Kanton Zürich
Staatskanzlei

Zusammenstellung des Vernehmlassungsergebnisses

17. Juni 2024
Referenz: SKZH.9070

Vorentwurf-Gesetz über digitale Basisdienste (Neuerlass)

A. Gegenstand der Vernehmlassung

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.

Grundlage für die Umsetzung der Strategie Digitale Verwaltung bilden die 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 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). Digitale Basisdienste bilden Gegenstand des Handlungsfelds 2 der SI Recht. Um digitale Basisdienste rechtssicher einsetzen zu können, bedarf es eines sachgemäss ausgestalteten Rechtsrahmens (siehe 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 Nr. 1230/2023 hat der Regierungsrat dem Normkonzept zugestimmt und die Staatskanzlei beauftragt, ihm einen Entwurf zu einem Gesetz über digitale Basisdienste im Sinne des Normkonzepts zu unterbreiten. Das Vorhaben setzt sowohl die skizzierten rechtlichen Bestrebungen im Rahmen der SI Recht als auch die vorgenannte Motion um.

Mit Regierungsratsbeschluss vom 7. Februar 2024 (RRB Nr. 147/2024) ist die Staatskanzlei ermächtigt worden, das Vernehmlassungsverfahren durchzuführen. In die Vernehmlassung geschickt wurde der *Vorentwurf mit erläuterndem Bericht des Gesetzes über digitale Basisdienste* vom 31. Januar 2024 (nachfolgend VE-Gesetz über digitale Basisdienste). Der Vorentwurf besteht aus einem Neuerlass sowie einer Nebenänderung des Gesetzes über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (LS 172.71).

B. Vernehmlassungsverfahren

Die Vernehmlassung und das Mitberichtsverfahren bei den Direktionen erfolgte vom 13. Februar bis 13. Mai 2024. Neben der Einladung per E-Mail an die potenziell in ihren Interessen Betroffenen wurde die Vernehmlassung auch per Mitteilung des Regierungsrates vom 13. Februar 2024 angekündigt. Die vollständigen Vernehmlassungsunterlagen wurden zeitgleich auf der Webseite des Kantons (https://www.zh.ch/de/politik-staat/gesetze-beschluesse/vernehmlassungen.html) veröffentlicht.

Zur Vernehmlassung eingeladen wurden:

Kantonsrat und im Kantonsrat vertretene Parteien

- Geschäftsleitung des Kantonsrats
- Parlamentsdienste
- Alternative Liste (AL)
- Christlich-Soziale Partei (CSP)
- Die Mitte
- Eidgenössisch-Demokratische Union (EDU)
- Evangelische Volkspartei (EVP)
- Freisinnig-Demokratische Partei (FDP Kanton Zürich)
- Grüne Partei (GRÜNE Kanton Zürich)
- Grünliberale Partei (GLP)
- Schweizerische Volkspartei (SVP Kanton Zürich)
- Sozialdemokratische Partei (SP Kanton Zürich)

Vertreterinnen und Vertreter aus der Wirtschaft und Zivilgesellschaft

- Behindertenkonferenz Kanton Zürich
- Demokratische Jurist*Innen Zürich (DJZ)
- Pro Juventute
- Pro Senectute
- Swico
- swissICT (Verband ICT-Werkplatz Schweiz)
- Treuhand Suisse (Sektion Zürich)

- Zürcher Anwaltsverband
- Zürcher Handelskammer (ZHK)

Verwaltung
- Direktionen des Regierungsrates (Mitbericht)

Gemeinden und ihre Organisationen
- Politische Gemeinden des Kantons Zürich
- Verband der Gemeindepräsidien des Kantons Zürich (GPV)
- Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute (VZGV)
- Verband Zürcher Schulpräsidien (VZS)
- Vereinigung Personal Zürcherischer Schulverwaltungen (VPZS)

Selbständige Anstalten, Körperschaften, öffentliche Stiftungen
- BVG- und Stiftungsaufsicht des Kantons Zürich
- Elektrizitätswerke des Kantons Zürich
- Gebäudeversicherung Kanton Zürich GVZ
- Sozialversicherungsanstalt Zürich SVA
- Integrierte Psychiatrie Winterthur – Zürcher Unterland
- Kantonsspital Winterthur
- Psychiatrische Universitätsklinik Zürich
- Universitätsspital Zürich (USZ)
- Pädagogische Hochschule Zürich (PHZH)
- Universität Zürich (UZH)
- Zentralbibliothek Zürich
- Zentrum für Gehör und Sprache
- Zürcher Hochschule der Künste
- Zürcher Hochschule für Angewandte Wissenschaften
- Christkatholische Kirchgemeinde Zürich
- Evangelisch-reformierte Landeskirche des Kantons Zürich
- Katholische Kirche im Kanton Zürich

Gerichte
- Verwaltungskommission der obersten kantonalen Gerichte

Verwaltungsunabhängige kantonale Stellen
- Datenschutzbeauftragte des Kantons Zürich (DSB)
- Ombudsmann des Kantons Zürich

Eingegangen sind Vernehmlassungsantworten von:

Kantonsrat und im Kantonsrat vertretenen Parteien
- FDP Kanton Zürich
- GRÜNE Kanton Zürich
- SP Kanton Zürich
- SVP Kanton Zürich

Vertreterinnen und Vertreter aus der Wirtschaft und Zivilgesellschaft
- asut (Schweizerischer Verband der Telekommunikation)
- DJZ
- Digitale Gesellschaft
- swissICT (Verband ICT-Werkplatz Schweiz)
- ZHK

Weitere
- Privatperson A
- Zwei private Unternehmen (Unternehmen B, Unternehmen C)

Verwaltung
- Direktionen des Regierungsrates (Mitbericht)

Gemeinden und ihre Organisationen
- Politische Gemeinden des Kantons Zürich
    - Gemeinde Dägerlen
    - Stadt Dietikon
    - Gemeinde Dietlikon
    - Gemeinde Eglisau
    - Gemeinde Embrach
    - Gemeinde Fällanden
    - Gemeinde Gossau
    - Gemeinde Hausen am Albis
    - Gemeinde Hinwil
    - Gemeinde Hochfelden
    - Gemeinde Höri
    - Gemeinde Langnau am Albis
    - Gemeinde Meilen
    - Gemeinde Niederweningen
    - Gemeinde Oberglatt
    - Gemeinde Pfäffikon
    - Gemeinde Pfungen
    - Gemeinde Rifferswil
    - Gemeinde Schlatt
    - Gemeinde Stallikon
    - Stadt Uster
    - Gemeinde Wangen-Brüttisellen
    - Stadt Wetzikon
    - Gemeinde Winkel
    - Stadt Winterthur
    - Gemeinde Zell
    - Gemeinde Zumikon
    - Stadt Zürich
- GPV
- VZGV
- VZS
- VPZS

Selbständige Anstalten, Körperschaften, öffentliche Stiftungen

- GVZ
- USZ
- PHZH
- UZH
- Evangelisch-reformierte Landeskirche des Kantons Zürich
- Katholische Kirche im Kanton Zürich

Verwaltungsunabhängige kantonale Stellen

- DSB
- Finanzkontrolle des Kantons Zürich

Explizit auf die Einreichung einer Stellungnahme verzichtet haben:

- Gemeinde Russikon
- Gemeinde Fehraltorf
- Verwaltungskommission der obersten kantonalen Gerichte

Insgesamt sind 56 Vernehmlassungsantworten und die Mitberichte aller Direktionen eingegangen. Drei Adressierte haben explizit auf die Einreichung einer Stellungnahme verzichtet.

Zehn Gemeinden sowie der VZS haben sich der *Stellungnahme des GPV* angeschlossen bzw. diese inhaltlich teilweise oder vollständig übernommen:

- Gemeinde Dägerlen
- Gemeinde Embrach
- Gemeinde Fehraltorf
- Gemeinde Hausen am Albis
- Gemeinde Hinwil
- Gemeinde Hochfelden
- Gemeinde Niederweningen
- Gemeinde Oberglatt
- Gemeinde Wangen-Brüttisellen
- Gemeinde Rifferswil
- VZS

12 Gemeinden sowie der VPZS haben sich der *Stellungnahme des VZGV* angeschlossen bzw. diese inhaltlich teilweise oder vollständig übernommen:

- Stadt Dietikon
- Gemeinde Fällanden
- Gemeinde Hinwil
- Gemeinde Höri
- Gemeinde Langnau am Albis
- Gemeinde Pfungen
- Gemeinde Rifferswil

- Gemeinde Schlatt
- Gemeinde Stallikon
- Gemeinde Wangen-Brüttisellen
- Stadt Wetzikon
- Gemeinde Zell
- Gemeinde Zumikon
- VPZS

Der Lesbarkeit halber wird in dieser Zusammenstellung jeweils nur der Verein bzw. Verband vermerkt und nicht sämtliche Gemeinden und Verbände aufgeführt, die sich einer jeweiligen Stellungnahme angeschlossen haben.

C. Allgemeiner Eindruck

Die Stossrichtung des Rechtsetzungsvorhabens wird mehrheitlich begrüsst. Betont wird etwa, dass der gemeinsame Rechtsrahmen für die elektronische Leistungserbringung der Verwaltung erforderlich sei. Die Entwicklungsoffenheit und Möglichkeit zur Zusammenarbeit mit namentlich dem Bund zur Stärkung der Interoperabilität werden begrüsst. Der modulare Aufbau des Gesetzes wird hierfür mehrheitlich für geeignet erachtet. Teilweise wird angeregt, die Struktur im Sinne einer Rahmengesetzgebung auszugestalten, um der Exekutive mehr Regulierungsspielraum zu bieten (genannt werden die entsprechenden Gesetze über die digitale Verwaltung in den Kantonen Bern und Graubünden). Vonseiten der Hochschulen und Spitäler wird darauf hingewiesen, dass trotz gewisser Parallelen zwischen der Forschung bzw. der Gesundheitsvorsorge und der Kantonsverwaltung doch erhebliche Unterschiede bestünden; diesen Unterschieden sei auch mit Blick auf ihre verwaltungsrechtliche Autonomie genügend Rechnung zu tragen.

Ein Grossteil der im Vorentwurf vorgeschlagenen Bestimmungen ist weitgehend unbestritten. Die Schaffung eines Rechtsrahmens für die Erbringung von Grundleistungen zugunsten der Einwohnerinnen und Einwohner wird begrüsst. Positiv aufgenommen wird auch das Bekenntnis zur Interoperabilität und die hierzu vorgeschlagene Delegationsgrundlagen zugunsten des Regierungsrates zur Verbindlicherklärung von Standards sowie zum Abschluss von Vereinbarungen mit dem Bund und anderen Kantonen. Vereinzelt wurde der Regelungsvorschlag für die Entwicklung bzw. Weiterentwicklung von digitalen Basisdiensten hinterfragt (§ 5 VE-Gesetz über digitale Basisdienste). In diesem Zusammenhang wurde auch angeregt, den Begriff des «digitalen Basisdienstes» weiter zu schärfen und gegebenenfalls im Gesetz zu definieren.

Eine Mehrheit der Teilnehmende der Vernehmlassung äusserte sich kritisch zum Regelungsvorschlag in § 17 VE-Gesetz über digitale Basisdienste betreffend die Nutzung von cloudbasierten Anwendungen im Rahmen des digitalen Arbeitsplatzes (DAP). Die hierzu vorgebrachten Anträge und aufgeworfenen Fragen sind unterschiedlich begründet. Einerseits betreffen sie rechtliche Einschätzungen dazu, ob überhaupt – insbesondere im Verhältnis zum Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG; LS 170.4) – weitere Rechtsgrundlagen erforderlich sind. Beantragt werden die ersatzlose Streichung von § 17 VE-Gesetz über digitale Basisdienste und/oder die Anpassung des Gesetzes über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (LS 172.71). Andererseits wird die technische Umsetzbarkeit der Vorgaben und ihre Auswirkungen im Arbeitsalltag infrage gestellt. In diesem Zusammenhang werden Anpassungen der Voraussetzungen für die Nutzung von cloudbasierten Anwendungen im Rahmen des DAP beantragt. Die weitergehenden Ausführungen finden sich unter E. bzw. die konkretisierten Anträge unter F.

D. Allgemeine Bemerkungen zur Vorlage

1. Parteien

FDP Kanton Zürich: Unterstützt werden die Digitalisierungsbestrebungen, die den Verkehr mit und unter den Behörden einfacher, schneller und effizienter machen. Mit dem Postulat KR Nr. 160/2021 betreffend «Digital first» fordert die FDP-Fraktion vom Regierungsrat bei neuen Gesetzen sicherzustellen, dass ein digitaler Vollzug erleichtert bzw. ermöglicht werde. Gefordert werden Anpassungen an den digitalen Wandel, Medienbruchfreiheit u.a.m. Der zur Vernehmlassung stehende Gesetzesentwurf zur Schaffung eines digitalen Basisdiensts solle für Nutzerinnen und Nutzer einen zentralen Zugang zu Leistungen der öffentlichen Organe ermöglichen. Dadurch solle ein Flickenteppich von Insellösungen vermieden werden. Die Vorlage müsse insgesamt technologieneutral ausgestaltet sein und es dürften keine Systemabhängigkeiten geschaffen werden. Dies gelte sowohl für § 7 – der Kanton kann den Authentifizierungsdienst des Bundes nutzen, muss aber nicht – als auch für § 17, wo in den Erläuterungen die Verschlüsselung mit dem Beispiel der Double Key Encryption vordefiniert werde, obwohl der betreffende Paragraf technologieneutral ausgestaltet sei. Auch die vorgegebenen Leitplanken bezüglich eines digitalen Arbeitsplatzes sollten

technologieneutral angewendet werden. Auf die Umsetzung der Vorlage sei deshalb besonderes Augenmerk zu richten. Erwartet wird, dass der beispielhaft in den Vernehmlassungsunterlagen genannte Anwendungskatalog von Dienstleistungen wie Bewilligungen aller Art, Einbürgerungsverfahren u.a.m. laufend erweitert werden könne. Dass mit diesem Gesetzesentwurf für die öffentlichen Organe keine Nutzungspflicht verbunden ist, sei angemessen, jedoch sei es zielführend, wenn später auch Gemeinden und weitere öffentliche Organe angehalten würden, ihre Leistungen elektronisch anzubieten.

GRÜNE Kanton Zürich: Begrüsst wird, dass DigiBasis entwicklungsoffen und zukunftsorientiert ausgestaltet sein soll. Damit werde dem Umstand Rechnung getragen, dass digitale Basisdienste sich laufend fortentwickelten. Es brauche auch eine umfassende Regelung über die digitale Verwaltung. Der Regierungsrat solle diese Diskussion zeitnah anstossen. Anerkannt werde die Notwendigkeit, rasch ein schlankes Gesetz zu schaffen, um digitale Basisdienste zu ermöglichen. Die im Bericht angesprochene Grundsatzdebatte über eine digitale Verwaltung müsse dennoch geführt werden und rasch starten. Gerade weil beispielsweise algorithmische Entscheidungssysteme (AES) immer häufiger eingesetzt und in grossem Tempo weiterentwickelt würden. Begrüsst werden weiter der «modulare» Aufbau des Gesetzes sowie die Verankerung, welche Personendaten der Nutzerinnen und Nutzer wie bearbeitet werden.

SP Kanton Zürich: Begrüsst wird die Schaffung eines Rechtsrahmens für digitale Basisdienste, der rechtliche Definition und Flexibilität abwäge und eine Zusammenarbeit mit anderen Kantonen und dem Bund ermögliche. Öffentliche Dienste müssten allen Personen unabhängig von Alter und sozioökonomischem Hintergrund gut zugänglich bleiben. Massnahmen zur Reduktion der digitalen Kluft in der Gesellschaft müssten zur Umsetzung kommen. Zudem müsse der Zugang zu allen Leistungen im Sinne der Barrierefreiheit (Behindertengleichstellungsgesetzes) für Personen, die digitale Verfahren nicht nutzen können, gewährleistet sein. Der Kanton verwalte viele vertrauliche Daten, die nicht für Aussenstehende zugänglich sein sollten. Der Datenschutz und der Schutz vor Cyberangriffen müsse an oberster Stelle stehen. Hier sei auch die Bedeutung von Open-Source-Software hervorzuheben.

SVP Kanton Zürich: Begrüsst wird grundsätzlich die Stossrichtung des Gesetzes über digitale Basisdienste. Es sei wichtig, nach dem Prinzip «digital first», aber nicht nach «digital only» vorzugehen. Erwartet werde eine deutliche Effizienzsteigerung, die sich auch in der Kantonalen Verwaltung bemerkbar machen solle. Die Basisdienste sollten auch von Gemeinden und Bürgerinnen und Bürgern genutzt werden können, um weitere digitale Medienbrüche zu verhindern. Die Anwendungen müssten durchgängig und verständlich gestaltet sein.

2. Vertreterinnen und Vertreter aus der Wirtschaft und Zivilgesellschaft

asut (Schweizerischer Verband der Telekommunikation): Grundsätzlich wird die Gesetzesvorlage begrüsst. Durch die Schaffung von Basisdiensten werde eine Vereinheitlichung von grundlegenden Diensten und Infrastrukturen angestrebt. Dies könne die digitale Transformation der öffentlichen Hand im Kanton Zürich beschleunigen und führe zu mehr Effizienz und tieferen Kosten, als wenn jedes einzelne öffentliche Organ die entsprechenden Dienste selbst konzipieren, beschaffen oder erbringen würde. Die Forderung nach Double Key Encryption in § 17 VE-Gesetz über digitale Basisdienste wird abgelehnt und eine erweiterte Regelung empfohlen, die technische, organisatorische und vertragliche Massnahmen kombiniert.

swissICT (Verband ICT-Werkplatz Schweiz): Die vorgeschlagenen Vorgaben in § 17 seien ersatzlos zu streichen (zur Begründung siehe F.).

Zürcher Handelskammer: Begrüsst wird insbesondere der vorgesehene zentrale Zugang zu den Leistungen der öffentlichen Organe sowie die entwicklungsoffene, zukunftsorientierte sowie interoperable Ausgestaltung des Gesetzesrahmens. Erwartet wird, dass der Umfang der angebotenen Leistungen deutlich erweitert werde, damit die Privatwirtschaft, aber auch die öffentliche Verwaltung von einer Effizienzsteigerung gleichermassen profitiere. Da die Anbietung von Leistungen im Gesetz nicht obligatorisch sei, sollten in einem nächsten Schritt die Gemeinden und weitere öffentliche Organe aufgefordert werden, möglichst viele Leistungen auch elektronisch anzubieten. Die vorgegebenen Leitplanken bezüglich eines digitalen Arbeitsplatzes in § 17, aber auch bezüglich der elektronischen Identifizierung in § 7 seien technologieneutral anzuwenden.

3. Weitere (Privatpersonen, private Unternehmen)

Privatperson A: § 17 VE-Gesetz über digitale Basisdienste sei ersatzlos zu streichen, da die verlangte End-to-End-Verschlüsselung weder rechtlich nötig noch praktikabel sei. Solle das Thema des ausländischen Behördenzugriffs geregelt werden, solle das Gesetz über die Auslagerung von Informatikdienstleistungen ersetzt werden.

Unternehmen B: Die vorgeschlagene Anforderung an die Verschlüsslung in § 17 VE-Gesetz über digitale Basisdienste schränke künftige Entwicklungen ein.

