Industrie- und Handelskammern
in Bayern

Stellungnahme der bayerischen Industrie- und Handelskammern zum Entwurf des Bayerischen Digitalgesetzes (BayDiG), Version 06.07.2021

A. Allgemeines

Die bayerischen IHKs begrüßen den vorliegenden Entwurf des Bayerischen Digitalgesetzes als umfassenden, allgemeinen Rechtsrahmen für die Digitalisierung von Gesellschaft, Wirtschaft, Staat und Verwaltung ausdrücklich. Damit geht Bayern nicht nur bundesweit voraus für einen digital erfolgreichen Standort.

Bürokratieabbau durch eine effiziente und digitale öffentliche Verwaltung sehen die bayrischen Unternehmen als dringendste Aufgabe für die nächste Bundesregierung. Dies zeigt auch die Befragung der bayerischen IHKs unter mehr als 1.300 Unternehmen aus Industrie, Handel und Dienstleistungen zu ihren Erfahrungen während der Corona-Pandemie sowie deren Forderungen an die Politik.
Darüber hinaus liegt viel Potenzial in der Stärkung der Digitalisierung am Standort. Nur so kann international im Digitalbereich Wettbewerbsfähigkeit erreicht werden. Hierfür liefert das Gesetz wichtige Regelungen.

Das Gesetz umfasst viele der auschlaggebenden Themen zur Digitalisierung. Allerdings wird hierzu im Gesetzentwurf häufig die Konkretisierung und Verbindlichkeit vermisst, die zu klaren Zielen, Regelungen und Maßnahmen führen müssen. Diese sollen, wo möglich, im Gesetz noch nachgeschärft oder zügig im Nachgang via Rechtsverordnungen und Maßnahmenpakete definiert werden. Um die Potenziale der Digitalisierung für Unternehmen nicht weiter verstreichen zu lassen, muss Bayern hier schnell agieren.

Gerade vor dem Hintergrund der laufenden Umsetzungsfristen für das Onlinezugangsgesetz (OZG) bis Ende 2022 besteht hoher Bedarf für eine möglichst zeitnahe und klare Definition der gesetzlichen Vorgaben, die die öffentliche Verwaltung in Bayern bei der Digitalisierung ihrer Leistungen berücksichtigen muss.
Wir regen daher zunächst an, das Gesetzgebungsverfahren so zügig wie möglich zum Abschluss zu bringen.

Zu berücksichtigen sind in einer digitalen Welt aber einheitliche gesetzliche Standards statt föderaler Diversität. Letztere würde Unternehmen, die bundes- bzw. EU-weit vertreten sind, in nicht zumutbarer Weise bürokratisch belasten. Unternehmen wie Verwaltung (insbesondere bundesweit organisierte öffentliche Stellen wie Industrie- und Handelskammern) benötigen hier einheitliche Rechtsrahmen und Rechtssicherheit. Für IHKs ist dies mit Blick auf das IHKG von besonderer Bedeutung. Denn

hiernach können IHKs zum einen Aufgaben an den DIHK (§ 11 Abs. 2 Nr. 4 a IHKG) bzw. an eine andere IHK oder an öffentlich-rechtliche Zusammenschlüsse in anderen Bundesländern (§ 10 Abs. 3, § 11 Abs. 2b IHKG) übertragen. Unterschiedliche rechtliche Spielregeln auf Landesebene wären hier kontraproduktiv. Insofern sollte ein Bayerisches Digitalgesetz bitte abgestimmt werden mit geplanten/vorhandenen EU-Regelungen (z. B. ePrivacy-VO, Digital Services Act, Digital Single Gateway-VO) und mit den noch fehlenden Digitalgesetzen des Bundes und der weiteren Bundesländern. Benötigt wird ein einheitlicher und übergreifender Rechtsrahmen. Bei länderübergreifenden Verfahren muss sichergestellt werden, dass ein Datenaustausch bzw. eine Datenübertragung mit anderen Bundes- bzw. EU-Ländern technisch reibungslos möglich ist.

