das BayDiG konkretisiert die allgemeinen Ziele und Instrumente bayerische Open Data- und Transparenzpolitik in Art. 14. Zu effektiven Umsetzung dieser allgemeinen rechtlichen Grundsätze sind allerdings weitergehende und detailliertere gesetzliche Regelungen erforderlich. Diese sind aktuell in Vorbereitung.

Zu Nr. 15

Digitale Technologien bieten gerade für Menschen mit Behinderung die Möglichkeit zu gleichberechtigter Teilhabe am gesellschaftlichen und beruflichen Leben. Mangels ausreichender Marktmacht sind jedoch gerade im Bereich der digitalen Barrierefreiheit zielgerichtete staatliche Maßnahmen erforderlich. Dies adressiert Art. 2 Satz 3 Nr. 15. Das Digitalgesetz versteht digitale Barrierefreiheit rechtlich als besondere Ausformung des digitalen Selbstbestimmungsrechts der Bürgerinnen und Bürger (vgl. Art. 10). Für die Umsetzung der Zielsetzung aus Nr. 15 sind jedoch auch zielgerichtet Investitionen und Bildungsangebote erforderlich.

Zu Art. 3 Digitale Entscheidungsfähigkeit des Freistaates Bayern

Art. 3 adressiert das Schlüsselthema „Digitale Souveränität“, das seit etwa einer Dekade immer stärker in den Focus der öffentlichen Diskussion und politischer Initiativen gerückt ist (vgl. z.B. Das Gaia X Projekt der Europäischen Union).

Der ursprünglich vor allem in ökonomischen Kontexten diskutierte Begriff der „Digitalen Souveränität“ (vgl. z.B. https://www.bmwi.de/Redaktion/DE/Publikationen/Industrie/industrie-4-0-und-digitale-wirtschaft.pdf%3F__ blob%3 DpublicationFile%26v%3D3) wird inzwischen deutlich weiter verstanden und u.a. auch auf die digitale Unabhängigkeit von Staaten und Staatengemeinschaften, wie der Europäischen Union übertragen (vgl. „Whitepaper GAIA-X“ (plusserver.com).

Das BayDiG verzichtet gleichwohl bewusst auf die Aufwertung des Schlagworts der „digitalen Souveränität“ zu einem Rechtsbegriff. In rechtlichen Kontexten verwendet, signalisiert der Begriff der „Souveränität“ (von Bodin bis Jellinek) ein Maß an Unabhängigkeit und Eigenständigkeit, der weder vom Freistaat Bayern, noch von der Bundesrepublik Deutschland angesichts der Bedingungen globaler (digitaler) Vernetzung und Interdependenz realistisch eingelöst werden könnte.

Stattdessen verwendet das Gesetz den offeneren Begriff der „digitalen Entscheidungsfähigkeit“.

Zu Abs. 1

Art. 3 Abs. 1 verpflichtet den Freistaat zur Förderung und Sicherung seiner digitalen Entscheidungsfähigkeit. Das Gesetz verzichtet angesichts der Dynamik der technologischen Entwicklung bewusst auf eine nähere oder abschließende Definition der Voraussetzungen digitaler staatlicher Entscheidungsfähigkeit. Umfasst sind jedenfalls neben der Beherrschung digitaler Schlüsseltechnologien und -kompetenzen, auch die Schaffung von Netzwerksicherheit und der Schutz sensibler und vertraulicher Daten auch im mobilen Bereich. Die Zielsetzung umfasst grundsätzlich alle Bereiche staatlichen Handelns und alle Ressortzuständigkeiten. Umfasst sind damit z. B. auch erforderliche Maßnahmen im Bereich der digitalen Bildung und Qualifizierung, aber auch die Weiterentwicklung und Förderung der wissenschaftlichen Forschung.

Die Zielbestimmung in Abs. 1 bringt zum Ausdruck, dass die Gewährleistung eigenständiger digitaler Handlungs- und Entscheidungsfähigkeit des Freistaates eine vom Gesetzgeber verbindlich vorgegeben Leitschnur staatlichen Handelns und damit auch jeder künftigen Digitalstrategie sein muss. Der Gesetzgeber verzichtet aber bewusst auf konkrete inhaltliche Zielvorgaben, durch welche konkreten technischen, organisatorischen, personellen oder finanziellen Maßnahmen die staatliche Zielsetzung optimal zu verwirklichen ist. Vielmehr umfasst die Zielbestimmung insofern einen Handlungsauftrag an die Staatsregierung, eine entsprechende Strategie zu entwickeln und laufend fortzuschreiben. Um die digitale Handlungs- und Entscheidungsfähigkeit des Freistaates im Sinne des Abs. 1 S. 1 zu sichern, unterhält der Freistaat gem. Satz 2 insbesondere staatliche Rechenzentren und staatlich verfügbare Netze und entwickelt eine geeignete Cloud-Strategie.

Zu Abs. 2

Abs. 2 verpflichtet den Freistaat in Konkretisierung der Zielbestimmung des Abs. 1 in besonderer Weise zur Sicherung der Funktionsfähigkeit und des Zugangs zu staatlichen kritischen Infrastrukturen und Netzen.

Zu Abs. 3

Abs. 3 verpflichtet die Gebietskörperschaften auf den Schutz der IT-Sicherheit. Die Norm wird durch die behördenbezogenen Regelungen des Teils 3 zur IT-Sicherheit konkretisiert.

Zu Abs. 4

Abs. 4 verpflichtet die staatlichen Behörden zum Einsatz offener Software und offener Austauschstandards, soweit dies wirtschaftlich und zweckmäßig ist. Der verstärkte Einsatz offener Software dient zuvörderst der nachhaltigen Steigerung und Sicherstellung der digitalen Souveränität der Bayerischen Staatsverwaltung. Insbesondere gilt es etwaige „Lock-in-Effekte“ (z.B. Wechselkosten) zu verringern und zukünftig vorzubeugen. Langfristig sollen zugleich weitere Potenziale von offener Software im Kontext von Innovation, Kostenvorteilen und dergleichen mehr erschlossen werden. Dies soll

vor allem die Sicherheit erhöhen, da bei der Nutzung proprietärer Software die Interoperabilität fehlt. Formate oder Protokolle der Dateien können oftmals nur mit Produkten der jeweiligen Hersteller ausgelesen werden. Der Staat soll aber Herr über seine Daten bleiben.

Die Vielfalt und die ganz unterschiedlichen Anforderungen der Behörden an Softwareprodukte verbieten allerdings pauschale und generalisierende gesetzliche Vorgaben zur Softwarebeschaffung. Um die erforderlichen Spielräume der Fachbehörden abzusichern, wird die gesetzliche Verpflichtung aus Abs. 4 daher unter einem Zweckmäßigkeits- und Wirtschaftlichkeitsvorbehalt gestellt. Von einer mangelnden Wirtschaftlichkeit und Zweckmäßigkeit ist unter anderem dann auszugehen, wenn geeignete freie Software am Markt nicht verfügbar ist, nur zu unverhältnismäßig hohen Kosten zu beschaffen ist oder wenn keine Betreuungs- und Wartungsstrukturen durch Dienstleister gewährleistet werden können. Ebenso bleiben datenschutzrechtliche Vorgaben, etwa aus Art. 25 DSGVO („Privacy by Design“), unberührt.

Zu Art. 4 Digitale Daseinsvorsorge:

Art. 4 knüpft an das Ziel der Förderung der digitalen Daseinsvorsorge in Art. 2 Satz 2 Nr. 2 an und konkretisiert diese Zielsetzung für den Teilbereich der Digitalisierung öffentlicher Dienste und Verwaltungsverfahren.

Zu Abs. 1

Abs. 1 normiert insoweit eine digitale Daseinsvorsorgeverantwortung aller Behörden. Diese umfasst die Bereitstellung digitaler Verwaltungsangebote im Sinne des Verwaltungsverfahrensrechts, aber auch sonstige digitale öffentliche Dienste und Infrastrukturen der Daseinsvorsorge.

Zu Abs. 2

Abs. 2 verlangt die Bereitstellung digitaler Ansprechpartner, um die Kenntnisse über und die Akzeptanz von digitalen Angeboten durch geeignete Maßnahmen der internen und externen Kommunikation zu erhöhen.

Zu Abs. 3

Bei der Digitalisierung der Verwaltung kommt den Kommunen als dominierenden Verwaltungsträgern in Bayern eine Schlüsselrolle zu. Eine Entkopplung des Digitalisierungsstands auf staatlicher und kommunaler Ebene ist daher entgegenzuwirken, dabei aber die kommunale Selbstverwaltung und Selbstverantwortung zu wahren. Hierzu dient die auf Unterstützung der Kommunen gerichtete Zielbestimmung des Abs. 3 Satz 1. Zur Umsetzung kommen gem. Satz 2 insbesondere die Bereitstellung zentraler bzw. einheitlicher Basiskomponenten, Anwendungen und Infrastrukturen in Betracht. Der Begriff der Gemeindeverbände umfasst auch Zweckverbände und Verwaltungsgemeinschaften, wobei die Besonderheiten ihrer Aufgaben zu berücksichtigen sind.

Die Aufgaben, Zuständigkeiten und Verantwortlichkeiten der Gemeindeverbände und Gemeinden bleiben gem. Satz 3 unberührt.

Zu Art. 5 Digitalisierung von Staat und Verwaltung:

Zu Abs. 1

Abs. 1 Satz 1 legt die vollständige Digitalisierung aller hierzu geeigneten Prozesse in Staat und Verwaltung im Freistaat Bayern als Ziel fest. Die Norm knüpft an die in den Programmen Bayern Digital I und II definierten Zielsetzungen an und entwickelt diese für die staatliche Verwaltung insgesamt fort. „Vollständig“ meint in diesem Zusammenhang die Digitalisierung interner wie externer Prozesse. Durch die Formulierung „sollen“ sind Ausnahmen von der Volldigitalisierung insbesondere aus sicherheitsrechtlichen Gründen zulässig. Zum Begriff der „Geeignetheit“ siehe umfassend Art. 17.

Zu Abs. 2

Mit der Regelung wird der Einsatz von Algorithmen bei digitalen Diensten und Verwaltungsverfahren, etwa in Form von Prüf- oder Entscheidungsalgorithmen, von besonderen Voraussetzungen abhängig gemacht. Damit wird erstmals eine Algorithmenkontrolle im allgemeinen Verwaltungsverfahrensrecht verankert. Die zuständige Behörde hat die Zweckmäßigkeit, d.h. die Eignung des Algorithmeneinsatzes zur Zielerreichung zu prüfen. Weiter muss die Objektivität des Algorithmus regelmäßig geprüft werden, um „automatisierte Diskriminierungen“ bzw. einen „Algorithmic bias“ zu vermeiden. Schließlich steht der Einsatz von Algorithmen unter einem Wirtschaftlichkeitsvorbehalt. Die Norm orientiert sich in der Begrifflichkeit an Art. 88 Abs. 5 AO. Weitergehende Anforderungen, die sich u.a. auch dem Rechtstaatsprinzip oder aus Anforderungen des Fachrechts ergeben, bleiben unberührt.

Zu Abs. 3

Abs. 3 S. 1 weist dem Staatsministerium für Digitales die Aufgabe der ressortübergreifenden Steuerung der Umsetzung des Online-Zugangsgesetzes in Bayern zu. S. 2 stellt klar, dass die Verantwortlichkeiten der Ressorts unberührt blieben. Dies gilt insbesondere auch für die durch oder auf Grundlage von Beschlüssen des IT-Planungsrats festgelegten Themenfeldverantwortlichkeiten für die OZG-Umsetzung. Zuständigkeiten, die von mehreren Ressorts ausgeübt werden, bleiben hiervon ebenso unberührt.

Zu Art. 6 Nachhaltigkeit:

Art. 6 enthält eine Verpflichtung der Verwaltung bei Ihrer Aufgabenstellung auch Aspekte der Ökologie und der Nachhaltigkeit zu berücksichtigen, insbesondere geht es dabei um den Dreiklang „Anschaffung, Betrieb und Entsorgung“. Digitalisierung ermöglicht es u.a. aber auch auf Dienstreisen zu verzichten und sie beispielsweise durch Videokonferenzen zu ersetzen; auch die Einrichtung von Telearbeitsplätzen kann dazu beitragen, gerade Großstädte vom Pendelverkehr zu entlasten.

Zu Art. 7 Personal und Qualifizierung:

Diese Vorschrift enthält Regelungen zur Personalgewinnung von IT-Fachkräften, sowie Vorschriften zur Weiterbildung und entsprechenden Qualifizierung der Bediensteten in den Behörden. Bayern will hier vor allem mit der Einrichtung eines „Digital Campus“ neue Wege bestreiten.

Zu Abs. 1

Abs. 1 Satz 1 sieht vor, dass die digitale Qualifizierung der Beschäftigten der öffentlichen Verwaltung vom Freistaat gefördert wird. Nach Abs. 1 Satz 2 sind geeignete Maßnahmen für die Gewinnung, Bindung und Entwicklung von IT-Fachkräften in der bayerischen Staatsverwaltung in den Personalentwicklungskonzepten der obersten Landesbehörden zu verankern. Satz 2 adressiert die Gewinnung, Bindung und Entwicklung von IT-Fachkräften in der bayerischen Staatsverwaltung. Angesichts des Wettbewerbs um IT-Fachkräfte bestehen ein Bedarf nicht nur an ressortspezifischen, sondern gerade auch an ressortübergreifenden Maßnahmen. Der Freistaat Bayern hat diesen Weg bereits mit dem Nachtragshaushaltsgesetz 2018 eingeschlagen, das ein Maßnahmenpaket zur Optimierung der Personalgewinnung und Stärkung der Personalbindung im IT-Bereich umfasst. Neben zusätzlichen Beförderungsmöglichkeiten wurden ein Zuschlag zur Gewinnung von IT-Fachkräften und die Möglichkeit zur schnelleren Verbeamtung vorgesehen.

Zu Abs. 2

Abs. 2 konkretisiert die Qualifizierungsaufgaben für die Fälle der Einführung neuer IT- oder E-Government-Verfahren sowie bei wesentlichen Erweiterungen oder sonstigen Änderungen bestehender Verfahren.

Kapitel 2. Digitale Rechte und Gewährleistungen

Das BayDiG will Bürgerinnen und Bürger und Unternehmen in Bayern in die Lage versetzen, auch unter Bedingungen der Digitalisierung als aktiv gestaltende Akteure zu handeln. Daher setzt das BayDiG im 2. Kapitel bei den Rechten von Bürgern und Unternehmen in der Digitalisierung an.

Kapitel 2 enthält hierzu ein System digitaler Rechte und Gewährleistungen

Die Einräumung subjektiver digitaler Rechte trägt der gewachsenen Bedeutung der digitalen Kommunikation über das Internet in allen Lebensbereichen Rechnung. In dem Maße, indem sich sowohl die nicht rechtsverbindliche, als auch die rechtsverbindliche private und gewerbliche Kommunikation in das Internet verlagert, gewinnt die Möglichkeit, für Kommunikationszwecke auch tatsächlich auf das Internet zurückgreifen zu können, für die effektive Wahrnehmung der Belange der Bürger und Unternehmen in Gesellschaft und Wirtschaft, Staat und Verwaltung an Bedeutung.

Mit der Gewährleistung von digitalen Zugangs- und Verfahrensrechten knüpft das BayDiG an die subjektiv-rechtliche Dimension des Verwaltungsverfahrensrechts und des BayEGovG an und entwickelt diese unter den aktuellen Bedingungen der Digitalisierung weiter. Die bisherigen nur punktuellen subjektiv-rechtlichen Regelungen zum Verfahren über den einheitlichen Ansprechpartner (vgl. Art. 71e BayVwVfG) im BayVwVfG wurden bereits mit dem BayEGovG auf grundsätzlich alle Behördendienste und Verwaltungsverfahren erweitertDas 2. Kapitel normiert „technikgebundene“ Zugangs- und Verfahrensrechte, das heißt Rechte, deren Ausübung notwendig die Bereitstellung von bestimmten technischen Infrastrukturen durch Dritte bzw. die Verwaltung (z.B. Internetzugang über Festnetz oder Mobilfunk, Einrichtung eines Nutzerkontos, , Nutzung von Verschlüsselungsverfahren, Beschaffung eines Lesegeräte etc.) schon voraussetzt. Regelmäßig wird auch eine Mitwirkung des Nutzers bzw. dessen Anschluss an bestimmte Dienste technische Voraussetzung für die Wahrnehmung digitaler Rechte sein. Die Rechte des 2. Kapitels begründen also kein Recht des Nutzers, einen eigenen Hardware-Zugang o. ä. auf Staatskosten zu erhalten. Aufgrund ihrer „Technikgebundenheit“ müssen Reichweite und inhaltliche Ausgestaltung der Rechte im Übrigen auf die korrespondierenden technischen Bereitstellungsverpflichtungen der Behörden abgestimmt werden.

Eine Gewähr für die jederzeitige uneingeschränkte Aktualität, Richtigkeit, Vollständigkeit und Verfügbarkeit der bereit gestellten Dienste ist mit den im Gesetz verankerten Rechten nicht verbunden. Im Übrigen bleiben die Haftungsbegrenzungen des Telemediengesetzes sowie das Recht der Behörden unberührt, technische Verfügbarkeiten im Rahmen von Nutzungsbedingungen zu regeln und Haftungsansprüche im Rahmen der allgemeinen gesetzlichen Vorgaben in zulässiger Weise zu begrenzen bzw. auszuschließen.

Zu Art. 8 Freier Zugang zum Internet

Zu Satz 1

In Satz 1 wird das Recht auf freien Zugang zum Internet als einfachgesetzliches Abwehrrecht normiert. Satz 1 stellt durch die Formulierung „über allgemein zugängliche Netze“ zugleich klar, dass sich das Recht nur im Rahmen vorhandener Infrastrukturen entfaltet, aber kein Recht auf Bereitstellung von technischen Internetzugängen umfasst. Das Wort „frei“ ist in diesem Zusammenhang daher auch nicht als „kostenfrei“ zu verstehen.

Mit der einfachgesetzlichen Normierung eines Abwehrrechts auf Zugang zum Internet trägt der Gesetzgeber der Tatsache Rechnung, dass der Zugang zum Internet beim heutigen Stand der Digitalisierung Voraussetzung für die wirksame umfassende Wahrnehmung praktisch aller Grundrechte geworden ist. Das Recht auf Internetzugang ist daher nicht mit dem Recht auf „Informationelle Selbstbestimmung“ oder einem anderen bereits normierten Grundrecht deckungsgleich.

Aufgrund der hohen Dynamik des Sachbereichs verzichtet der Gesetzgeber zum gegenwärtigen Zeitpunkt bewusst auf eine verfassungsrechtliche Regelung. Die Verankerung im einfachen Gesetzesrecht soll es ermöglichen, Erfahrungen mit der Wirksamkeit der Regelungen zu sammeln, die in einem späteren eventuellen Konstitutionalisierungsprozess einfließen können.

Zu Satz 2

Satz 2 stellt klar, dass durch Gesetz oder aufgrund von Gesetz normierte Zugangsbeschränkungen von der Vorschrift unberührt bleiben, etwa in öffentlichen Einrichtungen (z.B. Schulen) oder für Minderjährige. Gleiches gilt für vorrangige Regelungen des Bundesrechts.

Ein generelles Verbot des Zugangs zum Internet im Sinne einer allgemeinen, einschränkungslosen staatlichen Internetzugangsblockade gegen einzelne Personen oder Personengruppen ist dagegen gem. Satz 3 ausgeschlossen. Damit knüpft das Gesetz an die geltende Verfassungslage und die Rechtsprechung des EMRK an (vgl. z.B. Beschwerden Nr. 48226/10 und 14027/11, Urteil des EGMR vom 1. Dezember 2015) und verankert diese erstmal im einfachen Gesetzesrecht.

Als reines Abwehrrecht umfasst Art. 8 dezidiert keinerlei Leistungsansprüche etwa auf Bereitstellung von Internetzugangsinfrastrukturen (Breitband, Mobilfunk) oder sonstige Hard- oder Softwaredienste zur technischen Vermittlung des Internetzugangs. Mögliche Regelungen dieser Art obliegen mit Blick auf die Kompetenzverteilung im Telekommunikationsrecht ohnehin ausschließlich dem Bundesgesetzgeber.

Für die hier geplante abwehrrechtliche Regelung besitzt der Freistaat dagegen die Gesetzgebungskompetenz, da es nicht um Telekommunikationsrecht bzw. um den technischen Aspekt des Internets (Bereitstellung von technischen Vorrichtungen zum Internetempfang etc.) geht, sondern um die Regulierung des Internets z.B. durch Blockieren der digitalen Nutzung des World Wide Web (vgl. hierzu auch das Dokument des Wissenschaftlichen Dienstes des Bundestags, WD 2 - 3000 - 131/19 vom 25. November 2019). Landesrechtliche Befugnisse zu Internetzugangsbeschränkungen könnten sich z.B. aus dem Polizei- und Ordnungsrecht ergeben. Bei deren Ausübung ist Art. 6 von den Behörden zu beachten.

Zu Satz 3

Nach Satz 3 sind allgemeine staatliche Internetzugangsblockaden unzulässig (siehe die Erläuterungen oben).

Zu Art. 9 Digitale Handlungsfähigkeit

Die zunehmende Verlagerung der Verwaltungskommunikation ins Internet wirft die Frage nach der effektiven Ausübung von Verfahrensrechten insbesondere auch dann auf, wenn Dritte in die Kommunikation einzubeziehen sind, sei es als Vertreter, Bevoll-

mächtigte, Sorgeberechtigte, im Rahmen der Vormundschaft oder auch im Erbfall. Bisher sind digitale Dienste und Verfahren nur unzulänglich auf derartige Konstellationen ausgerichtet. Art. 10 verpflichtet den Freistaat Bayern daher auf die Bereitstellung digitaler Dienste hinzuwirken, die die umfassende digitale Handlungsfähigkeit der Beteiligten sicherstellen.

Zu Art. 10 Digitale Selbstbestimmung

Art. 10 dient der Förderung digitaler Selbstbestimmung und der Gewährleistung der Nutzerfreundlichkeit digitaler Angebote. Der Regelungszweck der Norm ist nicht mit der nach wie vor stark abwehrrechtlich geprägten Zielsetzung des Rechts auf informationelle Selbstbestimmung deckungsgleich. Vielmehr soll der Bürger in die Lage versetzt werden, seine digitale Kommunikation im privaten und geschäftlichen Bereich und bei Kontakten mit der Verwaltung seinen eigenen Handlungszielen entsprechend frei zu gestalten.

Zu Abs. 1

Abs. 1 normiert die Grundsätze der Nutzerfreundlichkeit und Barrierefreiheit für digitale Verwaltungsangebote des Freistaates Bayern. „Digitale Dienste“ im Sinne dieses Gesetzes sind dabei Dienstleistungen, die von Behörden zur Erfüllung öffentlicher Aufgaben in digitaler Form über ein Eingabegerät oder über allgemein zugängliche Netze angeboten werden.
Der Begriff der Nutzerfreundlichkeit im Sinne dieses Gesetzes ist nicht rein technokratisch („Nutzerfreundlichkeit ist, was ein Digitallabor als nutzerfreundlich definiert“), sondern vielmehr normativ zu konkretisieren. Die Wahrnehmung von Grundrechten in einer zunehmend digitalisierten Verwaltung setzt voraus, dass der Einzelne digitale Vorgänge nachvollziehen und sich seiner eigenen Rolle und der Auswirkungen digitaler Handlungen bewusst ist. Art. 12 DSGVO stellt nicht zuletzt auch deshalb auf Informationen in "präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" ab. In diesem Zusammenhang ist auch auf den vom Bundesverfassungsgericht entwickelten Grundrechtsschutz durch Verfahren hinzuweisen. Damit sind Konstellationen gemeint, in denen der Staat präventive organisatorische und verfahrensrechtliche Vorkehrungen zum Schutz von Grundrechten treffen muss. In diesem Sinne ist bei der nutzerfreundlichen Ausgestaltung digitaler Angebote des Freistaates Bayern gerade auch die Möglichkeit effektiver Wahrnehmung verfahrensrelevanter Grundrechte mit zu berücksichtigen.

Zu Abs. 2

Abs. 2 normiert zur Umsetzung des Regelungszwecks der Norm eine Förderverantwortung für den Freistaat in Hinblick auf geeignete allgemeine Informations- und Bildungsangebote, insbesondere auch im Bereich der Barrierefreiheit.

Zu Art. 11 Digitale Identität:

Zu Abs. 1

Nach Abs. 1 hat jeder das Recht auf Bereitstellung digitaler Identitätsdienste nach Maßgabe dieser Vorschrift. Diese Regelung knüpft an die handlungsbezogenen Normen zur digitalen Selbstbestimmung an, unterscheidet sich von diesen Vorschriften aber durch seine personenbezogene, auf Dauer angelegte Zielsetzung. Die Regelung stellt eine Schlüsselnorm des Gesetzes dar, da sie jeder Person auf Lebenszeit das Recht auf staatliche Bereitstellung digitaler Dienste einräumt, die dieser eine dauerhafte Speicherung und selbstbestimmte Nutzung aller personenbezogenen Informationen und Dokumente ermöglicht. Dies umfasst auch das Recht auf selbstbestimmte Verfügung über die personenbezogen gespeicherten Daten, einschließlich eines jederzeitigen informierten Löschungsrechts. Der Anspruch auf Bereitstellung digitaler Identitätsdienste gilt jedoch nur, wenn bereits eine geklärte und rechtlich gesicherte Identität vorliegt. Auch können rechtliche Einschränkungen in Bezug auf die Verwendung der Identitätsdokumente mit eID-Funktion einem Anspruch auf Bereitstellung digitaler Identitätsdienste entgegenstehen (z. B. Einschaltung der Online-Ausweisfunktion ab 16 Jahren, Betreuung, Strafgefangene).

Zur Digitalen Identität zählt auch die Gewährleistung einer sicheren und auf Dauer angelegten Behördenkommunikation, die einen jederzeitigen Rückgriff auf archivierte Informationen und Dokumente ermöglicht.

Der Begriff der „Digitalen Identität“ wird in Abs. 1 im Interesse der Entwicklungsoffenheit bewusst nicht abschließend definiert, sondern nur funktional konkretisiert. Der Begriff geht über die „digitale Identifizierung“ oder die Bereitstellung digitaler Identifizierungsmittel im Sinne der eIDAS-Verordnung hinaus. Er umfasst ohne abschließende Beschränkung alle digitalen Dienste, deren Bereitstellung erforderlich ist, um eine auf Dauer angelegte, personenbezogene, selbstbestimmte Nutzung digitaler Behördendienste, die dauerhafte Archivierung aller damit zusammenhängenden Informationen und deren dauerhafte Nutzung im Rahmen der digitale Abwicklung digitaler Verwaltungsverfahren nach dem jeweiligen Stand der Technik zu ermöglichen.

Abs. 1 stellt klar, dass insbesondere auch die digitale Vorlage und Archivierung von Belegen durch digitale Dienste sicherzustellen ist. Damit soll eine notwendige Voraussetzung für die vollständig digitale Abwicklung von Verwaltungsverfahren geschaffen werden. Hier setzt die digitale Übermittlung von Bescheiden voraus, dass die Empfänger in der Lage sind, diese digitalen Dokumente auch dauerhaft und sicher zu speichern, gegebenenfalls auch langfristig. Hier obliegt dem Freistaat eine Verantwortung, die Bürger auch in die Lage zu versetzen, eine solche Speicherung vorzunehmen.

Zu Abs. 2

Abs. 2 S. 1 konkretisiert das Recht im Sinne von Abs. 1 und verweist hierzu auf die Pflichten des Freistaates Bayern zu Bereitstellung digitaler Dienste gem. Art. 29 bis 31 Satz 2 normiert die Antragsvoraussetzungen für die Bereitstellung einer digitalen Identität unter Verweis auf Art. 31 Abs. 2. Die hier angesprochenen Dienste werden kontinuierlich nach dem Stand der Technik fortentwickelt.

