



Gesetz über digitale Basisdienste

A. Ausgangslage

Der Regierungsrat hat mit Beschluss vom 25. April 2018 (RRB Nr. 390/2018) die Strategie Digitale Verwaltung 2018–2023 festgesetzt. Mit dieser Strategie hat er die Grundlagen für eine gezielte und koordinierte Digitalisierung der Verwaltung und die Entwicklung eines digitalen Leistungsangebots gelegt. Das im Rahmen der Strategie festgesetzte Leitbild sieht vor, dass die kantonale Verwaltung eine offene und digital vernetzte Organisation sein soll, die sowohl nach innen als auch nach aussen bedürfnisgerecht, sicher und durchgängig digital agiert. Der Regierungsrat hat im September 2023 die Staatskanzlei beauftragt, die «Strategie Digitale Verwaltung 2025+» zur Festsetzung bis Ende 2024 vorzulegen (RRB Nr. 1043/2023).

Weiter ist für den strategische Rahmen auf die Strategie «Digitale Verwaltung Schweiz 2024–2027» hinzuweisen, die am 1. Januar 2024 in Kraft getreten ist. Als zentrales Handlungsfeld wird in dieser Strategieperiode unter anderem der Fokus auf Basisdienste und Infrastrukturen gelegt.

Grundlage für die Umsetzung der Strategie Digitale Verwaltung 2018–2023 bilden die vom Regierungsrat festgelegten Leitsätze «gemeinsam digital unterwegs». Die Umsetzung der Leitsätze erfolgt im Rahmen von fünf strategischen Initiativen (RRB Nrn. 1362/2021, 1331/2022 und 914/2023). Die strategische Initiative Recht (SI Recht) befasst sich dabei mit den rechtlichen Aspekten der digitalen Transformation. Diese sollen proaktiv und mit Blick auf die Bedürfnisse der Einwohnerinnen und Einwohner sowie Unternehmen angegangen werden (Ambition SI Recht, RRB Nr. 1331/2022, S. 5). Ein Ziel der strategischen Initiative ist der Auf- und Ausbau digitaler Basisdienste und die Schaffung der notwendigen Rechtsgrundlagen.

Digitale Basisdienste sind von entscheidender Bedeutung, um staatliche Leistungen nutzendenfreundlich anzubieten und effizient abzuwickeln. Unter einem digitalen Basisdienst (auch: digitale «Grund-/Basisleistung» oder «Basis-Service») kann mit Blick auf das Verständnis auf Bundesebene und in anderen Kantonen ein auf Informations- und Kommunikationstechnologien basierender Dienst verstanden werden, der eine gemeinsame, übergreifende Grundlage für darauf aufbauende Leistungen bildet. Ein digitaler Basisdienst besteht losgelöst von einer einzelnen Verwaltungsaufgabe und steht unbestimmt vielen öffentlichen Organen zur Verfügung.

Digitale Basisdienste, wie ein gemeinsamer Einstiegspunkt zu elektronisch angebotenen Leistungen der öffentlichen Organe oder eine Zugangslösung, ermöglichen es private Nutzerinnen und Nutzern ihre Rechte und Pflichten einfach, durchgängig und sicher digital wahrzunehmen. Nutzerinnen und Nutzer sollen sich effizient mit den Behörden austauschen und mit möglichst geringem Aufwand Geschäfte abwickeln können. Den öffentlichen Organen dienen digitale Basisdienste als gemeinsame Grundlage für das Erbringen von Leistungen und tragen zugleich zur digitalen Transformation der Verwaltung bei. Dies gilt sowohl innerhalb der einzelnen Verwaltungseinheiten als auch im Verhältnis zwischen Kanton, Gemeinden und dezentralen Verwaltungsträgern wie etwa Spitälern, Hochschulen oder der Gebäudeversicherung Kanton Zürich.

Digitale Basisdienste sind von weiteren Begrifflichkeiten abzugrenzen. Zu unterscheiden ist ein Basisdienst von den darauf aufbauenden Leistungen, welche von den öffentlichen Organen über ihre (Fach-)Anwendungen (Fachapplikationen) erbracht werden und sich nach der jeweiligen Fachgesetzgebung richten. Digitale Basisdienste unterstützen die öffentlichen Organe bei der Leistungserbringung bzw. machen die Leistungen für Nutzerinnen und Nutzer einfacher zugänglich. Solche Leistungen umfassen etwa die elektronische Abwicklung von Bewilligungen (Arbeitsbewilligungen, Bewilligungen im Gesundheitswesen oder im Bereich Taxi- und Limousinendienste), Steuererklärungen, Einbürgerungsverfahren oder den selbstbestimmte Leistungsbezug durch Menschen mit Behinderung.

Um digitale Basisdienste rechtssicher einsetzen zu können, bedarf es eines sachgemäss ausgestalteten Rechtsrahmens (siehe SI Recht, Handlungsfeld 2; RRB Nr. 1331/2022, S. 6). Aufgrund ihrer umfassenden Nutzungsmöglichkeiten können digitale Basisdienste in der Regel nicht auf bestehende Fachgesetze gestützt werden, sondern bedürfen einer eigenen Rechtsgrundlage. Für die Weiterentwicklung der digitalen Verwaltung und damit der digitalen Transformation ist die Schaffung dieser Rechtsgrundlagen als wichtig und dringlich einzustufen. Mit der Motion KR-Nr. 158/2021 betreffend Digitale Grundleistungen Kanton und Gemeinden hat der Kantonsrat den Regierungsrat beauftragt, gesetzliche Grundlagen für ein digitales, standardisiertes Grundleistungsangebot von Kanton und Gemeinden zu schaffen (Stichwort Digitaler Service Public). Gestützt darauf hat die Staatsschreiberin den Projektauftrag für das Rechtsetzungsvorhaben «Rechtsgrundlagen digitale Basisdienste (DigiBasis)» erteilt.

Mit Beschluss vom 25. Oktober 2023 (RRB Nr. 1230/2023) hat der Regierungsrat das Normkonzept verabschiedet und die Staatskanzlei beauftragt, ihm ein Gesetz über digitale Basisdienste (nachfolgend VE-Gesetz über digitale Basisdienste) im Sinne des Normkonzepts zu unterbreiten. Das Vorhaben adressiert sowohl die im Rahmen der SI Recht skizzierten rechtlichen Bestrebungen als auch die vorgenannte Motion.

B. Grundlagen

1. Rechtsetzungskompetenz

Im Sachgebiet der digitalen Verwaltung kommt den Kantonen für den Bereich der kantonalen Verwaltungstätigkeit und des kantonalen Verfahrensrechts die Rechtsetzungskompetenz zu. Der Bund hat demgegenüber in denjenigen Sachgebieten, in welchen er über Rechtsetzungszuständigkeiten verfügt, die nicht auf den Erlass von Grundsätzen beschränkt sind, die Kompetenz zum Erlass und zur Durchsetzung von verbindlichen technischen und organisatorischen Vorgaben. Dies betrifft insbesondere die Bereiche des Zivil- und Strafrechts. Für die Schaffung einer schweizweit einheitlichen elektronischen Verwaltungslandschaft besteht hingegen keine allgemeine Bundeszuständigkeit (vgl. zum Ganzen: VPB 1/2012 vom 1. Mai 2012, Gutachten vom 22. Dezember 2011 betreffend Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, EJPD, Bundesamt für Justiz, Ziff. 3.2 und Ziff. 4.1).

Entsprechend ist der Kanton grundsätzlich kompetent, die für die von ihm entwickelten digitalen Basisdienste erforderlichen Rechtsgrundlagen zu erlassen mit Ausnahme derjenigen Bereiche, in denen der Bund über eine ausschliessliche Gesetzgebungskompetenz verfügt. So ist der Kanton insbesondere für die Regelung eines elektronischen Identifikationsnachweises im Sinne eines Ausweises («E-ID») kompetenzrechtlich nicht zuständig.



2. Rechtslage im Kanton Zürich

Im Kanton Zürich räumen Regierungs- und Kantonsrat der digitalen Transformation hohe Priorität ein. Dies zeigt sich sowohl in den Legislaturzielen (vgl. RRB Nrn. 670/2019 und 871/2023) und der Strategie Digitale Verwaltung als auch in der mit verschiedenen parlamentarischen Vorstössen zum Ausdruck gebrachten Forderung nach einer raschen digitalen Transformation und der Schaffung der dafür notwendigen rechtlichen Grundlagen. Die digitale Transformation soll vorangetrieben werden, indem Vorhaben aus den strategischen Initiativen und den Direktionen gebündelt und effizient realisiert werden; das kantonale Recht soll unterstützend für die digitale Transformation gestaltet werden.

Erste Rechtsgrundlagen für digitale Basisdienste werden in der vom Kantonsrat am 30. Oktober 2023 verabschiedeten Revision des Verwaltungsrechtspflegegesetzes (VRG, LS 175.2) (vgl. Vorlage 5853) und der neu zu erlassenden Verordnung über elektronische Verfahrenshandlungen im Verwaltungsverfahren (VeVV) (vgl. RRB Nr. 1286/2023 mit der Ermächtigung zur Vernehmlassung) geschaffen.

Im Zuge des weiteren Ausbaus des Angebotes der digitalen Verwaltung sollen digitale Basisdienste verstärkt und immer umfassender zum Einsatz kommen. Um die Weiterentwicklung digitaler Basisdienste und deren Nutzungsmöglichkeiten stetig zu erweitern, besteht aus rechtlicher Sicht Handlungsbedarf.

Es bestehen zahlreiche Facherlasse, welche bereichsspezifische Aspekte regeln, wie z.B. das Gesetz über die Organisation des Regierungsrates und der kantonalen Verwaltung, welches namentlich allen Stellen der kantonalen Verwaltung Zugang zu den Personendaten erlaubt, soweit sie diese zur Erfüllung ihrer Aufgaben brauchen (§ 44 OG RR, LS 172.1). Digitale Basisdienste stellen demgegenüber direktionsübergreifende Strukturen dar. Die Schaffung solcher Strukturen verlangt im Allgemeinen neue Rechtsgrundlagen, welche sich kaum über Änderungen der Fachgesetze realisieren lassen. Je nach Sachbereich oder Art der bearbeiteten Daten bedarf es dabei zur Wahrung des Grundrechtsschutzes einer spezifischen formell-gesetzlichen Grundlage.

Verschiedene Erlasse des kantonalen Rechts beinhalten Regelungen, die aufgrund ihres Inhalts und/oder ihres Querschnittcharakters Bezugspunkte zum vorliegenden Rechtsetzungsvorhaben aufweisen und entsprechend zu berücksichtigen sind: Namentlich der verfassungsrechtliche Persönlichkeitsschutz (Art. 13 Abs. 2 Bundesverfassung, BV, SR 101) und verschiedene kantonalrechtliche Vorgaben, wie etwa das Gesetz über die Information und den Datenschutz (IDG, LS 170.4) sowie die dazugehörige Verordnung über die Information und den Datenschutz (IDV, LS 170.41). Gestützt auf das IDG regelt die Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8) unter anderem Aspekte der Informationssicherheit. Rechnung zu tragen ist ferner dem Lebenszyklus von Informationen («end-to-end») und somit der Phase der archivierten Geschäfte nach Massgabe der Archivgesetzgebung (Archivgesetz, LS 170.6, sowie Archivverordnung, LS 170.61).

Das IDG befindet sich momentan in Totalrevision (Vorlage 5923). Im Rahmen der Arbeiten zu DigiBasis gilt es, Überschneidungen, Wiederholungen und Doppelspurigkeiten zu vermeiden.



