Synopse **Beilage 1 zum Anhörungsbericht**

Gesetz über die Informationssicherheit (InfoSiG)

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	Gesetz über die Informationssicherheit (InfoSiG)			
	Der Grosse Rat des Kantons Aargau, gestützt auf die §§ 27 Abs. 1, 86 Abs. 1, 94 Abs. 1 und 97 Abs. 1 der Kantonsverfassung, *beschliesst:*			
	I.			
	1. Allgemeine Bestimmungen			
	§ 1 Zweck [1] Dieses Gesetz bezweckt die Gewährleistung der sicheren Bearbeitung von Informationen sowie des sicheren Einsatzes der Informatikmittel durch die Behörden des Kantons. [2] Damit sollen die folgenden öffentlichen Interessen geschützt werden: a) die innere Sicherheit,			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	b) die Entscheidungs- und Handlungsfähigkeit der Behörden und ihrer Verwaltungseinheiten sowie c) die Erfüllung der gesetzlichen und vertraglichen Verpflichtungen des Kantons zum Schutz von Informationen.			
	§ 2 Geltungsbereich [1] Dieses Gesetz gilt für den Grossen Rat, den Regierungsrat und die Gerichte (Behörden) sowie deren Verwaltungseinheiten. [2] Für die Gemeinden und andere Träger öffentlicher Aufgaben gelten die Bestimmungen über a) die klassifizierten Informationen des Kantons, soweit sie klassifizierte Informationen des Kantons bearbeiten sowie b) die Sicherheit beim Einsatz von Informatikmitteln, soweit auf Informatikmittel des Kantons zugegriffen wird.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[3] Absatz 2 findet keine Anwendung, wenn die Gemeinden und andere Träger öffentlicher Aufgaben eine mindestens gleichwertige Informationssicherheit gewährleisten.			
	§ 3 Sicherheitsrelevanz [1] Als sicherheitsrelevant im Sinne dieses Gesetzes gelten a) die Bearbeitung von als "vertraulich" oder "geheim" klassifizierten Informationen, b) jeglicher Umgang mit Informatikmitteln der Sicherheitsstufen "hoher Schutz" oder "sehr hoher Schutz" sowie c) der Zugang zu Sicherheitszonen.			
	§ 4 Verhältnis zu anderen Gesetzen [1] Für Informationen, deren Schutz auch in anderen Gesetzen geregelt ist, finden die Bestimmungen dieses Gesetzes ergänzend Anwendung.			
	2. Führung und allgemeine Massnahmen			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	2.1. Führung			
	§ 5 Führungsverantwortung [1] Die Behörden sind für die Informationssicherheit in ihren Zuständigkeitsbereichen verantwortlich. [2] Sie sorgen dafür, dass a) der Schutzbedarf der Informationen in den Aufgabenbereichen beurteilt wird, b) die Informationen ihrem Schutzbedarf entsprechend 1. nur Berechtigten zugänglich sind (Vertraulichkeit), 2. verfügbar sind, wenn sie benötigt werden (Verfügbarkeit), 3. nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität), 4. nachvollziehbar bearbeitet werden (Nachvollziehbarkeit),			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	c) die Informatikmittel, die sie zur Erfüllung ihrer gesetzlichen Aufgaben einsetzen, vor Missbrauch und Störung geschützt werden.			
	2.2 Allgemeine Massnahmen			
	2.2.1. Informationssicherheits-Risikomanagement			
	§ 6 Implementierung [1] Die Behörden stellen in ihren Zuständigkeitsbereichen ein wirkungsvolles Risikomanagement sicher, indem a) sie die Risiken für die Informationssicherheit laufend beurteilen, b) die erforderlichen Massnahmen treffen, um die Risiken zu vermeiden oder auf ein tragbares Mass zu reduzieren und c) die Übernahme der Verantwortung für Restrisiken regeln.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[2] Sie haben dabei den Grundsätzen der Zweckmässigkeit, der Wirtschaftlichkeit und der Benutzerfreundlichkeit Rechnung zu tragen.			