Zu Abs. 3

Satz 1 stellt klar, dass die Einrichtung und Nutzung der digitalen Identität für Bürgerinnen und Bürger in ihren privaten, nichtwirtschaftlichen Angelegenheiten freiwillig ist. Zur möglichen Verpflichtung zur Nutzung eines Organisationskontos siehe Art. 28 Abs. 3.

Abs. 3 verankert in Satz 2 das jederzeitige Zugriffs- und Löschungsrecht des Inhabers der Identität und regelt in Satz 3 die datenschutzrechtliche Aufsicht.

Zu Abs. 4

Absatz 4 stellt klar, dass die in der digitalen Identität gespeicherten amtlichen Dokumente der Privatsphäre des Inhabers zuzuordnen sind und sich damit gerade nicht in „amtlicher Verwahrung“ befinden (vgl. § 96 StPO). Die Norm verpflichtet den Freistaat die digitale Identität vor unberechtigten Zugriffen Dritter zu schützen. Die in der digitalen Identität gespeicherten Dokumente sind der Sphäre des Bürgers zuzuordnen. Daher ist ein Zugriff der Behörden, auf die im Rahmen der digitalen Identität gespeicherten Dokumente ohne Einwilligung des Inhabers nur unter den strafprozessualen Voraussetzungen der Beschlagnahme zulässig ist. Besondere gesetzliche Befugnisse bleiben unberührt.

Zu Art. 12 Rechte in der digitalen Verwaltung:

In einem demokratischen Rechtsstaat kann die digitale Verwaltung dauerhaft nur erfolgreich sein, wenn Bürger und Unternehmen die digitale Verwaltung als Instrument zur effektiven Wahrnehmung ihrer berechtigten Interessen verstehen. Die digitale Verwaltung sollte daher nicht nur technisch, sondern auch rechtlich konsequent auf den Nutzer ausgerichtet werden. Art 12 setzt inhaltlich und gesetzessystematisch bei den Bürgern und deren Rechten in der digitalen Verwaltung an.

Zu Abs. 1

Abs. 1 normiert (in Übernahme des Art 2 Satz 1 und 2 BayEGovG) ein Recht auf digitale Kommunikation mit den Behörden, auch im mobilen Bereich und auf digitale Durchführung von Verwaltungsverfahren. Die Norm verweist dabei in Satz 1 auf die korrespondierenden Behördenpflichten aus den Art 16 bis 18 und in Satz 2 auf die korrespondierenden Behördenpflichten in Art. 19.

Siehe im Übrigen Einleitung vor Art. 8.

Zu Abs. 2

Die Umstellung auf ein digitales Verfahren darf auch nicht zu Lasten grundlegender rechtsstaatlicher Verfahrensstandards gehen. So ist es beispielsweise weiterhin erforderlich eine zwingende Verschlüsselung bei sensiblen Personendaten vorzunehmen – ungeachtet der grundsätzlichen Zustimmung des Antragsstellers zum elektronischen Versand. Ebenso bleiben die Rechte auf Auskunft und Beratung gem. Art. 25 BayVwVfG und auf Anhörung gem. Art. 28 BayVwVfG unberührt. In diesen Fällen sollte die „ausschließlich digitale Option“ nicht dazu führen, dass die Beteiligten bei Auskunfts- Beratungs- oder Anhörungsbegehren in „Chatbot-Schleifen“ verfangen oder alternativlos auf „nervige Sprachcomputer“ (Zitat aus der Werbung eines privaten Internetservice-Providers für seine Premium-Hotline) verwiesen werden können. Art. 12 Abs. 2 begründet daher in Konkretisierung der allgemeinen Verfahrensrechte aus Art. 25 und Art. 28 BayVwVfG ein Recht des Beteiligten auf persönliche Beratung und Auskunft und auf persönliche Anhörung. Persönliche Beratung meint dabei jedoch nicht zwingend auch analoge Beratung, persönliche Beratung kann somit auch beispielsweise per Telefon oder E-Mail erfolgen.

Zur Gewährleistung der praktischen Wirksamkeit der Rechte aus Satz 1 hat die zuständige Behörde gem. S. 2 in datenschutzkonformer Weise die Kontaktdaten für die persönliche Beratung, Auskunft und Anhörung für die Beteiligten (angelehnt an § 5 TMG) „leicht erkennbar, unmittelbar erreichbar und ständig verfügbar“ zu halten. Gem. S. 3 ist der sofortige Vollzug vollständig automatisiert erlassener Entscheidungen nur aufgrund ausdrücklicher gesetzlicher Ermächtigung zulässig.

Zu Art. 13 Mobile digitale Dienste:

Art. 13 regelt die mobile Bereitstellung digitaler Verwaltungsdienste. Die Norm steht im Zusammenhang mit Art. 5, da mobile digitale Dienste ein zentraler Baustein der Volldigitalisierung der Verwaltung sind sowie mit Art. 12. Die Norm regelt die Bereitstellung von digitalen Verwaltungsservices in einer für Mobilgeräte optimierten Form. Weitergehende Ansprüche auf Bereitstellung von technischen Infrastrukturen, wie etwa Mobilfunknetzen ist hiermit nicht verbunden.

Zu Abs. 1

Abs. 1 verankert ein Recht auf mobile digitale Dienste, verknüpft dies aber zugleich mit den erforderlichen Ausführungsvorschriften des Abs. 2 sowie weiterer Ausführungsverordnungen.

Zu Abs. 2

Nach Art. 13 Abs. 2 stellen die staatlichen Behörden ihre hierzu geeigneten Dienste auch mobil zur Verfügung. Bei der mobilen Zurverfügungstellung ist die nutzerfreundliche Bedienung durch Smartphones und Tablets zu berücksichtigen. Die Regelung beschränkt sich auf das „Außenverhältnis zum Nutzer“ bzw. das Antragsverfahren und umfasst daher kein Fachverfahrensangebot zur Sachbearbeitung. Mit dem Verweis

auf die Bereitstellung über „allgemein zugängliche Netze“ wird klagestellt, dass die Norm das Vorhandensein eines allgemein zugänglichen Mobilfunkanschlusses voraussetzt und nicht gewährleistet.

Satz 2 normiert die Unterstützungszuständigkeit des Freistaates für den Ausbau mobiler kommunaler Dienste. Die eigenen Aufgaben und Zuständigkeiten der Kommunen bleiben unberührt.

Zu Art. 14 Offener Datenzugang:

Der offene Zugang zu Daten der öffentlichen Verwaltung ist für die informierte Teilhabe von Bürgerinnen und Bürgern am gesellschaftlichen und politischen Leben, für die Funktionsfähigkeit der Zivilgesellschaft, aber auch für informierte unternehmerische Entscheidungen und neue Geschäftsmodelle der Datenökonomie und damit für das volkswirtschaftliche Wachstum von wesentlicher Bedeutung. Impulse für rechtliche Regelungen zum offenen Datenzugang gehen insbesondere auch von der Europäischen Union aus, insbesondere durch die Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-II-Richtlinie) und für den Bereich der Geodaten durch die Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE-Richtlinie).

Mit Satz 1 wird die grundsätzliche Pflicht zur Gewährleistung eines offenen Datenzugangs verankert (Open Data). Satz 2 begründet eine erweiterte Verpflichtung der Behörden zur zielgruppenorientierten und nutzerfreundlichen Aufbereitung ihrer öffentlich zugänglichen Datenbestände. Bei der Ausgestaltung der Voraussetzungen des offenen Datenzugangs sollte vorrangig auf interoperable Standards/Normen gesetzt werden, um nicht Gefahr zu laufen, öffentliche Daten mit viel Aufwand je Anforderung individuell zusammenstellen zu müssen. Die nähere Bestimmung des offenen Datenzugangs erfolgt durch oder aufgrund Gesetzes (Satz 3). So dürfen beispielsweise Beschränkungen aus bereits normierten Auskunftsansprüchen nicht umgangen werden. Auch wird durch Art. 15 kein Anspruch auf Bereitstellung bestimmter Daten begründet, diese Frage bleibt einem gesonderten Gesetzgebungsverfahren vorbehalten.

Zu Art. 15 Digitalplan, Digitalbericht

Art. 15 begründet eine übergreifende Planungs- und Evaluierungsverantwortung der Staatsregierung für die Maßnahmen des Gesetzes sowie eine korrespondierende Berichtspflicht gegenüber dem Landtag. Bei der Erstellung des Digitalplans sowie der Digitalberichte sind alle Ressorts einvernehmlich miteinzubeziehen.

Im Rahmen des Digitalplans sind einvernehmlich zwischen den Ressorts die erforderlichen Priorisierungen bei der Umsetzung der Ziele und Maßnahmen dieses Gesetzes vorzunehmen und korrespondierend der erforderliche finanzielle und personelle Aufwand für die Umsetzung dieser Maßnahmen zu planen ebenso wie damit korrelierend die damit verbundenen finanziellen und personellen Einsparungen.

Die Staatsregierung kann im Rahmen des Digitalplans die Fördermaßnahmen nach Art. 2 konkretisieren, die erforderlichen Maßnahmen zur Umsetzung der Zielsetzungen der Art. 3 bis 7 definieren sowie die erforderlichen rechtlichen, technischen, organisatorischen, personellen und finanziellen Maßnahmen zur Umsetzung der Rechte und Gewährleistungen aus den Art. 8 bis 14 definieren.

Der Digitalbericht der Staatsregierung umfasst neben dem Sachstand der Umsetzung der Ziele des Allgemeinen Teils des Gesetzes auch den Bericht zum Umsetzungsstand der übrigen Teile des Gesetzes. Dabei sind auch die Ergebnisse der indikatorbasierten Evaluierung des Gesetzes zu berücksichtigen. Die Evaluierung wird auch die Umsetzungskosten für die Gemeindeverbände und Gemeinden umfassen.

Teil 2. Digitale Verwaltung

Kapitel 1. Digitale Kommunikation und Dienste

Zu Art. 16 Digitale Kommunikation:

Art. 16 knüpft an die kommunikationsbezogenen Bestimmungen des Art. 3 Abs. 1 und Abs. 2 BayEGovG an. Die allgemeine Kommunikationsnorm wird im BayDiG fortgeführt, rechtlich aber in wesentlichen Teilen durch die spezielleren Vorschriften zum Portalverbund überlagert.

Zu Satz 1

Satz 1 begründet eine abstrakte Verpflichtung der Behörden zur Eröffnung des Zugangs zur digitalen Kommunikation mit dem Bürger auf dem „Hinkanal“ zu den Behörden über öffentlich zugängliche Netze. Die Vorschrift gilt für alle Behörden im Anwendungsbereich des Gesetzes. Die Regelung modifiziert die Regelungen über die Zugangseröffnung in Art. 3a Abs. 1 BayVwVfG in Bezug auf die Zugangseröffnung durch Behörden, die in den Anwendungsbereich des Art. 1 fallen. Die Regelung reduziert das Entschließungsermessen der Behörde gemäß Art. 3a Abs. 1 BayVwVfG in Bezug auf die Zugangseröffnung. Dies entspricht weitgehend den rechtlichen Wirkungen im Verhältnis von § 2 Abs. 1 EGovG zu § 3a Abs. 1 VwVfG. Bei Behörden, die nicht in den Anwendungsbereich des Art. 1 fallen, bleibt es dagegen beim Grundsatz der Freiwilligkeit der Zugangseröffnung nach Maßgabe von Art. 3a Abs. 1 BayVwVfG. Bei Störungen in der digitalen Kommunikation gilt Art. 3a Abs. 3 BayVwVfG.

Im Zuge der Erarbeitung des BayDiG wurden erhebliche Anstrengungen unternommen, um Schriftformerfordernisse abzuschaffen oder zu reduzieren. Damit soll das E-Government vereinfacht und Hürden zur Nutzung von E-Government-Verfahren vermindert werden. In Art. 16 Satz 1 wird entsprechend zwischen digitalen Dokumenten (ohne formales Schriftformerfordernis) und schriftformersetzenden Dokumenten (im Sinn des Art. 3a BayVwVfG) unterschieden. Die Behörde kann ihre Verpflichtung aus Satz 1 bereits dadurch erfüllen, dass sie einen einzelnen Zugangskanal eröffnet, wenn dieser (auch) die übrigen Anforderungen des S. 1 erfüllt.

Die Vorschrift belässt den Behörden im Übrigen auch angemessene Spielräume hinsichtlich der Auswahl des die Schriftform ersetzenden Verfahrens. Die Anforderungen der Norm sind bereits erfüllt, wenn die Behörde ein E-Mail-Postfach eröffnet, da hierüber auch ein Empfang einer qualifiziert signierten E-Mail im Sinn von Art. 3a Abs. 2 BayVwVfG ermöglicht wird. Weitergehende Anforderungen aus dem Fachrecht hinsichtlich der Anforderungen an den Schriftformersatz bleiben unberührt. Alternativ kann die Behörde auch einen De-Mail Zugang eröffnen oder eine Identifizierung über den neuen Personalausweis anbieten.

Zu Satz 2

Satz 2 stellt für den Rückkanal von der Behörde zum Bürger klar, dass weiterhin der Grundsatz der Zugangseröffnungsfreiheit gilt. Satz 2 sichert die Dispositionshoheit des Bürgers hinsichtlich der Zugangseröffnung im Rückkanal ausdrücklich ab („soweit“). Die Norm stellt weiter klar („solange“), dass der Bürger den Rückkanal auch befristet öffnen bzw. schließen kann. Die Regelung des Satzes 2 hat insbesondere für zentrale „Bürgerportale“ und/oder „Bürgerkonten“ Bedeutung, bei denen eine Vielzahl von digitalen Verwaltungsdiensten „gebündelt“ angeboten werden sollen. Bei derartigen Portalen besteht ein besonderes Interesse des Bürgers wie auch der Verwaltung, rechtssicher, aber auch hinreichend flexibel festlegen zu können, ob und für welche Verfahren oder Verfahrensarten ein Zugang eröffnet wird und damit insbesondere auch eine digitale Verbescheidung möglich ist. Satz 2 sichert die Möglichkeit ab, dem Bürger im Rahmen von Bürgerportalen standardisierte Wahlmöglichkeiten einzuräumen, ob dieser den Zugang für alle oder nur für einzelne der über das Portal angebotenen Verfahren eröffnen will. Diese Flexibilität und Wahlfreiheit der Bürger kann zur Akzeptanz von Bürgerportalen beitragen. Die Anforderungen des Datenschutzrechts bleiben unberührt.

Zu Satz 3

Satz 3 verpflichtet die Behörden, für den Hinkanal zur Verwaltung und für den Rückkanal zum Bürger Verschlüsselungsverfahren anzubieten, z. B. verschlüsselte Internetverbindungen (SSL) oder verschlüsselte Dokumente/Online-Formulare. Satz 3 begründet allerdings nur eine Verpflichtung der Behörden, zusätzlich auch geeignete sichere Verfahren anzubieten. Die Regelung hindert die Behörde daher nicht daran, ihre Verpflichtung aus Satz 1 (auch) durch E-Mail-Dienste zu erfüllen. Ebenso steht es dem Bürger in Ausübung seines Rechts auf informationelle Selbstbestimmung frei, das Angebot auf verschlüsselte Kommunikation nicht zu nutzen und stattdessen auf die E-Mail-Kommunikation zurückzugreifen.

Die Wahl eines Verschlüsselungsverfahrens liegt im Organisationsermessen der jeweils zuständigen Behörde. Im staatlichen Bereich kann die zuständige oberste Landesbehörde im Rahmen bestehender Weisungsverhältnisse die Entscheidungen der nachgeordneten Behörden einheitlich festlegen. In der Regel wird, entsprechend der gesetzgeberischen Entscheidung im De-Mail-Gesetz, eine Transportverschlüsselung

ausreichen (De-Mail-Gesetz vom 28. April 2011, BGBl. I S. 666). Bei besonders sensitiven Datensätzen kann auch eine Ende-zu-Ende Verschlüsselung erforderlich sein. Ein Recht der Nutzer auf Eröffnung eines bestimmten technischen Verfahrens besteht damit nicht. Umgekehrt sind die Nutzer, vorbehaltlich besonderer Rechtsvorschriften, nicht verpflichtet, den von der Behörde angebotenen Rückkanal zu nutzen bzw. den Zugang hierfür zu eröffnen. Satz 4 lässt gegebenenfalls bereits bestehende Verpflichtungen der Behörden zum Angebot von Verschlüsselungsverfahren aufgrund von Telemedienrecht und sonstigem Fachrecht unberührt. Gleiches gilt für Verschlüsselungspflichten, soweit sich diese aus dem Datenschutzrecht ergeben. Unberührt bleiben auch die Verpflichtungen der Behörden zur digitalen Kommunikation mit den Gerichten nach Maßgabe des Gesetzes zur Förderung des digitalen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGB. I S. 3785 ff.).

Zu Satz 4

Satz 4 sichert die Ermessensspielräume der Behörde bezüglich der Art der technischen Umsetzung der Verpflichtungen ausdrücklich ab. Die Vorschrift stellt klar, dass die Wahl des technischen Verfahrens für die Zugangseröffnung und die Übermittlung von Dokumenten auf dem Hin- und Rückkanal im pflichtgemäßen Ermessen der jeweils zuständigen Behörde steht. Durch verwaltungsinterne Vorschriften kann die technische und organisatorische Ausgestaltung für sichere auf öffentlich zugänglichen Netzen basierende Dienste näher präzisiert und der erforderliche technische Sicherheitsstandard einheitlich vorgegeben werden. Ein Anspruch des Nutzers auf ein bestimmtes technisches Verfahren, eine bestimmte Art der Verschlüsselung oder ein bestimmtes technisches Sicherheitsniveau wird nicht begründet. Die Regelung gewährleistet, dass eine Behörde nicht zur Bereitstellung von technischen Verfahren oder Sicherheitsstandards verpflichtet ist, die mit Blick auf Art und Umfang der betroffenen Verwaltungstätigkeit mit unverhältnismäßig hohen Kosten oder Organisationsaufwand verbunden sind.

Zur einfachen Kommunikation mit dem Nutzer sollte jede Behörde über ein E-Mail-Postfach verfügen. Mit jedem E-Mail-Postfach können in technischer Hinsicht auch digitale Dokumente empfangen werden, die mit einer qeS versehen sind. Weiter kann die Verpflichtung aus Satz 1 aber auch dadurch erfüllt werden, dass die Behörde z. B. ein digitales Gerichts- und Verwaltungspostfach (EGVP) oder ein anderes Verfahren einrichtet, über das ihr digitale Dokumente schriftformersetzend übermittelt werden können. Beispiele für derartige Verfahren sind die digitale Steuererklärung (ELSTER) im Sinn von § 87a Abs. 6 Satz 1 AO und die vom Freistaat Bayern für staatliche und kommunale Behörden angebotenen zentralen Dienste „Bürgerkonto“ und „Postkorb“, soweit diese einen Schriftformersatz gemäß Art. 3 a Abs. 2 Satz 4 Nr. 1 BayVwVfG ermöglichen. Verpflichtungen zum Angebot von Verschlüsselungsverfahren aufgrund anderer Rechtsvorschriften (einschließlich des Datenschutzrechts) bleiben unberührt.

Zu Art. 17 Digitale öffentliche Dienste:

Art. 17 übernimmt die Bestimmungen des Art. 4 BayEGovG. Art. 17 und 18 gelten allgemein, also nicht nur für die öffentlich-rechtliche Verwaltungstätigkeit, sondern auch für die schlichte Verwaltungstätigkeit der Behörden.

Allgemeines

Art. 17 Abs. 1 verpflichtet Behörden, ihre hierzu geeigneten Dienste grundsätzlich auch über das Internet bereitzustellen. Der bisherige Verweis auf Wirtschaftlichkeit und Zweckmäßigkeit in Art. 4 Abs. 1 BayEGovG entfällt. Die Änderungen des Normtextes dienen in erster Linie der Klarstellung der ohnehin bereits nach Art. 4 Abs. 1 BayEGovG bestehenden Behördenpflichten. Die Zweckmäßigkeit einer auch digitalen Bereitstellung von Verwaltungsleistungen dürfte selten zu verneinen sein. Auch der bisherige allgemeine Wirtschaftlichkeitsvorbehalt läuft angesichts der Fortschritte der Digitalisierung, der aktiven Fördermaßnahmen des Freistaates und der im Gesetz neu verankerten Unterstützungsmaßnahmen des Freistaates in der überwiegenden Zahl der Fälle weitgehend leer.

Der Begriff der Dienste ist dabei weit zu verstehen. Erfasst werden insbesondere alle Arten von Informations-, Auskunfts- und Datenbereitstellungsdiensten. Erfasst werden digitale Mitteilungs- und Verkündungsblätter (vgl. Abs. 3) ebenso wie z. B. Geodatendienste, aber auch flankierende Informationsangebote zur Nutzung dieser Dienste (vgl. Abs. 1 Satz 2).

Die Regelung korrespondiert teilweise mit § 3 (Informationen zu Behörden und ihre Verfahren in öffentlich zugänglichen Netzen) und § 12 (Anforderung an die Bereitstellung von Daten) des EGovG des Bundes. Es werden jedoch andere Schwerpunkte gesetzt. Anders als im Bundesrecht begründet Art. 17 Abs. 1 ein subjektives Recht auf Zugang zu Behördendiensten, einschließlich Datendiensten sowie der zu ihrer Nutzung relevanten Informationen. Dafür wird auf Regelungen zu technischen Anforderungen an die Bereitstellung von Daten angesichts bereits bestehender gesetzlicher und untergesetzlicher Regelungen verzichtet (vgl. die Rechtsvorschriften zur Umsetzung der Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 345 vom 31. Dezember 2003, S. 90 bis 96) in der Fassung 26. Juni 2013 (Richtlinie 2013/37/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors [ABl. L 175 vom 27. Juni 2013, S. 1 bis 8]) und der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) [ABl. L 108 vom 25. April 2007, S. 1 bis 14]).

Zu Abs. 1

Satz 1 normiert ein Gebot an die Behörden, Dienste der Verwaltung grundsätzlich auch digital über öffentliche Netze bereitzustellen. Die Vorschrift begründet kein originäres Informations- oder Datenzugangsrecht, sondern setzt die Eröffnung eines analogen oder digitalen Zugangs zu Informationen oder Daten aufgrund des Fachrechts bereits voraus. Mit dem Begriff der Dienste werden sämtliche Dienstleistungen der Verwaltung erfasst, unabhängig davon, ob diese im Rahmen oder auf Grundlage eines Verwaltungsverfahrens erbracht werden. Hierzu zählen neben verfahrensgebundenen Diensten unter anderem auch Beratungs- oder Informationsangebote, die Bereitstellung von Daten oder sonstige Serviceleistungen für Bürger oder Unternehmen. Die Bestimmungen des Datenschutzrechts bleiben unberührt.

Durch Satz 1 werden die Behörden nunmehr angehalten, das gesetzgeberische Ziel des Ausbaus der E-Government-Angebote im Rahmen der von ihnen zu beurteilenden Möglichkeiten aktiv umzusetzen. Die Verpflichtung beschränkt sich auf das Außenverhältnis zum Bürger und umfasst keine innerbehördlichen Prozesse (zu diesen siehe Art. 6). Die Bereitstellung kann je nach Art des Dienstes und Leistungsfähigkeit der Behörde ganz oder teilweise erfolgen. Der Begriff der Geeignetheit ist nach dem Zweck der Norm weit zu verstehen. Öffentliche Dienste sind dann zur Digitalisierung geeignet, wenn deren digitale Bereitstellung technisch möglich und nicht mit unverhältnismäßigem Aufwand verbunden ist. Dabei steht den Behörden auch ein Spielraum offen, nach welchen Prioritäten in welcher zeitlichen Folge einzelne Dienste digital bereitgestellt werden. Um eine pflichtgemäße Ermessensausübung sicherzustellen, kann es für die Behörden sinnvoll sein, einen Digitalisierungsplan vorzulegen, der die geplanten Maßnahmen auf Basis von definierten Prioritäten in einem definierten Zeitraum festlegt. Bei der Ermessensausübung ist auch die OZG-Umsetzungsplanung und die Umsetzung des 12-Punkte Plans der Staatsregierung zur Digitalisierung der Verwaltung vom Februar 2020 zu berücksichtigen. Die Geeignetheit kann etwa aus sicherheitspolitischen Gründen entfallen (z. B. persönliche Vorsprache zur Identitätsklärung insbesondere im Ausländer- und Staatsangehörigkeitsrecht, aber auch im allgemeinen polizeilichen Ermittlungsverfahren). Auch bei grundsätzlich geeigneten Verfahren darf einer Behörde nicht verwehrt werden, im eigenen Ermessen die persönliche Vorsprache einer Person zu verlangen (vgl. „sollen“ im Gesetzeswortlaut).

Satz 2 begründet für Behörden die Verpflichtung über öffentlich zugängliche Netze die Informationen bereitzustellen, die für die sachgerechte digitale Inanspruchnahme ihrer Dienste erforderlich sind. Anders als in Satz 1 wird durch Satz 2 eine originäre, vom Fachrecht unabhängige Informationsbereitstellungspflicht normiert. Hierunter können je nach Art des Dienstes oder des Verfahrens insbesondere Informationen über die Aufgaben und Zuständigkeitsbereich einer Behörde, anfallende Gebühren, beizubringende Unterlagen, die zuständige Ansprechstelle und ihre Erreichbarkeit fallen. Die Regelung korrespondiert mit § 3 Abs. 1 und 2 des EGovG Bund, verzichtet aber angesichts der Vielzahl und Verschiedenartigkeit der erfassten Dienste auf die ausdrückliche Normierung von Katalogtatbeständen.

Die Möglichkeit von Behörden, im Rahmen ihrer Organisationsverantwortung zentrale Ansprechstellen zu schaffen, bleibt unberührt. Soweit der Behördenkontakt über zentrale Ansprechstellen erfolgt, genügt die Angabe der Kontaktdaten der zentralen Ansprechstelle über das Netz.

Zu Abs. 2

Abs. 2 stellt klar, dass für die Nutzung des digitalen Weges keine zusätzlichen Kosten erhoben werden. Diese Regelung korrespondiert mit einer Neuregelung im Kostengesetz. Dort wird sogar eine Gebührenermäßigung für die Nutzung des digitalen Weges vorgesehen.

Zu Abs. 3

Das amtliche Publikationswesen durchläuft einen grundlegenden Wandel von der papiergebundenen hin zur digitalen Veröffentlichung. Die Zahl der zusätzlich oder ausschließlich digitalen Veröffentlichungen nimmt auf der Bundes-, Landes und Kommunalebene zu. Mit der am 1. April 2012 in Kraft getretenen Änderung des Verkündungs- und Bekanntmachungsgesetzes (VkBkmG) vom 22. Dezember 2011 (BGBl. I S. 3044) wurde bereits die Überführung des Bundesanzeigers in die ausschließlich digitale Ausgabe vollzogen. § 15 EGovG des Bundes ermöglicht für sonstige Veröffentlichungen in amtlichen Mitteilungs- und Verkündungsblättern die Bekanntgabe in ausschließlich digitaler Form. Abs. 3 regelt alternativ die Voraussetzungen für die zusätzliche (Satz 1) und die ausschließliche (Satz 2) digitale Publikation.

Zu Satz 1

Satz 1 stellt klar, dass veröffentlichungspflichtige Mitteilungen und amtliche Verkündungen digital veröffentlicht werden sollen. Die Vorschrift erfasst alle aufgrund von Bundes-, Landes- oder Kommunalrecht veröffentlichungspflichtigen Mitteilungen und amtlichen Verkündungen. Die Regelung tritt für die bayerischen Behörden (mit Ausnahme der Bundesauftragsverwaltung) an die Stelle des § 15 EGovG Bund, der eine in der Zielsetzung ähnliche Regelung für Veröffentlichungspflichten aufgrund von Bundesrecht vorsieht.