Bundesweit einheitliche digitale IHK-Leistungen und Basiskomponenten

Mit ihrem eigenen E-Government-Programm haben die Industrie- und Handelskammern beispielsweise eine gemeinsame IT-Basisinfrastruktur mit Basiskomponenten wie einem Unternehmensverzeichnis als Grundlage für z. B. verschiedene Registerprojekte und Erlaubnisverfahren entwickelt. Gegenwärtig wird an weiteren bundesweit einheitlichen Basiskomponenten gearbeitet und an der Umsetzung von digitalen IHK-Leistungen im Rahmen der OZG-Umsetzung.
In den Fällen, in denen die IHKs hoheitliche Aufgaben erfüllen, tun sie dies meist in unmittelbarer Umsetzung von Bundesrecht (z.B. Prüfungen), ohne dass es dazu eines Erlasses von Ausführungsgesetzen des Landes bedarf, wie z. B. im Bereich der Berufsbildung. Eine bundesweit einheitliche Ausführung kann aber nur gelingen, wenn dafür auch eine länderübergreifend einheitliche Infrastruktur im IT-Bereich vorhanden ist. Zum einen erwarten die Unternehmen dies von den IHKs, zum anderen ist sie aber auch für die Einheitlichkeit des Verwaltungshandelns der IHKs notwendig. Eine Zersplitterung durch landesgesetzliche Vorgaben bei der IT-Nutzung (wie eine Mitnutzungsverpflichtung von z. B. Basiskomponenten der Länder) würde ein bundesweit einheitliches Vorgehen verhindern.
Eine Ausnahmeregelung für IHKs bzgl. der einheitlichen Nutzung von Diensten sollte hierergänzt werden.

Die IHKs in Bayern setzen ein eigenes IHK-Portal für ihre Kunden um, das mit dem Portalverbund interoperabel sein soll. Die im vorliegenden Gesetzentwurf und in den daraus folgenden Verordnungen getroffenen Regelungen sollten dem nicht entgegenstehen. Eine engmaschige Abstimmung sollte sichergestellt werden.

B. Zu den Vorschriften im Einzelnen

Zu Teil 1, „Allgemeiner Teil“
Kapitel 1, „Allgemeines, Digitalstandort, Digitale Technologien“

Artikel 1 Abs. 2 Nr. 4, Ausnahmen vom Anwendungsbereich
In Anbetracht der Vielzahl von (meist bundesweit geregelten) Prüfungsverfahren der IHKs ist eine explizite Ausnahmeregelung hierfür zu begrüßen.

Artikel 2: „Förderung der Digitalisierung“
Die hier aufgeführten, in der Begründung ganz treffend genannten „Metaziele“ sind allesamt wichtige, teilweise grundlegende Aspekte, die zum Erfolg der Digitalisierung des Standortes Bayern erheblich beitragen. Eine Voranstellung dieser Metaziele im Gesetz ist grundsätzlich zu begrüßen – ebenso wie die inhaltliche, nicht abschließende Auswahl.
Allerdings fehlt es durchweg an konkreten Maßnahmen oder Regelungen zur Erreichung dieser Ziele.
Der Verweis auf den Digitalplan (Art. 15) führt erstmal nicht zu einer Konkretisierung.

Solche Konkretisierungen könnten beispielhaft wie folgt ausgeführt werden:

Zu Punkt 3:
Die Maßnahmen des Freistaates Bayern zielen insbesondere auf die Förderung der digitalen Daseinsvorsorge, insbesondere leistungsfähiger digitaler Infrastrukturen
Die Grundlage für digitales, mobiles Arbeiten und für automatisierte mobile Lösungen von und für Unternehmen in Bayern ist ein sehr leistungsfähiges, stabiles und **schnelles Mobilfunknetz** für Telefonie und Daten. Dass diese Voraussetzung in Bayern noch nicht gegeben ist, zeigten mehrfach Umfragen unter den IHK-Mitgliedsunternehmen.
Konkret kann dies gelingen durch:

- **Mobilfunkstrategie des Freistaats formulieren**
  Für einen schnellen und erfolgreichen Mobilfunkausbau müssen die aktuell vielfältig in verschiedenen Ressorts und Verwaltungsebenen verteilten und regional mit unterschiedlichen Prioritäten versehen staatlichen Handlungsoptionen zusammengeführt und konsequent gemeinsam ausgerichtet werden. Dafür braucht es ein deutliches Bekenntnis aller beteiligten Akteure, Bayern innerhalb von zwei Jahren zum digitalen Mobilfunk-Spitzeninfrastrukturstandort machen zu wollen.
- **Informations- und Kommunikationsmaßnahmen ausweiten**
  In vielen Kommunen stockt der Ausbau, da Bedenken gegenüber Mobilfunkausbau bestehen. Um Mobilfunk-Mythen besser entgegentreten zu können und einer eher unentschlossenen Bevölkerung den Nutzen von Mobilfunkausbau präsenter zu machen, braucht es leicht verständliche und breit kommunizierte Informationen und eine dazugehörige Kommunikationskampagne.
- **Mehr Standorte für Mobilfunkinfrastruktur bereitstellen**
  Netzbetreiber berichten von großen Schwierigkeiten, Standorte zu finden bzw. bestehende zu bewahren. Kommunen sehen Unsicherheiten in Umgang und Gestaltung von Regelungen bei einer Bereitstellung von Standorten für Mobilfunkinfra-

struktur. Es braucht eine klare Ausrichtung der öffentlichen Hand, Mobilfunkstandorte zur Verfügung zu stellen und die Bereitstellung durch klare Richtlinien und ggf. durch einen zentralen Ansprechpartner für Problemfälle zu befördern.

