„IKT-Tauglichkeit“

Überprüfung legistischer Vorhaben auf Auswirkungen in Bezug auf die IKT

Leitfaden für Legistinnen und Legisten

Wien, 2018
Version 2.0

Inhaltsverzeichnis

Einleitung

Der Einsatz von IT-Systemen ist in der Verwaltung und in der Gerichtsbarkeit nicht mehr wegzudenken (siehe etwa die elektronischen Steuerverfahren über FinanzOnline, Informationssuche auf Behördenwebseiten, elektronische Antragstellung bei Behörden, Verfahrensautomation Justiz, Elektronischer Rechtsverkehr, Ediktsdatei, Grund- und Firmenbuch, …). Für eine moderne Verwaltung ist es bedeutsam, im Zug legistischer Tätigkeiten Behinderungen beim Einsatz von IT-Systemen zu vermeiden und die Auswirkungen legistischer Vorhaben auf IT-Systeme zu prüfen. Der gegenständliche Leitfaden zielt darauf ab, Legistinnen und Legisten über häufige Berührungspunkte zwischen Rechtsvorschriften und IT-Systemen zu informieren und einer umfassenden Betrachtung der gegenseitigen Auswirkungen herbeizuführen.

Im Folgenden werden Fragen zu möglichen relevanten Teilbereichen des Ihnen vorliegenden Entwurfs gestellt, die dabei helfen sollen, Handlungsbedarf zu erkennen und diesen entsprechend den Vorgaben umzusetzen.

Im Anhang finden Sie weiters eine „Checkliste“, die einen kurzen Überblick über die relevanten Fragestellungen gibt, um eine rasche Prüfung Ihres Vorhabens zu gewährleisten.

1 Elektronische Verfahrensabwicklung

Die Prüfung der IKT-Tauglichkeit bei der elektronischen Verfahrensabwicklung orientiert sich einerseits grob an einem typischen Verwaltungsverfahren, das sich in Antragstellung, Bearbeitung durch die Behörde und Zustellung an den Empfänger gliedert und andererseits an sonstigen Maßnahmen im Zusammenhang mit der Einrichtung oder dem Betrieb von elektronischen Services [z.B. Unternehmensservice-Portal (siehe Unternehmensserviceportalgesetz – USPG) oder Transparenzdatenbank (siehe Transparenzdatenbankgesetz 2012 – TDBG 2012)].

1.1 Antrag

1.1.1 Soll ein Antrag gestellt werden können bzw. sind Informationsverpflichtungen geregelt?

Beachten Sie, dass es grundsätzlich möglich sein soll, einen Antrag elektronisch einzubringen. 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 keine sachlichen Argumente dagegen sprechen. So soll etwa vermieden werden, dass Anträge ausschließlich auf Papierformularen eingebracht werden dürfen. In Angelegenheiten der öffentlichen Abgaben gelten die Vorgaben des § 86a BAO, der FinanzOnline-Verordnung 2006 (FOnV 2006) und der FinanzOnline-Erklärungsverordnung (FOnErklV).

Falls der Antrag eine Angelegenheit betrifft, die vom Anwendungsbereich des Dienstleistungsgesetzes – DLG umfasst wird wäre zu prüfen, ob das Anbringen gemäß § 10 Abs. 1 DLG auch elektronisch eingebracht werden kann. Soweit ein Antrag bei (einem ordentlichen) Gericht gestellt wird, wären die Besonderheiten des Elektronischen Rechtsverkehrs (ERV-VO) zu bedenken.

Spätestens ab 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[1] hat. Ausge-

[1] 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).

nommen sind lediglich Angelegenheiten, die nicht geeignet sind, elektronisch besorgt zu werden. Somit dürfen auch die materienspezifischen Regelungen eine Antragstellung in elektronischer Form nicht verhindern.

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: http://reference.e-government.gv.at/Veroeffentlichte-Informationen.493.0.html)

1.1.2 Ermöglichen die Regelungen einen barrierearmen Zugang?

Gemäß § 1 Abs. 3 E-Government-Gesetz – E-GovG sind behördliche Internetauftritte, die Informationen anbieten oder Verfahren elektronisch unterstützen – inkl. Webformulare – so zu gestalten, dass die Anforderungen für die Web-Zugänglichkeit auch hinsichtlich des barrierefreien Zugangs für behinderte Menschen eingehalten werden (beachten Sie auch sonstige entsprechende Bestimmungen (etwa Art. 7 B-VG oder das Bundes-Behindertengleichstellungsgesetz). Siehe dazu: http://reference.e-government.gv.at/Veroeffentlichte-Informationen.302.0.html

Als positives 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.