	2.2.2. Vorgehen bei Verletzungen der Informationssicherheit und Prävention			
	§ 7 Früherkennung und Vorsorgeplanung [1] Die Behörden stellen sicher, dass Verletzungen der Informationssicherheit schnell erkannt, deren Ursachen behoben und die Auswirkungen minimiert werden. [2] Um allfälligen schwerwiegenden Verletzungen der Informationssicherheit, welche die Aufgabenerfüllung gefährden könnten, begegnen zu können, sind Notfall- und Vorsorgeplanungen zu erstellen und regelmässig zu aktualisieren. [3] Die Widerstandsfähigkeit der Prozesse und Massnahmen ist kontinuierlich zu überprüfen und bei Vorliegen sicherheitsrelevanter Defizite sind unverzüglich entsprechende Massnahmen zu ergreifen.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[4] Das Vorgehen bei Verletzungen der Informationssicherheit und das Ergreifen präventiver und prädiktiver Massnahmen zu deren Minimierung sind kontinuierlich zu üben beziehungsweise zu evaluieren.			
	2.2.3. Klassifizierung			
	§ 8 Grundzüge der Klassifizierung [1] Informationen, deren Kenntnisnahme durch Unberechtigte zu einer Beeinträchtigung der öffentlichen Interessen gemäss § 1 Abs. 2 lit. a und b führen kann, sind zu klassifizieren. [2] Es sind folgende Klassifizierungsstufen vorgesehen: a) "intern", wenn die öffentlichen Interessen gemäss § 1 Abs. 2 lit. a und b beeinträchtigt werden können, b) "vertraulich", wenn die öffentlichen Interessen gemäss § 1 Abs. 2 lit. a und b erheblich beeinträchtigt werden können,			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	c) "geheim", wenn die öffentlichen Interessen gemäss § 1 Abs. 2 lit. a und b schwerwiegend beeinträchtigt werden können. 3 Die Klassifizierung ist auf die tiefste erforderliche Stufe und nach Möglichkeit zeitlich zu beschränken.			
	§ 9 Zuständigkeiten 1 Die Stelle, die schutzwürdige Informationen festhält oder herausgibt, weist sie einer Klassifizierungsstufe zu. 2 Klassifizierungen dürfen nur von der klassifizierenden oder der ihr übergeordneten Stelle geändert oder aufgehoben werden.			
	§ 10 Zugang zu klassifizierten Informationen			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[1] Zugang zu klassifizierten Informationen erhalten nur Personen, die Gewähr dafür bieten, dass sie die öffentlichen Interessen gemäss § 1 Abs. 2 lit. a und b nicht beeinträchtigen und die Informationen zur gesetzlichen oder vertraglichen Aufgabenerfüllung benötigen. [2] Spezialgesetzliche Verfahrensbestimmungen bleiben vorbehalten. [3] Der Zugang zu klassifiziertem Archivgut richtet sich nach den Bestimmungen der Archivierungsgesetzgebung. [4] Der Regierungsrat regelt durch Verordnung die Entklassifizierung von Archivgut.			
	2.2.4. Vertragliche Überbindung und Kontrolle			
	§ 11 Zusammenarbeit mit Dritten			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[1] Werden Dritte durch Vergabe eines öffentlichen Auftrags oder Auslagerung einer öffentlichen Aufgabe zu einer sicherheitsrelevanten Auftrags- beziehungsweise Aufgabenerfüllung beigezogen, sind ihnen die Anforderungen und Massnahmen nach diesem Gesetz vertraglich zu überbinden und deren Umsetzung angemessen zu überprüfen.			
