Angaben zur Stellungnahme

Thematik:
Gesetz über digitale Basisdienste

Teilnehmerangaben:
SwissICT
Rechtskommission
Vulkanstrasse 120
8048 Zürich

Kontaktangaben:
Kanton Zürich
Neumühlequai 10
8090 Zürich

E-Mail-Adresse: florian.bergamin@sk.zh.ch
Telefon: +41 43 258 84 02

Teilnehmeridentifikation:
148559

Bereich	Kapitel	Antrag / Bemerkung	Begründung
Vorentwurf Gesetz über digitale Basisdienste mit erläuterndem Bericht	Allgemeine Rückmeldungen	Erfasst von: Alexander Hofmann Sehr geehrte Damen und Herren Namens der swissICT reichen wir hiermit unsere Positionen zum Vorentwurf des Gesetzes über digitale Basisdienste ein und bedanken uns für die Gelegenheit zur Stellungnahme. swissICT ist ein im Jahr 2000 durch die Fusion zweier Verbände - Schweizerische Vereinigung für Datenverarbeitung (SVD, gegründet 1968) und Wirtschaftsinformatik-Fachverband (WIF, gegründet 1955) - gegründeter Verband und vertritt ICT-Anbieter, -Anwender sowie -Fachkräfte in der Schweiz. Mit 3'000 Mitgliedern ist swissICT der primäre Repräsentant des ICT-Werkplatzes Schweiz und der grösste Fachverband der Branche. Viele swissICT Mitglieder sind vom Gesetz über digitale Basisdienste direkt oder indirekt betroffen, sei es als Anwender von ICT-Leistungen (Adressaten des Gesetzes) oder als Anbieter von ICT-Dienstleistungen an Behörden und öffentliche Organe im Kanton Zürich. Die Stellungnahme beschränkt sich auf jene Punkte, welche für alle betroffenen Mitglieder von swissICT relevant und kritisch sind, also sowohl für Anbieter wie für Anwender. Im Zuge dieses Neuerlasses wird mit § 17 eine Regelung zur Nutzung von cloudbasierten Anwendungen im Rahmen des digitalen Arbeitsplatzes bei öffentlichen Organen vorgeschlagen. Mit «digitalem Arbeitsplatz» zielt man offenbar primär auf das Angebot M365 von Microsoft ab und will bei sensibleren Daten einen durch Verschlüsselungstechniken umgesetzten 100%-Schutz vor Zugriffen Dritter (inkl. des Cloud-Providers selbst) vorschreiben. Die in § 17 verankerten Anforderungen an die Verschlüsselung gehen aus unserer Sicht aus folgenden Gründen in eine falsche Richtung: - Das Gesetz würde de facto ein generelles Cloud-Verbot mit Ausnahme vollverschlüsselter Speicherdienste statuieren, was nicht angemessen ist 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 bedeutet, 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 gälte nicht nur für alle öffentlichen Organe des Kantons Zürich, sondern auch für alle Organisationen, die mit der Erfüllung öffentlicher Aufgaben betraut sind. Das ist ein weites Feld; es erfasst bspw. auch private Spitäler, die spitalambulante Leistungen erbringen und einen Leistungsauftrag des Kantons haben, private Spitexorganisationen oder bestimmte Anbieter im Bereich der Berufsbildung usw. - Funktionalitäten, welche den digitalen Arbeitsplatz ausmachen, würden in den heutzutage kommerziell angebotenen Lösungen massiv eingeschränkt oder verunmöglicht. Z.B. 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 funktionieren, können Dokumente z.B. auf dem Tablet oder Mobile nicht entschlüsselt werden. Sie können dort deshalb weder gelesen noch bearbeitet werden (inkl. Mail). Dies schränkt die Mobilität des digitalen Arbeitsplatzes ein. - Die Sicherheit würde nach aktuellem Stand der Technik schlechter – nicht besser: Wichtige Schutzmechanismen (z.B. Virenscan) greifen bei verschlüsselten Dokumenten nicht. Dies bedeutet, dass befallene Dokumente	

Bereich	Kapitel	Antrag / Bemerkung	Begründung
		wie z.B. Excel-Dateien mit Makros, ZIP-Dateien, Phishing-PDF etc. vom Cloud-Dienst und somit vom Schutzmechanismus nicht erkannt werden können. Vom Cloud-Provider in der Cloud zur Verfügung gestellte Sicherheitsfunktionen, welche ständig weiterentwickelt und aktuell gehalten werden, sind somit punktuell ausgehebelt. Lokale oder hybride Lösungen müssen dann separat geschützt werden, was riesige Sicherheitslücken hinterlässt und zu massiv höheren Kosten führen kann. Es ist unter Spezialisten und IT-Verantwortlichen in Unternehmen und Behörden breit anerkannt, dass das Niveau an Sicherheit, welche moderne Cloud-Lösungen heutzutage bereitstellen, «on-premise» nicht ohne erheblichen Zusatzaufwand erreicht werden kann. - Nach Einschätzung der Rechtskommission von swissICT ist eine solche Spezialbestimmung zudem gesetzgeberisch nicht notwendig. Für die Einführung von Cloud-Lösungen im Bereich des digitalen Arbeitsplatzes müssen keine Rechtsgrundlagen geändert oder neu geschaffen werden. Zudem basieren die in § 17 vorgeschriebenen technischen Einschränkungen auf einer umstrittenen und in der Lehre nicht vorherrschenden Rechtsauffassung. swissICT empfiehlt daher, § 17 ersatzlos aus dem Gesetzesentwurf zu streichen und beteiligt sich entsprechend an der Vernehmlassung. Bitte finden Sie unsere detaillierte rechtliche Kommentierung des Gesetzesartikels sowie der zugehörigen Erläuterungen im angehängten Dokument. Wir danken Ihnen im Namen unserer Mitglieder im Voraus dafür, dass Sie unsere Anregungen in geeigneter Weise berücksichtigen. Gerne stehen wir Ihnen für Rückfragen und weitere Diskussionen zur Verfügung. Freundliche Grüsse SwissICT – Rechtskommission Alexander Hofmann, Carmen De La Cruz **- Anhang A**	

Anhang A

Vorentwurf Gesetz über digitale Basisdienste mit erläuterndem Bericht
Detailkommentierung SwissICT

