Verordnung über die Informationstechnologie (IT-Verordnung, ITV) [1,2]

(Vom 1. September 2015)

Der Regierungsrat des Kantons Schwyz,

gestützt auf §§ 3 und 4 des Gesetzes über die Organisation der Regierungsrates und der kantonalen Verwaltung vom 27. November 1986[3] sowie § 42 Abs. 3 des Gesetzes über die Öffentlichkeit der Verwaltung und den Datenschutz vom 23. Mai 2007[4],

beschliesst:

I. Allgemeine Bestimmungen

§ 1 [5] Zweck

Diese Verordnung regelt Zuständigkeiten, Aufgaben und Sicherheitsanforderungen bei der Steuerung und beim Einsatz der Informationstechnologie (IT) in der kantonalen Verwaltung.

§ 2 [6] Geltungsbereich

[1] Die Verordnung gilt für:
a) die Departemente, Staatskanzlei und Ämter der kantonalen Verwaltung;
b) die Benutzer der kantonalen IT;
c) berechtigte Dritte, soweit die Sicherheit, Funktionsfähigkeit und Verfügbarkeit der IT betroffen sind.

[2] Für die kantonalen Gerichte, Anstalten und Schulen gilt diese Verordnung, soweit diese Informatikmittel oder digitale Leistungen des Kantons beziehen. Die Gerichte werden in diesem Fall gleich behandelt wie ein Departement, die Anstalten und Schulen wie ein Amt.

§ 3 [7] Ausnahmen

Die Verordnung kommt namentlich nicht zur Anwendung bei:
a) Funk-, Alarmierungs-, Schliess- und Einsatzleitsystemen sowie der Notruftelefonie der Kantonspolizei;
b) speziellen Informatikmitteln, die der polizeilichen Ermittlungsarbeit und weiteren spezifischen Polizeitätigkeiten dienen;
c) eigenen Netzen der kantonalen Schulen;
d) kantonalen Anlagen der Gebäudetechnik;
e) kantonseigenen Anlagen, die ausschliesslich der Steuerung technischer Prozesse dienen.

[2] Für die Informationstechnologie in diesen Bereichen ist das zuständige öffentliche Organ verantwortlich.

§ 4 [8] Begriffe

Im Sinne dieser Verordnung bedeuten:

a) Informationstechnologie (IT): die Steuerung, Planung und Einführung sowie der Betrieb und Unterhalt von Prozessen und Techniken, welche der elektronischen oder elektronisch unterstützten Bearbeitung von Informationen aller Art und deren Übermittlung inklusive Telekommunikation dienen;
b) Informatikmittel: Geräte, Einrichtungen und Dienste, insbesondere Kommunikationsnetzwerke, Betrieb- und Datenbearbeitungssysteme, Hard- und Software sowie Supportprogramme, die der elektronischen Erfassung, Verarbeitung, Speicherung, Übermittlung, Auswertung, Archivierung oder Vernichtung von Informationen dienen;
c) Basisdienste: Informatikmittel, die der verwaltungsweiten Grundversorgung und der Zusammenarbeit dienen, insbesondere Basisinfrastruktur und Querschnittsanwendungen, ausgenommen Fachanwendungen;
d) Fachanwendungen: Informatikmittel, welche zur Steuerung und Abwicklung von Geschäftsabläufen und zur spezifischen Aufgabenerfüllung des zuständigen öffentlichen Organs erforderlich sind;
e) digitale Leistungen: Dienstleistungen im Bereich IT, für die das Amt für Informatik zuständig ist und die es selbst oder durch beauftragte Dritte für die Benutzer erbringt;
f) Benutzer: natürliche oder juristische Person, welche zur Erfüllung einer öffentlichen Aufgabe von einem Informatikmittel Gebrauch macht;
g) Informationen: alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger;
h) Informationssicherheit: alle Massnahmen zum Schutz von Informationen und Informatikmitteln, die zur Gewährleistung ihrer Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit dienen;
i) Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept): strukturierte Beschreibung der Sicherheitsanforderungen an ein Informatikmittel, der geplanten und umgesetzten Sicherheitsmassnahmen sowie der verbleibenden Restrisiken;
j) IT-Sicherheit: organisatorische, personelle und technische Massnahmen im Bereich der Informationssicherheit, wie Sicherung der Stromversorgung und Netzwerkverbindungen, sichere Programme, Systeme zur Erkennung schädlicher Software, Einrichtung einer klaren und sicheren Informationsstruktur und -ablage, Schulung der Benutzer;
k) IT-Grundschutz: minimale organisatorische, personelle und technische Sicherheitsvorkehrungen im Bereich der IT-Sicherheit zur Gewährleistung des normalen Schutzbedarfs.

