KANTON AARGAU

DEPARTEMENT
FINANZEN UND RESSOURCEN

1. Mai 2024

ANHÖRUNGSBERICHT

Gesetz über die Informationssicherheit (InfoSiG)

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
BBl	Bundesblatt
BCM	Business Continuity Management (betriebliches Kontinuitätsmanagement)
CISO	Chief Information Security Officer (Gesamtverantwortlicher für Informationssicherheit)
GSK	Generalsekretärenkonferenz
IAM	Identity and Access Management (Identitäts- und Zugriffsverwaltung)
IB	Informatikbeauftragte Person
IK	Informatikkonferenz
IKT	Informations- und Kommunikationstechnologie bzw. -technik, d.h. Technik der Erfassung, Übermittlung, Verarbeitung und Speicherung von Informationen durch Computer und Telekommunikationseinrichtungen.
ISBP	Informationssicherheitsbeauftragte Person
ISK	Informationssicherheits-Konferenz
ISMS	Information Security Management System (Managementsystem für Informationssicherheit)
KRITIS	kritische Infrastrukturen
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022
NCSC	National Cyber Security Centre (Nationales Zentrum für Cybersicherheit)
NSP-AG	Network Security Policy Kanton Aargau vom 20. Februar 2017
ÖDB	Beauftragte für Öffentlichkeit und Datenschutz (des Kantons Aargau)
OGD	Offene Behördendaten ("open government data") sind Verwaltungs-Daten, die weder durch Datenschutz, Sicherheits- noch infolge von Urheberrechtsgründen geschützt sind.
PSP	Personensicherheitsprüfung
RLRS	Richtlinien Rechtssetzung (RLRS) des Regierungsrats des Kantons Aargau vom 15. August 2001 in der Fassung gemäss Revision vom 6. Juni 2018 (RRB Nr. 2018-000668)
SAR	Systematische Sammlung des Aargauischen Rechts
SIK	Schweizerischen Informatikkonferenz
SR	Systematische Rechtssammlung des Bundes
SVS	Sicherheitsverbund Schweiz
TOM	Technische und organisatorische Massnahmen

Zusammenfassung

Der rasante Wandel hin zu einer Informationsgesellschaft und die Digitalisierung bergen ungeahnte Chancen, jedoch auch erhebliche Risiken. Die zunehmende Abhängigkeit von Informations- und Kommunikationstechnologie (IKT) macht auch den Kanton Aargau verwundbarer gegenüber Ausfällen, Störungen und Missbräuchen dieser Technologien, namentlich nehmen die Angriffe auf Verwaltungssysteme stark zu. Die Gewährleistung der Informationssicherheit gehört zum Risikomanagement eines jeden Gemeinwesens und eines jeden Unternehmens. Sie umfasst die Gesamtheit aller Anforderungen und Massnahmen, mit denen die Vertraulichkeit, die Verfügbarkeit, die Integrität und die Nachvollziehbarkeit von Informationen gewährleistet werden kann.

Die Aufgaben der Informationssicherheit werden bereits heute im Rahmen der zur Verfügung stehenden Ressourcen wahrgenommen. Die entsprechenden Vorgaben finden sich jedoch weitgehend in verwaltungsinternen Dokumenten. Es handelt sich dabei vorwiegend um Regelungen, die sich an anerkannten Normen und Best Practices orientieren, aber heute noch nicht auf gesetzlichen Grundlagen beruhen. Weil zur Sicherstellung der Informationssicherheit oft Einschränkungen verfassungsmässiger Rechte und die Bearbeitung von besonders schützenswerten Personendaten notwendig sind, sind für die Informationssicherheit einheitliche gesetzliche Grundlagen zu schaffen. Zudem sind gemäss § 78 Abs. 1 KV "alle wichtigen Bestimmungen" vom Grossen Rat in der Form des Gesetzes zu erlassen. Aus diesem demokratischen Aspekt ergibt sich, dass die Stimmberechtigten mittelbar oder unmittelbar an den für sie besonders wichtigen Regelungen mitwirken können sollen. Aufgrund der Bedeutung, die der Informationssicherheit in der Zwischenzeit und angesichts der fortschreitenden digitalen Entwicklung in der Gesellschaft zukommt, sowie der damit verbundenen Risiken für die öffentliche Sicherheit, ist es zentral, dass die die Informationssicherheit als öffentliche Aufgabe und deren Grundsätze gesetzlich normiert werden. Im Wesentlichen gilt es, technologieneutral die Grundzüge betreffend die Informationssicherheit gesetzlich zu normieren und den Herausforderungen in diesem Bereich gesamtheitlich für die ganze Kantonale Verwaltung zu begegnen. Dies entspricht dem integralen Ansatz der internationalen Standards zur Informationssicherheit.

Mit dem vorgeschlagenen Gesetzesentwurf sollen die Sicherstellung der Informationssicherheit gesetzlich normiert und gleichzeitig Verbesserungen an der aktuellen Situation erzielt werden. Dies stellt einen wesentlichen Beitrag zur nachhaltigen Umsetzung der fortschreitenden Digitalisierung des Kantons dar, die sich der Kanton sowohl mit dem Entwicklungsleitbild 2021–2030 als auch mit der Strategie SmartAargau zum Ziel gesetzt hat. Zudem kann damit der Betrieb des für die Bevölkerung wichtigen Smart Service Portals sichergestellt werden. Das Gesetz soll auf die Risiken, Bedürfnisse und Möglichkeiten des Kantons Aargau ausgerichtet werden. Es ist mit seinen 32 Paragrafen deutlich schlanker als das am 1. Januar 2024 in Kraft getretene Bundesgesetz, welches über 100 Bestimmungen umfasst. Der Geltungsbereich des Gesetzes muss alle Personen und Organisationen erfassen, die vom Kanton mit der Bearbeitung seiner Informationen oder mit dem Zugriff auf seine Informatiksysteme und -netze betraut sind. Für die Gemeinden und andere Träger öffentlicher Aufgaben soll das Gesetz nur insoweit Geltung haben, als sie klassifizierte Informationen des Kantons bearbeiten oder deren Informatikmittel nutzen. Damit wird ein Mindestsicherheitsstandard für Gemeinden und andere öffentlich-rechtliche Institutionen gesetzlich vorgegeben. Dies ist mit Blick auf eine flächendeckende Informationssicherheit der kantonalen Gemeinwesen angezeigt.

Zusammengefasst werden im Gesetzesentwurf folgende Themen behandelt:

- Schutz öffentlicher Interessen
- Geltungsbereich, insbesondere für Gemeinden und andere Träger öffentlicher Aufgaben
- Begriffsdefinition 'Sicherheitsrelevanz'
- Verhältnis zu anderen Gesetzen
- Führungsverantwortung

- Beurteilung des Schutzbedarfs und Schutzziele sowie Schutz der Informatikmittel
- Implementierung eines Informationssicherheits-Risikomanagements
- Früherkennung und Vorsorgeplanung
- Klassifizierung von Informationen
- Vertragliche Überbindung und Kontrolle bei Zusammenarbeit mit Dritten
- Umgang mit Restrisiken
- Technische und organisatorische Massnahmen (TOM)
- Organisation der behördenübergreifenden Informationssicherheit des Kantons
- Kantonale Cyber-Organisation

Der Hauptinhalt des Gesetzes findet sich in den Kapiteln 2 und 3. Hier werden die oberste Führungsverantwortung, die allgemeinen Massnahmen und die technischen und organisatorischen Massnahmen (TOM) in Anlehnung an die branchenüblichen internationalen Standards gemäss ISO 27001 und NIST geregelt.

Im Zusammenhang mit der Schaffung von gesetzlichen Grundlagen für die Informationssicherheit sollen auch die verwaltungsinternen Organisationsstrukturen im Hinblick auf die aktuellen Herausforderungen angepasst werden. Die künftige Organisation soll den Anforderungen an eine zeitgemässe und möglichst sichere Informationssicherheit genügen können. Sie ist folglich anzupassen und zu stärken.

Dabei sollen die Aufgaben und Kompetenzen des Chief Information Security Officer (CISO) in eine Fachstelle für Informationssicherheit mit departements- und behördenübergreifenden Kompetenzen überführt werden (Kap. 7.5.1.1). Die Gefährdung der öffentlichen Interessen, die durch eine Verletzung der Informationssicherheit einher gehen kann, rechtfertigt es, dass diese Fachstelle gesetzlich bestimmte Kompetenzen erhält wie beispielsweise die autonome Durchführung von Überprüfungen aber auch die Möglichkeit des Ergreifens von Massnahmen, wenn Verletzungen der Informationssicherheitsvorgaben (Gesetz, Verordnung, Weisungen, Standards) festgestellt werden sollten. Sie soll folglich mit entsprechenden internen Weisungs-, Antrags- und Durchsetzungsbefugnissen ausgestattet werden. Die Ausstattung mit diesen weitreichenden Kompetenzen bringt es mit sich, dass die Fachstelle in Bezug auf die Informatik funktional unabhängig tätig sein muss. Aufgrund der durch die Verbundenheit und Nähe zur zentralen Informatik entstehenden Synergien ist aber eine organisatorische Verortung in der Abteilung Informatik Aargau (Departement Finanzen und Ressourcen) jedoch zwingend. Die Aufgaben lassen sich einfacher erfüllen, wenn sich die entsprechenden Befugnisse infolge der funktionalen Unabhängigkeit sowie der Direktunterstellung beim Regierungsrat legitimieren lassen. Die Fachstelle für Informationssicherheit soll deshalb als Stabsstelle direkt dem Regierungsrat unterstellt sein und diesem auch Bericht erstatten.

Zudem soll das politische Anliegen nach Aufbau und Einrichtung einer kantonalen Organisation für Cybersicherheit (GR.22.29 Postulat der FDP-Fraktion vom 18. Januar 2022 betreffend Cyberkriminalität) aufgenommen und umgesetzt werden. Es geht dabei um eine Organisation, die über die Verwaltungsgrenzen hinaus die Gemeinden, die Wirtschaft und die Gesellschaft einbezieht. Der Kanton übernimmt dabei aber nicht in erster Linie den Schutz der Informationen der erwähnten Institutionen und Behörden, er kann vielmehr mit einer kantonalen Cyber-Organisation dazu beitragen, dass mit Vernetzung, Informationsaustausch und Sensibilisierung auch ausserhalb der Verwaltungsgrenzen der Fokus vermehrt auf Risikominimierung, Prävention und Früherkennung gelegt wird. Die mit dem Gesetzesentwurf vorgeschlagene kantonale Cyber-Organisation (vgl. Kap. 7.5.2) richtet sich im Wesentlichen nach den Empfehlungen für die Umsetzung zur kantonalen Cyber-Organisation vom 12. Januar 2021 des Sicherheitsverbunds Schweiz (SVS).

Ein entsprechender Entwicklungsschwerpunkt zur Schaffung einer gesetzlichen Grundlage für die Informationssicherheit des Kantons wurde bereits im Aufgaben- und Finanzplan (AFP 2023–2026) aufgenommen (400E003) und vom Grossen Rat verabschiedet. Die gesetzlichen Grundlagen für die Informationssicherheit sollen am 1. Juli 2026 in Kraft treten.

Mit dem Inkrafttreten des InfoSiG ergeben sich unmittelbare Auswirkungen in personeller und finanzieller Hinsicht. Es handelt sich um die Konsequenzen aus der Schaffung der Cyber-Koordinationsstelle und um den Aufwand für die zentrale Fachstelle für Personensicherheitsprüfungen bei der Kantonspolizei. Da die entsprechende Aufgabenerfüllung mit den derzeitigen Ressourcen nicht zu bewältigen ist, bedarf es zweier Vollzeitstellen. Die Stellen werden unter Berücksichtigung des Anhörungsergebnisses im Rahmen des Aufgaben- und Finanzplans (AFP) 2026–2029 eingestellt werden.

Aufgrund der Herausforderungen infolge der ständigen Bedrohung der Informationssicherheit hat der Regierungsrat Sofortmassnahmen beschlossen, neue Zielvorgaben bezüglich zu erreichender Sicherheitsstandards gemacht und die Organisationsstrukturen der kantonalen Verwaltung angepasst. Die finanziellen und personellen Auswirkungen hängen dabei weitgehend vom Sicherheitsniveau ab, das erreicht werden soll. Das anvisierte Zielniveau sowie die dazu notwendigen Massnahmen für die gesamte kantonale Verwaltung und die Gerichte Kanton Aargau hat der Regierungsrat in einem neuen Entwicklungsschwerpunkt "Informationssicherheit" im Aufgaben- und Finanzplan (AFP) 2025–2028 (Aufgabenbereich 435 'Informatik') aufgenommen. Zur Gewährleistung des definierten Sicherheitsniveaus sind Investitionen in personelle und finanzielle Ressourcen notwendig. Nebst der angemessenen Verstärkung der Fachstelle für Informationssicherheit (heute lediglich 2,6 Stellen bei der Informatik Aargau) bedarf es zusätzlicher Ressourcen für die mit ihr eng verbundenen Stellen innerhalb von Informatik Aargau, welche mit der Wahrnehmung von informationssicherheitsspezifischen Aufgaben (Cybersecurity-Engineering, sicherheitsrelevante Stellen im Rahmen von Entwicklung, Bereitstellung und Betrieb von Applikationen, Plattformen und Infrastrukturen) betraut sind und für die Rolle der Informationssicherheitsbeauftragten Personen (ISBP) in den Departementen, der Staatskanzlei und den Gerichten Kanton Aargau. Die benötigten personellen und finanziellen Ressourcen werden im AFP 2025–2028 eingestellt. Für jene Massnahmen, die einen Verpflichtungskredit in der Kompetenz des Grossen Rats erfordern, wird dem Grossen Rat parallel zum Anhörungsstart eine entsprechende Botschaft unterbreitet.

---

1. Begriffe

Im Bereich der Informationssicherheit werden verschiedene Fachbegriffe verwendet. Basierend auf den Definitionen im Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020 (BBl 2020 9975 ff.) sowie in den Ausführungserlassen werden in Beilage 4 die wesentlichsten Fachbegriffe zum besseren Verständnis zusammengefasst und deren Bedeutung erläutert.

2. Ausgangslage

2.1 Entwicklung zu einer Informationsgesellschaft

2.1.1 Überblick

Die fortwährenden Entwicklungen im Bereich der Informatik beschleunigen einen gesellschaftlichen Wandel, welcher durch einen permanenten und ortsunabhängigen Zugriff auf Informationen geprägt ist. Als Begleiterscheinung der Globalisierung führt diese Entwicklung zu einer vernetzteren, mobileren und letztlich transparenteren Gesellschaft als je zuvor. Sämtliche Bereiche der Gesellschaft sind von diesem Wandel betroffen. Der Wandel hin zu einer Informationsgesellschaft fand und findet in

der Schweiz und im Kanton Aargau auf verschiedenen Ebenen und in diversen Projekten statt. Nachfolgend werden die für den Kanton wesentlichsten Entwicklungen dargestellt.

2.1.2 E-Government-Strategien Schweiz und Aargau

E-Government bezeichnet die Umsetzung von Prozessen, die Kommunikation und den Austausch von Informationen zwischen staatlichen Behörden und den Einzelpersonen durch den Einsatz von digitalen Informations- und Kommunikationstechniken. Seit dem Jahr 2007 besteht eine E-Government-Strategie Schweiz, welche unter der Federführung des Bundes in enger Zusammenarbeit mit den Kantonen und Gemeinden entwickelt wurde. Sie bildet die Basis für Bund, Kantone und Gemeinden, ihre Bestrebungen auf gemeinsame Ziele auszurichten, und legt Grundsätze, Vorgehen sowie Instrumente zu deren Umsetzung fest. Sie verfolgt drei strategische Ziele:

a) Die Wirtschaft wickelt den Verkehr mit den Behörden elektronisch ab.

b) Die Behörden haben ihre Geschäftsprozesse modernisiert und verkehren untereinander elektronisch.

c) Die Bevölkerung kann die wichtigen – häufigen oder mit grossem Aufwand verbundenen – Geschäfte mit den Behörden elektronisch abwickeln.

Die E-Government-Strategie "E-Government Schweiz 2020–2023" verabschiedete der Bundesrat am 20. November 2019 und in der Folge auch die Konferenz der Kantonsregierungen, der Schweizerische Städteverband und der Schweizerische Gemeindeverband. Die E-Government-Strategie Schweiz 2020–2023 konkretisiert verschiedene Aktionsfelder zur digitalen Verwaltung der Strategie "Digitale Schweiz" des Bundesrats. Sie wird per 1. Januar 2024 durch die Strategie «Digitale Verwaltung Schweiz 2024-2027» abgelöst, welche die gleichen Ziele verfolgt. Sie unterstützt unter Anwendung eines föderal-kooperativen Ansatzes die Strategie «Digitale Schweiz» – dies insbesondere im Wirkungsbereich Behördenleistungen - und trägt mit einer leistungsfähigen digitalen Verwaltung zu einer digitalen Schweiz bei.

Der Kanton Aargau hat im Mai 2019 das kantonale Programm Smart Aargau lanciert, um den digitalen Wandel in der kantonalen Verwaltung zu forcieren und aktiv zu gestalten. Im November 2020 gründeten 176 Gemeinden (entspricht 80 % der Gemeinden im Kanton Aargau) die Fit4Digital GmbH, um ihre digitale Zukunft proaktiv zu gestalten – professionell koordiniert und breit abgestützt. Im Zuge dieser Entwicklung wurde der vom Kanton und den Gemeinden gemeinsam getragene E-Government-Bereich neu organisiert und positioniert. Der Kanton Aargau und die Gemeindeammänner-Vereinigung sowie die Gemeindepersonal-Fachverbände schlossen eine neue Rahmenvereinbarung ab. Die bisherige Fachstelle unter dem Namen "E-Government Aargau" wurde durch die Fachstelle "Smart Services Aargau" ersetzt. Die Hauptaufgabe der Fachstelle "Smart Services Aargau" ist es, für Einwohnerinnen und Einwohner, sowie auch für die Wirtschaft und für Organisationen, ein zusammenfassendes, themenfokussiertes und gemeinsames Angebot von digitalen Dienstleistungen der öffentlichen Hand zu schaffen. Zu diesem Zweck wurde das Smart Service Portal entwickelt, auf welchem nach und nach digitale Dienstleistungsangebote von Kanton und Gemeinden sowie spezifische Digitalangebote der bei Fit4Digital mitmachenden Gemeinden zusammengeführt werden.