Satz 1 lässt die Anwendung des Datenschutzrechts unberührt. Eine digitale Veröffentlichung personenbezogener Daten soll daher nur erfolgen, wenn und soweit hierzu eine gesetzliche Verpflichtung besteht. Sind in einer Publikation personenbezogene Daten enthalten, ist datenschutzrechtlich zu prüfen, ob diese dauerhaft über öffentlich zugängliche Netze angeboten werden können.

Zu Satz 2

Satz 2 regelt die besonderen Voraussetzungen für eine ausschließlich digitale Bekanntmachung. Eine ausschließlich digitale Bekanntmachung ist möglich, wenn eine Veränderung der veröffentlichten Inhalte ausgeschlossen ist und die Einsichtnahme auch unmittelbar bei der die Veröffentlichung veranlassenden Stelle für jede Person

auf Dauer gewährleistet ist. Satz 2 ist nicht anwendbar, wenn Rechtsvorschriften der ausschließlich digitalen Bekanntmachung entgegenstehen, also ausdrücklich eine papiergebundene Bekanntmachung vorschreiben (z. B. Art. 76 der Verfassung). Die Tatsache, dass Rechtsvorschriften über Veröffentlichungspflichten bisher in der Regel von einer papiergebundenen Form ausgingen, steht der ausschließlich digitalen Bekanntmachung dagegen nicht entgegen.

Die Regelung zur Unveränderbarkeit des Inhalts trägt dem Umstand Rechnung, dass es eine wesentliche Vorbedingung für die Authentizität der verkündeten Fassung ist, dass veröffentlichte Dokumente nachträglich nicht mehr geändert oder gar gelöscht werden können.

Art. 17 Abs. 3 begründet ein Recht auf angemessenen Zugang zu digitalen amtlichen Veröffentlichungen, soweit die Behörde den digitalen Weg gewählt hat. Die Zugangsnorm erfasst alle veröffentlichungspflichtigen Mitteilungen und amtlichen Verkündungsblätter, also z. B. öffentliche und ortsübliche Bekanntmachungen (Art. 27a BayVwVfG in der Fassung des Gesetzentwurfs der Staatsregierung, LT-Drs. 17/2820), aber auch digitale Veröffentlichungen in amtlichen Mitteilungs- und Verkündungsblättern (vgl. § 15 EGovG).

Das Zugangsrecht gilt daher sowohl für Bekanntmachungen im Rahmen des Verwaltungsverfahrens im Sinne von Art. 9 BayVwVfG als auch für digitale amtliche Bekanntmachungen im Rahmen des Normerlasses, für die es etwa in der Gemeindeordnung, Landkreisordnung und Bezirksordnung sowie im LStVG Sondervorschriften gibt. Der Zugang ist angemessen auszugestalten, z. B. durch die Möglichkeit, einen digitalen Hinweis auf die Veröffentlichung zu erhalten bzw. diese digital zu abonnieren, Ausdrucke zu bestellen oder in öffentlichen Einrichtungen auf die Bekanntgabe zuzugreifen. Das Gebot der effektiven Zugänglichkeit bedingt, dass von Anfang an ein zukunftssicheres Format für die digitalen Dokumente gewählt werden muss, welches deren Interpretierbarkeit auch auf zukünftigen IT-Systemen gewährleistet.

Satz 2 stellt in diesem Zusammenhang klar, dass die Einsichtnahme auch unmittelbar bei der die Veröffentlichung veranlassenden Stelle auf Dauer für jede Person zu gewährleisten ist. Dadurch kann sichergestellt werden, dass auch der Teil der Bevölkerung, der zur Nutzung öffentlich zugänglicher Netze mangels der erforderlichen technischen Infrastruktur oder mangels persönlicher Fähigkeiten nicht in der Lage ist, auf die Veröffentlichung zugreifen kann. Hierzu kann z.B. ein papiergebundenes Exemplar zur Einsicht durch jedermann bereitgehalten werden oder eine Einsichtnahme über einen Bürger-PC ermöglicht werden.

Zu Satz 3

Nach Satz 3 wird das Nähere durch Bekanntmachung der Staatsregierung geregelt. Hierbei sind insbesondere auch Regelungen zur Gewährleistung des Datenschutzes zu treffen.

Abs. 3 lässt die Vorschriften des Datenschutzrechts hinsichtlich des „Ob“, des „Wie“ und des „Wie lange“ der digitalen Veröffentlichung unberührt. Eine digitale Veröffentlichung personenbezogener Daten soll daher nur erfolgen, wenn und soweit hierzu eine gesetzliche Verpflichtung besteht. Sind in einer Publikation personenbezogene Daten enthalten, ist datenschutzrechtlich zu prüfen, ob diese dauerhaft über öffentlich zugängliche Netze angeboten werden können. Ebenso sind Zugriffsmöglichkeiten und Löschungspflichten datenschutzkonform auszugestalten.

Zu Art. 18 Digitale Zahlungsabwicklung und Rechnungen:

Zu Abs. 1

Art. 18 Abs. 1 enthält Regelungen zum digitalen Zahlungsverkehr. Abs. 1 erfasst sämtliche Geldansprüche öffentlicher Kassen, unabhängig davon, ob diese ihren Rechtsgrund in einer öffentlich-rechtlichen Verwaltungstätigkeit einer Behörde gemäß Art. 1 Abs. 1 finden. Die Norm geht daher im Anwendungsbereich über die Grundsatzregelung des Art. 1 Abs. 2 dieses Gesetzes hinaus.

Halbsatz 1 begründet ein Recht, Gebühren und sonstige Forderungen der Behörden im digitalen Zahlungsverkehr zu begleichen. Der Begriff der Geldansprüche ist dabei weit zu verstehen. Er umfasst daher auch Geldbußen und Geldstrafen. Die Regelung zielt auf die Gewährleistung der Medienbruchfreiheit des Verwaltungsverfahrens auch in Bezug auf Zahlungsvorgänge in allen digitalen Verwaltungsverfahren auf allen Verwaltungsebenen. Dem entspricht die Verpflichtung der Behörde, den Zahlungsverkehr zu ermöglichen. Die Behörde kann ihre Verpflichtung bereits dadurch erfüllen, dass sie dem Zahlungspflichtigen eine Bankverbindung zur Abwicklung des digitalen Zahlungsverkehrs mitteilt. Der unbare Zahlungsverkehr im Verhältnis der Bürger zur öffentlichen Hand ist bereits heute in weiten Bereichen der Regelfall; so sind beispielsweise auch im justiziellen Bereich gemäß § 1 Satz 1 der Verordnung über den Zahlungsverkehr im Bereich der ordentlichen Gerichtsbarkeit und der Finanzgerichtsbarkeit (Zahlungsverkehrsverordnung Justiz/Finanzen – ZahlVJuFin) Zahlungen an Gerichte und Justizbehörden im Geschäftsbereich des Staatsministeriums der Justiz grundsätzlich unbar zu leisten.

Halbsatz 2 verpflichtet die Behörden, die Begleichung von Gebühren und sonstigen Forderungen auch durch die Bereitstellung von in den Antragsprozess integrierten digitalen Zahlungsmöglichkeiten über öffentlich zugängliche Netze bereitzustellen. Sofern sich das Verwaltungsverfahren in geeigneter Weise, also technisch und wirtschaftlich sinnvoll mit einem E-Payment-System verknüpfen lässt, ist regelmäßig nur eine solche Zahlungsmöglichkeit im Sinne des Gesetzes geeignet. Dies ist insbesondere dann der Fall, wenn Verwaltungsvorgänge vollständig über ein im Internet bereitgestelltes Verfahren abgewickelt werden. E-Payment-Systeme sind Systeme, die in die Websites öffentlicher Stellen integriert sind und ausgehend von der Behördenwebsite eine digitale Zahlungsabwicklung ermöglichen. Die gewählte Technologie muss den Anforderungen der öffentlichen Verwaltung entsprechen. Sie muss insbesondere datenschutzkonform ausgestaltet sein.

Die unbare Zahlungsmöglichkeit besteht nur, solange kein sofortiges anderweitiges Vollstreckungsinteresse besteht. Hierdurch wird sichergestellt, dass bei einem besonderen öffentlichen Interesse an einem Barinkasso (z. B. bei polizeilichen Straßenkontrollen) kein Anspruch auf digitales Bezahlen besteht.

Zu Abs. 2

Art. 18 Abs. 2 begründet gegenüber Auftraggebern im Sinne des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) ein Recht auf digitale Rechnungstellung. Die Norm erfasst damit abweichend von Art. 1 Abs. 1 gerade das fiskalische Handeln der öffentlichen Hand. Zudem knüpft Abs. 2 nicht an den Behördenbegriff, sondern an den weiteren Begriff des Auftragsgebers an.

Art. 18 Abs. 2 beinhaltet im Vergleich zur Vorgängerregelung im Art. 5 Abs. 2 BayEGovG nur kleinere Änderungen, die der besseren Lesbarkeit dienen. Zudem geht die Kompetenz zum Verordnungserlass auf die Staatsregierung über, die nun die nähere Ausgestaltung des digitalen Rechnungsverkehrs regeln kann.

Art. 18 Abs. 2 schafft den Rechtsrahmen zur verpflichtenden Entgegennahme digitaler Rechnungen durch Auftraggeber in Bayern im Sinne von § 98 GWB. Die Vorschrift ist zur Umsetzung der Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die digitale Rechnungstellung bei öffentlichen Aufträgen (ABl. L 133 vom 6. Mai 2014, S. 1 bis 11) zwingend erforderlich.

Zu Satz 1

In Satz 1 wird die Verpflichtung der öffentlichen Auftraggeber normiert, die Entgegennahme und Verarbeitung digitaler Rechnungen sicherzustellen. Anders als in Art. 1 knüpft Art. 18 Abs. 2 damit nicht an den Behördenbegriff, sondern an den Begriff des Auftraggebers im Sinne von § 98 GWB an. Satz 1 stellt weiter klar, dass die Verpflichtungen zur Entgegennahme digitaler Rechnungen nur für öffentliche Auftraggeber gelten, für die gemäß § 106a GWB eine Vergabekammer des Freistaat Bayern zuständig ist. Damit wird der Anwendungsbereich der Vorschrift vom Anwendungsbereich der entsprechenden Regelungen zur digitalen Rechnung im Bund und in anderen Bundesländern abgegrenzt. Durch die dynamische Verweisung auf § 106a GWB wird auch gewährleistet, dass eventuelle Änderungen des Auftraggeberbegriffs des GWB keine Folgeänderungen im BayDiG erforderlich machen.

Zu Satz 2

Satz 2 enthält eine Legaldefinition des Begriffs der digitalen Rechnung, die an Art. 1 der Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die digitale Rechnungstellung bei öffentlichen Aufträgen (ABl. L 133 vom 6. Mai 2014, S. 1 bis 11) angelehnt ist.

Kapitel 2. Digitales Verwaltungsverfahren

Zu Art. 19 Digitale Verfahren:

Zu Abs. 1

Art.19 enthält Regelungen zur Gewährleistung eines grundsätzlich medienbruchfreien elektronischen Verwaltungsverfahrens, einschließlich elektronischer Formulare und elektronischer Nachweise. Erfasst wird nur das nach Außen gerichtete Verwaltungshandeln im Sinn des BayVwVfG, nicht aber die interne Verwaltungsorganisation. (zum Begriff des Verwaltungsverfahrens siehe Art. 9 BayVwVfG). Rein behördeninterne Vorgänge, wie die Art und Weise der elektronischen Aktenführung, werden nicht erfasst.

Abs. 1 begründet ein Recht auf vollständige oder teilweise elektronische Durchführung des Verwaltungsverfahrens. Abs. 1 stellt klar, dass ein Anspruch auf (vollständige oder teilweise) elektronische Verfahrensdurchführung nicht besteht, soweit dies unzweckmäßig oder unwirtschaftlich ist. Abs. 1 sichert den diesbezüglichen Beurteilungsspielraum der Behörde ausdrücklich ab. Von der Verfahrensdurchführung in elektronischer Form kann damit auch weiterhin teilweise, aber auch vollständig abgesehen werden, wenn dies im Einzelfall oder bei bestimmten Verfahrensarten unzweckmäßig oder unwirtschaftlich ist. Soweit eine nur teilweise elektronische Verfahrensdurchführung, wie z.B. die elektronische Antragstellung, wirtschaftlich und zweckmäßig ist, ist die Behörde gehalten, das Verfahren teilweise elektronisch anzubieten. Die elektronische Durchführung muss rechtlich möglich sein; erforderlich ist also u. a. eine Zugangseröffnung durch die Beteiligten. Besondere Rechtsvorschriften bleiben unberührt. Die datenschutzrechtlichen Anforderungen an die elektronische Verfahrensdurchführung sind zu beachten. Bei Störungen in der elektronischen Kommunikation gilt Art. 3a Abs. 3 BayVwVfG.
Übergangsbestimmungen und weiterführenden Hinweisen siehe Art. 53b, 55 Abs.1.

Zu Abs. 2

Abs. 2 Satz 1 regelt die Verpflichtung zur Bereitstellung von elektronischen Formularen über das Internet als Teil des elektronischen Verwaltungsverfahrens. Die Regelung dient der teilweisen elektronischen Durchführung des Verwaltungsverfahrens. Die Vorschrift greift nur bei formulargebundenen Verfahren. Sie setzt voraus, dass Behörden zur Durchführung von Verwaltungsverfahren bereits Formulare bereithalten. Diese sind auch in elektronischer Form über das Internet bereitzustellen. Die Regelung findet unabhängig von der Bezeichnung als Formular, Vordruck, Formblatt oder ähnlichen Begriffen Anwendung. Die Verpflichtung nach Satz 1 greift ihrem Sinn und Zweck nicht, wenn Fachverfahren zur elektronischen Verfahrensabwicklung bereitgehalten werden oder wenn Urheberechte Dritter (an Musterformularen) entgegenstehen. Mit Satz 2 wird klargestellt, dass kein Schriftformerfordernis vorliegt, wenn dieses nicht explizit in der Norm angeordnet wird. Sofern die dem Formular zugrundeliegende Rechtsnorm für die Erklärung explizit Schriftform anordnet, ist auch künftig die Nutzung

eines elektronischen Schriftformsurrogats gemäß Art. 3a Abs. 2 BayVwVfG erforderlich. Für alle anderen durch Rechtsvorschrift angeordneten Formulare ist klargestellt, dass auch eine Übermittlung des elektronischen Formulars an die Behörde beispielsweise als ausgefülltes pdf-Dokument ohne Unterschrift möglich ist. Zu Übergangsbestimmungen und weiterführenden Hinweisen siehe Art. 53b, 55 Abs.1.

Zu Abs. 3

Die Identifikationsfunktion des Personalausweises ist für die Durchführung von Verwaltungsverfahren von wesentlicher Bedeutung. Art. 20 begründet daher ein Recht auf digitale Identifizierung in digitalen Verwaltungsverfahren über öffentlich zugängliche Netze. Art. 19 Abs. 3 gilt nur für die Identifizierung über öffentlich zugängliche Netze. Die Identifizierung unter Anwesenden ist nicht erfasst. Dies entspricht der Rechtslage auf Bundesebene.

Absatz 3 begründet eine Verpflichtung der Behörden in digitalen Verwaltungsverfahren einen digitalen Identitätsnachweis gemäß § 18 des Personalausweisgesetzes, § 12 des eID-Karte-Gesetzes bzw. § 78 Abs. 5 des Aufenthaltsgesetzes anzubieten. Die Regelung entspricht insoweit § 2 Abs. 3 EGovG.

Art. 19 Abs. 3 korrespondiert mit der Regelung zum digitalen Schriftformersatz durch Einsatz der eID-Funktion des neuen Personalausweises gemäß Art. 3a Abs. 2 Satz 4 Nr. 1 BayVwVfG. Durch die Regelung wird sichergestellt, dass staatliche Behörden nicht nur grundsätzlich verpflichtet sind, die eID-Funktion des nPA als Schriftformersatz anzuerkennen, sondern dass die Bürger auch tatsächlich die technische Möglichkeit haben, die eID-Funktion des nPA als Schriftformersatz zu nutzen. Klarzustellen ist, dass die Ausländerbehörden rein bundesgesetzlich nicht allen Ausländern einen digitalen Identitätsnachweis nach § 78 Abs. 5 AufenthG „anbieten“ können, da ein elektronischer Identitätsnachweis nur in elektronischen Aufenthaltstiteln enthalten ist, wenn die Identität des Ausländers durch die Ausländerbehörde zweifelsfrei festgestellt ist.

Für die Identifikation einer natürlichen oder juristischen Person, in Fällen für die keine Rechtsvorschrift zur Feststellung der Identität existiert, können weitere technische Systeme genutzt werden, um z. B. Zugangshürden zu E-Government-Verfahren zu verringern. So wird von der Steuerverwaltung die Lösung ELSTER und außerhalb der Steuerverwaltung die Lösung Authega eingesetzt, um einerseits die Identifikation von Steuerpflichtigen bei der Abgabe von Steuererklärungen und andererseits den sicheren Zugang und die Authentifizierung im Zuge der zentralen Bereitstellung digitaler Antrags- und Auskunftsverfahren zu ermöglichen. Das Bayernportal soll entsprechend den formellen Anforderungen abgestufte Dienste zur Identifikation anbieten, um einen einheitlichen Zugang für Bürger und Unternehmen sicherzustellen und zur Wirtschaftlichkeit der E-Government-Verfahren beizutragen.

Zusätzlich ist Abs. 3 erweitert worden, mit dem Ziel, die eID zu implementieren, wie sie im „Gesetz über eine Karte für Unionsbürger und Angehörige des europäischen

Wirtschaftsraums mit Funktion zum digitalen Identitätsnachweis“ (eID-Karte-Gesetz – eIDKG) vom 21. Juni 2019 geregelt ist.

Zu Art. 20 Digitale Verfahren als Regelfall

Zu Abs. 1

Abs. 1 modifiziert den „Grundsatz der digitalen Verfahrenswahlfreiheit“ in Richtung auf das digitale Verfahren als Regelverfahren.

Abs. 1 verankert in seinem Satz 1 erstmals den Grundsatz „Digital First“. Die E-Government-Gesetze des Bundes und der Länder und das OZG zielen bisher einheitlich darauf ab, digitale Verwaltungsangebote als „zusätzliche Option“ bereitzustellen (vgl. § 1 OZG: „auch digital“). Es besteht daher bisher auch keine Pflicht der Behörden, die als „zusätzliche Option“ bereitgestellten digitalen Verfahren in der Praxis als Regelfall einzusetzen und damit den Verwaltungsprozess insgesamt von der analogen auf die digitale Ebene zu verlagern.

Diese Lücke soll nunmehr mit Abs. 1 Satz 1 für staatliche Behörden geschlossen werden. Im Regelfall sollen staatliche Behörden Verwaltungsverfahren künftig digital durchführen, d.h. ihre Verwaltungsprozesse auf den digitalen Regelfall umstellen. Zum Begriff der „Geeignetheit“ siehe bereits unter Art. 17 Abs. 1.

Satz 2 betont jedoch, dass die Verfahren nutzerfreundlich im Sinne von Art. 10 ausgestaltet werden müssen.

Nach Satz 3 bleiben die Rechte der Bürger aus Art. 12 unberührt. Dies gilt insbesondere für das Recht auf nichtdigitale Verfahrensdurchführung gem. Art 12 Abs. 1 Satz 3. Im Ergebnis haben die Behörden also einerseits in der Regel digitale Verfahren anzubieten, zugleich aber das nichtdigitale Verfahren als „zusätzliche Option“ ohne zusätzliche Kosten anzubieten. Im Ergebnis kehrt sich durch die Norm das Regel-Ausnahme-Verhältnis zwischen digitalem und nichtdigitalem Verfahren zu Gunsten des „digitalen Regelfalls“ um.

Zu Abs. 2

Absatz 2 Satz 1 sieht die Möglichkeit vor, Verwaltungsleistungen, die über ein Organisationskonto angeboten werden, auch ausschließlich digital anzubieten. Damit wird der Tatsache Rechnung getragen, dass im unternehmerischen und sonstigen geschäftlichen Verkehr eine ausschließlich digitale Abwicklung beim heutigen Stand der Technik in der Regel als zumutbar angesehen werden kann. Die Norm schreibt die ausschließlich digitale Durchführung aber nicht vor, sondern lässt diese lediglich zu. Soweit die Behörde den digitalen Weg wählt, müssen die besonderen Anforderungen an die Nutzerfreundlichkeit im Sinne von Art. 12 Abs. 2 erfüllt werden. Welche Verfahren digital angeboten werden sollen, kann zum einen durch Verordnung (vgl. Art. 53 Abs. 1 Nr. 8) festgelegt werden, aber auch durch eigene Festlegung der Kommunen erfolgen. Letzteres dient der Stärkung der kommunalen Selbstverwaltung.

Abs. 2 Satz 2 enthält eine an § 150 Abs. 8 AO angelehnte Härtefallregelung. Mit dieser soll sichergestellt werden, dass die nicht digitale Abwicklung von Verwaltungsverfahren für den Beteiligten auch im geschäftlichen Verkehr über das Organisationskonto möglich bleibt, soweit dies für den Beteiligten persönlich oder wirtschaftlich unzumutbar ist. Dies ist angelehnt an § 150 Abs. 8 Satz 2 AO insbesondere der Fall, wenn die Schaffung der technischen Möglichkeiten für eine Datenfernübertragung nur mit einem nicht unerheblichen finanziellen Aufwand möglich wäre oder wenn der Beteiligte nach seinen individuellen Kenntnissen und Fähigkeiten nicht oder nur eingeschränkt in der Lage ist, die Möglichkeiten der Datenfernübertragung zu nutzen. Liegen die Voraussetzungen des Satzes 2 vor, hat der Beteiligte auch in diesen Fällen ein Recht auf nicht digitale Inanspruchnahme von Verwaltungsleistungen.

Zu Abs. 3

Abs. 3 erweitert und konkretisiert die Grundsatzregelung des Abs. 1 für Verwaltungsleistungen der Personalverwaltung und Personalwirtschaft. Nach Abs. 3 kann der Freistaat Bayern als Dienstherr bzw. Arbeitgeber Verwaltungsdienstleistungen im Bereich der Personalverwaltung und Personalwirtschaft gegenüber seinen Beschäftigten ausschließlich elektronisch anbieten und erbringen. Die Möglichkeit zur ausschließlich digitalen Verfahrensdurchführung weicht vom „Grundsatz der digitalen Verfahrenswahlfreiheit“ des Beteiligten ab. Zu den besonderen Anforderungen an die Nutzerfreundlichkeit und auf persönliche Beratung, Auskunft und Anhörung in digitalen Verfahren siehe Art. 9 und 10.

Die Regelung umfasst auch unter der Aufsicht des Freistaates Bayern stehende juristische Personen des öffentlichen Rechts. Auf diese Weise werden u. a. auch die Versorgungsanstalten erfasst. Klarzustellen ist, dass, soweit der Bayerische Versorgungsverband Verwaltungsleistungen (insbesondere Art. 44 VersoG) für das Personal seiner Mitglieder aus dem Bereich der Gemeindeverbände und Gemeinden erbringt, die Zuständigkeit zur Digitalisierungsentscheidung dieser Leistungen gem. Art. 4 Abs. 1 beim Bayerischen Versorgungsverband bleibt.

Zu Art. 21 Digitale Assistenzdienste

Art. 21 trifft Reglungen zu digitalen Assistenzdiensten. Um die flexible, zielgruppenorientierte Aufbereitung von digitalen Verwaltungsleistungen zu erleichtern, bietet es sich an, auch auf die Potentiale privater Dienstleister zurückzugreifen.

Art. 21 ermöglicht die Zulassung des Einsatzes digitaler Assistenzdienste von privaten Anbietern, um einen nutzerfreundlichen Zugang insbesondere zu komplexen Verwaltungsdienstleistungen zu erleichtern. Die entwicklungsoffene Regelung des Art. 21 zielt insbesondere darauf, bei komplexen Verwaltungsverfahren den Einsatz von privaten Dienstleistern zur Erleichterung der Antragstellung und der Verfahrensbeteiligung der Beteiligten zu ermöglichen.

Der Einsatz privater Dienstleister bei der Bereitstellung von Verwaltungsangeboten hat eine lange Tradition. In der analogen Welt greifen insbesondere kommunale Behörden bei ihrem behördlichen Formularangebot verbreitet auf private Formularverlage zurück, die auf Basis der amtlichen Anforderungen Formularmuster erstellen und nach amtlicher Freigabe drucken und bereitstellen. Diese klassische analoge Form der „Public-Private-Partnership“ bei der behördlichen Formularerstellung hat in der digitalen Welt eine Fortsetzung und Fortentwicklung im Bereich der Steuerverwaltung erfahren. Die Steuererklärung (vgl. § 149 ff AO) kann in digitaler Form in Form des ELSTER-Verfahrens digital bei den Finanzämtern eingereicht werden. Zusätzlich können aber auch private Anbieter Software-Lösungen zur Erleichterung der Steuererklärung anbieten.

Der in der Steuer erprobte und bewährte Einsatz von „digitalen Assistenten“ soll (analog der „Steuersoftware“ privater Anbieter) in Bayern grundsätzlich auch außerhalb der Steuerverwaltung für alle Verwaltungsverfahren freigegeben werden, deren Vollzug Behörden im Sinne des Art. 1 Abs. 2 obliegt. Die Anforderungen an den Einsatz digitaler Assistenzdienste werden in Art. 21 und im Verordnungswege näher bestimmt.

Die möglichen Anwendungsfälle der Rechtsvorschrift können und sollten - gerade wegen der entwicklungsoffenen Konzeption der Norm - nicht dezidiert festgeschrieben werden. Denkbare Fälle sind aber komplexere Masseverfahren, z.B. im Rahmen des Bau- und Anlagengenehmigungsrechts, im Bereich von Förderverfahren, oder ggfs. auch im Bereich des Sozialrechts, soweit dieses im Zuständigkeitsbereich des Landesgesetzgebers liegt.

Ebenso orientiert sich die Einbindung gewerblicher Anbieter am Verfahren ELSTER der Steuerverwaltung. Die elektronische Steuererklärung (vgl. §§ 149 ff. AO) kann sowohl direkt über ein Online-Verfahren der Finanzverwaltung als auch über Steuerprogramme kommerzieller Anbieter eingereicht werden.

Zur Sicherstellung formell korrekter Steuererklärungen, die maschinell verarbeitet werden können, stellt die Steuerverwaltung amtliche Schnittstellen zur Verfügung, über die kommerzielle Anbieter von Steuersoftware die Datensätze der Steuererklärung rechtlich verbindlich digital an die Steuerverwaltung übermitteln können.

Zu Art. 22 Zustimmung im digitalen Verfahren:

Art. 22 legt den Grundsatz der Zustimmungspflichtigkeit der Durchführung von digitalen Verwaltungsverfahren fest. Die Vorschrift wird durch die spezielleren Normen insb. der Art. 23 ff, 30 ff konkretisiert.

Zu Abs. 1

Abs. 1 legt grundsätzlich die Zustimmung als Voraussetzung für die Durchführung eines Verwaltungsverfahrens fest, soweit gesetzlich nichts anderes bestimmt ist. Die Norm legt zudem fest, dass die Zustimmung auch für alle Verwaltungsverfahren erteilt

werden kann, insbesondere wenn diese über ein Nutzerkonto erteilt wird und regelt die Reichweite der Zustimmung bei Weitergabe von Daten aus dem Nutzerkonto.

Zu Abs. 2

Abs. 2 regelt die Zustimmung über das Nutzerkonto als Regelfall. Nach Satz 2 ist die Zustimmung aus Gründen der Nachweisbarkeit und der Klarheit zu dokumentieren. Die Zustimmung kann mit Wirkung für zukünftige Anträge widerrufen werden. Abs. 2 schließt die Zustimmung im Fachverfahren nicht aus.