3. Rechtslage in anderen Kantonen

Auch in anderen Kantonen wurden Gesetze im Bereich der digitalen Verwaltung geschaffen oder sind in Erarbeitung. Umfassende Regelungsansätze mit neuen Gesetzen zur digitalen Verwaltung bestehen in den Kantonen Bern (Gesetz/Verordnung über die Digitale Verwaltung, BSG 109.1/109.111), Glarus (Gesetz über die digitale Verwaltung, GS II H/1) und Graubünden (Gesetz über die digitale Verwaltung, noch nicht in Kraft) bzw. werden im Kanton Wallis (Gesetz über die digitalen Dienste der Behörden) demnächst parlamentarisch beraten.

Vom Regelungsbereich her eingeschränkter sind Gesetze im Kanton Basel-Stadt (Gesetz über ein zentrales elektronisches Behördenportal, SG 153.300), im Kanton Basel-Landschaft (Gesetz über die elektronische Geschäftsabwicklung und Kommunikation, E-Government-Gesetz, SGS 164) sowie im Kanton Solothurn (Gesetz über das Behördenportal, BGS 116.1), welche primär die Rechtsgrundlagen für ein Behördenportal schaffen. Weitere Kantone befassen sich mit den E-Government-Strukturen des Kantons und der Gemeinden (beispielsweise der Kanton St. Gallen mit dem Gesetz über E-Government, sGS 142.3, oder der Kanton Freiburg mit dem Gesetz über E-Government, SGF 184.1). In anderen Kantonen bestehen verfahrensrechtliche Regelungen zum elektronischen Verkehr (beispielsweise im Zuger Verwaltungsrechtspflegegesetz, BGS 162.1).

4. Rechtslage auf Bundesebene

Auf Bundesebene adressieren verschiedene Rechtsetzungsvorhaben Aspekte der digitalen Verwaltung. Zu nennen sind insbesondere das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben vom 17. März 2023 (EMBAG, SR 172.019) und die dazugehörige Verordnung (beide seit 1. Januar 2024 in Kraft), sowie die Entwicklungen im Zusammenhang mit der elektronischen Identität (Rechtsetzungsvorhaben des Bundes für ein Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise, BGEID) und der Digitalisierung im Justizbereich (Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz, BEKJ, BBI 2023 679; vgl. hierzu das Projekt Justitia 4.0). Diese Entwicklungen auf Bundesebene sind im vorliegenden Rechtsetzungsvorhaben soweit als möglich zu berücksichtigen, um einen Beitrag namentlich zur Interoperabilität im föderalen Kontext zu leisten.

C. Ziele und Umsetzung

1. Ziele

Mit dem Rechtsetzungsvorhaben sollen einerseits Rechtsgrundlagen für bestehende digitale Basisdienste geschaffen werden und andererseits der Rechtsrahmen für künftige Entwicklungen im Bereich der digitalen Basisdienste geschaffen werden. Bestehende rechtliche Grundlagen und andere Rechtsetzungsvorhaben im Bereich der digitalen Verwaltung sollen sachgemäss ergänzt werden.

Den Nutzerinnen und Nutzern sollen die digitalen Basisdienste einen Mehrwert bringen, indem Private ihre Rechte und Pflichten einfach, durchgängig und sicher wahrnehmen können. Nebst der elektronischen Identifizierung soll ein zentraler Zugang auf verschiedenste Leistungen öffentlicher Organe ermöglicht werden.



Die Nutzung der digitalen Basisdienste erfolgt freiwillig; eine allgemeine Nutzungspflicht ist zum jetzigen Zeitpunkt nicht vorgesehen. Eine bereichsspezifische Pflicht für ein öffentliches Organ, bestimmte Leistungen auch oder nur noch elektronisch zur Verfügung zu stellen, wäre mittels Anpassung der entsprechenden Fachgesetzgebung möglich.

DigiBasis soll entwicklungs offen und zukunftsorientiert ausgestaltet sein. Digitale Basisdienste entwickeln sich laufend fort; es können bestehende Basisdienste mit neuen Nutzungsmöglichkeiten weiterentwickelt oder gänzlich neue Basisdienste geschaffen werden. Hierzu soll mit dem Gesetz über digitale Basisdienste ein gemeinsamer Rechtsrahmen geschaffen werden. Statt einer allgemeinen Regelung der Zusammenarbeit werden Bestimmungen zur Interoperabilität und der Entwicklung von digitalen Basisdiensten in das neue Gesetz aufgenommen.

2. Abgrenzung

Digitale Basisdienste berühren potenziell eine Vielzahl von Verwaltungstätigkeiten und weisen komplexe Schnittstellen innerhalb der Verwaltung sowie zwischen der Verwaltung und verwaltungsexternen Akteurinnen und Akteuren auf. Eine Abgrenzung zu Regelungsthemen, welche nicht Gegenstand des Rechtsetzungsvorhabens sind, ist daher besonders wichtig.

Von einer umfassenden Regelung über die digitale Verwaltung wird zum jetzigen Zeitpunkt abgesehen. Eine solche hätte staatsrechtlich weitreichende Auswirkungen, welche eine grundsätzlichere Diskussion erfordern würden.

Nicht Bestandteil des Rechtsetzungsvorhabens ist die demokratische Partizipation über digitale Kanäle, wie beispielsweise die E-Partizipation oder das E-Voting. Hierbei handelt es sich um ein speziell ausgeprägtes Grundthema des Staatsrechts, welches in DigiBasis nicht behandelt wird.

Organisationsstruktur, Aufgaben und Finanzierung von egovpartner, der Zusammenarbeitsorganisation von Kanton und Gemeinden, sind Gegenstand eines anderen Vorhabens und werden in DigiBasis ausgeklammert.

Nicht beabsichtigt sind Änderungen von Fachgesetzen. Deren Vorgaben sind weiterhin massgeblich für die Erbringung von Leistungen durch das öffentliche Organ (zum Beispiel über ihre Fachanwendungen) sowie die Organisation und Zuständigkeiten innerhalb der Verwaltung.

3. Normstufe, Regelungsdichte und Regelungsbestimmtheit

Alle wichtigen Rechtssätze des kantonalen Rechts sind in der Form des Gesetzes zu erlassen (Art. 38 Abs. 1 Satz 1 Kantonsverfassung, KV, LS 101). Dazu gehören gemäss Art. 38 Abs. 1 KV namentlich die wesentlichen Bestimmungen über Organisation und Aufgaben der Behörden sowie Zweck, Art und Umfang staatlicher Leistungen (lit. c und e). Weniger wichtige Rechtssätze, namentlich solche über den Vollzug der Gesetze, werden demgegenüber in der Form der Verordnung erlassen (Art. 38 Abs. 2 KV).

Leitlinie und gleichzeitige Herausforderung bei der Schaffung von Rechtsgrundlagen zu digitalen Basisdiensten ist es, bei der Gestaltung und Umsetzung der digitalen Verwaltung



Rechtssicherheit zu schaffen und zugleich Flexibilität hinsichtlich technischer Lösungen zu bewahren. Die Dichte und der Bestimmtheitsgrad sollen so gewählt werden, dass bedürfnisgerechte, wirkungsorientierte Entscheidungen getroffen werden können und eine Orientierung an der Nachfrage nach Leistungen der Verwaltung ermöglicht wird. Grundsätzlich sollen auf Dauer angelegte Regelungen auf Gesetzesstufe festgelegt werden. Dem Anspruch auf Flexibilität im Regelungsbereich mit technischen Entwicklungen kann demgegenüber mit einer Verordnungskompetenz des Regierungsrates Rechnung getragen werden.

4. Aufbau des Gesetzes

Der Neuerlass regelt die digitalen Basisdienste anwendungsorientiert, damit dem individuellen Regelungsbedarf der Basisdienste Rechnung getragen werden kann. Es ist davon auszugehen, dass das Gesetz regelmässig anzupassen sein wird. Mit dem gewählten «modularen» Aufbau können auch künftig erforderliche Bestimmungen zu neuen digitalen Basisdiensten aufgenommen und auf einfache Art und Weise in die Struktur des Gesetzes integriert werden.

Die Einleitenden Bestimmungen adressieren den Regelungsgegenstand und den Geltungsbereich: Regelungsgegenstand sind die im Gesetz geregelten digitalen Basisdienste. Der persönliche Geltungsbereich ist weit ausgestaltet und richtet sich an Nutzerinnen und Nutzer sowie an öffentliche Organe:

- Das Gesetz richtet sich einerseits an Nutzerinnen und Nutzer, also Privatpersonen wie Unternehmen, welche Leistungen der öffentlichen Organe beziehen oder im Austausch mit öffentlichen Organen stehen. Verankert wird, welche Personendaten in welcher Weise über sie bearbeitet werden. Die Rechte und Pflichten sind ebenfalls verankert.
- Andererseits fallen die öffentlichen Organe in den Geltungsbereich, wenn sie ihre Leistungen aufbauend auf digitalen Basisdiensten anbieten oder im Austausch mit Nutzerinnen und Nutzern von digitalen Basisdiensten stehen. Regelungsbedarf zeigt sich hierbei insbesondere bezüglich der Frage, welche Daten die öffentlichen Organe in welcher Weise bearbeiten dürfen und welche Rechte und Pflichten sie dabei haben.

Digitale Basisdienste tragen zum medienbruchfreien Arbeiten bei. Der 2. Abschnitt knüpft hier an und adressiert die Durchgängigkeit der Systeme verschiedener öffentlicher Organe (sog. Interoperabilität). Dies trifft einerseits für die öffentlichen Organe innerhalb des Kantons zu, etwa zwischen den Gemeinden und dem Kanton, andererseits in der Zusammenarbeit mit öffentlichen Organen anderer Kantone und des Bundes. Mit den Basisdiensten kann zudem der Kontakt zwischen öffentlichen Organen und den Nutzerinnen und Nutzern erleichtert werden. Zum Zweck der Stärkung der Interoperabilität sollen in diesem Abschnitt Delegationsgrundlagen zugunsten des Regierungsrates geschaffen werden, rasch und mit der notwendigen Flexibilität Standards und Schnittstellen für verbindlich erklären zu können und zudem Vereinbarungen mit dem Bund und anderen Kantonen im Bereich digitaler Basisdienste abschliessen zu können.

Digitale Basisdienste entwickeln sich ständig weiter. Die Nutzungsmöglichkeiten bestehender Basisdienste werden ausgebaut oder neue Basisdienste entwickelt. Die technologischen Möglichkeiten für die elektronische Abwicklung von Leistungen öffentlicher Organe erweitern sich ebenfalls laufend. Unter den Voraussetzungen im 3. Abschnitt sollen

die Nutzungsmöglichkeiten von bestehenden digitalen Basisdiensten ausgebaut bzw. neue digitale Basisdienste entwickelt werden können.

Im 4. Abschnitt werden folgende digitale Basisdienste geregelt:

- Elektronische Identifizierung: Für eine rechtssichere Interaktion mit öffentlichen Organen muss die Identität der Nutzerinnen und Nutzer in angemessener Qualität nachweisbar sein. Für den Zugriff auf elektronisch angebotene Leistungen ist es deshalb oftmals nötig, Kontakt- und Identitätsdaten zu erfassen. Die Nutzerinnen und Nutzer sollen sich über eine einheitliche Authentifizierungslösung des Bundes sicher identifizieren können, wenn dies für den Zugriff auf eine elektronisch angebotene Leistung erforderlich ist.
- Zentraler Zugang zu elektronisch angebotenen Leistungen öffentlicher Organe: Den Nutzerinnen und Nutzer sollen über einen Einstiegspunkt elektronisch angebotene Leistungen der öffentlichen Organe zugänglich gemacht werden.
- Digitaler Arbeitsplatz: Für das Erbringen von Leistungen (z.B. zur Erarbeitung von Akten oder zur Kommunikation der Mitarbeitenden verschiedener öffentlicher Organe untereinander) stehen den öffentlichen Organen verschiedenste Arbeitsmittel zur Verfügung. Die Nutzung von cloudbasierten Anwendungen im digitalen Arbeitsplatz ist an bestimmte Voraussetzungen geknüpft. Ergänzend wird eine Anpassung des Gesetzes über die Auslagerung von Informatikdienstleistungen vorgeschlagen (vgl. zur Nebenänderung die Schluss- und Übergangsbestimmungen).