- **Genehmigungsprozesse beschleunigen**
  Für den Aus- bzw. Aufbau des 4G/5G-Netzes sind viele neue Antennen nötig. Die dafür nötigen Genehmigungen dauern in der Regel 12 bis 24 Monate. Die Bundesregierung formulierte im Juni 2020 das Ziel, dies auf 3 Monate zu reduzieren. Um dies in Bayern zügig zu erreichen, braucht es praktikable Leitfäden auf Basis von Best Practice-Erfahrungen aus Kommunen. Standardisierte Prozesse und digitale Abwicklung sind zügig zu etablieren. Dafür sollen – analog zu den Breitbandpaten für das Festnetz - in den Landratsämtern Genehmigungsspezialisten für den Mobilfunkausbau benannt werden, die für Kommunen auch erster Ansprechpartner zum Mobilfunkausbau sind.
- **Innovationen mit 5G fördern**
  Die Innovationskraft von 5G soll sich schnell und in der Breite entfalten können. Insbesondere kleineren Unternehmen muss 5G zugänglich gemacht werden. In Pilot-Gründerzentren sollen 5G-Campusnetze aufgebaut und Nutzungskonzepte entwickelt werden, die sowohl Gründern als auch KMUs als Testumgebungen zugänglich sind.
  Unternehmen, insbesondere kleinere, sollen über die Möglichkeiten von 5G informiert und zur Konzeption eigener 5G-Anwendungen motiviert werden.

Zu Punkt 11:

Die Maßnahmen des Freistaates Bayern zielen insbesondere auf die Stärkung der IT-Sicherheit in Staat, Verwaltung und Wirtschaft
Die Details hierzu in der Begründung listen richtige Maßnahmen wie die Verbesserung der staatlichen IT-Sicherheit (LSI), der besseren Cybercrime-Bekämpfung (ZAC, Polizei) und dem Ausbau der Forschung für die IT-Sicherheit.
Leider adressiert das BayDiG nicht, wie die präventive Informationssicherheit der Wirtschaft unterstützt und verbessert werden kann. Vorhandene Ansätze wie z. B. die Förderung von IT-Sicherheit über den Digitalbonus bleiben unerwähnt.

Für Unternehmen ist eine zentrale Lotsen- und Anlaufstelle, die die Angebote zur IT-Sicherheit zentral koordiniert und ein schnell verständliches Angebot für Unternehmen zusammenstellt, sehr wünschenswert. Hierfür könnten das Angebot des Landesamtes für Informationssicherheit (LSI) oder auch die Initiative „Online – aber sicher!“ ausgebaut werden. Als erste Anlaufstelle und neutraler Ansprechpartner für Unternehmen sollte diese Einheit in einer Klammerfunktion sowohl Angebote des Freistaats, des Bundes und der EU, als auch hilfreiche privatwirtschaftliche Angebote einbeziehen, sodass im Präventions- wie auch im Krisenfall Unternehmen schnell einen Überblick über ihre Handlungsoptionen bekommen. Auf EU- und Bundesebene sollen die Angebote für Unternehmen zur IT-Sicherheit ebenfalls ausgebaut und mit den bayerischen Aktivitäten eng verzahnt werden.

Artikel 3, Abs. 4: Freie Software

Die Absicht, das Innovationspotenzial freier Software noch besser zu heben und in der eigenen Software-Beschaffung mit gutem Beispiel voranzugehen ist zu begrü-

ßen. Auch das grundsätzliche Ziel, bei der Softwareauswahl Abhängigkeiten von Software-Anbietern zu minimieren, um „Lock-in-Effekte“ z. B. durch Interoperabilität zu vermeiden, ist zu befürworten.
Allerdings zeigen Beispiele wie die OpenSource-Projekte großer Kommunen oder die Veränderung von Lizenzbedingungen (ehemals OpenSource-Software geht in Richtung proprietärer Software, wie z. B. Java), dass das Kriterium „Open Source“ nicht alleine entscheidend ist, um flexibel zu bleiben.
Entscheidende Kriterien sind weniger die Lizenzfragen (proprietär, welche Open Source Lizenz…), sondern die Eigenschaften der Software (z. B. Sourcecode öffentlich einsehbar, Interoperabilität mit anderer Software, Verwendung von Standards & Schnittstellen, Kosten im Zuge der Migration und zukünftigen Weiterentwicklungen etc.).
Zudem wird im Gesetzestext von „offener Software“ gesprochen, in der Begründung u. a. von „freier Software“. Einheitliche und eindeutig definierte Begrifflichkeiten sind wünschenswert.
Änderungsvorschlag:
Die Behörden des Freistaates Bayern sollen bei Neuanschaffungen Software auswählen, die transparent, zukunftsfähig und interoperabel ist, soweit dies wirtschaftlich und zweckmäßig ist. Den Gemeindeverbänden und Gemeinden wird gleiches empfohlen.