	3. Technische und organisatorische Massnahmen (TOM)			
	3.1. Sicherheit beim Einsatz von Informatikmitteln			
	§ 12 Sicherheitsverfahren [1] Die Behörden legen ein Verfahren zur Gewährleistung der Informationssicherheit beim Einsatz von Informatikmitteln fest. [2] Das Sicherheitsverfahren umfasst insbesondere			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	a) die Beurteilung des Schutzbedarfs der Informationen vor dem Einsatz beziehungsweise vor der Beschaffung von Informatikmitteln, b) die Bestimmung der sich aus dem Schutzbedarf ergebenden Sicherheitsstufe und der angemessenen Sicherheitsmassnahmen, c) die Umsetzung der Sicherheitsmassnahmen und deren Überprüfung, d) die Zuständigkeit für die Sicherheitsfreigabe von Informatikmitteln und für die Akzeptanz der Restrisiken, e) das Vorgehen bei Veränderung der Risiken. [3] Für die Informatikmittel gelten die Sicherheitsstufen			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	a) "sehr hoher Schutz", wenn eine Verletzung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Informationen, die damit bearbeitet werden, oder ein Missbrauch oder eine Störung des Informatikmittels die öffentlichen Interessen gemäss § 1 Abs. 2 schwerwiegend beeinträchtigen können, b) "hoher Schutz", wenn eine Verletzung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Informationen, die damit bearbeitet werden, oder ein Missbrauch oder eine Störung des Informatikmittels die öffentlichen Interessen gemäss § 1 Abs. 2 erheblich beeinträchtigen können, c) "Grundschutz" in allen anderen Fällen. [4] Für die Durchführung des Sicherheitsverfahrens ist diejenige Behörde zuständig, welche die Informatikmittel beschafft.			
	3.2. Physische Massnahmen			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	§ 13 Grundsatz [1] Die Behörden sorgen in ihrem Zuständigkeitsbereich für einen angemessenen physischen Schutz der Informationen und Informatikmittel.			
	§ 14 Sicherheitszonen [1] Die Behörden erklären Räumlichkeiten oder Bereiche als Sicherheitszonen, in denen a) Informationen der Klassifizierung "geheim" regelmässig bearbeitet oder b) Informatikmittel der Sicherheitsstufe "sehr hoher Schutz" betrieben werden. [2] Sie sind insbesondere befugt, a) das Mitführen bestimmter Gegenstände, insbesondere von Aufnahmegeräten, zu verbieten, b) sicherheitsempfindliche Bereiche mit Aufnahmegeräten überwachen zu lassen,			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	c) Taschen- und Personenkontrollen durchführen zu lassen, d) unangemeldet Raumkontrollen, auch in Abwesenheit der Angestellten, durchzuführen zu lassen.			
	3.3. Identitäts- und Zugriffsmanagement			
	§ 15 Identitätsverwaltungssysteme [1] Die Behörden können zwecks zentraler Verwaltung der Daten zur Identifizierung von Personen, die Zugang zu sicherheitsrelevanten Informationen und Informatikmitteln sowie zu Sicherheitszonen haben, Identitätsverwaltungssysteme betreiben. [2] Die Identitätsverwaltungssysteme übermitteln das Resultat der Prüfung an die angeschlossenen Informationssysteme, damit diese die Berechtigungen der identifizierten Personen ermitteln können. [3] Für jedes Identitätsverwaltungssystem ist eine verantwortliche Stelle zu bezeichnen.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	§ 16 Datenaustausch und -abgleich [1] Die Identitätsverwaltungssysteme können mit angeschlossenen Informationssystemen, mit Personal- und Benutzerverzeichnissen und mit anderen Identitätsverwaltungssystemen Daten austauschen und abgleichen. [2] Austausch und Abgleich sind auf Daten zu begrenzen, die im jeweiligen System bearbeitet werden dürfen.			