Zu Art. 23 Digitale Nachweise, Direktabruf von Belegen:

Zu Abs. 1

Abs. 1 regelt die Einreichung benötigter Nachweise und Unterlagen. Ziel der Vorschrift ist eine medienbruchfreie, durchgehende digitale Verfahrensabwicklung. So können Unterlagen auch digital eingereicht werden, soweit durch Rechtsvorschrift nichts anderes bestimmt ist. Sollte eine Behörde in bestimmten Verfahren die rein digitale Übermittlung von Nachweisen und Unterlagen für nicht ausreichend erachten, z. B. weil die eingereichten Dokumente regelmäßig auf Echtheit zu überprüfen sind, oder sollte im Einzelfall beispielsweise Zweifel an der Authentizität eines Dokuments bestehen, dann bleibt nach Satz 2 die Anordnung der Vorlage von Originalen oder beglaubigten Kopien möglich.

Zu Abs. 2

Abs. 2 soll das „Once-Only Prinzip“ stärken und einen Abgleich mit bereits in Registern gespeicherten Informationen ermöglichen. Mit der Vorschrift soll es ermöglicht werden, auf vorhandene Registereinträge zurückzugreifen, Aufwand für Neuerhebungen sind für die Behörden damit nicht verbunden.
Grundsätzlich muss der Bürger erforderliche Belege (z. B. Geburtsurkunden) selbst bei der ausstellenden Behörde (z. B. am Geburtsort) einholen und dann bei der einfordernden Behörde vorlegen. Künftig sollen in digitalen Verfahren nach Satz 1 die Behörden, die Belege fordern, diese bei Zustimmung des Betroffenen einholen, wenn die Informationen von der Behörde in digitaler Form aus Registern abgerufen werden können.
Die Zustimmung des Betroffenen erfolgt dabei einzelfallbezogen. Über die eventuell beim selbständigen Behördenabruf anfallenden Mehrkosten ist der Betroffene zu informieren, wobei im Regelfall nicht mit Mehrkosten zu rechnen ist. Satz 4 stellt zudem klar, dass sonstige gesetzliche Regelungen (z. B. aus dem Bundesrecht) unberührt bleiben.

Zu Art. 24 Bekanntgabe über Portale:

Zu Abs. 1

Ziel der Norm ist es, eine elektronische Bekanntgabe von Verwaltungsakten durch digitalen Datenfernabruf rechtssicher zu ermöglichen. Abs. 1 ist für den Sonderfall der

Bekanntgabe über in Verwaltungsportale integrierte Nutzerkonten lex specialis zu Art. 41 Abs. 2 BayVwVfG, der die elektronische Bekanntgabe allgemeinen regelt. Satz 1 stellt klar, dass eine digitale Bekanntgabe mit Einwilligung des Beteiligten auch durch Bereitstellung von Daten zum Abruf zulässig ist. Satz 2 sieht für den Datenabruf eine vorherige Authentifizierung vor. Bei der „Einwilligung“ im Sinne dieser Vorschrift handelt es sich nicht um eine Einwilligung im datenschutzrechtlichen Sinne.

Zu Abs. 2

Abs. 2 enthält eine Bekanntgabefiktion: Der Verwaltungsakt gilt am dritten Tag nach der Absendung der digitalen Benachrichtigung an den Abrufberechtigten als bekannt gegeben. Diese Fiktion gilt nach Satz 2 nicht, wenn die elektronische Benachrichtigung nicht oder zu einem späteren Zeitpunkt zugegangen ist. Im Zweifel hat nach Satz 3 die Behörde den Zugang der digitalen Benachrichtigung nachzuweisen. Gelingt ihr dieser Nachweis nicht, werden die Daten aber tatsächlich von einer dazu befugten Person abgerufen, gilt der Verwaltungsakt nach Satz 4 in dem Zeitpunkt als bekanntgegeben, in dem dieser Datenabruf tatsächlich durchgeführt wird.

Zu Abs. 3

Abs. 3 sieht vor, dass die Übermittlung der Benachrichtigung und der Abruf zu protokollieren sind. Dies dient der Transparenz und der Beweissicherung.

Zu Art. 25 Zustellung über Portale:

Mit Satz 1 wird die Frage der förmlichen Bekanntgabe im Wege der Zustellung durch Bereitstellung zum Datenabruf geregelt, wobei die Vorschriften aus dem VwZVG unberührt bleiben. Neben allen Anforderungen für die Bekanntgabe nach Art. 24 ist darüber hinaus erforderlich, dass der Beteiligte ausdrücklich in die Zustellung durch Bereitstellung zum Datenabruf eingewilligt hat (Satz 2). Die Einwilligung kann auch digital über das Nutzerkonto erteilt werden. Nach Satz 3 ist der Beteiligte vor der Einwilligung über die Rechtsfolgen der Zustellung zu informieren. Im Übrigen gelten die Regelungen des Art. 24. Auch hier ist die „Einwilligung“ wie in Art. 24 nicht im datenschutzrechtlichen Sinne zu verstehen.

Kapitel 3. Portalverbund Bayern

Zu Art. 26 Grundlagen

Mit dem neuen Art. 26 wird der Portalverbund Bayern geregelt. Ziel ist es einen Portalverbund zu schaffen, über den alle Verwaltungsleistungen der Behörden für alle Nutzer über einheitliche Nutzerkonten abgewickelt werden können.

Zu Abs. 1

In Abs. 1 Satz 1 wird die Errichtung des Portalverbunds Bayern und der barriere- und medienbruchfreie Zugang der Nutzer zu den elektronischen Verwaltungsleistungen der Behörden als Zweck des Portalverbunds Bayern normiert. Der Portalverbund Bayern übernimmt dabei die Funktion des Verwaltungsportals des Freistaates Bayern im Sinne von § 1 Abs. 2 OZG.Freistaates.

Der Portalverbund umfasst gem. Satz 2 das Bayernportal und das Organisationsportal für wirtschafts- und organisationsbezogene Verwaltungsleistungen.

Ein „Verwaltungsportal“ bezeichnet hierbei ein bereits gebündeltes digitales Verwaltungsangebot mit entsprechenden Angeboten einzelner Behörden; davon nicht erfasst sind verwaltungsinterne Portale. Ein Verwaltungsportal, dessen Angebote sich überwiegend an die aktiven und ehemaligen Beschäftigten von Behörden richten, ist somit kein Verwaltungsportal in diesem Sinne.

Zu Abs. 2

Mit Abs. 2 wird geregelt, welche Informationen die Behörden dem Nutzer zur Verfügung zu stellen haben. Über das BayernPortal werden von den fachlich zuständigen Ministerien aktuelle bayernweit gültige Informationen über on- und offline Verwaltungsleistungen und von den Behörden, die für den Vollzug zuständig sind, behördenspezifische Informationen, die Anschriften, Geschäftszeiten sowie postalische, telefonische und digitale Erreichbarkeitsdaten zur Verfügung gestellt. Mit Nummer 10 wird die Verordnung (EU) Nr. 2018/1724 (Single-Digital-Gateway-VO) an dieser Stelle konkretisiert. Die Behörden sind danach verpflichtet, die in Art. 4 dieser Verordnung genannten Informationen bereitzustellen.
Zusätzlich bestimmen die restlichen Nummern den weiteren Funktionsumfang des Portalverbunds Bayern und die damit verbundenen Verpflichtungen der Behörden.

Zu Art. 27 Bayernportal

Art. 27 definiert im Satz 1 das Bayernportal als allgemeines Verwaltungsportal des Freistaates Bayern. Im Satz 2 werden die Funktionen aufgezählt, die der Freistaat Bayern bereitstellt, um ein modernes Verwaltungsportal zu gewährleisten. Insbesondere wird über das Bayernportal die Identifizierung und Authentifizierung über das Bürgerkonto gem. Art. 29 Abs. 2 ermöglicht. Auch Justizleistungen können in das Bayernportal aufgenommen werden. Ein Anspruch, Justizleistungen über das Bayernportal abrufen zu können, wird dadurch allerdings nicht begründet.

Zu Art. 28 Organisationsportal Bayern:

Zu Abs. 1

Mit Beschluss vom 14.02.2020 hat der IT-Planungsrat den Freistaat Bayern und das Land Bremen beauftragt, ein auf der ELSTER Technologie basierendes einheitliches

Organisationskonto für Deutschland zu konzipieren und umzusetzen. Das Organisationskonto soll laut Beschluss des IT-Planungsrats vom 21.10.2020 zu einem „Single-Point-of-Contact“ für unternehmensbezogene Verwaltungs- unfleitungen in Deutschland weiterentwickelt werden. Aus diesen geänderten Rahmenbedingungen zieht Art. 28 Abs. 1 mit Rahmenregelungen für die Einrichtung eines Organisationsportals die notwendigen rechtlichen Konsequenzen.

Das Organisationskonto umfasst dabei im Wesentlichen:

- eine Web-Anwendung für Unternehmen, bei der die Unternehmen sämtliche für sie relevanten Verwaltungsleistungen zentralisiert vorfinden („Mein Organisationsportal“)
- einen zentralen Identifizierungsdienst für andere Verwaltungsleistungen („NEZO“/“NEZOP“)
- eine Postfachfunktion (inkl. Funktionspostfach) mit Bekanntgabemöglichkeit für Bescheide, die zudem die Infrastruktur für die Anbindung von Kommunen und Fachverfahren („Postfach 2.0“) gewährleistet.

Um den Unternehmer die Suche und das Auffinden von Verwaltungsleistungen so einfach als möglich zu gestalten und die bisherigen in Bayern bestehenden Lösungen optimal nutzbar zu machen, hat der Nutzer, d.h. das Unternehmen, zukünftig in Bayern verschiedene Möglichkeiten wie er seinen Online-Antrag erreicht und damit seine Verwaltungsleistung erfolgreich digital abwickelt:

- Alternative 1: Einstieg über das deutschlandweite ELSTER-basierte Unternehmensportal
- Alternative 2: Einstieg über das Unternehmensportal Bayern
- Alternative 3: Einstieg über das BayernPortal als „Allgemeine Verwaltungssuche“ in Bayern,
- Alternative 4: Direkter Einstieg in das Fachportal, z. B. kommunale Webseite

Über das Organisationsportal kann zudem der Zugang zu Justizleistungen eröffnet werden. Ein Anspruch, Justizleistungen über das Organisationsportal abrufen zu können, wird dadurch allerdings nicht begründet.

Zu Abs. 2

Die Norm schafft den Rechtsrahmen für die Umsetzung der Anforderungen der Single Digital Gateway Verordnung im Freistaat Bayern über das Organisationsportal. Die Norm schließt jedoch eine Anbindung bürgerbezogener Dienste im Sinne der Single Digital Gateway Verordnung auch an das Bayernportal nicht aus.

Zu Abs. 3

Abs. 3 verpflichtet die Behörden zur elektronischen Abwicklung, wenn der Nutzer Verwaltungsleistungen über das Portal beansprucht. Satz 2 sieht eine Ausnahmeregelung vor.

Zu Abs. 4

Abs. 4 ergänzt Abs. 3 und verpflichtet die Behörden die für die Abwicklung erforderlichen technischen und organisatorischen Voraussetzungen zu schaffen. Die Basiskomponenten (z. B. Organisationsportal, Organisationskonto oder E-Payment) stellt der Freistaat Bayern bereit. Gemeindeverbände und Gemeinden schließen sich dann an diese Basiskomponenten an bzw. nutzen diese. Der Freistaat und die Gemeindeverbände (bzw. die Gemeinden) tragen zusammen die Verantwortung für die der effizienten Verfahrensgestaltung dienenden technischen Einrichtungen, für die technischen Kommunikationsstandards und die Möglichkeiten zur medienbruchfreien Datenübermittlung.

Zu Art. 29 Nutzerkonto, Postfach:

Zu Abs. 1

Mit Art. 29 werden Regelungen zum Nutzerkonto und Postfach getroffen. Satz 1 stellt klar, dass der Freistaat Bayern ein Nutzerkonto Bayern als zentralen Dienst für die Behörden zur Verfügung stellt und definiert dessen Funktion angelehnt an § 2 OZG. Nach Satz 2 umfasst das Nutzerkonto auch ein Postfach. Satz 3 stellt klar, dass Nutzerkonten als Bürger- bzw. Organisationskonten angeboten werden können.

Nach der eIDAS-VO (Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über digitale Identifizierung und Vertrauensdienste für digitale Transaktionen im Binnenmarkt) steht das Nutzerkonto auch natürlichen und juristischen Personen des EU-Auslands offen.

Zu Abs. 2

Abs. 2 enthält Definitionen für das „Bürgerkonto“ und das „Organisationskonto“. Art. 14 ff. BayVwVfG finden auch hier bei Fragen rund um das Sorgerecht, bei Betreuungen und bei der Vertretung juristischer Personen Anwendung.

Zu Abs. 3

Die Identifizierung am Organisationskonto erfolgt nach Abs. 3 über das aus der Steuerverwaltung bekannte ELSTER-Verfahren, wobei nach Abs. 3 Satz 2 auch der Einsatz weiterer Identifizierungsmittel nicht ausgeschlossen ist.

Zu Abs. 4

In Abs. 4 S. 1 werden die Behörden verpflichtet, Nutzerkonten im Rahmen ihrer Online-Dienste anzubinden. Nach S. 2 werden rein verwaltungsinterne Portale von den Online-Diensten und damit von den Anbietungspflichten ausgenommen.

Zu Art. 30 Funktionsumfang des Nutzerkontos, Datenschutz:

Insgesamt soll es den Nutzern so leicht wie möglich gemacht werden, ein Nutzerkonto einzurichten (niedrige Eingangsschwelle), denn der Erfolg des Portalverbund Bayern steht und fällt mit seinen Nutzern. Umgekehrt will und muss sich der Staat auch bewusst von privaten E-Commerce Portalen unterscheiden: Daher soll der Nutzer jederzeit überprüfen können, welche Daten über ihn gespeichert sind und ob diese Daten für die konkrete Anwendung nun verwendet werden sollen oder nicht – der Anwender muss „Herr seiner Daten“ bleiben.

Abs.1

Abs. 1 Satz 1 stärkt daher die Transparenz, indem der Nutzer kontrollieren kann, welche Daten über ihn gespeichert sind. Im Nutzerkonto müssen alle gespeicherten Daten so aufgeführt werden, dass sie für den Nutzer jederzeit einsehbar sind. Der Nutzer hat zudem jederzeit die Möglichkeit, das Nutzerkonto und alle gespeicherten Daten selbständig zu löschen (Satz 2). Daten, die aus öffentlichen Authentifizierungsmitteln stammen, können durch Trennung des Authentifizierungsmittels gelöscht werden. Satz 3 gewährleistet dem Nutzer die IT-Sicherheit nach aktuellem technischem Stand.

Abs. 2

Ebenso ist ein dauerhaftes Speichern der Identitätsdaten des Nutzers möglich, aber nur, wenn dieser zustimmt. Dies macht eine erneute Abfrage der Identitätsdaten bei der Anmeldung im Nutzerkonto entbehrlich und ermöglicht eine entsprechende Personalisierung des Nutzerkontos. Für die Zustimmung enthält das Nutzerkonto einen speziellen Zustimmungsmanager. Auch soll der Anwender selbst steuern, ob und welche Daten in Formulare übernommen werden („Once-Only-Prinzip“). Aus diesem Grund sieht Satz 2 vor, dass Daten des Nutzers automatisiert übernommen werden können, aber nur wenn dieser zustimmt.

Abs. 3

Abs. 3 Satz 1 sieht zudem eine „Wallet-Funktion“ für den Nutzer vor, ein digitales Archiv für Dokumente, das nach Satz 2 vor unberechtigten Zugriffen und Veränderungen zu schützen ist. Satz 3 und 4 ermöglichen den mobilen Nachweis.

Abs. 4

Alle Datenverarbeitungsvorgänge müssen nach Abs. 4 in digital abrufbarer Form im Nutzerkonto gespeichert werden. Dieses „Datencockpit“ soll die praktische Wirksamkeit des Datenschutzes und die Nutzerfreundlichkeit zusätzlich erhöhen.

Zu Art. 31 Identifizierung am Nutzerkonto, Schriftformersatz:

Abs. 1

Art. 31 regelt die Identifizierung am Nutzerkonto. Der Identitätsnachweis kann dabei nach S. 1 durch unterschiedliche Identifizierungsmittel erfolgen. Gem. Satz 2 hat der Nutzer die Zustimmung zur Verarbeitung seiner Identitätsdaten grundsätzlich für jedes Verwaltungsverfahren gesondert zu erteilen. Im Interesse der Nutzerfreundlichkeit lässt Satz 3 auch eine generelle Zustimmung zu. Dies setzt gem. Satz 4 eine gesonderte Information über die rechtlichen Folgen voraus. Gem. Satz 5 ist die Zustimmung gesondert zu protokollieren und jederzeit widerrufbar.

Abs. 2

Abs. 2 ist lex specialis zu Art. 19 Abs. 3 und gilt für Nutzerkonten, während Art. 19 Abs. 3 auch digitale Anwendungen erfasst, die ohne Nutzerkonto verwendet werden (z.B. Beihilfeanträge).
Abs. 2 nimmt auf die Abgabenordnung Bezug und sieht vor, dass in Verwaltungsverfahren die Identifizierung des Nutzers in der Regel durch einen Identitätsnachweis nach § 18 PAuswG bzw. gleichgestellte Nachweise oder durch ein im Sinne von § 87a Abs. 6 Satz 1 der Abgabenordnung sicheres Verfahren durchgeführt wird, das den Datenübermittler authentifiziert und die Vertraulichkeit und Integrität des Datensatzes gewährleistet (ELSTER-Verfahren). Möglich ist auch ein anderes Identifizierungsmittel, das gesetzlich oder durch Rechtsverordnung der Staatsregierung zur Identifizierung am Nutzerkonto oder zum Ersatz der Schriftform zugelassen ist.
Satz 2 bestimmt, dass die Behörde in Einzelfällen auch von einer ELSTER- Identifizierung absehen kann, soweit Sicherheitsbedenken nicht entgegenstehen. Satz 3 stellt klar, dass bei Verfahren, bei denen gesetzlich ein Identitätsnachweis im Sinne von § 18 PAuswG (oder gleichgestellte Nachweise) vorgeschrieben ist, eine Identifizierung auch am Nutzerkonto ausschließlich mit diesen Verfahren erfolgen kann. Nach Satz 4 besteht in Ausnahmefällen über Satz 3 hinaus auch weiterhin die Möglichkeit, dass die Behörden ein höheres Authentifizierungsniveau vorsehen, etwa wenn sicherheitspolitische Belange betroffen sind.
Klarzustellen ist, dass die Ausländerbehörden rein bundesgesetzlich nicht allen Ausländern einen digitalen Identitätsnachweis nach § 78 Abs. 5 AufenthG „anbieten“ können, da ein elektronischer Identitätsnachweis nur in elektronischen Aufenthaltstiteln enthalten ist, wenn die Identität des Ausländers durch die Ausländerbehörde zweifelsfrei festgestellt ist.

Abs. 3

Abs. 3 sieht einen Schriftformersatz für das nach § 87a Absatz 6 Satz 1 der Abgabenordnung eingesetzte Verfahren vor (ELSTER-Verfahren). Im Interesse der unionsweiten Öffnung des digitalen Verwaltungsverfahren gilt gleiches auch für Verfahren, die

nach Maßgabe der eIDAS-VO (Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 auf dem Vertrauensniveau „hoch“ notifiziert worden sind.

Zu Art. 32 Rechtsgrundlage der Datenverarbeitung:

Art. 32 trifft Regelungen zur Datenverarbeitung im Zusammenhang mit dem Nutzerkonto.

Zu Abs. 1

Abs. 1 Satz 1 nennt die Daten, die zur Feststellung der Identität des Nutzers verarbeitet werden dürfen, wobei Abs. 1 hierbei zwischen natürlichen und juristischen Personen differenziert. Satz 2 erweitert die Datenverarbeitungsbefugnis auf Daten, die zum bestimmungsgemäßen Betrieb des Nutzerkontos (z. B. Sterbedatum zur Inaktivierung des Nutzerkontos) und zur Abwicklung von Verwaltungsverfahren über das Nutzerkonto erforderlich sind. Hier geht es insb. um Daten, die typischerweise von den Fachverfahren für eine Mehrzahl von Verwaltungsverfahren abgefragt werden.

Zu Abs. 2

Abs. 2 stellt klar, dass Daten im Sinne des Absatzes 1 auch zwischen den Nutzerkonten von Bund und Ländern ausgetauscht und auch portalübergreifend weitergegeben werden dürfen.
Die einzelnen Datenverarbeitungstatbestände werden durch Verordnung geregelt.

Zu Abs. 3

Abs. 3 Satz 1 legt fest, dass Daten im Sinne des Abs. 1 im Nutzerkonto zu speichern und zu aktualisieren sind, soweit die Daten für den Betrieb des Nutzerkontos erforderlich sind. Diese Daten können nach Satz 2 zur Abwicklung von Verwaltungsverfahren genutzt und in die hierfür bereitgestellten Verfahren und Formulare automatisiert übertragen werden.

Kapitel 4. Digitale Akten und Register

Zu Art. 33 Digitale Akten:

Art. 33 übernimmt die Vorschriften des Art. 7 BayEGovG zu elektronischen Akten und Registern mit nur geringfügigen redaktionellen Änderungen.

Gegenstand und Erfordernis der Regelung

Die digitale Aktenführung gehört bereits in vielen bayerischen Behörden zum Alltag. Bereits im BayEGovG wurde eine gesetzliche Regelung zur E-Akte aufgenommen. Im BayDiG knüpfen die Regelungen wie im BayEGovG für den staatlichen Bereich an die Bekanntmachung der Bayerischen Staatsregierung über die Rahmenvorschriften für

die digitale Aktenführung und das Übertragen und Vernichten von Papierdokumenten vom 27. Juni 2012 (FMBl S. 374, AllMBl S. 491, KWMBl S. 220, JMBl S. 66) an. Die gesetzlichen Regelungen beschränken sich auf die Normierung von Basisstandards für staatliche und nichtstaatliche Behörden. Inhaltlich ist für den staatlichen Bereich keine Änderung gegenüber der Bekanntmachung beabsichtigt. Mit der Normierung soll lediglich die bisherige Vorgehensweise der Praxis einer gesetzlichen Grundlage zugeführt werden, um potenzielle Unsicherheiten im Vollzug zu vermeiden. Die Regelungen im BayDiG legen keinen von §§ 6 und 7 EGovG abweichenden Standard fest. Insbesondere werden einheitliche Schutzziele (Integrität, Authentizität und Vertraulichkeit) verfolgt.

Im Einklang mit den bestehenden Rahmenvorschriften beschränkt sich Art. 33 auf die Regelung der wesentlichen Grundsätze der Einführung der digitalen Akte, der digitalen Aktenführung und des ersetzenden Scannens für alle Behörden im Anwendungsbereich des Gesetzes. Eine gesetzliche Regelung ist erforderlich, um nicht nur für staatliche, sondern auch für kommunale und sonstige nichtstaatliche Behörden im Freistaat Bayern einheitliche Grundsätze digitaler Aktenführung zu gewährleisten. Spezielle Vorschriften bleiben unberührt (vgl. Art. 1 Abs. 1). Die Verpflichtungen aus Art. 33 gelten ab Inkrafttreten der Norm für die Zukunft. Die Verpflichtung zur Überführung vorhandener Aktenbestände in die digitale Form besteht daher nicht.

Zu Abs. 1

Art. 33 Abs.1 Satz 1 Halbsatz 1 ist als „Soll-Vorschrift“ ausgestaltet. Im Regelfall haben staatliche Behörden (mit Ausnahme der staatlichen Landratsämter, die ebenfalls Halbsatz 2 unterfallen) ihre Akten und Register digital zu führen. Die Ausnahme für die Landratsämter folgt aus deren Charakter als Doppelbehörde. Da eine Einführung der digitalen Akte nur für das staatliche Landratsamt nicht praxistauglich erscheint, muss das Landratsamt als Doppelbehörde konsequenterweise von der Verpflichtung ausgenommen werden. Aus wichtigem Grund oder in atypischen Fällen kann die Behörde jedoch nach insoweit eröffnetem Ermessen von der digitalen Akten- und Registerführung abweichen. Das Gebot des Satz 1 kann sowohl durch vollständige als auch durch teilweise digitale Akten- oder Registerführung erfüllt werden. Die Soll-Vorschrift des Satz 1 belässt den zuständigen Behörden hinreichend Spielraum, in begründeten Fällen von der Einführung der digitalen Akte abzusehen. Im staatlichen Bereich können die zuständigen obersten Landesbehörden für ihren Bereich und für ihnen nachgeordnete staatliche Behörden Ausnahmen zulassen. Der Ministerratsbeschluss vom 07.01.2013 zur Einführung der digitalen Akte ist zu beachten.

Art. 33 Abs.1 Satz 1 Halbsatz 2 stellt für Behörden der Gemeinden, Gemeindeverbänden und sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts die Zulässigkeit der digitalen Akten- und Registerführung klar. Die Entscheidung über die Einführung digitalen Akten oder Register steht im nicht staatlichen Bereich jedoch ausdrücklich im Ermessen der jeweiligen Behörde, soweit gesetzlich nichts anderes vorgeschrieben ist.

Werden digitale Akten geführt und Vorgänge digital bearbeitet, ist gem. Satz 2 durch geeignete technisch-organisatorische Maßnahmen sicherzustellen, dass die Grundsätze ordnungsgemäßer Aktenführung als Ausformung des Rechtsstaatsprinzips eingehalten werden. Vertraulichkeit, Verfügbarkeit und Integrität der digitalen Akten müssen gewährleistet sein. Das eingesetzte Dokumentenmanagementsystem/Vorgangsbearbeitungssystem (DMS/VBS) muss diese Anforderungen erfüllen. Die rechtstaatlichen Grundsätze der Vollständigkeit, der Nachvollziehbarkeit, der wahrheitsgemäßen Aktenführung und der Verständlichkeit des Verwaltungshandelns sind zu beachten (vgl. § 18 Abs. 1 AGO).

Auch wenn digitale Formate nicht dem Urkundenbeweis zugänglich sind, werden originär digital hergestellte Dokumente einer Behörde gem. § 371a Abs. 3 S. 1 ZPO beweisrechtlich den öffentlichen Urkunden gleichgestellt. Sind sie darüber hinaus mit einer qualifizierten digitalen Signatur (qeS) versehen oder werden Sie mit einer absenderbestätigten De-Mail versendet, gilt zudem gem. § 371a Abs. 3 S. 2, 3 ZPO in Verbindung mit § 437 ZPO die Vermutung der Echtheit des Dokuments, so dass im Rechtsverkehr keine Beweisnachteile zu befürchten sind.

Zu Abs. 2

Abs. 2 enthält ein Gebot des digitalen Austauschs von Akten, Vorgängen und Dokumenten zwischen Behörden, die digitale Akten führen, um Medienbruch bei Schriftgutaustausch zu vermeiden. Hierbei sind die einschlägigen datenschutzrechtlichen Vorschriften zu beachten. Die Daten sind daher vor unbefugter Einsichtnahme Dritter und vor Veränderungen zu schützen, bspw. durch die Nutzung einer sicheren Kommunikationsinfrastruktur oder Übermittlung in einer auf dem Stand der Technik sicheren Form.

Zu Abs. 3

Zu Satz 1 und Satz 3

Auch wenn das BayDiG Bürgern und Behörden den Weg für eine digitale Kommunikation bereitet, werden auch nach der Einführung einer digitalen Akte weiterhin Papierunterlagen anfallen. Diese Unterlagen sollen unter Wahrung der Grundsätze ordnungsgemäßer Aktenführung und -aufbewahrung in ein digitales Format übertragen werden, um sie in digital gestützte Arbeitsabläufe einzubeziehen. Hierbei ist nach dem Stand der Technik sicherzustellen, dass die digitale Fassung mit dem Papierdokument übereinstimmt. Auf die Forderung nach einer bildlichen Übereinstimmung wurde bewusst verzichtet, um deutlich zu machen, dass Abweichungen in Größe und Farbe unschädlich sind, wenn diesen Informationen kein aktenrelevanter Aussagegehalt/Sachverhalt zu entnehmen ist.

