Die IT-Verträglichkeitsprüfung im Bereich der Rechtsetzung des Bundes

Bernhard Karning

Vorbemerkung

Die Informations- und Kommunikationstechnologien (IKT) haben im letzten Jahrzehnt massiv in die Verwaltung und in die Gerichtsbarkeit Einzug gefunden und sind aus dem (Behörden)-Alltag schon lange nicht mehr wegzudenken (zB die elektronischen Steuerverfahren über FinanzOnline, die Informationssuche auf Behördenwebseiten, die elektronische Antragstellung bei Behörden mittels Online-Formularen, elektronische Registerabfragen, Bürgerkartenfunktion, Verfahrensautomation Justiz, Elektronischer Rechtsverkehr, Ediktsdatei, Grund- und Firmenbuch, …). Daher ist es von immanenter Bedeutung, dass auch der Rechtsrahmen den Einsatz der – bundesweit in Fachgruppen abgestimmten - IKT-Elemente ermöglicht und somit eine moderne Verwaltung garantiert.

Aus einem Verwaltungsreformprojekt zur Prüfung legistischer Vorhaben auf Auswirkungen in Bezug auf die IKT ist daher unter der Federführung des Bundeskanzleramts bereits im Jahr 2011 ein Leitfaden zur "IKT-Tauglichkeit" hervorgegangen, der jedoch aktuell immer noch zu wenig beachtet wird. Ziel dieses Leitfadens ist es demgemäß der Legistin bzw. dem Legisten das nötige Gespür dafür zu geben, ob die facettenreichen Anforderungen der IKT durch den zu erstellenden bzw. vorliegenden Entwurf erfüllt sind, oder aber ob Anpassungsbedarf besteht.

Im Leitfaden werden Fragen zu möglichen relevanten Teilbereichen eines vorliegenden Entwurfs gestellt, die dabei helfen sollen, Handlungsbedarf zu erkennen und diesen entsprechend den Vorgaben umzusetzen. Als Abrundung findet sich am Ende eine "Checkliste", die tabellarisch einen Überblick über die relevanten Fragestellungen samt Verweisungen auf diese gibt, um eine rasche Prüfung eines Vorhabens zu gewährleisten. Kurz zusammengefasst: Dieser Leitfaden soll der Legistin bzw. dem Legist bei der Prüfung, ob der vorliegende Entwurf IT-relevante Regelungssachverhalte enthält, behilflich sein und bei einer IKT-Strategiekonformen Umsetzung des Vorhabens unterstützen.

Der Leitfaden wurde mit einem Rundschreiben[1] des Bundeskanzleramtes-Verfassungsdienst an die Bundesministerien mit dem Ersuchen um Inkenntnissetzung aller mit legistischen Aufgaben betrauten Bediensteten zur Verfügung gestellt und ist auch aktuell noch immer auf der Website des Bundeskanzleramts im Bereich Recht & Verfassung/Legistik unter http://archiv.bundeskanzleramt.at/DocView.axd?CobId=47411 frei abrufbar.

Die folgende Darstellung gibt somit den Leitfaden, an dessen Entstehung der Autor dieses Artikels maßgeblich beteiligt war, in aktualisierter[2] und durch illustrierende Beispiele[3] ergänzter Form wieder.

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 Betrieb von elektronischen Services (zB Unternehmensservice-Portal [s. Unternehmensserviceportalgesetz] oder Transparenzdatenbank [s. Transparenzdatenbankgesetz]).

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 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.

[1] BKA-602.271/0005-V/2/2012 vom 19. April 2012; das Rundschreiben wurde zur Kenntnis auch an die Parlamentsdirektion, alle Ämter der Landesregierungen und an die Verbindungsstelle der Bundesländer beim Amt der NÖ. Landesregierung versandt.

[2] S. Punkte 1.1.4 und 1.1.5 zum SVG und eIDAS-VO sowie 1.5 zur EU-DSGVO.