Das Gesetz ist unbefristet angelegt. Übergangsfristen für den Vollzug sind nicht vorgesehen.

D. Auswirkungen

Digitale Basisdienste können von Privaten und Unternehmen sowie von öffentlichen Organen genutzt werden:

- Für die Nutzerinnen und Nutzer bieten digitale Basisdienste einen Mehrwert, indem sie den Zugang zu elektronisch angebotenen Leistungen der öffentlichen Organe vereinheitlichen und erleichtern. Der Zugang steht den Nutzerinnen und Nutzern grundsätzlich freiwillig zur Verfügung. Eine Gebühr für die Nutzung des Webzugangs «Zürikonto» ist nicht vorgesehen. Auch für die Nutzung einzelner digitaler Basisdienste sind keine Gebühren vorgesehen. Insgesamt dürften sich die finanziellen Auswirkungen für die Nutzerinnen und Nutzer in einem überschaubaren Rahmen halten.
- Mit dem Gesetz über digitale Basisdienste soll keine Pflicht der öffentlichen Organe eingeführt werden, ihre Leistungen auch elektronisch anbieten zu müssen. Entsprechende Vorgaben hierfür ergeben sich aus dem Verfahrensrecht sowie nach Massgabe der Fachgesetzgebung. Mit den zur Verfügung gestellten digitalen Basisdiensten und der Schaffung gemeinsamer Grundlagen soll die Erbringung von Leistungen der öffentlichen Organe insgesamt vereinfacht werden. Indem digitale Basisdienste für eine Vielzahl von Abläufen in der Verwaltung genutzt werden können, können gemeinsame Lösungen vermehrt anstelle von Einzellösungen treten.



Da aufgrund der Vorlage keine neuen Verwaltungsaufgaben hinzukommen oder wegfallen, sind keine personellen Auswirkungen zu erwarten. Mit den einzelnen digitalen Basisdiensten verbundene finanzielle und personelle Aufwendungen sind im Zusammenhang mit der Beschaffung und Einführung von konkreten Lösungen im Rahmen der entsprechenden Projekte auszuweisen.

E. Regulierungsfolgeabschätzung

Gemäss dem Gesetz zur administrativen Entlastung der Unternehmen vom 5. Januar 2009 (EntlG, LS 930.1) ist der administrative Aufwand von Unternehmen bei der Erfüllung von Vorschriften möglichst gering zu halten. Zu diesem Zweck werden alle neuen oder zu ändernden Erlasse einer Regulierungsfolgeabschätzung unterzogen (§ 3 Abs. 2 EntlG in Verbindung mit § 5 der Verordnung zur administrativen Entlastung der Unternehmen vom 18. August 2010 [EntlV, LS 930.11]).

Das zu ändernde Gesetz und die Verordnung führen zu keinen Mehrbelastungen von Unternehmen im Sinne des EntlG. Da mit dem Gesetz über digitale Basisdienste keine umfassende Pflicht zur Schaffung oder Nutzung von digitalen Basisdiensten vorgesehen ist, ist nicht von weitreichenden personellen oder finanziellen Folgen für die Nutzerinnen und Nutzer (Private und Unternehmen) bzw. für die öffentlichen Organe auszugehen.

Kosten entstehen den öffentlichen Organen beim Aufbau, Betrieb und der Weiterentwicklung von digitalen Basisdiensten sowie beim Erbringen von elektronischen Leistungen durch die öffentlichen Organe. Digitale Basisdienste tragen zu Effizienzsteigerungen, Vereinheitlichungen und der Nutzung von Synergien bei, sodass die digitalen Basisdienste mittelfristig zu einer Kostensenkung beitragen.

Es liegt im Sinne von § 1 Abs. 2 lit. a und b EntlG, dass mit den digitalen Basisdiensten die Leistungserbringung der öffentlichen Organe unterstützt und der Verkehr mit den öffentlichen Organen erleichtert wird. Indem digitale Basisdienste für die Leistungserbringung effizienzsteigernd und damit beschleunigend wirken, wird zudem § 2 Abs. 1 EntlG Rechnung getragen. Weiter ist von Kosteneinsparungen (unter anderem beim Material und Versand) auszugehen.

F. Erläuterungen zu den einzelnen Bestimmungen

Nähere Erläuterungen zu den einzelnen Bestimmungen des Vorentwurfs finden sich in der nachfolgenden synoptischen Darstellung.

**Vorentwurf****Erläuterungen****Gesetz über digitale Basisdienste**

(vom)

Der Kantonsrat,

nach Einsichtnahme in den Antrag des Regierungsrates vom (...) und der [Kommission] vom (...),

beschliesst:

I. Es wird folgendes Gesetz erlassen:

1. Abschnitt: Einleitende Bestimmungen

Gegenstand

§ 1. Dieses Gesetz regelt:

Mit dem Gesetz werden die rechtlichen Anforderungen an den Betrieb und die Nutzung digitaler Basisdienste verankert. Unter einem digitalen Basisdienst (auch: digitale «Grund-/Basisleistung» oder «Basis-Service») ist mit Blick auf das Verständnis auf Bundesebene und in anderen Kantonen ein auf Informations- und Kommunikationstechnologien basierender Dienst zu verstehen, der eine gemeinsame, übergreifende Grundlage für darauf aufbauende Leistungen bildet. Ein digitaler Basisdienst besteht losgelöst von einer einzelnen Verwaltungsaufgabe und steht unbestimmt vielen öffentlichen Organen zur Verfügung.

- a. den Betrieb, die Nutzung und die Weiterentwicklung der in diesem Gesetz genannten digitalen Basisdienste,
- b. die Entwicklung neuer digitaler Basisdienste.

Geltungsbereich

§ 2. ¹ Dieses Gesetz gilt für öffentliche Organe, wenn sie in diesem Gesetz genannte digitale Basisdienste betreiben, nutzen und weiterentwickeln oder neue digitale Basisdienste entwickeln.

Um die Grundlagen für umfassende und effektive digitale Basisdienste im Kanton zu schaffen, wird der persönliche Geltungsbereich möglichst weit gezogen.

Der Begriff der öffentlichen Organe richtet sich nach § 3 IDG, wonach öffentliche Organe sind: der Kantonsrat, die Gemeindeparlamente sowie die Gemeindeversammlungen (lit. a), Behörden und Verwaltungseinheiten

**Vorentwurf****Erläuterungen**

des Kantons und der Gemeinden (lit. b) sowie Organisationen und Personen des öffentlichen und privaten Rechts, soweit sie mit der Erfüllung öffentlicher Aufgaben betraut sind (lit. c). In der Totalrevision des IDG soll der Begriff der öffentlichen Organe beibehalten werden (§ 5 Abs. 1 E-IDG gemäss Vorlage 5923).

Die Bestimmungen des Gesetzes über digitale Basisdienste gelten, wenn ein öffentliches Organ einen digitalen Basisdienst betreibt oder zur Erbringung einer Leistung nutzt. Bietet z.B. ein kantonales Amt eine Leistung auf elektronischem Weg an und möchte diese den Nutzerinnen und Nutzern über den zentralen Zugang zur Verfügung stellen, hat das Amt die entsprechenden Bestimmungen über den Zugang zu beachten. Die eigentliche Leistung erfolgt nach Massgabe der Fachgesetzgebung (beachte zudem § 44 Abs. 2 und 3 OG RR zur Bearbeitung von Personendaten im Rahmen der Aufgabenerfüllung). Das Gesetz über digitale Basisdienste kommt auch dann zur Anwendung, wenn das öffentliche Organ einen bestehenden digitalen Basisdienst weiterentwickelt oder einen neuen digitalen Basisdienst entwickeln will.

² Es gilt für private Nutzerinnen und Nutzer, wenn sie die in diesem Gesetz genannten digitalen Basisdienste nutzen.

Unter Nutzerinnen und Nutzern sind natürliche und juristische Personen zu verstehen, die einen digitalen Basisdienst *nutzen*, aber kein öffentliches Organ im Sinne von Abs. 1 sind. Zu beachten ist, dass Private, die digitale Basisdienste *anbieten und weiterentwickeln*, unter die Bestimmungen über die Auslagerung gemäss IDG fallen.

Die Nutzung der digitalen Basisdienste ist grundsätzlich freiwillig. Nutzt eine natürliche oder eine juristische Person einen digitalen Basisdienst, gelten die entsprechenden Bestimmungen über den betreffenden digitalen Basisdienst. Gewisse digitale Basisdienste umfassen primär Vorgänge zwischen den öffentlichen Organen. Entsprechend stehen solche «internen» digitalen Basisdienste den Nutzerinnen und Nutzern nicht zur Verfügung. Als Ausnahme zur freiwilligen Nutzung kann in einzelnen Sachbereichen vorgesehen sein, dass der Kontakt mit öffentlichen Organen oder die Vornahme eines Geschäftsvorganges (z.B. die Einreichung eines Bewilligungsgesuchs) primär oder ausschliesslich auf elektronischem Weg stattzufinden hat. Die Rechtsgrundlage für eine solche Pflicht ergibt sich aus dem Verfahrensrecht und/oder der Fachgesetzgebung.

³ Die Erbringung einer elektronisch angebotenen Leistung durch das öffentliche Organ richtet sich nach der Fachgesetzgebung.

Abs. 3 verdeutlicht, dass digitale Basisdienste unabhängig von den jeweiligen Aufgaben und der namentlich daraus resultierenden Leistung eines öffentlichen Organs bestehen. Entsprechend werden mit dem Gesetz über digitale Basisdienste namentlich keine Rechtsgrundlagen dafür geschaffen, dass eine Leistung eines öffentlichen Organs elektronisch angeboten wird. Hierfür haben die öffentlichen Organe die für sie geltenden Fachgesetze zu beachten. Bereichsspezifische Bestimmungen – gerade auch des Bundesrechts, etwa zur elektronischen Kommunikation in der Justiz – bleiben ebenfalls vorbehalten.



Eine Datenbearbeitung, die für das Erbringen einer Leistung erforderlich ist, erfolgt durch das für die elektronisch angebotene Leistung zuständige öffentliche Organ. Die Hoheit über die Daten im Rahmen der elektronisch angebotenen Leistung und somit auch der einzelnen Geschäftsfälle der Nutzerinnen und Nutzer bleibt beim zuständigen öffentlichen Organ. Die für die Datenbearbeitung erforderlichen Rechtsgrundlagen ergeben sich aus der Fachgesetzgebung. Das öffentliche Organ, das die Leistung elektronisch anbietet, bleibt für die Archivierung und die Einhaltung der Lösungsfristen verantwortlich.

2. Abschnitt: Interoperabilität

Standards und Schnittstellen

§ 3. ¹ Zur Gewährleistung der Durchgängigkeit der in diesem Gesetz geregelten digitalen Basisdienste kann der Regierungsrat für verbindlich erklären:

- a. die Anwendung von technischen und organisatorischen Standards,
- b. die Standardisierung der technischen Schnittstellen zu einer elektronisch angebotenen Leistung eines öffentlichen Organs.

Standardisierung kann dazu beitragen, dass unterschiedliche Systeme miteinander kompatibel sind und trägt somit zur Interoperabilität bei. Der Regierungsrat soll Standards und Schnittstellen für verbindlich erklären können. Statt einer starren Verankerung auf Gesetzesstufe soll mittels Verordnung rasch auf Bedürfnisse der öffentlichen Organe nach Standardisierung und Entwicklungen auf Bundesebene und in anderen Kantonen reagiert werden können. Künftige Entwicklungen sollen nicht unnötig durch starre Vorgaben blockiert werden. Ziel soll es sein, soweit möglich und erforderlich, regulatorisch zu einer gewissen Vereinheitlichung der Vorgaben beizutragen, die das Funktionieren der digitalen Basisdienste im Kanton oder den Anschluss an Lösungen anderer Kantone oder des Bundes erleichtern.