II. Grundsätze

§ 5 [9] Ziele

[1] Die IT unterstützt die Wirtschaftlichkeit, Wirksamkeit und Sicherheit von Geschäftsabläufen.

[2] Sie dient der Erfüllung der öffentlichen Aufgaben und richtet sich nach den Bedürfnissen der Benutzer.

§ 6 [10] Beschaffung

[1] Die Beschaffung von Informatikmitteln erfolgt gemäss der Binnenmarktgesetzgebung, den interkantonalen und kantonalen Vorschriften über das öffentliche Beschaffungswesen und der kantonalen Finanzhaushaltsgesetzgebung.
[2] Die Zulässigkeit der Beschaffung setzt voraus, dass:
a) der Bedarf nicht durch bestehende Basisdienste oder Fachanwendungen gleichwertig abgedeckt werden kann;
b) bei vertraglichen Abreden anerkannte Standardverträge verwendet werden;
c) die Anforderungen an den Datenschutz und die Informationssicherheit eingehalten werden;
d) bestehende Standards zwecks Kompatibilität und Revisionstauglichkeit der Informatikmittel übernommen werden;
e) das IT-Vorhaben vorgängig durch das Amt für Informatik geprüft und das Ergebnis berücksichtigt wurde;
f) die weitergehenden Vorgaben des Amts für Informatik beachtet werden.
[3] Die Departemente, die Staatskanzlei und die Ämter entwickeln grundsätzlich keine eigenen Informatikmittel. Vorbehalten bleiben Entwicklungen, Anpassungen oder Weiterentwicklungen durch das Amt für Informatik.

§ 7 [11]

§ 8 [12] Zusammenarbeit

[1] Bei der Weiterentwicklung der Basisdienste und der Fachanwendungen ist die harmonisierte Zusammenarbeit mit den Gemeinden und Bezirken, anderen Kantonen und dem Bund unter Wahrung der Grundsätze dieser Verordnung anzustreben.
[2] Die Departemente, die Staatskanzlei und die Ämter koordinieren ihre Zusammenarbeitsvorhaben mit dem Amt für Informatik.

III. Zuständigkeiten

§ 9 [13] Regierungsrat

Der Regierungsrat:
a) bestimmt und überwacht die mehrjährige strategische Ausrichtung der digitalen Verwaltung;
b) legt auf Antrag des Finanzdepartements die Organisation der Informatikmittel, IT-Vorhaben und Informationssicherheit fest;
c) erlässt Weisungen über die Informationstechnologie;
d) entscheidet bei Uneinigkeiten zwischen den Departementen, der Staatskanzlei, den Ämtern und dem Amt für Informatik.

§ 10 [14] Departemente, Staatskanzlei und Ämter

[1] Die Departemente, die Staatskanzlei und die Ämter sind für den Einsatz der ihnen bereitgestellten oder genehmigten Informatikmittel unter Einhaltung dieser Verordnung verantwortlich und:

a) treffen alle erforderlichen Massnahmen im Bereich der Informationssicherheit, um ihre Informationen und Informatikmittel vor missbräuchlichem Zugriff, unbefugter Bearbeitung, Beschädigung, Verlust und Funktionsbeeinträchtigung zu schützen oder schützen zu lassen;
b) koordinieren die Informatikbelange innerhalb ihres Zuständigkeitsbereichs und arbeiten mit dem Amt für Informatik unter Einhaltung der Weisungen und zentralen Führungsmethodik bei IT-Vorhaben zusammen;
c) melden IT-Vorhaben vor Beginn der Planung dem Amt für Informatik;
d) gewähren den Aufsichts- und Justizorganen im Umfang ihrer gesetzlichen Befugnisse und in Absprache mit dem Amt für Informatik Einsicht in die erforderlichen Informationen.