[3] S. Punkte 1.1.2 und 1.1.3.

Falls der Antrag eine Angelegenheit betrifft, die vom Anwendungsbereich des Dienstleistungsgesetzes (DLG) umfasst wird wäre zu prüfen, ob das Anbringen gemäß § 10 Abs. 1 Dienstleistungsgesetz auch elektronisch eingebracht werden kann. Soweit ein Antrag bei Gericht gestellt wird, wären die Besonderheiten des Elektronischen Rechtsverkehrs Rechtsverkehrs (vgl. Verordnung der Bundesministerin für Justiz über den elektronischen Rechtsverkehr [ERV 2006]) zu bedenken.

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 (s. 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-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]. S. 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 Formulierung 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 Weiterverarbeit-

barkeit,…). 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, saubererem 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 Bürgerkarte[4] (vgl. § 4 E-Government-Gesetz [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. § 4 Abs. 1 Signatur- und Vertrauensdienstegesetz {SVG} iVm. Art. 25 Abs. 2 eIDAS-VO]).

Es wird angeraten keine "neuen" oder abweichenden Methoden für die eindeutige Identifizierung einzuführen. Es wäre daher zu prüfen, ob für die Identifikation die Bürgerkarte vorzusehen ist.[5]

---

[4] Die "Handysignatur" ist eine Ausprägung der Bürgerkartenfunktion und daher auch rechtlich als solche zu behandeln.

[5] Weiters ist in diesem Zusammenhang auf das Regierungsprogramm der XXIV. Gesetzgebungsperiode hinzuweisen, das folgendes festlegt:
"[…] Ausweitung der Anwendungsmöglichkeiten um Amtswege und private Geschäfte sicher elektronisch abwickeln zu können.
a) Alle IT-Verfahren und Portale der Verwaltung des Bundes, der Länder und Gemeinden sollen die Anmeldung mit Bürgerkarte unterstützen. Alle neu einzurichtenden elektronischen Verfahren sollen auf die Identifikation mittels Bürgerkarte aufbauen. Bestehende andere elektronische Zugänge zu

1.1.5 Ist ein Unterschriftserfordernis geregelt?

Das Unterschriftserfordernis sollte grundsätzlich auch elektronisch erfüllt werden können. Die qualifizierte elektronische Signatur erfüllt gemäß § 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 oder zumindest technologieneutraler Formulierungen verwendet werden.

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.[6]

1.2.2 Ist es vorgesehen, dass personenbezogene Daten gespeichert werden?

Um Personen in der Datenanwendung eindeutig identifizieren zu können wird empfohlen, bereichsspezifische Personenkennzeichen (bPK) zu verwenden. Das bPK wird mit Hilfe der Stammzahl (§ 6 E-GovG) und der Benennung des Bereiches[7] berechnet. Das Wesen des bPK ist es, dass für unterschiedliche Bereiche unterschiedliche bPK generiert werden. Das

---

bestehenden Anwendungen des E-Government werden dadurch nicht beeinträchtigt und bleiben erhalten."

6 In diesem Zusammenhang ist auf das Regierungsprogramm der XXIV. Gesetzgebungsperiode hinzuweisen, das folgendes festlegt:
"[…] Optimierung von Registeranwendungen vor allem zur Vereinfachung der Urkundenvorlage für die Bürgerinnen und Bürger. Verbesserung der Qualität; Ermöglichung der automatisierten Abfragemöglichkeit bei wesentlichen Registern; rasche Umsetzung eines zentralen Personenstandsregisters; einvernehmliche Evaluierung der Errichtung einer gemeinsamen Organisation von Bund, Ländern, Städten und Gemeinden zum Betrieb und zur Entwicklung zentraler Registeranwendungen."

7 S. dazu die E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV).

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.

Im Übrigen wird auf das Rundschreiben des BKA-VD zur legistischen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz hingewiesen (http://www.bka.gv.at/DocView.axd?CobId=29801).