Unternehmen C: § 17 VE-Gesetz über digitale Basisdienste sei nicht sachgerecht und ersatzlos zu streichen. Die fehlende Datensicherheit-Governance und die Missachtung tatsächlich relevanter Risiken in Kontext der Cloud-Nutzung verschmälerten den Mehrwert des Vorentwurfes. Die Attraktivität des digitalen Arbeitsplatzes in der öffentlichen Verwaltung werde zudem für den mehrheitlichen Dateneinsatz mit normalem Schutzbedarf deutlich reduziert, was ebenso dazu führen könne, dass Talente sich nach anderen Arbeitgebern umsähen.

4. Gemeinden und ihre Organisationen

Stadt Dietikon: Begrüsst wird die freiwillige Nutzung, da neben der digitalen Entwicklung nicht vergessen werden dürfe, dass die staatlichen Dienstleistungen der ganzen Bevölkerung zur Verfügung stehen müssten. Die Nutzung von cloudbasierten Anwendungen sei zeitgemäss und für das Funktionieren der Verwaltung mit dem Bedarf nach unterschiedlichsten Softwares zwingend. Lösungen sollten möglich und praktisch gut umsetzbar sein.

Gemeinde Wangen-Brüttisellen: Die Schaffung der Rechtsgrundlagen für digitale Basisdienste wird als wichtig und notwendig erachtet. Beim Ausbau der Basisdienstleistungen seien die Gemeinden paritätisch miteinzubeziehen, da sie in der Umsetzung schlussendlich verantwortlich seien. Ebenfalls seien allfällige Kostenfolgen frühzeitig mit den Gemeinden zu klären. Weiter wird begrüsst, dass gemäss Regierungsratsbeschluss vermehrt gemeinsame Lösungen anstelle von Einzellösungen treten sollen. Synergien sollen wenn immer möglich gewinnbringend genutzt werden. Wichtig sei es, dass auf Verordungsstufe eine zukunftsgerichtete und offene Weiterentwicklung ermöglicht werde, da sich das Umfeld stetig verändere und Agilität

wichtig sei. Der Digitale Arbeitsplatz sei heute nicht mehr wegzudenken von einer zeitgemässen und effizienten Verwaltung. Es gelte das Gebot der höchstmöglichen Sicherheit in Bezug auf den Datenschutz. Jedoch sollen die gesetzlichen Bestimmungen mit Augenmass so festgelegt werden, dass zukünftig das Arbeiten in Cloudlösungen nicht gänzlich verhindert werde. Die in § 17 vorgesehenen Einschränkungen gehen diesbezüglich zu weit. Der Gemeinderat schliesse sich daher dem Antrag des GPV an.

Gemeinde Meilen: Begrüsst werden die Stossrichtung des Gesetzes über digitale Basisdienste sowie die damit einhergehenden Digitalisierungsschritte und die Vereinfachung der digitalen Kommunikation zwischen privaten Nutzenden bzw. Unternehmen auf der einen Seite und öffentlichen Organen auf der anderen Seite. Beantragt werden Anpassungen der vorgeschlagenen Regelung zum digitalen Arbeitsplatz (§ 17 VE-Gesetz über digitale Basisdienste).

Stadt Uster: Der Vorentwurf wird als gelungen betrachtet, zumal er wichtige Aspekte im Rahmen des digitalen Service Public auf Kantonaler und Gemeindeebene regle. Besonders begrüsst wird die Verankerung, dass öffentliche Organe den Authentifizierungsdienst des Bundes (AGOV) für die elektronische Identifizierung nutzen können und sollen. Noch zu schärfen sei der sehr weite Begriff des «Basisdienstes».

Stadt Wetzikon: Beantragt wird in Abweichung von der Stellungnahme des VZGV, an die sich die Stadt Wetzikon grundsätzlich anschliesst, eine ersatzlose Streichung von § 17. Es fehle zudem eine Regulierung zum Umgang mit der «Künstlichen Intelligenz»; hierzu solle eine Diskussion mit den Gemeinden aufgenommen werden. Zudem sei die Abstimmung mit dem Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben vom 17. März 2023 (EMBAG, SR 172.019) sicherzustellen. Der Fokus solle dabei insbesondere auf der Bereitstellung von anwendbaren Grundlagen für die Abwicklung von Prozessen, den Informationsfluss, die Datenharmonisierung und die Bereitstellung von IKT-Leistungen liegen.

Gemeinde Winkel: Unterstützt wird, dass DigiBasis entwicklungsoffen und zukunftsorientiert ausgestaltet sei. Weiterentwicklungen sollten aktiv angegangen werden. Unterstützt wird die Absicht, dass die Nutzung der digitalen Basisdienste freiwillig erfolgen soll. Gewünscht wird der Einbezug von egovpartner in die einzelnen Prozesse, um auch die Bedürfnisse der Gemeinden und Städte einfliessen zu lassen.

GPV: Grundsätzlich werden Harmonisierungsbestrebungen und eine weitere Professionalisierung im Bereich Digitalisierung auf Stufe Kanton mit direktem Nutzen für die Bevölkerung, Wirtschaft und die Kommunen im Kanton begrüsst. Es wird jedoch festgestellt, dass insbesondere in den Bereichen der IT, Digitalisierung, Kommunikationstechnologie und Künstlichen Intelligenz die gesetzlichen Bestimmungen weit hinter der Realität hinterherhinkten. So hätten sich die grossen Marktanbieter mit ihrer Software und ihren Cloudlösungen bereits überall durchgesetzt. Wolle man diese Anbieter ausschliessen, könne dies nur unter grösstem Aufwand und mit fragwürdigen Auswirkungen bezüglich Effizienz und Zusammenarbeit bewerkstelligt werden.

VZGV: Begrüsst werden die Schaffung von gesetzlichen Grundlagen für den Ausbau des digitalen Leistungsangebotes, die angestrebten gemeinsamen Lösungen anstelle von Einzellösungen sowie die Kompetenz des Regierungsrates zum Erlass von Ausführungsbestimmungen bei technischen Weiterentwicklungen. Unterstützt wird zudem, dass die Nutzung der digitalen Basisdienste freiwillig erfolgen soll. Beantragt werden Anpassungen betreffend den Regelungsvorschlägen zu Standards und Schnittstellen (§ 3 VE-Gesetz über digitale Basisdienste), zum Webzugang (§§ 10 und 16 VE-Gesetz über digitale Basisdienste) sowie zum digitalen Arbeitsplatz (§ 17 VE-Gesetz über digitale Basisdienste).

VZS: Der VZS lehnt sich in seinen Äusserungen an die Stellungnahme des GPV.

5. Selbstständige Anstalten und Körperschaften, öffentliche Stiftung

PHZH: Die Stossrichtung der Vorlage wird begrüsst, wonach die Digitalisierung der Verwaltung vorangebracht werden soll. Das Gesetz solle aber nicht nur im Bereich des klassischen Verwaltungshandelns und der Kernverwaltung gelten, sondern unter anderem auch für die Hochschulen und damit die PHZH. Hochschulen bewegen sich in einem speziellen Kontext, was es zu berücksichtigen gelte. Die PHZH unterstützt die Stellungnahme der UZH und weist auf weitere Punkte hin.

UZH: Grundsätzlich wird die Stossrichtung der Vorlage begrüsst, welche die Digitalisierung der Verwaltung und der Angebote voranbringen will. Das Tätigkeitsgebiet einer autonomen selbständigen Anstalt wie der UZH und insbesondere die Forschung und die Handhabung von Forschungsdaten seien jedoch anders gelagert als die

Funktionsweise einer kantonalen Verwaltung. Um die Forschungsfreiheit nicht einzuschränken, sei es zentral, dass die selbständigen Anstalten des Kantons vom Geltungsbereich des Gesetzes ausgenommen werden.

Evangelisch-reformierte Landeskirche des Kantons Zürich, Katholische Kirche im Kanton Zürich: Begrüsst wird, dass mit dem vorliegenden Gesetzesentwurf die rechtliche Grundlage für digitale Basisdienste geschaffen werde, das elektronische Angebot einer konkreten öffentlichen Leistung (einzelne Verwaltungsaufgabe) jedoch in der Fachgesetzgebung zu regeln sei. Auch wird die Einschätzung geteilt, dass das Gesetz über die digitalen Basisdienste möglichst weit zu fassen sei, um technische Weiterentwicklungen miteinzuschliessen. Nicht schlüssig sei, dass das Gesetz über die digitalen Basisdienste verlange, dass jeder Basisdienst im Gesetz selber explizit genannt werden müsse. Anstatt der Aufführung konkreter Basisdienste in diesem Gesetz solle geregelt werden, unter welchen Voraussetzungen Basisdienste generell betrieben, genutzt und (weiter-)entwickelt werden dürften. Andernfalls müsse für jeden neuen digitalen Basisdienst das vorliegende Gesetz geändert oder eine neue gesetzliche Grundlage geschaffen werden. Viele der Bestimmungen im 4. Abschnitt des Gesetzes könnten deshalb allgemeiner formuliert werden und damit für digitale Basisdienste generell Geltung beanspruchen. Die Themenbereiche «Authentifizierung/Identifikation», «Zentraler Zugang» und «cloudbasierte Anwendungen» könnten abstrakt formuliert werden, um künftige Lösungen mitzuerfassen. Dies würde dem Legalitätsprinzip genügen und die rechtsstaatlich fragwürdige Regelung zur Entwicklung von digitalen Basisdiensten (§§ 5 f.) überflüssig machen. Die bereits geplanten digitalen Basisdienste wie das «Zürikonto» könnten – soweit nötig – auf Verordnungsstufe im Detail geregelt werden.

Eine gesetzliche Regelung der Nutzung cloudbasierter Informatikdienstleistungen im Rahmen des digitalen Arbeitsplatzes wird im Grundsatz begrüsst. Allerdings gelte diese Regelung bereits aufgrund der Grundsätze des Datenschutzes nach IDG. Es stelle sich daher die Frage, ob es überhaupt einer zusätzlichen Regelung bedürfe. Auch mit einer solchen sei nicht restlos gewährleistet, dass Unberechtigte keinen Zugriff auf die auf diesem Weg gespeicherten Daten hätten. Die Nutzung von Cloud-Diensten, insbesondere von Microsoft 365, verursache aufgrund der Zusatzvereinbarung der Schweizerischen Informatik-Konferenz mit Microsoft erhebliche Lizenzierungskosten, die bei der Landeskirche bzw. bei der Römisch-katholischen Körperschaft und bei den

Kirchgemeinden erheblich ins Gewicht fielen. Es sei daher die Frage, ob die anfallenden Kosten als Folge der gesetzlichen Vorgaben in einem angemessenen Verhältnis zur nur beschränkt erreichbaren Datensicherheit stünden.

6. Verwaltungsunabhängige kantonale Stellen

DSB: Das Erlassprojekt DigiBasis und dessen Regelungsgegenstand werden begrüsst. Die Datenschutzbeauftragte sei bereits im Vorfeld der Vernehmlassung konsultiert worden und habe erste Inputs zur Vorlage einbringen können.

E. Übergreifende Anliegen nach Themenkreis

1. Begrifflichkeiten

Von einigen Vernehmlassungsteilnehmenden werden Legaldefinitionen angeregt. Zum Teil wird vorgebracht, dass der Begriff des «digitalen Basisdienstes» und der «Cloud» bzw. «cloudbasiert» ungenau seien. Dies führe zu Rechtsunsicherheiten. Namentlich in Bezug auf die Entwicklung und Weiterentwicklung von digitalen Basisdiensten sei eine Eingrenzung des Begriffs «digitaler Basisdienst» zu erwägen. Zugleich handle es sich um technische und sehr abstrakte Begriffe. Definitionsbedarf wird auch für den Begriff des «Digitalen Arbeitsplatzes» im Zusammenhang mit § 17 VE-Gesetz über digitale Basisdienste gesehen. Gerade im Hochschulbereich sei bei einer Definition die Integration und Unterstützung von persönlichen Geräten zu berücksichtigen.

2. Regelungsansatz

Verschiedene Vernehmlassungsteilnehmende begrüssen den vorgeschlagenen modularen Aufbau des Gesetzes über digitale Basisdienste. Damit könne der Entwicklungsoffenheit Rechnung getragen werden, indem die allenfalls notwendigen Rechtsgrundlagen für künftige digitale Basisdienste mittels Gesetzesrevisionen geschaffen würden. Andere schlagen als Regelungsansatz vor, allgemeine Anforderungen an digitale Basisdienste und Regelungsziele auf Gesetzesstufe aufzunehmen. Die Umsetzung könne auf Verordnungsstufe geregelt werden.

3. Geltungsbereich

Von den an der Vernehmlassung teilnehmenden selbständigen Anstalten wird beantragt, dass die selbständigen Anstalten vom Geltungsbereich des Gesetzes auszunehmen oder die Vorgaben für sie als optional, als «Kann»-Formulierungen auszugestalten seien. Die Gemeinden betonen, dass die sie betreffenden Vorgaben (namentlich zur Verbindlichkeit von Standards und Schnittstellen) unter ihren Einbezug zu erfolgen hätten.

4. Digitaler Arbeitsplatz

Mehrheitlich äussern sich die Vernehmlassungsteilnehmenden kritisch zu § 17. Die Begründungen lassen sich wie folgt gruppieren:

- Eine gesetzliche Regelung sei nicht erforderlich, da unter anderem bereits die bestehenden Vorgaben des Datenschutzes genügten.
- Die Vorgaben seien zu streng und in der Arbeitsrealität nicht umsetzbar. Insbesondere die Anforderungen an die Verschlüsselung hätten sehr hohe Kosten zur Folge und würden die Funktionalitäten von cloudbasierten Anwendungen des digitalen Arbeitsplatzes stark einschränken.
- Funktionsfähige Cloud-Lösungen, die insbesondere eine erhöhte Datensicherheit zum Schutz der Daten ermöglichten, überwögen das für äusserst minim erachtete Risiko eines ausländischen Behördenzugriffs.
- Die Bestimmung sei nicht technologieneutral ausgestaltet.

Vereinzelt wird die Schaffung einer Gesetzesgrundlage begrüsst.

Entsprechend der genannten Positionen werden unterschiedliche Anpassungen beantragt:

- Ersatzlose Streichung von § 17 VE-Gesetz über digitale Basisdienste;
- Anpassung der Voraussetzungen in § 17 VE-Gesetz über digitale Basisdienste;
- Nebenänderung des Gesetzes über die Auslagerung von Informatikdienstleistungen anstelle einer Regelung im Gesetz über digitale Basisdienste;
- Ergänzende Vorgaben nach § 17 VE-Gesetz über digitale Basisdienste.

F. Besondere Bemerkungen zu einzelnen Bestimmungen

Siehe nachfolgende synoptische Darstellung.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

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. [1] Dieses Gesetz regelt:

Evangelisch-reformierte Landeskirche des Kantons Zürich, Katholische Kirche im Kanton Zürich
Aus dem Gesetz ergebe sich weder direkt noch durch Verweis, was unter «digitaler Basisdienst» zu verstehen sei. Einerseits handle es sich dabei um einen sehr technischen Begriff, der nicht allgemein verständlich sei. Andererseits sei er abzugrenzen von den Fachapplikationen für konkrete Verwaltungsaufgaben. Es sei daher eine Legaldefinition im Gesetz vorzusehen.

a. den Betrieb, die Nutzung und die

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
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.	asut (Schweizerischer Verband der Telekommunikation) Das Gesetz gelte nicht nur für die öffentliche Verwaltung im engeren Sinne, sondern für alle öffentlichen Organe, wozu auch Spitäler oder Universitäten gehörten. Einige dieser Organisationen betrieben bereits eigene Basisdienste oder griffen auf Basisdienste Dritter zu, die sich in der Praxis bewährt hätten. Der Geltungsbereich gemäss § 2 im Zusammenspiel mit den Regelungen für die einzelnen Basisdienste solle so ausgelegt werden, dass bereits bestehende Basisdienste weiterbetrieben und auch weiterentwickelt werden könnten. USZ Die Spitäler seien im Bereich Digitalisierung mit eigenen Herausforderungen konfrontiert (Berufsgeheimnis, finanzielle Ressourcen). Teilweise sähen sie sich mit der anspruchsvollen Aufgabe konfrontiert, unter diesen Bedingungen eigene digitale Angebote zu entwickeln. Teilweise nutzten die Gesundheitsinstitutionen etablierte Angebote (z.B. HIN-Kommunikationslösungen), deren Einbindung mit erheblichem Aufwand verbunden gewesen sei. Es wäre für das USZ einschneidend, wenn die Nutzung bestehender, etablierter Angebote und die Entwicklung neuer, spezifisch für den Gesundheitsbereich geeigneter Angebote durch das neue Gesetz zusätzlich

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

erschwert würden. Die Regelungsdichte im Gesundheitswesen sei sehr hoch. Die zusätzliche Berücksichtigung neuer, bereichsfremder Anforderungen und die Einbindung vorgegebener Lösungen aus der Zentralverwaltung – u.U. verbunden mit erheblichem Anpassungsbedarf für bereichsspezifische Anforderungen – sei für das USZ nicht tragbar. Daher seien die selbständigen Anstalten vom Geltungsbereich des Gesetzes auszunehmen oder die Vorgaben des Gesetzes für diese als optional/Kann-Formulierungen auszugestalten. Für den Fall, dass der Geltungsbereich im vorgesehenen (überschiessenden) Umfang bestehen bleibe, seien Anpassungen im Sinne der nachfolgenden Hinweise erforderlich.

PHZH

Die Autonomie der Hochschulen sei zu wahren. Der Neuerlass sehe mit dem Betrieb, der Nutzung und der (Weiter-)Entwicklung der Digitalen Basisdienste verschiedene Kompetenzverschiebungen vor, was zu vermeiden sei (insbesondere. §§ 3, 4, 5 f., 7 und 10 des Vorentwurfs). Wie die UZH verfüge auch die PHZH bereits über bestehende eigene Portale und biete digitale Leistungen an, welche mindestens teilweise von SWITCH betrieben würden und mit der Authentifizierung/Identifikation von SWITCH, welche im Schweizer Hochschulumfeld etabliert sei, funktionierten. Die PHZH unterstützt den grundsätzlichen Antrag der UZH, die selbständigen Anstalten vom Geltungsbereich des Gesetzes auszunehmen oder die Vorgaben des Gesetzes für diese als optional/Kann-Formulierungen auszugestalten. Die im Vorentwurf erwähnten Genehmigungs- und Bewilligungsinstanzen seien hinsichtlich der Zuständigkeit bei selbständigen Anstalten zu überprüfen. Ferner sei es wichtig, dass weiterhin alternative Authentifizierungsdienste wie beispielsweise SWITCH edu-ID möglich seien.

