Kanton Zürich
Staatskanzlei
Frau Dr. jur. Kathrin Arioli
Neumühlequai 10
8001 Zürich

Per E-Mail an:
florian.bergamin@sk.zh.ch

Bern, 29. Mai 2024

Stellungnahme zum Gesetz über digitale Basisdienste (Neuerlass)

Sehr geehrte Frau Arioli,
sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 13. Februar 2024 vom Kanton Zürich eröffnete Vernehmlassung über das Gesetz über digitale Basisdienste (Neuerlass). Der Schweizerische Verband der Telekommunikation (asut) vertritt die Interessen der Kommunikationsinfrastruktur- und Netzwerkbranche in der Schweiz, wozu auch Betreiber und Anbieter von Cloud-Dienstleistungen gehören. Unsere Mitglieder sind daher direkt vom Gesetz über digitale Basisdienste betroffen. Gerne senden wir Ihnen hiermit unsere Einschätzungen zum Gesetzesentwurf.

Grundsätzlich begrüsst asut die Gesetzesvorlage. Durch die Schaffung von Basisdiensten wird eine Vereinheitlichung von grundlegenden Diensten und Infrastrukturen angestrebt. Dies kann die digitale Transformation der öffentlichen Hand im Kanton Zürich beschleunigen und führt zu mehr Effizienz und tieferen Kosten, als wenn jedes einzelne öffentliche Organ die entsprechenden Dienste selbst konzipieren, beschaffen oder erbringen würde. Als Verband der Informations- und Kommunikationstechnologien (ICT) beschränken wir uns in unserer Stellungnahme auf einige ausgewählte technische Aspekte.

Geltungsbereich §2
Das Gesetz gilt nicht nur für die öffentliche Verwaltung im engeren Sinne, sondern für alle öffentlichen Organe, wozu auch Spitäler oder Universitäten gehören. Einige dieser Organisationen betreiben bereits eigene Basisdienste oder greifen auf Basisdienste Dritter zu, die sich in der Praxis bewährt haben. Der Geltungsbereich gemäss §2 im Zusammenspiel mit den Regelungen für die einzelnen Basisdienste soll so ausgelegt werden, dass bereits bestehende Basisdienste weiterbetrieben und auch weiterentwickelt werden können (siehe auch Anmerkungen zur Authentifizierung).

Standards und Schnittstellen §3
Aus Sicht der Branche ist es richtig, dass sich der Regierungsrat an internationalen Standards und dem Stand der Technik orientiert. Dabei ist jedoch zu berücksichtigen, dass gerade im ICT-Bereich der technische Fortschritt sehr rasch erfolgt und Innovationszyklen immer kürzer werden. Wir empfehlen daher, dass der Regierungsrat vor Verbindlicherklärung von Standards betroffene Branchen

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

und Unternehmen anhört. Damit wird sichergestellt, dass diese Standards mit den Angeboten und Möglichkeiten des Marktes vereinbar sind.

Nutzung des Authentifizierungsdienstes des Bundes §7 / Anmeldung [zum Webzugang] §12
asut begrüsst und unterstützt die Einführung der e-ID des Bundes. Diese Vertrauensinfrastruktur stellt eine wichtige Grundlage für digitale Dienstleistungen bei der Verwaltung und in der Wirtschaft dar. Dies gilt im Grundsatz auch für den Authentifizierungsdienst des Bundes (AGOV). Gemäss §7 ist die Nutzung des AGOV durch öffentliche Organe freiwillig. In Bezug auf den Webzugang ist die Verwendung von AGOV jedoch gemäss §12 zwingend. Wie eingangs erwähnt, ist dies für diejenigen öffentlichen Organe problematisch, die bereits einen bestehenden Authentifizierungsdienst nutzen. Dies betrifft beispielsweise die Zürcher Hochschulen und die Universität, da alle Schweizer Hochschulen den Identifizierungsdienst und den Authentifizierungsdienst der Stiftung SWITCH verwenden. 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 abdeckt. Daher soll die Nutzung von AGOV für den Webzugang gemäss §12 mit einer Kann-Formulierung versehen werden, solange ein gleichwertiger Authentifizierungsdienst genutzt wird.