[2] Die Departemente und die Staatskanzlei:

a) wirken bei Vorhaben im Bereich der Basisdienste mit;
b) bestimmen einen Beauftragten für Informationssicherheit (ISB) in ihrem Zuständigkeitsbereich zur Aufgabenerfüllung nach § 17a Abs. 2.

[3] Die Ämter sind bei ihren Fachanwendungen im Rahmen der Vorgaben des Amts für Informatik zuständig für:

a) deren Auswahl, Planung, Beschaffung und Einführung;
b) deren Betrieb, und Unterhalt;
c) die Informationssicherheit und den Datenschutz.

§ 11 [15] Finanzdepartement

Dem Finanzdepartement obliegt:

a) die Entwicklung und Umsetzung der mehrjährigen strategischen Ausrichtung der digitalen Verwaltung;
b) die Beratung des Regierungsrates in allen Informatik- und Informationssicherheitsbelangen;
c) die Umsetzung der Organisation der Informatikmittel, IT-Vorhaben und Informationssicherheit;
d) die Bezeichnung des kantonalen Informationssicherheitsbeauftragten (KISB);
e) der Erlass von Vorgaben zur Steuerung und Abwicklung von IT-Vorhaben, insbesondere von Projekten, Beschaffungen, Auslagerungen und Weiterentwicklungen sowie der Informationssicherheit.
f) die Zusammenarbeit mit den Departementen, der Staatskanzlei, den Gerichten, Anstalten und Schulen zum Zweck einer geordneten und wirtschaftlichen Entwicklung der Informatik.

§ 12 [16]

§ 13 [17] Amt für Informatik

[1] Das Amt für Informatik ist verantwortlich für:

a) den Betrieb, den Unterhalt und die Weiterentwicklung der Basisdienste;
b) die Informationssicherung und -wiederherstellung;
c) die Fachaufsicht über den KISB;
d) die Bereitstellung wirtschaftlicher und wirksamer Informatikmittel;
e) die Gewährleistung einer angemessenen Redundanz und Standardisierung der Basisdienste;
f) den Beizug des Staatsarchivs bei der Planung von IT-Vorhaben;
g) die Genehmigung und Unterstützung von IT-Vorhaben;
h) die Bereitstellung eines IT-Ausbildungsangebotes für die Benutzer;
i) die Erarbeitung und Erbringung von digitalen Leistungen in Zusammenarbeit mit den Departementen, der Staatskanzlei und den Ämtern;
j) die Führung eines aktuellen, zentralen Benutzerverzeichnisses innerhalb der Telekommunikationssysteme.

[2] Es kann den Bezirken und Gemeinden für die Beratung und Koordination in Informatikbelangen zur Verfügung stehen.

§ 14 [18]

§ 15 [19] Telekommunikationssysteme

[1] Die Telekommunikationssysteme werden durch das Amt für Informatik bereitgestellt.

[2] Daneben bestehen folgende Zuständigkeiten:

a) das Hochbauamt veranlasst und überwacht die notwendigen baulichen Installationen im Telekommunikationsbereich in den Gebäuden der kantonalen Verwaltung in Koordination mit dem Amt für Informatik;
b) die Staatskanzlei führt die Telefonzentrale und ein aktuelles, zentrales Telefonnummernverzeichnis;
c) die Kantonspolizei und der kantonale Führungsstab sind für ihre spezifischen Kommunikationsbedürfnisse besorgt.