Artikel 6: Nachhaltigkeit

Neben den genannten Aspekten liegt ein effektiver Hebel auch im Betrieb klimaeffizienten Rechenzentrumsflächen und entsprechendem Erwerb von Servern.

Zu Teil 1, „Allgemeiner Teil“
Kapitel 2, „Digitale Rechte und Gewährleistungen“

Artikel 8: Freier Zugang zum Internet

Die Formulierung „Jede Person hat das Recht auf freien Zugang zum Internet über allgemein zugängliche Netze.“ wird als subjektives Abwehrrecht formuliert.
Dabei sollte klargestellt werden, dass mit „Person“ auch Unternehmen als juristische Personen gemeint sind.
Zudem stellt sich die Frage, ob statt „freien Zugang zum Internet“ alternativ „diskriminierungsfreier Zugang zum Internet“ eine treffendere Bezeichnung ist.

Artikel 10: Digitale Selbstbestimmung

In der Begründung wird der Aspekt der Nutzerfreundlichkeit deutlich mehr hervorgehoben als Ziel dieses Artikels als er im Gesetzestext herauszulesen ist. Hier sollte bereits im Gesetzestext die Gewährleistung der Nutzerfreundlichkeit digitaler Angebote deutlicher aufgenommen werden, z. B. mit der Verpflichtung, bei der Entwicklung / Überarbeitung digitaler Verwaltungsangebote grundsätzlich durch geeignete Maßnahmen den zukünftigen Kunden / Nutzer der Anwendung mit einzubeziehen.

Artikel 11: Digitale Identität

Es gibt inzwischen einige auf Basis der DSGVO aufgebauter Anbieter digitaler Identitäten in der EU oder Deutschland im Speziellen.
Eine rechtsverbindliche staatliche digitale ID ist zu begrüßen, die eine hohe Vertraulichkeit bei der Nutzung digitaler Dienste gewährleistet. Der Nutzer sollte hier aber frei entscheiden können. Damit muss gleichzeitig die Interoperabilität mit bestehenden Angeboten von privaten, europäischen Anbietern sichergestellt sein, da sonst eine staatliche ID in Konkurrenz zu den privaten Angeboten treten würde, was abzulehnen ist.
Die Verwendung von staatlichen Identitätsdiensten soll mittelfristig auch bei privatwirtschaftlichen digitalen Angeboten zur Anwendung kommen können.

Rechte und Pflichten einer digitalen Identität sollte Regelungen analog zu denen für natürliche und juristische Personen finden.

Artikel 15: Digitalplan, Digitalbericht

Sofern ein Digitalplan von allen Ressorts unterstützt wird, verspricht er ein hilfreiches Instrument zu sein, die oft ressortübergreifend notwendigen Maßnahmen zur Digitalisierung (z.B. Mobilfunkausbau) festzuschreiben. Allerdings fehlt auch hier ein Mindestmaß an Konkretisierung, z.B. zu Inhalt, Verbindlichkeit,…
Die in Abs. 2 benannte Frist von drei Jahren zur ersten Berichtspflicht zum Digitalplan ist deutlich zu lang gefasst. Dies sollte mindestens jährlich erfolgen ab Inkrafttreten dieses Gesetzes.

Zu Teil 2, „Digitale Verwaltung“
Kapitel 2, „Digitales Verwaltungsverfahren“

Zu Artikel 17, Absatz 3: Digitale öffentliche Dienste
Für die Gewährleistung der Integrität digital bekannt gemachter veröffentlichungspflichtiger Mitteilungen und amtlichen Verkündungsblätter können Blockchain-Lösungen wie das mit der IHK für München und Oberbayern, dem Bayerischen Digitalministerium, der HWK für München und Oberbayern und der Landeshauptstadt München entwickelte Cert4Trust eingesetzt werden.

Eine „auch“ digitale Bekanntmachung darf nicht zu Rechtsunsicherheiten führen. Es muss für den Norm- bzw. Mitteilungsadressaten klar sein, welches Medium das verbindliche ist. Ggf. müsste hier im Einzelfall zwischen formaler Bekanntmachung und zusätzlicher digitaler Veröffentlichung unterschieden werden.

Zu Artikel 18 Abs. 1, Halbsatz 2: „Digitale Zahlungsabwicklung und Rechnungen“

Wie in der Begründung weiter ausgeführt, sind die Behörden verpflichtet, die Begleichung von Gebühren und sonstigen Forderungen auch durch Bereitstellung von in den Antragsprozess integrierten digitalen Zahlungsmöglichkeiten bereitzustellen. Dieses begrüßenswerte Ziel erfordert aber ggf. auch Änderungen an anderer Stelle. So entsteht ein Kostenanspruch nach dem Kostengesetz erst mit der Beendigung der Amtshandlung. Damit ist die Integration von Bezahlungen in ein Antragsverfahren, z.B. in Form einer Vorkasse, zwar technisch abbildbar, stößt aber ggf. an andere rechtliche Grenzen.