Vorentwurf	Erläuterungen	Bemerkungen
C. Digitaler Arbeitsplatz		
Vorbemerkungen	Im Rahmen seiner Strategie zu Informations- und Kommunikationstechnologien (IKT-Strategie, vgl. RRB Nr. 383/2018) hat der Regierungsrat entschieden, die kantonale Verwaltung mit einem neuen, digitalen Arbeitsplatz (DAP) auszurüsten. Eine vergleichbare Entwicklung zeichnet sich auch in den Gemeinden und in den dezentralen Verwaltungseinheiten wie den Spitälern und den Hochschulen ab. Mittlerweile haben zahlreiche öffentliche Organe auf kantonaler und kommunaler Ebene einen DAP eingeführt oder prüfen dessen Einführung.	Eine fehlende gesetzliche Grundlage hierfür wurde offenbar bis heute nicht moniert.
	Zu ihrer Aufgabenerfüllung und für die Erbringung von Leistungen sind die Mitarbeitenden der öffentlichen Organe auf zeitgemässe digitale Arbeitsmittel angewiesen. Der DAP erhöht die Mobilität, unterstützt die Anforderungen an modernes, flexibles Arbeiten, entspricht den heutigen Sicherheitsstandards und vereinfacht den Betrieb. Verwendet werden Software-Anwendungen wie z.B. die Anwendungen von Microsoft 365 (Word, Excel, PowerPoint, Outlook, Teams, OneDrive usw.; nachfolgend M365). Nicht zum DAP gehören Fachanwendungen (z.B. eine Software für die Geschäftsverwaltung). Es ist zu erwarten, dass die Software- Anwendungen häufig über den externen Anbieter Microsoft bezogen und mindestens teilweise über dessen Cloud abgewickelt werden. Die Bestimmungen zum DAP sind aber technologie- und anbieterneutral und umfassen auch allfällige Anwendungen von anderen Anbietern (nachfolgend die "Cloud-Anbieterin").	Die Nutzung von Cloud-Diensten ist im Grundsatz als **administrative Hilfstätigkeit (Bedarfsverwaltung)** einzustufen. Als administrative Hilfstätigkeit ist die Beschaffung jener notwendigen Sachgüter oder Leistungen gemeint, die die Verwaltung zur Erfüllung ihrer öffentlichen Aufgabe benötigt. Beispiele dafür sind die Beschaffung von Büromaterial, der Abschluss von Werkverträgen für die Errichtung einer öffentlichen Baute oder eben das Beiziehen eines IKT-Leistungserbringers (vgl. Bericht der Bundeskanzlei vom 31.08.2022 «Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung», S. 12) Soweit für die eigentliche, legitimierungsbedürftige Tätigkeit des Staats das Erfordernis der gesetzlichen Grundlage eingehalten ist, ist die dazu gehörende administrative Hilfstätigkeit von der gesetzlichen Grundlage mit erfasst. Für diese leitet sich die gesetzliche Grundlage unmittelbar aus der Rechtsgrundlage für die jeweilige öffentliche Aufgabe ab. Eine besondere gesetzliche Grundlage ist für Tätigkeiten im Rahmen der Bedarfsverwaltung nicht erforderlich. Es genügt, dass für die Aufgabe, welcher die Hilfstätigkeiten dienen, eine genügende Rechtsgrundlage vorhanden ist. Mit der Begründung einer Aufgabe wird auch die Kompetenz verliehen, die dafür erforderlichen Mittel zu beschaffen. Das gilt auch für die Kompetenz, die Bereitstellung der erforderlichen Mittel Dritten zu übertragen (Outsourcing). Dies bedeutet, dass die Verwaltung keine ausdrückliche gesetzliche Genehmigung benötigt, Cloud-Dienste nutzen zu können. Je nach Sachbereich oder Natur der im Rahmen solcher Outsourcings allfällig bearbeiteter Daten können spezifischere Anforderungen gelten, namentlich dann, wenn Personendaten oder Amtsgeheimnisdaten Gegenstand eines Cloud-Projekts sind. Im Rahmen seiner Gesetzgebungskompetenz bezüglich der Bearbeitung von Personendaten durch kantonale Behörden, Gemeinden und Verwaltungsstellen hat der Kanton Zürich hierfür die folgenden Gesetze und Verordnungen erlassen: IDG, IDV, IVSV und für kantonale Organe zudem das Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1991 (LS 172.71). Diese Rechtserlasse konkretisieren den grundrechtlichen Persönlichkeitsschutz und die rechtsstaatlichen Grundsätze für das Bearbeiten von Personendaten für Behörden des Kantons Zürich, indem sie die Voraussetzungen und allgemeinen Grundsätze der Datenbearbeitung durch kantonal- und kommunal-zürcherische Behörden sowie die Rechte der betroffenen Personen festlegen, auch und insbesondere im Kontext eines Beizugs von Dienstleistern, welche im Auftrag der Behörden Personendaten bearbeiten. Der Bedeutung des Datenschutzes ist angemessen, dass dies in Form eines Gesetzes im formellen Sinn gemacht wurde, wobei diesbezüglich Differenzierungen möglich sind und eine Delegation auf die Verordnungsebene grundsätzlich möglich wäre.
	Heute wird der Einsatz von cloudbasierten Anwendungen durch das IDG, die IDV, die IVSV und für kantonale Organe zudem durch das Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1991 (LS 172.71) erfasst. Die Informationsbearbeitung durch Dritte (auch "Auftragsdatenbearbeitung" oder Bearbeitung im Auftrag genannt) ist gemäss § 6 Abs. 1 IDG bzw. § 9 Abs. 1 E-IDG (gemäss Vorlage 5923) zulässig und rechtmässig, wenn keine gesetzliche oder vertragliche Bestimmung der Auslagerung entgegensteht. Die Verantwortung für den Umgang mit Informationen verbleibt trotz der Übertragung der Informationsbearbeitung beim öffentlichen Organ (§ 6 Abs. 2 IDG sowie § 9 Abs. 2 Satz 1 E-IDG). Gemäss dem im heutigen § 6 Abs. 2 IDG nicht enthaltenen Satz 2 von § 9 Abs. 2 E-IDG hat das öffentliche Organ insbesondere sicherzustellen, dass die Dritten (d.h. die Cloud-Anbieterinnen) die Informationssicherheit gewährleisten, Informationen nur so bearbeiten, wie es das öffentliche Organ selbst tun darf und die Bearbeitung erst nach Bewilligung durch das öffentliche Organ an weitere Dritte übertragen wird. § 19 IDG bzw. § 36 E-IDG regeln die grenzüberschreitende Bekanntgabe von Personendaten an Empfängerinnen und Empfänger, die dem Europarats-Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten nicht unterstehen. In dieser Konstellation darf das öffentliche Organ Personendaten gemäss der Regelung im E-IDG gemäss Vorlage 5923 nur dann bekanntgeben, wenn (a) eine gesetzliche Grundlage dies erlaubt und dies dem Schutz der Interessen der betroffenen Person oder überwiegenden öffentlichen Interessen dient, (b) im Empfängerstaat ein angemessener Schutz für die Datenbearbeitung gewährleistet ist oder (c) das öffentliche Organ mit den Empfängerinnen und Empfängern angemessene Sicherheitsvorkehrungen vereinbart hat.	Dieser Abschnitt bestätigt, was oben bereits ausgeführt wurde, nämlich dass aus verfassungs- wie auch aus datenschutzrechtlicher Sicht genügende gesetzliche Grundlagen für eine Datenbearbeitung im Auftrag - auch durch "Cloud-Anbieterinnen" (wie immer dieser Begriff definiert wird) - bestehen. Das gilt auch für eine allfällige Bekanntgabe ins Ausland. **Eine weiteren gesetzlichen Grundlage für diese Bearbeitungstätigkeiten ist nicht notwendig.** Eine eigene gesetzliche Grundlage ist nach allgemeinen Prinzipien nur für gewichtigere Grundrechtseingriffe erforderlich. Der Regierungsrat hat denn auch bereits am 30. März 2022 einen Beschluss zur Nutzung von Microsoft 365 erlassen (RRB 542/2022). Darin wird festgehalten, dass für die Einführung von Cloud-Lösungen **keine Rechtsgrundlagen geändert oder geschaffen werden müssen, sondern die geltenden Bestimmungen einzuhalten sind**. Viele Städte und Gemeinden (z.B. Stadt Zürich, Stadt Bülach) sowie unzählige öffentliche Organe im Kanton setzen bereits heute beim digitalen Arbeitsplatz umfassend auf Cloud-Lösungen, insbesondere auf Microsoft 365. Diese Grundsätze sind schweizweit etabliert.