IV. Informationssicherheit [20]

§ 16 [21] Schutzziele und Schutzbedarf

[1] Die Schutzziele stellen sicher, dass Informationen und Informatikmittel:

a) nur für Berechtigte zugänglich sind (Vertraulichkeit);
b) bei Bedarf verfügbar sind (Verfügbarkeit);
c) nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität) und
d) ihre Nutzung nachvollziehbar gewährleistet ist (Nachvollziehbarkeit).

[2] Zur Erreichung der Schutzziele sind die Informationen und Informatikmittel einzuordnen nach:

a) normalem Schutzbedarf;
b) besonderem Schutzbedarf.

[3] Es gelten folgende allgemeinen Sicherheitsgrundsätze:

a) Informatikmittel sind unter Beachtung der Informatiksicherheit gegen Verlust und unerwünschte Einwirkungen zu sichern;

b) Informationen sind unter Beachtung der Informationssicherheit gegen unbefugten Zugriff und unbefugte Bearbeitung zu schützen;
c) soweit kein besonderer Schutzbedarf die Führung eines aktuellen ISDS-Konzepts erfordert, genügt der IT-Grundschutz.

§ 16a [22] Klassifikation

[1] Informationen sind in einem einfachen Prozess zu unterteilen in:
a) öffentlich: die Veröffentlichung erfolgt durch Freigabe des zuständigen öffentlichen Organs, soweit keine Risiken für die Informationssicherheit bestehen;
b) intern: die Kenntnisnahme durch Unbefugte kann die Erfüllung öffentlicher Aufgaben beeinträchtigen;
c) vertraulich: die Kenntnisnahme durch Unbefugte kann die Erfüllung öffentlicher Aufgaben erheblich beeinträchtigen;
d) geheim: die Kenntnisnahme durch Unbefugte kann die Erfüllung öffentlicher Aufgaben schwerwiegend beeinträchtigen.
[2] Nicht klassifizierte Informationen gelten als vertraulich, soweit sie Personendaten enthalten. Andernfalls sind sie als intern zu bewerten und haben einen normalen Schutzbedarf.
[3] Informatikmittel, die vertrauliche oder geheime Informationen enthalten, haben einen besonderen Schutzbedarf. Sein Umfang und die erforderlichen Massnahmen bestimmen sich durch das ISDS-Konzept.

§ 17 [23] Zuständigkeiten

[1] Der Regierungsrat trägt die Gesamtverantwortung für die Informationssicherheit und legt die strategischen Leitlinien der Informationssicherheit fest.
[2] Das Finanzdepartement:
a) erlässt Vorgaben zur Umsetzung des Schutzbedarfs und der Klassifikation;
b) genehmigt die zu verwendenden Informatikmittel mit besonderem Schutzbedarf;
c) steuert die Gewährleistung der Schutzziele mittels eines Informationssicherheits-Management-Systems (ISMS).
[3] Die Departemente, die Staatskanzlei und die Ämter:
a) bestimmen für ihre Informationen und Informatikmittel den Schutzbedarf und die Klassifikation;
b) führen nach den Vorgaben des KISB je ein aktuelles ISDS-Konzept für Informationen und Informatikmittel mit besonderem Schutzbedarf.
[4] Das Amt für Informatik unterstützt die Departemente, Staatskanzlei, Ämter und Benutzer bei der Festlegung und der Umsetzung von Sicherheitsmassnahmen.

§ 17a [24] Informationssicherheitsbeauftragte

[1] Der KISB nimmt insbesondere folgende Aufgaben wahr:
a) er führt und entwickelt das ISMS und erstellt die ISDS-Konzeptvorlage;
b) er berät und unterstützt die zuständigen Organe bei der operativen Umsetzung der Informationssicherheit;

c) er erstattet dem Finanzdepartement regelmässig Bericht über den Stand der Informationssicherheit in der kantonalen Verwaltung und informiert es über bekannte und neue Bedrohungen und über Massnahmen, die dagegen zu ergreifen sind;
d) er besorgt die fachliche Führung der ISB, erstellt ihr Pflichtenheft und bestimmt ihre Aus- und Weiterbildung;
e) er erlässt Richtlinien und Empfehlungen für die Benutzer und schult und sensibilisiert diese regelmässig im Bereich der Informationssicherheit.