1.1.3 Sind spezielle Formulare für Eingaben vorgesehen?

Beachten Sie, dass es grundsätzlich möglich sein soll, einen Antrag elektronisch einzubringen. Bestimmte Formulierungen verhindern eine solche Möglichkeit (zB „Vordrucke“, „Papiervordrucke“,…). In den meisten Fällen ist es zudem zweckmäßig, Online-Formulare für Eingaben vorzusehen (etwa Erleichterungen bei der Antragstellung, automatisierte Weiterverarbeitbarkeit,…) Um diese Erfordernisse zu erfüllen, sollte darauf geachtet werden zumindest technologieneutrale Formulierungen zu wählen.

Beachten Sie, dass es für die Ausgestaltung der Online-Formulare (zB Layout, Struktur,…) zwischen Bund und Ländern abgestimmte Empfehlungen gibt. Diese finden Sie unter der Internetadresse http://reference.e-government.gv.at/Veroeffentlichte-Informationen.302.0.html

Ein negatives Beispiel für die Überregulierung eines Formulars stellt § 15 Abs. 1 Patentamtsverordnung 2006 dar:

Die Anmeldungsunterlagen sind auf weißem, sauberem und nicht saugendem Papier, das frei von Falten oder Löchern und nicht geheftet oder gerollt ist, mit einem Gewicht von vorzugsweise 80 g/m² im Hochformat A4 (210 mm x 297 mm) einseitig zu drucken. […]

Dadurch wird jedenfalls ein elektronischer Antrag ausgeschlossen (arg. „Papier).

1.1.4 Wird ein Antragsteller elektronisch identifiziert?

Wenn eine Person eindeutig identifiziert werden soll, ist ein Einsatz der Funktion Bürgerkarte[2] (vgl. § 4 E-GovG) zweckmäßig. Diese ermöglicht eine eindeutige elektronische Identifikation und die einschreitende Person kann den Antrag mit der Bürgerkarte qualifiziert elektronisch signieren (die qualifizierte elektronische Signatur ist der handschriftlichen Unterschrift grundsätzlich rechtlich gleichgestellt (vgl. Art. 25 Abs. 2 eIDAS-VO[3] iVm § 4 Abs. 1 Signatur- und Vertrauensdienstegesetz (SVG)). Für Parteien und deren Vertreter, die an FinanzOnline teilnehmen gelten die Bestimmungen der FOnV 2006 welche die Verwendung von Teilnehmeridentifikation, Benutzeridentifikation und persönlichem Passwort (PIN) vorsehen.

1.1.5 Ist ein Unterschriftserfordernis geregelt?

Das 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 der Bürgerkarte kann eine qualifizierte elektronische Signatur erstellt werden und somit das Unterschriftserfordernis auch elektronisch erfüllt werden.

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.

[2] Die „Handysignatur“ ist eine Ausprägung der Bürgerkartenfunktion und daher auch rechtlich als solche zu behandeln.

[3] 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

1.2 Bearbeitung

1.2.1 Werden Regelungen über die Sammlung von Daten getroffen, die bereits bei anderen Behörden oder Institutionen verspeichert sind?

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.

1.2.2 Ist es vorgesehen, dass personenbezogene Daten gespeichert werden?

Bei der Verarbeitung von personenbezogenen Daten ist jedenfalls die unmittelbar anwendbare Datenschutz-Grundverordnung[4] (DSGVO) beachtlich. Sämtliche Regelungen im Zusammenhang mit der Verarbeitung von personenbezogenen 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“)).