Zu Artikel 19, Absatz 3: Digitale Verfahren
Die Identifizierung in digitalen Verwaltungsverfahren unter den hier genannten Anforderungen ist nach dem Wortlaut der Vorschrift in zwei Fällen erforderlich:

- wenn die Identität einer Person auf Grund einer Rechtsvorschrift festzustellen ist (Fall 1).
- wenn aus anderen Gründen eine Identifizierung für notwendig erachtet wird (Fall 2).

Diese Formulierung wirft eine Reihe von Fragen auf:

- Zu Fall 1:
  - Soll dies nur dann gelten, wenn gesetzlich (wie z. B. in § 150 e Absatz 2 Satz 1 GewO) explizit eine Identitätsfeststellung gemäß PAuswG, AufenthG und eID-Karte-Gesetz vorgesehen ist? Wenn ja, regen wir an, die Vorschrift hier eindeutig zu fassen, z. B. „*in denen sie die Identität einer Person nach § 18 PAuswG, § 78 Absatz 5 AufenthG oder § 12 eID-Karte-Gesetzes auf Grund einer Rechtsvorschrift festzustellen haben“.*
  - Oder soll dies in allen Fällen gelten, in denen eine Rechtsvorschrift eine Identifizierung oder Authentifizierung vorschreibt (z. B. Artikel 6 Absatz 4 Satz 2 BayEGovG und § 9 Absatz 1 Satz 2 OZG)? Wir regen an, hierzu

Ausführungen in die Gesetzesbegründung aufzunehmen, da diese Frage für die Behörden in Bayern von großer Bedeutung ist. Problematisch in diesem Zusammenhang ist insbesondere auch die uneinheitliche Verwendung von Begrifflichkeiten wie „Identitätsfeststellung“, „Identifizierung“ und „Authentifizierung“.

- Zu Fall 2:
  - Soll dies in allen Fällen gegeben sein, in denen gesetzliche Regelung eine Identifizierung und/oder Authentifizierung vorschreiben, die nicht den Anforderungen nach § 18 PAuswG oder § 78 Absatz 5 AufenthG entsprechen muss (z. B. Artikel 6 Absatz 4 Satz 2 BayEGovG und § 9 Absatz 1 Satz 2 OZG)?
  - Oder nur dann, wenn gesetzliche Regelungen explizit eine Identifizierung vorschreiben?
  - Oder in allen Fällen, in denen ein hohes Vertrauensniveau gemäß der Technischen Richtlinie TR-03107-1 zu beachten wäre? Sofern die Vorschrift in diesem Sinne ausgelegt werden soll, sehen wir eine klare Verankerung im Gesetzeswortlaut für erforderlich an.

Wir bitten hierzu zumindest um klarstellende Ausführungen in der Gesetzbegründung.

Zu Abs. 3 Ziff. 4:
Für die Identifikation in digitalen Verfahren, für die keine Rechtsvorschrift zur Feststellung der Identität existiert, sollen – je nach benötigtem Vertrauensniveau – auch andere technische Systeme genutzt werden.
Hier ist die Einschränkung im vorliegenden Gesetzentwurf auf andere sichere Verfahren, die gesetzlich oder durch Rechtsverordnung der Staatsregierung zugelassen sind, viel zu weit gehend und baut dabei unnötige Hürden für die Akzeptanz von E-Government-Lösungen auf.
Z. B. bei einem Verfahren mit normalem Vertrauensniveau müssen auch einfachere Lösungen zur Identifizierung möglich sein, die nicht alle aufwändig durch die Staatsregierung zugelassen werden müssen. Vielmehr muss in solchen Fällen auch die Möglichkeit bestehen, mit einfachen Standard-Lösungen eine Identifizierung und Authentifizierung durchzuführen. Der Grundsatz des „Once Only“ sollte auch hier greifen. Zusätzliche Regelungen der Staatsregierung („gesetzlich oder durch Rechtsverordnung“) bedarf es nicht, wenn hier auf die DSGVO und deren Regelungen für eine angemessene Sicherheit verwiesen würde. So könnte Ziff. 4 entweder dahingehend umformuliert werden, dass andere sichere Verfahren den Datenschutzregelungen (Art. 32 DSGVO bzw. Spezialvorschriften wie TKG) entsprechen müssen oder es könnte „im Übrigen auf die nach Art. 43 Abs. 1 S. 2 bestehende Verpflichtung zur Gewährleistung von angemessener Sicherheit“ verwiesen werden.

Zu Art. 20 Abs.3: Digitale Verfahren als Regelfall
Die Begründung führt aus, dass die Regelung des Absatzes 3 auch die unter Aufsicht des Freistaates stehenden juristischen Körperschaften gilt. Diese weite Aussage deckt sich nicht mit dem Wortlaut des Gesetzentwurfs.