[2] Die ISB sind insbesondere für die interne Umsetzung der Vorgaben im Bereich der Informationssicherheit und des ISMS zuständig.

V. Gebrauch und Missbrauch von Informatikmitteln [25]

§ 18 [26] Verantwortlichkeit

[1] Alle Benutzer und berechtigten Dritten sind für den rechtmässigen und sicheren Gebrauch der Informatikmittel verantwortlich.
[2] Diese Verordnung bildet einen integrierenden Bestandteil der Anstellungs- bzw. Auftragsbedingungen des Kantons.

§ 19 [27] Grundsätze

[1] Es dürfen nur die vom Amt für Informatik bereitgestellten oder genehmigten Informatikmittel verwendet werden.
[2] Die Informatikmittel dienen grundsätzlich der Erfüllung dienstlicher Aufgaben.
[3] Zugangsinformationen sind persönlich und dürfen nicht weitergegeben werden.
[4] Beim Einsatz privater Informatikmittel als Arbeitsmittel finden die Vorschriften dieser Verordnung Anwendung, soweit dies zur Gewährleistung der Informationssicherheit erforderlich ist.

§ 20 [28] Private Nutzung

[1] Die Verwendung von Informatikmitteln zu privaten Zwecken darf weder missbräuchlich sein noch den Dienstbetrieb erschweren, einschränken oder die Sicherheit gefährden.
[2] Sie unterliegt unter Vorbehalt abweichender Regelungen den gleichen Gebrauchs- und Missbrauchsvorschriften wie die dienstliche Benutzung.
[3] Private Informationen der Benutzer sind in einer separaten Ablage aufzubewahren, welche die Bezeichnung «privat» trägt.

§ 21 [29] Besondere Berechtigungen

[1] Ist der Benutzer verhindert und besteht Notwendigkeit und Dringlichkeit, hat der Vorsteher des Departements, der Staatskanzlei und des Amts oder eine von ihm schriftlich ermächtigte Person unter folgenden Vorbehalten Zugang zu dessen Informationen:

a) als «privat» gekennzeichnete Ablagen dürfen weder geöffnet noch gelöscht werden;
b) Informationen, deren privater Inhalt aus dem Betreff oder Dateinamen ersichtlich ist, dürfen weder geöffnet noch gelöscht werden;
c) alle übrigen Informationen dürfen zwecks Bearbeitung geöffnet werden;
d) Informationen, deren privater Inhalt erst nach dem Öffnen ersichtlich ist, dürfen nicht mehr weiterbearbeitet werden und der Benutzer muss so bald wie möglich über den Vorgang informiert werden;
e) über den Inhalt der geöffneten privaten Informationen ist Stillschweigen zu bewahren.

2 Bei Beendigung des Arbeits- bzw. Auftragsverhältnisses hat der Benutzer seine privaten Informationen zu löschen und die übrigen Informationen gemäss den Weisungen des Vorstehers des Departements, der Staatskanzlei und des Amts oder der von ihm schriftlich ermächtigten Person bereitzustellen.

3 Kann der Benutzer dieser Pflicht bis zur Beendigung des Arbeits- bzw. Auftragsverhältnisses nicht nachkommen, werden seine privaten Informationen in sinngemässer Anwendung von Abs. 1 aussortiert und gelöscht.