2.1.3 Strategie für eine digitale Schweiz

Zur Steuerung der "Digitalen Verwaltung" intensivieren der Bund, die Gemeinden und Städte ihre Zusammenarbeit, die im Jahr 2008 begann. Konkret haben der Bundesrat und die Plenarversammlung der Konferenz der Kantonsregierungen (KdK) hierzu Anfang April 2020 ein umfassendes Projekt beschlossen. Mithilfe dieses Projekts sollen bestehende personelle und finanzielle Ressourcen gebündelt und in einer neuen Organisation effektiver eingesetzt werden. Dies mit dem Ziel, der gesellschaftlichen Entwicklung hin zu einer Informationsgesellschaft mit einem beschleunigten Fortschritt der Digitalisierung in der Verwaltung gerecht zu werden. Per 1. Januar 2022 wurde hierfür die neue Zusammenarbeitsorganisation Digitale Verwaltung Schweiz (DVS) geschaffen. Die DVS fördert die

digitale Transformation der Verwaltungen in der Schweiz. Dies namentlich durch die Entwicklung von Standards und als politische Plattform, als welche sie die Aufgaben von E-Government Schweiz und der Schweizerischen Informatikkonferenz (SIK) übernimmt. Als gleichberechtigte Träger der DVS haben sowohl der Bund als auch die Kantone die öffentlich-rechtliche Rahmenvereinbarung über die Digitale Verwaltung Schweiz in der Bundesratssitzung vom 24. September 2021 beziehungsweise in der Plenarversammlung der KdK vom 17. Dezember 2021 ratifiziert. Im Kern regelt diese Rahmenvereinbarung die Zusammenarbeit von Bund und Kantonen im Bereich der digitalen Transformation ihrer Verwaltungen. Die Kantone beziehen hierzu ihre Gemeinden mit ein.

Der Bundesrat und die Kantonsregierungen wollen zukünftig gemeinsame Schlüsselprojekte im Bereich der Digitalisierung rasch anstossen und den Aufbau der digitalen Verwaltung vorantreiben. Diese Vorhaben sind in der Agenda «Nationale Infrastrukturen und Basisdienste Digitale Verwaltung Schweiz» (Agenda DVS) zusammengefasst. Der Bund hat durch die Vorfinanzierung der Agenda DVS in den Jahren 2022 und 2023 einen wichtigen Beitrag zur Umsetzung dieser Vorgaben geleistet. Der Bund ist zudem bereit, weiterhin bis zu zwei Drittel der Kosten für die Agenda DVS zu übernehmen. Für die Finanzierung von Projekten der Agenda DVS 2024-2027 wurden mit dem "Bundesgesetzes über den Einsatz der elektronischen Mittel zur Erfüllung von Behördenaufgaben (EMBAG)" und einer Finanzierungsvereinbarung zwischen Bund und Kantonen rechtliche Grundlagen geschaffen. Der Bundesrat hat an seiner Sitzung vom 9. Juni 2023 die Finanzierungsvereinbarung genehmigt. Anlässlich der Plenarversammlung der KdK am 23. Juni 2023 haben alle 26 Kantone der Unterzeichnung der von den Kantonsregierungen formell genehmigten Finanzierungsvereinbarung durch die KdK zugestimmt.

Für den Beitrag des Kantons Aargau an die Digitale Verwaltung Schweiz (Grundfinanzierung und Agenda DVS 2024–2027) hat der Grosse Rat einen Verpflichtungskredit in der Höhe von Fr. 3'445'596.– beschlossen (GRB Nr. 2023-1168).

Mit der Dachstrategie "Digitale Verwaltung Schweiz 2024–2027" soll zudem ein gemeinsames Verständnis für die Umsetzung und Weiterentwicklung der digitalen Verwaltung geschaffen werden. Der Bundesrat hat die Strategie DVS an seiner Sitzung vom 8. Dezember 2023 und die KdK an ihrer Plenarversammlung vom 15. Dezember 2023 verabschiedet.

2.1.4 Öffentlichkeitsprinzip

Mit der Einführung des Öffentlichkeitsprinzips im Rahmen des Inkrafttretens des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 (SAR 150.700) per 1. Juli 2008 wurde im Kanton Aargau ein Paradigmenwechsel vollzogen. Statt des Geheimhaltungsprinzips mit Öffentlichkeitsvorbehalt gilt seither das Öffentlichkeitsprinzip mit Geheimnisvorbehalt (§ 4 ff. IDAG). Dies mit dem Ziel, eine effektive, demokratische Kontrolle der Verwaltungstätigkeit durch die Einwohnerinnen und Einwohner zu ermöglichen, was einem modernen Staatsverständnis entspricht (vgl. § 4 Abs. 2 IDAG). Jede Person hat daher grundsätzlich Zugang zu den amtlichen Dokumenten und klar geregelte Informationsrechte. Die Tragweite des Grundsatzes der Öffentlichkeit geht über den rein rechtlichen Rahmen hinaus, denn er besagt letztlich, dass der Staat seine Informationen im Auftrag und im Namen der Bevölkerung bearbeitet. Wird der Zugang zu einem Dokument zum Schutz von überwiegenden öffentlichen oder privaten Interessen ausnahmsweise eingeschränkt, aufgeschoben oder verweigert (§ 5 Abs. 3 IDAG), ist das Dokument in der Folge seinem tatsächlichen Schutzbedarf entsprechend zu schützen.

2.1.5 Open-Government-Data Strategie Schweiz und Aargau

Daten sind der Rohstoff der Wissensgesellschaft. Zur Erfüllung ihrer gesetzlichen Aufgaben erhebt, erstellt, verwaltet, verarbeitet und speichert die öffentliche Verwaltung eine grosse Menge von Daten. Publikation und Bereitstellung dieser Daten bergen ein grosses Potenzial, das in der Schweiz und im Kanton Aargau nur teilweise ausgeschöpft wird. Eine Open-Government-Data-Strategie (OGD-Strategie) gibt vor, welche Strategie das entsprechende Gemeinwesen betreffend offene

Behördendaten, also jene Datenbestände des öffentlichen Sektors, die im Interesse der Allgemeinheit ohne jede Einschränkung frei zugänglich gemacht werden, verfolgt.

Mit dem Ziel, möglichst viele Daten der öffentlichen Verwaltung im Sinne von OGD offen und maschinenlesbar zugänglich sowie frei wiederverwendbar zu machen, genehmigte der Bundesrat am 16. April 2014 die OGD-Strategie Schweiz 2014–2018. Aufbauend auf der OGD-Strategie Schweiz legten der Kanton Aargau und die Aargauer Gemeinden in der OGD-Strategie Aargau 2017–2022 die Grundlage für den Ausbau des Zugangs zu Behördendaten und die Nutzung des Potenzials von OGD. Der Aargau übernimmt aus der OGD-Strategie Schweiz eine auf drei Schwerpunkten basierende Vision. Demgemäss soll OGD Innovation und wirtschaftliches Wachstum ermöglichen, Transparenz und Partizipation fördern sowie die Effizienz der Verwaltung erhöhen. Der kantonale Umgang mit OGD wird durch die interne Leit- beziehungsweise Richtlinie "OGD Policy Aargau" konkretisiert. Diese Policy dient als Hilfsmittel der kantonalen und kommunalen Verwaltung, um identifizieren zu können, welche Daten in welcher Form veröffentlicht werden dürfen. Die Umsetzung der Strategie liegt in der Verantwortung der Verwaltungseinheiten, die entsprechende Datenstämme halten.

Die Open-Government Data Strategie 2019–2023 des Bundes ist abgestimmt auf die Strategie "Digitale Schweiz" mit ihrem Aktionsplan sowie auf die Eckwerte für die nächste E-Government-Strategie Schweiz. Namentlich bei der Schaffung der rechtlichen Rahmenbedingungen besteht eine enge Zusammenarbeit mit dem E-Government. Offene und frei nutzbare Verwaltungsdaten fördern Transparenz, Partizipation und Innovation in allen gesellschaftlichen Bereichen. Um dies nachhaltig zu unterstützen und zu verankern, sollen die Daten von Bundesstellen zunehmend als offene, maschinenlesbare Verwaltungsdaten (OGD) auf dem Portal *opendata.swiss* publiziert werden. Daneben beschreibt die OGD-Strategie Schweiz 2019–2023 die Förderung einer national koordinierten Datenpublikation, die Gewährleistung hochqualitativer Daten und Beschreibungen, die Schaffung und Nutzung eines zentralen Registers mit Metadaten sowie die Förderung der Datennutzung. Der Regierungsrat stimmte der Erneuerung und der Entwicklung eines Masterplans zur Umsetzung der Open Government Data (OGD)-Strategie Kanton Aargau zu.

2.2 Risiken der Informationsgesellschaft beziehungsweise der Digitalisierung

2.2.1 Überblick

Die Nutzung von Informationssystemen und die Digitalisierung von Prozessen in allen Bereichen des Lebens hat durch die Corona-Pandemie rascher und stärker zugenommen als schon in den Jahren zuvor. Der gesellschaftliche Wandel hin zu einer Informationsgesellschaft beziehungsweise die Digitalisierung birgt jedoch nicht nur Chancen, sondern auch Risiken. Die zunehmende Abhängigkeit von Informations- und Kommunikationstechnologie (IKT) macht auch den Kanton Aargau verwundbarer gegenüber Ausfällen, Störungen und Missbräuchen dieser Technologien. Der wahre Wert von Informationen wird oft erst nach einem Cybervorfall und beim Eintreten negativer Auswirkungen erkannt. Informationen sind, im Zeitalter der Informationsgesellschaft, wertvoller als je zuvor und werden häufig auch als die Währung des 21. Jahrhunderts bezeichnet. Sowohl für öffentliche Stellen als auch für Unternehmen und Privatpersonen kann der Verlust, der Diebstahl, die unberechtigte Preisgabe oder der Missbrauch von Informationen äusserst unliebsame Folgen zeitigen. Insbesondere kann dies die Beeinträchtigung von öffentlichen Interessen aber auch erhebliche finanzielle Folgen nach sich ziehen. Zudem können die Rechte Dritter verletzt werden. Auch die Informations- und Kommunikationsinfrastruktur sowie die einzelnen Informatikmittel, die Behörden und Unternehmen zur Unterstützung ihrer Geschäftsprozesse einsetzen, sind verwundbar. Der Ausfall eines Informatiksystems kann je nachdem, wie heikel oder wichtig die damit bearbeiteten Informationen sind, erhebliche finanzielle Folgen nach sich ziehen oder in schwerwiegenden Fällen die Erfüllung gesetzlicher Aufgaben des Staates bedrohen. Er kann insbesondere die Handlungsfähigkeit des Staates ganz oder teilweise beeinträchtigen, was unerwünschte Folgen für den Kanton Aargau und seine Bevölkerung haben kann. Wenn ein Ausfall eines Informatiksystems die Betreiberin einer kritischen Infrastruktur betrifft, die Dienste erbringt, die für das Funktionieren der Gesellschaft, der Wirtschaft oder des öffentlichen

Sektors unerlässlich sind, kann dies schlimmstenfalls katastrophale Auswirkungen, einschliesslich des Verlusts von Menschenleben, zur Folge haben.

2.2.2 Gefahren für Informationen und Informatikmittel

Die Medien berichten fast täglich über Spionage, Angriffe, Ausfälle von Informatikdiensten und sonstige Ereignisse im Bereich der Informationssicherheit. Diese Gefahren werden auch in der vom Bundesrat verabschiedeten Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022 vom 18. April 2018 beschrieben. Gemäss NCS lassen sich fünf Arten von beabsichtigten unerlaubten Handlungen im Bereich der Informationstechnik (auch als "Cyber"-Angriffe bezeichnet) unterscheiden, wobei zu beachten ist, dass diese häufig in Kombination auftreten und zwischen ihnen Überschneidungen bestehen:

a) Cyber-Kriminalität: Im engeren Sinn Straftaten, die mit Hilfe von IKT verübt werden oder sich Schwachstellen dieser Technologien zu Nutzen machen und somit erst durch IKT ermöglicht werden, sowie im weiteren Sinn auch Straftaten, bei denen IKT als Tat- und Speichermedien verwendet werden, die aber auch ohne Einsatz von IKT möglich wären.

b) Cyber-Spionage: Tätigkeit, um im Cyber-Raum für politische, militärische oder wirtschaftliche Zwecke unerlaubt an Informationen zu gelangen.

c) Cyber-Sabotage und -Terrorismus: Cyber-Sabotage bezeichnet eine Tätigkeit, um im Cyber-Raum das zuverlässige und fehlerfreie Funktionieren von IKT zu stören oder zu zerstören, was je nach Art der Sabotage und des angegriffenen Ziels auch zu physischen Auswirkungen führen kann. Ein von Tätern mit terroristischen Motiven durchgeführter Sabotageakt wird als Cyber-Terrorismus bezeichnet.

d) Desinformation und Propaganda: Gezielte Verbreitung von Falschinformationen oder von illegal über Cyber-Angriffe beschafften Informationen mit dem Zweck der Diskreditierung von politischen, militärischen oder zivilgesellschaftlichen Akteuren.

e) Cyber in Konflikten: Während ein ausschliesslich im Cyber-Raum geführter Krieg (Cyber-War) gegenwärtig als unrealistisches Szenario betrachtet wird, zeigte sich, dass Cyber-Angriffe aller Arten als Mittel der Kriegsführung in verschiedenen Konflikten eingesetzt werden.

Diese Cyber-Gefahren, also Bedrohungen durch den oder beim Einsatz von Informationstechnik, sind ernst zu nehmen. Neben der organisierten Kriminalität, welche sich vor allem gegen Privatpersonen richtet, gibt es auch Staaten, die teilweise immense finanzielle und personelle Mittel einsetzen, um politische, diplomatische, wissenschaftliche und wirtschaftliche Spionage zu betreiben, aber auch um eine Destabilisierung demokratischer Ordnungen herbeizuführen. Dabei geht es nicht nur um den Schutz der Vertraulichkeit von Informationen, sondern mittelbar auch um den Schutz der Verfügbarkeit von öffentlichen und privaten Infrastrukturen und Diensten, die vom einwandfreien Funktionieren der Informationstechnik abhängen. Eine viel zitierte Gefährdung ist der im Juni 2010 entdeckte Angriff auf iranische Urananreicherungsanlagen mittels des Schadprogramms Stuxnet. Dennoch ist zu beachten, dass unbeabsichtigt herbeigeführte Ereignisse (menschliches Fehlverhalten und technische Ausfälle) wie Betriebsstörungen wegen technischen Versagens, Fehlmanipulationen oder Elementarereignisse wie ein durch eine unglückliche Verkettung von Zufällen verursachter längerer Stromausfall oder Brand deutlich öfter vorkommen und ebenso gravierende Auswirkungen zur Folge haben können. Eine zu enge Fokussierung auf den Bereich "Cyber" ist daher problematisch, denn es gibt auch wesentliche Gefahren für die Informationssicherheit, die nichts, wenig oder nur indirekt mit Informationstechnik und Angriffen auf diese zu tun haben.

2.2.3 Risiken für den Kanton Aargau

Die kantonalen Behörden, die Gemeinden und andere öffentlich-rechtliche Institutionen sind den erwähnten Gefahren genauso ausgesetzt wie private natürliche und juristische Personen. Sie betreiben nämlich auch Informations- und Kommunikationsinfrastrukturen, deren Störung, Ausfall oder

Zerstörung die Erfüllung kritischer gesetzlicher Aufgaben gefährden und somit gravierende Auswirkungen auf die Gesellschaft, die Wirtschaft oder den Staat haben kann. Zudem bearbeitet der Kanton zur Erfüllung seiner Aufgaben täglich grosse Mengen von Informationen. Unter diesen Informationen befinden sich auch solche, die aufgrund ihrer Natur klassifiziert und speziell zu schützen sind. Klassifizierte Informationen sind aber nicht die einzigen Informationen, die einen erhöhten Schutzbedarf aufweisen. Spionage zielte zwar in der Vergangenheit hauptsächlich auf die Beschaffung von militärischen und aussenpolitischen Informationen. Sie ist heute aber vermehrt wirtschaftsorientiert. Im harten globalen Wettbewerb schafft sich derjenige einen entscheidenden Vorteil, der sich das Wissen (Forschungs- und Entwicklungsergebnisse, Know-how) seiner Konkurrenten verschaffen kann. Entsprechend hat Spionage in der Wirtschaft und in der Industrie, insbesondere im hochtechnologischen Bereich, seit einigen Jahren zugenommen. Dies ist in Bezug auf die kantonale Verwaltung insofern von Belang, als sie die Privatwirtschaft in gewissen Bereichen reguliert; sie prüft bestimmte Produkte und entscheidet über deren Zulassung; sie kontrolliert Unternehmen; sie beschafft selber hochwertige Produkte und Dienstleistungen usw. Hierbei bearbeitet der Kanton etwa aufgrund seiner hoheitlichen Befugnisse mitunter auch Informationen, die Geschäfts- und Fabrikationsgeheimnisse Dritter beinhalten. Er kann daher ins Visier derjenigen geraten, die sich solche Informationen beschaffen wollen. Dritte, die ihre Informationen aufgrund einer gesetzlichen Pflicht oder eines Vertrags den kantonalen Behörden anvertrauen, erwarten zu Recht, dass diese auch dort zuverlässig geschützt werden.

Zudem bearbeitet der Kanton in grossem Umfang Personendaten. Diese dürfen nach den Vorschriften der Datenschutzgesetzgebung nur rechtmässig, zweckkonform sowie in verhältnismässigem Rahmen bearbeitet werden (vgl. §§ 8-11 IDAG). Sie müssen gemäss § 12 Abs. 1 IDAG mit angemessenen organisatorischen und technischen Massnahmen geschützt werden. Bei einem Datenmissbrauch können die Persönlichkeitsrechte der Personen, deren Daten bearbeitet werden, schwerwiegend verletzt werden. Gewisse Personendaten sind ebenso gefragt wie Technologieinformationen der Industrie. Es gibt einen blühenden Markt für die Beschaffung und die Bekanntgabe personenbezogener Daten.