	Die umfangreiche Auslagerung von Daten des Staates in eine von einer ausländischen Cloud-Anbieterin betriebene und kontrollierte Cloud-Infrastruktur bringt verschiedene, vielfach noch offene Rechtsfragen mit sich:		Das trifft nicht zu. Die Rechtslage diesbezüglich ist recht klar. Der Kanton Zürich vertritt bezüglich gewisser Rechtsfragen eine besonders strenge Haltung, steht damit schweizweit aber recht alleine da. Auch die Erläuterungen zu diesem Vorentwurf befassen sich interessanterweise überhaupt nicht mit den vielzähligen liberaleren Rechtsauffassungen.
	Einerseits wirft die Auslagerung Fragen des Grundrechtsschutzes auf, weil eine Auslagerung in die Cloud ein schwerer Eingriff in den verfassungsrechtlichen Persönlichkeitsschutz (Art. 13 Abs. 2 BV) darstellen kann. Mit der Auslagerung ist ein Kontrollverlust gegenüber der Cloud-Anbieterin verbunden, weil die Nachvollziehbarkeit der Datenbearbeitung und die Durchsetzung von Kontrollrechten der Betroffenen erschwert werden. Zudem resultiert ein Kontrollverlust gegenüber ausländischen Behörden, wenn diese aufgrund der ausländischen Rechtslage (vgl. z.B. den US CLOUD Act bzw. den Stored Communications Act [sog. lawful access]) die Cloud-Anbieterin zur Herausgabe von in der Cloud gespeicherten Daten verpflichten können. Diese Problematik besteht unabhängig von der Wahrscheinlichkeit eines Datenzugriffs durch ausländische Behörden und dem Standort der Server.		Man beklagt Kontrollverlust, indem die Amtsstelle im Kanton Betroffenenrechte nicht garantieren könne. Das ist falsch. Betroffenenrechte werden durch eine Auslagerung in die Cloud potentiell tangiert, aber weder preisgegeben noch ausgehebelt. Es ist selbstverständlich möglich, dass ausländische Behörden im Rahmen des lokalen Rechts und der entsprechenden Abläufe punktuell bestimmte Daten herausverlangen können, mehr aber nicht. Ein schwerer Eingriff ist dabei nicht zu erkennen. Was der Vorentwurf stattdessen fordert oder zumindest nahelegt (Speicherung «on premise» oder end-to-end Verschlüsselung), führt nicht zu besserer Sicherheit – ganz im Gegenteil: Eine Verschlüsselung der Abläufe in einer Office-Umgebung verunmöglicht eine praktikable und organisatorisch sichere Nutzung, was operationale Risiken und Kosten verursacht, Schatten-IT erhöht auch dadurch das Risiko für betroffene Personen. Sollte der Schutz bei Speicherungen «on premise» oder mit "end-to-end"-Verschlüsselung aber schlechter sein, würde höchstens ein Risiko von Herausgabeansprüchen ausländischer Behörden reduziert, dies aber zu einem überaus hohen Preis. Der Vorentwurf gibt somit eine Richtung vor, die Personendaten im Ergebnis gefährdet.
	Anderseits gilt es, die datenschutzrechtlichen Bestimmungen, die Vorgaben zum Schutz der Informationssicherheit der jeweiligen Organisationseinheit sowie des Amtsgeheimnisses zu beachten (Art. 320 Schweizerisches Strafgesetzbuch, SR 311.0) und sensible Informationen durch besondere Massnahmen zu schützen (§ 7 IDG).		Diese Vorgaben sind bekannt und im Bereich der Cloud-Verwendung auch mit ausländischen Anbieteren schon heute problemlos umzusetzen.
	Im Kanton Zürich ist die Nutzung von M365 für den DAP in der kantonalen Verwaltung grundsätzlich vorgesehen (RRB Nr. 542/2022, Dispositiv I). Der Beschluss gilt für alle der IKT-Strategie unterstehenden Organisationseinheiten[1] sowie für die Kantonspolizei. Die Direktionen und die Staatskanzlei sind beauftragt, zu beurteilen, ob organisationsspezifische Regelungen notwendig sind und im Bedarfsfall solche zu erlassen (RRB Nr. 542/2022, Dispositiv III). Die Finanzdirektion erliess am 27. Januar 2023 für die Kantonsverwaltung die Allgemeine Nutzungsrichtlinie Microsoft 365. Diese konkretisiert Grundsätze und Regeln der Datenbearbeitung im DAP.		
	[1] Der Geltungsbereich der IKT-Strategie umfasst die Direktionen des Regierungsrates und die Staatskanzlei sowie die unselbstständigen Anstalten. Der Regierungsrat kann Ausnahmen vom Geltungsbereich bewilligen. Jede Organisation (z. B. selbstständige Anstalten), die an Lösungen der kantonalen Verwaltung in spezifischen Bereichen partizipiert, ist verpflichtet, sich in diesem spezifischen Bereich an die Vorgaben der IKT-Strategie zu halten (siehe Ziff. 3 IKT-Strategie).		
	Für die Gemeinden bestehen noch keine entsprechenden kantonalrechtlichen Vorgaben.		
	Der Bund und andere Kantone bzw. ausserkantonale Gemeinden handhaben die Nutzung von Cloud-Diensten, insbesondere von M365, unterschiedlich.		

	In der Lehre zeichnet sich noch keine einheitliche Meinung ab.		Das trifft nicht zu. Die Rechtslage diesbezüglich ist recht klar. Der Kanton Zürich vertritt bezüglich gewisser Rechtsfragen indes eine besonders strenge Haltung, steht damit schweizweit aber recht alleine da. Auch die Erläuterungen zu diesem Vorentwurf befassen sich interessanterweise überhaupt nicht mit den vielzähligen liberaleren Rechtsauffassungen, übrigens auch aus Behördenkreisen sowie seitens Datenschutzaufsichtsbehörden. Ein kleiner Ausschnitt: **- Rechtsgutachten Laux Lawyers AG erstattet an das OIZ der Stadt Zürich** (https://www.lauxlawyers.ch/oiz-cloud-gutachten/). **- David Rosenthal: Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act,** in: Jusletter 10. August 2020; https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf) **- David Vasella: Kommentierung zum Tätigkeitsbericht der kantonal-zürcherischen Datenschutzbeauftragten** (https://datenrecht.ch/dsb-zuerich-taetigkeitsbericht-2022/) - **privatim Merkblatt Cloud-spezifische Risiken und Massnahmen** (https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen-2/)**:** *"Das Risiko einer solchen Rechtsverletzung ist in der Analyse zu* ***berücksichtigen*** *und* ***durch vertragliche Massnahmen*** *(v.a. Verpflichtung des Cloud-Anbieters, alle Rechtsbehelfe zu ergreifen, um die Herausgabe der Daten zu verhindern, und das öffentliche Organ umgehend über behördliche Herausgabebegehren zu informieren, soweit dies dem Cloud-Anbieter erlaubt ist)* ***so weit als möglich zu reduzieren*** *.* **- Aufsichtsstelle Datenschutz Basel Landschaft – Merkblatt "Datenbearbeitung im Auftrag" i.S.v. § 7 IDG** (https://www.baselland.ch/politik-und-behorden/besondere-behoerden/datenschutz/publikationen/merkblatter-musterschreiben/downloads-2/merkblatt-auftragsdatenbearbeitung-outsourcing.pdf/@@download/file/Merkblatt Auftragsdatenbearbeitung 1.1.pdf): *"Die Frage, ob die Möglichkeit eines sog. "lawful access" (bspw. in Anwendung des Cloud-Acts […]) einer Auslagerung ohne Verschlüsselung durch das öffentliche Organ grundsätzlich entgegensteht oder lediglich ein Risiko darstellt, ist umstritten.* ***Die ASD geht aktuell davon aus, dass diesbezüglich ein risikobasierter Ansatz zulässig ist."*** **Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Basel-Stadt für das Jahr 2020-2021** (https://www.bs.ch/publikationen/dsb/taetigkeitsbericht-datenschutzbeauftragten-jahr--2020-2021.html): *"Die Übermittlung von Personendaten innerhalb der Schweiz oder der EU an Anbieter:innen, die unter dem US-amerikanischen CLOUD Act stehen, ist unseres Erachtens nicht schon unzulässig; hier wäre erst die tatsächliche Bekanntgabe an die US-Behörden unzulässig, weil sie sich weder auf eine Vereinbarung mit den USA stützt noch den gesetzlichen Vorschriften über die Rechtshilfe folgt.* ***Das diesbezügliche Risiko ist nach unserer Auffassung einer Risikobetrachtung zugänglich."*** **Daniel Dzamko, Leiter Direktionsbereich Datenschutz beim EDÖB: Überlegungen zu Recht und Risiko bei behördlicher Cloudnutzung**, in Métille (Hrsg.), L'informatique en nuage: *"Nur eine vorsätzliche Begehung ist strafbar, wobei Eventualvorsatz genügt. In Anlehnung an Rosenthal wird der Eventualvorsatz wohl dann ausgeschlossen werden können, wenn die Verantwortlichen das Risiko einer Offenbarung sorgfäl-tig prüften, angemessene (fortdauernde) Massnahmen dagegen ergriffen und das Restrisiko als genügend tief erachteten, um darauf vertrauen zu können, dass es sich nicht realisieren werde. Um dies nachweisen zu können, wird eine Dokumentation der Umstände wichtig sein. Wann und nach welchen Kriterien im Kontext der behördlichen Cloud-Nutzung ein genügend tiefes Restrisiko erreicht wurde, kann hier nicht vertieft geprüft bzw. behandelt werden.* ***Immerhin lässt sich nach meinem Dafürhalten zustimmen, dass ein risikobasierter Ansatz mit Art. 320 StGB vereinbar ist."***
	Ein im Auftrag der Zusammenarbeitsorganisation egovpartner erstelltes und am 6. Juli 2023 erstattetes Gutachten bestätigt den in der Allgemeinen Nutzungsrichtlinie Microsoft 365 verfolgten Ansatz der kantonalen Verwaltung auch für die Zürcher Gemeinden.		