Die verbindliche Anwendung von technischen und organisatorischen Standards kann die Durchgängigkeit digitaler Basisdienste entscheidend vereinfachen.

Die Standardisierung der technischen Schnittstellen von Fachanwendungen zu digitalen Basisdiensten kann massgeblich zur Durchgängigkeit beitragen und damit auch die Entwicklung der digitalen Transformation der öffentlichen Organe gerade in der institutionsübergreifenden Zusammenarbeit entscheidend fördern.

² Er orientiert sich dabei an nationalen und internationalen Standards sowie am Stand der Technik.

Der Regierungsrat soll sich bei einer Verbindlicherklärung am aktuellen Stand der Technik orientieren. Begezogen werden können die national oder international entwickelten Standards (wie z.B. ISO-Standards, eCH-Standards usw.). Innerkantonale zu berücksichtigen ist die Archivtauglichkeit der Formate nach Massgabe der Archivgesetzgebung und der IVSV.



Vorentwurf

Erläuterungen

Vereinbarungen mit Bund und Kantonen

§ 4. Der Regierungsrat ist ermächtigt, Vereinbarungen mit dem Bund und anderen Kantonen zur Zusammenarbeit im Bereich der digitalen Basisdienste und zum Anschluss an digitale Basisdienste abzuschliessen.

Digitale Basisdienste werden unabhängig von einzelnen Verwaltungsaufgaben genutzt. Im föderalistischen Kontext bestehen verschiedene Bestrebungen im Bereich der Digitalisierung. Um bei Bedarf den Anschluss an Lösungen wie zum Beispiel eine Plattform des Bundes bzw. des Bundes gemeinsamen mit den Kantonen oder anderer Kantone sicherstellen zu können, müssen unter Umständen Vereinbarungen zwischen dem Kanton Zürich und dem Bund und/oder anderen Kantonen abgeschlossen werden.

Ein Beispiel ist die Vereinbarung zur Gründung einer Körperschaft, die eine zentrale Plattform für die Abwicklung der elektronischen Kommunikation in der Justiz aufbaut und betreibt (vgl. Art. 3 E-BEKJ). Gestützt auf § 4 VE-Gesetz über digitale Basisdienste soll der Regierungsrat namentlich diese Vereinbarung im eigenen Namen abschliessen können (§ 7 Abs. 3 lit. b OG RR).

3. Abschnitt: Entwicklung von digitalen Basisdiensten

Voraussetzungen

§ 5. ¹ Vor dem Erlass einer Rechtsgrundlage können bestehende digitale Basisdienste weiterentwickelt und neue digitale Basisdienste entwickelt werden, wenn:

Unter Entwicklung wird einerseits die Weiterentwicklung von bestehenden digitalen Basisdiensten verstanden. Hierunter fallen könnten beispielsweise neue elektronische Zugangsmöglichkeiten. Erfasst ist andererseits auch die Entwicklung neuer digitaler Basisdienste. Als Beispiel genannt werden kann eine zentrale Plattform für den Datenaustausch im Kanton.

§ 5 VE-Gesetz über digitale Basisdienste adressiert Situationen, in welchen die Inbetriebnahme eines digitalen Basisdienstes und das Inkrafttreten von erforderlichen Rechtsgrundlagen aufgrund der unterschiedlichen Geschwindigkeiten und Abhängigkeiten von technischer Entwicklung und Rechtsetzungsverfahren zeitlich auseinanderfallen. Dabei ist zu beachten, dass die Ausgestaltung der erforderlichen Rechtsgrundlagen für digitale Basisdienste in der Regel ohne ein fortgeschrittenes Projekt und erste Erfahrungen mit Nutzerinnen und Nutzern und daraus resultierenden Anpassungen des Produkts regelmässig nicht durchführbar sein dürfte. Damit digitale Basisdienste dennoch möglichst rasch entwickelt werden können sowie zur Stärkung der Rechtssicherheit und Planbarkeit in der Entwicklungsphase soll festgelegt werden, unter welchen kumulativ zu erfüllenden Voraussetzungen digitale Basisdienste bereits vor Erlass der erforderlichen Rechtsgrundlagen in Betrieb genommen werden dürfen.

**Vorentwurf****Erläuterungen**Abgrenzungen

Im Gegensatz zu Pilotversuchen geht es vorliegend um Übergangsphasen bei einem Projekt, das erstmals oder in einer weiterentwickelten Version in den Betrieb übergeben wird und die Rechtsgrundlagen nicht ausreichend schnell angepasst werden können. Das E-IDG reguliert die Durchführung von Pilotversuchen. Nach §§ 28 f. E-IDG gemäss Vorlage 5923 kann der Regierungsrat die Bearbeitung von besonderen Personendaten vor dem Erlass einer Rechtsgrundlage als Pilotversuche durch Verordnung bewilligen, wenn die Aufgaben, welche die fragliche Bearbeitung erfordern, ihrerseits in einem Gesetz geregelt sind (lit. a). Zudem sollen überdies ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden, damit die Eingriffe in die Grundrechte der betroffenen Personen möglichst begrenzt werden (lit. b). Schliesslich muss die Testphase für die praktische Umsetzung der Datenbearbeitung notwendig sein (lit. c).

Die Voraussetzungen nach § 5 VE-Gesetz über digitale Basisdienste sind nur dann anwendbar, wenn Rechtsgrundlagen überhaupt erforderlich sind. Kann ein digitaler Basisdienst auf einer bestehenden Rechtsgrundlage entwickelt bzw. weiterentwickelt werden, sind die Voraussetzungen nicht anwendbar.

- a. die erforderlichen Massnahmen für die Informationssicherheit und die Sicherstellung des Datenschutzes getroffen worden sind,

Als Voraussetzung für die Entwicklung von digitalen Basisdiensten wird in lit. a festgehalten, dass bestehende Vorgaben – namentlich des IDG – vom öffentlichen Organ weiterhin einzuhalten sind. So muss das öffentliche Organ bei einer beabsichtigten Bearbeitung von Personendaten deren Risiken für die Grundrechte der betroffenen Personen bewerten (Datenschutz-Folgenabschätzung) und bei einer beabsichtigten Bearbeitung von Personendaten mit besonderen Risiken für die Grundrechte der betroffenen Personen vorab der oder dem Beauftragten für den Datenschutz zur Prüfung unterbreiten (Vorabkontrolle; siehe zu beiden Verpflichtungen § 10 IDG).

- b. die Aufgaben, aufgrund derer die Bearbeitung von Personendaten in einem weiter- oder neu entwickelten digitalen Basisdienst erfolgen soll, in einem Gesetz geregelt sind oder das Rechtsetzungsverfahren gestartet worden ist und

In digitalen Basisdiensten werden Personendaten in der Art und vom Umfang her bearbeitet, die unter Umständen über die im Rahmen der Aufgabenerfüllung übliche Datenbearbeitung hinaus reicht. Vielfach besteht für die Datenbearbeitung daher Regelungsbedarf. Mit dieser Voraussetzung soll sichergestellt werden, dass die für die Entwicklung eines digitalen Basisdienstes erforderlichen Rechtsabklärungen getroffen worden sind. Wird ein normativer Handlungsbedarf festgestellt, ist dieser durch das zuständige öffentliche Organ beispielsweise in einem Projektdurchführungsauftrag auszuweisen und die Einleitung eines Rechtsetzungsverfahrens anzustreben.

- c. im Rahmen des weiter- oder neu entwickelten digitalen Basisdienstes keine besonderen Personendaten bearbeitet werden.

In einem weiter- oder neu entwickelten digitalen Basisdienst dürfen keine besonderen Personendaten bearbeitet werden, bis die entsprechenden Rechtsgrundlagen vorliegen. Die in §§ 28 f. E-IDG vorgesehenen Bestimmungen zur Durchführung von Pilotversuchen bleiben vorbehalten.



Vorentwurf

Erläuterungen

² Ist die Rechtsgrundlage fünf Jahre nach Beschluss nach § 5 nicht in Kraft gesetzt, gelten die Voraussetzungen für die Entwicklung als nicht erfüllt. Das öffentliche Organ kann dem Regierungsrat eine einmalige Verlängerung um zwei Jahre beantragen.

Ist die erforderliche Rechtsgrundlage spätestens fünf Jahre nach Beschluss gemäss § 5 VE-Gesetz über digitale Basisdienste nicht in Kraft gesetzt, kann das öffentliche Organ dem Regierungsrat eine einmalige Verlängerung um höchstens zwei Jahre beantragen. Diese zeitliche Begrenzung scheint sachgemäss, um allfälligen Verzögerungen im Rechtsetzungsprozess genügend Rechnung zu tragen.

Zuständigkeiten

§ 6. ¹ Der Regierungsrat bewilligt die Entwicklung von digitalen Basisdiensten des Kantons nach § 5.

Der erforderliche Beschluss für die Entwicklung von digitalen Basisdiensten des Kantons vor Erlass einer Rechtsgrundlage bzw. Revision des Gesetzes über digitale Basisdienste erfolgt durch den Regierungsrat. Dies ist sachgemäss, weil es sich bei digitalen Basisdiensten um direktionsübergreifende Dienste handelt, die von verschiedensten öffentlichen Organen genutzt werden können. Die jeweils erforderlichen Beschlüsse des Regierungsrates stärken weiter den Überblick über die im Kanton entwickelten digitalen Basisdienste.

² Für Gemeinden gilt § 5 sinngemäss. Zuständig für die Bewilligung ist der Gemeindevorstand.

Auch Gemeinden sollen digitale Basisdienste unter vorgegebenen Bestimmungen rechtssicher weiterentwickeln können, während sie parallel dazu die für den Betrieb dieser Dienste notwendigen Rechtsgrundlagen erarbeiten. Hierfür zuständig sein soll der Gemeindevorstand.

Mit der Vorlage werden indessen die Zuständigkeiten für die Leitungsorgane anderer öffentlicher Organe, etwa der Spitäler oder Hochschulen, nicht berührt. Sollen einem öffentlichen Organ die Entwicklung digitaler Basisdienste während einem laufenden Rechtsetzungsvorhaben zur Schaffung der notwendigen Rechtsgrundlagen durch die eigenen Leitungsorgane ermöglicht werden, müsste dies im entsprechenden Spezialgesetz des öffentlichen Organs geregelt werden.

4. Abschnitt: Digitale Basisdienste

A. Elektronische Identifizierung

Nutzung des Authentifizierungsdienstes des Bundes

§ 7. Das öffentliche Organ kann zur elektronischen Identifizierung einer Nutzerin oder eines Nutzers den vom Bund betriebenen Authentifizierungsdienst verwenden.

Für den Zugriff auf elektronisch angebotene Leistungen öffentlicher Organe ist es oftmals nötig, Kontakt- und Identitätsdaten der Nutzerinnen und Nutzer in angemessener Qualität zu erfassen. Mit einem Authentifizierungs- bzw. Authentisierungsvorgang erfolgt die Prüfung einer behaupteten Identität eines Subjekts. Das Vorhaben «Authentifizierungsdienst der Schweizer Behörden (AGOV)» des Bundes schafft ein nationales, einheitliches und standardisiertes Authentisierungs- und Identitätsverwaltungssystem. Mit AGOV



sollen sich natürliche Personen vor allen Schweizer Behörden sicher identifizieren können, wenn dies für eine Leistung eines öffentlichen Organs erforderlich ist. AGOV wird vom Bund betrieben und ist durch die Bundesgesetzgebung geregelt. Gestützt auf Art. 11 Abs. 3 EMBAG wird AGOV auch den Kantonen und Gemeinden als IKT-Mittel zur Verfügung gestellt. Die Kantone können den Dienst im Rahmen ihrer Bedarfsverwaltung einsetzen. Für die Verwendung von AGOV mit einem breiten Einsatzbereich schafft das Gesetz über digitale Basisdienste die kantonalrechtlich erforderlichen Grundlagen.