UZH

Die Zürcher Hochschulen verfügten bereits über bestehende eigene Portale und böten digitale Leistungen an,

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	welche mit etablierten Lösungen von SWITCH betrieben würden. Anpassungen der technischen Lösungen müssten durch weitere finanzielle Mittel gedeckt werden. Strengere Vorgaben könnten die Forschungsfreiheit gefährden und Wettbewerbsnachteil in der Forschung verschärfen. Daher seien die selbständigen Anstalten vom Geltungsbereich des Gesetzes auszunehmen oder die Vorgaben des Gesetzes für diese als optional/Kann-Formulierungen auszugestalten. Evangelisch-reformierte Landeskirche des Kantons Zürich, Katholische Kirche im Kanton Zürich Wer sich in der zürcherischen Gesetzgebung auskenne, vermute zwar, dass der Begriff «öffentliches Organ» im Vernehmlassungsentwurf mit der Verwendung dieses Begriffs im IDG übereinstimme. Diese Vermutung ergebe sich aber nicht aus dem Gesetz, weshalb auch hierfür eine Legaldefinition oder eine Verweisung auf das IDG anzubringen sei.
2 Es gilt für private Nutzerinnen und Nutzer, wenn sie die in diesem Gesetz genannten digitalen Basisdienste nutzen.	
3 Die Erbringung einer elektronisch angebotenen Leistung durch das öffentliche Organ richtet sich nach der Fachgesetzgebung.	
2. Abschnitt: Interoperabilität	

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
Standards und Schnittstellen	
§ 3. [1] Zur Gewährleistung der Durchgängigkeit der in diesem Gesetz geregelten digitalen Basisdienste kann der Regierungsrat für verbindlich erklären:	SP Kanton Zürich Es handle sich hierbei um Bedingungen, die nicht fakultativ sein sollten, sondern für eine moderne Softwareentwicklung und eine nachhaltige Investition notwendig seien. Eine neue Formulierung wird vorgeschlagen («Zur Gewährleistung der Durchgängigkeit der in diesem Gesetz geregelten digitalen Basisdienste erklärt der Regierungsrat für verbindlich:»); diese lasse genug Flexibilität, um die Verwaltung nicht einzuschränken. asut (Schweizerischer Verband der Telekommunikation) Es sei richtig, dass sich der Regierungsrat an internationalen Standards und dem Stand der Technik orientiere. Dabei sei jedoch zu berücksichtigen, dass gerade im ICT-Bereich der technische Fortschritt sehr rasch erfolge und Innovationszyklen immer kürzer würden. Der Regierungsrat solle daher vor Verbindlicherklärung von Standards betroffene Branchen und Unternehmen anhören. Damit werde sichergestellt, dass diese Standards mit den Angeboten und Möglichkeiten des Marktes vereinbar seien. Gemeinde Winkel Es sei wünschenswert, dass diese Standards in Zusammenarbeit mit egovpartner gesetzt würden, damit auch die Bedürfnisse der einzelnen Gemeinden einfliessen könnten und um allfälligen Mehraufwand der Gemeinden auszuschliessen. Stadt Zürich Dass dem Regierungsrat die Kompetenz für die Verbindlicherklärung von Standards und Schnittstellen erteilt

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

werde, sei zu begrüssen. Dabei solle er sich aber nicht nur an nationalen und internationalen Standards sowie dem Stand der Technik orientieren müssen, sondern auch vorgängig die von der Umsetzung betroffenen Gemeinwesen, v.a. auch die Gemeinden, anhören müssen.

USZ

Begrüsst werde das deutliche Signal des Vorentwurfs, dass technische und organisatorische Standards vereinheitlicht und Schnittstellen standardisiert werden sollten. Im Gesundheitswesen und insbesondere in der institutions- und grenzüberschreitenden Forschungszusammenarbeit sei diese Standardisierung bereits weiter fortgeschritten als im klassischen Verwaltungshandeln. Insbesondere das Swiss Personalized Health Network (SPHN) habe in den letzten Jahren in diesem Bereich wichtige Arbeit geleistet, in die das USZ direkt involviert gewesen sei. Vom DigiSanté-Programm seien auf Bundesebene weitere wichtige Impulse zu erwarten. Die Abstimmung mit zusätzlichen Anforderungen, die vom Regierungsrat unter dem neuen Gesetz verbindlich erklärt werden könnten, könne für das USZ zu erheblichem Aufwand führen. Soweit die Anforderungen für die selbständigen Anstalten nicht als Kann-Bestimmungen ausgestaltet würden, seien den Spitälern angemessene Übergangsfristen zu gewähren. Auch an dieser Stelle sei darauf hinzuweisen, dass zusätzliche, bereichsfremde Anforderungen zu erheblichem finanziellem Zusatzaufwand führen könnten.

PHZH

Die vorgeschlagene Bestimmung gebe dem Regierungsrat die Kompetenz, auch für Hochschulen die Anwendung von technischen und organisatorischen Standards vorzugeben, um die Durchgängigkeit der von den Hochschulen autonom erstellten digitalen Basisdienste zu gewährleisten. Was auf den ersten Blick als wünschenswert erscheine, könne in der Praxis dazu führen, dass im Austausch mit anderen kantonalen oder internationalen

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

Partnern für die Forschung und Lehre einschneidende Einschränkungen erfolgten. Eine derartige Verschiebung der Regelungskompetenzen zum Regierungsrat hin sei aus Sicht der PHZH und wohl der Hochschulen allgemein nicht wünschenswert. Auf den zusätzlichen Aufwand und die unbekannten finanziellen Folgen sowie die gegebenenfalls dringend notwendigen Übergangsfristen mache die UZH in ihrer Stellungnahme bereits aufmerksam.

UZH

Die Interoperabilität der Angebote sei zu begrüssen. Allerdings seien Anpassungen von Standards und Schnittstellen mit zusätzlichen Aufwänden und unbekannten finanziellen Kosten verbunden. Bei der Einführung neuer Anforderungen für die selbständigen Anstalten sei für deren Umsetzung eine angemessene Übergangsfrist zu gewähren sowie deren Finanzierung durch den Kanton sicherzustellen.

Evangelisch-reformierte Landeskirche des Kantons Zürich, Katholische Kirche im Kanton Zürich

Um die Interoperabilität von allen künftigen von öffentlichen Organen betriebenen, genutzten oder entwickelten digitalen Basisdiensten zu gewährleisten, solle auf den einschränkenden Teilsatz «der in diesem Gesetz geregelten» (Basisdienste) verzichtet werden.

Finanzkontrolle des Kantons Zürich

Ein dritter Absatz sei zu schaffen: «Grundsätzlich sind die digitalen Angebote über ein zentrales Portal im Sinne der Basisdienste anzubieten.» Die Bevölkerung und Unternehmen sollten die Möglichkeit haben, ihre Dienstleistungen möglichst einfach, ohne Medienbrüche und möglichst über nur ein Portal zu beziehen. Zudem könnten bei nur einem Portal für alle Dienstleistungen langfristig Kosten für die Basisinfrastruktur eingespart werden.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
a. die Anwendung von technischen und organisatorischen Standards,	VZGV In der Gesetzesvorlage wäre es aufschlussreich zu erfahren, ob es heute bereits Standards innerhalb der kantonalen Verwaltung gebe und wo der Regierungsrat Einsatzbereiche sehe. Dies sei eine wichtige Grundlage und Information für § 5 Abs. 1 VE-Gesetz über digitale Basisdienste.
b. die Standardisierung der technischen Schnittstellen zu einer elektronisch angebotenen Leistung eines öffentlichen Organs.	VZGV Sollten geplante organisatorische Standards die Geschäftsprozesse der Gemeinden und Städte betreffen, sollten diese einbezogen werden. Damit solle der Bezug zur Praxis optimal sichergestellt werden.
2 Er orientiert sich dabei an nationalen und internationalen Standards sowie am Stand der Technik.	GRÜNE Kanton Zürich Wenn immer möglich sollten offene Standards zur Anwendung kommen. Offene Standards trügen zu einer besseren Interoperabilität bei und verringerten die Abhängigkeit von einzelnen Anbietern. VZGV Die Berücksichtigung nationaler und internationaler Standards wird begrüsst. Es sei wo immer möglich darauf Bezug zu nehmen und Einzellösungen zu vermeiden. GVZ Es sei sinnvoll, dass sich der Regierungsrat an nationalen und internationalen Standards sowie dem Stand der Technik orientieren solle. Es wird angeregt, dass insbesondere die eCH-Standards berücksichtigt werden, um die Interoperabilität von Datenschnittstellen optimal zu gewährleisten.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
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.	SVP Kanton Zürich Die Zusammenarbeit mit dem Bund und anderen wird begrüsst. GVZ Begrüsst wird die schweizweite Koordination und damit Vereinheitlichung im Bereich der digitalen Basisdienste. Finanzkontrolle des Kantons Zürich Zur Stärkung der Governance im Bereich der Vereinbarungen mit Bund und Kantonen sei die Bestimmung (analog zu Art. 4 Abs. 2 EMBAG) zu ergänzen: «Die Vereinbarungen legen, soweit erforderlich, insbesondere folgendes fest: a. die Zuständigkeiten; b. die Organisation; c. die Finanzierung; d. das anwendbare Recht, insbesondere in den Bereichen Datenschutz und Informationssicherheit, Öffentlichkeit der Verwaltung, Personalrecht und Archivierung.»
3. Abschnitt: Entwicklung von digitalen Basisdiensten	
Voraussetzungen	
§ 5. [1] Vor dem Erlass einer Rechtsgrundlage können bestehende digitale Basisdienste weiterentwickelt und neue digitale	GRÜNE Kanton Zürich Die kumulativ zu erfüllenden Voraussetzungen nach § 5 Abs. 1 lit. a–c werden begrüsst.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
Basisdienste entwickelt werden, wenn:	SP Kanton Zürich § 5 sei zu ergänzen mit — d. die Softwareentwicklung in der Regel Open Source erfolgt ausser in Ausnahmefällen, die schriftlich begründet werden müssen zuhanden des Regierungsrates. — e. im Rahmen des Basisdienstes ausschliesslich nicht-proprietäre und lizenzabgabefreie Formate oder Standards verwendet werden. — f. die freie Weiterverwendung und Weiterentwicklung der entwickelten Software unabhängig von einer Partnerorganisation sichergestellt ist. — g. die Softwarelösung vom Kanton und nicht extern gehostet wird. Open Source Software in Verwaltungssoftware werde im EMBAG neu auch auf Bundesebene verankert. Durch diese Ergänzungen würden erstens die Cyber Security und der Datenschutz verbessert, da durch Open Source Software und internes Hosting transparent sei, was entwickelt worden sei und keine Backdoors eingebaut werden könnten. Zweitens verhinderten diese Ergänzungen einen Vendor-Lock-in, der zu einer ineffizienten Ressourcennutzung führen könne. Und drittens werde so die zukünftige Weiterentwicklung garantiert und eventuell auch die Zusammenarbeit mit anderen Kantonen / dem Bund erleichtert. UZH Es könne für die selbständigen Anstalten nicht gelten, dass der Regierungsrat die Entwicklung von digitalen Basisdiensten des Kantons nach § 5 VE-Gesetz über digitale Basisdienste bewillige. Es sei vorzusehen, welche Behörde die Entwicklung bei den selbständigen Anstalten bewilligen könne, sinnvollerweise wäre dies deren Aufsichtsorgan (bspw. Universitätsrat, Hochschulrat oder Spitalrat).

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

Evangelisch-reformierte Landeskirche des Kantons Zürich, Katholische Kirche im Kanton Zürich

Die hier vorgeschlagene Regelung sei als Blankettermächtigung an den Regierungsrat formuliert. Sie nenne Voraussetzungen, welche aufgrund von gleichgeordnetem Recht ohnehin gälten. Die Regelung erscheine rechtsstaatlich fragwürdig. Insbesondere fehle eine genügend bestimmte gesetzliche Grundlage für die Datenbearbeitung, wenn es genügen soll, dass ein Rechtsetzungsvorhaben lediglich gestartet ist. Zudem sei fraglich, ob in allen Fällen bereits bei der Entwicklung eines digitalen Basisdienstes vorab feststehe, dass keine besonderen Personendaten bearbeitet würden oder bearbeitet werden müssten.

DSB

Die Bestimmung zur Inbetriebnahme von digitalen Basisdiensten ohne Rechtsgrundlagen sei zu streichen und mit einer Bestimmung zu Pilotversuchen nach dem Vorbild von Art. 15 EMBAG zu ersetzen. Die Bestimmung zur Inbetriebnahme von digitalen Basisdiensten ohne Rechtsgrundlagen sei problematisch. Sie solle gemäss den Erläuterungen Situationen adressieren, 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 auseinanderfielen. Dabei würden jedoch die demokratischen Prozesse umgangen und das Legalitätsprinzip ausgehöhlt. Diese Situation werde durch die Tatsache verschärft, dass der Entwurf des Gesetzes keine Definition von digitalen Basisdiensten enthalte und somit praktisch nicht eingegrenzt werde. Die Situation werde weiter durch die Tatsache verschärft, dass es sich bei digitalen Basisdiensten oft um sehr grosse Digitalisierungsprojekte handeln dürfte. Würden solche Projekte potentiell 7 Jahre ohne Rechtsgrundlagen vorangetrieben, entstehe ein riesiger Druck auf den Gesetzgeber und eine freie Meinungsfindung zum Erlass von Rechtsgrundlagen (oder eben nicht) werde aufgrund

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	des fortgeschrittenen Stadiums des Projekts und der bereits investierten Ressourcen erschwert, wenn nicht verunmöglicht. Schliesslich werde die Situation durch die Tatsache verschärft, dass diese Regelung für alle öffentlichen Organe im Kanton Zürich gelte und so an enorm vielen Orten Digitalisierungsprojekte ohne Rechtsgrundlagen entstehen könnten. Dies dürfe nicht die Vision der Digitalisierung sein. Vergleichbare Gesetze wie das EMBAG enthielten keine Bestimmung, mit der eine Inbetriebnahme von Digitalisierungsprojekten ohne Rechtsgrundlagen möglich sei. Sinnvoller erscheine deswegen eine erweiterte, mit dem IDG abgestimmte, Regelung zu Pilotversuchen nach dem Vorbild von Art. 15 EMBAG. Solange der Begriff «digitale Basisdienste» nicht trennscharf definiert werde, könne der Anwendungsbereich dieser Bestimmung nicht eingegrenzt werden, weil potenziell sehr viele Digitalisierungsprojekte unter den Begriff «digitale Basisdienste» fallen könnten. Entsprechend sei eine enge Definition des Begriffs «digitale Basisdienste» in DigiBasis aufzunehmen, damit die bereits im Grundsatz problematische Bestimmung zur Inbetriebnahme von digitalen Basisdiensten ohne Rechtsgrundlagen in § 5 nicht zu extensiv angewendet werden könne. Sollte an der Bestimmung zur Inbetriebnahme von digitalen Basisdiensten ohne Rechtsgrundlagen in § 5 festgehalten werden, sei eine Definition des Begriffs «digitale Basisdienste» in das Gesetz aufzunehmen. Würde die Bestimmung zur Inbetriebnahme von digitalen Basisdiensten in § 5 gestrichen, reiche die aktuelle Beschreibung des Begriffs «digitale Basisdienste» in den Erläuterungen.
a. die erforderlichen Massnahmen für die Informationssicherheit und die Sicherstellung des Datenschutzes getroffen worden sind,	SVP Kanton Zürich Die Gewährleistung von Informationssicherheit und Datenschutz sei entscheidend, um sicherzustellen, dass ein Produkt ohne «Nebenwirkungen» eingesetzt werden könne.
b. die Aufgaben, aufgrund derer die	Evangelisch-reformierte Landeskirche des Kantons Zürich, Katholische Kirche im Kanton Zürich

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
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 c. Rahmen des weiter- oder neu entwickelten digitalen Basisdienstes keine besonderen Personendaten bearbeitet werden.	Es sei unklar, ob mit «Aufgabe» die Verwaltungsaufgabe (Fachgesetzgebung) oder der digitale Basisdienst gemeint sei.
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.	<u>GRÜNE Kanton Zürich</u> Fünf Jahre nach Beschluss nach § 5 zur Inkraftsetzung der Rechtsgrundlage seien ausreichend. Eine einmalige Verlängerung um zwei Jahre sei nicht notwendig. <u>Evangelisch-reformierte Landeskirche des Kantons Zürich, Katholische Kirche im Kanton Zürich</u> Für die einmalige Verlängerung der Entwicklungsphase eines digitalen Basisdienstes sei in allen Fällen der Regierungsrat zuständig. Hingegen solle für die Entwicklung ohne gesetzliche Grundlage je nach dem, auf welcher Ebene ein digitaler Basisdienst zur Anwendung gelangen solle, der Regierungsrat oder der Gemeindevorstand zuständig sein. Damit fielen die Zuständigkeiten in einem laufenden Prozess bzw. Vorhaben auseinander. Entweder sei in allen Fällen die generelle Zuständigkeit des Regierungsrates festzuschreiben (für alle Körperschaften des kantonalen öffentlichen Rechts, d.h. inklusive politische, Schul- und Kirchgemeinden und Zweckverbände) oder es sei in allen Fällen das Exekutivorgan der betreffenden Körperschaft als zuständig zu erklären.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
Zuständigkeiten	
§ 6. [1] Der Regierungsrat bewilligt die Entwicklung von digitalen Basisdiensten des Kantons nach § 5.	Evangelisch-reformierte Landeskirche des Kantons Zürich, Katholische Kirche im Kanton Zürich Das Gesetz bezwecke eine umfassende Regelung der digitalen Basisdienste. Es sei deshalb auch für die anderen öffentlich-rechtlichen Körperschaften wie die Römisch-katholische Körperschaft eine Kompetenzordnung für die Entwicklung vorzusehen, z.B. die «oberste leitende Behörde» oder das «oberste leitende und vollziehende Organ» (vgl. auch die Begründung zu § 5 Abs. 2).
[2] Für Gemeinden gilt § 5 sinngemäss. Zuständig für die Bewilligung ist der Gemeindevorstand.	
4. Abschnitt: Digitale Basisdienste	
A. Elektronische Identifizierung	DSB Die Verwendung der Terminologie «Identifizierung» sei zu überprüfen. Die Erläuterungen zu § 7 erwähnten unter dem Punkt «Abgrenzungen», dass die Begriffe «identifizieren» und «authentifizieren» zwei Vorgänge mit unterschiedlichem Regelungsbedarf bezeichneten, die auseinander zu halten seien. Da §§ 7 und 8 die Authentifizierung regelten, sei nicht ersichtlich, weshalb unter Punkt A von der elektronischen Identifizierung gesprochen werde. Konsequenterweise sei hier die elektronische Authentifizierung zu nennen anstatt der elektronischen Identifizierung.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
Nutzung des Authentifizierungsdienstes des Bundes § 7. Das öffentliche Organ kann zur elektronischen Identifizierung einer Nutzerin oder eines Nutzers den vom Bund betriebenen Authentifizierungsdienst verwenden.	SP Kanton Zürich Die Unabhängigkeit von amerikanischen Technologiekonzernen sei zu wahren, damit keine inakzeptable Abhängigkeitsverhältnisse entstünden. Ausserdem gehöre es zur digitalen Selbstbestimmung, keine Daten an diese Unternehmen weiterzugeben. Die Bestimmung sei zu ergänzen: «Es muss sichergestellt werden, dass die Nutzung eines Authentifizierungsdienstes nicht die Verwendung von proprietären Anwendungen (z.B. Google Playstore oder Apple App Store) erfordert. Bei der Verwendung anderer Verfahren dürfen Nutzende nicht auf kommerzielle Lösungen gezwungen werden. Sowohl Benutzbarkeit wie Installierbarkeit muss für mindestens eine Lösung uneingeschränkt möglich sein.». asut (Schweizerischer Verband der Telekommunikation) Die Einführung der e-ID des Bundes wird begrüsst und unterstützt. Diese Vertrauensinfrastruktur stelle eine wichtige Grundlage für digitale Dienstleistungen bei der Verwaltung und in der Wirtschaft dar. Dies gelte im Grundsatz auch für AGOV. Gemäss § 7 sei die Nutzung des AGOV durch öffentliche Organe freiwillig. In Bezug auf den Webzugang sei die Verwendung von AGOV jedoch gemäss §12 zwingend. Dies sei für diejenigen öffentlichen Organe problematisch, die bereits einen bestehenden Authentifizierungsdienst nutzen. Dies betreffe beispielsweise die Zürcher Hochschulen und die Universität, da alle Schweizer Hochschulen den Identifizierungsdienst und den Authentifizierungsdienst der Stiftung SWITCH verwendeten. Eine zwingende Anwendung von AGOV würde für die Zürcher Hochschulen und die Universität daher zu Schnittstellenproblemen in der Hochschullandschaft führen. Zudem würde dies auch zu Doppelspurigkeiten und Mehraufwand führen, da der AGOV nicht alle Bedürfnisse der Hochschulen abdecke. Daher solle die Nutzung von AGOV für den

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

Webzugang gemäss § 12 mit einer Kann-Formulierung versehen werden, solange ein gleichwertiger Authentifizierungsdienst genutzt werde.