	3.4. Personelle Massnahmen			
	3.4.1. Auswahl, Instruktion und Berechtigungen			
	§ 17 Voraussetzungen für den Zugang zu Informationen und Informatikmitteln [1] Die Behörden sorgen dafür, dass Personen, die Zugang zu sicherheitsrelevanten Informationen und Informatikmitteln sowie zu Sicherheitszonen haben a) sorgfältig ausgewählt,			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	b) risikogerecht identifiziert, c) funktionsgerecht aus- und weitergebildet sowie d) zur Geheimhaltung und besonderer Sorgfalt verpflichtet werden. [2] Sie können biometrische Verifikationsmethoden verwenden, wenn dies zur risikogerechten Identifizierung von Personen erforderlich ist. Die biometrischen Daten sind nach dem Wegfall der Zugangsberechtigung zu vernichten. [3] Sie können zudem die Versichertennummer gemäss Art. 50c des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) vom 20. Dezember 1946 [1)] systematisch als Personenidentifikator verwenden. [4] Den Personen gemäss Absatz 1 dürfen nur sicherheitsrelevante Informationen und Informatikmittel zur Verfügung stehen sowie Zugang zu Sicherheitszonen nur gewährt werden, wenn es für die Aufgabenerfüllung notwendig ist.			

[1)] SR|831.10

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[5] Die Anstellungsbehörde, die auftraggebende beziehungsweise die auslagernde Stelle entziehen die Berechtigungen, sobald die Anstellung oder der erteilte Auftrag endet oder die Aufgabe erfüllt ist. Sie dürfen gesperrt oder entzogen werden, wenn konkrete Anhaltspunkte für eine Gefährdung der Sicherheit vorliegen.			
	3.4.2. Personensicherheitsprüfung (PSP)			
	§ 18 Gegenstand und Voraussetzungen [1] Die Personensicherheitsprüfung (PSP) dient zur Beurteilung, ob ein Risiko für die Informationssicherheit bestehen könnte, wenn eine Person im Rahmen ihrer Funktion, ihres Auftrags oder infolge Auslagerung einer öffentlichen Aufgabe Zugang zu sicherheitsrelevanten Informationen oder Informatikmittel sowie zu Sicherheitszonen hat.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[2] Sie ist auf Antrag einer Anstellungsbehörde, eines Departements, eines wahlvorbereitenden Gremiums oder einer Vergabestelle durchzuführen, wenn die mit einer Tätigkeit verbundenen Sicherheitsrisiken die PSP rechtfertigen, namentlich wenn die zu prüfende Person a) häufig oder in grossem Umfang Zugang zu sicherheitsrelevanten Informationen oder Informatikmitteln, b) Einblick in wichtige politische oder sicherheitsrelevante Geschäfte oder c) regelmässig oder unbegleitet Zugang zu Sicherheitszonen gemäss § 14 hat. [3] Im Rahmen der PSP werden Daten über die Lebensführung der zu prüfenden Person erhoben, insbesondere über ihre engen persönlichen Beziehungen und familiären Verhältnisse, über ihre Straffälligkeit und finanzielle Lage.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[4] Eine PSP darf nur mit Einwilligung der zu prüfenden Person durchgeführt werden. Sie ist verpflichtet, an der PSP mitzuwirken. [5] Auf die Durchführung einer PSP kann verzichtet werden, wenn für die betreffende Person bereits eine PSP in den letzten zwei Jahren durchgeführt worden ist.			
	§ 19 Personenkreis [1] Eine PSP kommt in Betracht bei: a) Angestellten sowie Beamtinnen und Beamten vor Abschluss des Anstellungsverhältnisses bzw. vor der Wahl oder während der Dauer des Anstellungs- bzw. des Beamtenverhältnisses, b) Personen, die in ein Amt oder als Mitglied eines kantonalen Gremiums gewählt werden sollen, c) Privaten vor Beginn oder im Rahmen der ihnen übertragenen Aufgaben oder des ihnen vergebenen öffentlichen Auftrags.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[2] Von Absatz 1 lit. b sind folgende Funktionen ausgenommen: a) Mitglieder des Grossen Rats, b) Mitglieder des Regierungsrats, c) Richterinnen und Richter. [3] Die Behörden erlassen für ihren Zuständigkeitsbereich eine Liste der Funktionen, die eine PSP erfordern. Die Liste ist periodisch zu aktualisieren. [4] Für Personen, die klassifizierte Informationen des Bundes bearbeiten oder auf Informatikmittel des Bundes zugreifen, bleiben die Bestimmungen der Bundesgesetzgebung über die Informationssicherheit vorbehalten.			