Dem Stand der Technik genügen dabei insbesondere die in der TR-RESISCAN enthaltenen Hinweise zur technisch-organisatorischen Gestaltung des Scan-Prozesses. Grundsätzlich gilt, dass die getroffenen Maßnahmen der rechtsstaatlich gebotenen Dokumentationsfunktion der digitalen Akte gerecht werden müssen. Hilfreich kann

hierbei eine Orientierung an der (ihrerseits Grenzen ausgesetzten) Vorgehensweise der papiergebundenen Aktenführung sein, die sich zwar hinsichtlich ihres Mediums, nicht aber hinsichtlich ihrer Dokumentationsfunktion von der digitalen Akte unterscheidet. Aus diesem Grund ist nicht jede technisch und organisatorisch denkbare Maßnahme zum Schutz der Authentizität und Integrität der digitalen Akte rechtstaatlich grundsätzlich geboten. Dies kommt auch in den abgestuften Anforderungen der TR-RESISCAN zum Ausdruck. So fordert die Richtlinie bei einem normalen Schutzbedarf der eingescannten Dokumente weder eine vollständige Sichtprüfung noch die Verwendung einer digitalen Signatur.

Auf das Einscannen kann verzichtet werden, wenn der Scanvorgang technisch nicht möglich, zu aufwendig oder unwirtschaftlich ist. Soweit derartige Papierdokumente wegen ihrer Vorgangsrelevanz im Sinn des § 18 Abs. 1 AGO aufzubewahren sind, müssen sie zwangsläufig zu einem begleitenden Papier-Vorgang genommen werden (= sog. „hybride Aktenführung“). Zur Nachvollziehbarkeit der Beziehung zwischen Papierrestakte und vollständiger eAkte werden beiderseitig Verweise angelegt. Auf diese Weise wird auch bei nicht scanbaren Unterlagen die Aktenvollständigkeit gewährleistet.

Die digitale Kopie des Originals ist im Rahmen eines Beweisrechts nicht dem Urkundenbeweis, sondern grundsätzlich lediglich dem Augenscheinsbeweis zugänglich, da das Wesensmerkmal der Verkörperung auf einem unmittelbar, ohne technische Hilfsmittel lesbaren Schriftträger fehlt (§ 371 Abs.1 Satz 2 ZPO). Anders als bei nicht originär digital erzeugten Dokumenten (vgl. Ausführungen zu Abs. 1) sind auch die Beweisregeln des § 371a ZPO nicht einschlägig. Bei der Übertragung öffentlicher Urkunden durch eine Behörde findet allerdings § 371b ZPO Anwendung. Führt die Behörde bei der Übertragung öffentlicher Urkunden einen Übereinstimmungsnachweis, begründet der Scan damit grundsätzlich vollen Beweis für die beurkundete Erklärung (§ 415 ZPO analog). Sind Dokument und Nachweis darüber hinaus mit einer qualifizierten digitalen Signatur versehen, wird zudem gem. § 371b Satz 2 ZPO die Echtheit des digitalen Dokuments vermutet. Andernfalls muss das Gericht im Streitfall im Rahmen der freien Beweiswürdigung über den Einwand der nicht ordnungsgemäßen Übertragung entscheiden. Bei Einhaltung der Vorgaben der TR-RESISCAN wird die Beweiswürdigung in aller Regel nicht zu Lasten der Behörde ausfallen. Dasselbe trifft für den Fall zu, dass organisatorische Vorgaben („Scananweisung“) der Behörden für den Scanprozess bestehen und marktgängige DMS/VBS-Systeme zum Einsatz kommen. Der verwaltungsgerichtlichen Praxis der vergangenen Jahre ist, soweit ersichtlich, auch kein Fall zu entnehmen, in dem es auf diese Fragen entscheidungserheblich angekommen wäre.

Zu Satz 2

Erfolgt die Aktenführung digital, ist die weitere Aufbewahrung der Originale nach ordnungsgemäßer Übertragung in ein digitales Format und Speicherung in der digitalen

Akte im Hinblick auf die Grundsätze ordnungsgemäßer Aktenführung nicht mehr erforderlich. Sie können daher – vorbehaltlich besonderer gesetzlicher Aufbewahrungspflichten oder entgegenstehender Rechte Dritter – zurückgesendet oder vernichtet werden. Aus wirtschaftlichen wie organisatorischen Gründen wird dies in der Regel auch angebracht sein.

Vor einer etwaigen Vernichtung ist – analog zur papiergebundenen Aktenführung – sicherzustellen, dass keine Eigentums- oder Beweisführungsreche Dritter berührt werden. Dies ist in der Regel bei öffentlichen Urkunden (Ausweise, Pässe, Statusbescheinigungen, Zeugnisse, etc.) der Fall, die daher zurückgegeben werden müssen. Im Übrigen kann grundsätzlich davon ausgegangen werden, dass der Absender eines Schreibens das Schriftstück der Behörde nach § 929 BGB übereignet, es sei denn, diese sind ausdrücklich oder nach den Umständen erkennbar nur für die Dauer der Bearbeitung zur Verwahrung übergeben worden. Dies ist typischerweise bei Unterlagen von persönlich-privater Bedeutung sowie im Rechtsverkehr häufig genutzten Privaturkunden der Fall (Testament, Verträge). In der Regel enthalten Behördenakten allerdings Dokumente, in denen der übermittelte Sachverhalt und nicht der Urkundencharakter im Vordergrund steht. Die Beweisbestimmung wird daher bei der Übermittlung von privaten Schreiben häufig fehlen, da diese – im Gegensatz zu öffentlichen Urkunden – nach § 416 ZPO keinen Beweis für die Richtigkeit der in ihnen enthaltenen Erklärungen geben und damit hinsichtlich des entscheidungserheblichen Sachverhalts typischerweise keine Beweiseignung besitzen.

Zweckmäßig kann es sein, die zum Nachweis des Beginns eines Fristlaufs erforderlichen Dokumente (Zustellurkunden, Empfangsbestätigungen) bis zum rechtskräftigen Abschluss des Verfahrens von der Vernichtung auszunehmen. Bei mehrseitigen Verwaltungsrechtsverhältnissen kann dies schon wegen des Beweisführungsrechts Dritter erforderlich sein.

Trotz Beachtung dieser Vorgaben mit der Vernichtung einhergehende potenzielle Beweisnachteile zu Lasten der Verwaltung können angesichts der prozessualen Beweisregeln und dargelegten verwaltungsgerichtlichen Praxis in Kauf genommen werden. Eine Beeinträchtigung des Justizgewähranspruchs aus Art. 19 Abs. 4 GG ist bei Rücksendung entsprechender Urkunden ebenfalls nicht zu befürchten.

Zu Abs. 4

Durch Absatz 4 soll erreicht werden, die Barrierefreiheit auch im Innenverhältnis zu den Beschäftigten zu fördern.

Zu Art. 34 Einsicht in die digitale Akte:

Im Art. 34 wird das Recht auf digitale Akteneinsicht näher geregelt, wobei die Vorschrift kein Recht auf Akteneinsicht gewährt, sondern dieses bereits voraussetzt. Geregelt

wird daher nur die Art und Weise der Akteneinsicht. Art. 29 Abs. 3 BayVwVfG wird durch den vorliegenden Artikel ergänzt.

Die bereits bestehenden Regelungen zur Akteneinsicht im Verwaltungsverfahren (u. a. Art. 29 BayVwVfG, § 25 SGB X, § 9 AGO) gelten auch im Rahmen der digitalen Aktenführung. In Art. 34 wird angelehnt an § 8 EGovG des Bundes nunmehr im Interesse der Rechtsicherheit auch eine ausdrückliche Regelung zu Art und Weise der Einsicht in die digitale Akte getroffen.

Art. 34 S.1 stellt die Nutzerfreundlichkeit als Zweck der Norm heraus.

Art. 34 S. 2 normiert vier Möglichkeiten der digitalen Akteneinsicht: die Zurverfügungstellung eines Aktenausdrucks, die Wiedergabe auf einem Bildschirm, die Übermittlung digitaler Dokumente oder die Zugriffsgestattung auf den Inhalt der Akten.

Dabei sind die allgemeinen Voraussetzungen und Anforderungen an die Gewährung von Akteneinsicht zu beachten. Dies gilt insbesondere für die Berücksichtigung von Sicherheits- und Geheimhaltungsinteressen (z. B. Art. 29 Abs. 1 Satz 2, Abs. 2 und 3 BayVwVfG, § 9 Abs. 2 und 3 AGO), die auch bei einer digitalen Aktenführung sicherzustellen sind; ggfs. müssen daher geheimhaltungsbedürftige Informationen von der Einsichtnahme ausgenommen werden (Entfernung/Schwärzung/Zugriffsbeschränkung).

Das bei der Gewährung von Einsicht in die digitale Akte bestehende „technische“ Auswahlermessen muss sich maßgeblich am Zweck der Informationsgewährung orientieren. Dabei sind die Belange der Beteiligten besonders zu berücksichtigen. Wirtschaftlichkeits- und Zweckmäßigkeitsüberlegungen sind grundsätzlich nachrangig. Insbesondere ist bei der Art der Akteneinsichtsgewährung auch auf die technischen Möglichkeiten und Fähigkeiten der Verfahrensbeteiligten Rücksicht zu nehmen (Multiverfahrensmanagement). Dabei muss die Behörde u. a. darauf achten, auch weniger technikaffine Bevölkerungsgruppen nicht auszuschließen. In diesem Fall können z. B. Papierausdrucke gefertigt werden. Auch kann die Behörde dem Begehrenden die digitale Einsicht über den Bildschirm in den Behördenräumen (z. B. mittels digitalen Zugriffes auf das DMS/VBS) ermöglichen.

Daneben ist z. B. auch die Zurverfügungstellung des Inhalts der digitalen Akte mittels Datenträger oder über E-Mail-Versand zulässig. Bei der digitalen Übermittlung ist den Erfordernissen des Datenschutzes Rechnung zu tragen, insbesondere ist zu gewährleisten, dass die Integrität und Authentizität der Daten sichergestellt und deren Inhalte nicht unbefugt zur Kenntnis genommen und nicht missbräuchlich verwendet werden können. Die Daten sind daher grundsätzlich veränderungssicher (zumindest Schreibschutz) und bei E-Mail-Übertragung verschlüsselt zu übermitteln.

Der digitale Zugriff auf den Akteninhalt kann im Einzelfall gestattet werden, soweit Belange des Datenschutzes, der Datensicherheit, berechtigte Interessen Dritter oder sonstige öffentliche Belange nicht entgegenstehen.

Zu Art. 35 Digitale Register

Art. 35 normiert eine Verpflichtung für staatliche Behörden, ihre Akten und Register digital zu führen, für Landratsämter und sonstige Behörden wird lediglich die Zulässigkeit der digitalen Registerführung klargestellt. Art. 35 Satz 1 findet keine Anwendung auf Register, zu deren Führung staatliche Behörden nicht verpflichtet sind. Das Koordinierungsprojekt Registermodernisierung sieht einen dreiphasigen Zeitplan vor. Bis Ende 2021 werden Erprobungen und Umsetzungsvorbereitungen („Proof of Concept“) stattfinden und ein Steuerungsprojekt Registermodernisierung eingerichtet werden. Die technische Architektur soll zusammen mit den rechtlichen Grundlagen und der Governance weitestgehend bis Ende 2023 umgesetzt werden. Der Anschluss der im Rahmen von „Once-Only“ als am relevantesten eingestuften 19 „Top-Register“ und die Aufnahme des laufenden Betriebs soll bis Ende 2025 realisiert werden. Das technische System zur Umsetzung von „Once-Only“ in Deutschland soll etabliert, der Anschluss an die zentrale Infrastruktur flächendeckend (bzw. wo sinnvoll) sichergestellt sein.

Kapitel 5. Behördenzusammenarbeit, Rechenzentren

Zu Art. 36 Behördliche Zusammenarbeit:

Art. 36 übernimmt die bisherige allgemeinen Regelung des Art. 8 Abs. 1 und Abs. 4 BayEGovG zur behördlichen Zusammenarbeit. Basisdienste und zentrale Dienste (bisher Art. 8 Abs. 2 und Abs. 3) werden nunmehr im Art. 37 gesondert geregelt.

Art. 36 regelt die Verantwortlichkeiten und die Zusammenarbeit der Behörden im Bereich der digitalen Verwaltung im Bereich des E-Government. Die Regelungen sollen die Behördenzusammenarbeit, insbesondere die Zusammenarbeit von Freistaat und Kommunen erleichtern und diese auf eine rechtssichere Grundlage stellen. Die Regelung erfasst alle Behörden im Sinne des Art. 1 Abs. 1 des Gesetzes, einschließlich gemeinsamer Einrichtungen von Behörden. Bestehende gesetzliche Aufgaben und Zuständigkeiten werden durch die Regelung nicht geändert.

Satz 1 normiert Aufgabenzuweisungen und die Grundsätze der Behördenzusammenarbeit im Bereich der digitalen Verwaltung. Der Freistaat kann einerseits behördenübergreifende Dienste für Fachbehörden (als datenschutzrechtlich verantwortliche Stellen) bereitstellen („Basisdienste“), andererseits aber auch selbst (über eine staatlich bestimmte datenschutzrechtlich verantwortliche zentrale Stelle) Dienste für die behördenübergreifenden Nutzung anbieten („zentrale Dienste“). Durch die Eröffnung dieser Alternativen sollen flexible Rahmenbedingungen für die datenschutzkonforme Gestaltung der fortschreitenden technischen Zentralisierung der digitalen Verwaltung geschaffen werden.

Zu Satz 1

Mit Satz 1 stellt der Gesetzgeber klar, dass die Bereitstellung und Unterhaltung der zur Erfüllung ihrer jeweiligen öffentlichen Aufgaben erforderlichen digitalen Verwaltungsinfrastrukturen zu den öffentlichen Aufgaben der Behörden im Freistaat Bayern zählt.

Die Regelung trägt dem Umstand Rechnung, dass der Einsatz von digitalen Verwaltungsinfrastrukturen den Binnenbereich der Verwaltung ebenso berührt wie die Verfahrensrechte der Beteiligten, insbesondere (aber nicht nur) den Schutz und die Sicherheit personenbezogener Daten. Mit der digitalen Abwicklung der Verwaltungskommunikation im Rahmen des E-Government und dem regelmäßigen Anschluss an öffentliche Netze entstehen notwendig neue Risiken in Bezug auf die Sicherheit der digital erfassten Daten. Bestimmte Informations- und Kommunikationstechnologien, wie z. B. E-Aktenprogramme, steuern zudem auch das Verwaltungsverfahren selbst. Diesen Umständen trägt der Gesetzgeber dadurch Rechnung, dass er das E-Government als Aufgabe des Freistaates und der Kommunen definiert.

Der Begriff der digitalen Verwaltungsinfrastrukturen im Sinn des Art. 36 Abs. 1 bezieht sich auf den Einsatz von Informations- und Kommunikationstechnologien zur Erfüllung öffentlicher Verwaltungsaufgaben. Der Begriff orientiert sich am Zweck der Norm. Unter „digitalen Verwaltungsinfrastrukturen“ sind technische Einrichtungen (Hard- oder Software) zu verstehen, die von Behörden zur öffentlichen Aufgabenerfüllung genutzt werden. Hierzu zählen z. B. Hard- und Software-Lösungen der Verwaltung wie z. B. das „digitale Meldeverfahren“ oder das „Bürgerkonto“, Verwaltungsnetze wie das Bayerische Behördennetz, Rechenzentren, aber auch Gateways, Portale wie z. B. das Verwaltungsserviceportal Bayern, Konten, Postfächer, E-Payment-Plattformen, Geodatendienste wie die Geodateninfrastruktur Bayern und sonstige softwarebasierte „Basiskomponenten“ oder „Basisdienste“.

Zu Satz 2

Satz 2 konkretisiert die dem Freistaat und den Kommunen bei der Aufgabenerfüllung im Bereich der Informations- und Kommunikationstechnologie obliegende Verantwortung und hebt die Gewährleistung von Datensicherheit und die Förderung von der „gegenseitigen technischen Abstimmung“ (im Sinne von „Interoperabilität“) sowie der Barrierefreiheit besonders hervor.

Zu Satz 3

Satz 3 normiert für das Verhältnis der Behörden zueinander im Bereich der IT das Kooperationsprinzip. Satz 3 legt hierzu fest, dass die Behörden bei Entwicklung, Einrichtung und Betrieb von digitalen Verwaltungsinfrastrukturen zusammenwirken und sich diese Infrastrukturen gegenseitig zum Zweck der Aufgabenerfüllung überlassen können. Die datenschutzrechtlichen Bestimmungen, insbesondere die Vorgaben für eine Auftragsverarbeitung bleiben unberührt.

Zu Art. 37 Basisdienste und zentrale Dienste

Art. 37 knüpft an die bisherigen Regelungen des Art. 8 Abs. 2 und Abs. 3 BayEGovG an.

Zu Abs. 1

Abs. 1 entspricht weitgehend Art. 8 Abs. 2 BayEGovG. Mit der Norm schafft der Freistaat Bayern die Rechtsgrundlage, um digitale Verwaltungsinfrastrukturen als Basisdienste für staatliche und nichtstaatliche Behörden (insbesondere Kommunen) bereitzustellen. „Basisdienste“ sind ein Fall der Auftragsverarbeitung im Sinne des Art. 37 und sind als digitale Verwaltungsinfrastrukturen zu verstehen, die vom Freistaat zur behördenübergreifenden Nutzung bereitgestellt werden. Der Begriff der Basisdienste ist weit zu verstehen. Er umfasst sämtliche digitale Verwaltungsinfrastrukturen im Sinn des Art. 36 S. 1 („Hardware“ und „Software“), soweit diese von der zuständigen staatlichen Behörde für die behördenübergreifende Nutzung bereitgestellt werden. Hierzu können insbesondere auch alle automatisierten Verfahren zählen, die für eine Mehrzahl von Behörden zur Verfügung stehen können (z. B. Verwaltungs-PKI, Formularserver, Bayern-Mail etc.), aber ggfs. auch die für Staat und Kommunen angebotenen Basisdienste des Bayernportals (Bürgerkonto, Postkorb, E-Payment, je nach Ausgestaltung). Weitergehende Anforderungen an einzelne Dienste, z. B. aus § 21 in Verbindung mit § 2 Abs. 3 PAuswG bleiben unberührt, ebenso datenschutzrechtliche Anforderungen beispielsweise aus Art. 26 und Art. 28 Abs. 3 DSGVO. Basisdienste bilden den Regelfall, möchte die Behörde den „zentralen Dienst“ nach Abs. 2 nutzen, so bedarf dies einer gesonderter Begründung der bereitstellenden Behörde.

Zu Abs. 2

Abs. 2 übernimmt die bisherigen Regelungen des Art. 8 Abs. 3 BayEGovG.

Abs. 2 bestimmt, dass Behörden ihre Verpflichtungen auch durch den Anschluss an „zentrale Dienste“ erfüllen können. Zentrale Dienste sind digitale Verwaltungsinfrastrukturen, bei denen jedoch in Abgrenzung zu Abs. 1 die datenschutzrechtliche Verantwortung bei der bereitstellenden Stelle des Freistaates liegt.

Zu Satz 1

Mit der Regelung wird dem StMD und dem StMFH die Möglichkeit eröffnet, auch unmittelbar selbst und in eigener (datenschutzrechtlicher) Verantwortung behördenübergreifende zentrale Dienste anzubieten, um z. B. die digitale Identifizierung (z. B. Nutzung der eID Funktion des nPA im Rahmen eines Bürgerkontos) zu ermöglichen. Der Freistaat Bayern kann den Behörden digitale Verwaltungsinfrastrukturen als zentrale Dienste des Staatsministeriums für Digitales oder des Staatsministeriums der Finanzen und für Heimat bereitstellen. Damit ist das jeweilige Staatsministerium zugleich datenschutzrechtlich verantwortliche speichernde Stelle im Sinne des Datenschutzrechts. Die Verantwortung der angeschlossenen Behörden für ihre Fachverfahren bleibt unberührt.

Zu Satz 2

Nach Satz 2 liegt die datenschutzrechtliche Verantwortung beim bereitstellenden Staatsministerium.

Zu Satz 3

Satz 3 stellt klar, dass mit Zustimmung des Nutzers dessen personenbezogene Daten auch an die Behörden übermittelt werden können, deren Verfahren an die zentralen Infrastrukturen angeschlossen sind.

Zu Satz 4

Satz 4 normiert den datenschutzrechtlichen Grundsatz der Zweckbindung für Dienste im Sinne des Satz 1.

Zu Abs. 3

Abs. 3 Satz 1 enthält die Vermutung, dass behördenübergreifende Dienste in der Regel als Basisdienste bereitgestellt werden. Die datenschutzrechtliche Verantwortung liegt damit bei der nutzenden Stelle. Die von der Regelvermutung abweichenden Bereitstellung als zentrale Dienste ist gem. Satz 2 ausdrücklich festzustellen.

Zu Abs. 4

Abs. 4 Satz 1 erhält eine bedingte Verpflichtung des Freistaat Bayern, staatlichen und kommunalen Behörden behördenübergreifende Dienste zur Aufgabenerfüllung zur Verfügung zu stellen, soweit dies wirtschaftlich und zweckmäßig ist. Satz 2 stellt korrespondierend klar, dass die Behörden ihre Verpflichtungen aus dem Digitalgesetz auch durch den Anschluss an Dienste im Sinne der Abs. 1 und 2 erfüllen können.

Zu Abs. 5

Abs. 5 normiert, das Basisdienste und zentralen Dienste vom Bayerische Staatsministerium für Digitales im Einvernehmen mit dem Staatsministerium der Finanzen und für Heimat bereitgestellt werden.

Zu Art. 38 Auftragsverarbeitung durch staatliche Stellen

Ziel der Rechtsvorschrift ist es, die Anforderungen des Art. 28 DSGVO oder § 62 BDSG (i.V.m. Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG bzw. i.V.m. § 500 StPO ggfs. i.V.m. § 46 OWiG für den Bereich der JI-RL) in der öffentlichen Verwaltung mit möglichst geringem bürokratischem Aufwand zu erfüllen. Mit der Rechtsvorschrift wird klargestellt, dass die datenschutzrechtliche Auftragsverarbeitung durch staatliche Stellen mit öffentlichen Stellen grundsätzlich auf vertraglicher Basis (Angebot und Annahme) erfolgt. Zudem werden durch diese Regelung allgemeine Nutzungsbedingungen zur Verarbeitung personenbezogener Daten im Auftrag in den Vertrag einbezogen. Verarbeitet eine staatliche Stelle personenbezogene Daten im Auftrag einer öffentlichen Stelle, so wird durch Mitteilung gesetzlich festgelegter Informationen ein Vertrag über die Auftragsverarbeitung begründet. Dabei werden allgemeine Nutzungsbedingungen regelmäßig Bestandteil des Vertrags und regeln das datenschutzrechtliche Verhältnis zwischen staatlichen und öffentlichen Stellen. Der Auftragsverarbeiter muss eine staatliche Stelle sein. Staatliche Stellen sind solche, die dem Freistaat Bayern unmittelbar

zugeordnet sind. Öffentliche Stellen können sowohl dem Land, einer kommunalen Gebietskörperschaft oder dem Bund zugehören. Auch andere öffentlich-rechtliche Träger wie Anstalten des öffentlichen Rechts oder kommunale Zweckverbände werden hierunter gefasst. Des Weiteren werden als Ausfluss der in Art. 5 Abs. 2 DSGVO enthaltenen Rechenschaftspflicht transparente Regelungen hinsichtlich des Zustandekommens neuer und des Schicksals bereits bestehender Auftragsverarbeitungen getroffen. Jedenfalls die in diesem Artikel verwendeten Begriffe sind im Sinne der DSGVO zu verstehen. Der Begriff Textform ist im Sinne des § 126a BGB zu verstehen. Die Möglichkeit der Aufrechterhaltung bzw. des Abschlusses einzelvertraglicher Vereinbarungen bleibt gemäß Abs. 2 Satz 1 und 2 unberührt. Ebenso bleiben bestehende vertragliche Vereinbarungen der Gerichte von Art. 38 unberührt.

Zu Abs. 1

Nach Absatz 1 wird die datenschutzrechtliche Auftragsverarbeitung durch staatliche Stellen auf Grundlage eines Vertrages im Sinne des Art. 28 Abs. 3 Satz 1 Alt. 1 DSGVO oder § 62 Abs. 5 Satz 1 Alt. 1 BDSG begründet. Der breite Anwendungsbereich der Norm ermöglicht es auch, vor allem in den Bereich von Justiz und Inneres fallende Sachverhalte zu regeln, für die Art. 22 der Richtlinie (EU) 2016/680 einschlägig ist. Die Norm findet keine Anwendung, soweit die Auftragsverarbeitung anderweitig gesetzlich geregelt ist. Beispielhaft sei hierfür § 3a der Steuer-Zuständigkeitsverordnung genannt, der als lex specialis die Auftragsverarbeitung für Bereiche der Finanzverwaltung regelt.
Ebenso bleibt aber beispielhaft Art. 85a BayEUG für den Schulbereich unberührt. Die Vorschrift lässt daneben aber auch andere fachrechtliche Voraussetzungen insbesondere hinsichtlich Zulässigkeit, Begründung oder Durchführung von Auftragsverarbeitungsverträgen unberührt. Beispielsweise entbindet die Regelung nicht von der im Bereich des Sozialdatenschutzes gem. § 80 Abs. 1 SGB X bestehenden Anzeigepflicht gegenüber den Rechts- und Fachaufsichtsbehörden.
Satz 2 regelt, welche Informationen dem Auftragsverarbeiter in Textform vom Verantwortlichen mitzuteilen sind, um ein Auftragsverhältnis rechtssicher zu begründen. Für den Vertragsschluss gelten im Übrigen die allgemeinen Regeln über das Zustandekommen von Verträgen.

Zu Abs. 2

Nach Satz 1 werden bestehende Verträge über Auftragsverarbeitungsverhältnisse, an denen staatliche Stellen beteiligt sind, zu dem beim Inkrafttreten der Norm bestimmten Zeitpunkt ungültig, es sei denn, es erfolgt eine ausdrückliche und rechtzeitige Bestätigung dieser durch den Verantwortlichen und den Auftragsverarbeiter.
Der konkrete Inhalt des Vertrags wird nach Satz 2 regelmäßig durch allgemeine Nutzungsbedingungen zur datenschutzrechtlichen Auftragsverarbeitung (ANB-AVV) mitbestimmt. Demnach werden die ANB-AVV der Staatsregierung in der jeweils geltenden Fassung grundsätzlich Bestandteil des Vertrags, der nach Absatz 1 zustande

kommt. Allerdings haben Auftragsverarbeiter und Verantwortlicher stets die Möglichkeit, von den ANB-AVV abzuweichen und ihr Auftragsverarbeitungsverhältnis durch individualvertragliche Vereinbarung festzulegen. Die allgemeinen Nutzungsbedingungen zur datenschutzrechtlichen Auftragsverarbeitung werden von der Staatsregierung im Bayerischen Ministerialblatt bekannt gemacht. In der Bekanntmachung werden insbesondere die von Art. 28 Abs. 3 DSGVO oder § 62 Abs. 5 BDSG (i.V.m. Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG bzw. i. V. m § 500 StPO, ggfs. i.V.m. § 46 OwiG für den Bereich der JI-RL) aufgestellten Anforderungen näher ausgestaltet, soweit diese abstrakt-generell geregelt werden können und nicht im Einzelfall zwischen dem Verantwortlichen und dem Auftragsverarbeiter abgestimmt werden müssen.
Satz 3 stellt klar, dass in den allgemeinen Nutzungsbedingungen auch Regelungen zur Begründung von weiteren (Unter-)auftragsverarbeitungsverhältnissen i. S. v. Art. 28 Abs. 4 S. 1 DSGVO oder § 62 Abs. 4 BDSG (i. V. m. Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG bzw. i. V. m. § 500 StPO ggf. i. V. m. § 46 OWiG für den Bereich der JI-RL) getroffen werden können.