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: Soll elektronisch (nachweislich) zugestellt werden?

Die elektronische Zustellung von Dokumenten ist umfassend 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.[8]

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 wären die Besonderheiten des Elektronischen Rechtsverkehrs (ERV-VO) zu bedenken.

1.4 Nutzungsbedingungen

Wenn es 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 ECG, des TKG 2003 und allenfalls des KSchG zu berücksichtigen.

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 (zB mehrdeutiger Begriff des "Betreibers"). So sollte klar geregelt sein, wer datenschutzrechtlicher Auftraggeber und wer datenschutzrechtlicher Dienstleister ist. Durch die Erlassung der Datenschutz-Grundverordnung[9] werden für diese Zwecke wiederum neue Begriffe wie "Verantwortlicher" (Art. 4 Z 7) und "Auftragsverarbeiter" (Art. 4 Z 8) eingeführt.

---

[8] Das Regierungsprogramm der XXIV. Gesetzgebungsperiode legt dazu folgendes fest:
"[…] Bürgerinnen und Bürger sowie Unternehmerinnen und Unternehmer, die sich beim elektronischen Zustelldienst angemeldet haben, sollen die Erledigungen der Verwaltung in Form der elektronischen Zustellung erhalten."

[9] Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

Im Übrigen wird auf das Rundschreiben des BKA-VD zur legistischen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz hingewiesen (http://www.bka.gv.at/DocView.axd?CobId=29801).

2. IKT-Betriebssicht

2.1 Umsetzung

2.1.1 Sind die für die Umsetzung benötigten Datenbestände bereits in anderen Verfahren/Applikationen verwendet/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.

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 (zB Releasetermin der betroffenen Software) vorausschauend festgelegt werden.

2.1.4 Ist eine hohe Abhängigkeit von technischen Systemen Dritter zu erwarten? Ist bei diesen Systemen, zB auf Grund 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 (zB: 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 eine möglichst einfach 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 (zB Verwaltung) notwendig?

- Verfügbarkeit in Krisenfällen: Ist in Krisen- oder Katastrophenfällen ein Ausfall der IT-Anwendung akzeptabel oder müssen Vorkehrungen für katastrophensicheren Betrieb getroffen werden (zB Einhaltung von Fristen)?

- Ist im Falle einer Katastrophe ein eingeschränkter Betrieb (zB 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 auf Grund 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 (s. dazu auch das Österreichische Informationssicherheitshandbuch [https://www.sicherheitshandbuch.gv.at/]). Durch eine konsequente wiederkehrende Prüfung der Notwendigkeit der Datenverwendung (mit hohem Schutzbedarf) sowie durch Verwendung 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.

Für die datenschutzrechtlichen Aspekte wird auf das Rundschreiben des BKA-VD zur legistischen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz hingewiesen (http://www.bka.gv.at/DocView.axd?CobId=29801).

3.2.2 In welchem Umfang soll eine Haftung zugerechnet werden, wenn Informationen unrichtig sind oder Daten missbräuchlich verwendet 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. 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 und die Verwaltung zu vermeiden. Ein Grundprinzip zur Verhinderung der Manipulation von Daten stellt etwa die Verwendung des Vier-Augen-Prinzips (zB 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.

4. "Checkliste"

Fragestellung zur Prüfung	**Ja**	**s. 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 gespeichert 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		1.4

Fragestellung zur Prüfung	**Ja**	**s. Kapitel**
vorgesehen?		
Rollendefinitionen		
Wird klar zwischen technischen und datenschutzrechtlichen Begriffen unterschieden?		1.5
Betriebssicht		
Sind benötigte Datenbestände bereits an einem anderen Ort verwendet/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 auf Grund 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 verwendet bzw. verändert werden?		3.2.2
Soll durch Regelungen eine unberechtigte Veränderung von Daten verhindert werden?		3.2.3