	§ 20 Zentrale Fachstelle für PSP [1] Die Kantonspolizei führt als zentrale Fachstelle PSP durch.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[2] Die Fachstelle kann zur Durchführung der PSP ein Informationssystem betreiben, in dem besonders schützenswerte Personendaten und das Profiling von Personen bearbeitet werden können, wenn dies zur Beurteilung des Sicherheitsrisikos erforderlich ist.			
	§ 21 Datenerhebung [1] Die Fachstelle kann die für die PSP notwendigen und in einem engen Zusammenhang zur Aufgabenerfüllung stehenden Daten aus folgenden Quellen erheben: a) aus dem Strafregister, b) durch Einholen von Auskünften und Akten über hängige und abgeschlossene Strafverfahren bei den Strafbehörden,			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	c) aus den Datenbearbeitungs- und Informationssystemen der Kantonspolizei gemäss den §§ 50 Abs. 1 und 51a des Gesetzes über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG) vom 6.12.2005 [1)], d) aus den polizeilichen Datenbearbeitungs- und Informationssystemen des Bundes und anderer Kantone, soweit die Kantonspolizei zugriffsberechtigt ist, e) bei den Steuerbehörden, f) aus den Registern der Betreibungs- und Konkursbehörden, g) durch Einholen von Referenzen bei früheren Arbeitgebenden der zu prüfenden Person, wenn es um eine Anstellung oder eine Wahl gemäss § 19 Abs. 1 lit. a geht, h) durch Befragung der zu prüfenden Person,			

[1)] SAR 531.200

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	i) durch Befragung von Drittpersonen, wenn die zu prüfende Person zustimmt. 2 Daten über Dritte, die untrennbar mit Daten über die zu prüfende Person verbunden sind, dürfen nur bearbeitet werden, wenn dies für die Beurteilung des Sicherheitsrisikos unerlässlich ist. Die Fachstelle informiert die betroffenen Dritten über die Bearbeitung. 3 Die Fachstelle bewahrt die erhobenen Daten bis 10 Jahre nach Abschluss der sicherheitsrelevanten Tätigkeit auf und bietet sie danach dem Staatsarchiv an. 4 Wird das Prüfverfahren eingestellt, tritt eine geprüfte Person die vorgesehene Stelle nicht an oder lehnt sie den Auftrag ab, sind alle erhobenen Daten und Akten spätestens nach drei Monaten zu vernichten.			
	§ 22 Ergebnis der PSP			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[1] Die Fachstelle hält das begründete Ergebnis der Datenerhebung und Beurteilung der PSP mit einer der folgenden Erklärungen fest: a) Es besteht kein Sicherheitsrisiko, b) es besteht ein Sicherheitsrisiko, das mit Auflagen auf ein tragbares Mass reduziert werden kann, c) es besteht ein Sicherheitsrisiko. [2] Ein Sicherheitsrisiko besteht, wenn aus der Auswertung und Beurteilung der erhobenen Daten konkrete Anhaltspunkte vorliegen, dass die geprüfte Person die sicherheitsrelevante Tätigkeit mit hoher Wahrscheinlichkeit vorschriftswidrig oder unsachgemäss ausüben wird. [3] Die Wahrscheinlichkeit einer vorschriftswidrigen oder unsachgemässen Ausübung der sicherheitsrelevanten Tätigkeit ist als hoch einzustufen, wenn die konkreten Anhaltspunkte auf eine oder mehrere der folgenden persönlichen Eigenschaften hinweisen:			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	a) mangelnde persönliche Integrität oder Vertrauenswürdigkeit, b) Erpressbarkeit oder Bestechlichkeit, c) beeinträchtigtes Urteils- oder Entscheidungsvermögen. [4] Der geprüften Person ist Gelegenheit einzuräumen, zum Ergebnis der PSP Stellung zu nehmen und falsche Daten zu berichtigen.			