	Gleichzeitig empfiehlt das Gutachten, die Bestimmungen über die Datenbearbeitung mittels M365 in gesetzlicher Form zu verankern (Markus Schefer/Philipp Glass, Gutachten zum grundrechtskonformen Einsatz von M365 durch die Gemeinden im Kanton Zürich vom 6. Juli 2023 zuhanden von egovpartner).		Aus der Diskussion zu «besonderen Personendaten» leiten die Gutachter ab, dass die Bearbeitung einer gesetzlichen Grundlage bedürfe (§ 8 Abs. 2 IDG: «Das Bearbeiten besonderer Personendaten bedarf einer hinreichend bestimmten Regelung in einem formellen Gesetz»). Die Gutachter präzisieren, dass «die Nutzung der Cloudversionen der Apps» einer hinreichenden formell-gesetzlichen Grundlage bedürfe (gemeint ist wohl, dass technische Aspekte der Umsetzung formell-gesetzlich geregelt sein müssten). Diese Ableitung gestützt auf § 8 Abs. 2 IDG ist aber unzulässig, da das effektive Risiko klar unterhalb der Eingriffsschwelle liegt: Die Gutachter gehen davon aus, dass alle Einwohner im Kanton betroffen sind, also von einem jederzeit real drohenden Risiko von Datenzugriff für jede:n Bewohner:in im Kanton Zürich aus. Diese Sachverhaltsannahme ist aber spekulativ und theoretisch. Die Betroffenheit, die das Gutachten auf Basis des US CLOUD Act ausmacht, liegt deutlich unterhalb der Eingriffsschwelle der Rechtsordnung. Das Gutachten berücksichtigt nicht, dass eine Notwendigkeit zur Prüfung erst bei Strafverfolgung gegen eine:n Bewohner:in des Kantons besteht. Man kann nicht ernsthaft sagen, dass wegen des US CLOUD Act ein «latentes» Überwachungsrisiko gegenüber allen Bewohner:innen im Kanton Zürich entsteht. Somit ist eine besondere Gefahr einer Persönlichkeitsverletzung nicht begründet und die Forderung nach einer besonderen gesetzlichen Grundlage (§ 8 Abs. 2 IDG) ist nicht angebracht. Die Anforderungen an die gesetzliche Grundlage des Verwaltungshandelns sind ohne weiteres erfüllt (Art. 5 BV i.V.m. Art. 10 Abs. 2 KV). Dies wird übrigens auch von den Gutachtern bestätigt (Ziff. 5.3.1, S. 20, mit Verweis in Fn 81). Die Cloud-Nutzung ist bei korrekt umgesetztem Projekt somit nach Art. 5 BV i.V.m. Art. 10 Abs. 2 KV rechtmässig. Es besteht kein Bedarf für eine Prüfung nach Art. 36 BV, da Art. 13 Abs. 2 BV i.V.m. Art. 10 Abs. 2 KV nicht verletzt ist.
	Gestützt auf die obigen rechtlichen Überlegungen und aufgrund der Rückmeldungen zu diesem Rechtsetzungsvorhaben soll mit § 17 VE-Gesetz über digitale Basisdienste eine gesetzliche Grundlage für cloudbasierte Anwendungen im Rahmen des DAP geschaffen werden. Nicht Gegenstand der Bestimmung bilden cloudbasierte Dienste, die ausserhalb des DAP verwendet werden (z.B. im Rahmen von Fachanwendungen), sowie lokale Anwendungen (z.B. die Office-365-Apps wie Word, sofern sie lokal genutzt werden). Die Regelung von § 17 VE-Gesetz über digitale Basisdienste beinhaltet auch die Bearbeitung von Personendaten und Informationen, welche aus einer Fachanwendung stammen, im Rahmen der cloudbasierten Applikationen des DAP. So dürfen die Mitarbeitenden der öffentlichen Organe z.B. einen cloudbasierten E-Mail-Dienst nutzen, um miteinander zu kommunizieren, und dabei Personendaten und Informationen aus Fachanwendungen wie z.B. der Geschäftsverwaltungssoftware bearbeiten. § 17 VE- Gesetz über digitale Basisdienste stellt dabei für unterschiedliche Kategorien von Personendaten und Informationen unterschiedlich strenge Anforderungen an die Verschlüsselung.		Selbst wenn man die Notwendigkeit für eine zusätzliche formell-gesetzliche Grundlage i.S.v. § 8 Abs. 2 IDG bejahen würde, so doch ausschliesslich für besondere Personendaten. Zudem ist damit auch noch nicht gesagt, dass eine solche formell-gesetzliche Grundlage neben der Legitimierung der spezifschen Bearbeitung, auch noch die technischen und organisatorischen Sicherheitsanforderungen an eine solche Bearbeitung regeln muss. Das IDG kommt generell bezüglich der technischen und organisatorischen Sicherheitsmassnahmen gut ohne spezialgesetzliche Regelungen aus, auch für besondere Personendaten. § 7 IDG, insb. Abs. 2 bietet hierzu eine absolut genügende Grundlage.
	Die Bestimmung zum DAP richtet sich an öffentliche Organe, welche cloudbasierte Anwendungen im Rahmen des DAP nutzen wollen. Ob und bis zu welchem Grad sie Cloud-Dienste nutzen wollen, liegt in ihrer gegebenenfalls bestehenden Organisationsautonomie; es ist ohne Weiteres zulässig, wenn ein öffentliches Organ z.B. darauf verzichtet, besondere Personendaten in der Cloud zu bearbeiten.		
Informationsbearbeitung durch Dritte im Rahmen des digitalen Arbeitsplatzes			
§ 17. [1] Das öffentliche Organ kann die Bearbeitung von Informationen in Anwendungen des digitalen Arbeitsplatzes an Anbieterinnen von cloudbasierten Informatikdienstleistungen übertragen, wenn sich deren Rechenzentren in der Schweiz oder in der Europäischen Union befinden, und wenn:	§ 17 Abs. 1 VE-Gesetz über digitale Basisdienste bildet die gesetzliche Grundlage dafür, dass das öffentliche Organ, welches im Rahmen des DAP cloudbasierte Anwendungen nutzen möchte, die Bearbeitung von Informationen an die Cloud-Anbieterin zur cloudbasierten Bearbeitung übertragen kann. Die Bestimmung konkretisiert und ergänzt die Vorgaben in § 6 IDG bzw. § 9 E-IDG im Hinblick auf die cloudbasierten Anwendungen des DAP.		**Ersatzlos zu streichen.** Die Bestimmung ist weder notwendig noch hilfreich. Die gesetzliche Grundlage, so sie denn notwendig ist (was bestritten wird), befindet sich einzig im ersten Satzteil. Der zweite Satzteil enthält darüber hinaus eine nicht sachlich zu begründende Voraussetzung (Einschränkung), welche für die Zwecke der Konkretisierung von § 6 IDG ohnehin nicht notwendig ist.
	Zunächst hält § 17 Abs. 1 VE-Gesetz über digitale Basisdienste generell fest, dass sich der Standort der Server auf dem Gebiet der Schweiz oder der Europäischen Union befinden muss. Ein Zugriff auf die Daten durch einen Drittstaat ist damit nicht ausgeschlossen. Allerdings kann zumindest eine physische Beschlagnahmung der Server unter Umgehung der Rechtshilfe verhindert werden.		Wer im Kontext von M365 (und darum scheint es ja den Autoren des Gesetzesartikels vornehmlich zu gehen) der Vorstellung unterliegt, dass eine physische Beschlagnahmung eines Servers (ob unter Umgehung von Rechtshilfe oder nicht) irgendeinen Nutzen spenden könnte, sollte sich ernsthafter mit der Form der Daten/Dateispeicherung in Hyperscale-Cloud-Umgebungen befassen. Bei dieser Form der Dienstebereitstellung wird es niemals möglich sein, durch Beschlagnahme einzelner Server (oder auch einer ganzer Reihe davon) tatsächlich Inhalte zu erhalten. Die umfassende Virtualsierung und die dezentrale Speicherung der einzelnen dateiverschlüsselten Dateien verunmöglichen dies. Zudem ist nicht einzusehen, weshalb in Abweichung der Grundsätze in § 19 IDG nur Serverstandorte in der Schweiz und in der der EU möglich sein sollen.
	Sodann nimmt die Bestimmung eine Zweiteilung vor in (1) besondere Personendaten und vertrauliche sowie der Geheimhaltung unterliegende Informationen (§ 17 Abs. 1 lit. a VE-Gesetz über digitale Basisdienste) und (2) Informationen, die geschäftlich als "öffentlich" oder "intern" klassifiziert sind, sowie "normale" (d.h. nicht besondere) Personen- und Sachdaten (§ 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste):		