§ 22 [30] Missbrauch

1 Missbräuchlich ist jede Verwendung der Informatikmittel, die gegen diese Verordnung oder geltendes Recht verstösst.

2 Als missbräuchlich gilt insbesondere:

a) die Einrichtung, der Anschluss oder die Installation nicht genehmigter Informatikmittel;
b) die Manipulation von Informatikmitteln des Kantons;
c) Vorkehrungen zur Störung des Betriebs der Informatikmittel;
d) die Erstellung, Speicherung, Ausführung und Verbreitung von Fernsteuerungs-, Spionage- und Virenprogrammen;
e) der Versand von Informationen in Form von E-Mails oder in anderen Formaten in Täuschungs- oder Belästigungsabsicht und privater Massenversendungen;
f) die unbefugte Weitergabe und Bearbeitung von Informationen mit beleidigendem, diskriminierendem, rassistischem, pornografischem oder sonstigem herabsetzendem Inhalt;
g) das widerrechtliche Kopieren von Informationen oder Software jeglicher Art.

VI. Schutz- und Kontrollmassnahmen

§ 23 [31] Technischer Schutz

1 Die Schutzmassnahmen bezwecken die Überprüfung und Gewährleistung der technischen Sicherheit, Funktionsfähigkeit und Verfügbarkeit der bereitgestellten Informatikmittel.

2 Zum Schutz gegen technischen Schaden und Missbrauch werden vorrangig technische Massnahmen eingesetzt, wobei die Interessen von Benutzern und berechtigten Dritten angemessen zu berücksichtigen sind.

[3] Zur Vermeidung und Behebung von Schäden oder Missbrauch kann das Amt für Informatik namentlich:
a) ein geeignetes Überwachungs- oder Analysewerkzeug einsetzen;
b) den Zugang zu bestimmten Internetadressen oder Telefonnummern beschränken oder verhindern;
c) den Zugang zu oder den Betrieb von Informatikmitteln zeitweise oder dauerhaft einschränken;
d) eine Schwachstellenanalyse durch Einsatz anerkannter Methoden und Werkzeuge durchführen oder durch beauftragte Dritte durchführen lassen.

§ 24 [32] Aufzeichnungen

[1] Beim Benutzen der Informatikmittel können jederzeit Kommunikationsranddaten und Systemprotokolle aufgezeichnet werden:
a) bei der Anmeldung am PC;
b) beim Zugriff auf Basisdienste und Fachanwendungen;
c) beim E-Mailverkehr;
d) beim Internet-Zugriff;
e) bei Telefonieverbindungen.
[2] Die Aufzeichnungen dienen insbesondere:
a) zur Kontrolle der Einhaltung dieser Verordnung;
b) zur Behebung von Störungen bei den IT-Systemen;
c) zur Optimierung von Prozessen.
[3] Zur Auswertung dieser Aufzeichnungen können automatisierte Verfahren eingesetzt werden.

§ 25 Anonyme Auswertung

[1] Die Aufzeichnungen können jederzeit in anonymer Form ausgewertet werden.
[2] Die anonyme Auswertung dient ausschliesslich statistischen Zwecken und lässt keine Rückschlüsse auf einzelne Personen zu.

§ 26 [33] Pseudonyme Auswertung

[1] Wird aufgrund der anonymen Auswertung ein Missbrauch vermutet, kann das Amt für Informatik stichprobenartige, pseudonyme Auswertungen vornehmen.
[2] Der Vorsteher des betroffenen Departements bzw. der Staatskanzlei und des Amts wird über das Resultat der pseudonymen Auswertungen informiert.
[3] Pseudonyme Auswertungen können auch zur Prozessoptimierung eingesetzt werden, soweit die betroffenen Benutzer vorab über Art und Umfang der Auswertung informiert wurden.

§ 27 [34] Benutzerbezogene Auswertung

[1] Besteht nach der pseudonymen Auswertung ein konkreter Missbrauchsverdacht, können benutzerbezogene Auswertungen der Zugriffs-, E-Mail-, Internet- und Telefonprotokolle durch den Vorsteher des Departements oder der Staatskanzlei und nach vorheriger Konsultation des Amtsvorstehers schriftlich angeordnet werden.

[2] Das Amt für Informatik:
a) führt die benutzerbezogenen Auswertungen durch;
b) sichert die entsprechenden Protokolle;
c) informiert den Vorsteher des Departements oder der Staatskanzlei umgehend über das Ergebnis der Auswertungen.