GPV

Bezug genommen wird auf die Revision des VRG und betreffend das Inkrafttreten auf die Stellungnahme des GPV in der Vernehmlassung vom 29. Februar 2024 zum VE-VeVV verwiesen. Festgestellt wird, dass der Authentifizierungsdienst gemäss § 7 VE-Gesetz über digitale Basisdienste von entscheidender Bedeutung zum Vollzug der VRG-Änderungen sei. Der GPV geht davon aus, dass die dazu relevanten Basisdienste des Kantons rechtzeitig bereitgestellt würden.

VZS

Bezug genommen wird auf die Revision des VRG und betreffend das Inkrafttreten auf die Stellungnahme des VZS in der Vernehmlassung vom 11. März 2024 zum VE-VeVV verwiesen. Festgestellt werde, dass der Authentifizierungsdienst gemäss § 7 VE-Gesetz über digitale Basisdienste von entscheidender Bedeutung zum Vollzug der VRG-Änderungen sei. Der GPV gehe davon aus, dass die dazu relevanten Basisdienste des Kantons rechtzeitig bereitgestellt werden.

ZHK

Es erscheine wichtig, dass für eine rechtssichere Interaktion mit öffentlichen Organen die Identität der Nutzerinnen und Nutzer in angemessener Qualität nachweisbar sei. Der vorgeschlagene Authentifizierungsdienst des Bundes AGOV sei hierzu eine Lösung. Falls dieser Authentifizierungsdienst aber in der Umsetzungsphase als nicht zweckmässig erscheine, solle der Kanton für die öffentliche Verwaltung auch andere Authentifizierungsdienste nutzen können. Die ZHK fasst sodann die «kann» Formulierung in § 7 so auf, dass der Kanton den

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Authentifizierungsdienst des Bundes nutzen könne, aber auch andere, falls dies angemessen erscheine. UZH Auch andere Authentifizierungsdienste sollten zulässig sein. Öffentliche Organe sollten in keinem Fall dazu gezwungen werden, einen Authentifizierungsdienst des Bundes verwenden zu müssen. Die gemäss RRB und erläuterndem Bericht verlangte «einheitliche Authentifizierungslösung des Bundes » sei aktuell für den gesamten Hochschulbereich nicht geeignet, da die Schweizer Hochschulen bereits seit vielen Jahren eine gemeinsame standardisierte Identifizierungs- und Authentifizierungslösung über die gemeinsame Stiftung SWITCH realisiert hätten. Im Gesundheitssektor (Spitäler, Spitex-Organisationen, Arztpraxen) habe sich die Authentifizierungslösung von HIN (Health Info Net) durchgesetzt. Die gesetzliche Regelung der Verwendung einer heute (noch nicht) existierenden Lösung des Bundes solle aus dem Gesetz gestrichen werden oder eindeutig als Kann-Formulierung aufgenommen werden, da die Kosten der Bundeslösung und die damit verbundenen technischen Limiten noch nicht bekannt seien und der Umbau von bisher bewährten Lösungen auf eine neue, noch unbekannte Lösung des Bundes unnötigen Aufwand auslösen und bereits getätigte Investitionen vernichten würde. Neben dem Authentifizierungsdienst des Bundes seien auch andere anerkannte bzw. breit etablierte Authentifizierungsdienste (wie bspw. SWITCH, HIN) zuzulassen. Finanzkontrolle des Kantons Zürich Im Sinne der wirtschaftlichen Entwicklung sollten Doppelspurigkeiten im Bereich der Login-Lösungen so tief wie möglich gehalten werden. Entsprechend solle wo immer möglich auf die Bundesauthentifizierungslösung abgestützt werden. Damit werde die Nutzung für die Bevölkerung und Unternehmen vereinheitlicht und somit vereinfacht. «Kann» sei daher mit «soll» zu ersetzen.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
Datenbearbeitung § 8. [1] Das öffentliche Organ kann im Rahmen einer elektronisch angebotenen Leistung folgende Personendaten über den Authentifizierungsdienst des Bundes anfordern: 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 die Vertrauensstufe fest, die im Rahmen der elektronisch angebotenen	<u>SP Kanton Zürich</u> § 8 sei zu ergänzen mit einem Absatz 4: «Insbesondere das Geschlecht, die Nationalität und der Geburtsort sollten nur dann angefordert werden, wenn sie zwingend notwendig sind für die Ausübung einer Tätigkeit.» Es handle sich bei demografischen Informationen um besonders sensible Daten, die zusätzlich geschützt werden sollten. <u>SVP Kanton Zürich</u> Die Aufzählung der Personendaten sei passend. <u>Finanzkontrolle des Kantons Zürich</u> Eine abschliessende Auflistung auf Gesetzesstufe sei in Anbetracht der technologischen Entwicklung nicht sinnvoll. Zudem würde eine solche abschliessende Aufzählung in Zukunft potenziell Innovationen erschweren. Die Aufzählung sei zu entfernen.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
Leistung erforderlich ist. [3] Es fordert nur diejenigen Personendaten gemäss Abs. 1 an, die für die jeweilige Vertrauensstufe erforderlich sind.	
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.	GRÜNE Kanton Zürich Die klare Regelung der Verantwortlichkeiten sei begrüssenswert, da zielführend, um die Einhaltung der Informationssicherheit und des Datenschutzes zu gewährleisten.
B. Zugang zu elektronisch angebotenen Leistungen	
Webzugang	Gemeinde Winkel Die Kommunen seien direkt von dieser Möglichkeit betroffen, weshalb auch ihre Bedürfnisse mitberücksichtigt werden müssten. Insofern sei eine Zusammenarbeit auch in diesem Bereich mit egovpartner anzustreben und die

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

Koordination mit den Gemeinden/Städten im Gesetz zu verankern. Ausserdem sollten auch die Gemeinden bzw. Städte einen zentralen Zugang zu elektronisch angebotenen Leistungen der jeweiligen Kommune ermöglichen dürfen. Entsprechend sei diese Möglichkeit im Gesetz zu ergänzen.

ZHK

Mit dem Gesetz über digitale Basisdienste solle keine Pflicht für die öffentlichen Organe eingeführt werden, ihre (elektronischen) Leistungen auch über DigiBasis anbieten zu müssen. Entsprechende Vorgaben hierfür ergäben sich gemäss dem erläuternden Bericht des Regierungsrats zum Vorentwurf aus dem Verfahrensrecht sowie nach Massgabe der Fachgesetzgebung. Die Stärke der Umsetzung dieses Gesetzes werde sich an der Einfachheit, aber auch am Umfang der elektronisch angebotenen Leistungen messen. Es sei daher wünschenswert, dass in einem zweiten Schritt die Gemeinden und weitere öffentliche Organe aufgefordert würden, möglichst viele Leistungen auch elektronisch anzubieten. Dies solle den Gemeinden und den weiteren öffentlichen Organen auch einen Anreiz geben, noch nicht elektronisch zugängliche Dienstleistungen mittels der neu geschaffenen Plattform elektronisch anzubieten.

UZH

Es stelle sich die Frage, ob der Kanton mit dem geplanten Webzugang über das kantonale Konto auch Zugang zu elektronisch angebotenen Leistungen der selbständigen Anstalten (wie bspw. der Universität) zur Verfügung stellen wolle. Gemäss Formulierung im Vorentwurf «ermöglicht der Kanton … einen zentralen Zugang zu elektronisch angebotenen Leistungen der öffentlichen Organe». Wie bereits ausgeführt, habe die Universität bereits bestehende digitale Portale und Dienstleistungen. Diese dürften durch zusätzliche Vorgaben und Anbindungsvorgaben nicht tangiert werden. Beantragt wird daher eine Ausnahme für die selbständigen Anstalten.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
§ 10. [1] Der Kanton ermöglicht Nutzerinnen und Nutzern einen zentralen Zugang zu elektronisch angebotenen Leistungen der öffentlichen Organe.	SP Kanton Zürich § 10 sei zu ergänzen mit einem Absatz 4: «Insbesondere das Geschlecht, die Nationalität und der Geburtsort sollten nur dann angefordert werden, wenn sie zwingend notwendig sind für die Ausübung einer Tätigkeit.» Es handle sich bei demografischen Informationen um besonders sensible Daten, die zusätzlich geschützt werden sollten. SVP Kanton Zürich Ein öffentlicher und zentraler Zugang sei sehr wichtig, um die Digitalisierung geordnet weiter zu bringen. Demokratische Jurist*Innen Zürich Es solle unterschieden werden zwischen Nutzerinnen und Nutzern, die im eigenen Namen die Basisdienste benutzten und professionellen Vertreterinnen und Vertretern bzw. privaten Personen, Beratungsstellen usw., die Nutzerinnen und Nutzer unterstützten. Berufsmässig auftretenden Personen sollten sich nicht mit ihrem privaten Login einloggen müssen. Gleichzeitig müsse gewährleistet werden, dass sie nicht das Login der Nutzerinnen und Nutzer benötigten, um sich einzuloggen zu können, da sonst die Gefahr bestehe, dass über den Vertretungsumfang hinaus über den zentralen Webzugang weitere Daten eingesehen und Dienste in Anspruch genommen werden könnten. Ansonsten bestünde einerseits eine Missbrauchsgefahr; anderseits müssten die verschiedenen Zugänge auch aus praktischen Gründen klar voneinander getrennt werden. Digitale Gesellschaft Gemäss dem erläuternden Bericht sei davon auszugehen, dass die öffentlichen Organe ihre Leistungen künftig vermehrt auch oder unter Umständen – gestützt auf entsprechende rechtliche Grundlagen – ausschliesslich elektronisch zur Verfügung stellen würden. Diese grundsätzliche Absicht der Digitalisierung des

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Verwaltungswesens wird befürwortet. Dieser Prozess müsse allerdings stets nachhaltig ausgestaltet und auf die Inklusion aller potentiellen Nutzerinnen und Nutzer der digitalen Basisdienste ausgerichtet sein. Das vorliegende Vorhaben gehe zu weit, weil dadurch verschiedene Personengruppen vom Zugang zum Recht und zu staatlichen Leistungen ausgeschlossen würden, wodurch verfassungsmässige Rechte (Art. 8 Abs. 2 BV – Diskriminierungsverbot, Art. 29 Abs. 2 BV – Anspruch auf rechtliches Gehör) verletzt würden. Auch für Personen, die nicht über ein eigenes Endgerät mit Internetzugang oder das nötige IT-Knowhow verfügten, solle ein niederschwelliger Zugang zu den (elektronisch angebotenen) Leistungen der öffentlichen Organe gewährleistet werden. Sei dies nicht möglich, müsse die Leistung des öffentlichen Organs auch auf nicht elektronischem Weg angeboten werden. VZGV Der Einbezug der Gemeinden und Städte sei sicherzustellen. Für die Entwicklung und Weiterentwicklung von digitalen Leistungen sollten paritätisch zusammengesetzte Gremien eingesetzt werden. Da Gemeinden und Städte direkt betroffen und vielfach für die Umsetzung verantwortlich seien, sollten sie angemessen einbezogen werden.
2 Die Staatskanzlei betreibt hierzu einen Webzugang zu elektronisch angebotenen Leistungen der öffentlichen Organe.	Finanzkontrolle des Kantons Zürich Die Aufgabenzuordnung zur Staatskanzlei erkläre sich aus der Tatsache, dass die Staatskanzlei eine wesentliche Funktion im Rahmen der digitalen Transformation einnehme. Aus Sicht der Finanzkontrolle stelle sich jedoch die Frage, ob diese Aufgabenzuordnung auch in einem Regelbetrieb sinnvoll bleibe. GRÜNE Kanton Zürich Es müsse nicht auf Gesetzesstufe geregelt werden, welche kantonale Stelle den Webzugang betreibe: «Der Kanton betreibt» anstatt «Die Staatskanzlei betreibt».

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
3 Öffentliche Organe können ihre elektronisch angebotenen Leistungen über den Webzugang zur Verfügung stellen.	SP Kanton Zürich Änderungsvorschlag «Öffentliche Organe ~~können~~ müssen ihre elektronisch angebotenen Leistungen über den Webzugang zur Verfügung stellen.» Zudem seien neue Absätze 4 bis 7 zu ergänzen: — Neuer Absatz 4: Der Webzugang muss für die meist verbreiteten und genutzten Gerätearten (insbesondere PC als auch Mobile) optimiert sein. — Neuer Absatz 5: Die Barrierefreiheit der Basisdienste gemäss den neusten Barrierefreiheitsstandards muss gewährleistet werden. — Neuer Absatz 6: Der Webzugang muss auch in leichter Sprache zugänglich sein. — Neuer Absatz 7: Der Webzugang muss mittels normalen Webprotokollen und -clients möglich sein. Es dürfen keine proprietären Erweiterungen zur Nutzung notwendig sein. Es bestehe eine Kluft in der Verbreitung von PCs im Vergleich zu Smartphones. Viele Personen aus ärmeren Milieus besässen keinen PC, aber ein Smartphone. Umgekehrt gebe es auch Menschen, die einen PC bedienen könnten, aber kein Smartphone. Im Sinne der Bekämpfung der digitalen Kluft müsse der Webzugang daher sowohl für Mobile als auch für PC optimiert sein. Barrierefreiheit und leichte Sprache ermöglichten möglichst grossen Teilen der Gesellschaft die Nutzung der Basisdienste. DJZ Bei den Erläuterungen zu § 10 Abs. 1 werde erklärt, dass die staatlichen Organe ihre Leistungen unter Umständen (bei entsprechender gesetzlicher Grundlage) ausschliesslich auf elektronischem Weg anbieten könnten. Diese Absicht gehe zu weit, da sie verschiedene Personengruppen vom Zugang zum Recht ausschliessen würde und damit Verfassungsrecht (Diskriminierungsverbot (Art. 8 Abs. 2 BV), rechtliches Gehör (Art. 29 Abs. 2 BV)) verletzen würde. So begrüssenswert die Digitalisierung sei, bestehe auch die Gefahr, dass viele Personengruppen

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	heute und auch noch in absehbarer Zukunft vom Zugang zu den Diensten ausgeschlossen wären, würden diese ausschliesslich digital angeboten. Hinzu komme, dass im vorliegenden Gesetz auch die Sperrung (§ 14) und die Löschung (§ 15) des Zugangs vorgesehen seien. Auch diese Personen wären dann (zumindest temporär) vom Zugang zu den Leistungen der staatlichen Organe ausgeschlossen. Es genüge nicht, dass dafür unter Umständen eine weitere gesetzliche Grundlage nötig sein könnte. Es sei ein neuer Absatz 4 einzufügen: «Sämtliche Leistungen der öffentlichen Organe werden auch auf nicht elektronischem Weg angeboten.» Finanzkontrolle des Kantons Zürich «Können» sei durch «sollen» zu ersetzen.
Inhalt § 11. Die Nutzerin oder der Nutzer kann über den Webzugang: a. elektronische Verfahrenshandlungen nach dem Verwaltungsrechtspflegegesetz vom 24. Mai 1959 vornehmen, b. sich zum Abruf bereitstehende Anordnungen und Mitteilungen der öffentlichen Organe in einer Übersicht anzeigen lassen, c. Statusänderungen in Geschäftsvorgängen	DJZ Lit. d: Unterschiedliche Personengruppen hätten keine Möglichkeit, die digitalen Basisdienste zu nutzen. Sei es, weil es ihnen technisch nicht möglich sei (bspw. fehlende Ressourcen, Illettrismus, Fremdsprachigkeit) oder weil sie sich nicht hinreichend als Nutzer und Nutzerinnen identifizieren könnten (ausländische Personen ohne Aufenthaltsrecht, Personen ohne festen Wohnsitz, Personen in einer geschlossenen Institution etc.). Diesen Personen stünden heute u.a. Beratungsstellen oder private Freiwillige zur Seite. Es müsse eine Möglichkeit vorgesehen werden, dass diese Personen über Drittpersonen Zugang zu den Basisdiensten erhielten, ohne dass die Nutzerin oder der Nutzer online in den Basisdienste eine Berechtigung erteilen müsse, da ihr das Erteilen einer Berechtigung aus den oben genannten Gründen u.U. gerade nicht möglich sei. Neben diesen niederschwelligen Hilfeleistungen gebe es eine Reihe von Berufsmenschen, die Nutzerinnen oder Nutzer verträten (Anwältinnen und

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
einsehen sowie Benachrichtigungen hierzu einrichten und verwalten und d. eine andere Nutzerin oder einen anderen Nutzer zur Vornahme von Handlungen im Rahmen einer elektronisch angebotenen Leistung berechtigen.	Anwälte, Beratungsstellen). Auch hier müsse gewährleistet sein, dass Nutzerinnen und Nutzer professionell vertreten werden könnten, ohne dass sie im System der bevollmächtigten Person eine Berechtigung erteilen müssten. Es müsse eine Regelung erlassen werden, mit welcher Rechtsanwältinnen und Rechtsanwälte, Beratungsstellen oder Private sich für Nutzerinnen und Nutzer einloggen und in deren Namen und mit deren Vollmacht die digitalen Basisdienste verwenden könnten. Stadt Zürich Lit. c: Benachrichtigungskanäle sollten nicht auf SMS und E-Mail beschränkt sein, sondern auch moderne Kanäle wie Apps, oder Push-Mitteilungen berücksichtigen. Dies solle aus den Erläuterungen klar hervorgehen. UZH Lit. a: Die selbständigen Anstalten (z.B. Universität) würden die elektronischen Verfahrenshandlungen über eigenständige Plattformen zur Verfügung stellen, sobald das Gesetz in Kraft ist. Es wird davon ausgegangen, dass dies auch in Zukunft so möglich bleibe. Finanzkontrolle des Kantons Zürich Nachfolgende Aspekte seien entweder im Gesetz oder in eine Verordnung aufzunehmen: Die Pflege der eigenen Daten sollte, wo möglich und sinnvoll, über den Webzugang ermöglicht werden. Es sollte möglich sein, auf Belege von erledigten Geschäften zugreifen zu können und diese auch exportieren zu können, um eine persönliche Archivierung sicherzustellen. Es sollte möglich sein, die bisher physische Korrespondenz mit der Verwaltung über das gesicherte Portal abwickeln zu können.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
Anmeldung § 12. Die Anmeldung für die Nutzung des Webzugangs erfolgt über den Authentifizierungsdienst gemäss § 7.	asut (Schweizerischer Verband der Telekommunikation) Siehe die Ausführungen zu § 7. Stadt Zürich Fraglich sei, ob die Anmeldung mittels AGOV für jede Vertrauensstufe notwendig sei. Für niedrige Vertrauensstufen könnten auch alternative Authentifizierungsdienste zugelassen werden.
Datenbearbeitung § 13. Die Staatskanzlei: a. protokolliert die Anmeldungen der Nutzerinnen und Nutzer, b. bearbeitet Informationen im Webzugang, soweit dies zur Unterstützung der Nutzerinnen und Nutzer erforderlich ist.	Gemeinde Winkel Wenn auch die Kommunen den Webzugang gemäss § 10 ermöglichen können, müssten sie die Vorgaben nach § 13 ebenfalls erfüllen, weshalb neben der Staatskanzlei auch die Gemeinden zu nennen seien. Evangelisch-reformierte Landeskirche des Kantons Zürich, Katholische Kirche im Kanton Zürich Würden die Anmeldungen protokolliert, so sei auch die diesbezügliche Aufbewahrungsdauer bzw. Löschung der Daten zu regeln. Finanzkontrolle des Kantons Zürich Die Aufgabenzuordnung zur Staatskanzlei erkläre sich aus der Tatsache, dass die Staatskanzlei eine wesentliche Funktion im Rahmen der digitalen Transformation einnehme. Aus Sicht der Finanzkontrolle stelle sich jedoch die Frage, ob diese Aufgabenzuordnung auch in einem Regelbetrieb sinnvoll bleibe.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
[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.	DSB Es werde aus dem Gesetz nicht klar, wo der Unterschied zwischen den beiden Regelungen liege und weswegen es zwei verschiedene Arten des Bezugs von Daten über eine Nutzerin oder einen Nutzer brauche. Es sei in den Erläuterungen zu klären, inwiefern sich die Regelung über den Bezug von Daten in § 13 Abs. 2 von der Regelung über den Bezug von Daten in § 8 Abs. 1 unterscheide und weswegen beide Arten des Bezugs von Daten relevant seien. Sollten nicht beide Arten des Bezugs von Daten relevant sein, dann sei diese Bestimmung zu streichen.
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.	SP Kanton Zürich Ergänzung um einen neuen Absatz 4: «Die Sperrung des Webzugangs muss gemäss klar definierten begründbaren Kriterien erfolgen und in jedem Fall begründet werden. Es werden keine Deep Learning Systeme für diesen Entscheid eingesetzt. Die Entscheidung wird rein auf dem Nutzungsverhalten getroffen. Personendaten fliessen nicht in diesen Entscheid ein.» Die Sperrung eines Webzugangs sei ein einschneidender Schritt, der für die Nutzerin oder für den Nutzer verständlich sein solle. Deep-Learning-Systeme könnten in diesem Bereich zu inakzeptablen Biases führen. Finanzkontrolle des Kantons Zürich Eine Definition der Auswirkungen einer Nichtverfügbarkeit oder Sperrung bspw. auf Fristeneinhaltung und Betrieb sei aktuell noch nicht vorhanden. Daher könne die Bestimmung ergänzt werden (analog zu Art. 3 Abs. 5 EMBAG): «Die Risiken für den Datenschutz und die Informationssicherheit sowie für die Sicherheit und Verfügbarkeit von Daten und Diensten wird berücksichtigt.»