Die Schaffung einer Rechtsgrundlage nach Art. 6 Abs. 1 lit. c oder e DSGVO unter Beachtung der Auswirkungen auf die IT als Rechtsgrundlage für die Verarbeitung personenbezogener Daten wird grundsätzlich empfohlen und sollte möglichst folgende Informationen beinhalten: Benennung des/der Verantwortlichen, Zweck der Verarbeitung, Aufzählung der Datenarten, Aufzählung der betroffenen Personen(kategorien), allfällige Übermittlungen einschließlich Aufzählung der Übermittlungsempfänger und Zweck der Übermittlung und Aufbewahrungsfrist der Daten. Um Personen in Verarbeitungen eindeutig identifizieren zu können wird vor dem Hintergrund von Privacy by Design empfohlen, bereichsspezifische Personenkennzeichen (bPK) zu verwenden. Das bPK wird mit Hilfe der Stammzahl (§ 6 E-GovG) und der Benennung des Bereiches [siehe dazu die E-Government-Bereichsabgrenzungsverordnung (E-GovBerAbgrV)] berechnet. Das Wesen des bPK ist es, dass für unterschiedliche Bereiche unterschiedliche bPK generiert werden. Das bedeutet, dass das bPK für den Bereich Steuern und Abgaben verschieden vom bPK für den Bereich Bauen und Wohnen ist. Der dabei verwendete kryptografische Algorithmus stellt dabei sicher, dass ein bPK nicht in ein anderes bPK umgerechnet werden kann und dass auch von einem bPK nicht auf die Stammzahl zurück gerechnet werden kann. Trotz der Unmöglichkeit der Umrechnung behält das bPK die identifizierenden Eigenschaften der Stammzahl bei. Da aber verschiedene Bereiche verschiedene Kennzeichen haben, ist ein Abgleich der Datenbanken über dieses Kennzeichen nicht möglich.

[4] Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1.

1.2.3 Werden Personenidentifikatoren durch den Entwurf eingeführt (zB Unternehmenszahlen, Personenkennzahlen, …)?

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

1.2.4 Sollen Daten 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).

1.3 Zustellung

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 ermöglich 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 VO) zu bedenken.

Spätestens ab 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[5] hat. Ausge-

[5] 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).

nommen sind lediglich Angelegenheiten, die nicht geeignet sind, elektronisch besorgt zu werden. Unter den elektronischen Verkehr fällt auch die Zustellung von Dokumenten. Somit dürfen 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 ab diesem Zeitpunkt Unternehmen im Sinne des § 3 Z 20 Bundesstatistikgesetz 2000 grundsätzlich an der elektronischen Zustellung teilzunehmen haben, wodurch diese Empfängergruppe jedenfalls auch erreichbar sein sollte.

1.4 Nutzungsbedingungen

Wenn vorgesehen sein soll, dass der Benutzer vor Verwendung einer Applikation Nutzungsbedingungen akzeptiert, wird empfohlen ein Procedere für die Änderung dieser Nutzungsbedingungen vorzusehen. Da Nutzungsbedingungen vorwiegend privatrechtliche Vereinbarungen sind, wäre im Einzelfall zu prüfen, ob eine gesetzliche Regelung zweckmäßig ist. Jedenfalls sind hierbei insbesondere die entsprechenden anwendbaren Bestimmungen des ABGB, des UGB, des ECG, des TKG 2003 und allenfalls des KSchG zu berücksichtigen.

Nicht zu verwechseln sind Nutzungsbedingungen mit der Einwilligung (als Rechtsgrundlage) in die Verarbeitung der personenbezogenen Daten nach Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO. Sobald etwa eine „rechtliche Verpflichtung“ nach Art. 6 Abs. 1 lit. c oder ein „öffentliches Interesse“ bzw. die „Ausübung öffentlicher Gewalt“ nach Art. 6 Abs. 1 lit. e DSGVO für die Verarbeitung personenbezogener Daten vorliegt, ist die Einholung einer datenschutzrechtlichen Einwilligung nicht mehr erforderlich.

1.5 Rollendefinition

Wenn im Entwurf Begriffe verwendet werden, die auch im Datenschutzrecht vorkommen, sollte unmissverständlich zwischen den technischen, organisatorischen und datenschutzrechtlichen Bedeutungen unterschieden werden (z.B. mehrdeutiger Begriff des „Betreibers“). So sollte klar geregelt sein, wer datenschutzrechtlicher Verantwortlicher und wer datenschutzrechtlicher Auftragsverarbeiter ist.

2 IKT-Betriebssicht

2.1 Umsetzung

2.1.1 Sind die für die Umsetzung benötigten Datenbestände bereits in anderen Verfahren/Applikationen verarbeitet/gespeichert?

Es sollen nach Möglichkeit bereits existierende Verfahren ausgebaut werden („shared-service-Gedanke“). Dadurch kommt es zu Einsparungen bei Errichtung und Betrieb neuer Verfahren. Die Nutzung allfällig bereits bestehender Daten müsste ebenfalls datenschutzrechtlich durch legistische Maßnahmen ermöglicht werden.