[3] Der Vorsteher des Departements oder der Staatskanzlei informiert den betroffenen Benutzer und den Amtsvorsteher über das Ergebnis der benutzerbezogenen Auswertung.

§ 28 [35] Vorbehaltene Massnahmen

Vorbehalten bleiben dringliche, notwendige und verhältnismässige benutzerbezogene Auswertungen sowie die Weitergabe von Informationen:
a) an zur Schadenminderung beauftragte Dritte;
b) an die Aufsichts- und Justizorgane im Umfang ihrer gesetzlichen Befugnisse.

§ 29 [36] Vernichtung von Aufzeichnungen und Auswertungen

Die Vernichtung von Aufzeichnungen und Auswertungen nach spätestens sechs Monaten unterbleibt, wenn diese unverändert aufbewahrt werden müssen:
a) zu Beweiszwecken;
b) zur Durchführung einer behördlichen oder gerichtlichen Untersuchung;
c) zum Schutz der öffentlichen Sicherheit.

VII. Auslagerung

§ 30 [37] Zulässigkeit

[1] Die Auslagerung von Informatikmitteln oder digitalen Leistungen ist zulässig, sofern die gesetzlichen Vorschriften, insbesondere über den Datenschutz und den Finanzhaushalt sowie die Bestimmungen dieser Verordnung eingehalten werden.

[2] Die Auslagerung setzt eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt:
a) Inhalt der Leistungen der Parteien;
b) Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten;
c) Verantwortlichkeiten;
d) verwendete Techniken, einschliesslich Entwicklung und Wartung;
e) Zugriffs- und Zutrittsrechte;
f) Informationssicherheits- und Datenschutzkonzept;
g) Standorte der Hardware und der Informationsbearbeitung;
h) Kontrollrechte und Aufsicht;
i) Beizug von Dritten;
j) Leistungsstörungen und Konventionalstrafe;
k) angemessene Massnahmen;
l) Aufbewahrung und Archivierung;
m) Sicherstellung des Eigentums an Informationen und Hilfsprogrammen zur Weiterverwendung bei Auflösung des Vertrages;
n) Rückführung und Löschung der Informationen im Fall der Vertragsauflösung.

[3] Die auslagernde Verwaltungseinheit stellt durch organisatorische, technische und vertragliche Vorkehrungen sicher, dass die kantonale Aufgabenerfüllung auch dann ohne wesentliche Beeinträchtigung gewährleistet ist, wenn der Auftragnehmer Abmachungen nicht einhält oder die Geschäftstätigkeit einstellt.

§ 31 [38] Genehmigungspflicht

[1] Die Auslagerung von Informatikmitteln oder digitalen Leistungen von übergeordneter Bedeutung bedarf der Genehmigung des Regierungsrates. Dazu gehören insbesondere Auslagerungen:
a) von Basisdiensten;
b) an Organe des Bundes;
c) an Organe anderer Kantone.
[2] Die übrigen Auslagerungsvorhaben sind vom Amt für Informatik zu genehmigen.
[3] Die Auslagerung kann verweigert werden, wenn sie die Anforderungen nach § 30 nicht erfüllt.
[4] Bestehende Auslagerungen sind im Falle einer Vertragsanpassung oder mindestens alle vier Jahre auf ihre Zulässigkeit zu überprüfen.

VIII. Schlussbestimmungen

§ 32 Vollzug

Der Regierungsrat regelt das Verfahren und die Herausgabe von Daten nach den §§ 27 und 28.

§ 33 Inkrafttreten

[1] Diese Verordnung tritt am 1. Oktober 2015 in Kraft.[39]
[2] Sie wird im Amtsblatt veröffentlicht und in die Gesetzsammlung aufgenommen.