Zu Artikel 39 Bayernserver

Zu Abs. 1

Die Verwaltung muss zu jedem Zeitpunkt handlungsfähig sein. Wenn sich die Verwaltung auf digitale Prozesse stützt, müssen die genutzten Komponenten sicher, verlässlich und dem Stand der Technik entsprechend zur Verfügung gestellt werden. Die Rechenzentren sollen hierbei auch die Kommunen unterstützen.

Zu Abs. 2

Wie für das LSI ist eine gesetzliche Grundlage für die staatlichen Rechenzentren geboten und deren Aufgaben festzulegen.

Zu Abs. 3

Abs. 3 Abs. 1 regelt die Aufgaben des Bayernservers.

Absatz 3 Satz 2 zählt die Aufgaben des zentralen Rechenzentrums exemplarisch auf:

Zu Nr. 1: Das zentrale Rechenzentrum soll als Bündelungs- und Innovationsmotor der Verwaltung fungieren.
Zu Nr. 2: Die Basis für digitale Verwaltungsprozesse ist die Infrastruktur, insbesondere Verbindungsnetze und die Anschlüsse/Übergänge zum Internet. Die Verwaltung darf in ihrer Aufgabenausübung nicht von Dritten abhängig sein. Deshalb muss die Kontrolle der Basis eine staatliche Aufgabe sein. Nicht von der Infrastruktur erfasst ist das Client-Management und die LAN-Infrastruktur in den Behörden.
Zu Nr. 3: Digitale Verwaltungsprozesse, die von mehreren Verwaltungen genutzt werden können oder sollen (z. B. Datensicherung, Benutzerauthentifizierung), sollen

durch ein Kompetenzteam entwickelt und aktuell gehalten werden. Das Verfassungsgebot der Ressortunabhängigkeit ist einzuhalten.
Zu Nr. 4: Insbesondere für den Datenaustausch gemeinsamer digitaler Verfahren im Rahmen des OZG sind standardisierte Schnittstellen und Austauschprozesse zu entwickeln und vorzuhalten. Wirtschaftlich kann dies durch den Ansatz „einer für alle“ umgesetzt werden.
Zu Nr. 5: Die staatliche öffentliche Verwaltung soll die Möglichkeit erhalten, sich der Expertise des zentralen Rechenzentrums für die Entwicklung und den Betrieb in Sachen Digitalisierung zu bedienen.
Zu Nr. 6: Im Rahmen der zur Verfügung stehenden Haushaltsmittel und des zur Verfügung stehenden Personals soll für Fachverfahren die Unterstützung des zentralen Rechenzentrums herangezogen werden können. Dazu zählen insbesondere auch die Anforderungen des Schulrechenzentrums im zentralen Rechenzentrum.

Satz 3 eröffnet den Rechenzentren die Möglichkeit, unter Berücksichtigung der Wirtschaftlichkeit und Sparsamkeit Dritte/Dienstleister mit der Erfüllung bestimmter Aufgaben zu beauftragen. Die datenschutzrechtlichen Anforderungen aus Art. 28 DSGVO bleiben unberührt.

Satz 4 regelt die Aufgabenübertragung durch Dritte. Satz 5 ermöglicht den Rechenzentren im Rahmen der Umsetzung des Onlinezugangsgesetzes und von IT-Kooperationen auch den Betrieb von digitalen Verwaltungsverfahren für Behörden in anderen Bundesländern zu übernehmen, etwa nach dem Prinzip „Einer für Alle/Viele“ (EfA).

Zu Artikel 40 Staatlich verfügbare Netze

Zu Abs. 1

Die staatlich verfügbaren Netze dienen der Sprach- und Datenkommunikation und umfassen insbesondere das Corporate Network der Polizei (CNP), die Verwaltungsnetze wie das bayerische Behördennetz (BYBN) und den Digitalfunk BOS sowie weitere Kommunikationsnetze.
Die Verwaltung und die Organisationen des Freistaates Bayern müssen zu jedem Zeitpunkt handlungsfähig sein. Die staatlich verfügbaren Netze müssen deshalb ausfallsicher zur Verfügung gestellt werden, so gut es der Stand der Technik erlaubt.
Für die Netze der kritischen staatlichen Infrastrukturen bestehen besondere Anforderungen hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit (z. B. Ausfallsicherheit der aktiven Technik oder notwendige Härtung gegen Stromversorgungsausfälle, erhöhte Sicherheitsanforderungen an das Personal).

Zu Abs. 2

Aktuell werden die Netzleistungen im Rahmen von regelmäßigen Vergabeverfahren durch öffentliche Telekommunikationsanbieter erbracht.

Um die digitale Handlungs- und Entscheidungsfähigkeit des Freistaates entsprechend Art. 3 Abs. 1 zu sichern, kann der Freistaat insbesondere für die behördeninterne Kommunikation seine Fertigungstiefe erhöhen und eigene Netzinfrastrukturen aufbauen, besitzen und betreiben.

Der Freistaat kann Teile seiner Netzinfrastruktur anderen Infrastrukturanbietern zur Mitnutzung zu Verfügung stellen. Dabei kann er an geeigneten Zusammenarbeitsformen mit den Infrastrukturanbietern wie Verbänden oder Plattformen teilnehmen oder sich dieser bedienen.

Teil 3. IT-Sicherheit

Entsprechend der Art. 9 bis 17 BayEGovG werden in den Art. 41 bis 49 Regelungen zur IT-Sicherheit normiert. Gegenüber der bisherigen Rechtslage wurden punktuelle Änderungen vorgenommen.

Kapitel 1. Allgemeine Vorschriften

Zu Art. 41 Landesamt für Sicherheit in der Informationstechnik:

Die Regelung entspricht der Regelung des Art. 9 BayEGovG. Art. 41 regelt die Errichtung des Landesamts für Sicherheit in der Informationstechnik. Satz 2 normiert die Zuordnung zum Geschäftsbereich des Staatsministeriums der Finanzen und für Heimat.

Zu Art. 42 Aufgaben:

Bei Art. 42 handelt es sich um die unveränderte Übernahme des Art. 10 BayEGovG. Art. 42 regelt die Aufgaben des LSI.

Zu Abs. 1

Zu Nr. 1:

Aufgabe des LSI ist die Abwehr von Gefahren für die Sicherheit in der Informationstechnik an den Schnittstellen zwischen Behördennetz und anderen Netzen. Schwerpunkt des LSI wird der Schutz des Bayerischen Behördennetzes sein, das täglich Tausenden von Angriffen ausgesetzt ist. Zentrale Bedeutung hat hier die Überwachung des zentralen Internetübergangs, dem größten Einfallstor für Angriffe aus dem Internet. Erforderlich ist sowohl präventives als auch repressives Vorgehen. Dem LSI stehen hierzu die Befugnisse des zweiten Abschnitts zur Verfügung.

Zu Nr. 2:

Das LSI kann staatliche und an das Behördennetz angeschlossene Stellen bei der Abwehr von Gefahren für die Sicherheit in der Informationstechnik unterstützen. Die

Vorschrift ist aufgrund der schnelllebigen Entwicklung der Informationstechnologie bewusst weit gefasst, um eine Amtshilfe durch das LSI in möglichst vielen und auch zukünftig neuen Bereichen zuzulassen.
Die Aufgabe beschränkt sich bewusst auf die reine Unterstützungsleistung. Die Verantwortlichkeit der Behörden für die Sicherheit ihrer IT soll nicht auf das LSI übergeben.
Als Unterstützung kann das LSI bspw. einzelne Hard- und Softwarekomponenten (etwa Betriebssysteme, Textverarbeitungsprogramme oder Netzwerkkomponenten) auf Sicherheitsrisiken überprüfen. Damit entlastet es die IT-Stellen der einzelnen Behörden, die bereits geprüfte Produkte nicht erneut auf Einsatztauglichkeit in ihrem Bereich untersuchen müssen. Auch entfallen unnötige Mehrfachprüfungen, da Standardprodukte an einer zentralen Stelle geprüft werden.
Im Fall eines Angriffs kann ein Eingreif- und Reaktionsteam – eventuell sogar durch Vor-Ort-Service – bei der Abwehr mit seiner Fachexpertise behilflich sein.
Eine weitere Unterstützung kann in der Erteilung von Sicherheitszertifikaten liegen. Mit Genehmigung des originären Ausstellers des Sicherheitszertifikats, dass das LSI nach Vorliegen der Voraussetzungen hierzu befugt, kann es ein Zertifikat (bspw. Zertifizierung nach BSI-Grundschutz oder ISIS 12) verleihen. Möglich ist es auch, eigene, sog. LSI-Zertifikate, zu verleihen, die die Einhaltung von Sicherheitsrichtlinien oder bestimmten Standards bestätigen. Auch die Aufstellung eines eigenen LSI-Anforderungskatalogs ist denkbar.
Darüber hinaus kann das LSI als zentrale Stelle für IT-Sicherheit in der Verwaltung Verfahren und Geräte entwickeln, bereitstellen und betreiben, die staatlichen und an das Behördennetz angeschlossenen Einrichtungen zur Verfügung gestellt werden. In erster Linie wird es sich dabei um Krypto- und Sicherheitsmanagementsysteme handeln, die behördenübergreifend zum Einsatz kommen. Solche Systeme verschlüsseln u. a. die staatliche Kommunikation für Angreifer. Das LSI kann Schlüssel vergeben und „Public Key Infrastructures“ (PKI) zur Verteilung der Schlüssel betreiben. Auch sorgt das LSI dafür, dass die eingesetzten Anwendungen immer dem aktuellen Stand der Technik entsprechen. Werden diese Verfahren als Basisdienste oder zentrale Dienste bereitgestellt, können sie sogar von allen staatlichen und kommunalen Behörden genutzt werden.

Zu Nr. 3:

Das LSI muss ein für die staatliche informationstechnische Verwaltungsinfrastruktur angemessenes Sicherheitsniveau durchsetzen können. Hierfür kann es Mindeststandards entwickeln, die gemäß Art. 46 Satz 2 als Verwaltungsvorschriften festgelegt werden können. Unter die Mindeststandards fallen auch die bereits gültigen IT-Sicherheitsrichtlinien der Staatsregierung.

Zu Nr. 4:

Das LSI prüft, ob die eingesetzten informationstechnischen Systeme, Komponenten, Prozesse und IT-Sicherheitskonzepte der Staatsverwaltung und der an das Behördennetz angeschlossenen Stellen die sicherheitstechnischen Mindeststandards erfüllen. Hierfür hat es gemäß Art. 45 Abs. 1 ein Prüfungsrecht.

Zu Nr. 5:

Das LSI sammelt zentral Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen. Dabei beschäftigt es sich nicht nur mit aktuellen Ereignissen, auch Informationen über Zukunftstechnologien in der Branche werden untersucht und verprobt. Die Erkenntnisse stellt es den staatlichen und den an das Behördennetz angeschlossenen Stellen zur Verfügung. In Betracht kommen staatliche und kommunale Stellen, aber auch nationale oder internationale Einrichtungen wie das BSI, das European Cybercrime Center oder die Europäische Agentur für Netz- und Informationssicherheit können über neue Erkenntnisse informiert werden.
Schnelle Reaktionszeiten sind bei der Abwehr von Schadsoftware unabdingbar. Über aktuelle Bedrohungen hat es daher unverzüglich die betroffenen staatlichen und sonstige an das Behördennetz angeschlossenen Stellen zu unterrichten. Damit soll sichergestellt werden, dass diese rechtzeitigen Abwehrmaßnahmen gegen neue oder bevorstehende Bedrohungen ergreifen können. Als Annex zur Informationspflicht von Behörden kann das LSI darüber hinaus seine Erkenntnisse veröffentlichen. Dies ist sinnvoll, wenn die Informationen auch für Bürger, private Unternehmen oder sonstige Organisationen von Wichtigkeit oder Interesse sein können. Hierbei sollten die Informationen unter Berücksichtigung des Empfängerkreises durch klare und verständliche Handlungsempfehlungen über aktuelle Risiken und Bedrohungen und mögliche Abwehrmaßnahmen bestechen und über einfache Kanäle (bspw. soziale Medien) verteilt werden. Derartige Hinweise bedürfen keiner besonderen gesetzlichen Ermächtigung; Warnungen hingegen richten sich nach Art. 47.

Zu Nr. 6:

Das LSI übernimmt die Aufgabe als zentrale Kontaktstelle gemäß § 8b Abs. 2 Nr. 4 Buchst. c Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Die vom BSI erhaltenen Informationen gibt es an die Aufsichtsbehörden weiter. Ziel ist es, die Meldungen zu kanalisieren und dadurch die Gesamtsicherheitslage besser zu überblicken. Auch können die Informationen für andere Aufsichtsbehörden, die zunächst nicht direkt betroffen zu sein scheinen, von Nutzen sein. Je nach Komplexität der Meldung bereitet das LSI die Informationen des BSI für die Aufsichtsbehörde derart auf, dass auch technische Laien die Kritikalität der Informationen beurteilen können. In Einzelfällen kann eine unverzügliche Weitergabe notwendig sein.

Zu Abs. 2

Große Bedeutung kommt der Beratung und Warnung von staatlichen und kommunalen Stellen, öffentlichen Unternehmen, Betreibern kritischer Infrastrukturen und weiteren Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen zu. Auf Ersuchen können diese bei Fragen der IT-Sicherheit eingehend vom LSI unterstützt und beraten werden.
Ziel der Regelung ist insbesondere die Unterstützung von öffentlichen Unternehmen kleinerer und mittlerer Größe, die nicht die Schwellenwerte der BSI-KritisV erreichen und bislang nur unzureichend im Bereich der IT-Sicherheit vom Staat unterstützt werden. Ausfälle von Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen wie z. B. Betriebe des öffentlichen Personennahverkehrs oder lokale Energie- oder Wasserversorgungsunternehmen können regional große Schäden anrichten und müssen deshalb erforderlichenfalls mit staatlicher Unterstützung abgewehrt werden. Die Kosten werden in einer gesonderten Gebührenverordnung festgelegt.
Eine weitere Unterstützungsleistung kann die Erstellung und Fortschreibung von Informationssicherheitskonzepten sein, die staatliche Behörden und Kommunen gemäß Art. 43 Abs. 1 erstellen müssen. Bei dieser anspruchsvollen Aufgabe können sie im Rahmen von Art. 42 Abs. 1 Nr. 2 und Abs. 2 Unterstützung durch das LSI erhalten.
Auch bei anderen IT-Sicherheitskonzepten, wie sie bspw. bei einer Zertifizierung nach ISIS 12 oder ISO 27001 benötigt werden, kann das LSI andere Behörden etwa durch das Erstellen von Vorlagen oder die Übernahme der Projektleitung unterstützen.

Zu Abs. 3

Das LSI kann auf Ersuchen die Polizeien, Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz mit technischer Expertise – bspw. im Bereich Forensik, Kryptoanalyse oder BigData – unterstützen. In diesen Fällen wird es lediglich als Hilfsorgan tätig.

Zu Abs. 4

Zur Achtung der Gewaltenteilung ist das LSI nicht für die Kommunikationstechnik von Judikative, Legislative, des Obersten Rechnungshofs und des Landesbeauftragten für den Datenschutz zuständig. Allerdings steht die Gewaltenteilung im Interessenwiderstreit mit der Notwendigkeit der Absicherung des Behördennetzes. Aus diesem Grund ist das LSI wiederum zuständig, soweit diese Stellen am Behördennetz angeschlossen sind oder elektronische Verwaltungsinfrastrukturen bzw. zentrale Dienste im Sinne des Art. 42 nutzen. Dies ist gerechtfertigt, da der Anschluss an das Bayerische Behördennetz auf freiwilliger Basis erfolgt. Wer das erhöhte Sicherheitsniveau des Behördennetzes in Anspruch nehmen möchte, muss sich – zum Schutze aller – dem dort geltenden Sicherheitsdekret unterwerfen.
Soweit die Kommunikationstechnik von Judikative, Legislative, dem Obersten Rechnungshof und dem Landesbeauftragten für den Datenschutz ausschließlich in eigener Zuständigkeit betrieben wird, bleibt diese dem Zugriff des LSI verwehrt.

Zu Art. 43 Behördenübergreifende Pflichten:

Zu Abs. 1

Abs. 1 trifft Regelungen zur Sicherheit informationstechnischer Systeme.

Zu Abs. 2

Staatliche und sonstige an das Behördennetz angeschlossene Stellen sind nach Abs. 2 verpflichtet, Sicherheitslücken, Schadprogramme und erfolgte oder versuchte Angriffe unverzüglich an das Landesamt und die für sie zuständige oberste Dienstbehörde zu melden, soweit andere Vorschriften oder Vereinbarungen mit Dritten dem nicht entgegenstehen. Nur wenn das LSI über eine Bedrohung in Kenntnis gesetzt ist, kann es die anderen Behörden warnen. Vorschriften, die eine Weitergabe verhindern, können solche des Geheimschutzes oder über personenbezogene Daten sein, wobei die übermittelten Informationen in der Regel rein technischer Natur sind und keinen Personenbezug aufweisen. Auch privatrechtliche Verträge mit Herstellern können eine Unterrichtung verhindern. In solchen Fällen sollten die Behörden die Informationsweitergabe nicht unterlassen, sondern derart beschränken, dass Vertragsverletzungen vermieden werden. Unvollständige Informationen können zur IT-Sicherheit mehr beitragen als keine Informationen.
Die Meldeprozesse zwischen dem LSI und den Behörden können in allgemeinen Verwaltungsvorschriften bestimmt werden, für die es keine gesonderte Ermächtigung bedarf.

Zu Abs. 3

Staatliche und an das Behördennetz angeschlossene Stellen sind verpflichtet, das Landesamt bei Maßnahmen nach Art. 42 Abs. 1 Nr. 1, 2, 4 und 5 zu unterstützen. Dies gilt selbstverständlich nur vorbehaltlich datenschutzrechtlicher Vorschriften.
Klarstellend wird angemerkt, dass die Unterstützungsleistung der Rechenzentren insbesondere in der Übermittlung bereits erhobener Daten liegt. Sie ist erforderlich, wenn das LSI die Systeme, die die Daten erzeugen, nicht selbst betreibt. So wird bspw. der zentrale Internetübergang in das Behördennetz beim IT-Dienstleistungszentrum des Landesamts für Digitalisierung, Breitband und Vermessung betrieben. Dabei handelt es sich um ein komplexes Konglomerat verschiedenster Abwehr- und Kontrollmechanismen (Firewalls, VPNs, Proxy-Server, Anti-Viren-Systeme etc.). Schon Störungen im Promillebereich hätten erhebliche Auswirkungen auf das reibungslose Funktionieren des Behördennetzes. Die Fehlersuche würde sich aufgrund der Abstimmungsschwierigkeiten zweier Betreiber um ein Vielfaches erschweren. Die 140.000 Beschäftigten, die den Internetübergang nutzen, wären an ihrer Arbeit gehindert. Auch müssten jedes Mal die Auftraggeber als Verantwortliche im Rahmen von Auftragsdatenverarbeitungsverhältnissen der Übermittlung zustimmen.

Zu Abs. 4

Art. 43 BayDiG, der die behördenübergreifenden Pflichten regelt, wird um einen Abs. erweitert. Im neu eingefügten Abs. 4 wird eine Pflicht zur frühzeitigen Beteiligung des Landesamts bei der Planung und Umsetzung von maßgeblichen neuen Digitalisierungsvorhaben des Landes festgeschrieben.
Als IT-Sicherheitsbehörde ist das LSI zuständig für die Informationssicherheit auf Landesebene. In dieser Funktion gewährleistet das Landesamt nicht nur die Sicherheit der Informationstechnik der staatlichen Verwaltung, sondern ist auch Ansprechpartner für wesentliche Digitalisierungsmaßnahmen.
Um sicherzustellen, dass die Belange der IT-Sicherheit ausreichend und umfassend berücksichtigt werden, ist das LSI bei der Planung und Umsetzung von maßgeblichen neuen Digitalisierungsvorhaben von der jeweils zuständigen Stelle stets frühzeitig zu beteiligen. Dem LSI ist insoweit die Gelegenheit zur Stellungnahme einzuräumen.
Das einschränkende Kriterium der Maßgeblichkeit stellt klar, dass nicht jedes neue Digitalisierungsvorhaben die Beteiligung des Landesamts als Automatismus auslösen soll. Von der Verpflichtung erfasst werden sollen jedoch solche Vorhaben, die anhand ihrer Bedeutung und Tragweite eine Einbindung des Landesamts sinnvoll erscheinen lassen. Der jeweils zuständigen Stelle verbleibt hier ein Einschätzungsspielraum. Das bedeutet aber nicht, dass es in ihrem Belieben stünde, das Landesamt einzubinden, sondern dass sie in jedem Fall prüfen muss, ob das neue Digitalisierungsvorhaben als maßgeblich einzustufen ist oder nicht. Die Entscheidung ist im Rahmen des Vorhabenmanagements nach BayITR 01 zu dokumentieren.

Kapitel 2. Befugnisse

Zu Art. 44 Abwehr von Gefahren für die Informationstechnik:

Zu Abs. 1

Art. 44 stellt die zentrale Befugnisnorm für das LSI dar, um die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Behördennetzes nach Art. 42 Abs. 1 Nr. 1 effektiv und effizient mit technischen Mitteln zu gestalten.
Effektive Gefahrenabwehr kann nur durch ein einheitlich hohes Schutzniveau gewährleistet werden. Das beste IT-Sicherheitskonzept einer Behörde ist nutzlos, wenn der Angreifer durch nicht ausreichend gesicherte Kanäle einer anderen Behörde in das gesamte Netz eindringen kann. Dies gilt es nach wie vor zu verhindern.
Nach Satz 1 darf das LSI zur Gefahrenabwehr gegenüber staatlichen und an das Behördennetz angeschlossenen Stellen die nötigen Anordnungen treffen oder Maßnahmen ergreifen. Nur so kann ein homogenes Qualitätsniveau der IT-Sicherheit gewährleistet werden. Bei den zu ergreifenden Maßnahmen ist der Verhältnismäßigkeitsgrundsatz zu beachten, insbesondere ist stets das mildeste Mittel zur Erreichung des Zwecks zu wählen.
Die datenschutzrechtliche Generalklausel des Satz 2 dient dem legitimen Datenzugriff zur Gefahrenabwehr und wird konkretisiert durch Abs. 2. Zur Klarstellung wird deshalb jetzt ausdrücklich auf Abs. 2 Bezug genommen. Muss das LSI auf Systeme zugreifen, um bspw. Schadprogramme zu entfernen, so könnte es hierbei auf personenbezogene

Daten stoßen. Daher bedarf es korrespondierender datenschutzrechtlicher Befugnisse zu den allgemeinen Befugnissen des LSI aus Satz 1.

Zu Abs. 2

Abs. 2 konkretisiert die datenschutzrechtliche Generalbefugnis aus Art. 44 Abs. 1 Satz 2. Der Einleitungssatz begrenzt nunmehr normenklar die Datenverarbeitung auf das für die Erfüllung der jeweiligen Aufgabe erforderliche Maß.

Zu Nr. 1:

Nach Art. 44 Abs. 2 Nr. 1 kann das LSI weiterhin Protokolldaten, die beim Betrieb von Informationstechnik des Landes anfallen, erheben und automatisiert auswerten. Bei den Änderungen handelt es sich lediglich um redaktionelle Anpassungen.
Mit Protokolldaten sind sog. Logfiles von Servern, Firewalls, Web-Proxys, Clients etc. gemeint. Diese Logfiles protokollieren sog. Events, also Ereignisse über Anfragen von anderen Systemen, Softwareänderungen, Fehlermeldungen etc.
Setzt man Protokolldaten verschiedener Systeme in Korrelation und wertet diese aus, so können Unregelmäßigkeiten und damit potenzielle Bedrohungen erkannt werden. Protokolldaten, die für die Abwehr von Gefahren interessant sind, können unter anderem sein:
– Protokolldaten von Firewall-Systemen einschließlich Erhebungszeitpunkt, IP-Adresse und Port sowie vollständigem Domänennamen von ein- und ausgehenden Verbindungen sowie die durch die Firewall durchgeführte Aktion;
– Protokolldaten von Systemen zur Erkennung und Beseitigung von Schadsoftware einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen des betroffenen Systems, Kontextinformationen des Vorfalls, ausgegebener Meldung sowie Informationen über die Schadsoftware und die als Schadprogramm erkannten Daten;
– Protokolldaten von Systemen zur Erkennung von unerwünschten E-Mails einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen von ein- und ausgehenden Verbindungen, E-Mail-Adresse des Absenders und Empfängers einer Nachricht, deren Größe und eindeutiger Identifikationsnummer sowie Fehler- und sonstige Statusmeldungen und die als Schadprogramm erkannten Daten;
– Protokolldaten von Datenbankservern einschließlich Erhebungszeitpunkt, Anmeldename, IP-Adresse und vollständigem Domänennamen von Verbindungen und die Identifikationsnummer der ausgegebenen Meldung und deren Klartext;
– Protokolldaten von Web- und Proxyservern einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen von ein- und ausgehenden Verbindungen sowie dem einheitlichen Ressourcenzeiger (Uniform Resource Locator URL) und Kopfdaten und
– Protokolldaten 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.

Die nachfolgenden Nummern in Art. 44 Abs. 2 sind dagegen nicht auf Protokolldaten begrenzt.

Zu Nr. 2:

Nach Art. 44 Abs. 2 Nr. 2 kann das LSI wie bisher 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 Behördennetz 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. Hinzugekommen ist die Befugnis des LSI, auch Daten, die an vergleichbaren Schnittstellen innerhalb des Behördennetzes anfallen, zu erheben und automatisiert auszuwerten. Erfasst werden sollen damit Fälle wie zum Beispiel die sicherheitstechnische Untersuchung von E-Mails, die von verschiedenen Bereichen des Bayerischen Behördennetzes versandt werden. Die automatisierte Auswertung gestattet nicht die Speicherung der Inhalte über den für die technische Abwicklung des Kommunikations- und Erkennungsvorgangs ohnehin notwendigen Umfang hinaus.
Einzelheiten zur Datenverarbeitung und -übermittlung regeln Art. 48 und 49.

Zu Nr. 3:

Auf Grundlage von Art. 44 Abs. 2 Nr. 3 darf das LSI nunmehr ausdrücklich Daten aus öffentlich zugänglichen Quellen erheben und automatisiert auswerten, die Informationen mit Auswirkungen auf die Sicherheit der Informationstechnik des Landes oder der an das Behördennetz angeschlossenen Stellen haben können. Datenschutzrechtlich abgesichert werden soll mit der neu eingefügten Nr. 3 insbesondere der Einsatz von Werkzeugen/Diensten im Bereich „Open-Source Intelligence (OSINT)“. Ein Bedürfnis hierfür gibt es unter anderem, seitdem vermehrt dienstliche Accounts geleakt worden sind. Die Veröffentlichung einer dienstlichen E-Mail-Adresse mit einem geleakten Passwort auf einer Internetseite, die nicht unbedingt mit dem Behördennetz in unmittelbarer Verbindung steht, kann, wenn das Passwort verwendungsfähig ist, also den behördlichen Anforderungen an die Passwortgeneration entspricht, zu einer Gefahr für die Sicherheit in der Informationstechnik werden. Häufig werden dieselben Passwörter verwendet mit der Folge, dass durch die Erlangung einer Kombination von Passwort und E-Mail-Adresse eine Vielzahl von Logins auf unterschiedlichen Seiten möglich wird, selbst wenn der Leak auf einer behördenexternen Seite aufgetreten ist.
Es gehört zu den Aufgaben des LSI, dienstliche Accounts vor einem rechtswidrigen Zugriff zu schützen und damit einhergehende Gefahren zu erkennen, Informationen hierüber zu sammeln und die zuständigen Stellen zu unterrichten. Art. 44 Abs. 2 Nr. 3 gibt dem LSI nun die datenschutzrechtliche Befugnis, hierzu in öffentlich zugänglichen Quellen wie dem Internet zu recherchieren, um herauszufinden, wo welche Daten des

Freistaates oder der an das Behördennetz angeschlossenen Stellen veröffentlicht werden und wie sie ggf. genutzt werden.
Auch das frühzeitige Erkennen von unsicher konfigurierten exponierten Systemen ist für die IT-Sicherheit essenziell und gehört damit zu den Aufgaben des LSI.