	§ 23 Wiederholung [1] Die PSP ist spätestens nach 5 Jahren zu wiederholen. Für Personen in einer Funktion mit Amtsdauer jeweils vor der Wiederwahl. [2] Die PSP kann bei begründetem Anlass jederzeit wiederholt werden.			
	3.5. Sicherheitsspezifische Eignungsprüfung von Unternehmen			
	§ 24 Befähigungsnachweis			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[1] Sicherheitsrelevante Vergaben öffentlicher Aufträge und Übertragungen öffentlicher Aufgaben dürfen nur an Unternehmen erfolgen, die sich im Rahmen der Eignungsprüfung als befähigt erweisen, die öffentlichen Interessen gemäss § 1 Abs. 2 zu wahren. [2] Die Unternehmen sind durch gezielte Abfrage, welche die Eigenheiten der spezifischen Vergabe bzw. der Übertragung der öffentlichen Aufgabe berücksichtigt, aufzufordern Angaben zu liefern, die für die Beurteilung ihrer Eignung in sicherheitstechnischer Hinsicht notwendig sind, insbesondere a) zu den Eigentumsverhältnissen sowie zu geplanten Änderungen wie Fusionen, Beteiligungen, Übernahmen, b) zu Interessenbindungen von Mitgliedern der Unternehmensführung, c) zur Solvenz sowie zu allfälligen hängigen Pfändungs- und Konkursverfahren, d) zur Bezahlung von Steuern und Sozialabgaben sowie			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	e) einen Nachweis der Zertifizierung der Informationssicherheitsprozesse oder zumindest des Vorliegens eines dem Vorhaben angemessenen ISDS-Konzepts [1)].			
	4. Organisation			
	4.1. Verwaltungsinterne Organisation			
	§ 25 Fachstelle für Informationssicherheit [1] Zum Zwecke eines einheitlichen, behördenübergreifenden Vollzugs ist eine Fachstelle für Informationssicherheit als Stabsstelle des Regierungsrats zu schaffen. [2] Sie hat folgende Aufgaben: a) Fachliche Beratung und Unterstützung, b) Aufbau, Betrieb und Weiterentwicklung eines Informationssicherheits-Managementsystems,			

[1)] Informationssicherheits- und Datenschutzkonzept

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	c) Überprüfung der Einhaltung der Vorgaben der Informationssicherheit und Beantragung erforderlicher Massnahmen bei Nichteinhaltung, d) Durchgriff in Zusammenarbeit mit den betroffenen Stellen, wenn durch Nichthandeln eine unmittelbare Gefahr für die Informationssicherheit droht oder mit negativen Auswirkungen auf weite Teile der kantonalen Informatikinfrastruktur zu rechnen ist, e) Ergreifen von Massnahmen bei Cybervorfällen in der Verwaltung, f) Beurteilung der Risiken für die Informationssicherheit beim Einsatz neuartiger Technologien, g) Teilnahme bei wichtigen behördenübergreifenden Projekten und in allen mit der Umsetzung der Informationssicherheit betrauten Gremien, h) jährliche Berichterstattung an den Regierungsrat,			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	i) Erlass von technischen Weisungen und Standards. 3 Administrativ ist die Fachstelle für Informationssicherheit dem Departement Finanzen und Ressourcen beigeordnet.			
	4.2. Verwaltungsübergreifende Organisation			
	§ 26 Kantonale Cyber-Organisation 1 Zur Minimierung der Cyber-Risiken des Kantons ist eine verwaltungsübergreifende Organisation für die Gewährleistung der Cybersicherheit zu schaffen. 2 Die kantonale Cyber-Organisation sieht folgende Gremien und Stellen vor: a) Cyber-Ausschuss, b) Cyber-Koordinationsstelle, c) Kerngruppe Cyber. 3 Der Regierungsrat regelt die organisatorischen Belange durch Verordnung.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	§ 27 Cyber-Ausschuss [1] Der Cyber-Ausschuss besteht aus der Vorsteherin oder dem Vorsteher der Departemente Volkswirtschaft und Inneres sowie Finanzen und Ressourcen und aus der Staatsschreiberin oder dem Staatsschreiber. [2] Er hat insbesondere folgende Aufgaben: a) Aufsicht über die kantonale Cyber-Organisation, b) Wahlvorbereitung und Wahlvorschlag der Cyber-Koordinatorin oder des Cyber-Koordinators zuhanden des Regierungsrats, c) Genehmigung der Ziele und Prüfung der jährlichen Zielerreichung, d) Entscheid über Differenzen in der kantonalen Cyber-Organisation, e) Beurteilung der Bewältigung von Cybervorfällen.			