Diese Risiken sind für den Kanton nicht nur reine Theorie. In den vergangenen Jahren, aber auch jüngst, wurde regelmässig von Organisationen berichtet, die von Informationssicherheitsvorfällen betroffen waren und damit erheblichen mutmasslichen oder realen Schaden erfahren haben (zum Beispiel RUAG, Siegfried AG, NZZ, Xplain oder Angriffe auf kritische Infrastrukturen). Im ersten Quartal 2021 sah sich die Informatik Aargau (IT AG) kurzfristig gezwungen, mehrere aargauische Gemeinden temporär vom kantonalen Netzwerk zu trennen, nachdem das Monitoring wegen verdächtiger Aktivität aufgrund einer ausgenützten Sicherheitslücke anschlug (Schweregrad 9.8 auf einer Skala von 10). Von Angreifern aus dem Ausland wurde im gleichen Zeitraum erreicht, dass die Virtual Private Network (VPN) Infrastruktur, welche für die sichere Verbindung zwischen mobilen Arbeitsgeräten der Mitarbeitenden des Kantons Aargau und dem kantonalen Netzwerk aufgebaut wird, lahmgelegt wurde. Dieser Ausfall in den frühen Morgenstunden konnte durch das schnelle Eingreifen der Spezialisten der IT AG innert Stunden behoben und der Normalbetrieb wiederhergestellt werden. Nicht vergessen werden dürfen die Bedrohungen durch das mögliche Fehlverhalten von Mitarbeitenden des Kantons. Diese Ereignisse reichen von Diebstahl oder Verlust von mobilen Computern, Smartphones oder klassifizierten Informationsträgern über unberechtigte, meistens politisch motivierte Preisgabe von vertraulichen Informationen bis zu Betriebsstörungen wegen Server-Ausfällen, Netzwerk-Überlastungen oder fehlerhaften Software-Konfigurationen. Bei schweren oder wiederholten Vorfällen kann das Vertrauen in den Staat ernsthaft gestört werden, und es muss auch mit Schäden für Dritte und entsprechenden Forderungen aus möglichen Persönlichkeitsverletzungen gerechnet werden.

2.3 Informationssicherheit

2.3.1 Verortung

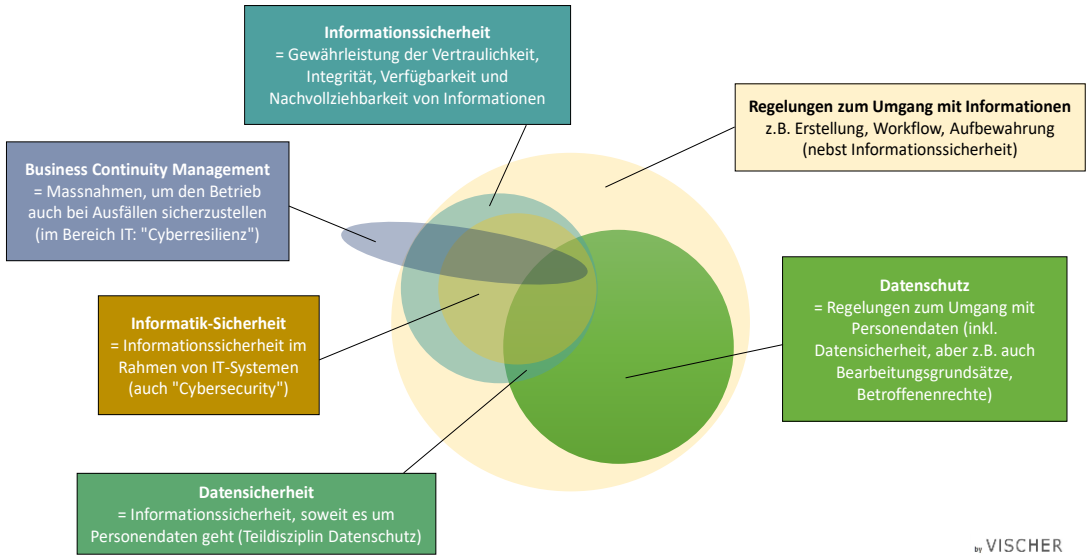
Die Gewährleistung der Informationssicherheit gehört als Thema zum Risikomanagement eines jeden Gemeinwesens und eines jeden Unternehmens. **Sie umfasst die Gesamtheit aller Anforderungen und Massnahmen, mit denen die Vertraulichkeit, die Verfügbarkeit, die Integrität und die Nachvollziehbarkeit von Informationen gewährleistet werden kann.** Informationssicherheit bezweckt mit anderen Worten folgende vier Schutzziele:

Tabelle 1: Die vier Schutzziele der Informationssicherheit

Vertraulichkeit	Informationen sind nur den berechtigten Personen zugänglich.
Verfügbarkeit	Informationen sind verfügbar, wenn sie benötigt werden.
Integrität	Informationen werden nicht unberechtigt oder unbeabsichtigt verändert.
Nachvollziehbarkeit	Informationen werden nachvollziehbar bearbeitet.

Die Schutzziele beziehen sich auf Informationen sämtlicher Art und ohne Rücksicht auf die Art des Informationsträgers. **Die Informationssicherheit darf demnach nicht auf die Informatiksicherheit (Schutz elektronisch gespeicherter Informationen und deren Verarbeitung) reduziert werden.** Vielmehr umfasst die Informationssicherheit alle Bearbeitungsvorgänge, also auch Papierdokumente und mündliche Äusserungen, und nicht nur die elektronische Bearbeitung. Demgegenüber bildet die Informatiksicherheit – wie auch die Datensicherheit gemäss § 12 IDAG oder die Umsetzung anderer Gesetze, die Anforderungen an den Schutz von Informationen festlegen – einen Bestandteil der Informationssicherheit (vgl. Abbildung 1). Informatiksicherheit meint Informationssicherheit im Rahmen von Informatiksystemen (aber z.B. nicht den physischen Schutz von Gebäuden), und Datensicherheit im Sinne des IDAG meint Informationssicherheit nur in Bezug auf Personendaten.

Abbildung 1: Verortung Informationssicherheit (Quelle: VISCHER AG)



2.3.2 Abgrenzungen

a) Beim Datenschutz geht es um den Schutz der Privatsphäre und der Persönlichkeit eines jeden Menschen im Bereich der Bearbeitung seiner Daten. Er garantiert natürlichen Personen ein Recht auf informationelle Mitwirkung und schützt diese Personen vor einer missbräuchlichen Verwendung der sich auf sie beziehenden Daten. Im Unterschied zum Datenschutz befasst sich die Informationssicherheit mit dem Schutz von Daten unabhängig davon, ob diese einen Personenbezug aufweisen oder nicht. Die Massnahmen zur Gewährleistung der Informationssicherheit soll Sicherheitsrisiken begegnen und die Daten zum Beispiel vor Manipulation, Verlust oder

unberechtigter Kenntnisnahme schützen. Dabei ist hier ebenfalls unerheblich, ob es sich um digitale oder analoge Informationen handelt und ob diese einen Personenbezug haben.

b) Die ordnungsgemässe Aktenführung und Archivierung unterstützt die Geschäftsbearbeitung und ermöglicht die Nachvollziehbarkeit und Transparenz staatlichen Handelns. Die Aktenführung umfasst die effiziente und systematische Planung, Durchführung und Kontrolle der Aufzeichnung von Geschäften und der fachgerechten Verwaltung der dabei entstehenden Dokumente. Die öffentlichen Organe sind gemäss Kapitel fünf des IDAG zum Archivwesen (§ 43 ff. IDAG) zur Sicherstellung, Registrierung und Bewahrung aller Dokumente verpflichtet, denen für die Wissenschaft und Öffentlichkeit Bedeutung zukommt. Die Aktenführung muss unabhängig von Verfahren, Systemen, Prozessen und Informationsträgern die Anforderungen der Authentizität, der Integrität, der Zuverlässigkeit und der Nutzbarkeit von Dokumenten erfüllen.

c) Das betriebliche Kontinuitätsmanagement (Business Continuity Management, BCM) ist ein Begriff der Betriebswirtschaftslehre und ein Managementprozess, der sicherstellt, dass kritische Geschäftsprozesse und Geschäftsfunktionen auch in Notsituationen verfügbar bleiben oder rechtzeitig wieder verfügbar sind. Es besteht eine enge Verwandtschaft zur Informationssicherheit, insbesondere mit dem Schutzziel "Verfügbarkeit". Die Informationssicherheit überlappt sich dort mit dem betrieblichen Kontinuitätsmanagement, wo es um die Gewährleistung der Verfügbarkeit von Informationen und deren Bearbeitungsmöglichkeiten (mithin also der dafür verwendeten Informationstechnik) geht. BCM will die Fähigkeit zur Geschäftsfortführung allerdings auch in anderen Bereichen sicherstellen.

d) An das BCM als vorbereitenden Prozess auf eine Krise schliesst sich das Krisenmanagement an und bezeichnet den systematischen Umgang mit Krisensituationen, wenn eine solche eintritt.

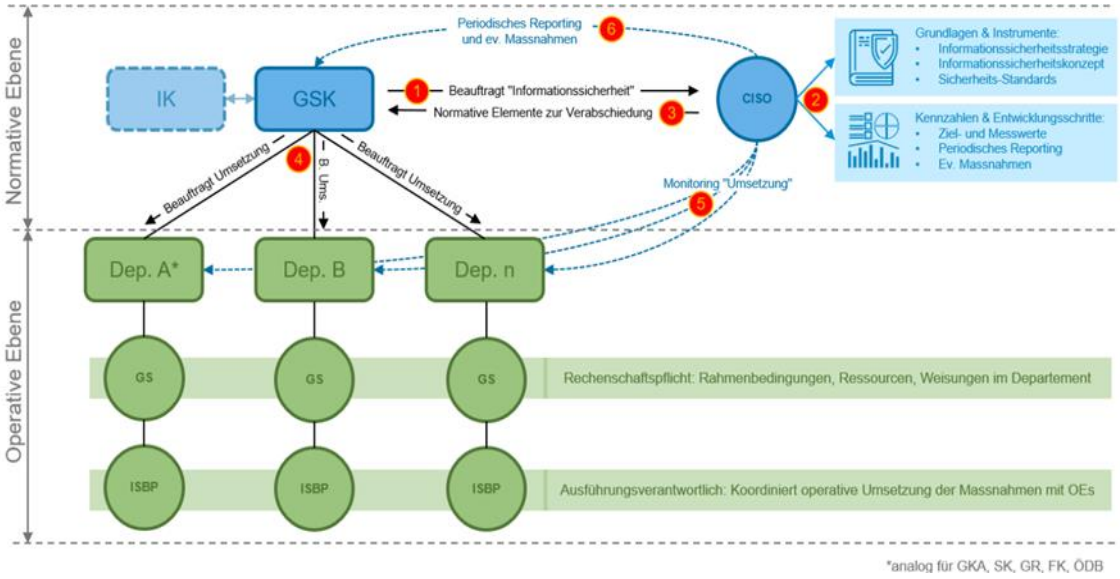
e) Der Begriff der Informatik- beziehungsweise der IT-Sicherheit meint die Sicherstellung der Vertraulichkeit, der Verfügbarkeit, der Integrität und der Nachvollziehbarkeit bei der elektronischen Bearbeitung von Informationen mittels Informatiksystemen. Der Begriff umfasst zwar alle vier Schutzziele der Informationssicherheit, beschränkt sich aber auf die Bearbeitung von elektronisch gespeicherten Daten und umfasst nicht Informationen, die beispielsweise auf Papier festgehalten sind.

f) Cybersicherheit (Cybersecurity) beschreibt den anzustrebenden Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert. Die Cybersicherheit umfasst sämtliche Risiken, Massnahmen, Prozesse und Aufgaben auf organisatorischer und technischer Ebene zur Identifikation, Analyse und Bewältigung von Cyberbedrohungen und -angriffen. Sie ist ein wichtiger Teil der Informationssicherheit mit Schnittstellen zu Krisenmanagement, Kommunikation, BCM, Informatiksicherheit, Datenschutz und Informationsschutz sowie IT-Prozessen an und für sich.

2.3.3 Organisation der Informationssicherheit in der kantonalen Verwaltung

Aktuell ist für die Führung und Steuerung der Informatik in der kantonalen Verwaltung die Generalsekretärenkonferenz (GSK) zuständig. Sie ist auch gestützt auf die Richtlinie der GSK mit der Gewährleistung, Aufrechterhaltung und Kontrolle der Informationssicherheit, namentlich mit der Etablierung eines wirkungsvollen Informationssicherheits-Managements beauftragt. Die dafür notwendigen Grundlagen und Instrumente werden durch den gesamtverantwortlichen für Informationssicherheit (Chief Information Security Officer; CISO) geschaffen und unterhalten. Die Umsetzung der Informationssicherheit ist in Zusammenarbeit zwischen den Departementen und der IT AG vorgesehen. Das heutige Governance-Modell in Bezug die Informationssicherheit des Kantons Aargau sieht wie folgt aus:

Abbildung 2: Heutiges Governance-Modell der Informationssicherheit des Kantons Aargau



Dieses Governance-Modell führt zur in den Abbildungen 3 und 4 dargestellten Organisation der Informationssicherheit inklusive Cybersicherheit:

Abbildung 3: Heutige Organisation der Informationssicherheit des Kantons Aargau

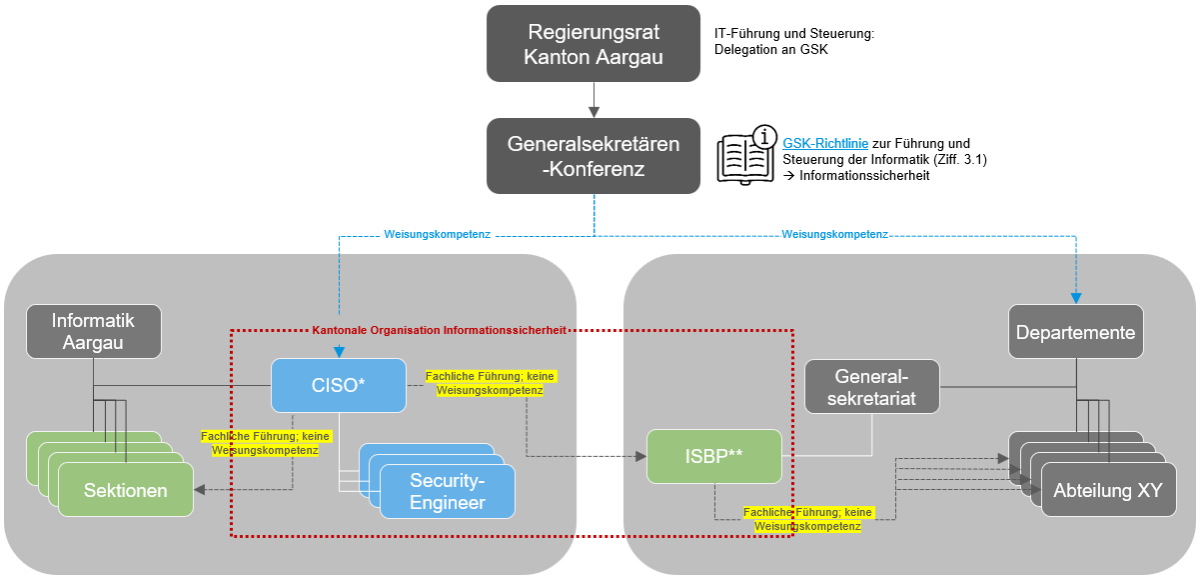
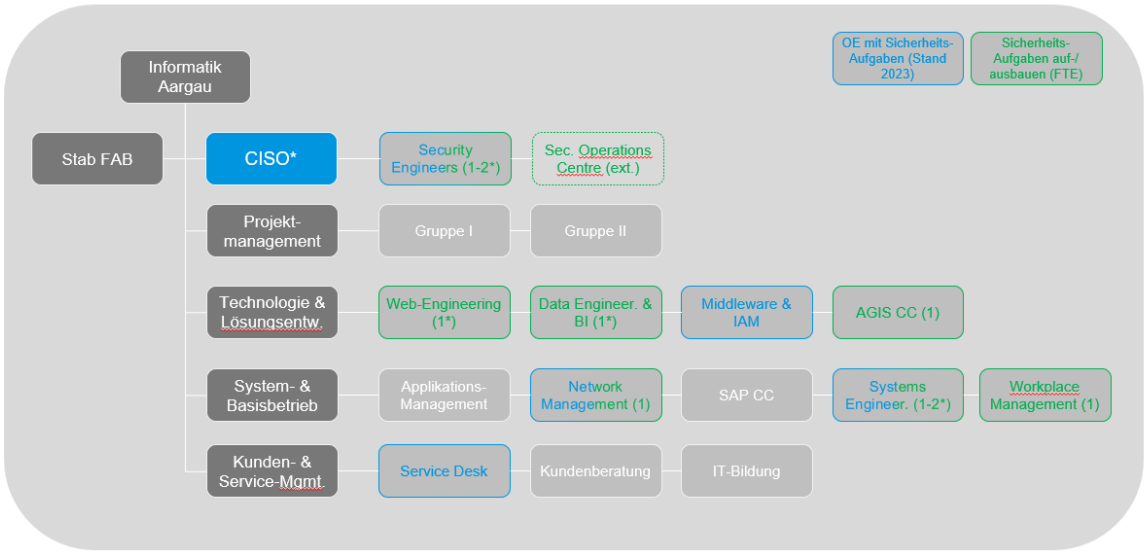


Abbildung 4: Heutige Organisation der Informationssicherheit der IT AG



2.3.3.1 Generalsekretärenkonferenz (GSK)

Die GSK koordiniert im Auftrag des Regierungsrats betriebliche Sachgeschäfte, die strategische Führung der Informatik und stimmt das Verwaltungshandeln in Querschnittsbereichen (Planung und Berichterstattung, Personal- und Infrastrukturbelange) ab. Die GSK hat am 8. November 2021 die Richtlinie der GSK für die Führung und Steuerung der Informatik in der kantonalen Verwaltung vom 8. November 2021 (nachfolgend: RL GSK Informatik) verabschiedet und per 1. Januar 2022 in Kraft gesetzt. Gemäss Ziffer 5.2 der RL GSK Informatik ist die IT AG für das periodische Reporting zum Informationssicherheits-Management verantwortlich, das die Etablierung, Aufrechterhaltung und Kontrolle der Informationssicherheit umfasst. Gestützt auf Ziffer 4 RL GSK Informatik erliess die GSK am 8. November 2021 das Reglement für die Informatikkonferenz (nachfolgend: RL GSK IK). Weiter hat die GSK am 30. August 2021 die Informationssicherheitsstrategie des Kantons Aargau erlassen. Die Informationssicherheitsstrategie legt die Aufgaben, Kompetenzen und Verantwortungen fest und kann als das zentrale Dokument der Informationssicherheit im Kanton Aargau bezeichnet werden. Die Gerichte Kanton Aargau (GKA) sind eingeladen, die Strategie zu beachten und umzusetzen.