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

Wegen der ersatzlosen Streichung der Ausnahme des § 8 Abs. 2 DSG 2000, wonach die Verwendung bereits zulässigerweise veröffentlichter Daten das Geheimhaltungsinteresse nicht beeinträchtigt, sollte im Rahmen legistischer Vorhaben die Verwendung bereits veröffentlichter Daten, wie beispielsweise die Veröffentlichung geografischer Daten mit Personenbezug (Adress-/Grundstücksdaten), expressis verbis ermöglicht werden.

2.1.2 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 Benutzern um Bürger oder geschultes Fachpersonal handelt. Von der Beantwortung dieser Fragen hängt freilich auch ab, wie ein Verfahren konzipiert und welcher Schulungsaufwand dafür kalkuliert werden muss.

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

2.1.4 Ist eine hohe Abhängigkeit von technischen Systemen Dritter zu erwarten? Ist bei diesen Systemen, z.B. aufgrund des technischen Fortschritts, mit häufigen Veränderungen und – damit verbunden – mit hohem Anpassungsbedarf zu rechnen?

In diesem Fall sollte die Möglichkeit von (technischen) Durchführungsverordnungen in Betracht gezogen werden, um gegebenenfalls auf neue Anforderungen schnell reagieren zu können (z.B.: Kraftfahrgesetz-Durchführungsverordnung 1967 – KDV, Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung).

2.1.5 Sollen Daten gesammelt werden, die von Interesse für die Allgemeinheit sein könnten?

Sofern nicht datenschutzrechtliche oder andere gewichtige Gründe dagegen sprechen, sollte danach getrachtet werden, Datenbestände von allgemeinem Interesse in einer frei zugänglichen Form als „Rohdaten“ zur Verfügung zu stellen („open data“). Falls eine derartige Intention verfolgt wird, wäre darauf zu achten, dass die Daten so gesammelt und verarbeitet werden, dass eine „open data Verwendung“ ohne nachträgliche Investitionen ermöglicht wird (Datenformate und Schnittstellen wären daher schon entsprechend zu konzipieren).

2.1.6 Sind die (Straf-)Tatbestände so formuliert, dass eine automatisierte Erfassung möglich ist?

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 gerichtlichen Straftatbeständen sollte, um deren Anwendung durch 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“ 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.

3 IKT-Sicherheit

3.1 Anforderungen an die Verfügbarkeit von IT-Systemen

Die Fristen für die Bearbeitung von Verwaltungsvorgängen bestimmen wesentlich die Kosten der IT-Systeme. 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?

3.2 Vertraulichkeit und Integrität

3.2.1 Welche Daten sind aufgrund gesetzlicher Bestimmungen oder technischer Standards (Stand der Technik) durch aufwändige Schutzmaßnahmen zu sichern?

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 (https://www.sicherheitshandbuch.gv.at/)). 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.

Die Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität dieser Daten beeinflussen die IT-Kosten einer Verwaltungsapplikation.

3.2.2 In welchem Umfang soll eine Haftung zugerechnet werden, 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 Haftungsregelungen des Art. 82 DSGVO für den Fall von Verstößen gegen die Datenschutz-Grundverordnung hingewiesen werden. Falls im Einzelfall Haftungsbeschränkungen vorgesehen werden sollen, wäre vor diesem Hintergrund die Zulässigkeit zu prüfen.

3.2.3 Soll durch Regelungen (etwa Kontrollpflichten) eine unberechtigte Veränderung von Daten verhindert werden?

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 die Verwendung des Vier-Augen-Prinzips (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.

3.3 Ist eine Datenschutz-Folgenabschätzung durchzuführen?

Eine Datenschutz-Folgenabschätzung ist dann durchzuführen, wenn die Datenverarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben wird. Gemäß Art. 35 Abs. 10 DSGVO kann die Datenschutz-Folgenabschätzung bereits im Gesetzgebungsprozess vorweg vorgenommen werden. Dies bedeutet, dass die Durchführung künftiger Datenschutz-Folgenabschätzungen für Verarbeitungen, die auf diesem Gesetz beruhen, entfallen kann. Darüber hinaus ist es von großer Bedeutung, dass Auswirkungen (sowohl in rechtlicher als auch in technischer Sicht), die durch die Durchführung einer Datenschutz-Folgenabschätzung für die IT entstehen, im Vorhinein analysiert werden.