	Kategorie 1 (lit. a): Bei Informationen und Personendaten der Kategorie 1 stehen rechtliche Bestimmungen der Übertragung der Informationsbearbeitung an eine Cloud-Anbieterin an sich entgegen (§ 6 Abs. 1 IDG und § 9 Abs. 1 E-IDG; vgl. die Erläuterungen zu § 17 Abs. 1 lit. a VE-Gesetz über digitale Basisdienste). Zulässig ist eine Übertragung bei solchen Informationen nur dann, wenn sie auch gegenüber der Cloud-Anbieterin wirksam verschlüsselt sind; liegt das Schlüsselmanagement hingegen bei der Cloud-Anbieterin oder hat diese anderweitig Zugriff auf die Schlüssel, besteht keine wirksame Verschlüsselung. Weil eine solche Verschlüsselung die Kenntnisnahme durch die Cloud- Anbieterin oder durch einen ausländischen Staat unterbindet, ist die Übertragung an eine Cloud- Anbieterin dennoch zulässig (vgl. auch Dominika Blonski, Cloud - alles Risiko? Rechtliche Vorgaben für die Auslagerung von Datenbearbeitungen in die Cloud, SJZ 2023, S. 993 ff., 997).		Die Einschränkungen basieren auf einer umstrittenen und in der Lehre nicht vorherrschenden Rechtsauffassung. Unbestritten ist, dass sämtliche bekannten Risiken im Rahmen der Einführung einer IT-Lösung adressiert und so gut wie möglich mitigiert werden müssen. Das geltende Recht schreibt dies vor. Das gilt auch für Cloud-Lösungen und das Risiko, dass ausländische Behörden aufgrund lokaler Gesetze Daten vom Cloud-Anbieter herausverlangen könnten. Es gibt aber weder unter dem IDG-ZH noch unter dem Berufs- und Amtsgeheimnis eine absolute Pflicht für öffentliche Organe, Datenherausgaben an fremde Behörden in jedem Fall zu verhindern (100% Schutz). Es braucht – wie bezüglich aller anderen Risiken – Schutzmassnahmen, und diese müssen wirksam und angemessen sein. Diese Auffassung ist breit abgestützt. Trotzdem fordert der Vorentwurf bezüglich dieses Risikos einen technisch umgesetzten 100%-Schutz für gewisse sensible Daten. Er folgt damit einer isolierten, besonders strengen Rechtsauffassung, welche schlecht begründet ist. Die Erläuterungen unterlassen es zudem sträflich (wie übrigens auch die zitierte Autorin), sich mit den vielzähligen andersgelagerten Lehrmeinungen auseinanderzusetzen. Nicht einmal die Konferenz der schweizerischen Datenschutzbeauftragten (privatim) teilt die in den Erläuterungen zitierten Begründungen umfassend. Auch die Bundeskanzlei bestätigt, dass es sich bei Behördenherausgaben (z.B. unter dem US CLOUD Act) um ein zusätzliches Risiko handelt, das aber nicht eine absolute Schranke darstellt, sondern vielmehr im Einzelfall zu beurteilen und ggf. angemessen zu mitigieren ist. Wenn ein Gesetz aber wie hier der Vorentwurf zu § 17 spezifische technische Massnahmen vorschreibt, deren Implementierung mit massiven neuen resp. anderen betrieblichen und sicherheitstechnischen Risiken verbunden ist, ist dies nicht mehr angemessen, sondern verhindert den digitalen Arbeitsplatz im Kanton Zürich nachhaltig und gefährdet dringend notwendige Digitalisierungsschritte. Es fällt auf, dass diejenigen Positionsbezüge, welche eine Verschlüsselung zwingend fordern, keine holisitische Sicht auf die Risikokontrolle nehmen (können), da sie notgedrungen abstrakt bleiben müssen; einzelne Anforderungen erscheinen so isoliert. Eine kombinierte Sicht auf Risiken und Massnahmen kann aber erst im konkreten Anwendungsfall gelingen.
	Kategorie 2 (lit. b): Bei Informationen und Personendaten der Kategorie 2 soll eine Übertragung der Informationsbearbeitung an eine Cloud-Anbieterin demgegenüber grundsätzlich zulässig sein. Auch solche Informationen sollten verschlüsselt werden; allerdings genügen insofern weniger strenge Vorgaben, als die Verschlüsselung nicht auch gegenüber der Cloud-Anbieterin wirksam sein muss bzw. ein Schlüsselmanagement durch die Cloud-Anbieterin (und damit auch ein einseitiger Zugriff durch die Cloud-Anbieterin) möglich bleibt. Das öffentliche Organ muss gemäss § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste aber alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen zur Minimierung des Risikos einer Bekanntgabe treffen und das verbleibende Restrisiko muss als vertretbar erscheinen (vgl. die Erläuterungen zu § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste). Wenn ausländische Behörden - z.B. der USA aufgrund des US CLOUD Act - auf diese Daten zugreifen, erfolgt eine grenzüberschreitende Bekanntgabe im Sinne von § 19 IDG bzw. § 36 E-IDG. Mit § 17 Abs. 1 VE-Gesetz über digitale Basisdienste wird die gesetzliche Grundlage für eine solche Bekanntgabe geschaffen, die gemäss § 19 lit. b IDG bzw. § 36 lit. a E-IDG erforderlich ist, wenn das Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten nicht gilt.		Es ist schlicht falsch, dass gemäss § 19 IDG eine gesetzliche Grundlage notwendig ist für eine grenzüberschreitende Bekanntgabe. Die erwähnte lit. b zielt auf ganz andere gesetzliche Grundlagen als es § 17 VE je sein kann. Zumal ja § 17 VE keinesfalls dafür geschaffen wurde um "bestimmte Interessen der betroffenen Personen oder überwiegende öffentliche Interessen zu schützen"! Die Kommentierung verschweigt zudem ärgerlicherweise, dass § 19 mit lit. a und lit. c IDG noch zwei weitere Tatbestände schafft, die eine grenzüberschreitende Übermittlung möglich machen (wenn das Übereinkommen nicht gilt): Gemäss lit. a würde ohne weiteres auch genügen, wenn im Empfängerstaat ein angemessener Schutz für die Datenübermittlung gewährleistet ist. Dies ist für die USA ohne weiteres dann der Fall, wenn der Adäquanzentscheid für die USA (auf Bundesebene durch den Bundesrat) bestätigt wird. Dies wird in den nächsten Monaten im Rahmen der bundesrätlichen Ratifizierung des CH-US Privacy Framework erwartet, die EU-Kommission hat diesen Adäquanzentscheid bereits vollzogen. Die befürchteten Datenherausgaben über den US CLOUD Act wären dann nach der hier vertretenen Lesart ohne weiteres gerechtfertigt. Nichts anderes ergab sich übrigens bereits aus dem Schrems II Urteil des EUGH, welches den US CLOUD Act diesbezüglich nicht tadelte (zu Recht). Gemäss lit. b von § 19 IDG wäre es dem öffentlichen Organ sodann auch ohne weiteres möglich, Daten bekanntzugeben nachdem vertragliche Sicherheitsvorkehrungen getroffen wurden. Microsoft hat die weitherum anerkannten EU Standardvertragsklauseln (Modul 3) etabliert und sichert umfassende (mehr als angemessene) Sicherheitsvorkehrungen zu, darunter auch eine sehr weitgreifende Defend-your-data Klausel, welche Microsoft sogar verpflichtet, Schweizer Blocking Statutes, wie bspw. Art. 320 StGB im gerichtlichen Verfahren um Herausgabe (unter US CLOUD Act) vorzuhalten.
	Mittels einer differenzierten Regelung sollen die genannten cloudbasierten Anwendungen in einer möglichst grundrechtskonformen Weise genutzt werden können. Die Regelung nimmt die heute auf Kantonsebene bestehende Regelung der Allgemeinen Nutzungsrichtlinie auf formell-gesetzlicher Ebene auf.		Die grundrechtskonforme Nutzung von cloudbasierten Anwendungen kann getrost den ausführenden öffentlichen Organen überlassen werden. Diese benötigen über die bestehenden Rahmenbedingungen in IDG, IDV etc. hinaus, keine weiteren Konkretisierungen, und schon gar nicht die Verkürzung der Massnahmenmittel (TOMs) auf eine solitäre technische Massnahme (end-to-end Verschlüsselung). Ein wichtiger Grundsatz des Legiferierens ist die Technologieneutralität. Diese wird hier unnötigerweise missachtet.