2.3.3.2 Generalsekretärinnen und Generalsekretäre

Die Generalsekretärinnen und Generalsekretäre sind für die Umsetzung der Informationssicherheit im eigenen Verantwortlichkeitsbereich rechenschaftspflichtig und tragen die Verantwortung für die Sicherstellung der personellen und finanziellen Ressourcen zur Umsetzung der Informationssicherheit. Es ist vorgesehen, dass Sie die Ausführungsverantwortung für die operative Umsetzung der Informationssicherheit im eigenen Zuständigkeitsbereich an die Informationssicherheitsbeauftragte Personen (ISBP) übertragen.

2.3.3.3 Informatikkonferenz (IK)

Die Informatikkonferenz (IK) unterstützt die GSK in der Erfüllung ihrer Aufgaben bei der strategischen Führung und der darauf abgestimmten taktischen/operativen Umsetzung der Informatik in der kantonalen Verwaltung, insbesondere durch eine zielgerichtete und lösungsorientierte Arbeit bei der Vorberatung von Informatikgeschäften. Die IK besteht aus den Informatikbeauftragten (IB) der fünf Departemente, der Staatskanzlei (SK) und der GKA sowie aus dem Leiter der IT AG und dem Leiter Kunden- und Servicemanagement der IT AG. Die Beschlüsse und Empfehlungen der IK gelten für die Departemente sowie die SK beziehungsweise als Empfehlung für die GKA und den Parlamentsdienst des Grossen Rats. Änderungen der Informationssicherheitsstrategie werden der IK vor der Verabschiedung durch die GSK zur Stellungnahme unterbreitet.

2.3.3.4 Chief Information Security Officer (CISO)

Der Chief Information Security Officer (CISO) ist für den Bereich der Informationssicherheit des Kantons insoweit verantwortlich, als er die Grundlagen, Instrumente und Prozesse zur Sicherstellung einer angemessenen Informationssicherheit (insbesondere mittels eines Informationssicherheits-Managementsystem [ISMS]) zu schaffen, zu unterhalten und weiterzuentwickeln hat. Für die operative Umsetzung dieser Vorgaben ist er nicht verantwortlich. Die Beauftragung erfolgt durch die GSK, welche die Informationssicherheit im Kanton steuert und entwickelt. Der CISO unterstützt die ISBP der Departemente, der Gerichte und der Staatskanzlei in allen Belangen der Informations- und Informatiksicherheit. Zudem erstattet der CISO periodisch Bericht zuhanden der GSK und der IK betreffend Informationssicherheit, führt Schwachstellen- und Risikoanalysen durch und stösst Änderungen beziehungsweise Ergänzungen der Informationssicherheitsstrategie, des Informationssicherheitskonzepts und der Sicherheits-Standards unter Wahrung der vorgesehenen Kompetenzen der GSK und der IK an. Wesentlich ist auch seine Aufgabe betreffend die "Hinzuziehung und Aktivierung der zuständigen Verantwortlichen bei Informationssicherheitsvorfällen und Aktivierung der Notfallorganisation in Krisenfällen". Schliesslich ist er kompetent zur Anordnung von Sofortmassnahmen in Not- und Krisenfällen unter Einbezug beratender Gremien und Spezialisten. Er ist in die Organisation der IT AG eingebettet.

2.3.3.5 Informationssicherheitsbeauftragte Person (ISBP)

Die Ausführungsverantwortung für die operative Umsetzung des Informationssicherheits-Managements obliegt gemäss Informationssicherheitsstrategie des Kantons Aargau vom 2. September 2021 (Ziffer 3.2.5) der ISBP: "Die Rolle der ISBP wird in der Regel durch den Informatikbeauftragten [IB] der Departemente, GKA und SK wahrgenommen […]." Entsprechend hat jede zuständige Instanz gemäss § 1 Abs. 2 der Verordnung über die wirkungsorientierte Steuerung von Aufgaben und Finanzen (VAF) vom 5. Dezember 2012 (SAR 612.311) sowie die Justizleitung als beauftragte Instanz gemäss § 1 Abs. 1 VAF eine ISBP. Die ISBP ist Ansprechperson für den CISO und die Fachbereiche, sowie Koordinationsstelle für die Informationssicherheit betreffend Themen im departementalen Zuständigkeitsbereich. Die ISBP ist bei Notfällen und in Krisensituationen die Ansprechperson im eigenen Zuständigkeitsbereich.

2.3.3.6 Security- und Cybersecurity Engineer

Der Security- respektive Cybersecurity-Engineer ist in der IT AG (im Security Team, zusammen mit dem CISO) angestellt und für den Bereich IT-Sicherheit verantwortlich. Zudem obliegt ihm insbesondere auch die fachliche Führung und Koordination des Computer Security Response Teams (CSIRT) bei sicherheitsrelevanten Ereignissen (Cyber-Vorfälle).

2.4 Politische Vorstösse

Im Grossen Rat sind im Bereich der Informations- und Cybersicherheit in den vergangenen Jahren verschiedene politische Vorstösse eingereicht worden. Im Folgenden werden die Vorstösse sowie deren Beantwortung durch den Regierungsrat aufgeführt:

GR.22.29 Postulat der FDP-Fraktion (Sprecher Dr. Bernhard Scholl, Möhlin) vom 18. Januar 2022 betreffend Cyberkriminalität (Detail Geschäft (ag.ch))

Mit dem Postulat wurde der Regierungsrat eingeladen zu überprüfen, ob die derzeitigen gesetzlichen Grundlagen für einen umfassenden Schutz durch Angriffe aus dem Cyberraum ausreichen. Zusätzlich sollen auch spezifisch die folgenden Themen überprüft werden:

- Aufbau und Einrichtung einer kantonalen Organisation für Cybersicherheit
- Meldepflicht für von Cybercrime betroffene Gemeinden, Unternehmen, inklusive Institutionen mit öffentlichen Aufträgen, respektive in öffentlicher Hand

- Vernetzung zwischen den verschiedenen staatlichen und privaten Akteuren
- Verstärkte Schulung aller Mitarbeitenden von staatlichen Organisationen

In der Begründung wird auf die Empfehlungen des Sicherheitsverbunds Schweiz (SVS) für die Umsetzung zur kantonalen Cyber-Organisation vom 12. Januar 2021 (nachfolgend: Empfehlungen SVS) Bezug genommen (verabschiedet von der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren [KKJPD] am 12. November 2020). Darin werden die Anforderungen an eine Cyber-Organisation im Kanton und deren Aufgaben, Kompetenzen, Verantwortlichkeiten und Prozesse, sowie die Schnittstellen mit den Cyber-Strukturen des Bundes aufgeführt. Die Ziele des Konzepts sind:

- Vermeidung eines Cyber-Angriffs durch geeignete Massnahmen, zum Beispiel durch Identifikation, Schutz und Detektion
- Minimierung des Schadens (finanziell und in Bezug auf Image) nach einem Angriff und raschestmögliche Betriebsaufnahme der wichtigsten Geschäftsprozesse
- Die adäquate Ablauf- und Aufbauorganisation ist genehmigt, eingeführt und geübt
- Sicherstellung des Zugangs zu einer stufengerechten Sensibilisierung und Schulung für alle Mitarbeitenden der Verwaltung

Der Regierungsrat war mit Stellungnahme vom 8. Juni 2022 bereit, das Postulat mit Erklärung entgegenzunehmen (RRB Nr. 2022-000694). In der Folge überwies der Grosse Rat anlässlich der Sitzung vom 6. September 2022 (GRB Nr. 2022-0561) das Postulat stillschweigend dem Regierungsrat.

In seiner Stellungnahme vom 8. Juni 2022 erläuterte der Regierungsrat einerseits, wie die bestehende Organisation aufgebaut ist und wie im Kanton die Cyberkriminalität bekämpft wird. Der Regierungsrat wies auf die Aufgaben- und Finanzpläne (AFP) 2020–2023 und 2021–2024 hin, in welchen für die Aufgabenbereiche Polizeiliche Sicherheit (AB 210) und Strafverfolgung (AB 250) jeweils Entwicklungsschwerpunkte betreffend die Bekämpfung der Cyberkriminalität festgelegt worden sind. Damit werde eine gezielte Weiterentwicklung bei der Bekämpfung der Cyberkriminalität und der digitalisierten Kriminalität verfolgt. Kantonspolizei und Staatsanwaltschaft würden bereits eng zusammenarbeiten und hätten in den erwähnten AFPs einen Stellenaufbau eingestellt.

Zum anderen verwies der Regierungsrat in der Beantwortung des Postulats darauf, er hätte das Departement Finanzen und Ressourcen am 15. September 2021 beauftragt, ein Normkonzept zur Schaffung rechtlicher Grundlagen für die Informationssicherheit zu erarbeiten, worunter auch die im Postulat erwähnten Themen (Organisation für Cybersicherheit, Meldepflichten, Vernetzung Akteure und verstärkte Schulung von Mitarbeitenden staatlicher Organisationen) fielen.

Dementsprechend sind die Anliegen der Postulanten im Rahmen des vorliegenden Projekts geprüft worden und die Ergebnisse in den Gesetzesentwurf eingeflossen, weshalb anlässlich der 2. Beratung des zu schaffenden Informationssicherheitsgesetzes die Abschreibung des Postulats beantragt werden kann.

GR.21.199 Interpellation Dr. Bernhard Scholl, FDP, Möhlin, vom 24. August 2021 betreffend Cyberkriminalität (Detail Geschäft (ag.ch))

Die Interpellation griff den Umstand auf, dass professionelle Cyberangriffe, ausgehend von organisierten Gruppen, in der jüngsten Vergangenheit stark zugenommen hätten und einen grossen wirtschaftlichen Schaden verursachten. In diesem Zusammenhang wollte der Interpellant vom Regierungsrat folgende Fragen beantwortet haben:

- Wie wird die IT-Sicherheit von kritischen Infrastrukturen (u.a. Verwaltung, Gerichte, kantonale Ämter und Anstalten, Spitäler, AEW, AKB, usw.) beurteilt?
- Was wird unternommen, um allfällige Mängel zu beheben?

- Bestehen in kritischen Infrastrukturen Prozesse zur Bedrohungsanalyse?
- Existieren Notfallpläne beim Ausfall einer kritischen Infrastruktur?
- Wie läuft die Zusammenarbeit mit den entsprechenden Stellen beim Bund, anderen Kantonen und den Gemeinden?
- Was wird betreffend IT-Schulung der Mitarbeitenden unternommen, dem oft schwächsten Glied der Sicherheitskette?

Mit Datum vom 17. November 2021 hat der Regierungsrat die Interpellation beantwortet. Er hielt insbesondere fest, dass jeweils das oberste Leitungsorgan der Unternehmen für das Risikomanagement und die Sicherheit der IT-Systeme verantwortlich sei. Der Regierungsrat verfüge über keine Organfunktion und somit über keine direkten Weisungsbefugnisse gegenüber den Organen seiner Beteiligungen. Aufsichts- und Eigentümerfunktion nehme er mit verschiedenen Instrumenten wie Eigentümerstrategie, -gesprächen, -versammlungen etc. wahr. Der Regierungsrat hielt fest, der Kanton Aargau wolle die IT-Sicherheit durch eine umfassende Informationssicherheit aufrechterhalten. Den Schutz von kritischen Infrastrukturen beurteilte er als gegeben. Der Regierungsrat erkannte keine Notwendigkeit in Bezug auf weitergehende Schutzmassahmen der Beteiligungen im Bereich der IT-Sicherheit. Die in der Interpellation erwähnten Beteiligungen hätten Managementsysteme für die Informationssicherheit implementiert und entwickelten diese laufend weiter. Der Regierungsrat erklärte, dass der Kanton Aargau dank Vorrichtungen gegen elementare Schäden wie Wasser oder Stromausfälle und gegen Cyber-Angriffe gewappnet sei. Auch erhielte der Kanton Aargau durch die Mitgliedschaft im inneren Zirkel des Nationalen Zentrums für Cybersicherheit (NCSC) zeitnah Informationen zu aktuellen Bedrohungslagen und Angriffen gegenüber dem Verwaltungssektor. Eine weitere wichtige Austauschplattform sei von den IT-Sicherheitsbeauftragten der Deutschschweizer Kantone über die Arbeitsgruppe IT-Sicherheit der Schweizerischen Informatik Konferenz (SIK) geschaffen worden. Abschliessend hielt der Regierungsrat fest, dass über E-Learning-Module bezüglich Informationssicherheit und Awareness- und Informationsvideos seitens CISO die Mitarbeitenden der kantonalen Verwaltung ausgebildet und sensibilisiert würden. Dem Schulungs-Bereich werde grosse Aufmerksamkeit gewidmet.

Im Rahmen der Beantwortung dieser Interpellation wies der Regierungsrat zudem darauf hin, dass derzeit in seinem Auftrag die Schaffung spezifischer rechtlicher Grundlagen für die Informationssicherheit vorbereitet werde.

Der Interpellant erklärte sich von der Antwort teilweise befriedigt und das Geschäft wurde erledigt (GRB Nr. 2022-0371).

GR.20.342 Interpellation Sabina Freiermuth, FDP, Zofingen, vom 15. Dezember 2020 betreffend Sicherheit der IT-Systeme an Aargauer Spitälern (Detail Geschäft (ag.ch))

Die Interpellantin zeigte auf, dass eine Cyberattacke auf ein Spital ein besonders beunruhigendes Szenario darstellt, da einerseits höchstvertrauliche und -schützenswerte Patientendaten betroffen sein können und andererseits der Spitalbetrieb lahmgelegt werden kann. Die Auswirkungen wären vielfältig und folgenschwer. Aus Sicht der Interpellantin muss den kritischen Infrastrukturen aus dem Gesundheitssektor deshalb besondere Beachtung geschenkt werden. Um eine funktionierende Gesundheitsversorgung sicherzustellen, muss es im Interesse des Kantons sein, Spitäler ausreichend vor Cyberangriffen zu schützen.

Mit Datum vom 10. März 2021 beantwortete der Regierungsrat die Interpellation. Dabei teilte er mit, für die Spitäler bestehe keine Meldepflicht bei Cyberattacken. Eine Umfrage bei den Spitälern im Kanton Aargau habe ergeben, dass eine Mehrheit von ihnen mindestens einmal von einer Cyberattacke betroffen gewesen oder sogar regelmässig betroffen sei. Die Attacken hätten in den meisten Fällen abgewehrt werden können. In den verbleibenden Einzelfällen hätten keine grossen Auswirkungen oder Schäden resultiert. Die Spitäler investierten viel in die IT-Sicherheit, müssten diesbezüglich

gegenüber dem Kanton aber keine Rechenschaft ablegen. Bei den Eigentümergesprächen sei die IT-Sicherheit kein Thema. Der Regierungsrat kam damals zum Schluss, es bestehe kein unmittelbarer Handlungsbedarf. (In der Zwischenzeit wurde dies geändert. Die Themen Informationssicherheit und Cyber-Sicherheit werden im Rahmen der Eigentümergespräche standardmässig angesprochen. Eine entsprechende Regelung soll im Rahmen der anstehenden Revision der PCG-Richtlinien geprüft werden).

Die Interpellantin erklärte sich von der Antwort befriedigt und das Geschäft wurde erledigt (GRB Nr. 2021-0132).

GR.16.159 Interpellation Sukhwant Singh-Stocker, GLP, Möhlin, vom 28. Juni 2016 betreffend IT-Sicherheitsvorkehrungen gegen Cyberkriminalität in Staats- und staatsnahen Betrieben wie Spitäler und Strafanstalten im Kanton Aargau (Detail Geschäft (ag.ch))

Auch diese Interpellation gründete auf der Tatsache, dass Cyberkriminalität rasant zunimmt und eine grosse Gefahr für den Datenmissbrauch und Sabotage von kritischen IT-Systemen darstellt. Der Interpellant verwies auf aktuelle Beispiele von Cyberangriffen. Gestützt auf den Umstand, dass die staatlichen Betriebe u.a. besonders schützenswerte Daten bearbeiten, welche für Cyberkriminelle von Interesse sein können und deshalb besonderen Schutzes bedürften, wollte der Interpellant vom Regierungsrat folgende Fragen beantwortet haben:

- Gibt es eine Cybercrime-Strategie, die kritische Informatiksysteme und sensible Daten vor Diebstahl und Sabotage umfasst?
- Wie ist die Strategie umgesetzt und deren Effektivität sichergestellt?
- Stehen ausreichend Ressourcen bzw. Mittel für die Cyberabwehr zur Verfügung?
- Gibt es Funktionen wie Sicherheitsexperten (CISO) sowie ein umfassendes Informationssicherheitsmanagement (ISMS), um den Cyberrisiken entgegenzuwirken?
- Gibt es ausreichende gesetzliche Grundlagen, um eine umfassende Cybersicherheit für sensible Daten und kritische Systeme zu gewährleisten?
- Wird vom Regierungsrat regelmässig ein Informatikrisiko bzw. Sicherheitsbericht verlangt?
- Mit welchen Massnahmen wird reagiert, falls der Bericht ein erhöhtes Risiko dokumentiert?

Mit Datum vom 21. September 2016 hat der Regierungsrat die Interpellation beantwortet. In seiner Beantwortung stellte der Regierungsrat fest, dass für eine vollumfängliche konsequente Vor- und Nachbearbeitung von Cyberaktivitäten die Ressourcen fehlten und dass die Organisation bei Abwehr, Erkennung, Bewältigung und die Regeneration von Cyberbedrohungen eine übergeordnete Koordination und Führung erforderte. Diese Punkte wurden im vorliegenden Normkonzept aufgenommen. Andererseits war der Regierungsrat damals noch der Ansicht, dass es ausreichend gesetzliche Grundlagen gäbe, um eine umfassende Cybersicherheit zu gewährleisten.

Der Interpellant erklärte sich von der Antwort teilweise befriedigt und das Geschäft wurde erledigt (GRB Nr. 2016-1586).

3. Rechtsgrundlagen

3.1 Übersicht

Im Bundesrecht finden sich für den Kanton lediglich rechtliche Grundlagen für gestützt auf Bundesrecht durch den Kanton zu bearbeitende Informationen. So sieht das Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020 vor, dass es auch für die Kantone gelten soll, sofern die Kantone klassifizierte Informationen des Bundes bearbeiten und sie auf Informatikmittel des Bundes zugreifen. Die Bestimmungen des ISG sollen

hingegen nicht gelten, wenn die Kantone eine mindestens gleichwertige Informationssicherheit gewährleisten (Art. 3 ISG). Andererseits gelten für das Bearbeiten von Personendaten durch kantonale Organe beim Vollzug von Bundesrecht die Art. 1-11a, 16, 17, 18-22 und 25 Abs. 1-3 des Bundesgesetzes über den Datenschutz (DSG) vom 19. Juni 1992 (SR 235.1), soweit keine kantonalen Datenschutzvorschriften bestehen, die einen angemessenen Schutz gewährleisten (Art. 37 Abs. 1 DSG). Dabei ist zu beachten, dass das DSG lediglich den Schutz der Persönlichkeit und der Grundrechte von natürlichen und juristischen Personen, über die Daten bearbeitet werden, bezweckt, und nicht die Informationssicherheit zum Inhalt hat, soweit es dabei nicht um Personendaten geht (vgl. Art. 1 in Verbindung mit Art. 3 Bst. b DSG).