Der Basisdienst darf von sämtlichen öffentlichen Organen verwendet werden, um Nutzerinnen und Nutzer einer elektronisch angebotenen Leistung zu identifizieren. Die Verwendung von anderen, gleichwertigen Authentifizierungsdiensten durch öffentliche Organe ist hiervon nicht betroffen.

Eine generelle Pflicht zur Nutzung eines Authentifizierungsdienstes besteht nicht. Die Nutzung von AGOV ist jedoch vorausgesetzt, um bestimmte Leistungen der öffentlichen Organe elektronisch in Anspruch zu nehmen. So wird AGOV namentlich für den Webzugang (§§ 10 ff. VE-Gesetz über digitale Basisdienste) verwendet.

Abgrenzungen

Der Vorgang der elektronischen Identifizierung ist vom eigentlichen Nachweis der Identität zu unterscheiden. Die Einführung und Ausstellung eines amtlichen elektronischen Identitätsnachweises im Sinne eines Ausweises (E-ID) ist Gegenstand von Bundesrecht. Entsprechende Rechtsgrundlagen werden im Kontext des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (BGEID) erarbeitet.

Identifizieren und authentifizieren bezeichnen zwei Vorgänge mit unterschiedlichem Regelungsbedarf, die auseinander zu halten sind. Es besteht insoweit ein Zusammenhang, als dass die E-ID künftig – als digitaler Identitätsnachweis – vorgewiesen und – via AGOV-Authentifizierung – daraus direkt ein Login-Vorgang für den Zugriff auf bestimmte elektronisch angebotene Leistungen abgeleitet werden können soll (vgl. Botschaft zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise vom 22. November 2023, BBl 2023 2842 S. 51).

Weiter unterscheidet sich der Authentifizierungsdienst von einer elektronischen Signatur. Unter einer elektronischen Signatur werden mit elektronischen Informationen verknüpfte Daten verstanden, mit denen die unterzeichnende bzw. signaturerstellende Person identifiziert und die Integrität der signierten elektronischen Informationen geprüft werden kann. Das VRG ermöglicht künftig den rechtsgültigen Einsatz von elektronischen Signaturen gemäss dem Bundesgesetz über die elektronische Signatur (SR 943.03) im Rahmen des Verwaltungsverfahrens (Änderung VRG vom 30. Oktober 2023; elektronische

**Vorentwurf****Erläuterungen**

Verfahrenshandlungen, Vorlage 5853; nachfolgend nVRG). Eine zusätzliche Regelung der elektronischen Signatur im VE-Gesetz über digitale Basisdienste ist nicht notwendig.

Datenbearbeitung

§ 8. ¹ Das öffentliche Organ kann im Rahmen einer elektronisch angebotenen Leistung folgende Personendaten über den Authentifizierungsdienst des Bundes anfordern:

Der Bund als Betreiber von AGOV bearbeitet Daten über die Identität von Personen nach Massgabe der bundesrechtlichen Vorgaben. Diese Daten können dem Kanton zur Verfügung gestellt werden. Hierfür sind kantonalrechtliche Grundlagen erforderlich, wie etwa zur Übermittlung der Ergebnisse der Authentifizierung an ein öffentliches Organ im Rahmen einer elektronisch angebotenen Leistung.

- a. amtlicher Name,
- b. amtliche Vornamen,
- c. Geburtsdatum,
- d. Nationalität,
- e. Geschlecht,
- f. Geburtsort,
- g. AHV-Nummer,
- h. verifizierte E-Mailadresse,
- i. Strasse,
- j. Hausnummer,
- k. Postleitzahl,
- l. Ort.

² Es legt die Vertrauensstufe fest, die im Rahmen der elektronisch angebotenen Leistung erforderlich ist.

Der Authentifizierungsdienst unterstützt Identitäten verschiedener Vertrauensstufen gemäss AGOV (AGOV-Authentifizierungsqualitäten, sog. AGOVaq). Werden Angaben nicht nur selbst deklariert, sondern auch verifiziert (nach bundesrechtlich geregelten Vorgängen), kann eine höhere Vertrauensstufe erreicht werden. Die Anforderung an die Stufe, die von der Nutzerin oder dem Nutzer zu erreichen ist, wird vom öffentlichen Organ im Rahmen der elektronisch angebotenen Leistung festzulegen sein.



Vorentwurf

Erläuterungen

³ Es fordert nur diejenigen Personendaten gemäss Abs. 1 an, die für die jeweilige Vertrauensstufe erforderlich sind.

Das öffentliche Organ hat die Vertrauensstufe der Identifizierung so zu wählen, wie sie für die einzelne elektronische Leistung erforderlich ist. Bereits aus dem datenschutzrechtlichen Grundsatz der Verhältnismässigkeit ergibt sich, dass eine Überidentifizierung nicht zulässig ist.

Verantwortung

§ 9. Das öffentliche Organ, das Personendaten gemäss § 8 bezieht, ist bei deren Bearbeitung im Rahmen einer elektronisch angebotenen Leistung für die Einhaltung der Informationssicherheit und des Datenschutzes verantwortlich.

Die Verwendung eines Authentifizierungsdienstes des Bundes durch kantonale öffentliche Organe kann Fragen zum Verhältnis zwischen Bundesrecht und kantonalem Recht aufwerfen. Die öffentlichen Organe des Kantons sind verantwortlich, wenn sie Daten aus einem gemeinsamen Informationsbestand bearbeiten, wie dies bei der Verwendung von AGOV und der Bearbeitung von Daten, die von AGOV angefordert werden, der Fall sein kann.

B. Zugang zu elektronisch angebotenen Leistungen

Webzugang

§ 10. ¹ Der Kanton ermöglicht Nutzerinnen und Nutzern einen zentralen Zugang zu elektronisch angebotenen Leistungen der öffentlichen Organe.

Elektronisch angebotene Leistungen sollen den Nutzerinnen und Nutzern zentral zur Verfügung stehen. Solche Leistungen umfassen anfänglich Bewilligungen (Arbeitsbewilligungen, Bewilligungen im Gesundheitswesen oder im Bereich Taxi- und Limousinendienste), Steuererklärungen, elektronisch abgewickelte Einbürgerungsverfahren oder der selbstbestimmte Leistungsbezug durch Menschen mit Behinderung. Das Leistungsangebot der öffentlichen Organe, das zentral zugänglich gemacht wird, kann nicht in einem abschliessenden Katalog aufgelistet werden. Vielmehr ist davon auszugehen, dass das Angebot stetig ausgebaut wird und die öffentlichen Organe ihre Leistungen künftig vermehrt auch oder unter Umständen – gestützt auf entsprechende rechtliche Grundlagen – ausschliesslich elektronisch zur Verfügung stellen werden.

² Die Staatskanzlei betreibt hierzu einen Webzugang zu elektronisch angebotenen Leistungen der öffentlichen Organe.

Die Staatskanzlei betreibt einen Webzugang, der als zentraler Einstiegspunkt zu elektronisch angebotenen Leistungen der öffentlichen Organe dient («Zürikonto»). Die Inanspruchnahme von elektronisch angebotenen Leistungen über den Webzugang ist für die Nutzerinnen und Nutzer freiwillig. In der Regel bleiben die Leistungen auch analog zugänglich. Vorbehalten bleiben anderslautende Bestimmungen in der Fachgesetzgebung oder im Verfahrensrecht. Eine generelle Nutzungspflicht wäre auf formell-gesetzlicher Stufe einzuführen.

**Vorentwurf****Erläuterungen**

³ Öffentliche Organe können ihre elektronisch angebotenen Leistungen über den Webzugang zur Verfügung stellen.

Eine umfassende Pflicht der öffentlichen Organe, ihre elektronisch angebotenen Leistungen an den zentralen Zugang anzuschliessen, ist nicht vorgesehen. Vorbehalten bleiben allfällige Anforderungen des Regierungsrates an die Interoperabilität (siehe § 3 VE-Gesetz über digitale Basisdienste).

Inhalt

§ 11. Die Nutzerin oder der Nutzer kann über den Webzugang:

Die nicht abschliessende Aufzählung in § 11 VE-Gesetz über digitale Basisdienste verankert die wesentlichen Nutzungsmöglichkeiten des Webzugangs.

a. elektronische Verfahrenshandlungen nach dem Verwaltungsrechtspflegegesetz vom 24. Mai 1959 vornehmen,

Mit der Änderung vom 30. Oktober 2023 des VRG (Elektronische Verfahrenshandlungen) wird künftig der rechtsgültige elektronische Verkehr mit den Verwaltungsbehörden ermöglicht. § 4e Abs. 1 nVRG sieht vor, dass elektronische Verfahrenshandlungen «über den für die Verwaltungsbehörde massgeblichen Kanal erfolgen» (Satz 1). Zusätzlich zu den vom Bund anerkannten Zustellplattformen sind weitere elektronische Kanäle als massgebliche Kanäle für die elektronische Vornahme von Verfahrenshandlungen zulässig, wie namentlich der hier geregelte Zugang.

b. sich zum Abruf bereitstehende Anordnungen und Mitteilungen der öffentlichen Organe in einer Übersicht anzeigen lassen,

Die Nutzerin oder der Nutzer kann sich zum Abruf bereitstehende Anordnungen und Mitteilungen der Verwaltungsbehörden in einer Übersicht anzeigen lassen. Der Abruf der Anordnung oder der Mitteilung selbst erfolgt in der entsprechenden elektronisch angebotenen Leistung des öffentlichen Organs.

c. Statusänderungen in Geschäftsvorgängen einsehen sowie Benachrichtigungen hierzu einrichten und verwalten und

Über den Webzugang sollen Statusänderungen in den Geschäftsvorgängen ersichtlich sein. Nicht angezeigt werden die Einzelheiten des Geschäftsvorganges, also zum Beispiel die Ablehnung oder Annahme eines Bewilligungsgesuchs. Angezeigt wird im Webzugang, dass sich der Status im Geschäftsvorgang verändert hat. Die Benachrichtigungen enthalten somit keine Angaben über den Inhalt der zum Abruf bereitgestellten Mitteilung.

Im Webzugang sollen die Nutzerinnen und Nutzer entscheiden können, ob und falls ja, wie sie über Statusänderungen in den verschiedenen Geschäftsvorgängen benachrichtigt werden möchten. Diese Einstellung nehmen sie vor, indem sie die Benachrichtigung über die zur Verfügung gestellten Kanäle aktivieren oder deaktivieren. Als Benachrichtigungskanäle stehen E-Mail oder SMS zur Verfügung. Die Hinterlegung einer Mobiltelefonnummer muss von den Nutzenden manuell erfasst werden.

d. eine andere Nutzerin oder einen anderen Nutzer zur Vornahme von Handlungen im Rahmen einer elektronisch angebotenen Leistung berechtigen.

Mit einer technischen Berechtigung können Nutzerinnen und Nutzer im Rahmen von elektronisch angebotenen Leistungen Handlungen für die berechtigende (natürliche oder juristische) Person vornehmen. Technisch kann dies mit einem Tool zur Berechtigungserteilung und -verwaltung erfolgen. So kann z.B. die

**Vorentwurf****Erläuterungen**

Nutzerin oder der Nutzer in der Rolle der Organisationseigentümerin oder des Organisationseigentümers darüber entscheiden, wer innerhalb der Organisation welche Geschäftsfälle einer Leistung eines öffentlichen Organs bearbeiten darf. Die Einzelheiten, wer welche Aufgaben im Rahmen eines Geschäftsvorganges für jemand anderen, z.B. für ein Unternehmen, übernehmen darf, sind durch das zuständige öffentliche Organ festzulegen. Diese technischen Berechtigungen sind von den rechtlichen Voraussetzungen abzugrenzen. Ob eine Nutzerin oder ein Nutzer rechtlich überhaupt eine Aufgabe für eine andere, natürliche oder juristische Person vornehmen darf, richtet sich nach Massgabe der gesetzlichen Vorgaben, welche für die elektronisch angebotene Leistung einschlägig sind.