Zu Nr. 4:

Ist ein Angriff auf die Informationstechnik anzunehmen, untersucht das Landesamt seiner gesetzlichen Aufgabe (Art. 42 Abs. 1 Nr. 1 und 2) entsprechend die Informationstechnik der betroffenen staatlichen oder an das Behördennetz angeschlossenen Stelle, um die Gefahr abzuwehren. Hierbei ist ein Zugriff auf die dort – flüchtig oder dauerhaft - gespeicherten Daten meist unvermeidlich. Es ist ferner davon auszugehen, dass regelmäßig personenbezogene Daten enthalten sein werden. Daher bedarf es einer gesetzlichen Befugnis, diese Daten zu verarbeiten. Die Befugnis zur Untersuchung ergibt sich bereits aus Art. 44 Abs. 1 Satz 1.
Aus diesem Grund ist eine Nr. 4 in Art. 44 Abs. 2 eingefügt worden. Die neue datenschutzrechtliche Befugnis ist an den Zweck der Bearbeitung des Angriffs gebunden. Der Umfang ist begrenzt auf die Daten, die in Zusammenhang mit dem möglichen Angriff stehen („soweit ein Angriff auf die Informationstechnik anzunehmen ist…“). Unschädlich ist, falls sich der Vorfall im Nachhinein doch nicht als Angriff erweisen sollte, wenn im Zeitpunkt der Untersuchung durch das LSI ein Angriff anzunehmen war.

Zu Abs. 3

Mit dem neu eingefügten Abs. 3 wird die Rolle des Landesamts bei der Verarbeitung personenbezogener Daten im Rahmen von Art. 42 Abs. 2 definiert. Nach Art. 42 Abs. 2 kann das LSI auf Ersuchen kommunale Stellen, öffentliche Unternehmen, Betreiber kritischer Infrastrukturen und weitere Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen beraten und unterstützen. Das LSI ist insoweit Auftragsverarbeiter der genannten Stellen. Damit ist in Kombination mit entsprechenden Auftragsverarbeitungsvereinbarungen eine gesetzliche Grundlage für die Auftragsverarbeitung nach Art. 28 Abs. 3 Satz 1 DSGVO geschaffen.

Zu Art. 45 Untersuchung der Sicherheit in der Informationstechnik:

Zu Abs. 1

Hier sind keine Änderungen im Vergleich zum BayEGovG erfolgt.
Das LSI kann die Sicherheit der Informationstechnik staatlicher und an das Behördennetz angeschlossener Stellen untersuchen und bewerten, mithin hat es ein Recht zur Prüfung einzelner Systemkomponenten bis hin zur Auditierung der gesamten IT-Infrastruktur. Damit wird sichergestellt, dass alle Stellen des Behördennetzes das er-

forderliche Sicherheitsniveau erfüllen. Zwingend zu beachten ist dabei, dass die Aufgabenerfüllung von unabhängigen Stellen wie dem Landtag, dem Obersten Rechnungshof oder dem Landesbeauftragten für den Datenschutz nicht behindert wird.
Über das Ergebnis der Prüfung erstellt das LSI einen Bericht, den es der untersuchten Stelle zur Verfügung stellt.

Zu Abs. 2

Abs. 2 dient dazu, Rechtssicherheit für umfassende Untersuchungen von IT-Produkten (z. B. mittels Reverse - Engineering) und IT-Systemen durch das LSI zur Erfüllung seiner Aufgaben herzustellen. Die gesetzliche Befugnis führt dazu, dass die Beschaffung von Daten und Informationen über den Aufbau und die Funktionsweise der Untersuchungsgegenstände durch das LSI nicht als „unbefugt“ im Sinne von § 202a Strafgesetzbuch (StGB) bzw. § 17ff. des Gesetzes gegen den unlauteren Wettbewerb (UWG) anzusehen ist.
Auf dem Markt bereitgestellte bzw. zur Bereitstellung auf dem Markt vorgesehene Untersuchungsgegenstände sind solche, die für einen Erwerb durch das LSI verfügbar sind. Die Formulierung „auf dem Markt bereitgestellte Produkte“ ist angelehnt an eine entsprechende Formulierung im Produktsicherheitsgesetz. Durch die Formulierung „zur Bereitstellung auf dem Markt vorgesehene“ Untersuchungsgegenstände wird klargestellt, dass die Untersuchungsbefugnis auch solche Produkte und Systeme erfasst, die zwar vom Hersteller bereits angekündigt wurden, aber noch nicht allgemein am Markt verfügbar sind. Untersuchungsrechte bei Herstellern, Anbietern und sonstigen Einrichtungen werden durch Abs. 2 nicht begründet.
Sollten Dritte mit der Untersuchung beauftragt werden, hat das LSI bei der Auswahl der Dritten die schutzwürdigen Interessen des Herstellers zu berücksichtigen. Hierzu gehört auch, dass es den beauftragten Dritten zur Wahrung einer entsprechenden Vertraulichkeit verpflichtet. Die Beauftragung eines direkten Konkurrenten des Herstellers ist in diesem Zusammenhang ausgeschlossen.
Neu hinzugekommen ist in Satz 1 die Befugnis, die informationstechnischen Produkte nicht nur zu untersuchen, sondern auch zu bewerten. Da die Untersuchung durch das LSI kein Selbstzweck ist, sondern zu konkreten Ergebnissen führen soll, gibt es das Bedürfnis für eine Bewertung. Erst aus einer Bewertung können Handlungsempfehlungen abgeleitet werden. Gleichzeitig weist eine Bewertung eine eigene Eingriffsqualität auf, so dass es einer gesonderten Rechtsgrundlage bedarf.
Durch die Untersuchungen des LSI sollen informationstechnische Produkte auch für andere besser einschätzbar werden. Daher wurde ein neuer Satz 2 eingefügt, der die Befugnis enthält, die Bewertung an die an das Behördennetz angeschlossenen Stellen und im Einzelfall an die in Art. 43 Abs. 2 genannten öffentlichen Stellen weiterzugeben. Damit sollen Stellen außerhalb des Landesamts von der Expertise des LSI profitieren können. Der hierin liegende Eingriff in die Rechte der Produktverantwortlichen ist dadurch gerechtfertigt, dass die Bewertung nur an die an das Behördennetz angeschlossenen Stellen weitergegeben werden darf, für dessen Sicherheit das LSI ver-

antwortlich ist. Nur im Einzelfall können Bewertungen auch an öffentliche Stellen weitergegeben werden, die das LSI auf Ersuchen in Fragen der Sicherheit in der Informationstechnik nach Art. 42 Abs. 2 berät und unterstützt. Eine allgemeine Veröffentlichung der Bewertung wäre hiervon nicht gedeckt. Insofern ist die Ausgestaltung in Satz 2 verhältnismäßig.

Zu Art. 46 Mindeststandards:

Hier sind keine Änderungen im Vergleich zum BayEGovG erfolgt.
Art. 46 weist dem LSI die Befugnis zu, allgemeine technische Mindeststandards für die IT-Sicherheit zu entwickeln. Auch hier ist es Ziel, ein einheitlich hohes Niveau der IT-Sicherheit bei den Behörden zu schaffen. Das Staatsministerium der Finanzen und für Heimat als zuständiges Staatsministerium kann im Einvernehmen mit den weiteren Staatsministerien und der Staatskanzlei diese Mindeststandards ganz oder teilweise als verbindliche allgemeine Verwaltungsvorschriften für alle staatlichen Stellen erlassen. Im Falle der IT-Sicherheitsrichtlinien geschieht dies bereits heute durch den IT-Beauftragten der Staatsregierung im Einvernehmen mit den Ressort-CIOs. Dieses Verfahren ist auch auf andere Mindeststandards übertragbar.
Nur durch derartige Vorgaben kann sichergestellt werden, dass Sicherheitslücken auf Seiten einer Behörde nicht die Gesamtsicherheit des Behördennetzes und damit aller anderen Behörden gefährden. Für Kommunen und unabhängige Stellen, die nicht an das Behördennetz angeschlossen sind, haben die Mindeststandards lediglich empfehlenden Charakter.
Nicht staatliche Stellen können durch Verwaltungsnutzung der Datenvorschriften des Landes nicht zur Einhaltung von Mindeststandards verpflichtet werden. Daher regelt Satz 3, dass für Landratsämter und die an das Behördennetz angeschlossenen, nicht staatlichen Stellen die Mindeststandards für die Teilnahme am Behördennetz gelten. Damit wird sichergestellt, dass die bislang gültigen Anschlussbedingungen für Teilnehmer am Bayerischen Behördennetz verpflichtend sind. Die Landratsämter werden aufgrund ihrer Doppelfunktion ausdrücklich erwähnt. Das Konnexitätsprinzip wird durch die Regelung nicht berührt, da der Anschluss am Behördennetz auf freiwilliger Basis erfolgt.

Zu Art. 47 Warnungen:

Hier sind keine Änderungen im Vergleich zum BayEGovG erfolgt.

Zu Abs. 1

Die Vorschrift regelt, dass das LSI aufgrund von gewonnenen Erkenntnissen über Sicherheitslücken, Schadprogramme oder unbefugte Datenverarbeitung Warnungen aussprechen und Sicherheitsmaßnahmen empfehlen darf. Um einen schnellen Informationsfluss zu gewährleisten, wird nach Abschluss der Errichtungsphase mittelfristig ein 24-Stunden/7-Tage-Betrieb angestrebt.

Zu Abs. 2

Mit Warnungen zu Hard- oder Softwareprodukten kann ein nicht unerheblicher Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb einhergehen. Schlimmstenfalls ist das betroffene Unternehmen in seiner Existenz gefährdet. Aus diesem Grund sind Informationen, die sich im Nachhinein als falsch oder unrichtig wiedergegeben herausstellen, unverzüglich zu berichtigen. Die Berichtigung erfolgt auf Antrag des Betroffenen oder, wenn erhebliche Belange des Gemeinwohls gefährdet sind, von Amts wegen.

Kapitel 3. Datenschutz

Zu Art. 48 Datenspeicherung und -auswertung:

Zu Abs. 1

Grundsätzlich richtet sich die Löschung nach dem Datenschutzrecht. Personenbezogene Daten sind vor allem dann zu löschen, wenn sie unrechtmäßig verarbeitet werden oder für den Zweck, für den sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.
Besonderheiten gilt es bei der Auswertung von automatisierten Daten nach Art. 44 i. V. m. Art. 48 Abs. 1 zu beachten. Die Norm stellt klar, dass Daten, die Personenbezug aufweisen oder dem Fernmeldegeheimnis unterliegen, bei der automatisierten Auswertung nach Art. 44 Abs. 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.).
In diesem Zusammenhang ist ein besonderes Augenmerk auf Daten zu legen, die dem Steuer- oder dem Sozialgeheimnis unterfallen. Bei der hierunter fallenden Kommunikation ist der Kreis der zugriffsbefugten Personen einzuschränken. Zudem muss durch Dokumentation nachvollziehbar sein, wer zu welchem Zeitpunkt welche Daten geprüft, ausgewertet oder sonst verarbeitet hat. Darüber hinaus muss den prüfenden Personen verdeutlicht werden, dass ein Verstoß gegen das Steuer- bzw. Sozialgeheimnis strafbewehrt ist und Disziplinarmaßnahmen nach sich zieht.
Im Übrigen gelten für die Löschung und Auswertung personenbezogener Daten die Vorschriften des Datenschutzrechts.

Zu Abs. 2

Abs. 2 regelt den Umgang mit Protokolldaten. Diese können für einen erforderlichen Zeitraum, längstens jedoch 12 Monate, gespeichert werden. Voraussetzung ist nach Nr. 1, dass tatsächliche Anhaltspunkte dafür bestehen, dass die Daten für den Fall der Bestätigung eines Verdachts nach Abs. 4 Satz 1 Nr. 2 zur Abwehr von Gefahren für die Informationstechnik erforderlich sein können. Dabei handelt es sich um das sog. Quick-Freezing-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 in BVerfGE 1 BvR 256/08 = NJW 2010, 833, Rn. 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 Abs. 2 Strafprozessordnung (StPO).

Die Möglichkeit zur Speicherung von Protokolldaten wird von drei auf maximal 12 Monate erhöht. Wie Cyber-Vorfälle gerade in der näheren Vergangenheit zeigen, erstrecken sich insbesondere spezialisierte Cyberangriffe, so genannte Advanced Persistent Threats (APTs), über einen mehrjährigen Zeitraum. Persistenz bezeichnet dabei das Bemühen der Angreifer, sich nachhaltig und unbemerkt in der Kommunikationstechnik des Landes oder das Behördennetz einzunisten. Eine wesentliche Eigenschaft eines APT-Angriffs ist dessen unterschwellige Vorgehensweise, durch die er lange unerkannt im System bleiben kann. Kennzeichnend ist, dass Angreifer vorsichtig und verdeckt vorgehen, so dass zwischen der initialen Infektion der Kommunikationstechnik des Landes und der Aufdeckung des Angriffs in der Regel große Zeiträume liegen. Um durch APT hervorgerufene Kompromittierungen erkennen und entfernen zu können, muss die Speicherdauer der Protokolldaten den Beginn des APT-Angriffs einschließen. Nur wenn das Vorgehen des Angreifers – auch im Nachhinein – aufgeklärt werden kann, kann die Kommunikationstechnik vor gleichartigen zukünftigen Bedrohungen geschützt werden. Die Zeitspanne zwischen Infektion und Entdeckung eines APT-Angriffs beträgt Monate, fortlaufende APTs bleiben in der Praxis zum Teil über Jahre unentdeckt. Um bei einem Vorfall die durch den APT hervorgerufenen Kompromittierungen zeitnah und besser erkennen und entfernen zu können, sollte daher die Speicherdauer der Protokolldaten den Zeitraum der gesamten Wirkdauer eines APTs möglichst einschließen. Eine Speicherdauer von 12 Monaten verbessert die Möglichkeit der Reaktion auf Angriffe wesentlich und gewährleistet zugleich einen angemessenen Schutz von personenbezogenen Daten.

Die Speicherhöchstdauer von 12 Monaten ist verhältnismäßig, insbesondere verfolgt sie einen legitimen Gemeinwohlzweck, ist geeignet, erforderlich und angemessen (vgl. BVerfG in BVerfGE 100, 313, 359 = NJW 2000, 55). Art. 10 Abs. 1 Grundgesetz verbietet nicht jede vorsorgliche Erhebung und Speicherung von Daten überhaupt, sondern schützt vor einer unverhältnismäßigen Gestaltung solcher Datensammlungen und hierbei insbesondere vor entgrenzenden Zwecksetzungen. Strikt verboten ist lediglich die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken (vgl. BVerfG 1 BvR 256/08 in NJW 2010, 833, Rn. 206).

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. Erforderlich ist nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt wird 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 verhindern. Weniger einschneidende Mittel, die ebenso weitreichende Aufklärungsmaßnahmen ermöglichen, sind nicht ersichtlich.

Die Maßnahme ist auch verhältnismäßig im engeren Sinne, das heißt angemessen. Regelmäßig können Schadprogramme erst mit zeitlichem Verzug von Tagen, Wochen oder gar mehreren Monaten bis zu Jahren aufgespürt werden. Im Anschluss muss dem LSI genug Zeit zur Verfügung stehen, die Daten zu analysieren. Unter Berücksichtigung des hohen Schutzbedarfs der staatlichen IT-Infrastruktur wird deshalb die maximale Speicherdauer der zur Erkennung von Schadprogrammen relevante Protokolldaten auf 12 Monate festgelegt.

Nach Nr. 2 ist eine Speicherung von Protokolldaten auch möglich, wenn die Daten zur Verhütung, Unterbindung oder Verfolgung damit zusammenhängender Straftaten erforderlich sein können. Die Regelung erlaubt die Speicherung von Daten, die bspw. bei einem versuchten Cyberangriff auf die IT-Infrastruktur angefallen sind. Nur so wird dem Freistaat Bayern als Geschädigtem die Möglichkeit gegeben, strafrechtliche Ermittlungen einleiten zu lassen. Zudem können die Sicherheitsbehörden diese Daten nutzen, um künftige Straftaten zu verhindern oder laufende Straftaten zu unterbinden.

Nach Satz 2 müssen die Daten im Gebiet der Europäischen Union gespeichert werden. Damit werden Vorgaben des Europäischen Gerichtshofs (EuGH) (vgl. EuGH C-293/12 Rn. 66 ff.; EuGH C-203/15 und C-698/15, Rn. 122) erfüllt.

Satz 3 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).

Das Recht auf informationelle Selbstbestimmung wird neben der Sicherstellung einer automatisierten Erkennung nach Satz 3 durch eine Pseudonymisierung der Daten nach Satz 4 geschützt. Aliase oder behördeninterne IP-Adressen sind für das Landesamt grundsätzlich bereits pseudonym, da die Auflösungen dem Landesamt nicht bekannt sind.

Zu Abs. 3

Abs. 3 regelt den Umgang von 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 2 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 sollen die Wahrung der Verhältnismäßigkeit sicherstellen. Allerdings ist die Anordnung 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 Art. 44 Abs. 1 ist die Hürde bei der Unerlässlichkeit nochmals erhöht.
Im Übrigen wird auf die Ausführung zu Abs. 2 verwiesen.

Zu Abs. 4

Liegt ein hinreichender Verdacht vor, so können weitere, auch nicht automatisierte Maßnahmen folgen. Dazu dürfen die Daten über die Abs. 2 und 3 hinaus verarbeitet und genutzt werden. Notwendige Untersuchungen der Daten sind zulässig, um einen Verdacht, dass die Daten eine Gefahr für die Informationstechnik etwa durch ein Schadprogramm, durch programmtechnische Sicherheitslücken, unbefugte Datennutzung oder -verarbeitung enthalten, zu bestätigen.
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. Beispielweise kann die Funktionsweise einer Schadsoftware untersucht oder ihre Signatur in Datenbanken von Anti-Viren-Software aufgenommen werden.
Ein hinreichender Verdacht liegt vor, wenn Anhaltspunkte vorliegen, 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 Abs. 1 StPO.
Auch ist eine über die Abs. 2 und 3 hinausgehende Verarbeitung und Nutzung der Daten zulässig, wenn bei der Verarbeitung oder Nutzung der Daten zu übermittelnde Daten (Art. 49 Abs. 2) festgestellt werden. Nr. 3 regelt damit auch den sog. Zufallsfund.

Werden bei der Analyse der Daten Hinweise auf eine Gefahr für Leib, Leben oder Freiheit einer Person oder Daten bekannt, die zur Verhütung und Unterbindung von Straftaten oder zur Verfolgung einer von Art. 49 Abs. 2 Nr. 2 umfassten Straftaten benötigt werden können, so dürfen diese u. a. gespeichert werden. Dies gilt auch, wenn sich letztlich der Verdacht, dass die Daten eine Gefahr für die Informationstechnik darstellen, nicht bestätigt. Damit wird verhindert, dass Daten gelöscht werden müssten und eine Übermittlung an die Sicherheitsbehörden, Polizei bzw. Strafverfolgungsbehörden nach Art. 49 Abs. 2 dann nicht mehr möglich wäre.

Während Abs. 2 und Abs. 3 lediglich eine automatisierte Auswertung und nicht personenbezogene Verwendung von Daten zulassen, kann sich Abs. 4 auch auf die inhaltliche Prüfung von Dokumenten, bspw. nach Schadcode, beziehen. Zur Gewährleistung der richterlichen Unabhängigkeit ist daher, wenn Daten verarbeitet werden, welche die richterliche Unabhängigkeit berühren, nach Satz 3 der jeweils zuständigen obersten Dienstbehörde zu berichten. Die obersten Dienstbehörden können die Berichte den jeweiligen Kontrollgremien weiterleiten. Darüber hinaus sind nach Satz 3 unabhängige Stellen wie der Landesbeauftragte für den Datenschutz und die auch anderweitig hervorgehobenen geschützten Träger von Berufs- oder besonderen Amtsgeheimnissen (vgl. Wilde u.a., Kommentar und Handbuch zum BayDSG, Art. 22 BayDSG, Rn. 7 ff.) zu unterrichten, soweit deren Datenverarbeitung berührt ist.

Zu Abs. 5

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 Art. 1 Abs. 1 Grundgesetz ergibt sich, dass ein Kernbereich privater Lebensgestaltung als absolut unantastbar geschützt ist (vgl. BVerfG in BVerfGE 119, 1 ff.). 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 Tatsache ihrer Erlangung und ihre Löschung sind zu dokumentieren.

Zu Art. 49 Datenübermittlung:

Zu Abs. 1

Abs. 1 regelt die Übermittlung der nach Art. 44 i. V. m. Art. 48 erlangten Daten. Die Vorschrift stellt sicher, dass eine Datenübermittlung an Rechenzentren und andere Betreiber von IT-Technik, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren erforderlich ist, möglich ist. Dies gilt unabhängig davon, ob die Gefahr für die Informations- und Kommunikationsinfrastruktur des Landes oder einer an das Behördennetz angeschlossenen, nicht-staatlichen Stelle besteht. Insofern ist die Einschränkung „des Landes“ zu streichen.

Zu Abs. 2

Ein Angriff auf die staatliche IT stellt zumeist auch eine Straftat (z. B. nach §§ 202a ff., 303a f. StGB) dar. Mit Abs. 2 wird dem LSI die datenschutzrechtliche Befugnis zur Datenübermittlung an Sicherheitsbehörden, Polizei und Strafverfolgungsbehörden eingeräumt. Als datenschutzrechtliche Zweckänderung und Weiterverarbeitungserlaubnis unterliegt die Regelung in besonderer Weise dem Grundsatz der Verhältnismäßigkeit, dem dadurch Rechnung getragen wird, dass nicht in sämtlichen Fällen Daten übermittelt werden dürfen bzw. sollen.
Nr. 1 wurde neu gefasst, um klarzustellen, dass die Polizei selbstverständlich auch eine Sicherheitsbehörde ist. Der Anwendungsbereich von Nr. 1 zielt primär auf die in Nr. 2 genannten Straftaten, weshalb deren Verhütung und Unterbindung künftig an erster Stelle genannt werden sollen, während die Gefahrenabwehr für höchstpersönliche Rechtsgüter nur einen Auffangtatbestand darstellt.

Neben Leib, Leben und Freiheit der Person gehören die spezifisch dem Aufgabenbereich des Verfassungsschutzes zugrunde liegenden Rechtsgüter der verfassungsmäßigen Ordnung sowie des Bestands und der Sicherheit des Bundes oder der Länder zu den Rechtsgütern von „überragendem verfassungsrechtlichen Gewicht“ (BVerfG, Urt. v. 19.05.2020 – 1 BvR 2835/17 – Rn. 163). Daraus rechtfertigt sich die Regelung des Art. 24 BayVSG, die eine allgemeine Übermittlungspflicht aller bayerischen Behörden für verfassungsschutzrelevante Erkenntnisse enthält. Dass insoweit grundsätzlich keine besonderen Übermittlungsschwellen erforderlich sind, hat das BVerfG im aktuellen Beschluss zum Antiterrordateigesetz II nochmals bestätigt (vgl. BVerfG, Beschl. v. 10.11.2020 – 1 BvR 3214/15 – Rn. 106, 119). Da das LSI von der Übermittlungspflicht des Art. 24 BayVSG nicht ausgenommen werden soll, bedarf es der Klarstellung. Die Regelung ist insbesondere deshalb von praktischer Bedeutung als Angriffe auf IT-Systeme oftmals einen nachrichtendienstlichen oder OK-bezogenen Hintergrund haben.

Für den präventiven Bereich beschränkt sich die Übermittlungsbefugnis auf die Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person sowie auf die Fälle der Verhütung und Unterbindung von in Art. 49 Abs. 2 Nr. 2 genannten Straftaten. Für den

Bereich der Strafverfolgung wiederum soll eine Übermittlung erfolgen, soweit die Tatsachen, aus denen sich die Gefahr für die Informationstechnik oder der diesbezügliche Verdacht ergibt, selbst den Verdacht einer Straftat begründen. Sog. Zufallsfunde sollen nur übermittelt werden, wenn die Voraussetzungen der Nr. 2 Buchst. b vorliegen. Die Vorschrift stellt die Übermittlung in ein intendiertes Ermessen des LSI. Sie lässt damit Spielraum für konkretisierende Absprachen zwischen dem LSI und den empfangenden Stellen, durch die vermieden werden kann, dass eine generelle Regelübermittlung bei ca. 40.000 versuchten Angriffen pro Tag die Kapazitäten aller beteiligten Stellen unnötig belasten würde. Es sollen nur Angriffe mit einem gewissen Grad an Erheblichkeit gemeldet und folglich nur diese Daten übermittelt werden.

Satz 2 gibt vor, dass das Staatsministerium der Finanzen und für Heimat im Einvernehmen mit dem Staatsministerium des Innern, für Sport und Integration und dem Staatsministerium der Justiz Verwaltungsvorschriften zum konkreten Verfahren der Zusammenarbeit zwischen LSI und den Sicherheitsbehörden, der Polizei und den Strafverfolgungsbehörden festlegt. Die neuen Bezeichnungen der Ministerien infolge veränderter Ressortzuständigkeiten werden mit der Anpassung übernommen.

Teil 4. Organisation

Im BayEGovG wurde im Interesse organisatorischer Flexibilität bewusst auf Organisationsregelungen verzichtet. Dem Grundsatz der organisationsrechtlichen Zurückhaltung ist auch das BayDiG verpflichtet. Die grundlegend veränderten verfassungsrechtlichen und einfachgesetzlichen Rahmenbedingungen (Art. 91c Abs. 5, OZG, SDG-Verordnung) haben allerdings zu einem erheblich erhöhten ebenenübergreifenden Kooperationsbedarf geführt, insbesondere zwischen dem Freistaat Bayern und den bayerischen Kommunen. Daher soll in Art. 50 der bisher auf Vereinbarung zwischen dem Freistaat Bayern und den Kommunalen Spitzenverbänden gegründete „E-Government-Pakt“ durch gesetzliche Regelungen in den Kommunalen Digitalpakt überführt werden, dessen Aufgaben zugleich weiter gefasst werden als bisher. Der Organisationsteil des Gesetzes enthält zudem Vorschriften zu Standardisierungsbeschlüssen.

Zu Artikel 50 Kommunaler Digitalpakt:

Artikel 50 schafft auf gesetzlicher Grundlage ein Gremium für die verwaltungsträgerübergreifende Zusammenarbeit zwischen dem Freistaat und den Gemeinden, Gemeindeverbänden und Landkreisen. Derzeit erfolgt die verwaltungsträgerübergreifende Zusammenarbeit zwischen dem Freistaat Bayern und den bayerischen Kommunen im E-Government Pakt der seine (nicht gesetzliche) Grundlage in einer Vereinbarung zwischen dem Staatsministerium der Finanzen und den Kommunalen Spitzenverbänden findet. Der Digitalpakt soll an die Stelle des bisherigen E-Government Pakts treten, die Interessen der beteiligten Ressorts angemessen widerspiegeln und dabei in seinen Funktionen gestärkt werden.

Zu Abs. 1

Abs. 1 enthält die gesetzliche Grundlage für die Errichtung des Digitalpakts im Freistaat Bayern. Mit „Digitalisierung“ im Sinne dieses Absatzes ist die Digitalisierung im Rahmen dieses Gesetzes (vgl. Art. 1) gemeint.

Zu Abs. 2

Abs. 2 regelt die Zusammensetzung des Gremiums. Neben den ständigen Mitgliedern können auch nichtständige Mitglieder hinzugezogen werden, wie etwa weitere Fachressorts bei fachlicher Betroffenheit oder der Landesbeauftragte für den Datenschutz bei datenschutzrelevanten Themen. Um der besonderen Relevanz des Datenschutzes Rechnung zu tragen sieht Abs. 5 zudem eine besondere Regelung zur Information und Beteiligung des Landesbeauftragten vor.

