Stellungnahme zum Gesetz zur Änderung des HEGovG und weiterer Vorschriften

im Ausschuss für Digitales und Datenschutz im Hessischen Landtag

Marco Holz, Markus Drenger

Chaos Computer Club Darmstadt e.V.

Inhaltsverzeichnis

1 Grundsätzliche Anmerkung zum Format des Gesetzesvorschlags

Das vorliegende Änderungsgesetz liegt - wie gewohnt - leider wieder nur im PDF-Format vor und ist aufgrund der immer noch üblichen Darstellungsform mit Änderungsbefehlen in Prosa schwer lesbar. Beim vorliegenden Änderungsantrag zum Änderungsgesetz verstärkt sich dieser Effekt nochmals. Dort heißt es beispielsweise: „1. Art. 1 wird wie folgt geändert: a) Nr. 2 a) erhält folgende Fassung: »a) Abs. 2 wird wie folgt gefasst: ›(2) Jede mit dem Vollzug von Verwaltungsleistungen betraute Stelle […]‹“.[1]

Eine Vorher-Nachher-Vorschau und maschinenlesbare, klickbare Referenzen auf erwähnte externe Gesetzestexte würden enorm zur besseren Lesbarkeit und Verständlichkeit beitragen. Hierzu bedarf es der Repräsentation von Gesetzen und Gesetzesänderungen in einem maschinenlesbaren Format nach einem international etablierten Standard.[2]

Durch die Nutzung einer Versionsverwaltungssoftware – wie z.B. Git – wären Änderungen an Gesetzestexten im Zeitverlauf darüber hinaus deutlich besser nachvollziehbar.

2 Grundsätzliches zum Sachverhalt

Insgesamt bleibt der Gesetzesentwurf in zentralen Aspekten der IT-Sicherheit und des Benutzer:innenerlebnis (*User Experience*) hinter den Erwartungen an einen modernen Staat zurück. Statt der konsequenten Nutzung von bestehenden, offenen Technologien setzt der öffentliche Sektor in vielen Bereichen noch zu sehr auf in die Jahre gekommene Eigenentwicklungen, die nicht dem Stand der Technik entsprechen. Der Gesetzesentwurf enthält jedoch auch sinnvolle Verbesserungen gegenüber dem Status quo. Hervorzuheben sind insbesondere die Einführung eines Digital-Checks und die Abkehr von De-Mail.

2.1 IT-Sicherheit

Staatliche IT-Systeme sind in der Vergangenheit häufig durch mangelnde IT-Sicherheit und die Nicht-Beachtung des Stand der Technik aufgefallen. Besonders hervorzuheben ist hier der unzureichende Einsatz von kryptographischen Verfahren und der Mythos „sicherer Verwaltungsnetze“.

Eine Vielzahl von IT-Sicherheitsvorfällen in Kommunen haben gezeigt, dass IT-Systeme der Verwaltung unzureichend vor gezielten Angriffen geschützt sind und sogar regelmäßig nicht-zielgerichteten

[1] Hier fehlt im Änderungsantrag übrigens ein schließendes Anführungszeichen.

[2] Initiativen wie https://openlegaldata.io/ und BundesGIT (siehe https://github.com/bundestag/gesetze) haben hier großartige Vorarbeit geleistet. Mit Akoma Ntoso (auch bekannt unter dem Namen LegalDocML) steht hierzu bereits ein international genutzter Standard bereit (siehe https://de.wikipedia.org/wiki/Akoma_Ntoso), der auch in der Referenzarchitektur Normsetzung des CIO Bund erwähnt wird (siehe https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/normsetzung.pdf?__blob=publicationFile&v=1).

Ransomware-Kampagnen (*Verschlüsselungstrojaner*) zum Opfer fallen.[3]

Hier besteht aus unserer Sicht Handlungsbedarf, das IT-Sicherheitsniveau des Landes und der Kommunen auf ein angemessenes Niveau anzuheben und mögliche Synergieeffekte in der Betriebsführung zu nutzen, um beispielsweise einen rund um die Uhr-Betrieb und die entsprechende Überwachung der IT-Systeme etablieren zu können. Zuständigkeiten und Befugnisse sollten kritisch geprüft werden. Unter Umständen wäre es sinnvoll, die Aufsicht des Landes über die Kommunen entsprechend auszugestalten und wirksame Kontrollmechanismen zu etablieren.

IT-Sicherheit darf zudem nicht nur auf Maßnahmen des IT-Betriebs abzielen, sondern muss auch bereits in der Konzeption von IT-Systemen und Infrastrukturkomponenten berücksichtigt werden (*Security-by-Design*). Interaktionen zwischen IT-Systemen müssen immer auch kryptographisch abgesichert werden und die Auswirkungen einer Kompromittierung dieser Systeme verstanden, bewertet und beim Design der IT-Systeme berücksichtigt werden (*Zero-Trust-Architektur*). Dies inkludiert auch die ununterbrochene Verschlüsselung vom Absender bis zum Adressaten einer Nachricht, sodass zwischengelagerte IT-Systeme keinen Einblick in die übermittelten Informationen bekommen (*Ende-zu-Ende-Verschlüsselung*).

Selbiges gilt für Fragen des Datenschutzes und der datensparsamen Umsetzung von Verwaltungsleistungen (*Privacy-by-Design*). Exemplarisch könnte statt des Austauschs vollständiger Akten ein Informationsaustausch im Rahmen eines Verwaltungsverfahrens auf die Feststellung einer bestimmten Tatsache beschränkt werden (z.B. der Austausch der Information „positiver Bescheid liegt vor“ statt der vollständigen Übermittlung eines Bescheides).

Zur Unterstützung bei der Verankerung dieser Prinzipien in der IT-Infrastruktur des Landes schlagen wir die Schaffung der Rolle des Chief Technology Officer (CTO) vor (s.u.).

2.2 Herausforderungen des Fachkräftemangels effektiv und zielgerichtet begegnen

Insbesondere in den letzten Jahren hat sich die öffentliche Verwaltung auf dem Arbeitsmarkt trotz interessanter Aufgabengebiete nicht gegenüber privatwirtschaftlichen Unternehmen durchsetzen können. Gründe dürften u.a. die für IT-Fachkräfte unattraktive Entlohnung, die fehlende Flexibilität bei (Vollzeit-)Homeoffice-Regelungen und weitere nicht-finanzielle Anreize im privaten Sektor sein. Der Aufbau dringend benötigter IT-Fähigkeiten in den Behörden wurde verschlafen und resultiert in einer starken Abhängigkeit von externen Dienstleistern und Beratungsunternehmen.

Besonders betroffen von dieser Entwicklung sind Kommunen.

Aufgrund der fehlenden Expertise in Behörden besteht oft bereits im Beschaffungsprozess ein hoher

[3] vgl. Bundeslagebild Cybercrime des Bundeskriminalamtes: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220509_PM_CybercrimeBLB.html

Beratungsbedarf, der nicht selten in unwirtschaftlichen oder nicht bedarfsgerechten IT-Lösungen resultiert.

