Bundeskanzleramt

IKT-Tauglichkeit – „Digi Ready Check“

Überprüfung legistischer Vorhaben auf Auswirkungen in Bezug auf die Informations- und Kommunikationstechnologie
Leitfaden für Legistinnen und Legisten

Wien, 2025

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Gesamtumsetzung: VII/2 Legistik, Stammzahlenregisterbehörde, E-Government-Strategie sowie EU und Internationales
Wien, 2025. Stand: 19. Januar 2026

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an-post.vii-2@bka.gv.at.

Inhalt

Einleitung

Die Digitalisierung ist unbestritten ein Kernpunkt des gesellschaftlichen Wandels. Die digitale Welt muss – auch im Sinn der grundlegenden politischen Vorgaben und bestehenden Strategien – in der vorbereitenden legislativen Arbeit berücksichtigt werden. Der Einsatz von IT-Systemen ist in der Verwaltung und in der Gerichtsbarkeit daher auch nicht mehr wegzudenken. Praxisorientierte, barrierefreie und nutzerfreundliche digitale Lösungen und neue Technologien sind keine Ziele, sondern ein Mittel zur Gewährleistung moderner und effektiver öffentlicher Verwaltung. Dies nutzt nicht nur der Wirtschaft und der Bevölkerung, sondern auch der Verwaltung selbst.

Eine Vielzahl an Rechtsvorschriften ist jedoch noch nicht ausreichend „digitalisierungstauglich“. Neu zu erlassene Regelungen müssen von vornherein so konzipiert werden, dass sie „digitalisierungsfit“ und leicht verständlich sind. Damit kann die Entwicklung unnötig komplexer und teurerer IT-Lösungen hintangehalten werden.

Folgende Grundsätze sind dabei für die legistische Arbeit relevant:

1. Sicherstellen barrierefreier digitaler Kommunikation ohne Medienbruch
2. Einfache und klare Regeln, die technologieneutral formuliert sind (Ermöglichen der digitalen Ausführung)
3. Wiederverwenden von Daten (Once Only)
4. Einhalten des Datenschutzes und der Informationssicherheit unter Berücksichtigung von „Privacy by Design“ und „Privacy by Default“
5. Ermöglichen der Automatisierung
6. Berücksichtigen vorhandener Infrastruktur und von etablierten und vereinbarten Standards
7. Etablieren von Kontrollmöglichkeiten zur Fehlervermeidung

Die Praxis zeigt, dass Regelungsvorhaben von technischen Entwicklungen profitieren würden – jedoch kommt diese Erkenntnis oftmals verspätet im Vollzug oder anlässlich von Digitalisierungsprojekten. Es ist essenziell, möglichst früh im Regelungsvorhaben die Digitalisierungspotenziale zu berücksichtigen. Das zeigen auch zahlreiche internationale Best Practices. Das Ziel ist es, finanziellen und ressourcenintensiven Mehraufwand durch verspätet sichtbar gewordene Regelungsnotwendigkeiten zu vermeiden. Auch die

Europäische Kommission verfolgt dieses Anliegen und hat im Rahmen der „Better Regulation“ Initiative[1] Toolboxes entwickelt, die unter anderem ein Tool zu „Digital-Ready Policymaking“ enthalten. Die Bundesregierung hat 2023 anlässlich der Zielsetzung einer aktiven Digitalisierungspolitik beschlossen, als Maßnahme die Einführung eines „Digi-Check“ neuer Gesetze umzusetzen.[2] Der Digi-Check sollte dabei nicht als „Checkliste“ formal nachträglich „abgehakt“ werden, sondern flächendeckend bereits ab Beginn der Gesetzesvorbereitung zum Einsatz kommen, damit die Potentiale der Digitalisierung ausgeschöpft werden. Das Einbinden der Praktiker steigert die Usability und Nutzerorientierung.

Für eine moderne Verwaltung ist es bedeutsam, die Auswirkungen legistischer Vorhaben auf IT-Systeme zu prüfen und bereits in der Legistik den Einsatz von IT-Systemen technologieneutral zu ermöglichen. Die geplanten Regelungen sollen vorab untersucht werden, ob sie für eine digitale Abwicklung tauglich sind. Dies bedeutet, möglichst automatisierte Verfahren zu erlauben, die Nutzung der Register zu ermöglichen und vollständig medienbruchlose Verfahren vorzusehen.

Digitaltaugliche Gesetzgebung soll gleichzeitig

- die Rechtsvorschriften vereinfachen,
- Bürokratie für alle Normadressaten abbauen (sowohl für die Wirtschaft und die Bevölkerung als auch notwendigerweise für die Verwaltung im Hinblick auf den Erfüllungsaufwand und die Aufgabenlast) und
- Deregulierung bzw. Alternativen zu bürokratischen Prozessen durch Self-Service bewirken (vgl. z. B. No-Stop-Shop-Prinzip, Vorbild „GISA-Express“, Informationspflichten auf Notwendigkeit und Potential von Genehmigungsfiktionen prüfen).

---

[1] https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox_de

[2] Siehe zuletzt den Beschluss der Bundesregierung zum „Digital Austria Act“, MRV Beschlussprotokoll 61/10 vom 1.6.2023 – https://www.bundeskanzleramt.gv.at/medien/ministerraete/ministerraete-seit-dezember-2021/61-mr-1-jun.html). Einbegleitet wurde diese Initiative von dem von der EU finanzierten TSI-Projekt mit dem Titel „Identifying Strategies for the Development and Implementation of Digital-Ready Legislation“, welches als Ergebnis eine entsprechende Roadmap zur Einführung eines Digi-Checks in der wirkungsorientierten Folgeabschätzung (WFA) vorgeschlagen hat. In einem Folgeprojekt mit der Universität für Weiterbildung Krems wurden sodann relevante Kriterien ausgearbeitet, die in diesen Leitfaden eingeflossen sind.

Vollzugsvisualisierung macht Vereinfachungspotentiale sichtbar und unterstützt die Praxistauglichkeit.

Der gegenständliche Leitfaden bildet eine Weiterentwicklung der Leitfäden aus 2012 und 2018[3] und zielt deshalb darauf ab, Legistinnen und Legisten über häufige Berührungspunkte zwischen Rechtsvorschriften und IT-Systemen zu informieren und eine möglichst umfassende Betrachtung der wechselseitigen Auswirkungen zu fördern. Im Folgenden werden Fragen zu möglichen relevanten Teilbereichen eines vorliegenden Entwurfs gestellt, die dabei helfen sollen, Handlungsbedarf zu erkennen und diesen entsprechend den Leitlinien umzusetzen.

Im Anhang findet sich weiters eine „Checkliste", die einen kurzen Überblick über die relevanten Fragestellungen gibt, um eine rasche Prüfung eines Vorhabens zu gewährleisten.

Schließlich wurde auf EU-Ebene nun ein neues Instrument verabschiedet, das unmittelbar im Zusammenhang mit dem „Digi-Check" steht: die Verordnung (EU) Nr. 2024/903 über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (IEA)[4]. Art. 3 dieser Verordnung führt eine Verpflichtung für Einrichtungen der Union sowie für öffentliche Stellen ein, vor einer Entscheidung über neue oder wesentlich geänderte „verbindliche Anforderungen" eine Interoperabilitätsbewertung durchzuführen. Viele zu prüfende Kriterien und die konkreten Details im Rahmen dieser obligatorischen Interoperabilitätsbewertung sind erst auf EU-Ebene zu entwickeln (im Rahmen von Durchführungsrechtsakten sowie „Leitlinien"). Der vorliegende Leitfaden versucht aber bereits zum jetzigen Zeitpunkt, einige Fragestellungen und in Zukunft noch zu vertiefende Prüfpunkte zu berücksichtigen. Daher handelt es sich zwangsläufig um ein „lebendes Dokument", das auch im Lichte der dynamischen EU-Entwicklungen weiter zu entwickeln sein wird.

[3] Siehe das Rundschreiben des BMVRDJ-VD vom 29.8.2019, BMVRDJ-602.271/0009-V 2/2019, https://www.bundeskanzleramt.gv.at/dam/jcr:ed6bb4f2-8ea0-4294-8dcf-f45631235125/bmvrdj_2019_pruefung_legistischer_vorhaben_leitfaden_ikt-tauglichkeit_version_20.pdf samt Anhang (Leitfaden in der Version 2.0): https://www.bundeskanzleramt.gv.at/dam/jcr:6be12f88-56d0-49dd-af41-c23dadda292a/leitfaden_ikt-tauglichkeit_version_2_2018.pdf

[4] ABl. L 2024/903 vom 22.3.2024, https://eur-lex.europa.eu/eli/reg/2024/903/oj

1 Kommunikation / Interaktion zwischen Bürgerinnen und Bürgern, Unternehmen und Behörden

Bewirkt die Vollziehung der Regelung eine Interaktion zwischen Bürgerinnen und Bürgern, Unternehmen oder Behörden?

Die Rechtsvorschriften müssen die digitale Kommunikation unterstützen. Jedoch sind nicht zuletzt aufgrund des § 1a Abs. 3 E-GovG für Bürgerinnen und Bürger grundsätzlich nach wie vor alternative Lösungen vorzusehen.

Wenn die Frage mit JA beantwortet werden kann, etwa weil ein Antrag gestellt oder eine Ausfertigung zugestellt werden soll, dann sind die folgenden Fragen zu betrachten.

1.1 Wird digitale Kommunikation zum Regelfall gemacht oder zumindest gefördert?

Generell sollte jedes Regelungsvorhaben sowohl eine behördeninterne bzw. behördenübergreifende als auch zu Bürgerinnen und Bürgern sowie Unternehmen externe elektronische Kommunikation ermöglichen.

Verantwortliche des öffentlichen Bereichs, die durch Bundesgesetz eingerichtet sind, sind gemäß § 1c E-GovG sogar untereinander zum elektronischen Verkehr verpflichtet. Ausgenommen sind Angelegenheiten, die nicht geeignet sind, elektronisch besorgt zu werden.

Auch das Recht auf elektronischen Verkehr mit Behörden gemäß § 1a Abs. 1 E-GovG muss seitens der Behörde dahingehend berücksichtigt werden, als eben eine elektronische Kommunikation sowohl zur Behörde als auch zum Betroffenen ermöglicht wird (siehe genauer dazu unter 1.3 und 1.11).