Kantonalrechtlich verweist § 13 Abs. 4 des Gesetzes über die Organisation des Regierungsrats und der kantonalen Verwaltung (Organisationsgesetz) vom 26. März 1985 (SAR 153.100) betreffend Bearbeitung, Archivierung und Schutz von Akten und Daten der kantonalen Verwaltung auf die Vorschriften des IDAG. Letzteres regelt die amtliche Information der Öffentlichkeit und den Zugang zu amtlichen Dokumenten, das Archivwesen sowie den Umgang mit Personendaten durch öffentliche Organe (§ 1 IDAG). Das IDAG stellt dabei lediglich den Schutz von Personendaten sicher, also von Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (vgl. § 1 Abs. 1 lit. b in Verbindung mit § 3 Abs. 1 lit. d IDAG), während die Schutzziele der Informationssicherheit (vgl. oben, Kapitel 2.3.1) für sämtliche Informationen gelten soll. Auch § 45 Abs. 4 des Gesetzes über die wirkungsorientierte Steuerung von Aufgaben und Finanzen (GAF) vom 5. Juni 2012 (SAR 612.300), nach welchem der Regierungsrat für alle Aufgabenbereiche Vorgaben zur Führung der Risikominimierung und des internen Kontrollsystems erlassen kann, stellt keine ausreichende Grundlage für den noch im Detail aufzuzeigenden Handlungsbedarf im Bereich der Informationssicherheit dar. Für diverse Massnahmen der Informationssicherheit fehlen weitestgehend die erforderlichen formell-gesetzlichen Grundlagen, namentlich für die Klassifizierung von Informationen, die Sicherheitseinstufung von Informatikmitteln, die Bezeichnung von Sicherheitszonen, den Einsatz von Informationssystemen zur zentralen Kontrolle von Identitäten, Personensicherheitsprüfungen (PSP), u.a. (vgl. Kapitel 4.2).

Statt in entsprechenden Rechtsgrundlagen finden sich verschiedene Vorgaben zur kantonalen Informationssicherheit in Dokumenten unterschiedlicher Art im Intranet des Kantons Aargau (Inka). Dabei werden einerseits spezifische Themen (z.B. sicherer E-Mail-Versand, Passwortrichtlinie und Authentisierungsverfahren) in Merkblättern, Richtlinien oder dergleichen festgehalten. Andererseits bildet die Informationssicherheitsstrategie des Kantons Aargau vom 2. September 2021 die Grundlage für das Informationssicherheitskonzept vom 6. April 2022 sowie weiterer Standards.

3.2 Rechtsvergleich

3.2.1 Bund

Das Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020 (SR 128) ist am 1. Januar 2024 in Kraft getreten. Es soll Lücken des geltenden Rechts schliessen und für alle Behörden und Organisationen des Bundes, Organisationen des öffentlichen Rechts, die kritische Infrastrukturen (KRITIS) betreiben (Art. 2 ISG) sowie für die Kantone gelten, sofern die Kantone klassifizierte Informationen des Bundes bearbeiten und sie auf Informatikmittel des Bundes zugreifen. Die Bestimmungen des ISG sollen nicht gelten, wenn die Kantone eine mindestens gleichwertige Informationssicherheit gewährleisten (Art. 3 Abs. 2 ISG). Das ISG soll die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, und den sicheren Einsatz der Informatikmittel des Bundes gewährleisten. Das ISG basiert auf anerkannten, in der Praxis erprobten internationalen Standards. Es legt dabei keine detaillierten Massnahmen zur Gewährleistung der Informationssicherheit fest, sondern schafft lediglich einen formell-gesetzlichen Rahmen, auf dessen Grundlage die jeweiligen Bundesbehörden auf Verordnungs- und Weisungsebene die Informationssicherheit konkretisieren werden. Das Gesetz regelt insbesondere

a) das Risikomanagement,

b) die Klassifizierung von Informationen,

c) die Sicherheit beim Einsatz von Informatikmitteln,

d) die personellen Massnahmen,

e) den physischen Schutz von Informationen und Informatikmitteln,

f) die Identitätsverwaltungs-Systeme (Identity and Access Management; IAM),

g) die Personensicherheitsprüfung,

h) die Betriebssicherheitsverfahren (Vergabe sicherheitsempfindlicher Aufträge an Externe),

i) den Betrieb kritischer Infrastrukturen sowie

j) die Organisation und den Vollzug.

Um ein möglichst einheitliches Sicherheitsniveau zu erreichen und die Kosten der Informationssicherheit zu senken, sollen die Anforderungen und Massnahmen standardisiert werden. Die Umsetzungskosten hängen weitgehend vom Sicherheitsniveau, das die Bundesbehörden erreichen wollen, und vom entsprechenden Ausführungsrecht ab.

Die Kantone müssen periodisch die Umsetzung und Wirksamkeit der Informationssicherheit nach Art. 3 ISG überprüfen (Art. 86 Abs. 1 ISG) und die Fachstelle des Bundes für Informationssicherheit über die Ergebnisse dieser Überprüfungen informieren (Art. 86 Abs. 2 ISG). Obwohl die Kantone demnach selbst für ihre Informationssicherheit zuständig bleiben, sollen die Kantone auf Instrumente und Fähigkeiten des Bundes zugreifen dürfen. Konkret werden Angestellte der Kantone, die sicherheitsempfindliche Tätigkeiten des Bundes ausüben, gestützt auf Art. 29 Abs. 1 Bst. b ISG sicherheitsüberprüft. Der Bundesrat legt fest, in welchen Fällen die Kantone die Leistungen der Fachstellen nach dem ISG für ihre eigene Informationssicherheit in Anspruch nehmen können und legt die Höhe der Gebühren für die entsprechenden Leistungen fest (Art. 86 Abs. 4 ISG).

Das ISG wurde am 18. Dezember 2020 in den Schlussabstimmungen von den Räten verabschiedet. Die Referendumsfrist lief am 10. April 2021 ab. Vom 12. Januar 2022 bis zum 14. April 2022 fand bereits die Vernehmlassung zur Änderung des ISG betreffend die Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen statt. Der Änderungsvorschlag stiess in der Vernehmlassung auf eine grosse Akzeptanz. Die Vorlage schafft die gesetzlichen Grundlagen zur Meldepflicht für Betreiberinnen und Betreiber kritischer Infrastrukturen und definiert die Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC), welches als zentrale Meldestelle für Cyberangriffe vorgesehen ist.

Vom 24. August 2024 bis zum 24. November 2022 führte der Bund die Vernehmlassung zum Ausführungsrecht zum Informationssicherheitsgesetz (ISG) durch. Der Bund hielt fest, für die Inkraftsetzung des ISG müssten drei Verordnungen erarbeitet und eine weitere Verordnung teilrevidiert werden:

- Verordnung über die Informationssicherheit bei der Bundesverwaltung und bei der Armee (Informationssicherheitsverordnung, ISV): Die neue ISV vereint, ergänzt und ersetzt mit der Cyberrisiken- und der Informationsschutzverordnung zwei bisherige Verordnungen. Die Verordnung regelt das Management der Informationssicherheit, den Schutz von klassifizierten Informationen, die Informatiksicherheit und die Massnahmen zur personellen und physischen Sicherheit. Die Bundesämter werden mit der ISV neu verpflichtet, ein Informationssicherheits-Managementsystem (ISMS) einzuführen.

Kantone sind von der ISV betroffen, wenn sie klassifizierte Informationen des Bundes bearbeiten oder auf Informatikmittel des Bundes zugreifen. Zumindest in diesen Fällen müssen sie die betreffenden Vorschriften einhalten oder eine mindestens gleichwertige Informationssicherheit gewährleisten;

- Verordnung über die Personensicherheitsprüfungen (VPSP): Diese fasst die Ausführungsbestimmungen zu den verschiedenen PSP zusammen. Diese Prüfungen sollen gemäss dem neuen Gesetz auf das Mindestmass reduziert werden, das zur Identifizierung von erheblichen Risiken für den Bund erforderlich ist. Damit sollen künftig deutlich weniger Prüfungen durchgeführt werden;
- Verordnung über das Betriebssicherheitsverfahren (VBSV): Sie regelt die Einzelheiten des durch das ISG eingeführten Betriebssicherheitsverfahrens. Das Verfahren wird durchgeführt, wenn die Bundesbehörden sicherheitsempfindliche Aufträge an Firmen vergeben. Die Vertrauenswürdigkeit dieser Firmen wird in Zusammenarbeit mit dem Nachrichtendienst des Bundes geprüft. Das BSV ist auf alle sicherheitsempfindlichen Aufträge anwendbar, die der Bund vergibt;
- Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV): Zusätzlich zu den drei neuen Verordnungen erfordert die Inkraftsetzung des ISG diverse Anpassungen der IAMV. Im gleichen Zug wird auch der Rahmen gesetzt, um künftig einen einheitlichen Login-Dienst für den Zugang zu Online-Diensten der Verwaltung aller föderalen Ebenen (E-Government) zur Verfügung zu stellen.

Das ISG mitsamt diesen Ausführungsverordnungen ist am 1. Januar 2024 in Kraft getreten.

3.2.2 Andere Kantone

Alle Kantone haben Regelungen auf verschiedenen Stufen (Verordnungen, Weisungen, u.a.). Anders als der Bund hat aber bisher noch kein Kanton ein Gesetz im formellen Sinn verabschiedet, das sich umfassend der Informationssicherheit widmet. Der Kanton Bern hat im ersten Quartal 2023 das Vernehmlassungsverfahren für ein neues Gesetz durchgeführt und der Regierungsrat hat im August 2023 die Botschaft an den Grossen Rat freigegeben. In anderen Kantonen finden sich vereinzelt in deren Datenschutzgesetzen, Informatikgesetzen oder in Gesetzen über die Digitale Verwaltung (E-Government-Gesetzgebung) Bestimmungen, welche als Grundlage für den Erlass von Verordnungen im Bereich der Informationssicherheit dienen (z.B. Basel-Landschaft, Basel-Stadt, St. Gallen und Zürich). Sofern die Informationssicherheit in den Kantonen in Erlassen geregelt wird, geschieht dies vornehmlich auf Verordnungsstufe. Entsprechende Verordnungen haben die Kantone Bern, Fribourg, Luzern, Schaffhausen, St. Gallen, Waadt, Zug und Zürich. Regelungsdichte und Regelungsinhalt dieser kantonalen Verordnungen unterscheiden sich jedoch stark. Alle diese Verordnungen regeln die Grundsätze für eine wirkungsvolle Informationssicherheit, insbesondere die Verantwortlichkeiten und Zuständigkeiten betreffend Risikoanalyse, sowie allgemein Fragen der Organisation und des Vollzugs der kantonalen Informationssicherheit. Nicht alle Kantone, die eine Verordnung erlassen haben, regeln darin beispielsweise ausdrücklich die Klassifizierung. Sofern eine Klassifizierung von Informationen vorgesehen ist, unterscheiden sich die Verordnungen ebenfalls stark. So sieht etwa der Kanton Luzern vor, dass Informationen hinsichtlich Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit zu klassifizieren sind, während der Kanton St. Gallen nur eine Klassifizierung seiner Informationen hinsichtlich Vertraulichkeit und Verfügbarkeit vorschreibt. Rechtliche Grundlagen für die PSP finden sich – soweit vorhanden – jeweils nicht in der Verordnung betreffend die Informationssicherheit, sondern in anderen Erlassen (z.B. Personalgesetz oder Polizeigesetz).

Der Rechtsvergleich mit den Kantonen zeigt, dass heute eine Tendenz zur spezialgesetzlichen Regelung der Informationssicherheit besteht.

4. Handlungsbedarf

Angesichts des beschriebenen digitalen Wandels und der damit zusammenhängenden Risiken stellt sich die Frage, inwiefern zur Gewährleistung der Informationssicherheit Regelungen in einem Gesetz im formellen Sinn erforderlich sind. Nachfolgend werden die wichtigsten Gründe hierfür aufgeführt.

4.1 Digitalisierung des Informationsaustausches und Vernetzung der Informatik

Zur Erfüllung ihrer verfassungsmässigen und gesetzlichen Aufgaben tauschen die Behörden des Kantons Informationen untereinander und mit Dritten aus. Sie stehen dabei in einem ständigen Dialog mit ihren öffentlichen und privaten Partnern und tauschen dabei Informationen aus, die Geschäfts- und Fabrikationsgeheimnisse Dritter beinhalten können. Dieser Informationsaustausch findet inzwischen zu einem wesentlichen Teil elektronisch statt. Gleichzeitig nimmt die Vernetzung der Informatiksysteme der kantonalen Behörden untereinander laufend zu. Die Systeme der verschiedenen Behörden weisen daher immer mehr gemeinsame Schnittstellen auf, wodurch sich das Risiko erhöht, dass sich Bedrohungen sowie Angriffe gegen eine Behörde auf die Zuständigkeitsbereiche anderer Behörden ausbreiten könnten. Werden Informationen auch ausserhalb einer Organisation bearbeitet oder von aussen hin auf Mittel der Informationstechnik zugegriffen, genügt der Schutz des eigenen Zuständigkeitsbereichs allein nicht mehr, weil die Schutzmassnahmen auch ausserhalb des eigenen Perimeters Wirkung erzielen müssen. Die Schutzmassnahmen müssen dem Schutzbedarf einer Information beziehungsweise des Informatikmittels entsprechend getroffen oder jenen auferlegt werden, die sie bearbeiten. Es ist deshalb unentbehrlich, dass die jeweils zuständigen Behörden verpflichtet werden, ihre personellen, organisatorischen, technischen und physischen Sicherheitsmassnahmen zum Schutz von Informationen und Informatikmitteln aufeinander abzustimmen. Gleichzeitig müssen Dritte, die Informationen des Kantons bearbeiten oder auf Mittel der kantonalen Informationstechnik zugreifen, die Sicherheitsvorgaben des Kantons erfüllen.

Die bestehenden gesetzlichen Grundlagen für die Informationssicherheit finden sich heute – meistens ohne ausdrückliche Erwähnung – verstreut in Einzelerlassen (vgl. Kapitel 3.1), die nur für bestimmte Behörden oder einen Teil der Informationen des Kantons gelten, zum Beispiel:

- § 13 Abs. 4 Organisationsgesetz verweist betreffend Bearbeitung, Archivierung und Schutz von Akten und Daten der kantonalen Verwaltung pauschal auf das IDAG. Für andere kantonale Behörden fehlt ein entsprechender Verweis.
- Gemäss geltendem Recht müssen lediglich Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, durch angemessene technische und organisatorische Massnahmen (sog. TOM) geschützt werden (§ 12 Abs. 1 IDAG).
- Die Klassifizierung von Informationen sowie die Sicherheit beim Einsatz von Informatikmitteln sind lediglich in der Form eines Standards der Informatikkonferenz (IK) festgelegt, der für die Departemente und die Staatskanzlei (SK) gilt, nicht aber für die anderen kantonalen Behörden. Diese sind heute grundsätzlich frei, ihre eigenen Klassifizierungsstufen festzulegen.
- Für die Behörden und insbesondere für kantonale Angestellte fehlen formell-gesetzliche Grundlage für die Personensicherheitsprüfung (PSP). Nur für gewisse Richterinnen und Richter findet sich in § 13 Abs. 9 des Gerichtsorganisationsgesetzes (GOG) vom 6. Dezember 2011 (SAR 155.200) eine gesetzliche Grundlage.
- Die Gewährleistung der Informationssicherheit erfolgt bei der Vergabe von sicherheitsrelevanten Aufträgen über die Auswahl geeigneter Unternehmen (Eignungsprüfung) im Rahmen des Vergabeverfahrens sowie über die Gestaltung der Verträge mit den Unternehmen, die mit der Ausführung von sensitiven Aufträgen betraut sind.

Der Geltungsbereich der Instrumente der Informationssicherheit muss alle Personen und Organisationen erfassen, die vom Kanton mit der Bearbeitung seiner Informationen oder mit dem Zugriff auf seine Informatiksysteme und -netze betraut sind. Nur so kann die erforderliche Sicherheit der Informationstechnik die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen gewährleistet werden.

4.2 Einschränkungen verfassungsmässiger Rechte und Bearbeitung von besonders schützenswerten Personendaten

Mit Massnahmen zur Risikominimierung in Bezug auf die Informationssicherheit können verfassungsmässige Rechte eingeschränkt und Personendaten tangiert werden. Insbesondere beim Einsatz von Informationssystemen zur zentralen Kontrolle von Identitäten kommt es zur Bearbeitung besonders schützenswerter Personendaten und ein Profiling kann nicht ausgeschlossen werden. Auch mit der Durchführung einer PSP kann ein erheblicher Eingriff in die Grundrechte privater natürlicher Personen verbunden sein[1]. Dasselbe gilt für die Klassifizierung von Informationen, die Sicherheitseinstufung von Informatikmitteln sowie die Bezeichnung von Sicherheitszonen, weil sie Voraussetzungen für die Durchführung einer PSP und daher für die Einschränkung der verfassungsmässigen Rechte massgebend sind.