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
[2] Die Nutzerin oder der Nutzer wird über die Sperrung informiert und kann sich zur Sperrung äussern. [3] In begründeten Fällen kann der Webzugang für die Nutzerin oder den Nutzer gelöscht werden. *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: a. alle über den Webzugang eingeleiteten Geschäftsfälle abgeschlossen sind, b. alle über den Webzugang bereitgestellten oder sich in technischer Bereitstellung befindlichen Mitteilungen abgerufen worden	DJZ Grundsätzlich sei keine Pflicht vorgesehen, die digitalen Dienste zu verwenden. Deswegen müsse es möglich sein, auch bei einem laufenden Geschäft auf den nicht digitalen Weg zu wechseln, wenn dies durch die Nutzerin oder den Nutzer dem öffentlichen Organ mitgeteilt werde. Eine lit. d sei einzufügen: «oder der Nutzer oder die Nutzerin definitiv auf die Nutzung der digitalen Dienste verzichtet und stattdessen eine physische Zustelladresse angibt.» PHZH Im Zusammenhang mit der Speicherung und Archivierung von Leistungsnachweisen an einer Hochschule und der allfälligen Nachweiserbringung von erlangten Diplomen wird der Wortlaut des Vorentwurfs als problematisch angesehen. In den Erläuterungen werde zwar erwähnt, dass die im Rahmen der elektronisch angebotenen Leistung erfassten Informationen von dieser Löschung des Webzugangs nicht betroffenen seien. Die im

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
sind und c. der Webzugang nicht gesperrt ist. 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.	Gesetzestext erwähnte Vernichtung der darin enthaltenen Daten erwecke jedoch einen anderen Anschein.
Kosten und Gebühren § 16. 1 Der Kanton trägt die Kosten für den Aufbau, den Betrieb, die Unterstützung und die Weiterentwicklung des Webzugangs.	SVP Kanton Zürich Dass der Kanton zu Beginn die Kosten übernehme, sei nachvollziehbar. Es müsse jedoch sehr genau darauf geachtet werden, Kostenbewusstsein und Budgetabschätzungen einzubeziehen. Skepsis besteht gegenüber den enormen Kosten, die mit der Digitalisierung einhergingen und heutzutage kaum abzuschätzen seien. Die Kostenfolge für Gemeinden solle mit einer «Kann-Formulierung» so stehen bleiben. Gemeinde Winkel Die beabsichtigten Kosten seien vorab mit den Vertretenden der Gemeinden und Städte zu besprechen, sodass Einfluss genommen werden könne. VZGV Sollte der Regierungsrat beabsichtigen, eine Kostenbeteiligung der Gemeinden und Städte vorzusehen, seien

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	diese frühzeitig einzubeziehen. Finanzkontrolle des Kantons Zürich Ein vierter Absatz sei einzufügen: «Der Regierungsrat wird ermächtigt zur Umsetzung und Nutzung der digitalen Basisdienstleitungen Anreize zu schaffen.»
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.	GPV Die Bestimmung solle mit folgender Ergänzung angepasst werden: «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 gemäss dem Kostendeckungs- und Äquivalenzprinzip. Der Regierungsrat regelt die Einzelheiten.» Es bestehe die Möglichkeit, dass der Kanton im Bereich der Basisdienste eine Monopolstellung erhalte. Es scheine daher wichtig, im Gesetz darauf hinzuweisen, dass die Tarife im Sinne des Kostendeckungs- und Äquivalenzprinzips ausgestaltet würden. GVZ Auf eine Kostenbeteiligung der «übrigen öffentlichen Organe» sei zu verzichten und damit Abs. 2 zu streichen. Diese Bestimmung stelle ein zusätzliches Hindernis dar, dass künftig möglichst viele kantonale Stellen die gleichen digitalen Basisdienste nutzten. Katholische Kirche im Kanton Zürich Grundsätzlich wäre es sehr begrüssenswert, wenn der Kanton die Plattform, wie z.B. das Zürikonto, die ohnehin erstellt werden soll, gleich für alle kirchlichen Bedürfnisse, Verwaltungsverfahren etc. miteinplanen und allen

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	katholischen Einwohnern Zugang zum kirchlichen Bereich ermöglichen würde. Auch für die Einwohner im Kt. Zürich wäre eine einzige Plattform für alle verwaltungstechnischen Anliegen mit demselben Konto viel benutzerfreundlicher als verschiedene Konten. Eine Gebühr oder Kostenbeteiligung sei angemessen. Die technische Umsetzung in verschiedenen Sektionen (Gemeinde, Kath. Kirche, Ref. Kirche etc.) solle mitberücksichtigt bzw. miteingeplant werden, sodass der Datenschutz für sensible Personendaten dabei stets gewährleistet sei. Das sei technisch auch umsetzbar. Es erscheine unklar, was mit dem Begriff «Kostenbeteiligung» gemeint sei, d.h. ob es sich um eine Beteiligung an den Entwicklungs- und Betriebskosten handle oder um eine Benutzungsgebühr zulasten öffentlicher Organe, die den Webzugang nutzten. Dies sei zu klären durch die Verwendung der Formulierung «Beteiligung an den Kosten gemäss Abs. 1» oder «Gebühr». <u>Evangelisch-reformierte Landeskirche</u> Es erscheine unklar, was mit dem Begriff «Kostenbeteiligung» gemeint sei, d.h. ob es sich um eine Beteiligung an den Entwicklungs- und Betriebskosten handle oder um eine Benutzungsgebühr zulasten öffentlicher Organe, die den Webzugang nutzten. Dies sei zu klären durch die Verwendung der Formulierung «Beteiligung an den Kosten gemäss Abs. 1» oder «Gebühr». Allerdings trage gemäss § 16 Abs. 1 eigentlich der Kanton die Kosten, weshalb nicht einzuleuchten vermöge, weshalb und wofür die öffentlichen Organe – zu denen auch der Kanton zähle – trotzdem eine Kostenbeteiligung leisten sollten (der Kanton müsste demnach die von ihm erbrachten Leistungen sich selber vergüten). § 16 Abs. 1 und 2 scheinen sich zu widersprechen. Allenfalls sei in § 16 Abs. 1 klarzustellen, für wen der Kanton die Kosten trage.
3 Die Nutzung des Webzugangs ist für	<u>SP Kanton Zürich</u>

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
die Nutzerinnen und Nutzer kostenlos. Gebühren für die Inanspruchnahme einer elektronisch angebotenen Leistung bleiben vorbehalten.	Öffentliche Dienste sollten kostenlos genutzt werden können. Der zweite Satz führe zu einer unklaren Situation und biete Missbrauchspotenzial. Daher wird folgende Änderung vorgeschlagen: «Die Nutzung des Webzugangs ist für die Nutzerinnen und Nutzer kostenlos. [Streichung von «Gebühren für die Inanspruchnahme einer elektronisch angebotenen Leistung bleiben vorbehalten.»]
C. Digitaler Arbeitsplatz	
Informationsbearbeitung durch Dritte im Rahmen des digitalen Arbeitsplatzes	DJZ § 17 sei ersatzlos zu streichen. Cloudbasierte Dienste von Drittanbietern gewährten die hohen Sicherheitsanforderungen an die Erbringung der Leistungen staatlicher Organe nicht. Eine Auslagerung ins europäische Ausland komme aus rechtsstaatlichen und staatspolitischen Gründen unter keinen Umständen in Frage. Die Überwachung der Anbieter im Ausland sei für die Schweizer Behörden mit einem derart grossen Aufwand verbunden, dass der kleine Vorteil einer cloudbasierten Datenspeicherung nicht überwiege. Die Daten seien zwingend auf einem Server am Standort des öffentlichen Organs zu sichern. Darüber hinaus sei es unklar, wie im Rahmen der Nutzung von Microsoft 365 eine wirksame Verschlüsselung gegenüber Microsoft selbst sichergestellt werden könne. Denn es liege in der Natur der Sache, dass Microsoft als Cloud-Anbieter bei der Nutzung von cloudbasierten Anwendungen auch ohne Mitwirkung des öffentlichen Organs auf die Personendaten sowie vertrauliche oder der Geheimhaltung unterliegende Informationen zugreifen könne. Der erläuternde Bericht halte ebenfalls fest, dass ein Zugriff auf die Daten durch einen Drittstaat nicht ausgeschlossen sei. Zudem könne eine US-Behörde gestützt auf den US CLOUD Act bei Microsoft als amerikanisches Unternehmen die Herausgabe von Daten (betreffend DAP) anordnen, die Microsoft sodann unverschlüsselt dieser US-Behörde zukommen

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	lassen müsse. Als problematisch wird diesbezüglich auch erachtet, dass die USA den Dienstanbieterinnen und -anbietern, die vom US Cloud Act betroffen sind, keinen genügenden Rechtsschutz gewähre. Schliesslich sei im Gesetz auch nicht vorgesehen, was bei einem möglichen Zusammenbruch des Systems passieren solle. swissICT (Verband ICT-Werkplatz Schweiz) Die Vorgaben würden faktisch ein generelles Cloud-Verbot mit Ausnahme vollverschlüsselter Speicherdienste statuieren, was nicht angemessen sei und Cloud-Dienste von Standard-Anbietern ausschliessen würde. Die geforderten strengen Anforderungen an die Verschlüsselung gälten nicht nur bei ausländischen Providern, sondern auch alle Cloud-Provider in der Schweiz wären davon betroffen. Dies bedeute, dass auch bei Schweizer Dienstleistern mit eigenen Cloud-Lösungen besonders sensible Daten durch den Kunden verschlüsselt werden müssten, ohne Zugriffmöglichkeit durch den Schweizer Provider. § 17 gelte nicht nur für alle öffentlichen Organe des Kantons Zürich, sondern auch für alle Organisationen, die mit der Erfüllung öffentlicher Aufgaben betraut seien. Das sei ein weites Feld; es erfasse bspw. auch private Spitäler, die spitalambulante Leistungen erbrächten und einen Leistungsauftrag des Kantons hätten, private Spitexorganisationen oder bestimmte Anbieter im Bereich der Berufsbildung usw. – Funktionalitäten, welche den digitalen Arbeitsplatz ausmachten, würden in den heutzutage kommerziell angebotenen Lösungen massiv eingeschränkt oder verunmöglicht. Zum Beispiel wären Inhaltssuchen in den verschlüsselten Daten im Cloud-Dienst nach aktuellem Stand der Technik nicht mehr möglich, ebenso wie die Zusammenarbeit (Collaboration) und das parallele Arbeiten auf Dokumenten. Da die Schlüssel «nur» auf dem eigenen Notebook funktionierten, könnten Dokumente z.B. auf dem Tablet oder Mobile nicht entschlüsselt werden. Sie könnten dort deshalb weder gelesen noch bearbeitet werden (inklusive Mail). Dies schränke die Mobilität des digitalen Arbeitsplatzes ein. Die Sicherheit würde nach aktuellem Stand der Technik schlechter – nicht besser: Wichtige Schutzmechanismen (z.B. Virenscan) griffen bei verschlüsselten Dokumenten

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	nicht. Dies bedeute, dass befallene Dokumente wie z.B. Excel-Dateien mit Makros, ZIP-Dateien, Phishing-PDF etc. vom Cloud-Dienst und somit vom Schutzmechanismus nicht erkannt werden könnten. Vom Cloud-Provider in der Cloud zur Verfügung gestellte Sicherheitsfunktionen, welche ständig weiterentwickelt und aktuell gehalten würden, seien somit punktuell ausgehebelt. Lokale oder hybride Lösungen müssten dann separat geschützt werden, was riesige Sicherheitslücken hinterlasse und zu massiv höheren Kosten führen könne. Es sei unter Spezialisten und IT-Verantwortlichen in Unternehmen und Behörden breit anerkannt, dass das Niveau an Sicherheit, welches moderne Cloud-Lösungen heutzutage bereitstellen, «on-premise» nicht ohne erheblichen Zusatzaufwand erreicht werden könne. Eine solche Spezialbestimmung sei gesetzgeberisch nicht notwendig. Für die Einführung von Cloud-Lösungen im Bereich des digitalen Arbeitsplatzes müssten keine Rechtsgrundlagen geändert oder neu geschaffen werden. Zudem basierten die in § 17 vorgeschriebenen technischen Einschränkungen auf einer umstrittenen und in der Lehre nicht vorherrschenden Rechtsauffassung. Die Bestimmung sei ersatzlos aus dem Gesetzesentwurf zu streichen. Digitale Gesellschaft Es sei unklar, wie bei der Nutzung der Anwendungen von Microsoft eine wirksame Verschlüsselung auch gegenüber Microsoft gewährleistet werden solle. Denn es liege in der Natur der Sache, dass Microsoft (Cloud-Anbieterin) bei der Nutzung von cloudbasierten Anwendungen auch ohne Mitwirkung des öffentlichen Organs auf die Personendaten sowie vertrauliche oder der Geheimhaltung unterliegende Informationen zugreifen könne. Der erläuternde Bericht halte fest, dass ein Zugriff auf die Daten durch einen Drittstaat nicht ausgeschlossen sei. Es könne allerdings zumindest eine physische Beschlagnahmung der Server unter Umgehung der Rechtshilfe verhindert werden. Dies sei unzutreffend, da einerseits eine US-Behörde gestützt auf den US CLOUD Act bei Microsoft als amerikanisches Unternehmen die Herausgabe von Daten (betreffend DAP) anordnen könne und

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Microsoft diese Daten sodann unverschlüsselt dieser US-Behörde zukommen lassen müsse. Problematisch sei, dass die USA den Dienstanbieterinnen und -anbietern, die vom US Cloud Act betroffen seien, keinen genügenden Rechtsschutz gewährten. Ausserdem gelte in der EU ab 2026 das e-Evidence-Paket. Es könne nicht ausgeschlossen werden, dass Cloud-Anbieterinnen vom Anwendungsbereich des e-Evidence-Pakets (siehe Bericht zur e-Evidence-Vorlage des BJ, Kapitel 2.3.2.3) erfasst seien. Sofern dies der Fall sei, könnten ab 2026 auch Behörden von EU-Mitgliedsstaaten von Cloud-Anbieterinnen, die sich in der EU befinden, die Herausgabe von Daten beantragen. Da Microsoft auch Niederlassungen in der EU habe, müsse die Anordnung auch in diesem Fall befolgt werden, d.h. die unverschlüsselten Daten müssten an die EU-Behörde übermittelt werden. § 17 sei dahingehend zu ändern, dass öffentliche Organe die Bearbeitung von Informationen nur an Cloud-Anbieterinnen übertragen könnten, bei denen technisch und rechtlich sichergestellt sei, dass ausländische Behörden nicht unter Umgehung der Rechtshilfe auf Personendaten sowie vertrauliche oder der Geheimhaltung unterliegende Informationen zugreifen könnten. <u>Privatperson A</u> § 17 VE-Gesetz über digitale Basisdienste sei ersatzlos zu streichen, da die verlangte End-to-End-Verschlüsselung weder rechtlich nötig noch praktikabel sei. Auch die meisten reinen Schweizer Anbieter würden die Anforderungen von lit. a nicht erfüllen können. Die technischen Ausführungen in den Erläuterungen machten den Eindruck, dass sie auf Missverständnissen beruhten. Technische Ausführungen seien nicht auf Gesetzesstufe zu verankern. Nicht sauber oder sinnvoll definierbare Begriffe wie «cloudbasiert» oder «Cloud-Anbieterin» seien nicht in einen Erlass aufzunehmen, da es sich hierbei um Auslagerungen von IT-Leistungen an ein privates Unternehmen handle. § 17 adressiere einzig das Risiko eines ausländischen Behördenzugriffs, wenn die Bearbeitung von dem Amtsgeheimnis unterliegenden Daten ins Ausland übertragen werde. Wenn also dieses