1.2 Wird es möglich sein, einen Antrag elektronisch einzubringen?

Beachten Sie, dass es grundsätzlich möglich sein soll, einen Antrag elektronisch einzubringen (vgl. auch Pkt.1.3). Die Einleitung eines digital gestützten Verfahrens soll grundsätzlich durch die Antragstellenden mit Hilfe eines elektronischen Formulars und gegebenenfalls dem Nachweis der Identität durch einen elektronischen Identitätsnachweis erfolgen.

Im Falle der Anwendbarkeit des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG wird die (elektronische) Antragstellung in § 13 AVG geregelt. Falls innerhalb des Anwendungsbereiches des AVG abweichende verfahrensrechtliche Regelungen getroffen werden sollen, ist darauf zu achten, dass diese Regelungen der Intention des § 13 AVG entsprechen, soweit dem keine sachlichen Argumente entgegenstehen. Es soll grundsätzlich möglich sein, einen Antrag elektronisch einzubringen. Bestimmte Formulierungen verhindern eine solche Möglichkeit (z. B. „Vordrucke“, „Papiervordrucke“, Vorgaben zur Ausgestaltung von Planunterlagen oder ähnlichen Antragsunterlagen). So soll etwa vermieden werden, dass Anträge ausschließlich auf Papierformularen eingebracht werden dürfen oder die physische Vorlage von unterschriebenen Dokumenten sowie Urkunden verlangt wird.

In der Praxis haben sich insbesondere Online-Formulare für Eingaben etabliert (Erleichterung bei der Antragstellung durch orts- und zeitunabhängigen Zugang, strukturierte Datenerfassung, automatisierte Datenübernahme / Weiterverarbeitbarkeit, …).

Um elektronische Einbringungsmöglichkeiten zu erfüllen, sollte darauf geachtet werden, zumindest technologieneutrale Formulierungen zu wählen. Für die Ausgestaltung der Online-Formulare (z. B. Layout, Struktur, …) gibt es zwischen Bund und Ländern abgestimmte Empfehlungen (AG PS E-Government Styleguide)[5].

Die Festlegung einer gewissen Strukturierung der Eingaben bzw. Unterlagen steht auch im Einklang mit § 13 Abs. 2 AVG (formalisiertes Erfassen der Sachverhaltsinformationen in strukturierter und standardisierter Weise).[6] Nach § 13 Abs. 2 AVG können besondere

[5] https://neu.ref.wien.gv.at/at.gv.wien.ref-live/ag-ps-e-government-stylguide

[6] Vgl. Mayrhofer/Parycek, Digitalisierung des Rechts – Herausforderungen und Voraussetzungen, in ÖJT (Hrsg), ÖJT 2022, Band IV/1: Digitalisierung des Rechts – Herausforderungen und Voraussetzungen, 109.

Übermittlungsformen an Stelle von E-Mails vorgesehen werden, technische Voraussetzungen und organisatorische Beschränkungen des elektronischen Verkehrs sind im Internet bekannt zu machen. Technische Voraussetzungen sind etwa „für die Abwicklung des Datenverkehrs erforderliche Spezifikationen (wie z. B. Schnittstellenbeschreibungen), die sich aus der Hard- und Softwareausstattung der Behörde ergeben". Organisatorische Beschränkungen sind Vorgaben hinsichtlich bestimmter „Formen der elektronischen Übermittlung (z. B. Webformulare), Beschränkungen auf bestimmte elektronische Adressen".[7]

In Angelegenheiten der öffentlichen Abgaben gelten die Vorgaben des § 86a BAO, der FinanzOnline-Verordnung 2006 (FOnV 2006) und der FinanzOnline-Erklärungsverordnung (FOnErklV).

Falls technische oder organisatorische Beschränkungen des elektronischen Verkehrs zwischen der Behörde und den Beteiligten geregelt werden sollen (so etwa die Festlegung von zulässigen Dateiformaten oder -größen), wäre darauf zu achten, dass diese den zwischen Bund, Ländern, Städten und Gemeinden (Gremium BLSG) abgestimmten Empfehlungen entsprechen (siehe dazu: Archiv Internet policy: Dokumentenformate[8])

Falls der Antrag eine Angelegenheit betrifft, die vom Anwendungsbereich des Dienstleistungsgesetzes – DLG oder der Landesgesetze über den Einheitlichen Ansprechpartner umfasst wird, wäre zu prüfen, ob das Anbringen gemäß § 10 Abs. 1 DLG auch elektronisch eingebracht werden kann. Gleichermaßen wäre zu prüfen, ob sich eine Verpflichtung zum elektronischen Datennachweis aufgrund der SDG-VO [9]ergibt. Soweit ein Antrag bei (einem ordentlichen, dem Bundesverwaltungs- oder Höchst-) Gericht gestellt wird, wären die Besonderheiten des Elektronischen Rechtsverkehrs (s. insbesondere ERV 2021) zu bedenken.

[7] Vgl. Thienel/Schulev-Steindl, Verwaltungsverfahrensrecht, 5. Auflage (2009), 112.
[8] https://ref.gv.at/archiv-internet-policy-dokumentenformate
[9] Verordnung (EU) 2018/1724 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012, https://eur-lex.europa.eu/eli/reg/2018/1724/oj

1.3 Wird ein digitales Verfahren ohne Medienbruch ermöglicht?

Seit dem 1.1.2020 ist zu beachten, dass gemäß § 1a Abs. 1 E-GovG idF. BGBl. I Nr. 40/2017 jedermann in den Angelegenheiten, die in Gesetzgebung Bundessache sind, das Recht auf elektronischen Verkehr mit den Gerichten und Verwaltungsbehörden[10] hat. Ausgenommen sind lediglich Angelegenheiten, die nicht geeignet sind, elektronisch besorgt zu werden.

Zu beachten ist weiters, dass gemäß Art. 6 SDG-VO alle in Anhang II angeführten Verfahren vollständig online abgewickelt werden können müssen, sofern das jeweilige Verfahren eingerichtet worden ist. Darüber hinaus muss für sämtliche Online-Verfahren im Anwendungsbereich der SDG-VO gemäß Art. 13 SDG-VO eine diskriminierungslose Abwicklung auch für grenzüberschreitende Nutzerinnen und Nutzer gewährleistet sein, sodass die Vorschrift so formuliert werden muss, dass nicht indirekt Diskriminierungen oder Hürden für grenzüberschfreitende Nutzungen geschaffen werden (siehe auch Pkt 1.6).

Ausschließlich elektronische Kommunikation bedarf gemäß § 1a Abs. 3 E-GovG seit der Novelle BGBl. I Nr. 117/2024 einer ausdrücklich (bundes-)gesetzlichen Regelung. Im Fall einer bundesgesetzlichen Regelung für die mittelbare Bundesverwaltung wären jedoch die Grenzen in kompetenzrechtlicher Hinsicht zu beachten, Verpflichtungen zur Schaffung von technischen Voraussetzungen für Landesbehörden vorsehen zu können.

Nach Möglichkeit sind Begriffe (inkl. verwandter Verben) wie „Anschlag an der Amtstafel“ oder „Auflage“ zu vermeiden oder durch technologieneutrale Begriffe zu ersetzen (z. B. „Veröffentlichung“ statt „Anschlag“; „Einsichtsfrist“ statt „Auflagefrist“). Zumindest zusätzlich zur Einsichtnahme bei der Behörde soll eine Veröffentlichung verfahrensrelevanter Inhalte, die dauerhaft oder nur während eines bestimmten Zeitraums (innerhalb dessen oftmals – sofern gesetzlich vorgesehen – an die Veröffentlichung anknüpfend Handlungen gesetzt werden müssen) zu veröffentlichen sind, auch im Internet leicht zugänglich und auffindbar erfolgen. Nach bestimmten (bundes)gesetzlichen Regelungen wird eine Einreichung von Unterlagen (in analoger Form, und zwar) in mehrfacher Ausfertigung gefordert. Dies stellt eine Hürde für die

[10] Behörden sind im funktionellen Sinn (in Vollziehung der Gesetze) zu verstehen. D.h. dass diese Regelung gegenüber allen Organen anzuwenden ist, die hoheitliche Aufgaben erfüllen. Es sind daher Stellen wie z. B. Beliehene umfasst, soweit sie hoheitliche Befugnisse ausüben (vgl. ErläutRV 1457 BlgNR 25. GP).

Bestrebungen dar, ein Verfahren von der Einreichung bis zum Bescheid ganzheitlich online und digital abwickeln zu können.

1.4 Wird ein antragloses bzw. No-Stop-Verfahren ermöglicht?

Verfahren werden üblicherweise entweder von Amts wegen oder auf Antrag eingeleitet. Ein No-Stop-Verfahren wird bei Vorhandensein einer bestimmten Datenlage automatisch, das heißt ohne Antrag, gestartet und durchgeführt. Gegenstand von derartigen Verfahren kann insbesondere die Gebührlichkeit staatlicher Leistungen sein. In einigen Fällen wurde ein solches Verfahren bereits etabliert (z. B. die antragslose Familienbeihilfe gemäß § 10a FLAG 1967 und die antragslose Arbeitnehmerveranlagung gemäß § 41 Abs. 2 Z 2 EStG 1988). No-Stop-Verfahren können den Zugang zum Recht (zu staatlichen Leistungen) erleichtern und verwaltungsökonomische Vorteile mit sich bringen.

1.5 Werden analoge Nachweispflichten vermieden bzw. durch digitale nutzerfreundliche Äquivalente ergänzt (Once Only)?

Mindestanforderung an die gesetzliche Bestimmung sollte sein, dass analoge Nachweise durch digitale Äquivalente ersetzt werden können (siehe dazu auch Kapitel 3).

Im Sinn des Once Only Prinzips werden Nachweis- und Vorlagepflichten soweit möglich durch verpflichtende (automationsunterstützte bzw. automatisierte) Registerabfragen ersetzt und der Register- und Systemverbund (§ 6 USPG) sollte gesetzlich vorgesehen werden. Die Gesetze forcieren Registermodernisierung und -vernetzung und legen fest, welche Daten Ausgangsbasis für andere Register bzw. Datenbanken sind (z. B. ZPR als führendes Register der Personenstandsdaten als Basis für ZMR). Damit soll auch die Registerqualität steigen, was zu einem höheren Automatisierungsgrad führt.