Insbesondere auf Landesebene besteht ein hoher Bedarf an Fachkräften mit breit aufgestellten IT-Kompetenzen. Die Modernisierung von staatlicher IT ist kein fertig einkaufbares Produkt (*commodity*), sondern erfordert insb. eine strategische Planung und Steuerung auf Grundlage fundierter, praktischer IT-Kompetenz und einem tiefen Verständnis der spezifischen Anforderungen der öffentlichen Verwaltung.

Besonders Punkten könnte die öffentliche Verwaltung bei weitreichenden Regelungen zur Mitarbeit an Open-Source-Projekten, Open-Data-Vorgaben und einem hohen Gestaltungsspielraum bei der Art und Weise der Aufgabenerledigung. Hierzu bedarf es grundlegender Reformen in der Arbeitsweise der öffentlichen Verwaltung.

2.3 Better for Less

Bereits 2010 beschreiben Liam Maxwell et at. in *Better for Less - How to make Government IT deliver savings*[4] das enorme Einsparpotential bei Staatsausgaben im IT-Sektor in Großbritanien bei gleichzeitiger Steigerung der Qualität staatlicher IT-Services. Bereits im Jahr 2013 konnte der Government Digital Service (GDS) Einsparungen in Höhe von 500 Millionen Pfund verzeichnen. Die sog. *Spend Controls* stellen dabei wesentliches Instrument des GDS dar. Sie stellen sicher, dass Ausgaben für digitale Services dem britischen *Technology Code of Practice* entsprechen, der u.a Nutzer:innenorientierung, eine Veröffentlichung der erstellen Software unter einer Open-Source-Lizenz, Barrierefreiheit, die Verwendung von offenen Standards und die Beachtung von Security- & Privacy-by-Design-Prinzipien einfordert.[5] Weitere wichtige Faktoren sind der Fokus auf marktübliche IT-Lösungen statt Sonderlösungen für die Verwaltung und die Vermeidung großer Rahmenverträge zur Stärkung der Konkurrenz zw. IT-Dienstleistern.[6]

Die Erkenntnisse aus Großbritannien und anderen Ländern finden in Deutschland noch zu selten Anwendung.

2.4 Monitoring von Kennzahlen

Ein wichtiges Instrument bei der Bewertung und Evaluation des Erfolgs von Digitalisierungsvorhaben ist die Erfassung von Kennzahlen. Angebote der Verwaltung sollten von Anfang an in der Lage sein, die Zufriedenheit der Nutzer:innen sowie die Häufigkeit der Nutzung der Services zu messen.

[4] https://ntouk.files.wordpress.com/2015/06/better-for-less-1.pdf
[5] https://www.gov.uk/guidance/the-technology-code-of-practice
[6] https://gds.blog.gov.uk/2013/06/10/better-for-less/

Sinnvoll erscheint auch die Messung der Anzahl an Verwaltungsvorgängen pro Leistung, wobei zw. offline und online beantragten Leistungen unterschieden werden sollte. Die sich hieraus ergebende prozentuale Nutzungsrate von Online-Services ist ein wichtiges Kriterium zur Bewertung des Erfolgs einer online angebotenen Verwaltungsleistung.

Kennzahlen zu Nutzer:innen-Zufriedenheit und Nutzungshäufigkeit sollten automatisiert (mind. einmal täglich) in einem offenen, maschinenlesbaren Format öffentlich als offene Daten bereitgestellt werden. Statistische Daten zu offline (vor Ort) initiierten Verwaltungsleistungen sollten mindestens vierteljährlich in einem maschinenlesbaren Format zur Verfügung gestellt werden.

2.5 Open-Source-Strategie

Große Hürde bei der Realisierung von digitalen Verwaltungsleistungen sind die oft fehlende Interoperabilität von IT-Systemen und unzureichende Steuerungsmöglichkeiten öffentlicher Auftraggeber bei der Produktentwicklung und -strategie einzelner IT-Produkte.

Aufgrund von starken Herstellerabhängigkeiten ist eine effektive Steuerung durch die öffentliche Verwaltung bei der Weiterentwicklung und Interoperabilisierung einzelner Fachverfahren und anderer IT-Systeme oft nur eingeschränkt möglich. Der im Rahmen einer Gesamtstrategie wünschenswerten Öffnung von „Datensilos“ und dem Zusammenspiel von Fachanwendungen unterschiedlicher Hersteller durch die Umsetzung von Schnittstellenstandards stehen häufig wirtschaftliche Interessen privater oder öffentlicher IT-Dienstleister entgegen. Die Vermarktung von teuren „Adaptern“ zu IT-Systemen anderer Hersteller, d.h. die Freischaltung von bereits implementierten Schnittstellen, ist ein Zeichen für die mangelnde Auftraggeber:innenkompetenz der öffentlichen Verwaltung.

In einem ersten Schritt erscheint daher die Vorgabe sinnvoll, von der Verwaltung finanzierte Eigenentwicklungen nach dem Prinzip „Public Money - Public Code“[7] unter einer offenen Softwarelizenz der Allgemeinheit und damit auch allen Kommunen zur Verfügung zu stellen.[8] Entsprechende Vorgaben sind unbedingt bereits in Beschaffungsprozessen zu berücksichtigen.

Der vermehrte Einsatz von Open-Source-Komponenten, die den Bedarfen der öffentlichen Verwaltung entsprechen, ermöglicht perspektivisch auch eine verbesserte interkommunale Zusammenarbeit bei der Umsetzung und kontinuierlichen Verbesserung von OZG-Dienstleistungen und internen Verwaltungsprozessen. Von einer Kommune finanzierte Verbesserungen an Softwarekomponenten stehen damit beispielsweise auch allen anderen Kommunen kostenneutral zur Verfügung.

Gleichzeitig wird durch das Open-Source-Modell die Auftraggeber:innenkompetenz der öffentlichen Verwaltung gestärkt. Statt von nur einem einzigen IT-Dienstleister bei der Erbringung bestimmter

[7] siehe https://publiccode.eu/

[8] Eine entsprechende Vorgabe findet sich auch in den vom IT-Planungsrat verabschiedeten Föderalen IT-Architekturrichtlinien: https://docs.fitko.de/arc/policies/foederale-it-architekturrichtlinien#sr8

Leistungen abhängig zu sein, kann die unter einer Open-Source-Lizenz veröffentlichte Software einem beliebigen am Markt aktiven IT-Dienstleister weiterentwickelt werden.

Bestehende IT-Dienstleister der öffentlichen Verwaltung haben bereits angekündigt, in Zukunft stärker nach diesem Entwicklungsmodell agieren zu wollen. IT-Dienstleister profitieren dabei u.a. von einer gesteigerten Reputation und höherer Attraktivität auf dem Bewerber:innenmarkt. Die Verwaltung profitiert nicht zuletzt auch von gesteigerter Softwarequalität durch den in diesem Modell ermöglichten Erfahrungsaustausch zw. der Open-Source-Community und IT-Dienstleistern und zwischen IT-Dienstleistern der öffentlichen Verwaltung untereinander.