Das Legalitätsprinzip verlangt, dass die wichtigsten Modalitäten eines Eingriffs in verfassungsmässige Rechte auf Gesetzesebene festgehalten werden.[2] Die von der Verfassung gewährleisteten grundlegenden Rechte des Einzelnen dürfen nur eingeschränkt werden, wenn dies in einer generell-abstrakten Norm vorgesehen ist (sog. Erfordernis des Rechtssatzes). Die grundlegenden Bestimmungen über die Einschränkungen verfassungsmässiger Rechte gehören in ein Gesetz im formellen Sinn (sog. Erfordernis der genügenden Normstufe; vgl. Art. 36 Abs. 1 zweiter Satz sowie Art. 164 Abs. 1 Bst. b der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 [SR 101; nachfolgend: BV] und § 8 Abs. 1, § 15 Abs. 2 sowie § 78 Abs. 1 der Verfassung des Kantons Aargau vom 25. Juni 1980 [SAR 110.000; nachfolgend: KV]). Je schwerer Einschränkungen sind, desto höher sind zudem die Anforderungen an die Bestimmtheit der Norm (sog. Erfordernis der genügenden Normdichte). Im Weiteren dürfen öffentliche Organe gemäss § 8 Abs. 2 IDAG besonders schützenswerte Personendaten grundsätzlich nur bearbeiten und ein Profiling nur durchführen, wenn ein Gesetz im formellen Sinn dies vorsieht oder dies für die Erfüllung einer klar umschriebenen gesetzlichen Aufgabe erforderlich ist. Formell-gesetzliche Grundlagen sind insbesondere nötig für:

4.3 Notwendigkeit eines systematischen und strukturierten Vorgehens

Der Kanton verfügt bereits heute über eine Informationssicherheits-Strategie. Deren Umsetzung hat durch Implementierung eines Informationssicherheits-Managementsystems (ISMS) zu erfolgen, da ansonsten grosse Risiken für die Informationssicherheit des Kantons bestehen.[3] Der Kanton Aargau verfügt zwar über ein ISMS, jedoch lässt sich dieses nicht auf eine hinreichende gesetzliche Grundlage abstützen. Eine solche bietet für kantonale Informationsbearbeitungen und -bestände – wie oben erwähnt – nur das IDAG und die VIDAG, welche einzelne Aspekte wie die periodische Überprüfung der TOM auf Zweck- und Verhältnismässigkeit vorschreibt. Das kantonale Datenschutzrecht fokussiert zudem einzig auf Personendaten und ist nur ausgerichtet auf den Zweck, die Persönlichkeit der betroffenen Personen zu schützen. Andere Schutzzwecke oder Kategorien von Informationen – namentlich solche, die sich auf den Kanton selbst oder juristische Personen beziehen – sind nicht erfasst.

[1] Vgl. [17.028] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953 ff., S. 2966 und 3038; Urteile des Bundesgerichts vom 6. November 2018 (1C_142/2018 und 1C_204/2018) Erw. 2.2.
[2] Vgl. [17.028] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953 ff., S. 3038.
[3] Vgl. SECORVO SECURITY CONSULTING GMBH (Hrsg.), Informationssicherheit und Datenschutz, Handbuch für Praktiker und Begleitbuch zum T.I.S.P., 3. Auflage, Heidelberg 2019, S. 1.

Zwar kann die Erstellung und der Betrieb eines ISMS (und damit verbunden auch eines Risikoinventars) im weitesten Sinne dadurch begründet und gerechtfertigt werden, dass dem Regierungsrat mit dem Organisationsgesetz die Schaffung einer "zweckmässigen Verwaltungsorganisation" übertragen wurde (§ 5 Abs. 1 Organisationsgesetz) und den Vorstehern der Departemente deren Leitung nach den Grundsätzen einer "rechtmässigen und rationellen Verwaltungsführung" obliegt (§ 29 Organisationsgesetz). Ein ISMS kann insofern als "Best Practice" im Bereich der Informationssicherheit und des Risiko-Managements betrachtet und daher vom Kanton schon heute verlangt werden. Jedoch sprechen drei wichtige Gründe dafür, dass die Grundzüge solcher Governance-Massnahmen gesetzlich ausdrücklich geregelt werden.

Erstens ist Informationssicherheit zu wichtig, als dass sich das Gemeinwesen darauf verlassen sollte, dass alle Teile der Verwaltung sie aus eigenem Antrieb in angemessener Weise sicherstellen – auch hinsichtlich der Governance ihrer Massnahmen und Restrisiken. Eine übergeordnete Informationssicherheitsstrategie ist zwar formuliert. Eine ausdrückliche rechtliche Grundlage, Investitionen zum Schutz der für den Kanton wichtigen Informationen tätigen zu können, besteht aber nur für den Bereich der Personendaten und nicht für Informationen generell.

Zweitens setzt ein angemessener Umgang mit Informationssicherheit nicht nur den Einsatz geeigneter technischer und organisatorischer Massnahmen der Informationssicherheit (TOM) voraus, sondern auch eine klare Zuweisung der Verantwortlichkeit für die Sicherstellung der Informationssicherheit. Primär sind die Behörden im Sinne von Kapitel 5 KV (Grosser Rat, Regierungsrat und Gerichte) für die Sicherstellung der Informationssicherheit in strategischer Hinsicht verantwortlich (oberste Führungsverantwortung). Ihnen wurden die Informationen anvertraut und sie tragen den Nutzen aus ihrer Verarbeitung, also kommt auch ihnen die entsprechende Verantwortung und damit die Rolle des Risikoträgers zu. Sie müssen auch über die mit der Implementation der TOM verbundenen Ausgaben und weiteren Folgen entscheiden und sie verantworten. Der Fachstelle für Informationssicherheit, der Informatik Aargau oder anderen Fachstellen, kommt hingegen die Verantwortung zu, für eine in operativer Hinsicht korrekte Umsetzung zu sorgen.

Drittens geht die Notwendigkeit aus der Tatsache hervor, dass im Rahmen einer gesetzlichen Regelung der wichtigsten Massnahmen der Informationssicherheit im selben Erlass auch geregelt wird, dass und wie diese TOM definiert, gesteuert, kontrolliert, aufrechterhalten und fortlaufend verbessert werden und wie mit den verbleibenden Restrisiken umzugehen ist.

4.4 Organisation

Die heutige Organisation der Informationssicherheit im Kanton Aargau (vgl. Kapitel 2.3.3) weist Lücken und Schwachstellen auf, zum Beispiel:

- Bereits heute verfügt die kantonale Verwaltung über ein aktuelles und durch die zuständigen Gremien verabschiedetes Normativ der Informationssicherheit, welches sich aus Informationssicherheitsstrategie, Informationssicherheitskonzept und verschiedenen Sicherheitsstandards zusammensetzt. Allerdings ist die Umsetzung noch nicht im notwendigen Mass fortgeschritten, was auf grosse Maturitätsunterschiede in den unterschiedlichen IT-Organisationseinheiten, fehlende Personalressourcen und Mangel an Spezialwissen zurückzuführen ist. In erster Priorität gilt es die offenen Positionen der informationssicherheitsbeauftragten Personen (ISBP) zu besetzen. Diese bilden in enger Zusammenarbeit mit dem CISO die Informationssicherheitsorganisation und betreiben und entwickeln das Informationssicherheits-Management-System (vgl. Abbildung 3).
- Die Weisungskompetenz des CISO beschränkt sich auf die Verwaltungseinheiten. Auf andere Behörden (Gerichte, Grosser Rat) und Organisationseinheiten (Gemeinden, Anstalten), welche die IT-Infrastruktur des Kantons nutzen, hat der CISO keine Möglichkeit einer massnahmenspezifischen Einflussnahme bei erkannter Sicherheitslücke oder bei einer Kompromittierung.

- Die operativen Vorgaben (Informationssicherheitskonzept, Standards etc.) für die Informationssicherheit werden durch den CISO und die Informatik Aargau ausgearbeitet und durch die IK, welche für den Erlass von interdepartementalen Vorgaben, Standards und Prozessen im Bereich der Informatik zuständig ist, in Kraft gesetzt. ist. Ihr wurde dieser Bereich vor Jahren zugewiesen, obwohl sich die Informationssicherheit nicht auf den Schutz von IKT-Mitteln beschränkt. Es fehlt folglich ein eigentliches – analog der IK für die Informatik – überdepartementales operatives, der Informationssicherheit dediziertes Gremium.
- Das Sicherheitsmanagement ist zu verbessern. Informationssicherheit wird weitgehend als technische Angelegenheit betrachtet. Demzufolge finden die geschäftsüblichen Führungstätigkeiten (z.B. Zielsetzung, Umsetzungskontrolle oder Wirksamkeitsprüfung) im Sicherheitsbereich nur selten Anwendung. Die Mitarbeitenden aller Stufen müssen kompetenter beraten, unterstützt und ausgebildet werden und auch sie sind bezüglich der Sicherstellung der Informationssicherheit in die Verantwortung zu nehmen.
- Das Sicherheitsbewusstsein (Führung und Mitarbeitende) ist zu wenig ausgeprägt. Die Ausbildungsmassnahmen erreichen die Personen, die sicherheitsempfindliche Aufgaben erfüllen, häufig nicht. Die angebotenen Schulungen finden auf freiwilliger Basis statt und werden kaum besucht.
- Die Kosten und prozentualen Anteile der Informationssicherheit an den gesamten IT-Kosten werden mehrheitlich nicht transparent dargelegt und nicht systematisch erhoben. Dies erschwert die Beurteilung der Wirtschaftlichkeit der Massnahmen und Vergleiche mit Industrie-Standards und vergleichbarer Organisationen.
- In Krisenfällen besteht nur eine ungenügend definierte Organisation, die sich darüber hinaus erst noch im Aufbau befindet. Die Informationssicherheit ist heute im Kantonalen Führungsstab (KFS) noch nicht etabliert, beispielsweise ist der CISO nicht eingebunden und Cyber-Vorfälle werden nicht regelmässig geübt.
- Es besteht heute keine über die Grenzen der Kantonsverwaltung hinausgehende Cyber-Organisation. Der diesbezügliche Handlungsbedarf wird nachstehend im Kapitel 5.2.4.2 beschrieben.

Die heutige Organisation wuchs aus sektoriellen fachlichen Bedürfnissen. Sie lieferte und liefert heute immer noch genügend Resultate. Mit der fortschreitenden Entwicklung zu einer Informationsgesellschaft wurden aber die Bedrohungen für Informationen und IKT-Mittel komplexer und dynamischer. Ihnen muss integral und professionell begegnet werden, was entsprechende rechtliche und organisatorische Vorkehrungen sowie erhöhtes Fachwissen und -kompetenz voraussetzt. Die Organisation des Kantons ist diesen Anforderungen anzupassen. Es müssen aber auch genügend Ressourcen zur Verfügung gestellt werden, um die Herausforderungen der dargelegten Entwicklung gewärtigen zu können.

Der Blick auf andere Kantone zeigt, dass kleinere Kantone ihre Informatik in einer öffentlich-rechtlichen Anstalt zusammengelegt (NW, OW, SH) oder in einer spezialgesetzlichen Aktiengesellschaft ausgelagert haben (AR). Zum Teil befasst sich der Datenschutzbeauftragte mit der Informationssicherheit, sofern es sich um Personendaten handelt (BE, FR) oder das Amt für Informatik übernimmt diese Aufgabe (VD). Fünf Kantone sehen in ihren Erlassen ausdrücklich einen CISO (BS, BL, GR, LU, SG, ZH) oder ein entsprechendes Gremium vor (LU, ZG), welches sich der Informationssicherheit widmet. Inwiefern die Rolle des oder der Informatikbeauftragen von der Rolle der oder des Informationssicherheitsbeauftragten auch in personeller Hinsicht getrennt wird, ergibt sich aus den kantonalen Erlassen nicht. Einzig für den Kanton Zürich lässt sich festhalten, dass dieser die beiden Rollen auch in personeller Hinsicht vollständig trennt und dafür neue Stellen geschaffen hat, damit die Umsetzung und anschliessende Kontrolle betreffend Informationssicherheit zukünftig nicht mehr

von derselben Person vorgenommen wird.[4] Der Kanton Zürich hat im Jahr 2021 für das kantonale Zentrum für Cybersicherheit 18 zusätzliche Stellen bewilligt.

4.5 Postulat der FDP-Fraktion vom 18. Januar 2022 betreffend Cyberkriminalität (GR.22.29)

Mit Ausnahme des Postulats der FDP-Fraktion vom 18. Januar 2022 betreffend Cyberkriminalität (GR.22.29), welches der Regierungsrat mit Erklärung entgegengenommen hat, sind die politischen Vorstösse im Themenfeld der vorliegenden Gesetzesvorlage erledigt (vgl. Kapitel 2.4).

Das offene Postulat (GR.22.29) verlangt zum einen die Prüfung, "ob die derzeitigen gesetzlichen Grundlagen für einen umfassenden Schutz durch Angriffe aus dem Cyberraum ausreichen", zum andern sollen folgender Punkte überprüft werden:

- Aufbau und Einrichtung einer kantonalen Organisation für Cybersicherheit
- Meldepflicht für von Cybercrime betroffene Gemeinden, Unternehmen, inklusive Institutionen mit öffentlichen Aufträgen, respektive in öffentlicher Hand
- Vernetzung zwischen den verschiedenen staatlichen und privaten Akteuren
- Verstärkte Schulung aller Mitarbeiter und Mitarbeiterinnen von staatlichen Organisationen

Das Postulat verweist in der Begründung auf die Empfehlungen SVS. Nachfolgend wird unter dem Aspekt des Handlungsbedarfs auf die zur Prüfung angeregten Punkte eingegangen.

4.5.1 Rechtliche Grundlagen für eine umfassende Abwehr von Cyberangriffen

Hauptsächlich wollen die Postulanten wissen, ob die derzeitigen gesetzlichen Grundlagen für einen umfassenden Schutz durch Angriffe aus dem Cyberraum ausreichen. Diese Frage kann nicht einfach beantwortet werden, da unklar ist, was beziehungsweise wer damit konkret gemeint ist. Wer soll gegen Angriffe aus dem Cyberraum durch gesetzliche Grundlagen umfassend geschützt sein? Sofern damit der strafrechtliche Schutz gegen Cyberangriffe generell gemeint ist, ist für die Schaffung neuer Strafbestimmungen nicht der Kanton zuständig, sondern der Bund. Sofern sich die Frage darauf bezieht, ob die gesetzlichen Grundlagen zur Sicherstellung der Cybersicherheit als Teilbereich der Informationssicherheit des Gemeinwesens Kanton Aargau ausreichen, ist diese Frage aufgrund der in den Kapiteln 4.2 und 5.1 aufgeführten Gründe zu verneinen. Es besteht diesbezüglich Handlungsbedarf, dem durch Schaffung des Gesetzes Rechnung getragen wird.

4.5.2 Aufbau und Einrichtung einer kantonalen Organisation für Cybersicherheit

Im Kanton Aargau besteht heute insofern eine kantonale Organisation, die sich mit Informationssicherheit beschäftigt, als die Cybersicherheit des Gemeinwesens "Kanton" zur Informationssicherheit gehört und innerhalb der im Kapitel 2.3.3 dargestellten Organisation gewährleistet wird. Demgegenüber obliegen die Aufgaben im Bereich der Bekämpfung der Cyberkriminalität der Kantonspolizei und der Staatsanwaltschaft. Der Handlungsbedarf in Bezug auf eine kantonale Cyber-Organisation ergibt sich einerseits aus dem allgemeinen Bedarf an einer möglichst wirksamen, risikominimierungsorientierten Organisation der Informationssicherheit insgesamt und zum anderen aus den im Postulat erwähnten Empfehlungen SVS. Die neue Organisation der Informationssicherheit wird im Umsetzungsvorschlag umschrieben (Kap. 5.2.4.2) und in den Ausführungen zu den §§ 25-29 (Kap. 7.5) detailliert erläutert.

[4] Vgl. Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich, Sitzung vom 2. Dezember 2020, Regierungsratsbeschluss Nr. 1193/2020: Informationssicherheit, Umsetzung in den Direktionen und der Staatskanzlei (Stellenpläne, gebundene Ausgabe) (abrufbar unter: www.zh.ch / Politik & Staat / Gesetze & Beschlüsse / Beschlüsse des Regierungsrats; zuletzt besucht am: 9. Juni 2022).

4.5.3 Meldepflicht für von Cybercrime betroffene Gemeinden, Unternehmen, inklusive Institutionen mit öffentlichen Aufträgen beziehungsweise solche in öffentlicher Hand

Nachdem der Bundesgesetzgeber mit der Änderung des ISG zu den geplanten Massnahmen des Bundes zum Schutz der Schweiz vor Cyberbedrohungen die Pflicht zur Meldung von Cyberangriffen (Art. 74a ff. ISG) beschlossen hat (BBl 2023 2296), besteht diesbezüglich kein Handlungsbedarf mehr. Die meldepflichtigen Behörden und Organisationen werden durch Umschreibung der sicherheitsrelevanten Bereiche definiert. Meldepflichtig sind Behörden aller föderalen Ebenen, die Hochschulen und kritischen Infrastrukturen der verschiedensten Bereiche wie Sicherheit und Rettung, Trinkwasserversorgung, Abwasserversorgung, Abfallentsorgung, Energieversorgung, -handel, -messung und -steuerung, Banken, Versicherungen und Finanzmarktinfrastrukturen, Gesundheitseinrichtungen sowie weitere Bereiche (vgl. Kap. 5.2.3.2).

4.5.4 Vernetzung zwischen den verschiedenen staatlichen und privaten Akteuren

Auch für diesen Punkt besteht Handlungsbedarf. Mit dem Aufbau der verwaltungsübergreifenden kantonalen Cyber-Organisation ist das Augenmerk auch auf die Vernetzung zwischen den staatlichen und privaten Akteuren zu richten. Es sei diesbezüglich auf die Ausführungen in Kapitel 5.2.4.2 und auf die Erläuterungen zur kantonalen Cyber-Organisation (§§ 26-29; Kap. 7.5.2) verwiesen.

4.5.5 Verstärkte Schulung der Mitarbeiterinnen und Mitarbeiter von staatlichen Organisationen

Die stufengerechte Aus- und Weiterbildung ist eine personelle Massnahme im Hinblick auf die Sicherstellung der Informationssicherheit insgesamt. Eine gezieltere Schulung in Cybersicherheit ist hiervon mitumfasst. Die Aus- und Weiterbildung von Mitarbeitenden im Bereich der Informationssicherheit gehört ihrerseits zum Informationssicherheitsmanagement der zuständigen Behörden und ist daher grundsätzlich mit den im Gesetzesentwurf vorgesehenen Absichten abgedeckt. Mit § 17 des Gesetzesentwurfs wird die Wichtigkeit der Aus- und Weiterbildung der Mitarbeitenden unterstrichen, indem festgeschrieben werden soll, dass die verantwortlichen Behörden für eine sorgfältige Auswahl sowie eine stufengerechte Aus- und Weiterbildung der Mitarbeitenden sorgen müssen, die Zugang zu klassifizierten Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen haben (vgl. Kap. 7.4.4.1). Soweit die Postulanten die Überprüfung betreffend eine "verstärkte Schulung aller Mitarbeiter und Mitarbeiterinnen von staatlichen Organisationen" fordern, ist vorab darauf hinzuweisen, dass in den Empfehlungen SVS lediglich die Schulung für alle Mitarbeitenden der Verwaltung als Ziel genannt wird (vgl. Empfehlungen SVS, S. 11). Es ist aber vorgesehen, dass im Aufgabenportfolio der Cyber-Koordinatorin beziehungsweise des Cyber-Koordinators auch die Erstellung von Ausbildungsunterlagen wie auch die Durchführung von Schulungen enthalten sind (§ 28 Abs. 1 lit. h; Kap. 7.5.2.3).