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Thema in irgendeiner Weise geregelt werden solle, dann solle die Regelung genau darauf beschränkt werden. Namentlich die Position der Datenschutzbeauftragten des Kantons Zürich, wonach Daten selbst dann vollumfänglich geschützt sein müssten, wenn sich die Anbieterin nicht mehr an den Vertrag halte, überzeuge nicht. Die Anforderungen eines Double-Key-Encryption-Verfahrens für M365 biete eine theoretische Lösung für einzelne Inhalte, führe aber zu massiven funktionalen Einschränkungen. In der Praxis werde es so gut wie nie eingesetzt. Es sei bisher ohne externe Verschlüsselung oder DKE nicht möglich, M365 so zu betreiben, dass Microsoft sich technisch keinen Zugang zum Schlüssel verschaffen könne. Die Systeme von Microsoft müssten in der Lage sein, die Inhalte zu entschlüsseln, damit sie damit arbeiten könnten: Microsoft könne sich, wenn sie denn wolle oder müsse, immer Zugang zu den Daten im Klartext verschaffen, auch ohne, dass das Organ zustimme. Dem US CLOUD Act werde bei fehlender End-to-End-Verschlüsselung im Fall von M365 (und in anderen Fällen) dadurch entgegengetreten, dass mit besonderen Massnahmen die US-Muttergesellschaft von Microsoft Irland (dem Vertragspartner des Kantons Zürich) in die Lage versetzt werde, die Herausgabe von Daten an US-Behörden trotz technischem Zugriff verweigern zu können. Das US-Recht biete solche Handhabe; die End-to-End-Verschlüsselung sei also nicht der einzige Schutz. Das Gutachten Schefer/Glass habe dies übersehen. Diese anderen Schutzmassnahmen lägen der entwickelten Beurteilungsmethode «Rosenthal» zugrunde, die der Regierungsrat zum Standard für den Kanton erklärt habe. Solle das Thema des ausländischen Behördenzugriffs vernünftig geregelt werden, dann solle § 3 des Gesetzes über die Auslagerung von Informatikdienstleistungen durch eine entsprechende Regelung ersetzt werden. Sie solle die Auslagerung an private Unternehmen nur aber immerhin dann erlauben, wenn aufgrund der getroffenen technischen und organisatorischen Massnahmen ein angemessener Schutz vor unbefugter Einsichtnahme, Veränderung oder Verlust bestehe und insbesondere «kein Grund zur Annahme» bestehe, dass eine

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	ausländische Behörde auf die dem Amtsgeheimnis unterliegenden Informationen des öffentlichen Organs zugreifen werde. Es gebe keinen Grund, eine separate Regelung der Auslagerung von Informatikleistungen für digitale Arbeitsplätze zu treffen. Es sei jetzt eine gute Gelegenheit, die in die Jahre gekommene Regelung im Gesetz über Auslagerung von Informatikdienstleistungen an heutige Verhältnisse anzupassen. Damit wäre Rechtssicherheit gewonnen, und die Diskussion könnte sich auf die tatsächlichen Herausforderungen von «Cloud-Diensten» fokussieren. Unternehmen B Der enge Fokus des Erläuterungsberichts auf Double Key Encryption (DKE) scheine vor allem das Ziel zu haben, den gesetzesmässigen Zugriff von ausländischen Strafbehörden auf Daten zu verhindern, wenn sich diese in der Obhut der Cloud Anbietern befänden. Treffe dies zu, dann lasse diese Argumentation die Tatsache ausser Acht, dass ein derartiges Szenario äusserst unwahrscheinlich sei. Dies lasse sich anhand der Evidenz erkennen, welche verschiedene Cloud-Anbieterinnen betreffend die Zahl solcher Zugriffe veröffentlichten. Nach vorne gerichtet verpflichte sich Microsoft heute vertraglich, in jedem Fall und ohne Ausnahme, Schweizer Recht zu respektieren, sollte sie mit der Anfrage einer nicht-europäischen Regierung zur Datenherausgabe konfrontiert sein. Deshalb sei zumindest die Frage aufgeworfen, ob die sehr restriktive Form der DKE und die damit einhergehenden Einschränkungen verhältnismässig seien zur Kontrolle eines Risikos, dessen Eintrittswahrscheinlichkeit äusserst klein sei. Dies insbesondere, da es konkrete und bewährte Alternativen gebe, die in der Praxis von Organen mit höchsten Ansprüchen an die Datensicherheit erfolgreich eingesetzt würden. Unternehmen C Die Bestimmung adressiere primär ein Problem: den Zugriff auf Behördendaten durch einen fremden Staat. Der

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Vorschlag lasse einen ganzheitlichen Ansatz einer Datensicherheits-Governance vermissen. Datensicherheit in der Cloud sei mehr als das Risiko eines Zugriffes durch einen fremden Staat; der Vorschlag lasse einen risikobasierten Ansatz in seiner Gesamtheit vermissen. § 17 sei nicht technologieneutral formuliert – die Verschlüsselung solle als einzige technische Massnahme implementiert werden; mit dem Fokus auf eine Massnahme würden operative und sicherheitstechnische Risiken geschaffen. In den meisten Fällen würden die öffentlichen Organe nicht in der Lage sein, die geforderte Massnahmen selbst umzusetzen (Schlüssel-Management sei sehr anspruchsvoll) und es sei absehbar, dass dadurch neue Abhängigkeiten geschaffen würden. Die Verschlüsselung werde ein kollaboratives Zusammenarbeiten wesentlich erschweren. § 17 schaffe neue Sicherheitsrisiken (z. B. aufgrund unzureichender Anomaliedetektion und fehlendem Know-how beim öffentlichen Organ). Insgesamt würden dadurch Mehrkosten beim IT-Betrieb geschaffen, ohne wesentlichen Mehrwert bei der Datensicherheit. Es gebe keine gesetzgeberische Notwendigkeit für § 17. Der Regierungsrat habe mit dem Beschluss vom 30. März 2022 (RRB Nr. 542/2022) klargestellt, dass für die Implementierung von Cloud-Lösungen wie Microsoft 365 keine neuen rechtlichen Grundlagen geschaffen werden müssten. Die bestehenden Vorschriften seien ausreichend und würden bereits von zahlreichen Städten und Gemeinden im Kanton sowie weiteren öffentlichen Organen bei der Umsetzung digitaler Arbeitsplätze rechtskonform genutzt. Eine gesonderte technische Anleitung durch ein Gesetz sei demnach nicht erforderlich. § 17 stelle einen unrechtmässigen Eingriff in die Autonomie der Gemeinden und weiteren öffentlichen Organe dar und könne die notwendige Digitalisierung behindern. Änderungen der rechtlichen Grundlagen seien für den DAP durch öffentliche Organe nicht erforderlich. Eine starre Regelung verhindere organisationsgerechte Sicherheit. Die Argumentation des § 17 basiere auf einer übertriebenen Risikowahrnehmung. Es werde ein einzelnes (nota

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	bene unbestritten äusserst niedriges) Risiko hochstilisiert, indem behauptet werde, dass US-Cloud-Anbieter auf Anfrage sämtliche Daten jederzeit und uneingeschränkt an US-Behörden weitergäben. Dies sei irreführend. Microsoft verpflichte sich in ihren Verträgen zu umfangreichen Kontroll- und Schutzmassnahmen gegen eine solche Datenweitergabe, die sich in der Praxis als effektiv erwiesen hätten. Mit einem Hosting der Daten (data at rest) in der Schweiz seien die Daten in der Schweiz gespeichert. Zusätzlich sei mit der Lokalisierung der Cloud Services, welche ebenfalls in der Schweiz möglich sei und so vertraglich verlangt werden könne, auch die Prozessierung der Daten in der Schweiz durchsetzbar. Keine Behörde erhalte einen direkten, pauschalen oder uneingeschränkten Zugriff auf die Daten. Vielmehr wären zuerst zwischenstaatliche Rechtsverfahren notwendig, um eine Datenherausgabe zu verlangen. § 17 fokussiere einseitig auf den Zugriff durch ausländische Behörden über Cloud-Anbieter. Vernachlässigt würden dabei grössere Risiken. Sicherheitsmassnahmen würden fehlinterpretiert. Die Gesamtsicherheit digitaler Arbeitsplätze sei unzureichend berücksichtigt. Statt die Aufmerksamkeit auf ein vergleichsweise geringes Risiko zu richten, wäre es effektiver, die öffentlichen Organe bei der Umsetzung von einer ganzheitlichen Datensicherheits-Governance zu unterstützen. Diese würde alle relevanten Sicherheitsaspekte berücksichtigen und die Risiken wirkungsvoller adressieren. § 17 berge operative und sicherheitstechnische Risiken und dies zu massivem Zusatz. § 17 sehe eine umfassende «end-to-end»-Verschlüsselung für sensible Daten vor. Diese Anforderung sei für Plattformen wie Microsoft 365 weder passend noch notwendig, führe jedoch zu erheblichen operationellen und sicherheitstechnischen Zusatzrisiken sowie zu stark erhöhten Kosten. Verschiedene Kantone und öffentliche Einrichtungen hätten die im Erläuterungsbericht vorgeschlagenen Eigenverschlüsselungsmethoden und Gateway-Lösungen geprüft und verworfen. Die Gründe lägen in den

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	beträchtlichen operativen Aufwänden und den erheblichen zusätzlichen Betriebsrisiken sowie den grösseren Einbussen bei Funktionalität und Sicherheit. Es sei vorhersehbar, dass die meisten öffentlichen Organe nicht in der Lage sein würden, eigene Verschlüsselungsinfrastrukturen zu implementieren oder zu betreiben, hauptsächlich aufgrund fehlenden Fachwissens. Dies zeige sich schon darin, dass bereits heute Defizite in der IT-Sicherheit-Organisation bei vielen Organen bestünden. Viele Beteiligte hätten bereits heute Probleme, die «zumutbaren organisatorischen, technischen und vertraglichen Massnahmen zur Minimierung der Risiken» zu definieren. Die Gesetzgebung solle sich eher auf Risk Governance, das Risikomanagement insgesamt und die Etablierung von Know-how konzentrieren. Dies würde effektiver dazu beitragen, relevante Risiken zu adressieren und die Sicherheit mit dem Mindset «Zero Trust» zu erhöhen, als einseitig die Implementierung von Verschlüsselungstechnologien durch öffentliche Organe zu fordern. Neue Abhängigkeiten würden geschaffen, da die meisten öffentlichen Organe nicht über die nötigen Ressourcen oder das erforderliche Know-how verfügten, um die geforderte Verschlüsselung eigenständig zu verwalten. Daraus resultiere die Notwendigkeit, auf Drittanbieter für den Betrieb einer ausgelagerten Verschlüsselungsinfrastruktur zurückzugreifen. Diese Abhängigkeit von externen Anbietern führe zu finanziellen Mehrkosten und schaffe neue Sicherheitsrisiken. Ein zusätzlicher Anbieter, der überwacht werden müsse, stelle einen weiteren potenziellen Angriffspunkt für Hacker dar. Der Fall Xplain habe die damit verbundenen Risiken deutlich gemacht. Er habe auch nochmals aufgezeigt, dass schlussendlich das öffentliche Organ verantwortlich bleibe und jeden Anbieter überwachen müsse. Vor und während der Benutzung des Services müssten durch das öffentliche Organ geeignete Kontrollen fortwährend geprüft werden und bei Verletzung durch das öffentliche Organ Sanktionen durchgesetzt werden. Die Überwachung dieser Drittanbieter sei keineswegs trivial und gerade bei kleineren

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

öffentlichen Organen oft durch Budgetbeschränkungen limitiert. Zudem sei zu erwarten, dass bei einer Annahme dieser Gesetzgebung nur eine begrenzte Anzahl von Anbietern solche Schlüsselmanagementlösungen offeriert würden. Das berge das Risiko, dass wenige Anbieter plötzlich die Schlüssel für eine Vielzahl von öffentlichen Organen im Kanton Zürich verwalteten, was sie zu einem attraktiven Ziel für Angriffe mache.

Die strengen Anforderungen an die Verschlüsselung gälten nicht nur bei ausländischen Providern, sondern auch alle Cloud-Provider in der Schweiz wären davon betroffen. Dies bedeute, dass auch bei Schweizer Dienstleistern sowie öffentlichen Organen mit eigenen Cloud-Lösungen besonders sensible Daten durch den Kunden verschlüsselt werden müssten, ohne Zugriffmöglichkeit durch diese Schweizer Provider. Damit statuiere § 17 ein generelles Cloud-Verbot, mit Ausnahme vollverschlüsselter Speicherdienste. Die obligatorische Verschlüsselung aller in der Cloud gespeicherten Dokumente und Informationen würde die Nutzbarkeit von Cloud-Diensten, wie beispielsweise jenen von Microsoft (z.B. Teams), erheblich einschränken. Selbst wenn nur besonders schützenswerte Inhalte verschlüsselt würden, blieben viele wesentliche Cloud-Funktionen auf diesen Inhalten unanwendbar. Verschlüsselte Dokumente in der Cloud seien für wichtige Sicherheitsmechanismen, wie Virenscans, nicht zugänglich. Infizierte Dateien, beispielsweise Excel-Dokumente mit Makros, ZIP-Dateien oder Phishing-PDFs, würden von den Schutzmechanismen der Cloud-Dienste nicht erkannt. Sicherheitsfunktionen, die von Cloud-Anbietern wie Microsoft 365 bereitgestellt und kontinuierlich weiterentwickelt würden, könnten ohne Lösungen am Endpoint so umgangen werden. Lokale oder hybride Lösungen müssten daher separat geschützt werden, was erhebliche Aufwände mit sich bringe. Ausserdem bestehe ein hohes Risiko, dass Mitarbeitende sogenannte Schatten-IT vermehrt nutzen würden, weil sie auf die modernen Arbeitsmittel nicht verzichten wollten.

<u>Gemeinde Dietlikon</u>

Die Rechenzentren sollten sich aus Sicherheitsgründen nur in der Schweiz und nicht auch in der EU befinden

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	müssen. Gemeinde Eglisau Die rechtliche Notwendigkeit und Praktikabilität von § 17 VE-Gesetz über digitale Basisdienste sei erneut zu prüfen. Eine praxisorientierte Lösung sei anzustreben, sodass bisherige Anwendungen, Software- und Cloudlösungen weiterhin genutzt werden könnten. Gemeinde Gossau § 17 VE-Gesetz über digitale Basisdienste sei ersatzlos zu streichen. Er basiere auf falschen (rechtlichen wie faktischen) Annahmen, sei gesetzgeberisch weder notwendig noch hilfreich, berge operative und sicherheitstechnische Risiken, führe zu massiv höheren Kosten, zementiere eine umstrittene, parteiische und unzureichend begründete Rechtsauffassung, gefährde die dringend notwendige Digitalisierung der Behörden (wie auch von Privaten), statuiere faktisch ein Cloud-Verbot (auch für Schweizer Anbieter) und behindere Innovationen und den Aufbau von Know-how. Gemeinde Pfäffikon Verwiesen wird auf eine auf den 28. März 2024 datierte Stellungnahme zur Vernehmlassung «Nein zum unnötigen und schädlichen § 17 (Cloud-Nutzung beim digitalen Arbeitsplatz»). § 17 VE-Gesetz über digitale Basisdienste sei ersatzlos zu streichen. Der Paragraf basiere auf falschen (rechtlichen wie faktischen) Annahmen, sei gesetzgeberisch weder notwendig noch hilfreich, berge operative und sicherheitstechnische Risiken, führe zu massiv höheren Kosten, zementiere eine umstrittene, partikuläre und schlecht begründete Rechtsauffassung, gefährde die dringend notwendige Digitalisierung der Behörden (wie auch von Privaten), statuiere faktisch ein Cloud-Verbot (auch von Schweizer Anbietern) und verhindere Innovationen und den Aufbau von Know-how.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

Gemeinde Pfungen

§ 17 sei ersatzlos zu streichen, da er weder notwendig noch hilfreich sei, weitere Unsicherheiten nach sich ziehe, operativ und sicherheitstechnische Risiken berge, zu massiv hohen Kosten führe, die dringend notwendige Digitalisierung der Behörden gefährde sowie faktisch ein Cloud-Verbot statuiere.

Stadt Wetzikon

§ 17 sei ersatzlos zu streichen. Der Regierungsrat habe die Nutzung von M365 bereits am 30. März 2022 beschlossen (RRB Nr. 542/2022). Eine gesetzliche Regelung, die insbesondere spezifische technische Voraussetzungen festlege, sei nicht notwendig. Im Weiteren brauche es keine zusätzlich spezifischen Gesetzesbestimmungen über die datenschutzrelevanten Bestimmungen hinaus.

Stadt Winterthur

Vorgebracht werden grosse Bedenken, was die Praktikabilität von § 17 des Vorentwurfs betrifft: Die Notwendigkeit des Erlasses von Vorschriften, welcher die Übertragung der Bearbeitung von Informationen an Anbieterinnen und Anbieter cloudbasierter Informatikdienstleistungen deutlich erschwere (insbesondere durch den Zwang zur Verschlüsselung von besonderen Personendaten gegenüber den Anbietenden) sei rechtlich umstritten und führe zu einem deutlichen Mehraufwand im Umgang mit solchen Lösungen. Die rechtliche Notwendigkeit der fraglichen Bestimmung sei nochmals zu prüfen und abzuwägen sowie den Bedenken bezüglich der Praktikabilität Rechnung zu tragen. Falls eine Regelung notwendig sei, sei eine Lösung vorzuschlagen, welche der bisher gelebten Praxis des Kantons Zürich und vieler Gemeinden gerecht werde.

Stadt Zürich

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Die Definition/Abgrenzung von digitalen Basisdiensten bzw. dem in § 17 VE-Gesetz über digitale Basisdienste geregelten Digitalen Arbeitsplatz (wenn denn § 17 beibehalten werden soll) zu Fachapplikationen solle in den Erläuterungen oder sogar im Gesetz geschärft werden. Gemäss Erläuterungen werde festgelegt, dass digitale Basisdienste von weiteren Begrifflichkeiten abzugrenzen seien. Zu unterscheiden sei ein Basisdienst von den darauf aufbauenden Leistungen, welche von den öffentlichen Organen über ihre (Fach-)Anwendungen (Fachapplikationen) erbracht würden und sich nach der jeweiligen Fachgesetzgebung richteten. Digitale Basisdienste unterstützten die öffentlichen Organe bei der Leistungserbringung bzw. machten die Leistungen für Nutzerinnen und Nutzer einfacher zugänglich. Es werden Fragen aufgeworfen, ob zum Beispiel eine mittels DAP erstellte PowerApp als Fachanwendung gälte und diese rechtskonform sei und ob das Städtische «Mein Konto» als ein digitaler Basisdienst zu verstehen sei. Mit dem Gesetz würden zwei Bereiche vermischt: Digitale Basisdienste und datenschutzmässig motivierte Verbote, die nicht in ein Gesetz über Digitale Basisdienste gehörten. Es sollten nur Aspekte geregelt werden, die zur direkten Erbringung von Leistungen gegenüber Privatpersonen und Organisationen notwendig seien. Regelungen, die deren technologische Umsetzung und Datenauslagerung an Dritte umfassten (Digitaler Arbeitsplatz), seien in diesem Gesetz ein Fremdkörper. GPV Grosse Bedenken beträfen die Praktikabilität von § 17 des Vorentwurfs: Die Notwendigkeit des Erlasses von Vorschriften, welcher die Übertragung der Bearbeitung von Informationen an Anbieterinnen und Anbieter von cloudbasierten Informatikdienstleistungen deutlich erschwere (insbesondere durch den Zwang zur Verschlüsselung von besonderen Personendaten gegenüber der Anbietenden) sei rechtlich umstritten und führe zu einem deutlichen Mehraufwand im Umgang mit solchen Lösungen. Die rechtliche Notwendigkeit der fraglichen Bestimmung in § 17 sei nochmals zu prüfen und abzuwägen sowie den Bedenken bezüglich der Praktikabilität