Zur Vermeidung der Forderung von Nachweisen bestehen mittlerweile mehrere Konstellationen:

- Gemäß § 7 USPG muss bereits bei der Ausarbeitung von Entwürfen für ein Gesetz, eine Verordnung oder eine Maßnahme grundsätzlicher Art, welche eine Informationsverpflichtung (Nachweiserbringung) enthalten soll, die

Informationsverpflichtungsdatenbank abgefragt werden, um eine Nutzung dieser vorhandenen Daten zugrunde zu legen (vgl. dazu auch Pkt. 2.3)

- Gemäß § 17 Abs. 2 E-GovG haben Behörden, die die Richtigkeit von personenbezogenen Daten zu beurteilen haben, die in einem elektronischen Register eines Verantwortlichen des öffentlichen Bereichs enthalten sind, nach Maßgabe der technischen Möglichkeiten, wenn die Einwilligung des Betroffenen zur Datenermittlung oder eine gesetzliche Ermächtigung zur amtswegigen Datenermittlung vorliegt, die Datenermittlung im Wege des Datenfernverkehrs, selbst durchzuführen. Die erforderliche Datenabfrage wäre primär direkt – über den Register- und Systemverbund (RSV) gemäß § 6 Abs. 2 USPG – aus den Registern zu beziehen. Demnach können Daten auf ihre Richtigkeit geprüft werden. Nach dem Gesetzeswortlaut und dem BLSG-Leitfaden11 muss eine betroffene Person daher zwar die Nachweise für die Richtigkeit ihrer Angaben nicht mehr erbringen, aber sie muss die Daten bekanntgeben. Das Ziel ist, dass – sofern die Person identifiziert ist – die Daten amtsseitig erhoben und gegebenenfalls die Formularfelder automatisch befüllt werden.
  Bei grenzüberschreitenden Verfahren im Anwendungsbereich der SDG-VO soll die Datenermittlung im Wege des SDG-Once-Only Systems erfolgen (siehe dazu gleich Pkt. 1.6).

Eine ausdrückliche Rechtsgrundlage ist für Rechtsunterworfene und Rechtsanwendende transparent (Art 18 B-VG; § 1 Abs. 2 und § 4 Abs. 3 Z 1 DSG). Dies fördert medienbruchfreie Verfahren, steigert die Effizienz und Datenqualität und beschleunigt die Verfahrensführung durch Automatisierung.

Davon unberührt bleibt die Ermittlungspflicht der Behörde gemäß § 39 Abs. 2 AVG, wonach die Ermittlung jener Daten zulässig ist, die nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet (plausibel) sind.[12] Es handelt sich dabei nicht um eine Erlaubnis, alle erforderlichen Register abfragen zu dürfen, sondern nur um eine Klarstellung, dass alle rechtlich zulässigen Mittel ausgeschöpft werden können.

---

[11] Bund-Länder-Städte-Gemeinde (BLSG), Leitfaden zu § 17 Abs. 2 E-GovG 2.0.1.

[12] Vgl. Hengstschläger/Leeb, AVG § 39 RZ 7 (Stand 1.4.2021, rdb.at), die unter Bezug auf ein Erkenntnis des VwGH ausdrücklich festhalten: „Die Schaffung der für die Entscheidung notwendigen sachverhaltsmäßigen Grundlagen ist danach also auch im Fall der Verfahrenseinleitung auf Antrag die amtswegig wahrzunehmende Aufgabe der Behörde.“ Vgl. dazu ua. auch BVwG 27.05.2020, W214 2224203-1; 16.12.2018, W211 2179560-1; 18.12.2019, W211 2213604-1.

1.6 Berücksichtigt die Regelung, dass digitale Verfahren auch grenzüberschreitend bzw. für Personen/ Unternehmen aus anderen EU-Mitgliedstaaten diskriminierungsfrei abwickelbar sind?

Gemäß Art. 13 SDG-VO ((EU) 2018/1724) ist sicher zu stellen, dass ein auf nationaler Ebene festgelegtes Verfahren nach Art. 2 Abs. 2 lit. b, auf das nicht grenzüberschreitende User online zugreifen und online abwickeln können, auch grenzüberschreitenden Usern diskriminierungsfrei mit Hilfe derselben oder einer alternativen technischen Lösung online zugänglich und abwickelbar ist. Dies betrifft beispielsweise die Notwendigkeit, dass englischsprachige Informationen verfügbar, dass qualifizierte elektronische Signaturen aller Mitgliedstaaten verwendbar sein müssen oder dass die Nutzung von anerkannten eIDs der anderen Mitgliedstaaten möglich sein muss, sofern eine sichere Authentifizierung (mit ID Austria) gefordert ist. Eine Diskriminierung grenzüberschreitender Nutzer wäre es etwa auch dann, wenn zB ein Online-Formular nur österreichische Adressen oder z. B. 4-stellige Postleitzahlen akzeptiert.

In diesem Zusammenhang ist auf die Verpflichtung für öffentliche Stellen hinzuweisen, die vor einer Entscheidung über neue oder wesentlich geänderte „verbindliche Anforderungen“ (z. B. Gesetz, Verordnung etc.) die damit „transeuropäische digitale öffentliche Dienste“ regeln, bereitstellen, verwalten oder erbringen eine Interoperabilitätsbewertung gemäß Art. 3 Abs. 1 IEA durchzuführen haben.

1.7 Berücksichtigen die Regelungen die rechtlichen Anforderungen an die Barrierefreiheit?

Die Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen (Web-Accessibilty Richtlinie) wurde in Bundes- und Landesrecht umgesetzt.[13] Demnach sind Websites und mobile Anwendungen so zu gestalten, dass diese für die Nutzer, insbesondere für Menschen mit Behinderungen,

[13] Vgl. § 3 Abs. 2 Web-Zugänglichkeits-Gesetz, § 31a Burgenländisches Antidiskriminierungsgesetz, § 46 Kärntner Landes-Gleichbehandlungsgesetz 2022, § 12 NÖ Antidiskriminierungsgesetz 2017, § 15b Oö. Antidiskriminierungsgesetz, § 4c Salzburger Teilhabegesetz, § 1 Steiermärkisches Web-Zugangs-Gesetz, § 14b Tiroler Antidiskriminierungsgesetz 2005, § 10a Vorarlberger Antidiskriminierungsgesetz, § 10a Wiener Antidiskriminierungsgesetz.

besser zugänglich werden (technische Anforderungen an die Barrierefreiheit unter https://www.w3.org/WAI/).[14] Die Websites und mobilen Anwendungen sind besser zugänglich zu machen, indem sie wahrnehmbar, bedienbar, verständlich und robust gestaltet sind. In diesem Zusammenhang sind auch die sonstigen Bestimmungen, die die Barrierefreiheit adressieren, wie etwa Art. 7 B-VG oder das Bundes-Behindertengleichstellungsgesetz zu beachten.

1.8 Wird ein Antragsteller elektronisch identifiziert und ist dabei sichergestellt, dass die Funktion E-ID (ID Austria) für die eindeutige Identifikation einer Person eingesetzt wird?

Wenn eine natürliche Person eindeutig identifiziert werden soll bzw. muss (§ 3 Abs. 1 E-GovG; BLSG Spezifikation Sicherheitsklassen Version 4.0; Vorgaben iSd rechtlichen Rahmenbedingungen der Netz- und Informationssicherheit), ist ein Einsatz der Funktion E-ID (vgl. § 4 E-GovG) zweckmäßig. Diese ermöglicht eine eindeutige elektronische Identifikation und die einschreitende Person kann den Antrag mit dem E-ID (ID-Austria) qualifiziert elektronisch signieren; die qualifizierte elektronische Signatur ist der handschriftlichen Unterschrift grundsätzlich rechtlich gleichgestellt (vgl. Art. 25 Abs. 2 eIDAS-VO[15] iVm § 4 Abs. 1 Signatur- und Vertrauensdienstegesetz (SVG)).

Bei den Umsetzungen, die eine sichere Identitätsfeststellung mittels E-ID (ID-Austria) verlangen, muss jedenfalls auch sichergestellt werden, dass die gemäß Art. 6 Abs. 2 eIDAS-VO gegenseitig anzuerkennenden elektronischen Identifizierungsmittel anderer Mitgliedstaaten (sofern das Sicherheitsniveau dieser notifizierten elektronischen Identifizierungsmitteln dem Sicherheitsniveau „hoch“ entspricht) gleichwertig verwendet werden können. Die Vorschrift muss daher so formuliert sein, dass sie dem nicht entgegensteht. Gegebenfalls könnte bei ausschließlicher Nennung des E-ID im Gesetzeswortlaut in den Erläuterungen klarstellend auf diese gegenseitige Anerkennung

[14] Als zusätzliches Beispiel kann etwa § 29 Abs. 7 Zustellgesetz (Leistungen der Zustelldienste) genannt werden: „Die Zustellleistung (Abs. 1) ist so zu erbringen, dass für behinderte Menschen ein barrierefreier Zugang zu dieser Leistung nach dem jeweiligen Stand der Technik gewährleistet ist.“

[15] Verordnung (EU) 2014/910 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257 vom 28.8.2014 S. 73

von elektronischen Identifzierungsmitteln gemäß Art. 6 Abs. 2 eIDAS-VO bzw. § 6 Abs. 5 E-GovG[16] hingewiesen werden.

1.9 Sofern vertretungsweises Handeln ermöglicht wird, ist sichergestellt, dass eine Einzelvertretungsbefugnis mittels E-ID (ID Austria) genutzt werden kann?

Der E-ID (ID-Austria) ermöglicht im Falle einer bestehenden Einzelvertretungsbefugnis eine entsprechende Stellvertretung für natürliche als auch nicht-natürliche Personen (vgl. § 5 E-GovG).

1.10 Wird ein Unterschriftserfordernis geregelt und ist sichergestellt, dass dieses mittels qualifizierter Signatur umgesetzt werden kann?

Ein Unterschriftserfordernis iSd § 886 ABGB sollte nur normiert werden, wenn dies für das konkrete Verfahren tatsächlich erforderlich ist. Das Erfordernis der Schriftform wird– sowohl bei konventionell als auch bei auf technische Weise eingebrachten Anbringen – im Allgemeinen auch ohne Unterschrift des Einschreiters Genüge getan.[17] Ein allfälliges Unterschriftserfordernis sollte grundsätzlich auch elektronisch erfüllt werden können. Die qualifizierte elektronische Signatur erfüllt gemäß Art. 25 Abs. 2 eIDAS-VO iVm § 4 Abs. 1 SVG das rechtliche Erfordernis der Schriftlichkeit im Sinne des § 886 ABGB. Durch die Verwendung des elektronischen Identitätsnachweises (ID Austria) kann eine qualifizierte elektronische Signatur erstellt werden und somit das Unterschriftserfordernis auch elektronisch erfüllt werden. Zu beachten ist in der technischen Umsetzung, dass jegliche qualifizierte Signatur gleichermaßen verwendet werden können muss, sodass die Umsetzungslösung nicht ausschließlich auf eine Signatur mittels ID Austria abstellen darf, sondern auch die Möglichkeit gegeben werden muss, das zu signierende Dokument auf andere Weise qualifiziert zu signieren (z. B. durch die Möglichkeit des Downloads des

[16] § 6 Abs. 5 E-GovG: Elektronische Identifizierungsmittel eines anderen Mitgliedstaats der Europäischen Union, die die Anforderungen des Art. 6 Abs. 1 eIDAS-VO erfüllen, können bei Verantwortlichen des öffentlichen Bereichs wie ein E-ID für Zwecke der eindeutigen Identifikation im Sinne dieses Bundesgesetzes verwendet werden.