Zu Teil 2, „Digitale Verwaltung“
Kapitel 3, „Portalverbund Bayern“

Artikel 21: Digitale Assistenzdienste
Industrie- und Handelskammern setzen überwiegend digitale Assistenzdienste ein, die eine IHK-Gemeinschaftseinrichtung, ein Tochterunternehmen der DIHK oder eine IHK entwickelt hat. Insofern regen wir an, Art. 21 über einen Absatz 3 wie folgt zu ergänzen: „Körperschaften des öffentlichen Rechts dürfen digitale Assistenzdienste zulassen und einsetzen, welche organisationsintern entwickelt wurden. Diese sind bekannt zu machen. Die Vorgaben des Art. 21 Abs. 2 sind hierbei zu beachten.“

Artikel 22: Zustimmung im digitalen Verfahren
Die Datenschutzgesetze (DSGVO, BayDSG, OZG u. a.) verwenden ausschließlich den Begriff „Einwilligung“ statt „Zustimmung“. In Anlehnung an dieses einheitliche Wording sollte dieser Begriff durchgängig auch im BayDIG verwendet werden. Daher sollten z. B. in Art. 22, Art. 23 Abs. 2 S. 1 -E und in Art. 30 Abs. 2 BayDIG-E der Begriff „Zustimmung“ durch „Einwilligung“ ersetzt werden.

Art. 24 Abs. 1: Bekanntgabe über Portale
Bei der Bekanntgabe von Verwaltungsakten sollte ein einheitliches Wording verwendet werden. Art. 24 Abs. 1 S. 1 BayDiG-E regelt, dass Bescheide „dem Beteiligten oder einem von ihm benannten Dritten“ bekannt gegeben werden. § 9 Abs. 1 S. 1 OZG spricht vom „Nutzer und seinem Bevollmächtigten“. Die Bekanntgabe über ein Portal/elektronisches Postfach setzt eine Einwilligung voraus. Die Personen, an die hier über ein Portal/elektronisches Postfach Bescheide bekannt gegeben werden dürfen, sind in einer Einwilligung korrekt anzugeben. Ist das Wording in zwei gesetzlichen Vorschriften unterschiedlich, stehen öffentliche Stellen spätestens bei der Formulierung einer rechtswirksamen Einwilligungserklärung vor einem nicht lösbaren Konflikt. Der Punkt ist wichtig, da es sich um einen wesentlichen Bestandteil einer Einwilligung handelt, d. h. es geht um eine Wirksamkeitsvoraussetzung. Eine unzureichende Angabe kann zur Unwirksamkeit einer Einwilligung führen, Eine Bekanntgabe eines Verwaltungsaktes wäre in einem derartigen Fall mangels rechtkonformer Einwilligung nicht wirksam.

Artikel 26, Absatz 1: Portalverbund Bayern
Für mehr Klarheit sollte in diesem Artikel inkl. der folgenden aufgenommen werden, dass Elemente des Portalverbund Bayerns auch die Vielzahl von kommunalen Portalen und Fachportalen, wie z.B. das der bayerischen IHKs, sind. Die in den kommunalen und Fachportalen angebotenen digitalen Verwaltungsleistungen werden gem. der Angaben in Art. 26 in den beiden federführenden Portalen des Portalverbunds auffindbar gemacht. Die Verfahren selbst werden in den Fachportalen abgewickelt.

Es sollte außerdem nochmals klar differenziert werden, dass diverse Basiskomponenten des Freistaats (z.B. E-Payment) für die Nutzung z. B. in Kommunen angeboten werden – sie aber keine Nutzungsverpflichtung für Körperschaften des öffentlichen Rechts oder öffentlicher Auftraggeber sind. Diese sind in der Regel anders organisiert, z. B. via bundesweit einheitliche Lösungen.

Art. 27: Bayernportal

In Absatz 1 Satz 2 Nr. 1 ist das Wort „anbieten“ versehentlich doppelt angegeben. Dies sollte korrigiert werden.

Art. 28 Abs. 3: Organisationsportal Bayern

In der Gesetzesbegründung wird explizit darauf hingewiesen, dass Absatz 3 S. 2 eine Ausnahmeregelung enthält. In der vorliegenden Fassung fehlt dieser Satz und sollte ergänzt werden.

Art. 30, Abs. 2: Funktionsumfang des Nutzerkontos, Datenschutz

Diese Regelung betrifft die Zustimmung des Nutzers, dass seine personenbezogenen Daten aus dem Nutzerkonto automatisch in die zur Antragstellung bereit gestellten Formulare übernommen werden können. Hier wird zunächst der Begriff „Zustimmung des Nutzers“ verwendet. Gemeint ist wohl eine Einwilligung des Nutzers in die Datenübermittlung. In der Sache selbst geht es darum, dass die jeweilige Behörde auf vorhandene personenbezogene Daten eines Nutzers zugreifen darf und mit diesen Daten dann das Formular vorausgefüllt wird.