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Rechnung zu tragen. Falls eine Regelung notwendig sei, sei eine Lösung vorzuschlagen, die der bisher gelebten Praxis des Kantons Zürich und vieler Gemeinden gerecht werde. Beantragt wird folgende Änderung: «Das öffentliche Organ kann die Bearbeitung von Informationen in Anwendungen des digitalen Arbeitsplatzes an Anbieterinnen von cloudbasierten Informatikdienstleistungen übertragen, wenn sich die Nutzdaten in Rechenzentren in der Schweiz oder in der Europäischen Union befinden, und wenn: …» Mit der Änderung solle dem Umstand Rechnung getragen werden, dass bereits heute viele Gemeinden Cloud-Dienste an Microsoft ausgelagert hätten. Microsoft betreibe weltweit Rechenzentren, wobei die Microsoft-Kunden wählen könnten, dass die Nutzdaten in der Schweiz liegen müssten. Gewisse Metadaten zu Benutzer- oder Kundenidentitäten sowie Basisdienste (nicht Daten) wie beispielsweise das Systemmonitoring würden jedoch auch in den USA betrieben. Insofern dürfte die Formulierung gemäss Entwurf zu einem Ausschluss von Microsoft als Cloud-Provider führen. Ganz grundsätzlich sei es sinnvoller, im Gesetz den Datenstandort statt den Rechenzentrumsstandort einzuschränken. Stadt Zürich § 17 sei ersatzlos zu streichen. Die Regelungen zum Digitalen Arbeitsplatz seien ein Fremdkörper im Gesetz über digitale Basisdienste. Die darin enthaltenen Vorgaben seien hauptsächlich datenschützerischer Natur und sollten, wenn schon, in den entsprechenden Gesetzen geregelt werden. Der Inhalt von § 17 sei zudem höchst problematisch. Er erlaube die Übertragung von besonderen Personendaten sowie vertraulichen oder der Geheimhaltung unterliegenden Informationen an eine Cloud-Anbieterin, ob dies nun eine Schweizerische oder eine ausländische Anbieterin sei, wenn die Cloud-Anbieterin ohne Mitwirkung des öffentlichen Organs auf die Daten zugreifen könne. Um einen solchen Zugriff verhindern zu können, sei ein Schlüssel nötig, auf den nur das übertragende Organ Zugriff habe. Dadurch könnten wesentliche Cloud-Funktionalitäten, insbesondere auch die für

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	die Digitalisierungsbestrebungen so wichtigen Kollaborationsmöglichkeiten, sicherheitserhöhende Funktionalitäten (wie z.B. Virenschutz) und die Möglichkeiten zur Bearbeitung via mobiler Geräte (z.B. Handy oder Tablet) für solche Informationen nicht eingesetzt werden. Durch die nicht vorhandenen Sicherheits-Features werde die Gefährdung auch der (noch) nicht in einer Cloud betriebenen Systeme massiv erhöht, wenn solche Informationen mit eigenem Schlüssel in die Cloud übertragen würden. Die Fokussierung auf Zugriffsmöglichkeiten von Cloud-Anbieterinnen lasse zudem vollständig ausser Acht, dass auch eigene, nicht genügend professionell gemanagte Systeme eine Gefährdung für die in § 17 Abs. 1 lit. b aufgeführten Informationen bedeuteten (z.B. fehlende automatisierte Überwachung, fehlende Alarmierungen, grosszügige Einräumung von Zugriffsrechten, etc.). Eine Übertragung solcher Daten in eine Cloud werde somit faktisch unterbunden und die öffentlichen Organe gezwungen, kostenintensive Parallelsysteme zu betreiben, wenn sie Daten, die nicht der Einschränkung von § 17 Abs. 1 b entsprechen, in die Cloud übertragen wollten. Ob die öffentlichen Organe solche doppelten Ausgaben auf die Länge in Kauf nehmen wollten, erscheine mehr als zweifelhaft. Somit werde eine Cloud-Nutzung insgesamt verunmöglicht. ZHK Begrüsst wird die hohe Wertung des Datenschutzes im Gesetz. Allerdings bestünden neben einer wirksamen Verschlüsselung noch verschiedene weitere Möglichkeiten, um Daten vor dem unberechtigten Fremdzugriff durch Dritten zu schützen, wie zum Beispiel organisatorische Kontrollen über Zugriffsrechte oder eine vertragliche Zusicherung der Cloud-Anbieter. Die wirksame Verschlüsselung mit dem Beispiel der Double Key Encryption werde in den Erläuterungen bereits vordefiniert, obwohl das Gesetz technologieneutral ausgestaltet sei. § 17 sei auch technologieneutral anzuwenden.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

GVZ

Wohlwollend wird zur Kenntnis genommen, dass klare rechtliche Grundlagen zur Nutzung von Cloud-Diensten geschaffen würden.

USZ

Beantragt wird die Streichung von § 17. Sollte die Bestimmung im Gesetz verbleiben, sei ihr Anwendungsbereich auf die Zentralverwaltung zu beschränken. Das Projekt zur Einführung des DAP sei ein Projekt der kantonalen Verwaltung. Das USZ sei erstaunt, dass die entsprechenden Regelungen auch auf Arbeitsplätze in den selbständigen Anstalten anwendbar sein sollten. Die selbständigen Anstalten seien hinsichtlich der Arbeitsplatzanforderungen für ihre Mitarbeitenden heterogen und auch in ihren Bestrebungen, diese Anforderungen in ihrer Digitalisierungsstrategie umzusetzen, mit je eigenen Herausforderungen konfrontiert. In der Entwicklung des kantonalen DAP habe das USZ keine Gelegenheit gehabt, seine Bedürfnisse und Besonderheiten einzubringen. Der Arbeitsplatz eines Arztes, einer Forschenden oder einer Pflegefachperson müsse Anforderungen erfüllen, die sich von jenen der Zentralverwaltung ganz wesentlich unterschieden. § 17 würde einen rechtsstaatlich heiklen Eingriff in die verwaltungsrechtliche Autonomie der selbständigen Anstalten darstellen und dringlich notwendige Digitalisierungsschritte behindern. Sofern die selbständigen Anstalten nicht vom Geltungsbereich des neuen Gesetzes ausgenommen würden, sei zumindest die Regelung des DAP der Zentralverwaltung nicht auf alle öffentlichen Organe auszudehnen.

Lediglich im Sinne einer vorsorglichen Auseinandersetzung mit dem für das USZ nicht passenden § 17 des Vorentwurfs sei Folgendes anzumerken: Der Bestimmung zum DAP liege die Diskussion um Angebote eines bestimmten Anbieters (Microsoft mit den M365 Services) zugrunde. Das sei in mehrfacher Hinsicht problematisch.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Zunächst handle es sich um eine Regelung, die lediglich in ihrer sprachlichen Ausprägung generell-abstrakt erscheine. Inhaltlich betreffe sie einen konkreten Sachverhalt. Die Bestimmung passe auch nicht zum Regelungsgegenstand eines Gesetzes über Basisdienste. § 17 würde zudem eine Sonderregelung für einen bestimmten Fall einer Auftragsbearbeitung von Personendaten schaffen. Die Auftragsbearbeitung sei Regelungsgegenstand des Datenschutzrechts, das im kantonalen Recht im IDG und in der dazugehörigen Verordnung verortet sei. In der aktuellen Totalrevision des IDG sei keine Norm vorgesehen, die § 17 VE-Gesetz über digitale Basisdienste entspreche. Das Projekt DigiBasis dürfe nicht als «Hintertür» dienen, um den Regelungsgehalt des totalrevidierten IDG noch vor Verabschiedung durch den Kantonsrat zu verändern. Das gelte umso mehr, als der Regelungsgehalt auf einer umstrittenen und in der Lehre nicht vorherrschenden Rechtsauffassung beruhe. Der Fokus dieser Rechtsauffassung auf ein einziges potenzielles Risiko mit einer extrem geringen Eintretenswahrscheinlichkeit (lawful access durch US-Behörden) stehe einer Realität gegenüber, in der Gesundheitsinstitutionen fast unvorstellbar häufigen Cyber-Angriffsversuchen ausgesetzt seien, deren Abwehr äusserst anspruchsvoll sowie kosten- und ressourcenintensiv sei. Die gesetzliche Sonderregelung für Rechenzentren in der Schweiz und der EU wecke sodann Bedenken im Hinblick auf internationale Regelungen und Verpflichtungen. Die direkte gesetzgeberische Bezugnahme auf eine bestimmte technische Lösung (Double Key Encryption) sei nicht technologieneutral und verletze damit eine der zentralen inhaltlichen Anforderungen an Gesetzgebungsprojekte im Bereich der Digitalisierung. Ob die angesprochene technische Lösung überhaupt praktikabel sei, werde sich erst noch zeigen müssen. Es seien massive operationelle und sicherheitstechnische Zusatzrisiken zu befürchten, verbunden mit kaum tragbaren Kosten. Es bestehe also die Gefahr, dass das Gesetz bei seinem Inkrafttreten bereits überholt wäre. Damit sei eine weitere Anforderung an Gesetzgebung im Bereich der Digitalisierung nicht erfüllt.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

PHZH

§ 17 sei zu streichen. Weder die Einschränkung auf Rechenzentren nur in der Schweiz und der EU noch die spezifische Regelung explizit nur für cloud-basierte Lösungen ergäben Sinn. Zudem sei es nicht nachvollziehbar, weshalb für den DAP andere Vorgaben gelten sollten als für Fachanwendungen. Im Vorentwurf nicht geregelt sei ferner, wann eine Software-Anwendung unter DAP falle und wann sie als Fachanwendung gelte, für welche andere Anforderungen gälten. Sollte tatsächlich eine solche Unterscheidung getroffen werden, müsse eine klarere Abgrenzung vorgenommen und im Gesetz verankert werden. Es sei sodann davon auszugehen, dass die internationale Forschungszusammenarbeit sowie der akademische Austausch über die Grenzen der EU hinaus erschwert würden, zumal § 17 generell von Informationen und nicht etwa von Personendaten spreche.

Im Vorentwurf fehle eine klare und präzise Definition des Begriffs «DAP». In § 17 werde zwar der Umgang mit Informationen im Rahmen des digitalen Arbeitsplatzes geregelt, jedoch bleibe unklar, was genau unter einem «Digitalen Arbeitsplatz» zu verstehen sei. Insbesondere an Hochschulen, wo die Integration und Unterstützung von BYOD (Bring Your Own Device)-Geräten ein zentraler Bestandteil der digitalen Strategie sei, werde diese Unklarheit problematisch. Studierende und Mitarbeiter nutzten häufig ihre persönlichen Geräte, um auf akademische und administrative Ressourcen zuzugreifen. Diese Besonderheiten der Hochschulumgebung machten es umso notwendiger, den «DAP» im Gesetzestext eindeutig zu definieren. Eine eindeutige Definition des «Digitalen Arbeitsplatzes» in den Gesetzestext sei aufzunehmen und dabei die Besonderheiten der BYOD-Nutzung mitzuberücksichtigen.

UZH

§ 17 sei ersatzlos zu streichen: Mit diesem Paragrafen zum «digitalen Arbeitsplatz» werde offenbar primär auf das

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Angebot M365 von Microsoft abgezielt («Lex Microsoft»). Der digitale Arbeitsplatz solle damit anders behandelt werden als die Auslagerung von Dienstleistungen an Dritte, welche ja so möglich seien – auch in Bezug auf besondere Personendaten. Diese richteten sich nach den Vorgaben der geltenden gesetzlichen Anforderungen. Eine singuläre Verschärfung der Anforderungen und ein damit verbundenes faktisches Cloud-Verbot beim digitalen Arbeitsplatz habe mit dem Regelungsbereich des Gesetzes nichts zu tun. Vorgaben, die für die Ausführung der Tätigkeit in der Verwaltung einzuhalten seien, ergäben sich bereits aus anderen kantonalen Gesetzen. Eine zusätzliche Verschärfung dieser Vorgaben, wie sie hier nun erfolgen solle, sei abzulehnen. Falls zusätzliche Vorgaben zu Datenschutz und Datensicherheit gemacht werden sollten, sei dies im entsprechenden Gesetz (bspw. dem IDG) vorzunehmen. Die vorgeschlagene Bestimmung wird aus verschiedenen Gründen kritisiert: Die Einschränkung auf die Rechenzentren in der Schweiz und der EU sei eine neue Vorgabe. Auf Gesetzesstufe sollten generell-abstrakte Vorgaben gemacht werden. Durch Staatsverträge könnten sich die Bedingungen für andere Länder laufend verändern. Die Vorgaben seien nicht technologieneutral. Die angedachte technische Lösung (Double Key Encryption) für die besonderen Personendaten (lit. a) gehe ganz allgemein über die heutigen Anforderungen nach IDG hinaus (die Informationssicherheit ist zu gewährleisten, die Bearbeitung darf nur so erfolgen, wie es das öffentliche Organ tun darf, die Bearbeitung durch Dritte darf nur mit Einwilligung des öffentlichen Organs geschehen). Die Vorgaben seien zudem nicht technologieneutral und die Double Key Encryption werde heute noch nicht so angeboten, als dass sie für die angedachte Lösung praktikabel wäre (da sie mit anderen Nachteilen verbunden sei) sowie die Einführung grosse finanzielle Aufwände nach sich zöge, die nicht getragen werden könnten und die Lösung verunmöglichten. Gesetzgeberisch sei die Bestimmung weder notwendig noch hilfreich. Der digitale Arbeitsplatz und insbesondere

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	die Nutzung von M365 durch öffentliche Organe benötige keine Änderungen der Rechtsgrundlagen und auch keine neu zu schaffende gesetzliche Grundlage. Mit Beschluss vom 20. März 2022 (RRB Nr. 542/2022) habe der Regierungsrat die Nutzung von M365 zugelassen. Darin werde festgehalten, dass für die Einführung von Cloud-Lösungen keine Rechtsgrundlagen geändert oder geschaffen werden müssten, sondern die geltenden Bestimmungen einzuhalten seien. § 17 greife rechtswidrig in die verwaltungsrechtliche Autonomie der öffentlichen Organe und Gemeinden ein und behindere dringlich notwendige Digitalisierungsschritte. Die Einschränkungen basierten auf einer umstrittenen und in der Lehre nicht vorherrschenden Rechtsauffassung. Die Vorgaben führten zu operativen und sicherheitstechnischen Risiken sowie massiv höheren Zusatzkosten. § 17 verlange für sensible Daten eine umfassende «end-to-end-Verschlüsselung». Insbesondere für M365 sei dies weder geeignet noch nötig, berge aber massive operationelle und sicherheitstechnische Zusatzrisiken, und führe zu massiv höheren Zusatzkosten. Die Einführung von modernen Cloud-Lösungen werde durch diese gesetzlich vorgeschriebenen technischen Massnahmen de facto verunmöglicht bzw. massiv verteuert. Der Paragraf basiere auf falschen Vorstellungen über den massgeblichen Sachverhalt: Damit werde ein einzelnes (und überdies unbestritten äusserst kleines und unwahrscheinliches) Risiko völlig überbewertet, indem behauptet werde, dass US-Cloud-Anbieter quasi im Sinne eines automatischen Mechanismus sämtliche Daten jederzeit an US-Behörden weitergeben würden. Dies treffe nicht zu. Microsoft verpflichte sich in ihren Verträgen zu umfassenden Prüf- und Abwehrmassnahmen gegen die Weitergabe von Daten, welche sich in der Praxis als effektiv herausgestellt hätten. Es werde keiner (US-)Behörde ein direkter, indirekter, pauschaler oder uneingeschränkter Zugriff auf Daten gewährt. Die Unterscheidung der Vorgaben und Voraussetzungen für verschiedene Arten von Daten (besondere Personendaten und «normale» Personendaten) sei im Bereich von Tools, welche unstrukturierte Daten bearbeiteten, nicht praktikabel oder zielführend. Sie führten automatisch zur Notwendigkeit, stets die strengsten Anforderungen zu erfüllen. Bei E-Mail-Korrespondenz oder kollaborativer Bearbeitung von Dokumenten könne

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	nicht getrennt werden, wann welche Arten von Daten bearbeitet würden. Die Art der Daten könne sich während der Bearbeitung verändern, sodass «normale» Personendaten zu «besonderen » Personendaten würden. Auch müsste bei jedem Dokument oder Vorgang individuell neu entschieden werden, welche Art von Daten es beinhalte, was nicht praktikabel und fehleranfällig sei. Wenn im Kanton Zürich M365 als digitaler Arbeitsplatz grundsätzlich vorgesehen sei, würde dieser Entscheid nun durch diese neuen Vorgaben unterlaufen und wieder rückgängig gemacht. Das geltende Recht schreibe vor, dass sämtliche bekannten Risiken im Rahmen der Einführung einer IT-Lösung adressiert und so gut wie möglich mitigiert werden müssten. Dies gelte auch für Cloud-Lösungen. Ebenso müsse das Risiko, dass ausländische Behörden aufgrund von lokalen Gesetzen Daten vom Cloud-Anbieter herausverlangen könnten, analysiert und angemessen mitigiert werden. Eine absolute Pflicht für öffentliche Organe, Datenherausgaben an fremde Behörden unter allen Umständen zu verhindern (100% Schutz) gebe es weder unter dem kantonalen IDG noch unter dem Berufsgeheimnis oder dem Amtsgeheimnis. Wie bezüglich aller anderen Risiken brauche es Schutzmassnahmen, welche wirksam und angemessen seien. Diese Auffassung sei breit abgestützt. Trotzdem fordere der Vorentwurf bezüglich dieses Risikos über das geltende Recht hinaus eine absolute Nulltoleranz, also einen technisch umgesetzten 100%-Schutz für gewisse sensible Daten (faktisch – wie oben gesehen – auch für alle Daten). Eine 100%-ige Sicherheit für sensible Daten sei lebensfremd. Die Bundeskanzlei halte dazu fest, dass es sich bei Behördenherausgaben (u.a. unter dem US-Cloud-Act) um ein zusätzliches Risiko handle, welches aber nicht eine absolute Schranke darstelle, sondern im Einzelfall zu beurteilen und gegebenenfalls angemessen zu mitigieren sei. Gemäss den Erläuterungen wolle man den Einsatz eines digitalen Arbeitsplatzes erleichtern, um so einen zeitgemässen digitalen Arbeitsplatz zur Verfügung zu stellen, modernes, flexibles Arbeiten zu ermöglichen, hohe Sicherheitsstandards zu erfüllen (professionelle Lösungen mit grossem finanziellen Mitteleinsatz/Fachwissen in der Cloud vs. individuelle, organisationsspezifische on-site Lösungen mit unterschiedlich professionellen personellen und finanziellen

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

Ressourcen bzw. Sicherheitsstandards). Den Vorteilen, die ein digitaler Arbeitsplatz biete, stehe gemäss den Erläuterungen die Befürchtung entgegen, dass der amerikanische Staat über einen «lawful access» auf dem Rechtsweg Zugang zu den Daten erhalte. Der Zugriff könne nur erfolgen, wenn der Rechtsweg eingehalten werde (kein direkter Zugriff/Beschlagnahmung der Server z.B. in der Schweiz). Die Wahrscheinlichkeit sei praktisch äusserst gering (Anwendung Methode Rosenthal). Die Vorgaben verhinderten den kosteneffizienten Einsatz eines digitalen Arbeitsplatzes, da sie heute noch gar nicht umgesetzt werden könnten. Damit werde die Digitalisierung insgesamt erschwert, wenn nicht verhindert, was weder im Sinne des Steuerzahlers noch der Bevölkerung liegen könne. Die Vorgaben stünden mit den Zielen der Digitalisierung der Verwaltung im Widerspruch.

Katholische Kirche im Kanton Zürich

Grundsätzlich entspreche der Text den gesetzlichen Vorgaben, allerdings könne eine Lösung z.B. mit MS 365 von SIK (Schweizerische Informatikkonferenz) unter Umständen sehr kostenintensiv werden. Das sei für die Römisch-katholische Körperschaft und die Kirchgemeinden nicht stemmbar. Der Text entspreche den Vorgaben des IDG, ausser der Handhabung des Verschlüsselungskeys. Die Handhabung des Schlüssels (ob private key oder public key) sei im IDG nicht vorgeschrieben, mache aber durchaus Sinn. Wenn der Inhaber der Daten – die öffentliche Behörde – den private key bei sich habe, könne die Cloud-Anbieterin nicht ohne die Mitarbeit des Dateninhabers Daten einsehen oder weitergeben. Falls § 17 so übernommen würde, sei diese Einschränkung als Verschärfung des IDG zu sehen.