[17] Vgl. Hengstschläger/Leeb, AVG § 13 Abs. 4 RZ 23

Dokuments, Anbringen der qualifizierten Signatur in der gewohnten Nutzerumgebung und Upload des signierten Dokuments).

Es sollten daher Begriffe wie „auf Papier“ bzw. „Vordrucke“ etc., die eine elektronische Unterschriftsleistung nicht ermöglichen, vermieden werden. (Verwendung zumindest technologieneutraler Formulierungen)

In Angelegenheiten der öffentlichen Abgaben gilt § 86a Abs. 1 BAO, demzufolge das Fehlen einer Unterschrift keinen Mangel darstellt, die Abgabenbehörde und das Verwaltungsgericht jedoch, wenn es die Wichtigkeit des Anbringens zweckmäßig erscheinen lässt, dem Einschreiter die unterschriebene Bestätigung des Anbringens mit dem Hinweis auftragen können, dass dieses nach fruchtlosem Ablauf einer gleichzeitig zu bestimmenden angemessenen Frist als zurückgenommen gilt.

Der Einsatz von (Rund-)Siegeln und Stempeln sollte nicht mehr normiert werden. Sofern erforderlich, sollte die Verwendung elektronischer Siegel vorgesehen werden. Jedenfalls sollte eine elektronische Abwicklung mittels elektronischer Siegel ermöglicht werden.

1.11 Wird eine elektronische Zustellung ermöglicht?

Die elektronische Zustellung von Dokumenten ist, soweit die für das Verfahren geltenden Vorschriften nicht anderes bestimmen, im 3. Abschnitt des Zustellgesetzes (ZustG) geregelt. Wenn abweichende Regelungen getroffen werden (vgl. betreffend die Zulässigkeit Art. 11 Abs. 2 B-VG), sollte sichergestellt werden, dass eine elektronische Zustellung nicht ausgeschlossen wird. Insbesondere die elektronische Zustellung über einen elektronischen Zustelldienst sollte ermöglicht werden. Wenn das Verfahren eine Angelegenheit betrifft, die vom Anwendungsbereich des Dienstleistungsgesetzes umfasst ist, wäre sicherzustellen, dass das Dokument gemäß § 10 Abs. 2 DLG auch elektronisch zugestellt werden kann. Für den Justizbereich (ordentliche Gerichtsbarkeit) wären die Besonderheiten des Elektronischen Rechtsverkehrs (ERV 2021) zu bedenken.

Spätestens seit dem 1.1.2020 ist zu beachten, dass gemäß § 1a E-GovG idF. BGBl. I Nr. 40/2017 jedermann in den Angelegenheiten, die in Gesetzgebung Bundessache sind,

das Recht auf elektronischen Verkehr mit den Gerichten und Verwaltungsbehörden[18] hat. Ausgenommen sind lediglich Angelegenheiten, die nicht geeignet sind, elektronisch besorgt zu werden. Unter den elektronischen Verkehr fällt auch die Zustellung von Dokumenten. Somit sollten auch die materienspezifischen Regelungen eine Zustellung in elektronische Form nicht verhindern. Als Vorteil der elektronischen Zustellung kann dabei hervorgehoben werden, dass gemäß § 1b E-GovG Unternehmen im Sinne des § 3 Z 20 Bundesstatistikgesetz 2000 grundsätzlich an der elektronischen Zustellung teilzunehmen haben, wodurch diese Empfängergruppe jedenfalls auch erreichbar sein sollte.

1.12 Werden in das Regelungsvorhaben die Perspektiven verschiedener Expertinnen und Experten miteinbezogen?

Die Einbeziehung von Expertinnen und Experten aus den allfenfalls das Regelungsvorhaben fachlich vollziehenden Dienststellen oder aus anderen tangierten Fachbereichen (z. B. IT oder Datenschutz[19]) zu einem möglichst frühen Zeitpunkt, fördert in der Praxis die möglichst rasche und reibungslose Umsetzung des Vorhabens unter geringen Adaptierungsschleifen zu einem späteren Zeitpunkt.

1.13 Kann das Verfahren aus der Perspektive der Betroffenen bzw. Nutzerinnen und Nutzern verständlich, zugänglich und einfach gestaltet werden?

Die Einbeziehung der von der geplanten Regelung Betroffenen erleichtert das Erkennen der Bedürfnisse und Anforderungen und somit auch die Gestaltung der Regelung als nutzerfreudlich. Dabei gelten sowohl Bürgerinnen und Bürger sowie Unternehmen als auch die vollziehenden Dienststellen als Betroffene. Deren Zufriedenheit steigert auch die Akzeptanz und somit die erfolgreiche Implementierung eines Regelungsvorhabens.

---

[18] Behörden sind im funktionellen Sinn (in Vollziehung der Gesetze) zu verstehen. D.h. dass diese Regelung gegenüber allen Organen anzuwenden ist, die hoheitliche Aufgaben erfüllen. Es sind daher Stellen wie z. B. Beliehene umfasst, soweit sie hoheitliche Befugnisse ausüben (vgl. ErläutRV 1457 BlgNR 25. GP). Siehe dazu jedoch für die Landes- und Gemeindeverwaltung § 25 Abs. 1 E-GovG.

[19] z. B. Datenschutzkoordinatoren oder Datenschutzbeauftragte

2 Datenverarbeitung

Bewirkt die Regelung in der Vollziehung die analoge oder digitale Verarbeitung von Daten?

Wenn die Frage mit JA beantwortet werden kann, dann sind die folgenden Fragen zu betrachten:

2.1 Werden mit der Regelung Datenermittlungen bzw. Informationsverpflichtungen vorgesehen, obwohl diese Informationen bereits in bestehenden Registern oder bei anderen Behörden verfügbar sind?

Es sollen nach Möglichkeit bereits existierende Verfahren ausgebaut werden („shared-service-Gedanke“). Dadurch kommt es zu Einsparungen bei Errichtung und Betrieb neuer Verfahren.

Eine gemeinsame Nutzung von personenbezogenen Daten (zB in Datenbanken) durch Behörden bzw. Einrichtungen ist nur unter Einhaltung der datenschutzrechtlichen Vorgaben (siehe insbesondere den Verhältnismäßigkeitsgrundsatz gemäß § 1 Abs. 2 DSG sowie die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 DSGVO) zulässig und gebietskörperschaftsübergreifend insbesondere das Doppeltürmodell[20] zu berücksichtigen. Es gilt jedoch zu beachten, dass Abfrageberechtigungen in Bundesgesetzen unterschiedlich ausgestaltet sind und es nicht in jedem Fall einer ausdrücklichen Befugnisnorm zum Erhalt der personenbezogenen Daten bedarf. Beispielsweise wird im Bereich von behördlichen Zustellungen regelmäßig eine ZMR-Abfrage durchgeführt, da die Wohnung oder eine sonstige Unterkunft als Abgabestelle und somit als Zustelladresse gilt (§ 2 Z 3 und 4 ZustG). Die gesetzlich

[20] vgl. Punkt 8.3 des Rundschreibens des Bundesministeriums für Justiz zur legistischen Ausgestaltung von Vorschriften über die Verarbeitung personenbezogener Daten vom 5. Februar 2025, GZ 2025-0.073.307. Das Doppeltürmodell kommt auch dann zur Anwendung, wenn der Materiengesetzgeber, der den Zugriff auf ein Register einrichten möchte, die Verarbeitung der betreffenden personenbezogenen Daten für Zwecke der Privatwirtschaftsverwaltung (oder auch für Zwecke privater Personen) anordnet.

übertragene Aufgabe, die in § 16a Abs. 4 Meldegesetz 1991 (MeldeG) gefordert wird, ergibt sich hier aus dem Erfordernis der Zustellung von Schriftstücken in behördlichen Verfahren. Demgegenüber reicht es bei Verknüpfungsanfragen im Sinne des § 16a Abs. 3 MeldeG nicht aus, dass die Daten zur Besorgung einer gesetzlich übertragenen Aufgabe erforderlich sind. Vielmehr bedarf es hier einer ausdrücklichen gesetzlichen Ermächtigung zur Abfrage von bestimmten personenbezogenen Daten (arg: „soweit dies gesetzlich vorgesehen ist“), in denen auch die Suchkriterien näher zu definieren sind. Im Bereich der („schlichten“) Hoheitsverwaltung bzw. wenn personenbezogene Daten aus diesem Bereich (weiter)verarbeitet werden, ist jedenfalls eine entsprechende gesetzliche Rechtsgrundlage erforderlich (siehe § 1 Abs. 2 DSG sowie iwS auch Art. 18 B-VG).

Ein Anwendungsbeispiel wäre etwa die Abfrage zentraler Register (z. B. ZMR, ZPR).

Zudem sind auch auf die Verwendung bereits veröffentlichter Daten, wie beispielsweise die Veröffentlichung geografischer Daten mit Personenbezug, die oben genannten datenschutzrechtlichen Grundsätze anzuwenden.

2.2 Sollen Daten kryptographisch gesichert verarbeitet (Authentizität des Inhalts) oder historisiert werden?

Um die Authentizität von elektronischen Daten zur gewährleisten, wird empfohlen, elektronische Signaturen einzusetzen (dies können einfache, fortgeschrittene oder qualifizierte elektronische Signaturen sein). Soweit es um die Sicherstellung der Integrität geht, wären auch andere kryptografische Mechanismen zweckmäßig.