	§ 28 Cyber-Koordinationsstelle			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[1] Zum Zwecke der Koordination und des Informationsaustausches zwischen den staatlichen und privaten Akteuren sowie zur Stärkung der Widerstandsfähigkeit in Verwaltung, Wirtschaft und Bevölkerung ist eine Cyber-Koordinationsstelle zu schaffen. [2] Sie hat insbesondere folgende Aufgaben: a) Zentrale Anlaufstelle für Fragen zur Informationssicherheit, b) Koordination und Informationsaustausch zwischen staatlichen und interkantonalen Fachstellen sowie Institutionen und der Wirtschaft, c) Koordination der Umsetzung von Massnahmen aus der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), d) Leitung der Kerngruppe Cyber, e) Abgabe von Empfehlungen bei erkanntem Sicherheitsdefizit,			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	f) Koordination von Übungen, namentlich mit dem KFS und den kritischen Infrastrukturen, g) Beratung und Unterstützung von Projekten zur Förderung der Informationssicherheit, h) Erstellen von Ausbildungsunterlagen und Durchführung von Schulungen, i) Sensibilisierung von Verwaltung, Wirtschaft und Bevölkerung, j) Planung und Durchführung von Präventionskampagnen, k) jährliche Berichterstattung an den Regierungsrat.			
	§ 29 Kerngruppe Cyber [1] Zur operativen Unterstützung der Cyber-Koordinationsstelle ist eine Kerngruppe Cyber einzusetzen. [2] Sie hat insbesondere folgende Aufgaben:			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	a) Fachliche Unterstützung der Cyber-Koordinationsstelle aus den Bereichen Informations- und Informatiksicherheit, Datenschutz, Cyberkriminalität und Katastrophenschutz, b) Beurteilung der Bedrohungslage, c) Beaufsichtigung der Bewältigung erheblicher Cybervorfälle innerhalb der Verwaltung, d) Ziehen von Lehren aus der Bewältigung von Cybervorfällen, e) Informationsaustausch zwischen Cyberspezialistinnen und -spezialisten der in Litera a erwähnten Bereiche.			
	5. Vollzug			
	§ 30 Ausführungsbestimmungen [1] Die Behörden erlassen die für den Vollzug dieses Gesetzes erforderlichen Ausführungsbestimmungen durch Dekret, Verordnung bzw. Reglement.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	[2] Soweit der Grosse Rat und die Gerichte keine eigenen Ausführungsbestimmungen erlassen haben, gelten für sie die Verordnungen und Weisungen des Regierungsrats sinngemäss.			
	6. Schlussbestimmungen			
	§ 31 Übergangsbestimmung [1] Die Klassifizierung der im Zeitpunkt dieses Gesetzes vorhandenen Informationen hat spätestens bis 5 Jahre nach Inkrafttreten dieses Gesetzes zu erfolgen.			
	§ 32 Inkrafttreten [1] Der Regierungsrat bestimmt den Zeitpunkt des Inkrafttretens.			
	II.			
	Keine Fremdänderungen.			
	III.			
	Keine Fremdaufhebungen.			
	IV.			

Geltendes Recht	Entwurf des Regierungsrats vom …	Abweichende Anträge der Kommission X vom …	Stellungnahme des Regierungsrats	Ergebnis der 1. Beratung vom …
	Der Regierungsrat bestimmt das Inkrafttreten der Änderungen unter Ziff. I. und II.			
	Aarau, Präsident / Präsidentin des Grossen Rats ... Protokollführer / Protokollführerin ...			