a. das öffentliche Organ besondere Personendaten sowie vertrauliche oder der Geheimhaltung unterliegende Informationen auch gegenüber der Cloud- Anbieterin wirksam verschlüsselt, so dass die Cloud-Anbieterin darauf nicht ohne Mitwirkung des öffentlichen Organs zugreifen kann und	Die Bearbeitung von besonderen Personendaten sowie von Informationen, die vertraulich sind oder der Geheimhaltung unterliegen, soll grundsätzlich mittels lokaler Anwendungen stattfinden. Erfasst sind die folgenden Informationen:		**Esatzlos zu streichen.** Diese Bestimmung ist weder geeignet noch nötig. Sie birgt aber massive operationelle und sicherheitstechnische Zusatzrisiken, zu massiv höheren Kosten. Was das für den digitalen Arbeitsplatz in der Praxis bedeutet: Funktionalitäten, welche den digitalen Arbeitsplatz ausmachen, werden massiv eingeschränkt oder verunmöglicht. Werden sämtliche Dokumente und Informationen, welche in der Cloud gespeichert werden, mit eigenem Schlüssel (end-to-end) verschlüsselt, sind praktisch sämtliche Cloud-Dienste (z.B. von Microsoft) nicht mehr einsetzbar. Werden «nur» Teile bzw. die Informationen und Daten mit besonders schützenswerten Inhalten verschlüsselt, können viele wichtige Cloud-Funktionen auf den verschlüsselten Inhalten nicht mehr angewendet werden. Was bedeutet dies in der Praxis: 1) Die Triage besonders schützenswerter und anderer Daten wird sehr schwierig. Das Arbeiten im digitalen Arbeitsplatz wird dadurch unnötig verkompliziert. 2) Inhaltssuchen und in verschlüsselten Daten sind im Cloud-Dienst nicht mehr möglich. 3) Die Zusammenarbeit (Collaboration) und das parallele Arbeiten auf Dokumenten ist nicht mehr möglich. 4) Da die Schlüssel «nur» auf dem eigenen Notebook funktionieren, können Dokumente z.B. auf dem Tablet oder Mobile nicht entschlüsselt werden. Sie können dort deshalb weder gelesen noch bearbeitet werden (inkl. Mail). Dies schränkt die Mobilität des digitalen Arbeitsplatzes ein. 5) Hybride Ansätze (z.B. Exchange Hybrid) haben in der Praxis sehr starke Einschränkungen von Funktionalitäten (z.B. Planner / ToDo / Teams-Raum-Kalender etc.) zur Folge und benötigen doppelte Infrastruktur, was zusätzliche Komplexität und Kosten verursacht. Fazit: Der digitale Arbeitsplatz in der öffentlichen Verwaltung ist gefährdet bzw. wird stark eingeschränkt. Somit schwindet die Attraktivität vom Arbeitsplatz und Talente werden sich andere Arbeitgeber suchen. Zudem: Die Sicherheit wird schlechter – nicht besser Wichtige Schutzmechanismen (z.B. Virenscan) greifen bei verschlüsselten Dokumenten nicht. Dies bedeutet, dass befallene Dokumente wie z.B. Excel mit Makros, ZIP-File, Phishing-PDF etc. vom Cloud-Dienst und somit vom Schutzmechanismus nicht erkannt werden können. Vom Cloud-Provider (insb. sehr ausgeprägt bei Microsoft 365) in der Cloud zur Verfügung gestellte Sicherheitsfunktionen, welche ständig weiterentwickelt und aktuell gehalten werden, sind somit punktuell ausgehebelt. Lokale oder hybride Lösungen müssen dann separat geschützt werden, was riesige Sicherheitslücken hinterlässt. Der Ukraine-Krieg zeigt deutlich auf, dass ungenügend gesicherte «on-premise» Behörden- und Verwaltungs-Umgebungen zu den beliebtesten und gefährdetsten Zielen für kriegerisch motivierte Hacker-Angriffe gehören.[1] Es ist heutzutage unter Spezialisten und IT-Verantwortlichen in Unternehmen und Behörden breit anerkannt, dass das Niveau an Sicherheit, welche moderne Cloud-Lösungen heutzutage bereitstellen, «on-premise» nicht erreicht werden kann. [1] *"We remain the most concerned about government computers that are running "on premise" rather than in the cloud. This reflects the current and global state of offensive cyber espionage and defensive cyber protection. As the SolarWinds incident demonstrated 18 months ago, Russia's intelligence agencies have extremely sophisticated capabilities to implant code and operate as an Advanced Persistent Threat (APT) that can obtain and exfiltrate sensitive information from a network on an ongoing basis. There have been substantial advances in defensive protection since that time, but the implementation of these advances remains more uneven in European governments than in the United States. As a result, significant collective defensive weaknesses remain."* - Brad Smith (Vice-Chairman Microsoft); Defending Ukraine: Early Lessons from the Cyber War (https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/)
	Besondere Personendaten: Der Begriff der besonderen Personendaten ist gleich auszulegen wie in § 3 Abs. 4 IDG bzw. § 5 Abs. 4 E-IDG. Dazu gehören namentlich Personendaten, die durch besondere Amtsgeheimnisse geschützt sind. Besondere Personendaten sind etwa Informationen über die Inanspruchnahme von Sozialhilfeleistungen (§ 3 Abs. 4 lit. a Ziff. 3 E-IDG). Diese Informationen sind durch das Sozialhilfegeheimnis geschützt (§ 47 Sozialhilfegesetz, LS 851.1).		Die strengen Anforderungen an die Verschlüsselung gälten nicht nur bei ausländischen Providern, sondern auch alle Cloud-Provider in der Schweiz wären davon betroffen (wie auch immer man "Cloud-Provider" definiert). Dies bedeutet, dass auch bei Schweizer Dienstleistern mit eigenen "Cloud"-Lösungen, besonders sensible Daten durch den Kunden verschlüsselt werden müssten, ohne Zugriffmöglichkeit durch den Schweizer Provider. Damit wird im praktischen Ergebnis ein generelles Cloud-Verbot statuiert, mit Ausnahme voll-verschlüsselter Speicherdienste.
	Vertrauliche und der Geheimhaltung unterliegende Informationen: Die Umschreibung umfasst einerseits Informationen, die geschäftlich als "vertraulich" oder "geheim" klassifiziert sind. Anderseits sind Informationen erfasst, welche aufgrund eines besonderen (d.h. nicht bloss des allgemeinen) Amtsgeheimnisses oder eines Berufsgeheimnisses der Geheimhaltung unterliegen. Teils handelt es sich dabei um besondere Personendaten (so z.B. Personendaten, die durch das Sozialhilfegeheimnis geschützt sind [vgl. § 3 Abs. 4 lit. a Ziff. 3 IDG]).		