2.6 Offene Standards

Der Einsatz von offenen Standards stellt ein weiteres wichtiges Instrument zur Vermeidung eines Vendor-Lock-In (Herstellerunabhängigkeit) und zur Schaffung von größtmöglicher Interoperabilität von IT-Systemen der Verwaltung dar. Entsprechende Vorgaben zur *Aktenführung in offenen Dokumentformaten* wie dem OpenDocument-Format (ODF) fehlen im HEGovG. Auch bei der Realisierung von digitalen Verwaltungsleistungen sollte die Nutzung von offenen Datenstandards gemäß der Definition der Free Software Foundation Europe[9] zur verbindlichen Vorgabe gemacht werden. Auf die Nennung konkreter Standards sollte zugunsten der Technologieoffenheit jedoch verzichtet werden.

2.7 Zeitgemäße volldigitale und effiziente Verwaltungsleistungen

Im vorliegenden Gesetzentwurf fehlen Vorgaben für eine dringend nötige *Ende-zu-Ende-Digitalisierung*. Eine Digitalisierung der öffentlichen Verwaltung kann nur erfolgreich sein, wenn neben einem Komfortgewinn für Antragsteller:innen auch eine effiziente Bearbeitung von Verwaltungsverfahren auf Seiten der zuständigen Fachbehörden ermöglicht wird. Erst mit der Restrukturierung von Prozessen und der Einführung bzw. Weiterentwicklung von Systemen zur Vorgangsbearbeitung (Fachverfahren) entfaltet die digitale Umsetzung von Verwaltungsleistungen ihr eigentliches Potential.

Wo kein Ermessensspielraum bei der Vorgangsbearbeitung besteht, sollten Leistungen zur Entlastung von Verwaltungspersonal und Steigerung des Benutzererlebnis vollständig automatisiert abgebildet werden. Für die *vollständig automatisierte Abwicklung von Verwaltungsleistungen* sollten Performanceanforderungen definiert werden (z.B. „Eine Bescheidung einer Verwaltungsleistung auf Grundlage automatisierter algorithmischer Entscheidungsfindung hat innerhalb von 3 Minuten zu erfolgen.“).

Eine algorithmische Entscheidungsfindung ist auf deterministische Verfahren zu beschränken (*Ausschluss von KI zur Entscheidungsfindung*). Zur Herstellung einer vollständigen Transparenz über automa-

[9] siehe https://fsfe.org/freesoftware/standards/index.de.html

tisierte Entscheidungsprozesse, empfiehlt sich die Verpflichtung zur Veröffentlichung der eingesetzten Algorithmen.[10][11]

Verwaltungsleistungen sollten nach dem Prinzip *API-first* immer zuerst über maschinenlesbare Schnittstellen bereitgestellt werden. Der API-first-Ansatz trägt dabei zur Entkopplung der Systeme zur Antragstellung und Antragsbearbeitung bei. Dies ermöglicht die Integration von Antragsprozessen in unterschiedliche private oder vom Staat bereitgestellte Systeme zur Antragstellung. Die lose Kopplung[12] von Front- und Backend ermöglicht eine Austauschbarkeit einzelner Fachverfahren oder Systeme zur Antragstellung und ebnet damit den Weg für eine kosteneffiziente technische Modernisierung von Verwaltungs-IT.

Bei der Bereitstellung von APIs sollten einheitliche Qualitätskriterien wie die Bereitstellung von qualitativ hochwertiger technischer Dokumentation und maschinenlesbaren Schnittstellen-Spezifikationen auf einer öffentlich zugänglichen Dokumentationsplattform sowie die Definition von angemessenen Übergangsfristen bei nicht-abwärtskompatiblen API-Änderungen eingeführt werden. Hierzu empfiehlt sich die Schaffung einer Unterstützungseinheit beim Hess. Digitalministerium zur Definition und Unterstützung bei der Einhaltung dieser Qualitätskriterien. Mindeststandards wie die generelle Pflicht zur Veröffentlichung von technischer Dokumentation & Schnittstellen-Spezifikationen sowie eine Übergangsfrist von 3 Monaten für nicht-abwärtskompatible Änderungen sollten im Gesetzesvorschlag definiert werden.

2.8 Ergänzender Hinweis: Unsere Stellungnahme zum Kommunalbericht 2019

Viele der hier genannten Punkte finden sich auch in unserer Stellungnahme zum Kommunalbericht 2019 im Unterausschuss für Finanzcontrolling und Verwaltungssteuerung im Hessischen Landtag wieder.[13] Insbesondere der Fokus auf Offene Ansätze (Freie Software, Offene Daten, Offene Standards), die Befähigung der Verwaltung zur eigenständigen Bewertung und (Weiter-)Entwicklung von IT-Lösungen durch den Aufbau von qualifiziertem IT-Fachpersonal, die Einbindung der Expertise aus der Zivilgesellschaft und der Abbau von Beratungs- und Herstellerabhängigkeiten zählen nach wie vor zu den entscheidenden Erfolgsfaktoren für eine gelungene Verwaltungsmodernisierung.

Unsere Stellungnahme zum Kommunalbericht gibt hierzu konkrete Handlungsvorschläge und zeigt zahlreiche Beispiele für gelungene Vorhaben auf, die diese Prinzipien berücksichtigen.

[10] Das Bundesfinanziministerium veröffentlicht bereits seit über 15 Jahren die Programmablaufpläne für den Lohnsteuerabzug: https://www.bundesfinanzministerium.de/Web/DE/Themen/Steuern/Steuerarten/Lohnsteuer/Programmablaufplan/programmablaufplan.html

[11] Seit diesem Jahr betreibt die Niederlande unter https://algoritmes.overheid.nl/ ein nationales Algorithmen-Register.

[12] geringe technische Abhängigkeit zwischen Softwaresystemen

[13] siehe https://www.chaos-darmstadt.de/2020/stellungnahme-zum-kommunalbericht-2019/

3 Anmerkungen zum vorliegenden Gesetzesentwurf

3.1 § 3 Elektronische Kommunikation

Die Idee des technikoffenen Charakters der Neuregelung ist zu begrüßen. In der Umsetzung der Neuregelung ergeben sich jedoch eine Reihe von fortbestehenden Problemen.