2.3 Werden neue Meldepflichten (Informationsverpflichtungen) eingeführt?

Informationsverpflichtungen sind gemäß § 2 Z 1 USPG dann gegeben, wenn eine aus einer Rechtsvorschrift resultierende Pflicht eines Unternehmens oder einer Bürgerin oder eines Bürgers besteht, Informationen zusammenzustellen oder bereitzuhalten und diese – unaufgefordert oder auf Verlangen – einer Behörde oder anderen Institution zur Verfügung zu stellen oder zu übermitteln. Wird eine solche Informationsverpflichtung bei der Ausarbeitung von Entwürfen für ein Gesetz, eine Verordnung oder eine Maßnahme grundsätzlicher Art, welche eine Informationsverpflichtung für Bürgerinnen und Bürger

oder Unternehmen enthalten soll, formuliert, so ist gemäß § 7 USPG von der jeweils zuständigen Bundesministerin/vom jeweils zuständigen Bundesminister in der Informationsverpflichtungsdatenbank anzufragen, ob eine diesbezügliche Informationsverpflichtung bereits von einem bestehenden Gesetz, von einer bestehenden Verordnung oder von einer bestehenden Maßnahme grundsätzlicher Art begründet wird. Diesfalls hat die mit der Ausarbeitung des Entwurfs betraute Bundesministerin/der mit der Ausarbeitung des Entwurfs betraute Bundesminister nach Maßgabe der technischen Möglichkeiten und unter Einhaltung der datenschutzrechtlichen Vorgaben eine Nutzung dieser vorhandenen Daten ihrem/seinem Entwurf zugrunde zu legen. Liegt eine diesbezügliche Informationsverpflichtung nicht vor, so hat die mit der Ausarbeitung des Entwurfs betraute Bundesministerin/der mit der Ausarbeitung des Entwurfs betraute Bundesminister zu prüfen, ob die für ihren/seinen Entwurf erforderliche Informationsverpflichtung auf eine bereits bestehende ähnliche Informationsverpflichtung abgestimmt werden kann.

2.4 Werden Daten verarbeitet, die von Interesse für die Allgemeinheit sein könnten?

Im Sinne des Grundsatzes „konzeptionell und standardmäßig offen“ gemäß § 1 IWG 2022 soll die Verwendung offener Daten gefördert und die Weiterverwendung von Dokumenten erleichtert werden, insbesondere um dadurch die Erstellung neuer Informationsprodukte und -dienste zu unterstützen.

Sofern nicht datenschutzrechtliche oder andere gewichtige Gründe dagegensprechen, sollten vorhandene Dokumente von allgemeinem Interesse in einer frei zugänglichen Form als „Rohdaten“ zur Verfügung gestellt werden („open data“). Derartige Daten sollten bereits so gesammelt und verarbeitet werden, dass eine „open data Verwendung“ ohne nachträgliche Investitionen möglich ist. Datenformate und Schnittstellen wären daher im Vorfeld entsprechend zu konzipieren.

Im Übrigen ist auf die proaktive Veröffentlichungspflicht gemäß § 4 Informationsfreiheitsgesetz (IFG) hinzuweisen, wonach Informationen von allgemeinem Interesse (z. B. Gutachten, Studien und Verträge) von der informationspflichtigen Stelle von sich aus über ein zentrales Informationsregister gemäß § 5 IFG (data.gv.at) zugänglich zu machen sind. Die Prüfung, ob es sich um Informationen von allgemeinem Interesse

handelt, könnte wenn möglich bereits im legistischen Prozess vorweggenommen und in den Erläuterungen behandelt werden.

2.5 Sind Nutzungsbedingungen bzw. ein Prozedere für deren Anpassung für die Nutzung von Services vorgesehen?

Wenn vorgesehen sein soll, dass User vor Verwendung einer Applikation Nutzungsbedingungen akzeptieren, wird empfohlen, ein Procedere für die Änderung dieser Nutzungsbedingungen vorzusehen. Da Nutzungsbedingungen vorwiegend privatrechtliche Vereinbarungen sind, wäre im Einzelfall zu prüfen, ob eine Regelung zweckmäßig ist (z. B. USP-Nutzungsbedingungenverordnung). Jedenfalls sind hierbei insbesondere die entsprechenden anwendbaren Bestimmungen des ABGB, des UGB, des ECG, des TKG 2021 und allenfalls des KSchG zu berücksichtigen.

3 Datenschutz und Datensicherheit

Bedingt die Regelung Anforderungen an den Datenschutz und/oder die Datensicherheit?

Wenn die Frage mit JA beantwortet werden kann, dann sind die folgenden Fragen zu betrachten:

3.1 Ist es vorgesehen, dass personenbezogene Daten verarbeitet werden?

Bei der Verarbeitung personenbezogener Daten ist jedenfalls die unmittelbar anwendbare Datenschutz-Grundverordnung[21] (DSGVO) beachtlich. Sämtliche Regelungen im Zusammenhang mit der Verarbeitung personenbezogener Daten sind daher im Einklang mit der DSGVO zu gestalten (Begrifflichkeiten, Verarbeitungszweck, Grundsätze der Datensparsamkeit, Datenminimierung und Speicherbegrenzung sowie insbesondere Datenschutz durch Technikgestaltung („Privacy by Design“)).

Für die Vorgaben, die sich aus dem Grundrecht auf Datenschutz (§ 1 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999) sowie aus der DSGVO ergeben, darf auf das **Rundschreiben des Bundesministeriums für Justiz zur legistischen Ausgestaltung von Vorschriften über die Verarbeitung personenbezogener Daten vom 5. Februar 2025, GZ 2025-0.073.307**, verwiesen und um dementsprechende Beachtung ersucht werden.

3.2 Werden Personenidentifikatoren durch den Entwurf eingeführt (z. B. Unternehmenszahlen, Personenkennzahlen, …)?

Zu beachten ist, dass die vorgesehenen Identifikatoren den datenschutzrechtlichen Vorgaben entsprechen müssen. Bereichsspezifische Personenkennzeichen (bPK)

[21] Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO), ABl. Nr. L 119 vom 04.05.2016 S. 1, zuletzt berichtigt durch ABl. Nr. L 74 vom 04.03.2021 S. 35.

entsprechen bereits konzeptuell dieser Vorgabe und sollten daher bevorzugt eingesetzt werden.

Hinzuweisen ist in diesem Zusammenhang auch auf die Stellungnahme des Datenschutzrates vom 17. November 2010 betreffend die Verwendung des bPK in der Verwaltung und in aktuellen Regelungsvorhaben, in der der Datenschutzrat vor allem folgendes festhält:

„[…] Der Datenschutzrat hat sich bereits wiederholt ablehnend zur Verwendung der Sozialversicherungsnummer für Bereiche, die nicht der Ingerenz der Sozialversicherung unterliegen – quasi als „Personenkennzeichen" – ausgesprochen (vgl. GZ BKA-817.246/0004-DSR/2010 ua.)."

In diesem Zusammenhang wird auch auf die Zweckbindung der Versicherungsnummer gemäß § 460d ASVG hingewiesen (Zwecke der Sozialversicherung und des Arbeitsmarktservice).

3.3 Wird der Einsatz bereichsspezifischer Personenkennzeichen bzw. der Stammzahl geprüft?

Das Identitätsmanagement des österreichischen E-Governments verwendet zur eindeutigen Identifikation in Datenverarbeitungen gemäß §§ 8 ff E-GovG im Hinblick auf natürliche Personen das bereichsspezifische Personenkennzeichen[22] gemäß § 9 E-GovG und für Betroffene, die keine natürlichen Personen sind, die Stammzahl gemäß § 6 Abs. 3 E-GovG (Firmenbuchnummer, Ordnungsnummer des Ergänzungsregisters für sonstige Betroffene, Global Location Number/GLN, Vereinsregisternummer). Diese Kennziffern sind bevorzugt für die Identifizierung einzusetzen und um eine eindeutige Zuordnung im jeweiligen Bereich bzw. mit anderen Datenverarbeitungen (bei rechtlicher Zulässigkeit) auch technisch zu ermöglichen.

[22] Allgmeine Informationen zum bereichssspezifischen Personenkennzeichen siehe auch: https://www.bundeskanzleramt.gv.at/agenda/digitalisierung/stammzahlenregisterbehoerde/bereichsspezifische-personenkennzeichen/beschreibung.html

3.4 Sind Daten aufgrund gesetzlicher Bestimmungen oder technischer Standards durch Schutzmaßnahmen besonders zu sichern?

Regelungen betreffend Datensicherheitsmaßnahmen sind grundsätzlich nicht erforderlich; sie ergeben sich dem Grunde nach bereits aus Art. 32 DSGVO. Soll durch das Vorhaben eine besondere Schutzwürdigkeit von Daten normiert (§ 1 Abs. 2 DSG) oder bestehen diese bereits aufgrund anderer gesetzlicher Bestimmungen (z. B. Informationssicherheitsgesetz oder Netz- und Informationssystemsicherheitsgesetz), so sind diese auch entsprechend vorzusehen.

Der Schutz der Vertraulichkeit wird durch Sicherheitsmaßnahmen umgesetzt, die in den technischen Konzepten der IKT-Strategie des Bundes festgelegt werden (siehe dazu auch das Österreichische Informationssicherheitshandbuch[23]). Durch eine konsequente wiederkehrende Prüfung der Notwendigkeit der Datenverarbeitung (mit hohem Schutzbedarf) sowie durch Verarbeitung solcher Daten nur in Bereichen, in denen bereits entsprechende Sicherheitsmaßnahmen existieren, können die Kosten beträchtlich gesenkt werden.

3.5 Sollen gesonderte Haftungsregelungen bestehen, wenn Informationen unrichtig sind oder Daten missbräuchlich verarbeitet bzw. verändert werden?

Grundsätzlich ist die Haftung für einen Schaden, den der Bund, die Länder, die Gemeinden und sonstigen Körperschaften und Anstalten des öffentlichen Rechts durch ihr schuldhaftes Handeln in Vollziehung der Gesetze zugefügt haben, in Art. 23 B-VG und vor allem in den Bestimmungen des Amtshaftungsgesetzes abschließend geregelt. Außerdem darf auf die Haftungs- und Schadenersatzregelungen des Art. 82 DSGVO für den Fall von Verstößen gegen die DSGVO hingewiesen werden. Falls im Einzelfall Haftungsbeschränkungen vorgesehen werden sollen, wäre vor diesem Hintergrund die Zulässigkeit zu prüfen.

[23] https://www.sicherheitshandbuch.gv.at/

3.6 Kann durch Kontrollpflichten sichergestellt werden, dass eine unbefugte Manupulation bzw. Veränderung der Daten verhindert wird?

Die Datenintegrität hat zum Ziel, die unberechtigte Veränderung von Daten zu verhindern und damit Schaden für die betroffenen Personen und die Verwaltung zu vermeiden.