Hier ist zunächst zu überlegen, ob der Nutzer hierzu in generalisierter Form bzw. allgemein eine Einwilligung erteilt, die dann für sämtliche Arten von Anträgen bei einer bayerischen Behörde gelten soll. Oder erfolgt diese Einwilligung jeweils immer vor einem bestimmten Antrag.

Letzteres wäre wohl nicht im Sinne der Digitalisierung, da dann jede Antragstellung eine Einwilligung vorgeschaltet wäre. Hier sehen wir noch Klärungsbedarf. Allerdings dürfte es datenschutzrechtlich eine Herausforderung sein, eine derart allgemein gehaltene Einwilligung rechtswirksam zu formulieren.

Art. 31 Abs. 1: Identifizierung am Nutzerkonto, Schriftformersatz

Auch hier sollte das Wording angepasst und der Begriff „Zustimmung“ durch „Einwilligung“ ersetzt werden. Ferner muss in Abs. 1 Satz 2 klargestellt werden, wem gegenüber ein Nutzer seine Einwilligung abgeben muss. Dies müsste bei einer einmaligen temporären Nutzung nur gegenüber der öffentlichen Stelle sein, die Identifikationsdaten mit Einwilligung des Nutzers an eine andere öffentliche Stelle weiterleitet; nicht jedoch sollte ein Nutzer in diesem Fall eine Einwilligung gegenüber der empfangende öffentlichen Stelle abgeben. Damit wäre sichergestellt, dass das BayDiG und das OZG den Sachverhalt einheitlich regeln. Denn das OZG sieht in § 8 OZG für eine temporäre (einmalige) Nutzung der Identifikationsdaten keine Einwilligung eines Nutzers vor. Dies ist nach OZG nur für eine dauerhafte Nutzung erforderlich.

Zu Teil 2, „Digitale Verwaltung“
Kapitel 4, „Digitale Akten und Register“

Artikel 34: Einsicht in die digitale Akte

Im Sinne der Nutzerfreundlichkeit sollten mindestens zwei der genannten Möglichkeiten angeboten werden.
Geprüft werden sollte zudem eine Kompatibilität mit anderen gesetzlichen Rechten wie dem Recht auf Erhalt einer Kopie nach Art. 15 Abs. 3 und 4 DSGVO. Da das BayDiG bestehende Datenschutzreglungen unberührt lässt, bestehen nach Art. 10 BayDSG mögliche Einschränkungen für das Auskunftsrecht, welches u. a. durch eine Einsichtnahme gewährt werden kann, auch bezogen auf Rechte aus Art. 34 BayDiG-E. Sollte dies nicht der Fall sein, müssten diese ergänzt werden. Denn diese Ausnahmen haben in der Praxis für öffentliche Stellen eine grundsätzliche Bedeutung.

Art. 37 Abs. 2, Basisdienste und zentrale Dienste

Hier sollte in S. 3 statt „Zustimmung“ der Begriff „Einwilligung“ verwendet werden. Ferner sollte klargestellt werden, ob Satz 3 von einer Einwilligung im Einzelfall oder von einer generellen Einwilligung ausgeht. Allerdings dürfte eine generelle Einwilligung datenschutzrechtlich zu allgemein sein und damit kaum rechtswirksam formuliert werden können.

Art. 38 Auftragsverarbeitung durch staatliche Stellen

Diese Vorschrift sieht gewisse Erleichterungen bei einem massenhaften Abschluss von Auftragsverarbeitungsverträgen vor. Bei einer Auftragsverarbeitung durch staatliche Stellen mit öffentlichen Stellen soll per Gesetz ein Vertrag über die Auftragsverarbeitung begründet werden. Diese Handhabung ist zu begrüßen. Allerdings sollte überlegt werden, ob im Zuge der Digitalisierung und im Gleichlauf mit der DSGVO auch ein elektronischer Abschluss eines Vertrags über Auftragsverarbeitung im BayDiG als gesetzlich mögliche Option eingeräumt werden sollte.

Zu Teil 2, „Digitale Verwaltung“
Kapitel 5, „Behördenzusammenarbeit, Rechenzentren“

Artikel 39, Abs. 2, Satz 1: Staatliche Rechenzentren
Für ein gebündeltes und kompetentes Vorgehen in der Digitalisierung sollten die ministeriellen Zuständigkeiten von der Infrastruktur über Rechenzentren bis hin zu den verwaltungsinternen und externen Digitalisierungsthemen und Projekten in einer Zuständigkeit liegen.