3.1.1 Recht auf Verschlüsselung

- **Problem**: In der Gesetzesbegründung kommt der Wunsch zur Anwendung kryptographischer Verfahren nach dem Stand von Wissenschaft und Technik zum Ausdruck. Alle in Abs. 2 (neu) genannten technischen Kommunikationsinfrastrukturen unterstützen jedoch von Haus aus keine Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik ab dem Endgerät der Absender:in. Das Postfach im Nutzer:innenkonto unterstützt derzeit gar keine Inhaltsdatenverschlüsselung. Die Folge ist eine erhebliche, zentrale Aggregation personenbezogener Daten, die mit einem erheblichen strukturellen Risiko für die Betroffenen einhergeht. Eine Ende-zu-Ende-Verschlüsselung ist auch bei De-Mail standardmäßig nicht vorgesehen.[14] Das besondere elektronische Behördenpostfach fällt als Kontaktmöglichkeit weitestgehend aus, das vorgesehene eBO scheint aufgrund der hohen jährlichen Kosten für die Teilnehmer:innen ähnlich erfolgreich zu werden wie das gescheiterte De-Mail.
- **Lösung**: Der CCC forderte bereits 2020 im Innenausschuss des Deutschen Bundestags ein kompromissloses Recht auf Verschlüsselung und kritisierte mit Verweis auf De-Mail und beA das regelmäßige und zielsichere scheitern deutscher Alleingänge in der Verschlüsselung[15]. Die im Gesetzesentwurf genannten Infrastrukturen widersprechen diesen Forderungen des CCC: „Nur frei verfügbare, überprüfbare und offene Protokolle sollen genutzt werden dürfen.“ Wir empfehlen eine Vorgabe zur Offenheit und Überprüfbarkeit kryptographischer Verfahren in das Gesetz aufzunehmen. Um dem bereits in der Gesetzesbegründung zum Ausdruck gebrachten Wunsch einer Ende-zu-Ende-Verschlüsselung („eine für Dritte unverständliche Form“) gerecht zu werden, wird die Aufnahme der folgenden Formulierung vorgeschlagen: „Es muss eine Ende-zu-Ende-Verschlüsselung für die Verschlüsselung der Inhaltsdaten zwischen den beteiligten Akteuren eingesetzt werden. Kommen bei der Übermittlung der Inhaltsdaten mehr als zwei technische Systeme zum Einsatz, so müssen die zwischengeschalteten Systeme ihren Dienst ohne Kenntnis der Inhaltsdaten erfüllen können und DÜRFEN NICHT in die Lage versetzt werden, Inhaltsdaten im Klartext einzusehen.“

[14] Jedoch ist die Nutzung von PGP und S/MIME nach Installation zusätzlicher Software möglich
[15] siehe https://www.ccc.de/de/updates/2020/ccc-fordert-kompromissloses-recht-auf-verschlusselung

3.1.2 Nutzung etablierter Technologien statt Eigenentwicklungen der Verwaltung

- **Problem**: Die im Gesetzentwurf genannten Kommunikationslösungen sind in der breiten Öffentlichkeit kaum bekannt und werden kaum genutzt. Für öffentliche Stellen besteht zur Umsetzung des § 3 Abs. 2 eine freie Wahl der genannten zusätzlichen Kommunikationslösungen. Erfahrungsgemäß werden öffentliche Stellen aufgrund der geringen Nutzungszahlen der vorgeschlagenen Lösungen verständlicherweise nicht freiwillig alle zur Verfügung stehenden Kommunikationslösungen anbieten. Hierdurch entsteht ein Flickenteppich aus unterschiedlichsten Kontaktmöglichkeiten, die alle gleichermaßen wenig genutzt werden.
- **Lösung 1**: Die Bereitstellung eines E-Mail-Postfachs, das auch den Empfang von verschlüsselten Nachrichten ermöglicht, wäre für Bürger:innen ein einfach zugänglicher Weg zur Kommunikation mit Landesbehörden. Das BMI bietet diese Möglichkeit bereits an.[16] Wir empfehlen in diesem Zusammenhang eine Ergänzung des § 3, Abs. 1 um die Vorgabe, dass auch eine verschlüsselte Kommunikation nach dem Stand der Technik ermöglicht werden muss (vgl. § 3 Abs. 1 EGovG NRW).
- **Lösung 2**: Zugunsten der Verpflichtung zur Ermöglichung einer verschlüsselten E-Mail-Kommunikation in § 3, Abs. 1 kann auf die Nennung unterschiedlicher konkreter Lösungen in Abs. 2 verzichtet werden. Wir empfehlen daher, Abs. 2 zu streichen und die Erreichbarkeit von Behörden via verschlüsselter E-Mail in Abs. 1 zu regeln. Sofern der gesetzgeberische Wunsch zur Bereitstellung eines Postfachs im Nutzerkonto nach § 2 Abs. 7 OZG fortbesteht, könnte diese Eigenentwicklung der öffentlichen Verwaltung unter Berücksichtigung der Vorgaben für sichere, Ende-zu-Ende-verschlüsselter Kommunikation (s.o.) als zusätzliche, verpflichtende Kommunikationslösung aufgenommen werden.
- **Lösung 3**: Statt Bürger:innen zur Nutzung von eigenen Kommunikationslösungen der Verwaltung zu drängen, sollten Bürger:innen zur Kommunikation mit der Verwaltung - wie auch bei der Kommunikation mit der Privatwirtschaft - bereits bekannte Dienste nutzen können. Zusätzlich zur verbindlich geregelten Erreichbarkeit aller öffentlicher Stellen via verschlüsselter E-Mail empfehlen wir daher eine KANN-Klausel zur Kommunikation über von Bürger:innen frei gewählte Kommunikationswege. Bürger:innen wären demnach in der Lage, mit öffentliche Stellen nach eigenem Wunsch über weit verbreitete Kommunikationslösungen (z.B. Messenger-Apps) zu interagieren, sofern diese von der jeweiligen Stelle angeboten werden (vgl. § 4 Abs. 1 EGovG NRW).

3.1.3 Poststellen-Problematik

- **Problem**: Das bestehende HEGovG zenmentriert in §3 Abs. 1 das Konzept von Poststellen, wie sie aus der analogen Welt bekannt sind. In der digitalen Welt, ergeben sich hierbei erhebliche

[16] siehe https://www.bmi.bund.de/DE/service/kontakt-uebersicht/kontaktuebersicht-node.html. Weitere Informationen hierzu finden sich auf der Webseite des BSI: https://www.bsi.bund.de/dok/11486410

Datenschutz- und IT-Sicherheitsprobleme. Durch die Zentralisierung des Postein- und ausgangs in „einen [einzigen] Zugang für die Übermittlung elektronischer Dokumente“ können rechtlich besonders geschützte personenbezogene Daten (beispielsweise Psychartriebescheide in Gesundheitsämtern) von einer zentralen Stelle sowie auch von den zuständigen Mitarbeiter:innen der zentralen IT oder des beauftragten IT-Dienstleisters eingesehen werden. Diese Praxis verstößt gegen geltende Datenschutzvorschriften.
- **Lösung**: Statt der Vorgabe, nur einen einzigen Zugang zur Übermittlung signierter, elektronischer Dokumente pro Behörde zu schaffen, sollte die Annahme elektronisch signierter Dokumente grundsätzliche Vorgabe für alle von öffentlichen Stellen bereitgestellten Zugänge (E-Mail-Adressen) werden.

3.1.4 Umsetzungsfrist

- **Problem**: Öffentliche Stellen sind in der Regel bereits in der Lage, Dokumente auf digitalem Wege zu empfangen. Qualifizierte elektronische Signaturen werden jedoch nicht durchgängig anerkannt. Das Gesetz definiert hierzu keine Umsetzungsfrist.
- **Lösung**: Im Gesetz sollten Umsetzungsfristen definiert werden, ab denen öffentliche Stellen digital eingereichte Dokumente mit qualifizierter elektronischer Signatur - analog zu papierhaft eingereichten Dokumenten - akzeptieren müssen.