	Die vorgeschlagene Regelung schliesst es nicht aus, dass besondere Personendaten sowie vertrauliche und der Geheimhaltung unterliegende Informationen mittels cloudbasierter Anwendungen bearbeitet werden. Allerdings muss das öffentliche Organe diese Informationen gemäss der vorgeschlagenen Lösung wirksam verschlüsseln. Wirksam ist eine Verschlüsselung, wenn sie auch gegenüber der Cloud-Anbieterin besteht, was etwa bei der sog. Double Key Encription (DKE) der Fall ist. Die Verschlüsselung muss es ausschliessen, dass die Cloud-Anbieterin ohne Mitwirkung des öffentlichen Organs Kenntnis von den Informationen erlangen kann. Dies soll eine Kenntnisnahme unter Umgehung der Regeln der internationalen Rechtshilfe sowie ohne Gewährleistung von Kontroll- und Verfahrensrechten verunmöglichen. Erforderlich ist damit, dass die Schlüsselhoheit beim öffentlichen Organ verbleibt und somit nur ein einseitiger Zugriff durch das öffentliche Organ möglich ist; das öffentliche Organ darf eine Auftragnehmerin oder einen Auftragnehmer mit der Verwaltung der Schlüssel beauftragen (sog. Cloud Access Security Broker [CASB]), sofern es sich dabei nicht um die Cloud-Anbieterin handelt und es ausgeschlossen ist, dass die Cloud-Anbieterin oder Dritte mit möglichem Zugriff auf die Daten (insbesondere eine ausländische Behörde) die Schlüssel von der Auftragnehmerin bzw. vom Auftragnehmer herausverlangen können. Verschlüsselt eine Cloud-Anbieterin die Daten selbst und/oder hat sie Zugang zu den Schlüsseln (im Fall von Microsoft etwa der Microsoft-Managed- Key [MMK]), genügt dies nicht für die in § 17 Abs. 1 lit. a VE-Gesetz über digitale Basisdienste genannten Informationen.	Für besondere Personendaten und vertrauliche/geheime Informationen muss die Verschlüsselung auch gegenüber dem Cloud-Anbieter wirksam sein. Das bedeutet, der Cloud-Anbieter darf keinen Zugriff auf die Schlüssel haben. Standardangebote von Cloud-Anbietern wie Microsoft, bei denen der Anbieter die Verschlüsselung übernimmt und Zugriff auf die Schlüssel hat (z.B. Microsoft Managed Key), genügen für diese nicht. Das bedeutet, dass die Vorgaben des Gesetzes für solche Informationen mit den Standardangeboten von Cloud-Anbietern wie Microsoft nicht umsetzbar sind. Der Vorentwurf liesse konkret bei Microsoft 365 nur noch die folgenden technischen Lösungsansätze zu: **Cloud Access Security Broker (auch "Service Encryption Gateway"):** Bei dieser Lösung werden Dritte (sog. Gateway Provider) eingesetzt, welche Daten verschlüsseln, bevor diese in die Infrastrukturen von Microsoft 365 hochgeladen werden. Solche Lösungen hindern Microsoft daran, den Inhalt zu lesen. Es werden aber Schlüssel des Gateway Providers benötigt, und die Verantwortung für das Schlüsselmanagement liegt bei diesem Gateway Provider (resp. beim öffentlichen Organ). Solche Lösungen gehen mit gewichtigen Einschränkungen einher, z.B. können dabei weder Emails noch deren Anhänge auf Malware, Spam oder weitere Sicherheitsrisiken hin untersucht werden. Die Praxistauglichkeit solcher Lösungen ist nicht gegeben. Dies zeigen verschiedene Erfahrungsberichte aus anderen Kantonen (z.B. Bern, Zug). Was verlockend klingt, geht in Tat und Wahrheit mit massiven anderweitigen Risiken und Funktionseinschränkungen einher und ist technisch und organisatorisch mit hohen Komplikationsrisiken verbunden. Die Absicherung gegenüber Microsoft könnte mit einer solchen Lösung zwar verbessert werden; es müsste aber dem Gateway-Provider Vertrauen gegeben werden. Qualitativ verändert sich die Risikosituation somit nicht (es wird einem Provider Vertrauen geschenkt). **Double Key Encryption:** Hier werden einzelne sensitive Inhalte (z.B. Dateien) verschlüsselt, nicht der Service an sich. Da für den Zugriff zwei Schlüssel, je einer von Microsoft und einer vom Kunden, benötigt wird, kann Microsoft alleine die Datei nicht entschlüsseln. Für diese Lösung müssen die zu schützenden Daten klassifiziert werden, und der Service ist nur auf gewisse Dateitypen und Emails anwendbar. Die Verantwortung für das kundenseitige Schlüsselmanagement liegt beim öffentlichen Organ. Auch bei dieser Lösung gilt es einschneidende Einschränkungen zu beachten. Die so verschlüsselten Dateien können z.B. im Rahmen der Email-Lösungen nicht auf Malware, Spam und Sicherheitsbedrohungen geprüft werden, ebenso können die Inhalte nicht indexiert und durchsucht 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.	Ohne Verschlüsselung gegenüber der Cloud-Anbieterin zulässig bleibt die Bearbeitung von Informationen gemäss § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste. Diese Bestimmung betrifft alle von § 17 Abs. 1 lit. a VE-Gesetz über digitale Basisdienste nicht erfassten Informationen, d.h. die "normalen" Personendaten sowie Informationen, die geschäftlich als "öffentlich" oder "intern" klassifiziert sind und nicht einem besonderen Amtsgeheimnis oder dem Berufsgeheimnis unterstehen. Bei diesen Informationen gilt insofern ein risikobasierter Ansatz, als das öffentliche Organ gemäss § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen zur Minimierung des Risikos einer Bekanntgabe treffen muss und das verbleibende Restrisiko als vertretbar erscheint.	**Ersatzlos zu streichen.** Die Bestimmung liefert gegenüber § 7 IDG (insb. auch Abs. 3) keinerlei Mehrwert und ist deshalb weder notwendig noch hilfreich.
	Was die zu treffenden technischen, organisatorischen und vertraglichen Massnahmen angeht, ergeben sich die Anforderungen aus der Datenschutzgesetzgebung (insbesondere § 7 IDG) und internen Umsetzungsvorgaben, die im Einzelfall - je nach Sensitivität der betroffenen Informationen - unterschiedlich streng sein können. In technischer Hinsicht genügt eine Verschlüsselung. Gemeinsamer Zweck der entsprechenden Massnahmen ist letztlich, dass das öffentliche Organ seine Verantwortung (§ 6 Abs. 2 IDG bzw. § 9 Abs. 2 E-IDG) auch tatsächlich wahrnehmen kann.	**Diese Bestimmung ist zu streichen.** Sie liefert gegenüber § 7 IDG (insb. auch Abs. 3) keinerlei Mehrwert und ist deshalb weder notwendig noch hilfreich.
	Sodann erwähnt die Bestimmung das Restrisiko, welches im Rahmen einer Risikoanalyse zu beurteilen ist. In einem ersten Schritt ist dessen Eintretenswahrscheinlichkeit abzuschätzen. In einem zweiten Schritt ist das Restrisiko als vertretbar oder nicht vertretbar zu bewerten; die Bestimmung zählt in nicht abschliessender Weise Aspekte auf, die dabei miteinzubeziehen sind:	**Diese Bestimmung ist zu streichen.** Sie liefert gegenüber § 7 IDG (insb. auch Abs. 3) keinerlei Mehrwert und ist deshalb weder notwendig noch hilfreich.
	Die Bestimmung nimmt Bezug auf die Bedeutung der Information und gibt damit vor, dass die Abwägung stets mit Blick auf die konkreten Informationen vorgenommen werden muss. Sie kann für verschiedene Informationen unterschiedlich ausfallen, z.B. je nachdem wie sensitiv die entsprechenden Informationen sind. Zu berücksichtigen ist auch, dass dieselbe Information in unterschiedlichen Zusammenhängen und je nach Verknüpfung mit anderen Informationen unterschiedlich sensitiv sein kann.	**Diese Bestimmung ist zu streichen.** Sie liefert gegenüber § 7 IDG (insb. auch Abs. 3) keinerlei Mehrwert und ist deshalb weder notwendig noch hilfreich.