Anmeldung

§ 12. Die Anmeldung für die Nutzung des Webzugangs erfolgt über den Authentifizierungsdienst gemäss § 7. Für die Anmeldung beim Zugang ist eine elektronische Identifizierung über den Authentifizierungsdienst gemäss § 7 VE-Gesetz über digitale Basisdienste erforderlich. Mit der Anmeldung werden die betroffenen Personendaten mit dem Webzugang verbunden.

Datenbearbeitung

§ 13. ¹ Die Staatskanzlei:

Über den Webzugang können die Nutzerinnen und Nutzer zu den elektronisch angebotenen Leistungen gelangen. Die Datenbearbeitung im Rahmen des Webzugangs ist dabei rechtlich zu unterscheiden von der Datenbearbeitung, welche im Rahmen der einzelnen Leistungen der öffentlichen Organe in den Fachanwendungen stattfindet. Die Datenbearbeitung zwecks Leistungserbringung erfolgt durch die öffentlichen Organe auf Grundlage der Fachgesetzgebung und § 44 OG RR. Zur Sicherstellung der Funktionalität des Webzugangs ist in eingeschränktem Rahmen eine Datenbearbeitung auch im Webzugang erforderlich; die mit dem Gesetz über digitale Basisdienste zu schaffenden Rechtsgrundlagen beziehen sich auf diese Datenbearbeitung.

a. protokolliert die Anmeldungen der Nutzerinnen und Nutzer,

Für den sicheren Betrieb des Zugangs und die Nachvollziehbarkeit der Nutzung werden sämtliche Anmeldungen protokolliert. Eine Auswertung der Zugriffsdaten kann auf Seiten der öffentlichen Organe erforderlich werden, wenn beispielsweise der Verdacht auf eine unrechtmässige Nutzung besteht (siehe hierzu § 14 VE-Gesetz über digitale Basisdienste). Die Daten müssen daher für eine gewisse Zeitdauer aufbewahrt werden können. Auf Verordnungsstufe sind weitere Einzelheiten zu regeln, wie voraussichtlich die Einsichtnahme in die aufgezeichneten Daten und die Dauer der Speicherung.

**Vorentwurf****Erläuterungen**

b. bearbeitet Informationen im Webzugang, soweit dies zur Unterstützung der Nutzerinnen und Nutzer erforderlich ist.

Nutzerinnen und Nutzer sollen bei Bedarf Unterstützung erhalten, wenn beispielsweise eine Nutzerin oder ein Nutzer infolge einer von ihr oder ihm geänderten E-Mailadresse nicht mehr auf ihren oder seinen Webzugang zugreifen kann. Zu diesem Zweck ist vorausgesetzt, dass die Staatskanzlei als Betreiberin des Webzugangs auf die im Webzugang enthaltenen Daten zugreifen und sie bearbeiten kann.

Für Fragestellungen zu einem spezifischen Geschäftsvorgang ist das öffentliche Organ zuständig.

² Das öffentliche Organ kann zur Erbringung der elektronisch angebotenen Leistung die für die Identifizierung erforderlichen Personendaten gemäss § 8 Abs. 1 über den Webzugang anfordern.

Ist für die Erbringung einer elektronisch angebotenen Leistung die Identifizierung einer Nutzerin oder eines Nutzers erforderlich, kann das öffentliche Organ die hierfür erforderlichen Personendaten über den Webzugang anfordern. Zu beachten ist der datenschutzrechtliche Grundsatz der Verhältnismässigkeit, wonach eine Überidentifizierung nicht zulässig ist.

Sperrung des Webzugangs

§ 14. ¹ Bei Verdacht auf eine unrechtmässige Nutzung kann der Webzugang auf Verlangen der Nutzerin oder des Nutzers oder von Amtes wegen vorläufig gesperrt und damit für die Nutzerin oder den Nutzer unzugänglich gemacht werden.

Mit einer vorläufigen Sperrung werden folgende Zwecke verfolgt: Einerseits soll der Verursachung eines möglichen Schadens vorsorglich entgegengewirkt werden und andererseits die Möglichkeit geschaffen werden, notwendige Abklärungen vorzunehmen. Ein Verdacht auf unrechtmässige Nutzung genügt. Die Sperrung erfolgt auf Verlangen der nutzenden Person oder von Amtes wegen und hat zur Folge, dass der Webzugang nicht mehr genutzt werden kann, bis die notwendigen Abklärungen durch die Betreiberin des Zugangs erfolgt sind.

² Die Nutzerin oder der Nutzer wird über die Sperrung informiert und kann sich zur Sperrung äussern.

Die von der Sperrung betroffene Person wird über die Sperrung in Kenntnis gesetzt; so hat sie die Möglichkeit, darauf zu reagieren.

³ In begründeten Fällen kann der Webzugang für die Nutzerin oder den Nutzer gelöscht werden.

Sollte sich der Verdacht, der zu einer Sperrung führte, als begründet erweisen, kann der Webzugang für die Nutzerin oder den Nutzer gelöscht werden. Die in den elektronischen Leistungen gehaltenen Daten der Nutzerin oder des Nutzers sind von einer Löschung des Webzugangs nicht betroffen.

Löschung des Webzugangs

§ 15. ¹ Die Löschung des Webzugangs für die Nutzerin oder den Nutzer und damit die Vernichtung der darin vorhandenen Daten und die Entziehung der Berechtigungen der Nutzerin oder des Nutzers kann von der Nutzerin oder dem Nutzer verlangt werden, wenn:

Eine Person soll grundsätzlich die Möglichkeit haben, auf eigenes Verlangen hin den Webzugang löschen zu lassen. Mit der Löschung des Webzugangs werden die darin enthaltenen Daten vernichtet und vorhandene (technische) Berechtigungen der Nutzerin oder des Nutzers entzogen. Nach der Löschung kann sich die

**Vorentwurf****Erläuterungen**

Nutzerin oder der Nutzer nicht mehr im Webzugang anmelden. Die im Rahmen der elektronisch angebotenen Leistung erfassten Informationen sind von der Löschung des Webzugangs nicht betroffen.

Die Löschung des Webzugangs ist unter den in lit. a–c aufgeführten Voraussetzungen zulässig.

- a. alle über den Webzugang eingeleiteten Geschäftsfälle abgeschlossen sind, Die Löschung des Webzugangs setzt voraus, dass alle über ihn eingeleiteten Geschäftsfälle abgeschlossen sind, dies umfasst insbesondere auch die über den Webzugang eingeleiteten Verfahrenshandlungen nach VRG.
- b. alle über den Webzugang bereitgestellten oder sich in technischer Bereitstellung befindlichen Mitteilungen abgerufen worden sind und Mit dieser Voraussetzung soll verhindert werden, dass Mitteilungen eines öffentlichen Organs an die Nutzerin oder den Nutzer nicht zur Kenntnis genommen werden.
- c. der Webzugang nicht gesperrt ist. Damit eine Sperrung des Webzugangs nicht durch die Löschung des alten und die Erstellung eines neuen Webzugangs umgangen werden kann, kann ein gesperrter Webzugang nicht gelöscht werden. Zur Sperrung siehe § 14 VE-Gesetz über digitale Basisdienste .

² Ein über fünf Jahre ungenutzter Webzugang sowie die darin enthaltenen Daten der Nutzerin oder des Nutzers werden ohne Einhaltung der Voraussetzungen gemäss Abs. 1 vernichtet. Die Löschung eines verwaisten Webzugangs ist nicht an die Voraussetzungen von Abs. 1 geknüpft. Einzig die Zeitdauer von fünf Jahren ohne Nutzung des Webzugangs ist für die Löschung massgebend.

Kosten und Gebühren

§ 16. ¹ Der Kanton trägt die Kosten für den Aufbau, den Betrieb, die Unterstützung und die Weiterentwicklung des Webzugangs. Der Kanton trägt die Kosten für den Aufbau, den Betrieb und die Unterstützung (Support) sowie die Weiterentwicklung des Webzugangs. Die Weiterverrechnung innerhalb der Zentralverwaltung richtet sich nach den für die öffentlichen Organe des Kantons festgelegten Grundsätzen zur IKT-Verrechnung (vgl. RRB Nr. 1233/2020).

² Der Regierungsrat kann die übrigen öffentlichen Organe zu einer Kostenbeteiligung verpflichten, wenn sie ihre elektronisch angebotene Leistung über den Webzugang verfügbar machen. Die Höhe der Kostenbeteiligung richtet sich nach der Art und dem Umfang der Leistung. Der Regierungsrat regelt die Einzelheiten. Für alle öffentlichen Organe, die nicht Teil der Kantonsverwaltung sind, ist eine separate Rechtsgrundlage für deren Kostenbeteiligung erforderlich. Wird eine elektronisch angebotene Leistung der übrigen öffentlichen Organe über den Zugang erreichbar, kann eine Beteiligung an den gemäss § 16 Abs. 1 VE-Gesetz über digitale Basisdienste anfallenden Kosten vorgesehen werden. Die Einzelheiten werden durch den Regierungsrat in einer Verordnung geregelt.

³ Die Nutzung des Webzugangs ist für die Nutzerinnen und Nutzer kostenlos. Die Nutzung des Webzugangs ist für die Nutzerinnen und Nutzer kostenlos. Für die Leistungen, welche an den Webzugang angeschlossen sind, darf ein öffentliches Organ weiterhin Gebühren auf Grundlage der Fachgesetzgebung sowie gemäss der Gebührenordnung für die Verwaltungsbehörden (LS 682) erheben.



C. Digitaler Arbeitsplatz

Vorbemerkungen

Im Rahmen seiner Strategie zu Informations- und Kommunikationstechnologien (IKT-Strategie, vgl. RRB Nr. 383/2018) hat der Regierungsrat entschieden, die kantonale Verwaltung mit einem neuen, digitalen Arbeitsplatz (DAP) auszurüsten. Eine vergleichbare Entwicklung zeichnet sich auch in den Gemeinden und in den dezentralen Verwaltungseinheiten wie den Spitälern und den Hochschulen ab. Mittlerweile haben zahlreiche öffentliche Organe auf kantonaler und kommunaler Ebene einen DAP eingeführt oder prüfen dessen Einführung.

Zu ihrer Aufgabenerfüllung und für die Erbringung von Leistungen sind die Mitarbeitenden der öffentlichen Organe auf zeitgemässe digitale Arbeitsmittel angewiesen. Der DAP erhöht die Mobilität, unterstützt die Anforderungen an modernes, flexibles Arbeiten, entspricht den heutigen Sicherheitsstandards und vereinfacht den Betrieb. Verwendet werden Software-Anwendungen wie z.B. die Anwendungen von Microsoft 365 (Word, Excel, PowerPoint, Outlook, Teams, OneDrive usw.; nachfolgend M365). Nicht zum DAP gehören Fachanwendungen (z.B. eine Software für die Geschäftsverwaltung). Es ist zu erwarten, dass die Software-Anwendungen häufig über den externen Anbieter Microsoft bezogen und mindestens teilweise über dessen Cloud abgewickelt werden. Die Bestimmungen zum DAP sind aber technologie- und anbieterneutral und umfassen auch allfällige Anwendungen von anderen Anbietern (nachfolgend die «Cloud-Anbieterin»).