3.1.5 Unklare Trennung zw. HEGovG und HVwVfG

- **Problem**: § 3 Abs. 3 enthält in der bestehenden Fassung die begrüßenswerte Möglichkeit der Identifizierung mittels eID nach § 18 Personalausweisgesetz bzw. nach § 78 Abs. 5 Aufenthaltsgesetz. § 3 Abs. 6 enthält eine Regelung zum Verzicht auf ein Unterschriftenfeld bei elektronischer Versendung an eine Behörde. Eine generelle Regelung zum Schriftformersatz findet sich jedoch in § 3a Abs. 2 HVwVfG.
- **Lösung**: Zur besseren Lesbarkeit empfehlen wir eine Konsolidierung der entsprechenden Regelungen oder ersatzweise die Aufnahme eines Verweises auf § 3a Abs. 2 HVwVfG.

3.2 § 3a Rechtsgrundlage der Datenverarbeitung in Nutzerkonten

3.2.1 Rechtsgrundlage der Datenverarbeitung

- **Problem**: Die gewählte Formulierung „Einwilligung der Nutzenden“ in § 3a suggeriert, eine Einwilligung gemäß Art. 6ff. DSGVO sei Rechtsgrundlage für die Datenverarbeitung.
- **Lösung**: Die Formulierung „auf Veranlassung der Nutzenden“ schafft Klarheit, dass keine Datenverarbeitung auf Basis einer Einwilligung nach DSGVO vorliegt.

3.2.2 Faxgeräte verbannen

- **Problem**: Eine Kommunikation mit Nutzenden via Fax entspricht nicht dem Stand der Technik, bietet keine Verschlüsselung nach dem Stand der Technik und ist nicht mehr zeitgemäß.
- **Lösung**: In § 3a Abs. 3 sollte daher zugunsten einer Verwaltungsmodernisierung auf die Verarbeitung von Telefaxnummern verzichtet werden.

3.2.3 Zwei-Faktor-Authentifizierung

- **Problem**: Nutzer:innenkonten verarbeiten hoch-sensible Daten. Ein Zugriff auf Nutzer:innenkonten sollte daher besonders geschützt sein.
- **Lösung**: Die in der Gesetzesbegründung bereits erwähnte Zwei-Faktor-Authentifizierung sollte zwingend auf Basis etablierter Standards[17] basieren und für dauerhafte Nutzer:innenkonten verpflichtend sein.

3.3 § 3b Bekanntgabe von Verwaltungsakten im Postfach eines Nutzerkontos

3.3.1 Wahlfreiheit beim genutzten Zustellkanal

- **Problem**: Eine Nutzung staatlicher Postfach-Lösungen stellt für Verwaltungskund:innen eine vermeidbare Hürde in der Nutzung von Verwaltungsservices dar. Privatpersonen müssen zur Kommunikation einen weiteren Zustellkanal im Blick behalten, der ausschließlich für die Kommunikation mit Behörden genutzt wird. Unternehmen stehen vor der Herausforderung, täglich Nachrichten aus multiplen web-basierten Postfächern der Verwaltung manuell abrufen zu müssen.
- **Lösung 1**: Analog zu unseren Anmerkungen zu § 3 sollte auch für die Kommunikation der Verwaltung mit Antragsteller:innen prinzipiell eine Wahlfreiheit der betroffenen Person zur genutzten Kommunikationslösungen bestehen. Wir empfehlen eine explizite Aufnahme der Möglichkeit, Verwaltungskund:innen auf eigenen Wunsch über eine frei gewählte, sicher verschlüsselte Kommunikationslösung zu kontaktieren und Verwaltungsakte über diese Kommunikationslösung bekannt zu geben (z.B. Zustelldienste, verschlüsselte E-Mail oder Messenger-App). Ähnlich zur technologieneutralen Formulierung in § 4 EGovG NRW, die beispielsweise auch Messenger erfasst, sollten auch hier weitere verschlüsselte Kommunikationstechnologien zugelassen werden. Eine Auflistung unterstützter Anwendungen könnte etwa per Erlass bekannt gegeben werden. Wir empfehlen, das hessische Meldegesetz um zusätzliche, freiwillige Datenfelder zu ergänzen, damit digitale Kontaktmöglichkeiten hinterlegt werden können.

[17] TOTP, U2F

- **Lösung 2**: Ein von der Verwaltung bereitgestelltes Postfach nach § 2 Abs. 7 OZG kann ein sinnvolles Angebot für Nutzer:innen darstellen, die auf eigenen Wunsch nicht auf private Kommunikationslösung zurückgreifen möchten. Die Freiwilligkeit der Nutzung des von der Verwaltung bereitgestellten Postfachs ist in diesem Zusammenhang sehr zu begrüßen. Durch die freie Wahl der Kommunikationslösung können Nachrichten in ein System unter der Hoheit der betroffenen Person zugestellt werden, statt in einem von der Verwaltung bereitgestellten und kontrollierten Portal. Dies fördert die Möglichkeiten der Integration einer Government-2-Citizen-Kommunikation in von Verwaltungskund:innen bereits genutzte Kommunikationslösungen und steigert damit insgesamt die Attraktivität der Nutzung von Verwaltungs-Services.
- **Lösung 3**: Zur vereinfachten Kontaktaufnahme sollten von der Verwaltungskund:in frei bestimmte Kommunikationskanäle auch im Nutzer:innenkonto hinterlegt werden können. Bei der Umsetzung ist unbedingt darauf zu achten, dass auch in diesem Fall eine Ende-zu-Ende-verschlüsselte Kommunikation zwischen der beteiligten Fachbehörde und der betroffenen Person gewährleistet ist. Eine Zustellung von Nachrichten durch das Backend des Nutzer:innenkontos würde eine sog. „Umschlüsselung“ von Nachrichten[18] erfordern und ist daher explizit auszuschließen.
- **Lösung 4**: Die Regelung in § 41 Abs. 2a HVwVfG zum „Abruf nur nach Authentifizierung der berechtigten Person“ sollte dahingehend ergänzt werden, dass eine Hinterlegung des gewünschten Kommunikationskanals im Nutzer:innenkonto oder eine Identifizierung der betroffenen Person via eID den Anforderungen zur Authentifizierung der berechtigten Person genügt. Die berechtigte Person sollte dabei nachweisen, dass sie Zugriff auf den hinterlegten Kommunikationskanal hat. Hierzu sendet das Nutzer:innenkonto einen Token an den hinterlegten Kommunikationskanal, der anschließend von der berechtigten Person im Nutzer:innenkonto eingegeben werden muss (analog zur Freigabe von Zahlungen via SMS-TAN).