Ein Grundprinzip zur Verhinderung der Manipulation von Daten stellt etwa das Vier-Augen-Prinzip (z. B. Zugriffsrechte, Definition von Rollen und Rechten) dar. Inwieweit solche Sicherheitsaspekte beachtet werden sollen, hängt freilich von den konkreten Umsetzungsanforderungen ab und wäre im Einzelfall zu beurteilen.

3.7 Werden Anforderungen an die Verfügbarkeit (z. B. Betriebszeiten, Wiederherstellungsziele) von IT-Systemen gestellt?

Die Fristen für die Bearbeitung von Verwaltungsvorgängen bestimmen wesentlich die Kosten der IT-Systeme. Der Normtext verschweigt sich normalerweise dazu. Wenn jedoch bereits im Normtext verfügt wird, dass ein Register „jederzeit“ oder „während der Amtsstunden“ verfügbar sein muss, dann ist das eine unausweichliche Vorgabe für Umsetzung bzw. den Dienstleister. Idealerweise werden die Vorgaben für den IT-Betrieb in einem Service-Level-Agreement (SLA) mit dem Betreiber der IT-Systeme vertraglich geregelt. Bei der Definition der Anforderungen sollten vorab folgende Aspekte für eine möglichst exakte Einschätzung bedacht werden:

- Zeitliche Verfügbarkeit: Müssen die Systeme nur für den Verwaltungsbetrieb während der Amtsstunden verfügbar sein oder ist eine Verfügbarkeit rund um die Uhr gefordert?
- Verfügbarkeit für Zielgruppen: Ist die Verfügbarkeit nur für bestimmte Zielgruppen (z. B. Verwaltung) notwendig?
- Verfügbarkeit in Krisenfällen: Ist in Krisen- oder Katastrophenfällen ein Ausfall der IT-Anwendung akzeptabel oder müssen Vorkehrungen für katastrophensicheren Betrieb getroffen werden (z. B. Einhaltung von Fristen)?
- Ist im Falle einer Katastrophe ein eingeschränkter Betrieb (z. B. für eine kleinere Benutzergruppe in einem Krisenzentrum) erforderlich/möglich?
- Sind zusätzliche Übertragungssysteme mit besonderer Krisensicherheit für den Zugriff auf zentrale Systeme erforderlich?

3.8 Werden Maßnahmen gesetzt, um die technologische Souveränität (z. B. keine Abhängigkeiten von einzelnen Anbietern) sicherzustellen?

Technologische Souveränität ist ein Teilaspekt digitaler Souveränität, die die Fähigkeit beschreibt, in der (digitalen) Welt selbstbestimmt zu handeln und sich dem Willen anderer Akteure widersetzen zu können. Eine vollständige Unabhängigkeit im Sinne einer Autarkie in allen Technologiebereichen ist nicht der Anspruch digitaler Souveränität. Es sollten jedoch die Referenzen auf den bestehenden europäischen Rahmen (europäischen Erklärung zu den digitalen Rechten und Grundsätzen[24], Digitale Dekade[25], AI Continent Action Plan, Data Union Strategy, Rechtsrahmen z. B. Data Governance Act, Data Act, Interoperability Act) beachtet werden.

[24] Europäische digitale Rechte und Grundsätze | Gestaltung der digitalen Zukunft Europas
[25] Europas digitale Dekade: Ziele für 2030 | Europäische Kommission

4 IKT-Betriebssicht

Muss zur Umsetzung der Regelung ein IT-System oder eine IT-Lösung angepasst oder neu entwickelt werden?

Wenn die Frage mit JA beantwortet werden kann, dann sind die folgenden Fragen zu betrachten:

4.1 Werden bestehende E-Government-Instrumente und -bausteine (z. B. ID-Austria, elektronische Zustellung, RSV, Portalverbund, definierte Standards und Schnittstellen) genutzt?

In Österreich existiert schon eine Reihe von ausgezeichnet etablierten Instrumenten des E-Government (s. insb in diesem Zusammenhang auch die BLSG-Konventionen; ggf. sind weiters die Vorgaben des Interoperable Europe Act zu beachten), die nicht nur flächendeckend verfügbar sind, sondern auch gesetzlich eine Grundlage haben (z. B. ID Austria und bereichsspezifische Personenkennzeichen für die Identifizierung oder MeinPostkorb für die elektronische Zustellung etc.).

Es sollte möglich sein, behördenübergreifende Anwendungen elektronisch zu nutzen. Daher sollte im Regelungsvorhaben, soweit datenschutzrechtlich zulässig, die Grundlage dafür getroffen werden, dass bestehende E-Government Technologien (Portalverbund, zwischen Bund und Ländern abgestimmte Empfehlungen, Schnittstellen, …) genutzt werden.

Das einheitliche Festlegen und flächendeckende Nutzen dieser Standards und Schnittstellen ermöglicht das Ineinandergreifen der IT-Komponenten. Diese Interoperabilität soll nicht nur im Anwendungsbereich des Interoperable Europe Act (IEA) gefördert werden, sondern ist auch auf nationaler Ebene durch verpflichtend einzhaltende Standardisierungen im Sinn des Austrian interoperability framework sinnvoll. Eine solche verpflichtende Vorgabe von Standards ermöglicht es, dass kompatible IT-Komponenten entwickelt werden, die miteinander verzahnt werden können. Durch das Nutzen der bestehenden öffentlichen IT-Infrastruktur werden propritäre Lösungen und ressourcenintensive Dopplungen vermieden und behördenübergreifende Kohärenz

gewährleistet. Bestehendes ist soweit möglich zu nutzen, um effiziente, einheitliche und interoperable Lösungen (vgl. insbesondere auch „Lösungen für ein interoperables Europa“ gemäß Art. 7 Abs. 1 IEA für transeuropäische digitale öffentliche Dienste) zu gewährleisten.

4.2 Wurden für die Umsetzung Open-Source-Lösungen in Betracht gezogen?

Im Rahmen des IEA sollte die Verwendung von Open-Source-Lizenzen gefördert werden, um die Rechtsklarheit und die gegenseitige Anerkennung von Lizenzen in den Mitgliedstaaten zu verbessern.[26]

4.3 Wird berücksichtigt, dass die bestehende Infrastruktur genutzt werden kann, anstatt parallel separate, proprietäre Lösungen zu verwenden?

Wie für E-Government-Instrumente ist es auch im Bereich der allgemeinen technischen Infrastruktur zur Vermeidung von ressourcenintensiven Doppelungen geboten, möglichst auf bestehende Lösungen zurück zu greifen.

4.4 Wird berücksichtigt, dass das elektronische Verfahren auch auf mobilen Endgeräten (z. B. Smartphone, Tablet) nutzbar ist?

Die Marktdurchdringung von Smartphones ist sehr hoch in Österreich. Daher ist es eine logische Konsequenz, die digitalen Verwaltungsangebote möglichst flächendeckend für mobile Endgeräte anzubieten.

Im Sinne eines „Mobile First“-Ansatzes als Konzept für mobil optimiertes Webdesign sollen sich das Design bzw. die Struktur einer Website an der Usability auf mobilen

[26] Siehe Art. 4 und ErwG 36 IEA

Endgeräten (Smartphones) orientieren, um auch ein „Mobile Government“ zu ermöglichen.[27]

4.5 Ist die Art und Größe des Benutzerkreises/der Zielgruppe bestimmbar?

Je nach Benutzerkreis ergeben sich unterschiedliche Anforderungen. So soll etwa bereits im Vorfeld beurteilt werden, ob ein Verfahren grenzüberschreitend, bundesweit oder etwa (lediglich) behördenintern genutzt werden kann. Zudem könnte bereits eruiert werden, ob es sich bei den Usern um jedermann oder geschultes Fachpersonal handelt. Von der Beantwortung dieser Fragen hängt freilich auch ab, wie ein Verfahren konzipiert und welcher Schulungsaufwand dafür kalkuliert werden muss.

4.6 Ist bei der Umsetzung mit intensivem Einsatz von IKT oder dem Datenaustausch zwischen mehreren Partnern zu rechnen?

In diesem Fall sollte berücksichtigt werden, dass die Umsetzung komplexer IT-Verfahren zeitaufwändig ist. Kurze Umsetzungsfristen für die Implementierung eines Verfahrens bedeuten regelmäßig höhere Kosten. Das Vorsehen von entsprechenden Vorlaufzeiten (späteres Inkrafttreten einer gesetzlichen Regelung) kann diese Kosten senken – sofern diese Möglichkeit besteht und zweckmäßig ist.

Oftmals wird der 1. Jänner für das Inkrafttreten von Gesetzen gewählt. In der Praxis ist dies ein Termin, zu welchem die Verfügbarkeit von IT- Personal in der Regel reduziert ist. Außerdem ist mit dem gleichzeitigen Inkrafttreten von Gesetzen häufig auch eine Spitzenbelastung in der Vorbereitungsphase der Umsetzung verbunden. Diese Umstände sollten bei der Umsetzung legistischer Vorhaben, die die IKT betreffen, in die

[27] Siehe die Entwicklung von „E-Government“ zu „M-Government“ und die politische Zielsetzung, „mobile first“ voranzubringen, zB in der EU-Ministererklärung „Berlin Declaration on Digital Society and Value-based Digital Government“ https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government und auf globaler Ebene die von Österreich co-geleitete mobile Government Working Group der Weltbank mit der „How-To-Note“ der Weltbank zu mGovernment: documents1.worldbank.org/curated/en/099090502242339893/pdf/P16948204d12890d6081470029196913af6.pdf

Überlegungen miteinbezogen und „geeignete“ Umsetzungstermine (z. B. Releasetermin der betroffenen Software) vorausschauend festgelegt werden.

4.7 Ist eine hohe Abhängigkeit von technischen Systemen Dritter zu erwarten?

Eine Abhängigkeit von technischen Systemen Dritter stellt ein Risiko für die Verfügbarkeit des Systems sowie die Gefahr steigender Kosten dar und sollte daher bei der Festlegung von gesetzlichen Dienstleistern mitbedacht und möglichst vermieden werden.

4.8 Wird berücksichtigt, dass eingesetzte Technologien sich rasch ändern (zB durch technologieneutrale Formulierungen oder vereinfachte Anpassungsmöglichkeiten)?

Die Regelung sollte daher technologieneutral formuliert sein (z. B.: „unter Einsatz geeigneter technischer Mittel“). Alternativ sollte die Möglichkeit von (technischen) Durchführungsverordnungen in Betracht gezogen werden, um gegebenenfalls auf neue Anforderungen schnell und flexibel (ohne einen neuerlichen Gesetzgebungsprozess anstoßen und durchzführen zu müssen) reagieren zu können (z. B.: Kraftfahrgesetz-Durchführungsverordnung 1967 – KDV, Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung).