Heute wird der Einsatz von cloudbasierten Anwendungen durch das IDG, die IDV, die IVSV und für kantonale Organe zudem durch das Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1991 (LS 172.71) erfasst. Die Informationsbearbeitung durch Dritte (auch «Auftragsdatenbearbeitung» oder «Bearbeitung im Auftrag» genannt) ist gemäss § 6 Abs. 1 IDG bzw. § 9 Abs. 1 E-IDG (gemäss Vorlage 5923) zulässig und rechtmässig, wenn keine gesetzliche oder vertragliche Bestimmung der Auslagerung entgegensteht. Die Verantwortung für den Umgang mit Informationen verbleibt trotz der Übertragung der Informationsbearbeitung beim öffentlichen Organ (§ 6 Abs. 2 IDG sowie § 9 Abs. 2 Satz 1 E-IDG). Gemäss dem im heutigen § 6 Abs. 2 IDG nicht enthaltenen Satz 2 von § 9 Abs. 2 E-IDG hat das öffentliche Organ insbesondere sicherzustellen, dass die Dritten (d.h. die Cloud-Anbieterinnen) die Informationssicherheit gewährleisten, Informationen nur so bearbeiten, wie es das öffentliche Organ selbst tun darf und die Bearbeitung erst nach Bewilligung durch das öffentliche Organ an weitere Dritte übertragen wird. § 19 IDG bzw. § 36 E-IDG regeln die grenzüberschreitende Bekanntgabe von Personendaten an Empfängerinnen und Empfänger, die dem Europarats-Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten nicht unterstehen. In dieser Konstellation darf das öffentliche Organ Personendaten gemäss der Regelung im E-IDG gemäss Vorlage 5923 nur dann

**Vorentwurf****Erläuterungen**

bekanntgeben, wenn (a) eine gesetzliche Grundlage dies erlaubt und dies dem Schutz der Interessen der betroffenen Person oder überwiegenden öffentlichen Interessen dient, (b) im Empfängerstaat ein angemessener Schutz für die Datenbearbeitung gewährleistet ist oder (c) das öffentliche Organ mit den Empfängerinnen und Empfängern angemessene Sicherheitsvorkehrungen vereinbart hat.

Die umfangreiche Auslagerung von Daten des Staates in eine von einer ausländischen Cloud-Anbieterin betriebene und kontrollierte Cloud-Infrastruktur bringt verschiedene, vielfach noch offene Rechtsfragen mit sich:

- Einerseits wirft die Auslagerung Fragen des Grundrechtsschutzes auf, weil eine Auslagerung in die Cloud ein schwerer Eingriff in den verfassungsrechtlichen Persönlichkeitsschutz (Art. 13 Abs. 2 BV) darstellen kann. Mit der Auslagerung ist ein Kontrollverlust gegenüber der Cloud-Anbieterin verbunden, weil die Nachvollziehbarkeit der Datenbearbeitung und die Durchsetzung von Kontrollrechten der Betroffenen erschwert werden. Zudem resultiert ein Kontrollverlust gegenüber ausländischen Behörden, wenn diese aufgrund der ausländischen Rechtslage (vgl. z.B. den US CLOUD Act bzw. den Stored Communications Act [sog. lawful access]) die Cloud-Anbieterin zur Herausgabe von in der Cloud gespeicherten Daten verpflichten können. Diese Problematik besteht unabhängig von der Wahrscheinlichkeit eines Datenzugriffs durch ausländische Behörden und dem Standort der Server.
- Andererseits gilt es, die datenschutzrechtlichen Bestimmungen, die Vorgaben zum Schutz der Informationssicherheit der jeweiligen Organisationseinheit sowie des Amtsgeheimnisses zu beachten (Art. 320 Schweizerisches Strafgesetzbuch, SR 311.0) und sensible Informationen durch besondere Massnahmen zu schützen (§ 7 IDG).

Im Kanton Zürich ist die Nutzung von M365 für den DAP in der kantonalen Verwaltung grundsätzlich vorgesehen (RRB Nr. 542/2022, Dispositiv I). Der Beschluss gilt für alle der IKT-Strategie unterstehenden Organisationseinheiten¹ sowie für die Kantonspolizei. Die Direktionen und die Staatskanzlei sind beauftragt, zu beurteilen, ob organisationsspezifische Regelungen notwendig sind und im Bedarfsfall solche zu erlassen (RRB Nr. 542/2022, Dispositiv III). Die Finanzdirektion erliess am 27. Januar 2023 für die Kantonsverwaltung die Allgemeine Nutzungsrichtlinie Microsoft 365. Diese konkretisiert Grundsätze und Regeln der Datenbearbeitung im DAP.

¹ Der Geltungsbereich der IKT-Strategie umfasst die Direktionen des Regierungsrates und die Staatskanzlei sowie die unselbstständigen Anstalten. Der Regierungsrat kann Ausnahmen vom Geltungsbereich bewilligen. Jede Organisation (z. B. selbstständige Anstalten), die an Lösungen der kantonalen Verwaltung in spezifischen Bereichen partizipiert, ist verpflichtet, sich in diesem spezifischen Bereich an die Vorgaben der IKT-Strategie zu halten (siehe Ziff. 3 IKT-Strategie).



Für die Gemeinden bestehen noch keine entsprechenden kantonalrechtlichen Vorgaben. Der Bund und andere Kantone bzw. ausserkantonale Gemeinden handhaben die Nutzung von Cloud-Diensten, insbesondere von M365, unterschiedlich. In der Lehre zeichnet sich noch keine einheitliche Meinung ab. Ein im Auftrag der Zusammenarbeitsorganisation egovpartner erstelltes und am 6. Juli 2023 erstattetes Gutachten bestätigt den in der Allgemeinen Nutzungsrichtlinie Microsoft 365 verfolgten Ansatz der kantonalen Verwaltung auch für die Zürcher Gemeinden. Gleichzeitig empfiehlt das Gutachten, die Bestimmungen über die Datenbearbeitung mittels M365 in gesetzlicher Form zu verankern (Markus Schefer/Philipp Glass, Gutachten zum grundrechtskonformen Einsatz von M365 durch die Gemeinden im Kanton Zürich vom 6. Juli 2023 zuhanden von egovpartner).

Gestützt auf die obigen rechtlichen Überlegungen und aufgrund der Rückmeldungen zu diesem Rechtsetzungsvorhaben soll mit § 17 VE-Gesetz über digitale Basisdienste eine gesetzliche Grundlage für cloudbasierte Anwendungen im Rahmen des DAP geschaffen werden. Nicht Gegenstand der Bestimmung bilden cloudbasierte Dienste, die ausserhalb des DAP verwendet werden (z.B. im Rahmen von Fachanwendungen), sowie lokale Anwendungen (z.B. die Office-365-Apps wie Word, sofern sie lokal genutzt werden). Die Regelung von § 17 VE-Gesetz über digitale Basisdienste beinhaltet auch die Bearbeitung von Personendaten und Informationen, welche aus einer Fachanwendung stammen, im Rahmen der cloudbasierten Applikationen des DAP. So dürfen die Mitarbeitenden der öffentlichen Organe z.B. einen cloudbasierten E-Mail-Dienst nutzen, um miteinander zu kommunizieren, und dabei Personendaten und Informationen aus Fachanwendungen wie z.B. der Geschäftsverwaltungssoftware bearbeiten. § 17 VE-Gesetz über digitale Basisdienste stellt dabei für unterschiedliche Kategorien von Personendaten und Informationen unterschiedlich strenge Anforderungen an die Verschlüsselung.

Die Bestimmung zum DAP richtet sich an öffentliche Organe, welche cloudbasierte Anwendungen im Rahmen des DAP nutzen wollen. Ob und bis zu welchem Grad sie Cloud-Dienste nutzen wollen, liegt in ihrer gegebenenfalls bestehenden Organisationsautonomie; es ist ohne Weiteres zulässig, wenn ein öffentliches Organ z.B. darauf verzichtet, besondere Personendaten in der Cloud zu bearbeiten.

Informationsbearbeitung durch Dritte im Rahmen des digitalen Arbeitsplatzes

§ 17. ¹ Das öffentliche Organ kann die Bearbeitung von Informationen in Anwendungen des digitalen Arbeitsplatzes an Anbieterinnen von cloudbasierten § 17 Abs. 1 VE-Gesetz über digitale Basisdienste bildet die gesetzliche Grundlage dafür, dass das öffentliche Organ, welches im Rahmen des DAP cloudbasierte Anwendungen nutzen möchte, die Bearbeitung von Informationen an die Cloud-Anbieterin zur cloudbasierten Bearbeitung übertragen kann. Die Bestimmung



Vorentwurf

Erläuterungen

Informatikdienstleistungen übertragen, wenn sich deren Rechenzentren in der Schweiz oder in der Europäischen Union befinden, und wenn:

konkretisiert und ergänzt die Vorgaben in § 6 IDG bzw. § 9 E-IDG im Hinblick auf die cloudbasierten Anwendungen des DAP.

Zunächst hält § 17 Abs. 1 VE-Gesetz über digitale Basisdienste generell fest, dass sich der Standort der Server auf dem Gebiet der Schweiz oder der Europäischen Union befinden muss. Ein Zugriff auf die Daten durch einen Drittstaat ist damit nicht ausgeschlossen. Allerdings kann zumindest eine physische Beschlagnahmung der Server unter Umgehung der Rechtshilfe verhindert werden.

Sodann nimmt die Bestimmung eine Zweiteilung vor in (1) besondere Personendaten und vertrauliche sowie der Geheimhaltung unterliegende Informationen (§ 17 Abs. 1 lit. a VE-Gesetz über digitale Basisdienste) und (2) Informationen, die geschäftlich als «öffentlich» oder «intern» klassifiziert sind, sowie «normale» (d.h. nicht besondere) Personen- und Sachdaten (§ 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste):

- *Kategorie 1 (lit. a):* Bei Informationen und Personendaten der Kategorie 1 stehen rechtliche Bestimmungen der Übertragung der Informationsbearbeitung an eine Cloud-Anbieterin an sich entgegen (§ 6 Abs. 1 IDG und § 9 Abs. 1 E-IDG; vgl. die Erläuterungen zu § 17 Abs. 1 lit. a VE-Gesetz über digitale Basisdienste). Zulässig ist eine Übertragung bei solchen Informationen nur dann, wenn sie auch gegenüber der Cloud-Anbieterin wirksam verschlüsselt sind; liegt das Schlüsselmanagement hingegen bei der Cloud-Anbieterin oder hat diese anderweitig Zugriff auf die Schlüssel, besteht keine wirksame Verschlüsselung. Weil eine solche Verschlüsselung die Kenntnisnahme durch die Cloud-Anbieterin oder durch einen ausländischen Staat unterbindet, ist die Übertragung an eine Cloud-Anbieterin dennoch zulässig (vgl. auch Dominika Blonski, Cloud – alles Risiko? Rechtliche Vorgaben für die Auslagerung von Datenbearbeitungen in die Cloud, SJZ 2023, S. 993 ff., 997).
- *Kategorie 2 (lit. b):* Bei Informationen und Personendaten der Kategorie 2 soll eine Übertragung der Informationsbearbeitung an eine Cloud-Anbieterin demgegenüber grundsätzlich zulässig sein. Auch solche Informationen sollten verschlüsselt werden; allerdings genügen insofern weniger strenge Vorgaben, als die Verschlüsselung nicht auch gegenüber der Cloud-Anbieterin wirksam sein muss bzw. ein Schlüsselmanagement durch die Cloud-Anbieterin (und damit auch ein einseitiger Zugriff durch die Cloud-Anbieterin) möglich bleibt. Das öffentliche Organ muss gemäss § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste aber alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen zur Minimierung des Risikos einer Bekanntgabe treffen und das verbleibende Restrisiko muss als vertretbar erscheinen (vgl. die Erläuterungen zu § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste). Wenn ausländische Behörden – z.B. der USA aufgrund des US CLOUD Act – auf diese Daten zugreifen, erfolgt eine grenzüberschreitende Bekanntgabe im Sinne von § 19 IDG bzw. § 36 E-

**Vorentwurf****Erläuterungen**

IDG. Mit § 17 Abs. 1 VE-Gesetz über digitale Basisdienste wird die gesetzliche Grundlage für eine solche Bekanntgabe geschaffen, die gemäss § 19 lit. b IDG bzw. § 36 lit. a E-IDG erforderlich ist, wenn das Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten nicht gilt.