3.3.2 Unerklärliche Defizite in der Umsetzung der Nutzer:innenkonten-Postfächer

- **Problem**: Eigenentwicklungen der öffentlichen Verwaltung entsprechen nach wie vor häufig nicht dem Stand von Wissenschaft und Technik. Auch die Begründung des vorliegenden Gesetzesentwurfs offenbart Defizite in der Umsetzung der Nutzer:innenkonten-Postfächer: „Da die Erfassung und Protokollierung des tatsächlichen Abrufs und damit eine beweissichere Feststellung des tatsächlichen Zugangs durch die am Portalverbund beteiligten Behörden gegenwärtig technisch zu aufwändig und auf absehbare Zeit nicht durchgängig gewährleistet ist […]“ / „[…] da es derzeit technisch noch nicht durchgängig möglich ist, den tatsächlichen Abruf des Verwaltungsaktes zu protokollieren und an das zuständige Fachverfahren zurückzumelden“. Die Argumentation, diese beweissichere Feststellung sei „technisch zu aufwändig“, kann nicht nachvollzogen werden. Entsprechende technische Verfahren sind etabliert. Eine entsprechen-

[18] Entschlüsselung und Wieder-Verschlüsselung von Nachrichten durch das Nutzer:innenkonto zum Zwecke der Vermittlung zw. der zustellenden Behörde und dem Kommunikationsdienst der betroffenen Person

de Lesebestätigungsfunktion findet sich in allen gängigen Messenger-Apps und wird auch von nahezu allen gängigen E-Mail-Clients unterstützt. Bürger:innen ist nicht zuzumuten, aufgrund dieses technisch unbegründeten Mängels ein von der Verwaltung bereitgestelltes Postfach jederzeit im Blick zu behalten und Nachrichten innerhalb von drei Tagen aktiv abzurufen. Auch die Möglichkeit, sich über neue Nachrichten benachrichtigen zu lassen, ändert an dieser Tatsache wenig.

- **Lösung 1**: Zur Umsetzung des Stand der Technik sollten entsprechende Vorgaben im Gesetz ergänzt werden, statt das Gesetz den unzulänglichen Lösungen der öffentlichen Verwaltung anzupassen. Das Land Hessen sollte sich dafür einsetzen, die nötigen technischen Voraussetzungen im genutzten Nutzer:innenkonto umzusetzen.
- **Lösung 2**: Die Verpflichtung, eingegangene Nachrichten im Postfach des Nutzer:innenkontos jederzeit innerhalb von drei Tagen abzurufen, wird für eine dauerhaft niedrige Akzeptanz des Postfachs bei Verwaltungskund:innen sorgen. Zur Steigerung der Attraktivität und damit der Nutzungszahlen des Postfachs, sollte daher auf die Nutzer:innen-unfreundliche Zustellfiktion zugunsten der Regelung aus § 41 Abs. 2a HVwVfG verzichtet werden.
- **Lösung 3**: In § 41 Abs. 2a HVwVfG könnte die explizite Regelung aufgenommen werden, die in die von der betroffenen Verwaltungskund:in gewählte Kommunikationslösung integrierte Lesebestätigungsfunktion als gleichwertiges Mittel zur Bestätigung eines Abrufs von Nachrichten zuzulassen, sofern die zustellende Behörde entsprechende Protokollierungspflichten erfüllt. Die adressierte Person ist auf diesen Umstand explizit hinzuweisen.

3.3.3 Zeitgemäße technische Qualität der Nutzer:innenkonten-Postfächer sicherstellen

- **Problem**: Im aktuellen Gesetzesentwurf fehlen Vorgaben zur Bereitstellung der Funktionalität des Postfachs über standardisierte, maschinenlesbare Schnittstellen (APIs). Eine Bereitstellung solcher standardisierter APIs würde Nutzer:innen den Abruf von Postfach-Nachrichten über frei gewählte Client-Software ermöglichen.
- **Lösung 1**: Analog zur Bereitstellung von Verwaltungsleistungen über maschinenlesbare Schnittstellen sollte die Vorgabe zur Bereitstellung der Funktionalitäten des Postfachs über eine standardisierte, maschinenlesbare Schnittstelle im Gesetzestext aufgenommen werden.
- **Lösung 2**: Daneben empfiehlt sich die Bereitstellung einer Referenzimplementierung (App) unter einer freien Softwarelizenz (Open-Source) in enger Abstimmung/Kooperation mit Bund und Ländern. Die Wahlfreiheit der genutzten Client-Software (App) sollte explizit im Gesetzestext festgehalten werden.
- **Lösung 3**: Neben der Bereitstellung der App über die App-Stores bekannter Smartphone-Hersteller sollten von der Verwaltung bereitgestellte Apps immer auch ohne Registrierung bei

diesen Unternehmen nutzbar sein.[19] Die Möglichkeit der Nutzung einer App ohne vorherige Registrierung bei einem privaten Unternehmen sollte hierzu im Gesetzestext festgehalten werden.

3.3.4 Benachrichtigung über neue Postfach-Nachrichten

- **Problem**: Die in § 3b definierte Möglichkeit zur Benachrichtigung über neue Nachrichten im Postfach des Nutzer:innenkontos beschränkt sich auf das Kommunikationskanal E-Mail.
- **Lösung 1**: Zur Steigerung der Attraktivität des Postfachs sollte hier die Möglichkeit der Hinterlegung weiterer frei wählbarer, sicherer oder unsicherer Kommunikationskanäle (Messenger-Apps, SMS, …) geschaffen werden.
- **Lösung 2**: Im Gesetzestext sollte explizit definiert werden, dass eine Benachrichtigung über unsichere Kanäle keine unverschlüsselten Inhaltsdaten enthalten darf. Ein Hinweis wie “Es liegen neue Nachrichten vor” sollte aber auch über unsichere Kanäle möglich sein.

3.4 § 4 Informationen zu Behörden und über ihre Verfahren in öffentlich zugänglichen Netzen

- **Problem**: Die Neuregelung zur Bereitstellung allgemeiner Leistungsinformationen gemäß FIM ist grundsätzlich sehr zu begrüßen. Es fehlen jedoch Vorgaben zur Bereitstellung der Leistungsinformationen in maschinenlesbarer Form über öffentlich erreichbare Schnittstellen.
- **Lösung 1**: Der bestehende Abs. 2 sollte um die Vorgabe erweitert werden, dass die genannten Informationen in maschinenlesbarem Format erfasst und bereitgestellt werden müssen. Statt einer Bereitstellung der Informationen über behördliche Webseiten in unstrukturiertem Format, empfiehlt sich die einheitliche Pflege der Informationen im Hessen-Finder.
- **Lösung 2**: Zur Umsetzung des Open-Data-Grundsatzes empfiehlt sich eine Verpflichtung zur öffentlichen Bereitstellung der gepflegten Informationen in einem standardisierten Format über eine maschinenlesbare Schnittstelle. Diese Vorgabe dürfte in weiten Teilen bereits durch die Bereitstellung über die Schnittstellen des Portalverbund Onlinegateway umgesetzt sein.[20] Neben der Bereitstellung der Daten über eine maschinenlesbare Schnittstelle sollten die Daten auch als vollständiger Datensatz im Rohformat zum Download bereitstehen.[21] Die Bereitstellung der Informationen über Schnittstellen kann auch von Behörden selbst genutzt werden, um Leistungsinformationen auf ihren eigenen Webseiten darstellen zu können. Dadurch entfällt der

[19] z.B. durch Bereitstellung einer APK-Datei auf einer Webseite der Verwaltung oder durch Nutzung alternativer App-Stores wie https://f-droid.org/
[20] siehe https://docs.fitko.de/resources/pvog/
[21] vgl. Bereitstellung der Leistungsinformationen in Baden-Württemberg unter https://www.service-bw.de/xzufi/

doppelte Pflegeaufwand auf der eigenen Webseite und im Hessen-Finder, was nicht zuletzt auch die Datenqualität im Hessen-Finder verbessern dürfte.