5. Umsetzung

5.1 Schaffung gesetzlicher Grundlagen

5.1.1 Gesetzesstufe

Die Notwendigkeit der Schaffung eines Gesetzes für die Informationssicherheit ergibt sich aus der Verfassung. Gemäss § 78 Abs. 1 KV erlässt der Grosse Rat in der Form des Gesetzes "alle wichtigen Bestimmungen". Aus diesem demokratischen Aspekt ergibt sich, dass die Stimmberechtigten mittelbar oder unmittelbar an den für sie besonders wichtigen Regelungen mitwirken können sollen. Aufgrund der Bedeutung, die der Informationssicherheit in der Zwischenzeit und angesichts der fortschreitenden digitalen Entwicklung in der Gesellschaft zukommt, und angesichts der latenten Risiken für die öffentliche Sicherheit, ist es zentral, dass die Informationssicherheit als öffentliche Aufgabe und deren Grundsätze gesetzlich normiert werden. Wie unter Kapitel 4.2 bereits ausgeführt, dürfen die von der Verfassung gewährleisteten grundlegenden Rechte des Einzelnen nur eingeschränkt werden, wenn dies in einer generell-abstrakten Norm vorgesehen ist (sog. Erfordernis des

Rechtssatzes). Die grundlegenden Bestimmungen über die Einschränkungen verfassungsmässiger Rechte gehören somit in ein Gesetz im formellen Sinn. Verschiedene für die Gewährleistung der Informationssicherheit notwendige technische und organisatorische Massnahmen können in Grundrechte eingreifen. Die entsprechenden Normen bedürfen folglich einer Regelung auf Gesetzesstufe. Es ist auch zu beachten, dass die Bestimmungen Elemente der Leistungs- und Eingriffsverwaltung[5] enthalten. Soweit es sich um Leistungsverwaltung handelt, dienen sie auch der Gewährleistung der Sicherheit von erheblichen Investitionen. Es handelt sich demnach zweifellos um wichtige Bestimmungen im Sinne von § 78 Abs. 1 KV. Schliesslich müssen auch die Grundzüge und Grundsätze (ohne Rahmen keine Verordnung) in einem formellen Gesetz normiert werden, erst recht, wenn damit Eingriffe in Grundrechte verbunden sind.

Auch dürfen die Bedeutung und die Wirkung der Schaffung gesetzlicher Grundlagen auf die Gemeinden und die Bevölkerung nicht unterschätzt werden. Ein Gesetz richtet den Fokus auf ein bestimmtes, aktuelles Thema und kann die Informationssicherheit stärker und besser ins Bewusstsein der potenziell Betroffenen rufen. Für die Gemeinden bedeutet es aufgrund des Geltungsbereichs, dass sie einen Mindeststandard an Informationssicherheit gewährleisten müssen im Umgang mit klassifizierten Informationen des Kantons und mit gemeinsam genutzten Applikationen, um den Erfordernissen des Gesetzes zu genügen. Dies wird Ansporn bieten, um ihrerseits im Rahmen ihrer Autonomie für eine angemessene Informationssicherheit zu sorgen und eventuell auch Kooperationen mit anderen Gemeinden einzugehen. Der Bevölkerung wird damit aufgezeigt, dass Informationssicherheit nicht eine Geheimdisziplin der Verwaltung ist, sondern dass es darum geht, auch ihre Informationen, welche die Verwaltung in physischer oder elektronischer Form erhalten hat und bearbeitet, zu schützen. Zudem erreicht man damit in weiten Teilen der Bevölkerung eine Sensibilisierung in Bezug auf das Thema Informationssicherheit, was per se ein künftig noch stärker zu verfolgendes Ziel sein wird.

Durch die Schaffung einer gesetzlichen Grundlage wird die Informationssicherheit zur öffentlichen Aufgabe, was dem Regierungsrat künftig ermöglichen wird, gestützt auf § 9a des Gesetzes über die Organisation des Regierungsrates und der kantonalen Verwaltung (Organisationsgesetz) vom 26. März 1985 (SAR 153.100) Beteiligungen oder Kooperationen an beziehungsweise mit Unternehmungen einzugehen. Solche Formen des Zusammenwirkens können künftig durchaus in Betracht kommen, um das in der Privatwirtschaft vorhandene Know-how nicht nur einzukaufen, sondern vielmehr um an der Wissensgenerierung beteiligt zu sein und diese zu fördern. Ohne Schaffung einer gesetzlichen Grundlage sind solche Beteiligungen und Kooperationen nicht möglich, weil sie der Erfüllung öffentlicher Aufgaben vorbehalten sind.

5.1.2 Prüfung Integration in bestehende Erlasse

Wie aus dem Handlungsbedarf hervorgeht, sind für diverse Themen der Informationssicherheit Grundlagen in einem Gesetz im formellen Sinn erforderlich. Im Rahmen der Erarbeitung des Normkonzepts wurden bestehende Erlasse (IDAG, OG, GOG, GVG) einer näheren Prüfung hinsichtlich Anpassung unterzogen, zumal a priori nicht ein neues Gesetz geschaffen werden sollte, solange eine Anpassung bestehender Erlasse in Betracht kommt. Dabei muss jeweils das Augenmerk auch speziell auf die Regelungsdichte gerichtet werden, so dass vor allem die Grundzüge einer Neuregelung in die Gesetzesform fliessen sollen. Eine normative "Überladung" soll vermieden werden. In diesem Sinne wurden die rechtsetzerischen Möglichkeiten durchleuchtet und geprüft, ob die neuen Normen zur Informationssicherheit in bestehende Erlasse integriert werden sollen oder ob die Schaffung eines neuen Gesetzes angezeigt ist.

Die Rechtsgrundlagen des Kantons zum Schutz von Informationen sind sektoriell ausgeprägt, kaum aufeinander abgestimmt und lückenhaft. Dies erschwert die Steuerung von politischen und

[5] Leistungsverwaltung nennt man jene Verwaltungstätigkeit, durch die den Privaten staatliche Leistungen, insbesondere wirtschaftliche und soziale Leistungen vermittelt werden (z.B. Sozialversicherungen, Fürsorge, Förderung der Landwirtschaft); Eingriffsverwaltung nennt man jene Verwaltungstätigkeit, die in die Rechte und Freiheiten der Privaten eingreift. Die Eingriffsverwaltung ist in der Regel hoheitlicher Natur (z.B. baupolizeiliche Einschränkungen, Enteignung, Einziehen von gesundheitsgefährdenden Stoffen) [HÄFELIN / MÜLLER / UHLMANN, Allgemeines Verwaltungsrecht, 7. A., Zürich 2015, Rz. 33 ff.]

operativen Geschäften, die einen Bezug zum Schutz von Informationen haben. Da die Zuständigkeiten je nach Fachgebiet geteilt sind, nimmt der Koordinationsaufwand immer mehr zu. Deshalb erscheint es angezeigt, dass alle Massnahmen, die der Kanton zum Schutz von Informationen treffen muss, in einem einzigen Erlass geregelt werden. Dieser integrale Ansatz entspricht auch den internationalen Standards. Auch in der Schweiz zeigt sich eine klare Tendenz zu diesem integralen Ansatz. Der Bund hat mit dem ISG bereits einen solchen Einheitserlass geschaffen und der Kanton Bern befinden sich derzeit in einem entsprechenden Rechtsetzungsprozess.

Geprüft wurde insbesondere eine Integration in das IDAG. Dies erscheint zwar auf den ersten Blick naheliegend, weisen doch die Klassifizierung von Informationen, die Sicherheit beim Einsatz von Informatikmitteln, der physische Schutz von Informationen und Informatikmitteln sowie die eingesetzten Identitätsverwaltungssysteme eine gewisse sachliche Nähe zu den im IDAG geregelten Themen des Datenschutzes auf. Diesen Gemeinsamkeiten stehen aber auch konzeptionelle Unterschiede gegenüber. Die Datenschutzgesetzgebung ist im Verhältnis zu den Regelungen zur Informationssicherheit als Spezialgesetzgebung zu betrachten und weist einen sachlich engeren Regelungsbereich auf (Umgang mit Personendaten, nicht Informationen generell). Es werden nicht Daten geschützt, sondern die Grundrechte beziehungsweise die Persönlichkeit von Personen, deren Daten bearbeitet werden. Der Schutz der Persönlichkeit zielt dabei primär auf das Datenbearbeiten durch Private ab, der Schutz der Grundrechte auf den Schutz vor Eingriffen durch staatliche Behörden. Das Datenschutzrecht ergänzt und konkretisiert somit einerseits den verfassungsmässigen Schutz der informationellen Selbstbestimmung (Art. 13 Abs. 2 BV), andererseits den bereits durch das Zivilgesetzbuch (Art. 28 ZGB) gewährleisteten Schutz der Persönlichkeit. Es ist daher wesentlich, den Datenschutz von der Informationssicherheit, die den Staat vor ungesetzlichem Stören seines Handelns schützen soll, klar abzugrenzen. Eine Integration der Normen betreffend die Informationssicherheit in das bestehende IDAG würde sich daher kompliziert gestalten beziehungsweise würde mutmasslich gar eine Totalrevision dieses Erlasses erfordern. Aus denselben Gründen lehnt nicht zuletzt auch die ÖDB eine Regelung im IDAG ab, denn ihres Erachtens brächte die Kombination von Regelungen des Umgangs mit Personendaten und nicht personenbezogenen Daten das IDAG aus dem Lot und würde eher zur Unübersichtlichkeit des Erlasses führen als zur harmonischen Zusammenführung der beiden Themenbereiche. Dass es eines Zusammenspiels der beiden Bereiche bedarf, um einen ganzheitlichen Schutz zu gewähren, ist unbestritten. Dies kann aber besser erreicht werden, wenn man die konzeptionellen Unterschiede der beiden Bereiche als solche erkennt und dementsprechend rechtsetzerisch umsetzt.

Geprüft wurde ferner die Ergänzung beziehungsweise Änderung anderer bestehender Gesetze (GVG; Organisationsgesetz; GOG; Dekret über das öffentliche Beschaffungswesen [DöB] vom 23. März 2021 [SAR 150.920]; Gesetz über die Grundzüge des Personalrechts [Personalgesetz, PersG] vom 16. Mai 2000 [SAR 165.100]). Auch diese Lösung hätte den Vorteil gehabt, dass auf die Schaffung eines neuen Gesetzes hätte verzichtet werden können. Sie hätte aber auch entscheidende Nachteile. Alle anzupassenden Gesetze verfügen über unterschiedliche Geltungsbereiche, was einen nach einem integralen Ansatz gesteuerten Vollzug praktisch verhindern würde. Die erkannten Lücken könnten somit – wenn überhaupt – nur mit einem unverhältnismässig grossen Koordinationsaufwand geschlossen werden. Eine solche Lösung würde faktisch auch die erforderliche behördenübergreifende Anwendung einheitlicher Kriterien und Massnahmen zumindest erschweren, wenn nicht gar verhindern. Weiter ist zu beachten, dass es sich bei den Massnahmen der Informationssicherheit um sehr spezifische Massnahmen handelt und deren Umsetzung von den Regelungen betreffend Klassifizierung, Einstufung von Informatikmitteln und Schutzzonen abhängt. Eine Normierung von Massnahmen der Informationssicherheit in verschiedenen Erlassen würde dazu führen, dass neue Zuständigkeiten und Verantwortlichkeiten definiert werden müssten, was den Koordinationsaufwand sowohl rechtlich als auch organisatorisch beträchtlich erhöhen würde.

5.1.3 Einheitliches Regelwerk

Mit dem neu zu schaffenden Gesetz soll die Grundlage für ein einheitliches Regelwerk zur Steuerung und Führung der Informationssicherheit des Kantons Aargau geschaffen werden. Dieses erstreckt sich von der generell-abstrakten Ebene des Gesetzes, über Ausführungsbestimmungen in einer Verordnung bis hin zu Weisungen, technischen Standards und anderen verbindlichen Vorgaben. Das vom InfoSiG angeführte neue Regelwerk soll dabei als einheitliche Rechtsgrundlage den Neuerungen, Besonderheiten und spezifischen Anpassungsbedürfnissen der Informationssicherheit Rechnung tragen. Aufgrund dessen soll in inhaltlicher Hinsicht auf gesetzlicher Stufe die Informationssicherheit in Form von Grundsätzen geregelt werden. Damit kann nicht nur den unterschiedlichen Bedürfnissen besser Rechnung getragen, vielmehr kann dadurch auch rascher auf Entwicklungen und neue Bedrohungen reagiert werden. Um einen einheitlichen Vollzug zu gewährleisten unter Berücksichtigung der Vollzugsautonomie der Behörden sind folgende Regeln zu beachten:

- **"Opting-out"-Regelung:** Jede Behörde vollzieht in ihrem Bereich den Erlass selbständig und erlässt entsprechendes Ausführungsrecht. Das Vollzugsrecht des Regierungsrats gilt jedoch für die übrigen Behörden sinngemäss, solange sie keine eigenen Regelungen erlassen.
- **Standards:** Der Regierungsrat soll ermächtigt werden, standardisierte Anforderungen und Massnahmen nach dem Stand von Wissenschaft und Technik festzulegen, die für die anderen Behörden als Empfehlungen gelten. Dabei handelt es sich nicht um grundsätzliche Organisationsfragen, sondern um untergeordnete Prozesse, Mittel und Dienstleistungen (Erhebung des Schutzbedarfs von Informationen, Methoden für die Risikobeurteilung, Verschlüsselung usw.). Damit soll ein einheitliches Sicherheitsniveau erreicht werden, es sollen aber auch die Projekt- und Umsetzungskosten reduziert werden. Der Regierungsrat soll die Möglichkeit haben, die Festlegung an kompetente Fachorgane, insbesondere an die Fachstelle für Informationssicherheit (vgl. Erläuterungen zu § 25, Kap. 7.5.5.1) zu delegieren.

Mit einer solchen Lösung wird die Unabhängigkeit der Behörden beim Vollzug gewahrt. Dieser erfolgt dezentral. Das angestrebte einheitliche Sicherheitsniveau wird durch eine einheitliche Doktrin, durch die Erarbeitung von Standards sowie durch die professionelle Unterstützung von Fachorganen erreicht. Zu beachten ist, dass hiermit hauptsächlich der behördenübergreifende Rahmen normiert wird, während für den Vollzug in der kantonalen Verwaltung allein der Regierungsrat zuständig ist.

Die Unabhängigkeit der Behörden wird jedoch gemäss dem vorgeschlagenen Gesetzesentwurf in einem Punkt tangiert. Es ist für die einheitliche und konsequente Durchsetzung der Informationssicherheit von essentieller Wichtigkeit, dass dem CISO beziehungsweise künftig der Fachstelle für Informationssicherheit die Möglichkeit gegeben ist, über die Behördengrenzen hinaus unaufgefordert Überprüfungen vorzunehmen, ob die Vorgaben der Informationssicherheit eingehalten sind und bei Nichteinhaltung und erkannter Sicherheitslücke entsprechende Massnahmen zu beantragen (§ 25 Abs. 1 lit. c; Kap. 7.5.1.1). Ohne dieses Weisungs- und Durchgriffsrecht der Fachstelle für Informationssicherheit ist eine wirkungsvolle Kontrolle des Vollzugs nicht gegeben. Das Risiko für die Informationssicherheit wäre erheblich, zumal Cyber-Angreifer nicht vor Departements- oder Behördengrenzen Halt machen. Eine Kompromittierung eines Systems einer Behörde hat aufgrund der heutigen Vernetzung die Kompromittierung der Systeme der gesamten oder zumindest eines Grossteils der Verwaltung zur Folge. Oder anders ausgedrückt, wird eine Behörde, die sich nicht an die Sicherheitsvorgaben hält, unweigerlich zum Einfallstor für einen Angriff auch auf die Systeme der übrigen Verwaltung.

Die Informationssicherheit soll den groben Zügen nach in normativer Hinsicht künftig wie folgt aufgebaut sein:

Abbildung 5: Aufbau künftige Informationssicherheit Kanton Aargau.

5.2 Neuer Erlass

5.2.1 Allgemeine Bemerkungen

Da es sich um einen neuen Erlass handelt, besteht die Umsetzung darin, einen vollständigen Gesetzestext zu schaffen. Dabei war es auch ein klares Ziel, eine möglichst tiefe Regelungsdichte zu erzielen. Nachfolgend wird lediglich zum Zweck der Übersichtsgewinnung die Struktur des Erlasses (Kap. 5.2.2) aufgeführt, woraus die wesentlichen Themen der Informationssicherheit erkennbar sind. Nicht erkennbar ist hingegen, auf welche Themen im Rahmen der rechtsetzerischen Auseinandersetzung ausdrücklich verzichtet wurde (Kap. 5.2.3). Dabei geht es um Themen, die im Normkonzept noch als möglicher Gesetzesinhalt betrachtet wurden.

5.2.2 Erlassstruktur

Nebst dem Auftrag, ein Gesetz zu schaffen, dass technologieneutral die Grundzüge der Informationssicherheit beinhaltet, die es den Behörden ermöglichen sollen, technische und organisatorische Ausführungsbestimmungen zu erlassen, bestand das Ziel auch darin, auf einer klaren Gesetzessystematik aufbauen zu können. Dieses klare Grundgerüst des Gesetzes sieht wie folgt aus:

1. Allgemeine Bestimmungen
2. Führung und allgemeine Massnahmen
   - 2.1 Führung
   - 2.2 Allgemeine Massnahmen
     - 2.2.1 Informationssicherheits-Risikomanagement
     - 2.2.2 Vorgehen bei Verletzungen der Informationssicherheit und Prävention
     - 2.2.3 Klassifizierung
     - 2.2.4 Vertragliche Überbindung und Kontrolle
3. Technische und organisatorische Massnahmen (TOM)
   - 3.1 Sicherheit beim Einsatz von Informatikmitteln
   - 3.2 Physische Massnahmen
   - 3.3 Identitäts- und Zugriffsmanagement
   - 3.4 Personelle Massnahmen
     - 3.4.1 Auswahl, Instruktion und Berechtigungen
     - 3.4.2 Personensicherheitsprüfung (PSP)
   - 3.5 Sicherheitsspezifische vergaberechtliche Eignungsprüfung

4. Organisation
   4.1 Verwaltungsinterne Organisation
   4.2 Verwaltungsübergreifende Organisation
5. Vollzug
6. Schlussbestimmungen

5.2.3 Nicht aufgenommene Themen

5.2.3.1 Betriebssicherheitsverfahren

Der Bund sieht im ISG ein Verfahren vor, wonach bei der Vergabe von sicherheitsempfindlichen Aufträgen die Behörden dafür sorgen müssen, dass nur Unternehmen öffentliche Aufträge erhalten, welche befähigt sind, die Informationssicherheit zu gewährleisten. Das Verfahren soll einerseits der Prüfung der Vertrauenswürdigkeit der zu beauftragenden Betriebe dienen. Andererseits soll es ermöglichen, die notwendigen Massnahmen zur Wahrung der Informationssicherheit während der Ausführung von sicherheitsempfindlichen Aufträgen zu kontrollieren und durchzusetzen. Das Verfahren darf nur mit Einwilligung des Betriebs durchgeführt werden. Die erforderliche Zustimmung der betroffenen Betriebe stellt gemeinhin kein Problem dar, weil diese ein finanzielles Interesse an der Auftragserteilung haben. Der Bund hat in Aussicht gestellt, dass die Kantone auf die Leistungen des Bundes zurückgreifen können. Die Durchführung der Betriebssicherheitsverfahren würde diesfalls durch die Fachstelle des Bundes auf Antrag der zuständigen kantonalen Behörde erfolgen. Von einem solchen Leistungsbezug und folglich von einer Normierung im Gesetz, in welchen Fällen ein Betriebssicherheitsverfahren beim Bund von wem zwingend eingeleitet werden müsste, soll jedoch aus nachfolgenden Gründen abgesehen werden.