5 Digitale Kontrollmöglichkeiten

Gibt es in der Praxis Evidenz für Fehleranfälligkeiten?

Wenn die Frage mit JA beantwortet werden kann, dann ist die folgende Frage zu betrachten:

5.1 Können potentielle Betrugs- und Fehleranfälligkeiten über transparente digitale Überprüfungsmöglichkeiten gemindert bzw. verhindert werden?

Die Möglichkeit der digitalen Kontrolle und der Verhinderung von Betrug und Fehlern sollte berücksichtigt werden. Digitale Lösungen sollten für Kontrollzwecke genutzt werden können. Gleichzeitig sollte geprüft werden, ob durch das Regelungsvorhaben neue Betrugsmöglichkeiten eröffnet werden und wenn ja, wie das Kontrollverfahren geplant werden kann, um mit diesen Risiken umzugehen.

6 Einfachheit und Klarheit

Sind die Regeln klar, einfach, eindeutig und konsistent formuliert (keine Denksportaufgabe)?

Wenn Rechtsvorschriften viele Ausnahmen, Anforderungen oder Ermessensspielräume beinhalten oder unklar bzw. komplex formuliert sind, kann ihr Vollzug schwierig sein – auch digital. Einfache Regeln bedeuten nicht unbedingt einen kurzen Gesetzestext. Jedenfalls sollten überflüssige Wörter im Gesetzestext vermieden werden.

6.1 Regeln: Werden durch kohärente und logische Systematik eindeutige Entscheidungsstrukturen für die IT-Umsetzung formuliert?

Bei der legistischen Formulierung sollte generell darauf geachtet werden, dass Tatbestände in der Weise abgefasst werden, dass eine automatisierte elektronische Verarbeitung möglich ist: Unterschiedlich zu behandelnde Fallkonstruktionen sollten nicht in einer „gesetzestechnischen Einheit“ (Absatz, Ziffer, Litera, usw.) geregelt, sondern in getrennten „Einheiten“ behandelt werden. Andernfalls müssten für die IKT-Umsetzung künstliche Fallvarianten eingeführt werden, die den eindeutigen Gesetzesbezug für die Handhabung sowohl bei der Programmierung als auch für die Anwender erschweren, wodurch die Fehlerwahrscheinlichkeit erheblich steigt.

Insbesondere bei der Abfassung von Straftatbeständen sollte, um deren Anwendung durch Straf- und Sicherheitsbehörden, Staatsanwaltschaften und Gerichte zu erleichtern und eine möglichst einfache Erfassung in der IKT zu ermöglichen, darauf geachtet werden, dass Straftatbestände in gesonderten Paragraphen aufgenommen und diese mit deutlicher Überschrift („gerichtlich strafbare Handlung“, „Verwaltungsübertretungen“, „Strafbestimmungen“ oä) bezeichnet werden. Verschiedene Tathandlungen sollten in einzelne Absätze aufgenommen werden, verschiedene Varianten zumindest mit Ziffern bezeichnet werden. Nach Möglichkeit zu vermeiden wäre, in ein- und demselben Absatz unterschiedliche Strafdrohungen vorzusehen.

Folgende Aspekte sind dabei beispielsweise zu berücksichtigen:

- strukturiertes Format (siehe 2.5)
- präzise Definition der Syntax und Hierarchie
- semantische Klarheit (siehe 2.2 und 2.3), Vermeiden unbestimmter Rechtsbegriffe
- logische Verknüpfungen eindeutig formulieren (Wenn-Dann-Regeln), Querverweise oder Verschachtelungen können die maschinelle Verarbeitung erschweren
- strikte Trennung zwischen Tatbestand (Kriterien) und Rechtsfolge

6.2 Begriffe: Werden Rechtsbegriffe innerhalb des Regelungsvorhabens einheitlich und konsistent verwendet?

Nur durch die einheitliche Begriffsverwendung innerhalb des Regelgungvorhabens kann eine automatisierte Verarbeitung erfolgen.

6.3 Wird sichergestellt, dass dieselben Definitionen von Daten bzw. Begriffen verwendet werden, die bereits in Registern von Verantwortlichen des öffentlichen Bereichs existieren?

Bestehen in anderen Regelungsvorhaben Begriffe bzw. Datenbezeichnungen, die im geplanten Regelungsvorhaben dieselbe Bedeutung bzw. demselben Datum entsprechen, so ist eine entsprechend einheitliche Beriffsverwendung vorzusehen. Die einheitliche Verwendung von Begriffen mit derselben Bedeutung erleichtert in der Folge auch eine allenfalls automatisierte Verfahrensabwicklung.

6.4 Ist der Ablauf des Verfahrens im Gesetz so klar beschrieben, dass er sich in einzelne Arbeitsschritte (Workflow) gliedern lässt?

Die klar strukturierte Abgrenzung von allgemeiner Regel und allfälligen Ausnahmen erleichtert in der Folge auch eine allenfalls automatisierte Verfahrensabwicklung.

Idealerweise verfolgt der Aufbau des Regelungsvorhabens eine klar erkennbare Arbeitsaufgabenabfolge in einzelnen Schritten. Diese ablaufprozessartige Beschreibung

(Workflow) erleichtet in der Folge auch eine allenfalls automatisierte Verfahrensabwicklung.

7 Automatisierte Verfahrensabwicklung

Sofern ein Verfahren geregelt wird: Kann oder soll der Vollzug der Regelung (teil-) automatisiert erfolgen?

Voraussetzung für (Teil-)Automatisierung[28] ist in der Regel, dass die automatisierten Teile der Entscheidung nach streng objektiven Kriterien getroffen werden können. Dies ist dann der Fall, wenn kein Zweifel daran besteht, welche tatsächlichen Informationen relevant sind und welche Rechtswirkungen eintreten, wenn das eine oder das andere Kriterium vorliegt. Eine verstärkte Anwendung objektiver Kriterien zur Steigerung des Automatisierungsgrades öffnet Ressourcen für komplexere Fälle.

Wenn die Entscheidung oder Elemente einer Entscheidung auf einem Ermessensspielraum beruhen, wird der Umfang der Automatisierung regelmäßig eingeschränkt. Wenn Ermessensregeln festgelegt werden, sollte bereits zum Zeitpunkt der Gesetzgebung geprüft werden, ob es eine relevante Datengrundlage gibt, die in den Ermessensspielraum einbezogen werden sollte.

Wenn die Frage mit JA beantwortet werden kann, dann sind die folgenden Fragen zu betrachten:

7.1 Wird die Standardisierung des Verfahrensrechts unterstützt und Sonderverfahrensrecht vermieden?

Klare, einheitliche Vorgaben und Standardisierungen vereinfachen den Vollzug und führen zu Beschleunigung. Demgegenüber hemmt Sonderverfahrensrecht die Digitalisierung und Automatisierung: Es ist „essentiell, dass alle im AVG vorgesehenen Verfahrensschritte –

[28] Es darf darauf hingewiesen werden, dass das AVG einer automatisierten Entscheidung derzeit grundsätzlich entgegensteht und abweichende Materiengesetze an der Erforderlichkeitsschranke des VfGH zu messen wären. Zudem sind jedenfalls die Anforderungen des Art. 22 DSGVO zu beachten. Weiters wird beim Einsatz von KI auf die Risikoklassifizierungen des AI Acts hingewiesen.

vom Antrag über die Kundmachungen und mündliche Verhandlungen bis zur Bescheiderstellung mit Auflagen und der Klausulierung von Beilagen etc. – für alle Verfahren auf Basis unterschiedlicher Materiengesetze einheitlich, medienbruchfrei und benutzerfreundlich umsetzbar sind. Dies wird durch abweichende Verfahrensbestimmungen in den Materiengesetzen erschwert."[29]

7.2 Bestehen bereits die rechtlichen Grundlagen für das (teil-)automatisierte Verfahren?

Die Gesetzgebung sollte die vollständige oder teilweise digitale Umsetzung der Rechtsvorschriften unterstützen. Generell müssen die Vorschriften technologieneutral gegenüber spezifischen Anwendungen sein, um sicherzustellen, dass sie nicht die Verwendung von Technologien regeln, die später veraltet sind. Erfahrungen aus öffentlichen IT-Projekten sollten genutzt werden, damit die Anwenderinnen und Anwender sowie die rechtlichen, technischen und betriebswirtschaftlichen Kompetenzen von Anfang an und kontinuierlich in öffentliche Digitalisierungsprojekte einbezogen werden.

In einigen Fällen wurde ein solches Verfahren bereits etabliert; zu nennen sind etwa die antragslose Familienbeihilfe gemäß § 10a FLAG 1967 und die antragslose Arbeitnehmerveranlagung nach § 41 Abs. 2 Z 2 EStG 1988. In Österreich wurden im Jahr 2022 88 % des bestehenden Bedarfs an Einkommensteuererklärungen online abgedeckt. Der Ausbau der „Digitalen Verwaltung" ermöglicht allen Bürgerinnen und Bürger sowie Unternehmen, Amtsgeschäfte digital abwickeln zu können. Unabhängig vom digitalen Angebot muss aus Gründen der Inklusion grundsätzlich der Behördenweg auch weiterhin analog möglich sein (vgl. § 1 Abs. 1 letzter Satz, § 1a Abs. 3 E-GovG).

Beim Einsatz von Künstlicher Intelligenz ist insbesondere die Risikoklassifizierungen des AI Acts zu berücksichtigen.

[29] Wirthumer, Aspekte der (Teil-)Automatisierung des Verwaltungsverfahrens und der oberösterreichische Weg zum Digitalen Amt, in: Braun-Binder/Bußjäger/Eller, Auswirkungen der Digitalisierung auf die Zuordnung und Erlassung behördlicher Entscheidungen (2021), 105 mwN.

7.3 Werden die Rechtsvorschriften so formuliert, dass Ermessensentscheidungen auf Fälle beschränkt werden, in denen sie erforderlich sind?