Zu Abs. 3

Abs. 3 regelt die Informationsrechte des Gremiums.

Zu Abs. 4

Abs. 4 zählt die Bereiche auf, zu denen der Digitalpakt einstimmig Empfehlungen aussprechen kann.

Zu Abs. 5

Abs. 5 regelt die Einbindung des Landesbeauftragten für den Datenschutz bei datenschutzrelevanten Themen und Empfehlungen des Digitalpakts.

Zu Abs. 6

Der Digitalpakt benötigt eine Geschäftsstelle für die Vor- und Nachbereitung der Gremienarbeit und die damit verbundenen Verwaltungsaufgaben. Abs. 6 legt die organisatorische Einrichtung der Geschäftsstelle fest. Der Digitalpakt bestimmt auch die Einzelheiten der Sitzungsregularien (Sitzungsrhythmus, Einladung, Tagesordnung, Abstimmungsverfahren, Niederschrift usw.) in eigener Zuständigkeit. Abs. 6 bietet auch dafür die gesetzliche Grundlage.

Zu Artikel 51 Standardisierungsbeschlüsse:

Zu Abs. 1

Abs. 1 bestimmt, dass das Staatsministerium für Digitales verbindliche IT-Interoperabilitäts- oder IT-Sicherheitsstandards oder die Nutzung von Basisdiensten im Einvernehmen mit dem Staatsministerium der Finanzen und für Heimat und im Einvernehmen mit den sonstigen Ressorts und dem Kommunalen Digitalpakt festlegen kann. Die Regelung adressiert Standards, die in der Zuständigkeit des CIOs der

Staatsregierung liegen und trägt der diesbezüglichen Zuständigkeitsverteilung zwischen StMD und StMFH Rechnung. Nach Satz 2 ist das Landesamt für Sicherheit in der Informationstechnik zu beteiligen.

Zu Abs 2

Diese Vorschrift regelt im Abs. 2 die Umsetzung von Standardisierungsbeschlüssen, insbesondere Standardisierungsbeschlüsse des IT-Planungsrats. Gemäß § 1 Abs. 1 S. 1 Nr. 2 des Vertrages über die Errichtung eines IT-Planungsrates und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Art. 91 c GG (IT-Staatsvertrag) (Anlage des Gesetzes zu dem Staatsvertrag zur Ausführung von Art. 91 c GG), ist der IT-Planungsrat befugt, fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards zu beschließen. Diese Beschlüsse entfalten Bindungswirkung und sind vom Bund und von den Ländern in ihren jeweiligen Verwaltungsräumen umzusetzen (§ 3 Abs. 3 S. 2 IT-Staatsvertrag), sodass eine Gremienbefassung auf Landesebene wegen mangelnder Entscheidungskompetenz entbehrlich ist (LT-Drs. 15/7724, S. 76).
Die Vorgaben des IT-Planungsrates werden durch den vorliegenden „Transformationsartikel“ automatisch übernommen. Ein Diskurs über die im IT- Planungsrat behandelten Themen erfolgt innerhalb Bayerns bereits über den Rat der Ressort-CIOs. Auf Planungsratsebene werden die Belange Bayerns dann in dem föderalen Instrument und zentralen Gremium zur Einführung einheitlicher bundesweiter Standards mit eingebracht.
In Bezug auf die X-Standards bringt Bayern sich koordiniert ein, da diese Standards nach Verabschiedung des IT-PLR in Bayern gelten.
Wie bei einer Mehrzahl der Bundesländer (ausgenommen die Stadtstaaten) werden die Beschlüsse des IT- Planungsrates direkt auch für die bayerischen Kommunen bindend sein. Damit muss nicht mehr über das „ob“, sondern lediglich über das „wie“ diskutiert werden. Da sich der Freistaat mit dem Staatsvertrag von 2010 dazu verpflichtet hat, die Beschlüsse des IT- Planungsrates in seinem Verwaltungsraum, also sowohl für die staatlichen wie auch kommunalen Verwaltungen bindend einzuführen, trägt der Transformationsartikel dazu bei, die Einführungsprozesse zu beschleunigen und zu vereinfachen. Mit der weiteren Ergänzung und einem Verweis auf Abs. 1 kann eine „bayernspezifische“ Anpassung durch Rechtsverordnung vorgenommen und gesteuert werden.

Nach Abs. 2 Satz 2 kann das Staatsministerium für Digitales nach Beteiligung des Kommunalen Digitalpakts im Benehmen mit dem Staatsministerium der Finanzen und für Heimat Ausführungsbestimmungen festlegen.

Teil 5. Übergangs- und Schlussbestimmungen

Zu Art. 52 Experimentierklausel:

Der vorliegende Artikel wurde weitgehend aus dem BayEGovG übernommen. Die Experimentierklausel ermöglicht es zeitlich und räumlich begrenzte Ausnahmen von Zuständigkeits- und Formvorschriften des Landesrechts durch Rechtsverordnung des StMD im Einvernehmen mit der Staatskanzlei und den betroffenen Ressorts vorzusehen.

Inhaltlich soll die Experimentierklausel zukünftig auf die Vorschriften über die Zustellung erstreckt werden. Satz 1 Nr. 3 wird entsprechend geändert.

Zu Art. 53 Verordnungsermächtigungen:

Idee des Art. 53 ist es, eine zentrale Norm für alle Verordnungsermächtigungen zu bilden. Im Folgenden werden nur einzelne besonders erläuterungsbedürftige Nummern näher ausgeführt.

Zu Abs. 1

Abs. 1 enthält die Ermächtigungen, die die Staatsregierung treffen kann.

Zu Nummer 3:

Nummer 3 normiert eine Verordnungsermächtigung zur Umsetzung der übrigen Anforderungen der Richtlinie 2014/55/EU. Die Verordnung ist lex specialis auch zu Art. 1. Sie kann Einzelheiten der Entgegennahme und Verarbeitung der digitalen Rechnung regeln und Ausnahmen von der Verpflichtung zur Entgegennahme und Verarbeitung digitaler Rechnungen vorsehen. Dem Verordnungsgeber bleibt es damit insbesondere überlassen, näher zu regeln, ob digitale Rechnungen (in Umsetzung der Richtlinie 2014/55/EU) nur im Oberschwellenbereich entgegengenommen werden müssen oder ob (über die Verpflichtung aus der Richtlinie hinaus) sämtliche Rechnungen erfasst werden sollen. Im Rahmen einer Verordnung können zudem die erst noch auf Unionsebene festzusetzenden technischen Anforderungen an die digitale Rechnung normiert werden. Ebenso können mögliche abweichende unionsrechtliche Anforderungen an die Rechnungstellung in besonderen Fällen, z. B. im Bereich der EU-Fonds, berücksichtigt werden.

Die Bayerische Staatsregierung hat von der Verordnungsermächtigung im alten Art. 5 Abs. 2 Satz 3 BayEGovG mit § 3 Abs. 1 des Gesetzes vom 24. Juli 2020 (GVBl. S. 388) zur Änderung der Bayerischen E-Government-Verordnung (BayEGovV) vom 8. November 2016 (GVBl. S. 314, BayRS 206-1-1-D) Gebrauch gemacht.

Zu Nummer 6:

Durch Rechtsverordnung kann die Staatsregierung gem. Nummer 6 festlegen, dass die Behörden für bestimmte Verwaltungsleistungen Zugangstor-Dienste im Sinne der Art. 4 bis 7 anbieten oder Anforderungen im Sinne der Art. 9 bis 16 der Verordnung (EU) Nr. 2018/1724 einzuhalten haben.

Nummer 6 verweist damit auf die Anforderungen der Verordnung (EU) Nr. 2018/1724 – Verordnung vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012.

Die Verordnung (EU) Nr. 2018/1724 sieht die Einrichtung eines einheitlichen digitalen Zugangstores für Informationen, Online-Verfahren, Hilfs- und Problemlösungsdienste sowie Feedback und Statistik vor. In Art. 6 i. V. m. Annex II der Verordnung werden Verfahren aufgelistet, die vollständig online bereitzustellen sind. Dort wird klargestellt, was unter der vollständigen Online-Bereitstellung eines Verfahrens zu verstehen ist. Dies ist dann gegeben, wenn der Nutzer alle Interaktionen mit der zuständigen Behörde digital, aus der Ferne und über einen Online-Dienst vornehmen kann.

Unter den in der Verweisungsnorm der Nummer 6 genannten Pflichten aus der Verordnung (EU) Nr. 2018/1724 sind die Anforderungen an die vollständig digitale Abwicklung von Verwaltungsverfahren gem. Art. 6 Abs. 2, die Qualitätsanforderungen der Informationen über Rechte und Pflichten gem. Art. 9 Abs. 1 und die Qualitätsanforderungen an Informationen zum Verfahren gem. Art. 10 Abs. 1 und 2 besonders hervorzuheben.

Nach Art. 6 Abs. 2 Verordnung (EU) Nr. 2018/1724 setzt eine vollständige digitale Abwicklung voraus, dass

- die Identifizierung der Nutzer, die Bereitstellung von Informationen und die Vorlage von Nachweisen, die Signierung und die endgültige Einreichung digital aus der Ferne gewährleistet ist, wobei die Abwicklung über einen Dienstkanal erfolgen soll, der die Nutzer in die Lage versetzt, die Anforderungen im Zusammenhang mit dem Verfahren in nutzerfreundlicher und strukturierter Weise zu erfüllen,
- die Nutzer eine automatische Empfangsbestätigung erhalten, es sei denn, das Ergebnis des Verfahrens wird sofort übermittelt,
- das Ergebnis des Verfahrens digital oder — soweit zur Einhaltung geltender Vorschriften des Rechts der Union oder des nationalen Rechts erforderlich — physisch übermittelt wird, sofern das Fachrecht eine Übermittlung des Ergebnisses vorsieht, und
- die Nutzer eine digitale Benachrichtigung über den Abschluss des Verfahrens erhalten.

Nach Art. 9 Abs. 1 müssen Informationen über Rechte und Pflichten folgenden Anforderungen genügen:

- Sie müssen nutzerfreundlich sein, damit die Nutzer die Informationen leicht finden und verstehen können und
- in der Lage sind zu erkennen, welche Informationen für ihre jeweilige Situation relevant sind;
- sie müssen genau und umfassend genug sein, um die Informationen abzudecken, die die Nutzer haben müssen,
- um ihre Rechte unter vollständiger Einhaltung der geltenden Vorschriften und Pflichten auszuüben;
- gegebenenfalls enthalten sie Verweise bzw. Links zu Rechtsvorschriften, technischen Spezifikationen und Leitfäden;
- sie enthalten die Bezeichnung der zuständigen Behörde oder Stelle, die für den Inhalt der Informationen verantwortlich ist;
- sie enthalten die Kontaktangaben von allen relevanten Hilfs- oder Problemlösungsdiensten, wie z. B. eine Telefonnummer, eine E-Mail-Adresse, ein Online-Kontaktformular oder andere häufig verwendete elektronische
- Kommunikationsmittel, das für die Art des angebotenen Dienstes und die Zielgruppe dieses Dienstes am besten geeignet ist;
- sie enthalten das Datum der letzten Aktualisierung der Informationen, falls vorhanden, oder
- wenn die Informationen nicht aktualisiert wurden, das Veröffentlichungsdatum der Informationen;
- sie sind gut strukturiert und so dargestellt, dass die Nutzer die benötigten Informationen schnell finden können;
- sie sind auf dem neuesten Stand; und
- sie sind in klarer und verständlicher Sprache abgefasst, die dem Bedarf der potenziellen Nutzer angepasst ist.

Nach Art. 10 Abs. 1 und Abs. 2 müssen die Behörden den Nutzern Zugang zu einer hinreichend umfassenden, klaren und nutzerfreundlichen Erklärung folgender Elemente von Verfahren verschaffen:

- der relevanten Schritte des Verfahrens, die der Nutzer zu unternehmen hat, einschließlich etwaiger Ausnahmen gemäß Art. 6 Abs. 3 von der Pflicht der Mitgliedstaaten, das Verfahren vollständig online bereitzustellen;
- der Bezeichnung der zuständigen Behörde, die für das Verfahren zuständig ist, einschließlich ihrer Kontaktdaten;
- der für das Verfahren zulässigen Mittel zur Authentifizierung, Identifizierung und Unterzeichnung;
- der Art und des Formats der vorzulegenden Nachweise;
- der Rechtsbehelfe, die im Falle von Streitigkeiten mit den zuständigen Behörden im Allgemeinen zur Verfügung stehen;
- der anfallenden Gebühren und der Online-Zahlungsmethoden;

- etwaiger Fristen, die vom Nutzer oder von der zuständigen Behörde einzuhalten sind, und wenn es keine Fristen gibt,
- der durchschnittlichen, geschätzten oder voraussichtlichen Zeit, die die zuständige Behörde zur Abwicklung des Verfahrens benötigt;
- etwaiger Vorschriften über oder Rechtsfolgen für die Nutzer, die sich aus einer nicht erfolgten Antwort der zuständigen Behörde ergeben, einschließlich Regelungen zur Genehmigungsfiktion oder andere Verschweigensregelungen;
- jeder zusätzlichen Sprache, in der das Verfahren abgewickelt werden kann.
- Liegen keine Regelungen zur Genehmigungsfiktion oder sonstige Verschweigensregelungen oder ähnliche Regelungen vor, so unterrichten die zuständigen Behörden die Nutzer gegebenenfalls über etwaige Verzögerungen und Fristverlängerungen oder die sich daraus ergebenden Folgen.

Zu Nummer 11:

Demnach kann die Staatsregierung Einzelheiten zu Planung, Errichtung, Betrieb, Bereitstellung, Nutzung, Sicherheit und technischen Standards digitaler Verwaltungsinfrastrukturen durch Rechtsverordnung festlegen und hierbei auch die erforderlichen Regelungen zu Aufgaben und Befugnissen von Behörden treffen. Die verfassungsrechtlich gewährleistete Autonomie von kommunalen und funktionalen Selbstverwaltungskörperschaften ist zu wahren. Das Konnexitätsprinzip bleibt unberührt. Eine Befugnis zur Absenkung geltender Standards ist mit der Vorschrift nicht verbunden.

Zu Abs. 2

Abs. 2 enthält die Ermächtigungen, die das Staatsministerium für Digitales im Einvernehmen mit der Staatskanzlei treffen kann.

Zu Abs. 3

Abs. 3 enthält die Ermächtigungen, die das Staatsministerium für Digitales im Einvernehmen mit den zuständigen Fachministerien treffen kann. Die Vorschrift reflektiert die koordinierte Zuständigkeit des StMD, stellt aber auch sicher, dass Vorschriften nur mit Zustimmung der fachlich betroffenen Ressorts erlassen werden können. Damit wird der Tatsache Rechnung getragen, dass Interoperabilitätsstandards und Mindestleistungskataloge notwendig auch die Fachzuständigkeiten von Ressorts berühren.

Zu Abs. 4

Abs. 4 enthält die Ermächtigungen, die das Staatsministerium für Digitales treffen kann.

Zu Abs. 5

Die digitale Verwaltungslandschaft befindet sich im Zuge rechtlicher Änderungen (insb. OZG) in einem Veränderungsprozess. Konkrete Herausforderungen ergeben sich unter anderem daraus, dass sich die OZG-Umsetzung immer mehr als staatlich-kommunale Gemeinschaftsaufgabe erweist. Hier soll es durch die Verordnungsermächtigung möglich sein, Aufgaben hinreichend flexibel auf hierzu geeignete öffentliche Rechenzentren wie die AKDB zu übertragen. Keinesfalls darf eine Aufgabenübertragung mit einer Einbuße an IT-Sicherheit einhergehen oder der vom Ministerrat beschlossenen Konsolidierung der Rechenzentren zu wider laufen. Klarzustellen ist in diesem Zusammenhang, dass Beleihungen nichtstaatlicher Stellen mit staatlichen Aufgaben auf diesem Wege nicht erfolgen können. Durch Rechtsverordnung delegiert werden kann allenfalls technischer Support im Verwaltungsablauf, nicht aber entscheidende oder vollziehende Verwaltungszuständigkeit. Die Vorgaben des Vergaberechts sind jedoch im Einzelfall zu prüfen.

Zu Abs. 6

Die Ermächtigung ermöglicht es, durch Rechtsverordnung die Gemeinden in die Lage zu versetzen, für ihr Gemeindegebiet eine Flächenmanagement-Datenbank zu errichten. Diese unterstützt die Gemeinden dabei, die vorrangige Innenentwicklung nach § 1 Abs. 5 BauGB und § 1a Abs. 2 BauGB und das Ziel 3.2 des Landesentwicklungsprogramms Bayern (LEP) umzusetzen. Mit Hilfe einer Flächenmanagement-Datenbank können die vorhandenen Innenentwicklungspotenziale erfasst und Baulücken, Brachflächen und Leerstände einer neuen Nutzung zugeführt werden. Dabei können auch Regelungen für die weitere Verwendung personen- und grundstücksbezogener Daten getroffen werden.

Zu Art. 53a Änderung weiterer Rechtsvorschriften

Zu Abs. 1 Änderung des Kostengesetzes

Mit der Neuregelung im KG soll dem Äquivalenzprinzip Rechnung getragen werden. Der digitale Verwaltungsweg im Sinne des Art. 20 ist für die öffentliche Hand zumindest mittelfristig günstiger, die entsprechende Kostenersparnis soll daher an den Bürger weitergereicht werden. Zudem soll dem Bürger für die Nutzung des digitalen Wegs eine Kostenersparnis gewährt werden, um so auch monetäre Anreize zu geben, den digitalen Weg zu beschreiten. Für eine Zeit- und damit auch Kostenersparnis ist es bereits ausreichend, wenn der Bürger den Antrag digital einreicht (Hinkanal).
Für die entsprechende Bestimmung zur Ermäßigung bietet sich das Kostenverzeichnis (KVz) zum Kostengesetz (KG) an, das gemäß Art. 5 Abs. 1 Satz 1 KG vom Staatsministerium der Finanzen und für Heimat im Benehmen mit den betroffenen Ressorts erlassen wird. Die Verringerung der jeweils festgesetzten Gebühr darf dabei 100 € nicht überschreiten. Das Kostenverzeichnis bietet als Rechtsverordnung die nötige

Flexibilität, den vorgesehenen Ermäßigungsrahmen adäquat auszufüllen. Die Ergänzung soll bei den Allgemeinen Bestimmungen als Lfd. Nr. 1.II.2/ KVz verortet werden. Die Regelung des Art. 5 Abs. 2 Satz 4 und 5 betreffen den Bereich der Gebühren für Amtshandlungen. Durch die Ergänzung des Art. 21 Abs. 3 Satz 1 wird erreicht, dass die Ermäßigungsmöglichkeiten auch für die Benutzungsgebühren nach Art. 21 anzuwenden sind.

Zu Abs. 2 Änderung der Gemeindeordnung

Zu Nummer 1:

Das amtliche Publikationswesen durchläuft einen grundlegenden Wandel von der papiergebundenen hin zur elektronischen Veröffentlichung. Das Bayerisches Digitalgesetz erlaubt es in Art. 18 Abs. 3 Satz 2 grundsätzlich, veröffentlichungspflichtige Mitteilungen und amtliche Verkündungen ausschließlich in elektronischer Form zu veröffentlichen, soweit dem keine Rechtsvorschriften entgegenstehen. Die elektronische Bekanntmachung gemeindlicher Satzungen ist bisher nur zusätzlich, nicht aber als Alternative erlaubt. Insofern stellt Art. 26 Abs. 2 GO eine entgegenstehende Vorschrift im Sinne von Art. 23 Abs. 3 Satz 2 dar. Sollen gemäß der Intention des Bayerischen Digitalisierungsgesetzes auch hier die Vorteile genutzt werden, die die Digitalisierung bietet, bedarf es der Änderung der GO, soweit für die Bekanntmachung von Satzungen bislang die Bekanntgabe in Druckwerken vorgesehen ist. Durch die Streichung des Wortes „anderen“ wird klargestellt, dass die Amtsblätter der Gemeinden, der Verwaltungsgemeinschaften, des Landkreises und des Landratsamtes auch dann nicht mehr als Druckwerk erscheinen müssen, wenn darin eine Satzung bekanntgemacht wird. Nur noch alternativ kann auf regelmäßig erscheinende Druckwerke wie Tageszeitungen zurückgegriffen werden, wenn die Bekanntmachung in einem der genannten Amtsblätter ausscheidet. Amtsblätter können dann auch nur elektronisch veröffentlicht werden, selbst wenn sie Satzungen enthalten.

Zu Nummer 2:

Durch die Ergänzung von Art. 26 Abs. 2 Satz 2 Halbsatz 2 Alternative 1 GO können die Gemeinden und Verwaltungsgemeinschaften für die Bekanntmachung ihrer Satzungen unter den Vorbehalten des Art. 23 Abs. 3 Satz 2 den Weg der ausschließlichen elektronischen Bekanntmachung wählen.

Zu Nummer 3:

Die Änderung erleichtert es den Gemeinden, öffentliche Aufträge und Konzessionen elektronisch abzuwickeln.

Zu Abs. 3 Änderung der Landkreisordnung

Die Änderung erleichtert es den Landkreisen, öffentliche Aufträge und Konzessionen elektronisch abzuwickeln.

Zu Abs. 4 Änderung der Bezirksordnung

Die Änderung erleichtert es den Bezirken, öffentliche Aufträge und Konzessionen elektronisch abzuwickeln.

Zu Abs. 5 Änderung des Gesetzes über die kommunale Zusammenarbeit

Zu Nummer 1:

Da für öffentlich-rechtliche Willenserklärungen unter anderem die De-Mail als Schriftformersatz zugelassen ist (vgl. Art. 3a Abs. 2 Satz 4 Nrn. 2 und 3 BayVwVfG) und sich für zivilrechtliche Willenserklärung die Notwendigkeit der qualifizierten elektronischen Signatur aus § 126a BGB ergibt, kann der Verweis auf die qualifizierte elektronische Signatur in Art. 37 Abs. 1 KommZG gestrichen werden.

Zu Nummer 2:

Die Änderung dient der redaktionellen Anpassung an die Vorschriften zu Verpflichtungserklärungen der anderen kommunalen Gesetze.

Zu Nummer 3:

Die Änderung erleichtert es den Zweckverbänden, öffentliche Aufträge und Konzessionen elektronisch abzuwickeln.

Zu Nummer 4 und Nummer 5:

Es handelt sich um eine redaktionelle Anpassung aufgrund des neu einzufügenden Halbsatzes 2 in Art. 37 Satz 1 KommZG.

Zu Abs. 6 Änderung des Bayerischen Besoldungsgesetzes

Die Streichung des Zustimmungserfordernisses des Beamten/der Beamtin zur elektronischen Bereitstellung von Bezügemitteilungen als Voraussetzung der Zugangsfiktion ist erforderlich, da der Freistaat Bayern nach Art. 20 Abs. 3 als Dienstherr bzw. Arbeitgeber Verwaltungsdienstleistungen im Bereich der Personalverwaltung und Personalwirtschaft gegenüber seinen Beschäftigten ausschließlich elektronisch anbieten und erbringen kann.

Zu Art. 53b Änderung des Bayerischen Digitalgesetzes

Art. 53b knüpft an Art. 6 BayEGovG an, entwickelt die Pflicht zur digitalen Verfahrensdurchführung jedoch deutlich weiter.

Zu Abs. 1

Im Abs. 1 Satz 1 wird angeordnet, dass Behörden geeignete Verwaltungsverfahren oder Teile hiervon zur Erfüllung staatlicher und staatlich übertragener Aufgaben auch digital durchführen. Die Vorschrift entwickelt die schon bisher in Art. 6 Abs. 1 BayEGovG enthaltende Verpflichtung aller Behörden weiter, ihre Verwaltungsleistungen auch digital anzubieten. Diese Verpflichtung umfasst sowohl die digitale Antragstellung im „Hinkanal“ als auch die digitale Rückübermittlung auf Verlangen des Adressaten im „Rückkanal“. Der bisherige generelle Zweckmäßigkeits- und Wirtschaftlichkeitsvorbehalt des Art. 6 Abs. 1 BayEGovG wird in Satz 2 nunmehr im Wesentlichen auf den Selbstverwaltungsbereich beschränkt. Zum Begriff der „Geeignetheit“ siehe hierzu bereits unter Art. 17 Abs. 1.

Die Änderungen des Normtextes dienen in erster Linie der Klarstellung der ohnehin bereits nach Art. 6 Abs. 1 BayEGovG bestehenden Behördenpflichten. Die Zweckmäßigkeit einer auch digitalen Bereitstellung von Verwaltungsverfahren dürfte selten zu verneinen sein. Auch der bisherige allgemeine Wirtschaftlichkeitsvorbehalt kann angesichts der Fortschritte der Digitalisierung, der aktiven Fördermaßnahmen des Freistaates und der im Gesetz neu verankerten Unterstützungsmaßnahmen des Freistaates weitgehend ins Leere laufen. Die Verpflichtung der Behörden auch zur digitalen Rückübermittlung setzt allerdings voraus, dass der Adressat die entsprechenden Voraussetzungen in seiner Sphäre (Nutzerkonto) schafft.

Zu Abs. 2

Abs. 2 Satz 1 regelt die Verpflichtung zur Bereitstellung von online ausfüllbaren elektronischen Formularen über das Internet als Teil des digitalen Verwaltungsverfahrens. Die Vorschrift greift nur bei formulargebundenen Verfahren. Der Begriff der Verwaltungsleistung orientiert sich am OZG, siehe auch Art. 53 Abs. 1 Nr. 8.

Abs. 2 Satz 1 definiert eine Mindestanforderung an die digitale Bereitstellung von Verwaltungsangeboten. Konsequenter Weise greift die Vorschrift gem. Abs. 2 Satz 2 nicht ein, wenn die Behörde Verwaltungsleistungen nicht nur als Online-Formular, sondern als „vollständig digitalen“ Prozess im Sinne des sog. „OZG Reifegradmodells“ anbietet. Nach dem „Reifegrad Modell“ ist von einer „vollständig digitalen“ Abwicklung im Sinne des § 1 OZG ist auszugehen, wenn eine Verwaltungsleistung zumindest den „Reifegrad 3“ erfüllt. Erforderlich hierfür ist, dass Antrag und Nachweise elektronisch eingereicht und der Bescheid im Rückkanal elektronisch bekanntgegeben werden kann (siehe: https://leitfaden.ozg-umsetzung.de/display/OZG/2.2+Digitale+Services+im+

Sinne+des+OZG, abgerufen am 20.02.2021). Im Ergebnis soll Abs. 2 Satz 2 verhindern, dass die Behörden ein und denselben Antrag mehrfach digital anbieten müssen, einmal als digitales Formular und einmal als Online-Antrag im Sinne des OZG.

Mit Satz 3 wird klargestellt, dass nur dann ein Schriftformerfordernis vorliegt, wenn dies explizit in der Norm angeordnet wird. Ein bloßes Unterschriftsfeld in einem Formular begründet dagegen noch kein Schriftformerfordernis.

Zu Art. 54 Einschränkung von Grundrechten

Hier sind keine Änderungen erfolgt im Vergleich zum BayEGovG. Das Fernmeldegeheimnis könnte verletzt werden, wenn durch das LSI Daten eines Telekommunikationsvorgangs zwischen einem Bürger und einer staatlichen oder kommunalen Behörde ausgewertet werden.
Nach Art. 19 Abs. 1 Satz 2 i. V. m. Art. 10 Grundgesetz dürfen Beschränkungen des Fernmeldegeheimnisses nur aufgrund eines Gesetzes angeordnet werden, das wiederum das Grundrecht unter Angabe des Artikels nennen muss.

Zu Art. 55 Inkrafttreten, Außerkrafttreten

Enthält Regelungen zum Inkraft- bzw. Außerkrafttreten.Das Außerkrafttreten der Art. 53a und Art. 53b 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.