Informationsbearbeitung durch Dritte im Rahmen des digitalen Arbeitsplatzes §17 Ziff. 1
Die Nutzung cloudbasierter Dienste soll nur zulässig sein, wenn sich die entsprechenden Rechenzentren in der Schweiz oder der Europäischen Union befinden. Es fehlt jedoch eine sachliche Begründung, wieso beispielsweise weitere Länder aus dem Europäischen Wirtschaftsraum (Liechtenstein, Norwegen und Island) oder Grossbritannien nicht zulässig sind. Es soll daher geprüft werden, ob diese Liste erweitert werden kann (z.B. gemäss Anhang 1 der Datenschutzverordnung).

Informationsbearbeitung durch Dritte im Rahmen des digitalen Arbeitsplatzes §17 Ziff. 1 Lit. a
Besonders schützenswerte Personendaten sowie vertrauliche oder geheime Informationen erfordern gemäss §17 Ziff. 1 Lit. a eine sogenannte «Double Key Encryption». Danach müssen nicht nur die Daten in den Clouddiensten verschlüsselt sein, sondern auch die dazu notwendigen Schlüssel dürfen dem Cloudanbieter nicht zugänglich sein. Dieses Prinzip ist komplexer, schwerfälliger und aufwändiger, da eine zusätzliche Organisation für die Schlüsselverwaltung berücksichtigt werden muss. Dies hat negative Auswirkungen auf die Flexibilität und Agilität bei der Gestaltung des digitalen Arbeitsplatzes und führt zu einem erhöhten Aufwand und grösseren Kosten. Dies würde insbesondere kleinere öffentliche Organe betreffen, welche nicht auf entsprechende interne IT-Ressourcen zugreifen können, sondern externe Dritte damit beauftragen müssen.

Die «Double Key Encryption» würde zudem die Funktionalität des digitalen Arbeitsplatzes deutlich einschränken. Colaborations-Lösungen, die Nutzung von AI-Algorithmen, aber auch Sicherheitsfunktionen wie Virenschutz, Phishing-Prävention oder Backup-Lösungen wären nicht mehr durch den Cloudanbieter mögliche oder würden deutlich eingeschränkt.

Die explizite Forderung nach «Double Key Encryption» im vorliegenden Gesetzesentwurf überrascht, da die heute etablierte Praxis im Risikomanagement bei der Informationssicherheit nicht ausschliesslich auf technische Massnahmen abstützt. Vielmehr wird eine optimale Kombination von technischen, organisatorischen und vertraglichen Massnahmen eingesetzt. Dies reduziert nicht nur die Komplexität sowie Aufwand und Kosten, sondern erlaubt auch eine weitergehende Differenzierung des Schutzniveaus der Daten und Informationen.

Zudem fehlen im erläuternden Bericht zu §17 Ziff. 1 Lit. a der Hinweis, dass es neben der «Double Key Encryption» auch andere technische Massnahmen gibt, bei denen das Schlüsselmanagement in der Hand des betreffenden Organs bleibt.

Aus diesen Gründen lehnen wir die einschränkende Forderung nach «Double Key Encryption» ab und empfehlen eine erweiterte Regelung, welche technische, organisatorische und vertragliche Massnahmen kombiniert.

Informationsbearbeitung durch Dritte im Rahmen des digitalen Arbeitsplatzes §17 Ziff. 1 Lit. b
In diesem Paragrafen wird der Umgang mit Informationen geregelt, die nicht besonders schützenswert, vertraulich oder geheim sind. Die Formulierung «alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen» ist dabei aus mehreren Gründen unglücklich. Einerseits ist gänzlich unbestimmt, welches Schutzniveau erreicht werden soll und welche Massnahmen noch als zumutbar gelten. Dies führt zu Unklarheiten und letztlich zu Rechtsstreitigkeiten zwischen öffentlichen Organen und Cloud-Anbietern. Zudem geht diese Formulierung faktisch über «Double Key Encryption» hinaus, falls diese als zumutbar klassifiziert wird, da zusätzlich organisatorische und vertragliche Massnahmen gefordert werden. Daher soll §17 Ziff. 1 Lit. b konkretisiert werden oder allenfalls ganz gestrichen werden, falls die Anforderungen gemäss Datenschutzgesetz für diese Informationen ausreichen.

Wir danken Ihnen bestens für die Berücksichtigung unserer Anliegen. Bei Fragen stehen wir mit unseren Experten gerne zur Verfügung.

asut – Schweizerischer Verband
der Telekommunikation

Peter Grütter
Präsident