DSB

Die Regelung wird begrüsst. § 17 stelle eine unabdingbare Rechtsgrundlage für die cloudbasierte Informationsbearbeitung durch Dritte im Rahmen des DAP dar. § 17 lege die Rahmenbedingungen fest, die für

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	eine grundrechts- und datenschutzkonforme Datenbearbeitung zu beachten seien, wenn Anwendungen des DAP an Anbieterinnen von cloudbasierten Dienstleistungen ausgelagert würden. Dies schaffe die notwendige Rechtssicherheit für die öffentlichen Organe und sorge für die entsprechende Transparenz gegenüber den betroffenen Personen. Grundlegend sei die Festlegung, dass solche Anwendungen nur in der Schweiz oder EU betrieben werden dürften, was für klare rechtliche Rahmenbedingungen und einen gleichwertigen Datenschutz sorge. Kumulativ gehöre dazu, dass besondere Personendaten und Daten unter einem spezifischen Geheimnisschutz (lit. a) auch gegenüber dem Auftragsbearbeiter wirksam zu verschlüsseln seien. Damit sei sichergestellt, dass das öffentliche Organ die geeigneten und erforderlichen Massnahmen der Datensicherheit umsetze. Für die «sonstigen Informationen» (lit. b) seien Kriterien aufgeführt, die im Einzelfall eine Beurteilung der vertretbaren Risiken für die Grundrechte der betroffenen Personen verlangten. Es gelte dabei zu berücksichtigen, dass dies im Rahmen der datenschutzrechtlichen Vorgaben zu erfolgen habe, auf welche in Absatz 2 korrekterweise hingewiesen werde. Insgesamt erweise sich diese Bestimmung als ausgewogene Lösung für die Nutzung von cloudbasierten Dienstleistungen und damit als notwendige Voraussetzung für eine rechtskonforme Umsetzung cloudbasierter Lösungen, die den Aspekten des Datenschutzes und der Informationssicherheit Rechnung trage. Damit sei diese Gesetzesbestimmung auch die Grundlage, um den öffentlichen Organen weitergehende und vertiefte Anleitungen zur Nutzung von cloudbasierten Dienstleistungen zur Verfügung stellen zu können. Die aktuelle Regelung des DAP im DigiBasis beschränke sich auf das Thema der Informationsbearbeitung durch Dritte (§ 17). Der DAP brauche zusätzliche rechtliche Regulierungen, die in diesem Zusammenhang erlassen werden könnten. Dies betreffe insbesondere folgende Datenbearbeitungen:

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

1. Biometrische Verifikationsmethoden: Im Rahmen der Anmeldung beim DAP würden auch biometrische Merkmale verwendet. Biometrische Daten stellten besondere Personendaten dar (§ 3 Abs. 4 lit. a Ziff. 2 IDG). Das Bearbeiten besonderer Personendaten bedürfe einer hinreichend bestimmten Regelung in einem formellen Gesetz (§ 8 Abs. 2 IDG). Für die Verwendung von biometrischen Merkmalen beim DAP gebe es derzeit keine entsprechende Regelung. Sie könne im DigiBasis geschaffen werden. Vorbild dafür könne Art. 20 Abs. 2 Bundesgesetz über die Informationssicherheit beim Bund (ISG, SR 128) sein: «Sie (Behörden und Organisationen) können biometrische Verifikationsmethoden verwenden, wenn dies zur risikogerechten Identifizierung von Personen erforderlich ist. Die biometrischen Daten werden nach dem Wegfall der Zugangsberechtigung vernichtet.» Dieser Regelungsbedarf erstrecke sich nicht nur auf den DAP, wie er in der Kantonsverwaltung betrieben werde.
2. Auftragsdatenbearbeitung beim Service Desk: Beim DAP der Kantonsverwaltung gebe es einen Fluss von Informationen der DAP-nutzenden Organisationseinheit zum AFI im Zusammenhang mit der Datenbearbeitung beim Service Desk. Dieser Datenfluss stelle eine Auftragsdatenbearbeitung dar (§ 6 IDG). Sollte das AFI nicht planen für diese (und andere) Auftragsdatenbearbeitungen mit allen DAP-nutzenden Organisationseinheiten einen Auftragsdatenbearbeitungsvertrag (ADV) abzuschliessen, müsse die Auftragsdatenbearbeitung durch das AFI im Rahmen des Service Desk und deren Rahmenbedingungen gesetzlich geregelt werden. Das DigiBasis würde sich hier als Regelungsort anbieten. Dieser Regelungsbedarf erstrecke sich voraussichtlich nur auf den DAP, wie er in der Kantonsverwaltung betrieben werde.
3. Auftragsdatenbearbeitung beim Laufwerk «H»: Beim DAP der Kantonsverwaltung gebe es einen Fluss von Informationen der DAP-nutzenden Organisationseinheit zum AFI im Zusammenhang mit der Nutzung des

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Laufwerks «H». Dieser Datenfluss und die Zugriffsmöglichkeiten des AFI stellten Auftragsdatenbearbeitungen dar (§ 6 IDG). Sollte das AFI nicht planen, für diese (und andere) Auftragsdatenbearbeitungen mit allen DAP-nutzenden Organisationseinheiten einen ADV abzuschliessen, müsse die Auftragsdatenbearbeitung durch das AFI im Rahmen des Laufwerks «H» und deren Rahmenbedingungen gesetzlich geregelt werden. DigiBasis würde sich hier als Regelungsort anbieten. Dieser Regelungsbedarf erstrecke sich voraussichtlich nur auf den DAP, wie er in der Kantonsverwaltung betrieben werde. Finanzkontrolle des Kantons Zürich Auf die Nennung von Technologien sei zu verzichten. Eine gesetzliche Festschreibung von Technologien werde nicht dem technischen Fortschritt gerecht. Insbesondere die Nennung des digitalen Arbeitsplatzes und der Cloud erscheine problematisch.
§ 17. [1] Das öffentliche Organ kann die Bearbeitung von Informationen in Anwendungen des digitalen Arbeitsplatzes an Anbieterinnen von cloudbasierten Informatikdienstleistungen übertragen, wenn sich deren Rechenzentren in der Schweiz oder in der Europäischen Union befinden, und wenn:	SP Kanton Zürich Ergänzung mit lit. c: «Die Cloud-Anbieterin nicht durch höheres Recht in einem Land ausserhalb der Schweiz zur Weitergabe an Geheimdienste verpflichtet ist.» Dies beziehe sich vor allem auf Amerikanische und Chinesische Anbieter, die durch höheres Recht verpflichtet seien, ihren jeweiligen Geheimdiensten eine Backdoor zur Datenlieferung einzubauen. asut (Schweizerischer Verband der Telekommunikation) Die Nutzung cloudbasierter Dienste solle nur zulässig sein, wenn sich die entsprechenden Rechenzentren in der Schweiz oder der Europäischen Union befänden. Es fehle eine sachliche Begründung, wieso beispielsweise weitere Länder aus dem Europäischen Wirtschaftsraum (Liechtenstein, Norwegen und Island) oder Grossbritannien nicht zulässig seien. Es solle daher geprüft werden, ob diese Liste erweitert werden könne (z.B.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	gemäss Anhang 1 der Datenschutzverordnung).
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	asut (Schweizerischer Verband der Telekommunikation) Besonders schützenswerte Personendaten sowie vertrauliche oder geheime Informationen erforderten gemäss § 17 Ziff. 1 lit. a eine sogenannte «Double Key Encryption». Danach müssten nicht nur die Daten in den Clouddiensten verschlüsselt sein, sondern auch die dazu notwendigen Schlüssel dürften dem Cloudanbieter nicht zugänglich sein. Dieses Prinzip sei komplexer, schwerfälliger und aufwändiger, da eine zusätzliche Organisation für die Schlüsselverwaltung berücksichtigt werden müsse. Dies habe negative Auswirkungen auf die Flexibilität und Agilität bei der Gestaltung des digitalen Arbeitsplatzes und führe zu einem erhöhten Aufwand und grösseren Kosten. Dies würde insbesondere kleinere öffentliche Organe betreffen, welche nicht auf entsprechende interne IT-Ressourcen zugreifen könnten, sondern externe Dritte damit beauftragen müssten. Die DKE würde zudem die Funktionalität des digitalen Arbeitsplatzes deutlich einschränken. Kollaborations-Lösungen, die Nutzung von AI-Algorithmen, aber auch Sicherheitsfunktionen wie Virenschutz, Phishing-Prävention oder Backup-Lösungen wären nicht mehr durch den Cloudanbieter möglich oder würden deutlich eingeschränkt. Die explizite Forderung nach DKE im vorliegenden Gesetzesentwurf überrasche, da die heute etablierte Praxis im Risikomanagement bei der Informationssicherheit nicht ausschliesslich auf technische Massnahmen abstütze. Vielmehr werde eine optimale Kombination von technischen, organisatorischen und vertraglichen Massnahmen eingesetzt. Dies reduziere nicht nur die Komplexität sowie Aufwand und Kosten, sondern erlaube auch eine weitergehende Differenzierung des Schutzniveaus der Daten und Informationen. Zudem fehle im erläuternden Bericht zu §17 Ziff. 1 Lit. a der Hinweis, dass es neben der DKE auch andere technische Massnahmen gebe, bei denen das Schlüsselmanagement in der Hand des betreffenden Organs bleibe. Aus diesen Gründen wird die einschränkende Forderung nach «Double Key Encryption» abgelehnt und es wird eine erweiterte Regelung empfohlen, welche technische, organisatorische und

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

vertragliche Massnahmen kombiniert.

Gemeinde Meilen

Selbst mit der Lockbox-Funktion, weiche die Gemeinde Meilen (und auch andere Gemeinden) als Zugriffsschutz von Microsoft beziehe und bezahle, könnten sich die Gemeinden nicht abschliessend gegen den vom Gesetzestext verlangten Zugriff der Cloud-Anbieterin schützen. Die immer wieder erwähnte Double Key Encryption habe nach dem Kenntnisstand der Gemeinde Meilen bisher in keiner Gemeinde umgesetzt werden können. Im Sinne einer für die Gemeinden in der heutigen Arbeitsrealität umsetzbaren Gesetzesvorgabe schlägt der Gemeinderat Meilen folgende Formulierung vor: «(...) 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 grundsätzlich nicht ohne Mitwirkung des öffentlichen Organs zugreifen kann und (...)».

Gemeinde Rifferswil

Speziell weise der Gemeinderat – insbesondere in Übereinstimmung mit dem GPV, wogegen die Kritik des VZGV zu wenig dezidiert ausfalle – darauf hin, dass § 17 VE-Gesetz über digitale Basisdienste absolut nicht praktikabel sei und viele der heute problemlos bereits bestehenden Lösungen verunmöglicht würden. Nebst der vom GPV vorgeschlagenen Variante wird darauf hingewiesen, dass der vorgesehene Zwang zur Verschlüsselung von speziellen Personendaten auch gegenüber den Cloud-Anbetern zumindest mit den aktuellen IT-Lösungen der meisten Gemeinden schlicht nicht praktikabel sei. In vielen Fällen sei er Cloud-Anbieter identisch mit dem Support-Anbieter, womit dessen unabdingbare Arbeit verhindert würde. Es sei auch nicht praktikabel zu verlangen, dass besondere Personendaten anders behandelt werden als nicht besondere, da die Daten z.B. im Einwohnerregister

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen

nicht getrennt geführt werden. Beantragt wird insbesondere, dass § 17 Abs. 1 lit. entweder ganz zu streichen sei oder in massiv abgeschwächter, empfehlender Form aufgenommen werde. Ferner werde darauf verwiesen, dass die dem § 17 Abs. 1 lit. a entsprechenden Verschlüsselungsmassnahmen in den allgemeinen Richtlinien für Informationssicherheit und Datenschutz (Punkt 8.4) aktuell nicht haltbar und völlig unpraktikabel seien.

Stadt Uster

§ 17 Abs. 1 lit. a nehme eine zu restriktive Haltung in Sachen Datenschutz ein. Mit der Forderung, dass «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» werde eine Zusammenarbeit mit Dritten extrem erschwert und sei kaum mehr praktikabel.

Beispielsweise dürften so die Anbieter, welche auch für den Support der Cloudumgebung und der Gemeindefachsoftware der Stadt Uster zuständig sind, nicht auf deren Lösungen zugreifen, solange nicht gewährleistet wäre, dass sie keinerlei potenziellen Zugriff auf Personendaten hätten, oder sie müssten während ihres Zugriffs durch die Stadt Uster überwacht werden, und das unabhängig davon, welche vertraglichen Bestimmungen bezüglich Einhaltung von Datenschutz, Verschwiegenheit u.Ä. im Vorfeld vereinbart worden seien.

§ 17 Abs. 1 lit. a könne gestrichen, dafür lit. b als allgemein gültig für alle Informationen formuliert werden: «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.» Damit solle gewährleistet sein, dass sich das öffentliche Organ um den

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	nötigen Schutz der Daten unter Abwägung möglicher Risiken kümmere. VZGV Änderung: «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 grundsätzlich nicht ohne Mitwirkung des öffentlichen Organs zugreifen kann» (Ergänzung: grundsätzlich). Die erwähnten Vorgaben seien mit den aktuell verfügbaren Sicherheitsmassnahmen kaum umsetzbar. Die Nutzung der Dienste entspreche jedoch der Arbeitsrealität der Gemeinden und Städte. UZH Die Ausführungen in den Erläuterungen betreffend «Personendaten, die durch besondere Amtsgeheimnisse geschützt sind…» (Zitat Erläuterungen zu § 17 lit. a, erster Spiegelstrich, Seite 26) könnten nicht nachvollzogen werden. Gemäss Art. 320 StGB gebe es nur ein Amtsgeheimnis, und nicht ein normales und ein besonderes. Evangelisch-reformierte Landeskirche Die vorgesehene Verpflichtung zur vollständigen Verschlüsselung könne dazu führen, dass keine Cloudanwendungen mehr möglich seien, da entsprechende Anbieterinnen mit den erforderlichen technischen Möglichkeiten fehlen. Dies wäre für eine öffentlich-rechtliche Körperschaft weder organisatorisch noch ökonomisch sinnvoll und auch nicht sicher.
b. das öffentliche Organ die sonstigen Informationen durch alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen schützt und das	GRÜNE Kanton Zürich Problematisch sei ein Zugriff der Cloud-Anbieterin bzw. eines Drittstaates unter Umgehung der Rechtshilfe auf die sonstigen Informationen, die nicht unter § 17 Abs. 1 lit. a fielen. Dementsprechend seien alle Informationen des DAP unter strengen Vorgaben zu verschlüsseln. Lit. b sei zu streichen und in § 17 Abs. 1 lit. a zu integrieren.

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
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.	asut (Schweizerischer Verband der Telekommunikation) In diesem Paragrafen werde der Umgang mit Informationen geregelt, die nicht besonders schützenswert, vertraulich oder geheim seien. Die Formulierung «alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen» sei dabei aus mehreren Gründen unglücklich. Einerseits sei gänzlich unbestimmt, welches Schutzniveau erreicht werden solle und welche Massnahmen noch als zumutbar gälten. Dies führe zu Unklarheiten und letztlich zu Rechtsstreitigkeiten zwischen öffentlichen Organen und Cloud-Anbietern. Zudem gehe diese Formulierung faktisch über «Double Key Encryption» hinaus, falls diese als zumutbar klassifiziert werde, da zusätzlich organisatorische und vertragliche Massnahmen gefordert würden. Daher solle § 17 Ziff. 1 lit. b konkretisiert werden oder allenfalls ganz gestrichen werden, falls die Anforderungen gemäss Datenschutzgesetz für diese Informationen ausreichen. Gemeinde Meilen Die Formulierung «alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen» lasse künftig viele Möglichkeiten offen und schaffe keine Klarheit. Praktisch könne das mit einer permanent aktualisierten Liste der zumutbaren organisatorischen und technischen Massnahmen umgesetzt werden. Dem Gemeinderat sei jedoch klar, dass dies eine konkrete Massnahme wäre, welche nicht ins Gesetz, das allgemein gehalten sein müsse, gehöre. Daher schlägt der Gemeinderat Meilen folgende Formulierung vor: «(...) das öffentliche Organ die sonstigen Informationen durch zumutbare organisatorische, technische und vertragliche 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.»

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Gemeinde Winkel Die Formulierung «alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen» lasse künftig viele Möglichkeiten offen und schaffe keine Klarheit. Praktisch könne das mit einer permanent aktualisierten Liste der zumutbaren organisatorischen und technischen Massnahmen umgesetzt werden. Die Hürden sollten nicht so hoch angesetzt werden, dass damit eine Umsetzung im Arbeitsalltag verunmöglicht werde. Die Formulierung «zumutbare, organisatorische, technische und vertragliche Massnahmen» sollte ausreichend sein. VZGV Die Formulierung «alle zumutbaren, organisatorischen, technischen und vertraglichen Massnahmen» sei durch «zumutbare, organisatorische, technische und vertragliche Massnahmen» zu ersetzen. Die Formulierung «alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen» lasse künftig viele Möglichkeiten offen und schaffe keine Klarheit. Praktisch könne das mit einer permanent aktualisierten Liste der zumutbaren organisatorischen und technischen Massnahmen umgesetzt werden. Konkrete Massnahmen seien nicht auf Gesetzesstufe zu verankern. Die Hürden sollten nicht so hoch angesetzt werden, dass eine Umsetzung im Arbeitsalltag damit verunmöglicht werde.
2 Im Übrigen gelten die Bestimmungen des Gesetzes über die Information und den Datenschutz.	Gemeinde Meilen Es solle sichergestellt werden, dass durch das neue IDG in Bezug auf die Informationsbearbeitung durch Dritte im Rahmen des digitalen Arbeitsplatzes nicht weitere Einschränkungen für die Gemeinden dazukämen, welche ein zeitgemässes kollaboratives Arbeiten erschwerten. VZGV Es solle sichergestellt werden, dass durch das neue IDG in Bezug auf die Informationsbearbeitung durch Dritte im

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
	Rahmen des digitalen Arbeitsplatzes nicht weitere Einschränkungen für die Gemeinden und Städte dazukämen, welche ein zeitgemässes kollaboratives Arbeiten erschwerten.
5. Abschnitt: Schluss- und Übergangsbestimmungen Änderungen des bisherigen Rechts II. 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.	Privatperson A Statt einer Regelung im Gesetz über digitale Basisdienste wird eine Nebenänderung des Gesetzes über die Auslagerung von Informatikdienstleistungen vorgeschlagen (siehe oben unter § 17). Finanzkontrolle des Kantons Zürich Auf die Nennung von Technologien sei zu verzichten. Eine gesetzliche Festschreibung von Technologien werde nicht dem technischen Fortschritt gerecht. Insbesondere die Nennung des digitalen Arbeitsplatzes und der Cloud erscheine problematisch. Daher sei «cloudbasiert» zu löschen.
[bisheriger § 3 Abs. 2 wird zu § 3 Abs. 3]	

Vorentwurf	Besondere Bemerkungen zu einzelnen Bestimmungen
III. Dieses Gesetz untersteht dem fakultativen Referendum.	