Teil 3: „IT-Sicherheit“
Kapitel 1: „Allgemeine Vorschriften“

Artikel 41 und 42: Landesamt für Sicherheit in der Informationstechnik (LSI)
Ganz ähnlich wie das Bundesamt für die Sicherheit in der Informationstechnik (BSI) für die Bundes-IT und kritische Infrastrukturen soll das LSI für die Landes-IT ausgebaut werden.
Dies erscheint sinnvoll, damit die staatliche IT des Freistaates abgesichert wird. Der Zugriff auf Leistungen des LSI sollte allen öffentlichen Stellen (auch juristischen Personen des öffentlichen Rechts wie IHKs) möglich sein. In einer vernetzten Welt kann Sicherheit in der Beratung nicht partiell nur für bestimmte Kategorien öffentlicher Stellen erfolgen.

Zudem kann das LSI gemäß Artikel 42 (2) „auf Ersuchen … 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."
Diese und ähnliche Aufgabenstellungen sieht auch der gesetzliche Auftrag des BSI vor. Um Doppelungen zu vermeiden, sollten die Angebote von BSI und LSI eng abgestimmt sein.

Teil 3: „IT-Sicherheit“
Kapitel 2: „Befugnisse“
Von den Erkenntnissen des LSI muss auch die Wirtschaft zur Verbesserung der Sicherheit profitieren. Daher sollten die Mindeststandards (**Artikel 46**) und Warnungen (**Artikel 47)** öffentlich verfügbar sein und auch für Unternehmen einen Orientierungsrahmen bieten. Ferner sollten diese Mindeststandards mindestens bundesweit, bei Bedarf auf EU-weit abgestimmt sein.
Hinsichtlich **Artikel 45** „Untersuchung der Sicherheit in der Informationstechnik“ formuliert (2), dass Untersuchungsergebnisse nur intern weitergegeben werden können. Auf Seite 116 f wird dies konkretisiert im Sinne, dass „Eine allgemeine Veröffentlichung der Bewertung“ nicht möglich ist, da dies ein „Eingriff in die Rechte der Produktverantwortlichen“ sei. D.h. Einschätzungen des LSI bzgl. der Sicherheit von IT bleiben für Unternehmen nicht nutzbar. Ziel sollte sein, dass auch die Wirtschaft von gewonnen Sicherheitserkenntnissen profitiert. Dies könnte entweder direkt durch das LSI erfolgen oder ggf. über das BSI, z. B. ggf. auch über das geplante freiwillige

IT-Sicherheitskennzeichen des BSI, in das Sicherheitseinschätzungen einfließen können.

Teil 3: „IT-Sicherheit“
Kapitel 3 Datenschutz

Art. 48: Datenspeicherung und –auswertung

In den Erwägungsgründen sollte erläutert werden, welche Anforderungen zu erfüllen sind, damit gem. Absatz 1 personenbezogene Daten als spurlos gelöscht gelten. Die DSGVO selbst definiert den Begriff „Löschen“ nicht. Dort gibt es auch den Begriff „spurloses Datenlöschen“ nicht. Technisch wären gelöschte Daten nur dann nicht wiederherstellbar, wenn Dateien irreversibel gelöscht werden (z. B. Schreddern von Festplatten, Überschreiben von Dateien mit „Nullern“).
In der Begründung zu Abs. 4 werden die Begriffe „Verarbeiten und Nutzen“ verwendet. Die DSGVO kennt nur noch den Begriff „Verarbeiten“. Insofern sollte auch in der Gesetzesbegründung ausschließlich dieses Wording verwendet werden.

Teil 4: „Organisation“

Art. 50: Kommunaler Digitalpakt

Der Kommunale Digitalpakt ist ein hilfreiches Gremium, das die verwaltungsübergreifende Zusammenarbeit in der Digitalisierung fördert.
Um die dringend notwendige stärkere Nutzerorientierung der digitalen Verwaltungsangebote besser sicherzustellen, sollten in diesem Gremium auch Vertreter der Nutzer, der Bürger und insbesondere der Unternehmen, aufgenommen werden. Die bayerischen IHKs stehen hierfür gerne bereit.

Vorschlag für einen zusätzlichen Artikel:

"**Überprüfung der Echtheit digitaler Dokumente**".
Um Prozesse vollständig digital abbilden zu können, muss eine Möglichkeit geschaffen werden, digitale Dokumente automatisiert auf Echtheit zu prüfen. Die Ermöglichung der Validierung von Dokumenten über Blockchain Lösungen sollte gleichgesetzt werden mit den aktuell vorgesehenen Mechanismen zur elektronischen Signatur etc. Dabei könnte man eventuell auch einen Schritt weitergehen und auch die Möglichkeit bereits vorsehen, dass für Anträge die geforderten Nachweise nicht mehr als digitales Abbild eines Dokuments eingereicht werden müssen, sondern es ausreicht, die benötigte Information in das Verfahren zu übermitteln. Hintergrund ist dabei auch der Wunsch, statt bestehende Prozesse / Mechanismen digital abbilden zu wollen (z.B. Beglaubigung, Siegel) doch die neuen Technologien zu nutzen, um effizientere / bessere Lösungen zu finden.