3.5 § 6 Nachweise

- **Problem**: Die aktuelle Regelung verhindert die Umsetzung von Security- und ggf. Privacy-by-Design-Ansätzen.
- **Lösung 1**: Die Nachweis-ausstellende Behörde muss in der Lage sein, die Einwilligung der betroffenen Person unabhängig prüfen zu können. Hierzu empfiehlt sich die Aufnahme einer Regelung analog zu Art. 16 Abs. 1 in Kombination mit Art. 14 Abs. 1 der Durchführungsverordnung (EU) 2022/1463.[22] Demnach können Nachweis-ausstellende Behörden verlangen, dass betroffene Personen auf eine von der Behörde bereitgestellte Webseite zwecks Identifizierung und Authentifizierung weitergeleitet werden. Nachweis-ausstellende Behörden werden so in die Lage versetzt, die Einwilligung der betroffenen Person eigenständig - z.B. mittels eID-Authentifizierung - zu prüfen, ohne auf die Sicherheit der von der Nachweis-einholenden Behörde bereitgestellten IT-Systeme vertrauen zu müssen (*Zero-Trust*).
- **Lösung 2**: Eine Übermittlung vollständiger Bescheide, Urkunden, etc. zwischen Behörden ist in den meisten Fällen nicht notwendig und sollte daher nach dem Grundsatz der Datensparsamkeit vermieden werden. Stattdessen sollte sich der Informationsaustausch auf die tatsächlich im Verwaltungsverfahren nötigen Fakten beschränken (z.B. die Information, *ob* ein entsprechender Bescheid für eine bestimmte Person vorliegt). Auf die Übermittlung weiterer Informationen (beispielsweise das Einkommen/Vermögen des Auszubildenden, der Ehegatt:in und von Eltern im Falle eines BAföG-Bescheids) sollte und kann verzichtet werden. Entsprechende Vorgaben zur Reduzierung des Informationsaustauschs auf die tatsächlich benötigten Fakten sollten im Gesetz aufgenommen werden.

3.6 § 17 Elektronische Aktenführung

- **Problem**: Der Gesetzentwurf verpasst die Chance, zeitgemäße Regelungen zur Führung von elektronischen Akten vorzugeben.
- **Lösung 1**: Die geplanten Regelungen zur elektronischen Aktenführung sollten ergänzt werden um Regelungen zur Speicherung von Daten und Dokumenten in offenen Dateiformaten sowie zu beweissichernden Maßnahmen, etwa entsprechenden kryptographischen Signaturen und Zeitstempeln, um eine Revisionsfähigkeit herzustellen. Eine nachträgliche Vollständigkeitsprüfung

[22] Durchführungsverordnung zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 (SDG-Verordnung) des Europäischen Parlaments und des Rates

ist sonst bei einer gezielten Löschung nicht durchführbar, was die Arbeit von Untersuchungsausschüssen oder des Rechnungshofes beeinträchtigen kann.
- **Lösung 2**: Die Erlaubnis für die Weiterführung papiergebundener Akten sollte kritisch geprüft und regelmäßig evaluiert werden. Wir schlagen daher vor, dass Behörden, die papiergebundene Akten weiterführen wollen, dies gegenüber dem CIO begründen. Der CIO sollte eine befristete Ausnahmegenehmigung erteilen dürfen. Dem Landtag sollte zur Evaluierung durch den CIO über die im Laufe eines Jahres erteilten Ausnahmen Bericht erstattet werden.
- **Lösung 3**: Vor dem Hintergrund der OZG-Umsetzung sollten Systeme zur elektronischen Aktenführung in der Lage sein, auch maschinenlesbare Datensätze (z.B. Anträge) zu verarbeiten bzw. zu speichern.

3.7 § 11 Amtliche Mitteilungs- und Verkündungsblätter

- **Problem**: Der Gesetzesentwurf verpasst die Chance, eine zeitgemäße digitale Verkündung von Gesetzen und Verordnungen einzuführen.
- **Lösung**: Rechtsvorschriften sollten barrierefrei in einem standardisierten, offenen und maschinenlesbaren Format verkündet und in einer Versionsverwaltung gepflegt werden, sodass auch Änderungen an Gesetzestexten einfach nachvollziehbar sind. Wir verweisen an dieser Stelle auf unsere grundsätzlichen Anmerkungen zum Format des Gesetzesvorschlags (s.o.).

3.8 § 13 Bevollmächtigte oder Bevollmächtigter der Landesregierung für E-Government und Informationstechnik

- **Problem**: Notwendige Kenntnisse und Fähigkeiten für die Rolle des CIO sind nicht definiert.
- **Lösung 1**: Mindestanforderungen für die Person des CIO schaffen: Ähnlich wie für den Hessischen Datenschutzbeauftragten sollten Anforderungen an die Person gestellt werden, etwa entsprechende, nachgewiesene Kenntnisse im IT-Management.
- **Lösung 2**: Schaffung der Rolle des Chief Technology Officer (CTO) mit entsprechenden Fähigkeiten zur Weiterentwicklung der IT-Infrastruktur des Landes Hessen mit Fokus auf die eingesetzten Technologien, wie sie in anderen Ländern und in der Privatwirtschaft bereits seit Jahren üblich ist.[23]

3.9 § 15 E-Government-Rat

- **Problem**: Die Entscheidungen des E-Government-Rat sind derzeit nicht öffentlich auffindbar und intransparent. Staatliches Verwaltungshandeln und die Funktionsweise der öffentlichen Verwal-

[23] In Großbritannien gibt es die Rolle des CTO beispielsweise bereits seit 2016.

tung sollten jedoch für Bürger:innen transparent und nachvollziehbar sein. IT-Entscheidungen können sich direkt auf die Ausgestaltung von Grundrechten auswirken oder diese einschränken und sollten daher in besonderem Maße transparent kommuniziert werden. Die nur sporadische Beteiligung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit entspricht keinem modernen Verständnis von Datenschutz und Informationsfreiheit und birgt die Gefahr, Digitalisierungsvorhaben zu verzögern, wenn wichtige datenschutzrechtliche Belange erst spät im Umsetzungsprozess bedacht werden.

- **Lösung 1**: Sämtliche Sitzungsunterlagen und Entscheidungen des E-Government-Rat sind proaktiv online zu veröffentlichen.
- **Lösung 2**: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit ist als ständiges Mitglied am E-Government-Rat zu beteiligen.

3.10 § 18 Digitaltaugliche Normen

3.10.1 Berücksichtigung der Belange der IT-Sicherheit und des Datenschutzes

- **Problem**: Die vorgeschlagenen zu prüfenden Aspekte im Rahmen des Digitalchecks berücksichtigen keine Belange der IT-Sicherheit und des Datenschutzes.
- **Lösung**: Im Rahmen des Digitalchecks ist die Berücksichtigung von Security- und Privacy-by-Design-Prinzipien zu prüfen. Insbesondere sollte sichergestellt werden, dass der Wortlaut des Gesetzes keine Annahmen über die technische Architektur von IT-Systemen trifft, die einer Umsetzung ebendieser Prinzipien widerspricht. Gesetzliche Vorgaben sollten sich auf die Definition von Anforderungen beschränken und darüber hinaus keine konkreten Vorgaben zu technischen Lösungen oder zur Architektur von IT-Systemen treffen. Technische Implikationen der gewählten Formulierungen sollten stets von qualifiziertem IT-Fachpersonal geprüft werden.