[1] GS 24-47 mit Änderungen vom 11. Februar 2025 (GS 27-60).
[2] Erlasstitel in der Fassung vom 11. Februar 2025.
[3] SRSZ 143.110.
[4] SRSZ 140.410.
[5] Fassung vom 11. Februar 2025.
[6] Abs. 1 Bst. b und c sowie Abs. 2 in der Fassung vom 11. Februar 2025.
[7] Abs. 1 Bst. b in der Fassung vom und Abs. 2 neu eingefügt am 11. Februar 2025.
[8] Abs. 1 Bst. a bis h in der Fassung vom und Bst. i bis k neu eingefügt am 11. Februar 2025.
[9] Abs. 1 in der Fassung vom 11. Februar 2025.
[10] Abs. 1 bis 3 in der Fassung vom 11. Februar 2025.
[11] Aufgehoben am 11. Februar 2025.
[12] Abs. 1 in der Fassung vom und Abs. 2 neu eingefügt am 11. Februar 2025.
[13] Abs. 1 Bst. a bis d in der Fassung vom und Bst. e aufgehoben am 11. Februar 2025.
[14] Überschrift, Abs. 1 Bst. a bis d, Abs. 2 in der Fassung vom, Abs. 1 Bst. e aufgehoben am und Abs. 3 neu eingefügt am 11. Februar 2025.
[15] Abs. 1 Bst. a bis e in der Fassung vom und Bst. f neu eingefügt am 11. Februar 2025, bisheriger Bst. e wird zu Bst. f.

[16] Aufgehoben am 11. Februar 2025.
[17] Abs. 1 Bst. a bis c sowie e bis j und Abs.2 in der Fassung vom, Abs. 3 aufgehoben am 11. Februar 2025, bisheriger Abs. 3 wird zu Abs. 2.
[18] Aufgehoben am 11. Februar 2025.
[19] Überschrift, Abs. 1 und 2 Bst. a und c in der Fassung vom 11. Februar 2025.
[20] Haupttitel in der Fassung vom 11. Februar 2025.
[21] Überschrift, Abs. 1 und 2 in der Fassung vom, Abs. 3 neu eingefügt am 11. Februar 2025.
[22] Neu eingefügt am 11. Februar 2025.
[23] Abs. 1 und 2 Bst. a bis c in der Fassung vom, Abs. 3 und 4 neu eingefügt am 11. Februar 2025.
[24] Neu eingefügt am 11. Februar 2025.
[25] Haupttitel in der Fassung vom 11. Februar 2025.
[26] Abs. 1 in der Fassung vom 11. Februar 2025.
[27] Abs. 1 und 3 in der Fassung vom, Abs. 4 neu eingefügt am 11. Februar 2025.
[28] Abs. 1 und 3 in der Fassung vom 11. Februar 2025.
[29] Überschrift, Abs. 1 bis 3 in der Fassung vom 11. Februar 2025.
[30] Abs. 1 und 2 Bst. a bis c sowie e bis g in der Fassung vom 11. Februar 2025.
[31] Abs. 1 bis 3 Bst. a und b in der Fassung vom, Abs. 3 Bst. c und d neu eingefügt am 11. Februar 2025.
[32] Abs. 1 Einleitungssatz und Bst. b, Abs. 2 Bst. b in der Fassung vom, Abs. 2 Bst c und Abs. 3 neu eingefügt am 11. Februar 2025.
[33] Abs. 2 in der Fassung vom und Abs. 3 neu eingefügt am 11. Februar 2025.
[34] Überschrift, Abs. 1, Abs. 2 Bst. a und c sowie Abs. 3 in der Fassung vom 11. Februar 2025.
[35] Abs. 1 in der Fassung vom 11. Februar 2025.
[36] Abs. 1 in der Fassung vom 11. Februar 2025.
[37] Abs. 1 und 2 Bst. f, g, m und n in der Fassung vom 11. Februar 2025.
[38] Abs. 1 in der Fassung vom, Abs. 3 und 4 neu eingefügt am 11. Februar 2025.
[39] Änderungen vom 11. Februar 2025 am 1. März 2025 (Abl 2025 443) in Kraft getreten.