Ermessensentscheidungen senken das Automatisierungspotential. „Konditional programmierte Verwaltungsvorschriften in Form von „Wenn-Dann“-Regeln eignen sich im besonderen Maße zur Automatisierung (…). Eventuell vorliegende Ermessensbegriffe sind auf ihre Vermessbarkeit zu überprüfen, um durchgehende vollumfängliche Automatisierung von Verwaltungsverfahren zu ermöglichen.“[30]

7.4 Wurde das Verfahren / die Datenflüsse visuell dargestellt?

Visualisierungen des Vollzugs eines Regelungsvorhabens unterstützen komplexe Sachverhalte und Auswirkungen der Regelung einfacher zu verstehen und darzustellen. Dabei können die Aspekte der Digitalsierung frühzeitig erkannt werden und entsprechend berücksichtigt werden. Außerdem können die Zusammenhänge (etwa bei der Wiederverwendung von Daten) und eventuelle Bruchstellen für die Umsetzung von automatisierbaren Prozessen aufgezeigt werden. Die Visualisierung kann auch als Basis für eine allfälllige autmatisierte Verfahrensabwicklung dienen und erleichtet diese in der Folge somit.

[30] Mayrhofer/Parycek, Digitalisierung des Rechts – Herausforderungen und Voraussetzungen, in ÖJT (Hrsg), ÖJT 2022, Band IV/1: Digitalisierung des Rechts – Herausforderungen und Voraussetzungen, 133.

8 Weiterführende Informationen

Digitales Österreich
(https://www.bundeskanzleramt.gv.at/agenda/digitalisierung/digitales-oesterreich.html)
Umfangreiche Seite des Bundeskanzleramts zu E-Government.

Reference Server (https://neu.ref.wien.gv.at/)
Auf dieser Webseite stehen die gemeinsam erarbeiteten Vorschläge der Arbeitsgruppen und die daraus resultierenden Ergebnisse in Form von Konventionen (Empfehlungen) bzw. weiteren Konzepten (Informationen) zur Verfügung.

Rundschreiben BMVRDJ-VD
(https://www.bundeskanzleramt.gv.at/agenda/verfassung/legistik/e-recht-legistische-richtlinien.html l)
Hier finden Sie Informationen zum elektronischen Rechtserzeugungsprozess (E-Recht), zur korrekten Verwendung von Formatvorlagen und zu Fragen, die hinsichtlich der legistischen Richtlinien oder anlässlich eines Begutachtungsverfahrens auftreten können.

Österreichisches Informationssicherheitshandbuch
(https://www.sicherheitshandbuch.gv.at/)
Das 2010 neu überarbeitete und neu strukturierte "Österreichische Informationssicherheitshandbuch" beschreibt und unterstützt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheits-Managementsystems in Unternehmen und der öffentlichen Verwaltung.

9 Anhang – „Digi Ready Check-Liste“

Digi Ready Check-Liste; Fragestellungen zur Prüfung eines Vorhabens

Tabelle 1 Bewirkt die Vollziehung der Regelung eine Interaktion zwischen Bürgerinnen und Bürgern, Unternehmen oder Behörden?

Frage	**Ja**	**Nein**	**siehe**
Wird digitale Kommunikation zum Regelfall gemacht oder zumindest gefördert?			1.1
Wird es möglich sein, einen Antrag elektronisch einzubringen?			1.2
Wird ein digitales Verfahren ohne Medienbruch ermöglicht?			1.3
Wird ein antragloses bzw. No-Stop-Verfahren ermöglicht? *z. B.: antragslose Familienbeihilfe*			1.4
Werden analoge Nachweispflichten vermieden bzw. durch digitale nutzerfreundliche Äquivalente ergänzt (Once Only)?			1.5
Berücksichtigt die Regelung, dass digitale Verfahren auch grenzüberschreitend bzw. für Personen/ Unternehmen aus anderen EU-Mitgliedstaaten diskriminierungsfrei abwickelbar sind? *z. B.: englischsprachige Informationen und die Möglichkeit der Verwendung qualifizierter elektronischer Signaturen aller Mitgliedstaaten*			1.6
Berücksichtigen die Regelungen die rechtlichen Anforderungen an die Barrierefreiheit?			1.7

Frage	Ja	Nein	siehe
Wird ein Antragsteller elektronisch identifiziert und ist dabei sichergestellt, dass die Funktion E-ID (ID Austria) für die eindeutige Identifikation einer Person eingesetzt wird?			1.8
Sofern vertretungsweises Handeln geregelt wird, ist sichergestellt, dass eine Einzelvertretungsbefugnis mittels E-ID (ID Austria) genutzt werden kann?			1.9
Wird ein Unterschriftserfordernis geregelt und ist sichergestellt, dass dieses mittels qualifizierter Signatur umgesetzt werden kann?			1.10
Wird eine elektronische Zustellung ermöglicht?			1.11
Werden in das Regelungsvorhaben die Perspektiven verschiedener Expertinnen und Experten miteinbezogen?			1.12
Kann das Verfahren aus der Perspektive der Betroffenen bzw. Nutzerinnen und Nutzern verständlich, zugänglich und einfach gestaltet werden?			1.13

Tabelle 2 Bewirkt die Regelung in der Vollziehung die analoge oder digitale Verarbeitung von Daten?

Fragen	Ja	Nein	siehe
Werden mit der Regelung Datenermittlungen bzw. Informationsverpflichtungen vorgesehen, obwohl diese Informationen bereits in bestehenden Registern oder bei anderen Behörden verfügbar sind?			2.1
Sollen Daten kryptographisch gesichert verarbeitet (Authentizität des Inhalts) oder historisiert werden? *z. B.: durch den Einsatz von elektronischen Signaturen*			2.2

Fragen	Ja	Nein	siehe
Werden neue Meldepflichten (Informationsverpflichtungen) eingeführt?			2.3
Werden Daten verarbeitet, die von Interesse für die Allgemeinheit sein könnten? *z. B.: im Sinne von „Open Data“*			2.4
Sind Nutzungsbedingungen bzw. ein Prozedere für deren Anpassung für die Nutzung von Services vorgesehen?			2.5

Tabelle 3 Bedingt die Regelung Anforderungen an den Datenschutz und/oder die Datensicherheit?

Frage	Ja	Nein	siehe
Ist es vorgesehen, dass personenbezogene Daten verarbeitet werden?			3.1
Werden Personenidentifikationen durch den Entwurf eingeführt (z. B. Unternehmenszahlen, Personenkennzahlen, …)?			3.2
Wird der Einsatz bereichsspezifischer Personenkennzeichen bzw. der Stammzahl geprüft?			3.3
Sind Daten aufgrund gesetzlicher Bestellungen oder technischer Standards durch Schutzmaßnahmen gesondert zu sichern?			3.4
Sollen gesonderte Haftungsregelungen bestehen, wenn Informationen unrichtig sind oder Daten missbräuchlich verarbeitet bzw. verändert werden?			3.5
Kann durch Kontrollpflichten sichergestellt werden, dass eine unbefugte Manupulation bzw. Veränderung der Daten verhindert wird?			3.6

Frage	Ja	Nein	siehe
Werden Anforderungen an die Verfügbarkeit (z. B. Betriebszeiten, Wiederherstellungsziele) von IT-Systemen gestellt?			3.7
Werden Maßnahmen gesetzt, um die technologische Souveränität (z. B. keine Abhängigkeiten von einzelnen Anbietern) sicherzustellen? *z. B.: technologische Schlüsseltechnologien selbst entwickeln bzw. kontrollieren, um unabhängig und selbstbestimmt agieren zu können*			3.8

Tabelle 4 Muss zur Umsetzung der Regelung ein IT-System oder eine IT-Lösung angepasst oder neu entwickelt werden?

Frage	Ja	Nein	siehe
Werden bestehende E-Government-Instrumente und –bausteine (z. B. ID-Austria, elektronische Zustellung, RSV, Portalverbund, definierte Standards und Schnittstellen) genutzt?			4.1
Wurden für die Umsetzung Open-Source-Lösungen in Betracht gezogen?			4.2
Wird berücksichtigt, dass die bestehende Infrastruktur genutzt werden kann, anstatt parallel separate, proprietäre Lösungen zu verwenden?			4.3
Wird berücksichtigt, dass das elektronische Verfahren auch auf mobilen Endgeräten (z. B. Smartphone, Tablet) nutzbar ist?			4.4
Ist die Art und Größe des Benutzerkreises/der Zielgruppe bestimmbar?			4.5
Ist bei der Umsetzung mit intensivem Einsatz von IKT oder dem Datenaustausch zwischen mehreren Personen zu rechnen?			4.6
Ist eine hohe Abhängigkeit von technischen Systemen Dritter zu erwarten?			4.7

Frage	Ja	Nein	siehe
Wird berücksichtigt, dass eingesetzte Technologien sich rasch ändern (z. B. durch technologieneutrale Formulierungen oder vereinfachte Anpassungsmöglichkeiten)?			4.8

Tabelle 5 Gibt es in der Praxis Evidenz für Fehleranfälligkeiten?

Frage	Ja	Nein	siehe
Können potentielle Betrugs- und Fehleranfälligkeiten über transparente digitale Überprüfungsmöglichkeiten gemindert bzw. verhindert werden?			5.1

Tabelle 6 Sind die Regeln klar, einfach, eindeutig und konsistent formuliert (keine Denksportaufgabe)?

Frage	Ja	Nein	siehe
Regeln: Können durch kohärente und logische Systematik eindeutige Entscheidungsstrukturen für die IT-Umsetzung formuliert werden?			6.1
Begriffe: Werden Rechtsbegriffe innerhalb des Regelungsvorhabens einheitlich und konsistent verwendet?			6.2
Wird sichergestellt, dass dieselben Definitionen von Daten bzw. Begriffen verwendet werden, die bereits in Registern von Verantwortlichen des öffentlichen Bereichs existieren?			6.3
Ist der Ablauf des Verfahrens im Gesetz so klar beschrieben, dass er sich in einzelne Arbeitsschritte (Workflow) gliedern lässt? *z. B.: klare Unterscheidung zwischen allgemeinen Regeln und Ausnahmen*			6.4

Tabelle 7 Sofern ein Verfahren geregelt wird: Kann oder soll der Vollzug der Regelung (teil)automatisiert erfolgen?

Frage	**Ja**	**Nein**	**siehe**
Wird die Standardisierung des Verfahrensrechts unterstützt und Sonderverfahrensrecht vermieden?			7.1
Bestehen bereits die rechtlichen Grundlagen für das (teil-) automatisierte Verfahren?			7.2
Werden die Rechtsvorschriften so formuliert, dass Ermessensentscheidungen auf Fälle beschränkt werden, in denen sie erforderlich sind?			7.3
Wurde das Verfahren / die Datenflüsse visuell dargestellt?			7.4

Bundeskanzleramt
Ballhausplatz 2, 1010 Wien
+43 1 531 15-0
post.vii-2@bka.gv.at
bundeskanzleramt.gv.at