	Zu berücksichtigen sind weiter der Bearbeitungszweck, d.h. die öffentliche Aufgabe, zu deren Erfüllung die Informationen bearbeitet werden, und die Art und Weise der Bearbeitung. Bei der Art und Weise des Bearbeitens relevant sind beispielsweise die Intensität (Anzahl Datensätze, Anzahl betroffene Personen) und die Dauer der Bearbeitung, die Speicherung von Daten, der Einsatz von Technologien der Künstlichen Intelligenz usw.		**Diese Bestimmung ist zu streichen.** Sie liefert gegenüber § 7 IDG (insb. auch Abs. 3) keinerlei Mehrwert und ist deshalb weder notwendig noch hilfreich.
	Die Nutzung von Cloud-Diensten wirkt sich auf die Grundrechte derjenigen Personen aus, welche die übertragenen Informationen bzw. Personendaten betreffen, weil sie mit einem rechtlichen und faktischen Kontrollverlust verbunden ist. Dieser Kontrollverlust ist erhöht, wenn die Cloud-Anbieterin nicht nur dem schweizerischen Recht unterstehen. Wenn die Cloud-Anbieterin ausländischen Regulierungen (z.B. dem US CLOUD Act) untersteht, besteht ein Risiko, dass ein Drittstaat auf die Informationen zugreift und gemäss dem ausländischen Recht keine bzw. im Vergleich zum schweizerischen Recht nur eingeschränkte Rechtsbehelfe gegen diesen Zugriff bestehen. Auch das Durchführen von Kontrollen wird erschwert. Somit führt die Übertragung der Bearbeitung von Informationen an eine Cloud-Anbieterin zu rechtlichen und faktischen Einschränkungen der Kontrollrechte über die Bearbeitung sowie zum Risiko der Datenbekanntgabe ins Ausland.		Es wird ein einzelnes (nota bene unbestritten äusserst niedriges) Risiko hochstilisiert, indem behauptet wird, dass US-Cloud-Anbieter auf Anfrage sämtliche Daten jederzeit an US-Behörden weitergeben. Dies ist Unsinn. Gerade Microsoft verpflichtet sich in ihren Verträgen zu umfassenden Prüf- und Abwehrmassnahmen gegen die Weitergabe von Daten, welche sich in der Praxis als effektiv herausstellen. Keiner Behörde wird direkter, pauschaler oder uneingeschränkter Zugriff auf Daten gewährt. Offenbar zweifeln die Autoren des Erläuterungsberichts an den Abläufen, wie ein Gericht in den USA mit der Staatsanwaltschaft arbeitet. Man sollte besser diesbezüglich in weitere Sachverhaltsklärung investieren, es wären dann Einschätzungen mit konkretem Sachverhaltsbezug möglich. Der Nutzen wäre höher.
	Für die Nutzung von Cloud-Diensten spricht demgegenüber regelmässig der Aspekt der Effizienz der Aufgabenerfüllung. Die Einführung von cloudbasierten Anwendungen ermöglicht eine flexible und skalierbare Arbeitsinfrastruktur auf dem Stand der Technik. Dabei wird auch eine Optimierung der Verwaltungsabläufe und eine Steigerung der Kosteneffizienz erwartet. Ferner wird davon ausgegangen, dass die Nutzung von externen Cloud-Diensten die Sicherheit erhöht, weil die Cloud-Anbieterinnen Sicherheitsvorkehrungen treffen, welche die Sicherheitsmassnahmen der Nutzerinnen und Nutzer beim lokalen Gebrauch von Anwendungen übersteigen. Umgekehrt ist mit jeder Übertragung immer ein Risiko für die Informationssicherheit verbunden. Dies gilt etwa mit Blick auf das Risiko der falschen Handhabung der Cloud-Services durch die Nutzenden beim öffentlichen Organ; wobei dieses Risiko umgekehrt freilich auch beim lokalen Gebrauch bzw. beim Gebrauch von IT-Anwendungen insgesamt besteht.		
[2] Im Übrigen gelten die Bestimmungen des Gesetzes über die Information und den Datenschutz.	Der VE-Gesetz über digitale Basisdienste konkretisiert und ergänzt die Bestimmungen zur Informationsbearbeitung im Auftrag (§ 6 IDG bzw. § 9 E-IDG), zur Informationssicherheit (§ 7 IDG bzw. § 10 E-IDG) sowie zur Datenschutz-Folgenabschätzung (§ 10 IDG bzw. § 32 E-IDG). Er bildet zudem im Falle der Informationen gemäss § 17 Abs. 1 lit. b VE-Gesetz über digitale Basisdienste eine gesetzliche Grundlage im Sinne von § 19 lit. b IDG bzw. § 36 lit. a E-IDG. Die Bestimmungen des IDG bzw. E-IDG und des VE-Gesetz über digitale Basisdienste kommen kumulativ zur Anwendung, was mit dem deklaratorischen Verweis in § 17 Abs. 2 VE-Gesetz über digitale Basisdienste klargestellt wird.		**Ersatzlos zu streichen.**
			Fazit: § 17 über die Cloud-Nutzung beim digitalen Arbeitsplatz ist ersatzlos zu streichen, weil er • auf falschen Annahmen – rechtlich wie faktisch – basiert, • gesetzgeberisch weder notwendig noch hilfreich ist, • operative und sicherheitstechnische Risiken birgt, • zu massiv höheren Kosten führt, • eine umstrittene, partikuläre und schlecht begründete Rechtsauffassung zementiert, • die dringend notwendige Digitalisierung der Behörden (aber auch von Privaten) gefährdet, • faktisch ein Cloud-Verbot (auch von Schweizer Anbietern!) statuiert, und so • Innovationen und Knowhow-Aufbau verhindert.