3.10.2 Grundsatz der offenen Daten

- **Problem**: Die vorgeschlagenen zu prüfenden Aspekte berücksichtigen keine Prüfung der Bereitstellung von offenen Daten nach dem Open-by-Default-Prinzip.
- **Lösung**: Im Rahmen des Digitalchecks ist zu prüfen, ob in dem vom Normungsvorhaben betroffenen Bereich Potentiale zur Bereitstellung von offenen Daten bestehen. Falls ja, sollten entsprechende Verpflichtungen zur Bereitstellung dieser Daten in das Normungsvorhaben aufgenommen werden.

3.10.3 Berücksichtigung der FIM-Bausteine Datenfelder und Prozesse

- **Problem**: Die vorgeschlagenen zu prüfenden Aspekte berücksichtigen den FIM-Baustein „Leistungen“, jedoch nicht die Bausteine „Datenfelder“ und „Prozesse“.
- **Lösung**: Neben der Bereitstellung von Leistungsinformationen in standardisierter Form, sollte im Rahmen des Digitalchecks auch die Verfügbarkeit von maschinenlesbaren Datenformaten (Baustein Datenfelder) und modellierten Geschäftsprozessen (Baustein Prozesse) sichergestellt werden. Um spätere (Detail-)Korrekturen in der Modellierung zu ermöglichen, ist hierbei jedoch von der Rechtsverbindlichkeit der im Rahmen des Digitalchecks erstellten Artefakten abzuraten. Dies schließt eine verpflichtende Nutzung von auf diesen Artefakten *basierenden* Daten- und Prozessmodellen jedoch nicht aus.

3.10.4 Automatisierung von Verwaltungsleistungen

- **Problem**: Es fehlen Regelungen zur Prüfung einer vollständigen Automatisierung von Verwaltungsleistungen.
- **Lösung**: Wir empfehlen, in Abs. 2 Nr. 4 die Prüfung der Möglichkeiten einer vollständigen Automatisierung von Verwaltungsleistungen vorzunehmen, sofern bei deren Bearbeitung kein Ermessensspielraum besteht.

3.10.5 Konsultationsverpflichtungen und öffentliche Kommentierungsphase

- **Problem**: Digitalisierungs-verhindernde Formulierungen oder die unzureichende Berücksichtigung von Security-/Privacy-by-Design-Ansätzen fallen häufig erst spät im Gesetzgebungsprozess auf.
- **Lösung**: Wir empfehlen eine Aufnahme von Konsultationsverpflichtungen und eine verpflichtende öffentliche Kommentierungsphase für alle Gesetzesvorhaben im Anwendungsbereich des Digitalchecks.

3.11 § 19 Experimentierklausel

- **Problem 1**: Wir sehen die Experimentierklausel kritisch. Aus unserer Sicht ist sie zu unbestimmt und erfüllt nicht die Voraussetzungen einer Rechtsgrundlage zur Datenverarbeitung nach Art. 6 Abs. 1 lit c DSGVO.
- **Problem 2**: Der oder die Hessische Beauftragte für Datenschutz und Informationsfreiheit ist weisungsfrei, eine Mitwirkung an der Genehmigung behördlicher Datenverarbeitung steht im Widerspruch zur unabhängigen Kontrolle der Datenverarbeitung in der öffentlichen Verwaltung.

4 Anmerkungen zum Änderungsantrag der SPD

4.1 Zu Nr. 1 a)

- Eine Ausweitung der Pflichten zur elektronischen Kommunikation auf Kommunen halten wir für sinnvoll und dringend notwendig, die Einschränkung auf Behörden, die mit dem Vollzug von Verwaltungsleistungen betraut sind, jedoch nicht. Die Kommunalebene ist für einen Großteil der Verwaltungskontakte verantwortlich. Eine Verpflichtung der Kommunalebenen zur Erreichbarkeit über verschlüsselte, digitale Kommunikationskanäle ist daher ein essentieller Baustein für eine höhere Zufriedenheit der Bevölkerung bei Verwaltungskontakten.
- Wie in unseren Anmerkungen zu § 3 beschrieben (s.o.), empfehlen wir die Aufnahme einer grundsätzlichen Möglichkeit zur verschlüsselten Kommunikation mit allen Behörden in § 3 Abs. 1 und eine Streichung des Abs. 2.

4.2 Zu Nr. 1 b)

- Die Regelung zum Unterschriftsfeld existiert bereits in § 3 Abs. 6. In § 3a Abs. 2 HVwVfG existiert bereits eine Regelung zum Schriftformersatz. Die vorgeschlagene Regelung zum Verzicht auf eine elektronische Signatur oder eine sonstige Form der Unterschrift, sofern keine gesetzliche Regelung dies anordnet, ist aus Gründen des Datenschutzes, zur Vermeidung von nicht-notwendigen Zugangshürden und zur Vermeidung von allgegenwärtigem Identifizierungs-Zwang, auch in Fällen, in denen dies eigentlich gar nicht nötig ist, (sog. *Over-Identification*) sehr zu begrüßen.

4.3 Zu Nr. 1 d)

- Die vorgeschlagene Regelung zur Evaluierung von internen Verwaltungsabläufen ist sehr zu begrüßen. Wir empfehlen zusätzlich die Aufnahme einer Prüfung, ob Verwaltungsleistungen vollständig automatisiert abgewickelt werden können.

4.4 Zu Nr. 1 f)

- Wir begrüßen die vorgeschlagenen Berichtspflichten, weisen jedoch darauf hin, dass eine entsprechende Transparenz nicht nur gegenüber dem Landtag, sondern auch gegenüber der Öffentlichkeit hergestellt werden sollte (*Open Government*). Wie oben bereits beschrieben, empfehlen wir die Bereitstellung von Kennzahlen als Offene Daten.

4.5 Zu Nr. 1 h)

- Die grundsätzliche Intention des neuen § 18 (Weiterbildung und Qualifizierung) ist zu begrüßen. Zur nachhaltigen Verbesserung der Umsetzungsfähigkeiten der öffentlichen Verwaltung erscheinen jedoch deutlich weitreichendere Maßnahmen nötig. Insbesondere vor dem Hintergrund des massiven Fachkräftemangels braucht es ganzheitliche Konzepte, wie die dringend benötigten Kompetenzen innerhalb der Verwaltung aufgebaut und langfristig gehalten werden können.

4.6 Zu Nr. 2

- Der Vorschlag ist zu begrüßen. Es fehlen jedoch Regelungen zur Bereitstellung von Förderinformationen als offene Daten und zur Verfügbarkeit der Verwaltungsverfahren über maschinenlesbare Schnittstellen (s.o.).

Vielen Dank für die Möglichkeit zur Stellungnahme.