In diesem Zusammenhang darf auch auf diverse Stellungnahmen des Datenschutzrates zu legistischen Vorhaben, insbesondere aus dem Jahr 2017 (abrufbar unter: https://www.justiz.gv.at/web2013/home/verfassungsdienst/datenschutzrat/stellungnahmen/stellungnahmen-des-datenschutzrates-2017~2c94848b60c168850160e9428e565dfa.de.html) verwiesen werden, in denen jeweils wie folgt ausgeführt wird:

„Art 35 Abs. 10 DSGVO sieht unter den angeführten Voraussetzungen eine Ausnahme von der Datenschutz-Folgenabschätzung durch Verantwortliche für Verarbeitungen vor, die auf einer Rechtsgrundlage im Recht des Mitgliedstaates, dem der Verantwortliche unterliegt, beruhen und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte.“

4 Weiterführende Informationen

Digitales Österreich

https://www.digitales.oesterreich.gv.at

Umfangreiche Seite des Bundesministeriums für Digitalisierung und Wirtschaftsstandort zu E-Government.

Reference Server

http://reference.e-government.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.justiz.gv.at/web2013/home/verfassungsdienst/legistik~2c94848b60c168850160d54bdcef2912.de.html

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.

IKT-Relevante Rechtsvorschriften

https://www.digitales.oesterreich.gv.at/gesetze

Übersicht über die relevanten “Kernvorschriften” im E-Government Bereich.

5 Anhang – „Checkliste“

Fragestellung zur Prüfung	**Ja**	**siehe Kapitel**
Antrag		
Soll ein Antrag gestellt werden können?		1.1.1
Sind Informationsverpflichtungen geregelt?		1.1.1
Ermöglichen die Regelungen einen barrierearmen Zugang?		1.1.2
Sind spezielle Formulare für Eingaben vorgesehen?		1.1.3
Wird ein Antragsteller elektronisch identifiziert?		1.1.4
Ist ein Unterschriftserfordernis geregelt?		1.1.5
Bearbeitung des Antrags		
Werden Regelungen über die Sammlung von Daten getroffen, die bereits bei anderen Behörden oder Institutionen verspeichert sind?		1.2.1
Ist es vorgesehen, dass personenbezogene Daten gespeichert werden?		1.2.2
Werden Personenidentifikatoren durch den Entwurf eingeführt?		1.2.3
Sollen Daten gesichert verarbeitet oder historisiert werden?		1.2.4
Zustellung		
Sind Regelungen über die Zustellung von Dokumenten enthalten?		1.3
Nutzungsbedingungen		
Sind Nutzungsbedingungen bei Einstieg in eine Applikation vorgesehen?		1.4
Rollendefinitionen		
Wird klar zwischen technischen und datenschutzrechtlichen Begriffen unterschieden?		1.5
Betriebssicht		
Sind benötigte Datenbestände bereits an einem anderen Ort verarbeitet/gespeichert		2.1.1
Ist die Art und Größe des Benutzerkreises/ der Zielgruppe bestimmbar?		2.1.2
Ist bei der Umsetzung mit intensivem Einsatz von IKT oder dem Datenaustausch zwischen mehreren Partnern zu rechnen?		2.1.3
Ist eine hohe Abhängigkeit von technischen Systemen Dritter zu erwarten? Ist bei diesen Systemen mit häufigen Veränderungen und mit Anpassungsbedarf zu rechnen?		2.1.4
Sollen Daten gesammelt werden, die von Interesse für die Allgemeinheit sein könnten?		2.1.5
Sind (Straf-)Tatbestände so formuliert, dass eine automatisierte Erfassung möglich ist?		2.1.6
Sicherheit		
Werden Anforderungen an die Verfügbarkeit von IT-Systemen gestellt?		3.1
Sind Daten aufgrund gesetzlicher Bestimmungen oder technischer Standards durch aufwändige Schutzmaßnahmen zu sichern?		3.2.1
Soll explizit eine Haftung geregelt werden, wenn Informationen unrichtig sind oder Daten missbräuchlich verarbeitet bzw. verändert werden?		3.2.2
Soll durch Regelungen eine unberechtigte Veränderung von Daten verhindert werden?		3.2.3
Ist eine Datenschutz-Folgenabschätzung durchzuführen?		3.3