Mittels einer differenzierten Regelung sollen die genannten cloudbasierten Anwendungen in einer möglichst grundrechtskonformen Weise genutzt werden können. Die Regelung nimmt die heute auf Kantonsebene bestehende Regelung der Allgemeinen Nutzungsrichtlinie auf formell-gesetzlicher Ebene auf.

- a. das öffentliche Organ besondere Personendaten sowie vertrauliche oder der Geheimhaltung unterliegende Informationen auch gegenüber der Cloud-Anbieterin wirksam verschlüsselt, so dass die Cloud-Anbieterin darauf nicht ohne Mitwirkung des öffentlichen Organs zugreifen kann und

Die Bearbeitung von besonderen Personendaten sowie von Informationen, die vertraulich sind oder der Geheimhaltung unterliegen, soll grundsätzlich mittels lokaler Anwendungen stattfinden. Erfasst sind die folgenden Informationen:

- *Besondere Personendaten:* Der Begriff der besonderen Personendaten ist gleich auszulegen wie in § 3 Abs. 4 IDG bzw. § 5 Abs. 4 E-IDG. Dazu gehören namentlich Personendaten, die durch besondere Amtsgeheimnisse geschützt sind. Besondere Personendaten sind etwa Informationen über die Inanspruchnahme von Sozialhilfeleistungen (§ 3 Abs. 4 lit. a Ziff. 3 E-IDG). Diese Informationen sind durch das Sozialhilfegeheimnis geschützt (§ 47 Sozialhilfegesetz, LS 851.1).
- *Vertrauliche und der Geheimhaltung unterliegende Informationen:* Die Umschreibung umfasst einerseits Informationen, die geschäftlich als «vertraulich» oder «geheim» klassifiziert sind. Andererseits sind Informationen erfasst, welche aufgrund eines besonderen (d.h. nicht bloss des allgemeinen) Amtsgeheimnisses oder eines Berufsgeheimnisses der Geheimhaltung unterliegen. Teils handelt es sich dabei um besondere Personendaten (so z.B. Personendaten, die durch das Sozialhilfegeheimnis geschützt sind [vgl. § 3 Abs. 4 lit. a Ziff. 3 IDG]).

Die vorgeschlagene Regelung schliesst es nicht aus, dass besondere Personendaten sowie vertrauliche und der Geheimhaltung unterliegende Informationen mittels cloudbasierter Anwendungen bearbeitet werden. Allerdings muss das öffentliche Organe diese Informationen gemäss der vorgeschlagenen Lösung *wirksam* verschlüsseln. Wirksam ist eine Verschlüsselung, wenn sie auch gegenüber der Cloud-Anbieterin besteht, was etwa bei der sog. Double Key Encryption (DKE) der Fall ist. Die Verschlüsselung muss es ausschliessen, dass die Cloud-Anbieterin ohne Mitwirkung des öffentlichen Organs Kenntnis von den Informationen erlangen kann. Dies soll eine Kenntnisnahme unter Umgehung der Regeln der internationalen Rechtshilfe sowie ohne Gewährleistung von Kontroll- und Verfahrensrechten verunmöglichen. Erforderlich ist damit, dass die Schlüsselhoheit beim öffentlichen Organ verbleibt und somit nur ein einseitiger Zugriff durch das öffentliche

**Vorentwurf****Erläuterungen**

Organ möglich ist; das öffentliche Organ darf eine Auftragnehmerin oder einen Auftragnehmer mit der Verwaltung der Schlüssel beauftragen (sog. Cloud Access Security Broker [CASB]), sofern es sich dabei nicht um die Cloud-Anbieterin handelt und es ausgeschlossen ist, dass die Cloud-Anbieterin oder Dritte mit möglichem Zugriff auf die Daten (insbesondere eine ausländische Behörde) die Schlüssel von der Auftragnehmerin bzw. vom Auftragnehmer herausverlangen können. Verschlüsselt eine Cloud-Anbieterin die Daten selbst und/oder hat sie Zugang zu den Schlüsseln (im Fall von Microsoft etwa der Microsoft-Managed-Key [MMK]), genügt dies *nicht* für die in § 17 Abs. 1 lit. a VE-Gesetz über digitale Basisdienste genannten Informationen.

- b. das öffentliche Organ die sonstigen Informationen durch alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen schützt und das verbleibende Risiko einer Bekanntgabe insbesondere angesichts der Bedeutung der Informationen, des Zwecks und der Art und Weise ihrer Bearbeitung sowie der Grundrechte der betroffenen Personen vertretbar ist.

Ohne Verschlüsselung gegenüber der Cloud-Anbieterin zulässig bleibt die Bearbeitung von Informationen gemäss § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste. Diese Bestimmung betrifft alle von § 17 Abs. 1 lit. a VE-Gesetz über digitale Basisdienste nicht erfassten Informationen, d.h. die «normalen» Personendaten sowie Informationen, die geschäftlich als «öffentlich» oder «intern» klassifiziert sind und nicht einem besonderen Amtsgeheimnis oder dem Berufsgeheimnis unterstehen. Bei diesen Informationen gilt insofern ein risikobasierter Ansatz, als das öffentliche Organ gemäss § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen zur Minimierung des Risikos einer Bekanntgabe treffen muss und das verbleibende Restrisiko als vertretbar erscheint.

Was die zu treffenden technischen, organisatorischen und vertraglichen Massnahmen angeht, ergeben sich die Anforderungen aus der Datenschutzgesetzgebung (insbesondere § 7 IDG) und internen Umsetzungsvorgaben, die im Einzelfall – je nach Sensitivität der betroffenen Informationen – unterschiedlich streng sein können. In technischer Hinsicht genügt eine Verschlüsselung. Gemeinsamer Zweck der entsprechenden Massnahmen ist letztlich, dass das öffentliche Organ seine Verantwortung (§ 6 Abs. 2 IDG bzw. § 9 Abs. 2 E-IDG) auch tatsächlich wahrnehmen kann.

Sodann erwähnt die Bestimmung das Restrisiko, welches im Rahmen einer Risikoanalyse zu beurteilen ist. In einem ersten Schritt ist dessen Eintretenswahrscheinlichkeit abzuschätzen. In einem zweiten Schritt ist das Restrisiko als vertretbar oder nicht vertretbar zu bewerten; die Bestimmung zählt in nicht abschliessender Weise Aspekte auf, die dabei miteinzubeziehen sind:

- Die Bestimmung nimmt Bezug auf die Bedeutung der Information und gibt damit vor, dass die Abwägung stets mit Blick auf die konkreten Informationen vorgenommen werden muss. Sie kann für verschiedene Informationen unterschiedlich ausfallen, z.B. je nachdem wie sensitiv die entsprechenden

**Vorentwurf****Erläuterungen**

Informationen sind. Zu berücksichtigen ist auch, dass dieselbe Information in unterschiedlichen Zusammenhängen und je nach Verknüpfung mit anderen Informationen unterschiedlich sensitiv sein kann.

- Zu berücksichtigen sind weiter der Bearbeitungszweck, d.h. die öffentliche Aufgabe, zu deren Erfüllung die Informationen bearbeitet werden, und die Art und Weise der Bearbeitung. Bei der Art und Weise des Bearbeitens relevant sind beispielsweise die Intensität (Anzahl Datensätze, Anzahl betroffene Personen) und die Dauer der Bearbeitung, die Speicherung von Daten, der Einsatz von Technologien der Künstlichen Intelligenz usw.
- Die Nutzung von Cloud-Diensten wirkt sich auf die Grundrechte derjenigen Personen aus, welche die übertragenen Informationen bzw. Personendaten betreffen, weil sie mit einem rechtlichen und faktischen Kontrollverlust verbunden ist. Dieser Kontrollverlust ist erhöht, wenn die Cloud-Anbieterin nicht nur dem schweizerischen Recht unterstehen. Wenn die Cloud-Anbieterin ausländischen Regulierungen (z.B. dem US CLOUD Act) untersteht, besteht ein Risiko, dass ein Drittstaat auf die Informationen zugreift und gemäss dem ausländischen Recht keine bzw. im Vergleich zum schweizerischen Recht nur eingeschränkte Rechtsbehelfe gegen diesen Zugriff bestehen. Auch das Durchführen von Kontrollen wird erschwert. Somit führt die Übertragung der Bearbeitung von Informationen an eine Cloud-Anbieterin zu rechtlichen und faktischen Einschränkungen der Kontrollrechte über die Bearbeitung sowie zum Risiko der Datenbekanntgabe ins Ausland.

Für die Nutzung von Cloud-Diensten spricht demgegenüber regelmässig der Aspekt der Effizienz der Aufgabenerfüllung. Die Einführung von cloudbasierten Anwendungen ermöglicht eine flexible und skalierbare Arbeitsinfrastruktur auf dem Stand der Technik. Dabei wird auch eine Optimierung der Verwaltungsabläufe und eine Steigerung der Kosteneffizienz erwartet. Ferner wird davon ausgegangen, dass die Nutzung von externen Cloud-Diensten die Sicherheit erhöht, weil die Cloud-Anbieterinnen Sicherheitsvorkehrungen treffen, welche die Sicherheitsmassnahmen der Nutzerinnen und Nutzer beim lokalen Gebrauch von Anwendungen übersteigen. Umgekehrt ist mit jeder Übertragung immer ein Risiko für die Informationssicherheit verbunden. Dies gilt etwa mit Blick auf das Risiko der falschen Handhabung der Cloud-Services durch die Nutzenden beim öffentlichen Organ; wobei dieses Risiko umgekehrt freilich auch beim lokalen Gebrauch bzw. beim Gebrauch von IT-Anwendungen insgesamt besteht.

**Vorentwurf****Erläuterungen**

² Im Übrigen gelten die Bestimmungen des Gesetzes über die Information und den Datenschutz.

Der VE-Gesetz über digitale Basisdienste konkretisiert und ergänzt die Bestimmungen zur Informationsbearbeitung im Auftrag (§ 6 IDG bzw. § 9 E-IDG), zur Informationssicherheit (§ 7 IDG bzw. § 10 E-IDG) sowie zur Datenschutz-Folgenabschätzung (§ 10 IDG bzw. § 32 E-IDG). Er bildet zudem im Falle der Informationen gemäss § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste eine gesetzliche Grundlage im Sinne von § 19 lit. b IDG bzw. § 36 lit. a E-IDG. Die Bestimmungen des IDG bzw. E-IDG und des VE-Gesetz über digitale Basisdienste kommen kumulativ zur Anwendung, was mit dem deklaratorischen Verweis in § 17 Abs. 2 VE-Gesetz über digitale Basisdienste klargestellt wird.

5. Abschnitt: Schluss- und Übergangsbestimmungen*Änderungen bisherigen Rechts*

I. Das Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (LS 172.71) wird wie folgt geändert:

[neu] § 3. ² Für Auslagerungen im Rahmen der Anwendungen des digitalen Arbeitsplatzes an Anbieterinnen von cloudbasierten Informatikdienstleistungen gelten zudem die Bestimmungen des Gesetzes über digitale Basisdienste.

Für Auslagerungen durch kantonale öffentliche Organe gilt das Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (LS 172.71). Mit dem Verweis soll klargestellt werden, dass für die spezifischen Fragen der Cloud-Nutzung im Rahmen der Anwendungen des DAP die spezifischen Bestimmungen des Gesetzes über digitale Basisdienste gelten.

[bisheriger § 3 Abs. 2 wird zu § 3 Abs. 3]

II. Dieses Gesetz untersteht dem fakultativen Referendum.