Der Bund hat im August 2022 einen Vorentwurf zur Verordnung über das Betriebssicherheitsverfahren (VBSV) in die Vernehmlassung gegeben. Daraus ging hervor, wie die Datenerhebung (Art. 9) erfolgen soll und welche Daten erhoben werden sollen. Gemäss Art. 9 Abs. 3 VBSV wird lediglich eine Selbstdeklaration der Betriebe eingefordert, die "wahrheitsgemäss Auskunft erteilen" müssen. Dabei geht es (nicht abschliessend) um Daten über die Eigentumsverhältnisse, die Zusammensetzung der Unternehmensführung, allfällige Interessenbindungen des obersten Kaders und von Mitgliedern der Unternehmensführung, die Solvenz, die Bezahlung der Steuern und Sozialabgaben, Referenzen aus früheren Beschaffungsverfahren. Es stellt sich hier die Frage, welcher Mehrwert gegenüber der Eignungsprüfung im Rahmen des Vergabeverfahrens besteht, zumal die Befähigung zur Gewährleistung von Informationssicherheit und Datenschutz bereits heute im Rahmen der Eignungsprüfung durch die Vergabestellen geprüft wird. Der vom Bund betriebene Aufwand erscheint als nicht verhältnismässig in Relation zum Resultat, zumal dasselbe Ergebnis ohne weiteres im Vergabeverfahren erzielt werden kann. Dies aber mit dem entscheidenden Vorteil, dass keine Sistierung des Vergabeverfahrens notwendig ist, weil die Prüfung durch eine Bundesstelle ausserhalb des Vergabeverfahrens vorzunehmen ist. Danach müsste das Resultat wieder ins Vergabeverfahren eingespeist werden und die Vergabestelle hätte bei entsprechendem Resultat der Prüfung den Ausschluss eines oder mehrerer Unternehmen zu verfügen. Es muss davon ausgegangen werden, dass die Vergabeverfahren dadurch tendenziell länger würden, was in vergaberechtlicher Hinsicht nicht anzustreben ist. Vielmehr soll neu gesetzlich eine Verpflichtung zur spezifischen Eignungsprüfung bei sicherheitsrelevanten Vergaben öffentlicher Aufträge, aber auch bei der Übertragung von öffentlichen Aufgaben an Private, die in aller Regel ebenfalls nach vergaberechtlichen Kriterien erfolgt, statuiert werden (vgl. § 24 und die Erläuterungen in Kap. 7.4.5.1). In diesen Fällen muss die Informationssicherheit zwingend berücksichtigt werden und darf nicht dem Ermessen der Vergabestellen anheimgestellt bleiben. Im Grundsatz ist dies eine submissionsrechtliche Thematik, jedoch rechtfertigt sich eine Regelung im InfoSiG, da es ganz spezifisch um die Wahrung der mit dem InfoSiG verfolgten öffentlichen Interessen geht.

Der CISO beziehungsweise die Fachstelle für Informationssicherheit werden künftig vermehrt in die sicherheitsrelevanten Vergabeverfahren, die in den letzten Jahren bereits merklich zugenommen haben, einzubinden sein.

5.2.3.2 Kantonale Meldepflicht bei Cyberangriffen

Das Postulat der FDP-Fraktion vom 18. Januar 2022 betreffend Cyberkriminalität (GR.22.29) forderte sinngemäss eine spezifische Überprüfung hinsichtlich Einführung einer kantonalen Meldepflicht für von Cybercrime betroffene Gemeinden, Unternehmen, Institutionen mit öffentlichen Aufträgen respektive solcher in öffentlicher Hand (vgl. Kapitel 2.4).

In der Zwischenzeit hat der Bundesgesetzgeber die Änderung des ISG zu den geplanten Massnahmen des Bundes zum Schutz der Schweiz vor Cyberbedrohungen (Kapitel 5 des ISG) beschlossen (BBl 2023 2296). Eine Massnahme sieht spezifisch die Pflicht zur Meldung von Cyberangriffen (Art. 74a ff. ISG) vor. In Art. 74b ISG werden die meldepflichtigen Behörden und Organisationen aufgeführt. Im Wesentlichen trifft die Meldepflicht Behörden und Organisationen, wenn durch Cyberangriffe ausgelöste Funktionsstörungen Auswirkungen auf das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung haben (Art. 74c e contrario). Der Kreis der Meldepflichtigen umfasst grundsätzlich jene Bereiche, welche aus Sicht der Cybersicherheit besonders lohnende Ziele für Cyberangriffe darstellen. Meldepflichtig sind Behörden aller föderalen Ebenen, die Hochschulen und kritischen Infrastrukturen der verschiedensten Bereiche wie Sicherheit und Rettung, Trinkwasserversorgung, Abwasserversorgung, Abfallentsorgung, Energieversorgung, -handel, -messung und -steuerung, Banken, Versicherungen und Finanzmarktinfrastrukturen, Gesundheitseinrichtungen sowie weitere Bereiche.

Damit hat sich das Anliegen des Postulats weitgehend erfüllt. Gemeinden sind meldepflichtig und auch Unternehmen, soweit sie unter den Positivkatalog von Art. 74b Abs. 1 lit. a-u ISG fallen und nicht ein Ausnahmefall gemäss Art. 74c ISG darstellen. Dasselbe gilt für Träger öffentlich-rechtlicher Aufgaben wie Anstalten, Körperschaften und Stiftungen. Der Text des Postulats differenziert nicht, aber es kann nicht darum gehen, undifferenziert alle Angriffe auf Unternehmen zu erfassen, sondern es gilt diejenigen Unternehmen und Institutionen zu schützen, deren Lahmlegung durch Cyberangriffe negative Auswirkungen auf den Kanton haben können. Diese Unternehmen sind bereits durch die Meldepflicht des ISG erfasst, weshalb es keiner parallelen, zusätzlichen Regelung durch den Kanton bedarf, aber auch keiner ergänzenden kantonalen Regelung im Sinne einer Meldepflicht für alle Unternehmen. Der Kanton wird auch über entsprechende Meldungen seitens der Bundesbehörden (Bundesamt für Cybersicherheit, BACS) informiert. Immer dann, wenn der Verdacht besteht, dass der Kanton selbst vom entsprechenden Angriff betroffen sein könnte, wird die Meldung weitergegeben. Aus den vorerwähnten Gründen wird deshalb auf die Statuierung einer kantonalen Meldepflicht verzichtet.

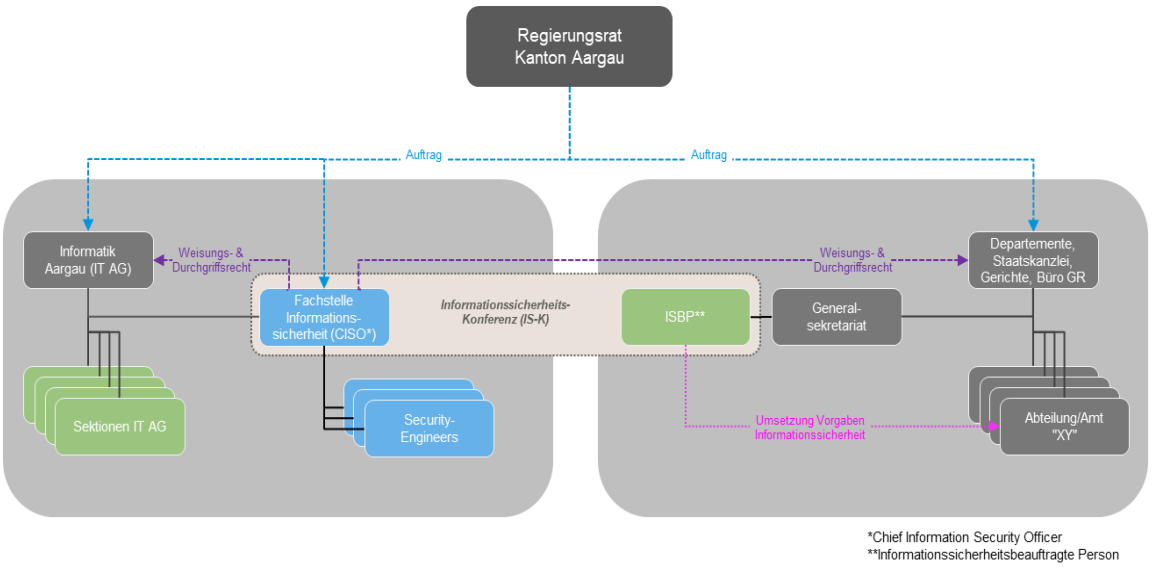
5.2.4 Organisation

Die Organisationsstrukturen sind für eine sach- und risikogerechte Informationssicherheit absolut zentral. Das neue Gesetz ist daher nicht zuletzt auch ein Organisationserlass. Dabei gilt es, auf Gesetzesstufe lediglich den behördenübergreifenden Rahmen zu normieren, während für den Vollzug in der kantonalen Verwaltung allein der Regierungsrat zuständig ist. Neu ist auch eine verwaltungsübergreifende Organisation zu schaffen, welche zur Minimierung der Cyber-Risiken im ganzen Kanton beitragen soll (Kap. 7.5.2).

5.2.4.1 Kantonale Verwaltung

Die künftige Organisation der kantonalen Verwaltung soll grundsätzlich auf der heutigen Organisation basieren. Sie soll und muss jedoch im behördenübergreifenden Rahmen in ihren Grundzügen gesetzlich fixiert und optimiert werden. Die behördenübergreifenden Befugnisse sollen künftig der zentralen Fachstelle für Informationssicherheit (Kap. 5.2.4.1.1) zukommen.

Abbildung 6: Künftige Organisation der Informationssicherheit des Kantons Aargau



Nicht auf Gesetzesebene zu regeln sind diejenigen Rollen, die für den Vollzug in den Departementen zuständig sind. Die organisatorische Regelung obliegt diesbezüglich dem Regierungsrat. Im Rahmen des Gesetzgebungsverfahrens gilt es, zur Stärkung und Kompetenzbildung dieser Stellen beizutragen. Nachfolgend soll ein Überblick über die geplante, auf Verordnungsebene zu regelnde interne Organisationsstruktur gegeben werden. Vorgeschlagen wird eine departementale Beauftragtenrolle (ISBP) und ein überdepartementales Koordinationsorgan, das sich spezifisch der Informationssicherheit widmen soll. Dadurch wird den teilweise dezentral erbrachten IT-Leistungen Rechnung getragen. Dabei geht es um Funktionen, die alle Querschnittaufgaben der Informationssicherheit erfüllen sollen. Aus Gründen der Übersichtlichkeit wird die Organisation als Ganzes dargestellt, um nicht einen lediglich partiellen Eindruck der vorgesehenen Gesamtorganisationsstrukturen zu vermitteln.

5.2.4.1.1 Zentrale Fachstelle für Informationssicherheit

Die Informationssicherheit muss – wie bereits mehrfach erwähnt (vgl. Kap. 4.3 und 5.1.2) – nach einem integralen Ansatz organisiert, gesteuert und überprüft werden. Diverse, bereits heute wahrgenommene Aufgaben, werden von verschiedenen Fachorganen erfüllt. Sie sind nach einer sektoriellen, departementalen Betrachtungsweise konzipiert und nicht spezifisch aufeinander abgestimmt. Eine verbesserte Koordination allein genügt nicht, um den integralen Ansatz zu verwirklichen. Deshalb soll eine zentrale Fachstelle für Informationssicherheit als Kompetenzzentrum für die departements- und behördenübergreifenden Aufgaben geschaffen werden. Ihr Auftrag ist im Grundsatz als beratend und unterstützend zu verstehen. Die Fachstelle für Informationssicherheit soll aber behördenübergreifend tätig sein und über entsprechende Weisungs- und Durchsetzungsbefugnisse verfügen, welche die Vollzugsautonomie der Behörden tangieren können. Aber die Gefährdung der öffentlichen Interessen, die durch eine Verletzung der Informationssicherheit einher gehen kann, rechtfertigt es, dass die Fachstelle gesetzlich bestimmte Kompetenzen erhält wie beispielsweise die autonome Durchführung von Überprüfungen aber auch die Möglichkeit des Ergreifens von Massnahmen, wenn Verletzungen der Informationssicherheitsvorgaben (Gesetz, Verordnung, Weisungen, Standards) festgestellt werden sollten. Der Informationssicherheit ist nicht geholfen, wenn sich die Fachstelle in einer solchen Situation nicht einbringen kann und insbesondere, wenn sie sich nicht durchzusetzen vermag. Es ist vorgesehen, die Funktion des heutigen CISO der kantonalen Verwaltung in jene der Leiterin beziehungsweise des Leiters der Fachstelle für Informationssicherheit umzuwandeln. Die konkreten Aufgaben der Fachstelle sind abschliessend im Gesetz festzuhalten (Kap. 7.5.1.1).

5.2.4.1.2 Informationssicherheitsbeauftragte Person (ISBP)

Die Funktion der Informationssicherheitsbeauftragten Person (ISBP) ist für den Vollzug insofern zentral, als sie vor allem auch eine Managementfunktion darstellt. Die ISBP werden sich nicht primär mit hochtechnischen Informationssicherheitsfragen befassen, sondern im Auftrag ihrer Behörde (oder der Departemente und der SK) die Informationssicherheit steuern sowie die Umsetzung der beschlossenen Massnahmen begleiten. Den Fokus werden sie auch auf das Risikomanagement sowie auf die Koordination mit anderen Bereichen legen müssen. Eine wirksame Aufgabenerfüllung durch die ISBP setzt – neben einer klaren Unterstützung durch die Führung – eine enge Zusammenarbeit mit den Stellen voraus, die für das allgemeine Risikomanagement, den Datenschutz und die Umsetzung der Sicherheitsmassnahmen zuständig sind. Die ISBP werden also als Drehscheibe zwischen Führung und denjenigen Stellen, die für die Umsetzung der Massnahmen zuständig sind, agieren. Da es sich hierbei um eine behördeninterne Funktion handelt, bedarf es keiner gesetzlichen Grundlage. Vielmehr wird es Sache des Regierungsrats sein, die Zuständigkeiten und die Aufgaben durch Verordnung zu definieren und zu regeln.

5.2.4.1.3 Koordinationsorgan Informationssicherheit

Auch das Koordinationsorgan Informationssicherheit ist ein rein behördeninternes Gremium und deren Zuständigkeiten und Aufgaben folglich im Rahmen der Verordnungskompetenz des Regierungsrats zu regeln. Eine Konferenz der ISBP, in welcher alle Behörden, die Fachstelle für Informationssicherheit (CISO) und punktuell die ÖDB vertreten sind, stellt eine zentrale Massnahme dar. Die für die fachliche Steuerung der Umsetzung zuständigen ISBP werden umfassende Kenntnisse der Probleme der Informationssicherheit in ihrem Zuständigkeitsbereich, insbesondere bei der Umsetzbarkeit, Wirksamkeit und Wirtschaftlichkeit der Vorschriften sowie der beschlossenen Massnahmen erhalten. Die Konferenz wird dem einheitlichen, behördenübergreifenden und risikobasierten Vollzug sowie der Koordination mit der ÖDB dienen.

Heute fehlt formell ein Koordinationsorgan für den Vollzug der Informationssicherheit. Faktisch nimmt zwar die Informatikkonferenz (IK) diese Aufgabe wahr (vgl. Kap. 2.3.3.3), jedoch liegt ihr Fokus eher auf der IKT-Sicherheit. Mit Blick auf die Wichtigkeit der Informationssicherheit erscheint ein eigenes, dediziertes Koordinationsorgan für dieses Thema als angemessen.

5.2.4.2 Kantonale Cyber-Organisation

Die Behörden des Kantons tauschen Informationen nicht nur untereinander, sondern auch mit Dritten aus. Sie stehen in einem ständigen Dialog mit ihren öffentlichen und privaten Partnern und tauschen dabei Informationen aus, die auch Geschäfts- und Fabrikationsgeheimnisse Dritter beinhalten können. Dieser Informationsaustausch findet inzwischen zu einem wesentlichen Teil elektronisch statt. Gleichzeitig nimmt die Vernetzung der Informatiksysteme unter den Behörden des Kantons laufend zu. Die Systeme der verschiedenen Behörden weisen daher immer mehr gemeinsame Schnittstellen auf, wodurch sich das Risiko erhöht, dass sich Bedrohungen sowie Angriffe gegen eine Behörde auf die Zuständigkeitsbereiche anderer Behörden ausbreiten könnten. Werden Informationen auch ausserhalb einer Organisation bearbeitet oder wird von aussen hin auf Mittel der Informationstechnik zugegriffen, genügt der Schutz des eigenen Zuständigkeitsbereichs allein nicht mehr, weil die Schutzmassnahmen auch ausserhalb des eigenen Perimeters Wirkung erzielen müssen. Insbesondere die Cyber-Bedrohungen sind ein Querschnittsthema, das sowohl die Verwaltungen und die Gerichte, aber auch die Wirtschaft und besonders die kritischen Infrastrukturen, wie auch weitere Institutionen sowie die Bevölkerung betreffen. Es ist daher notwendig, dass die Informationssicherheit auch ausserhalb der Verwaltungsgrenzen, in der Wirtschaft, Gesellschaft und in den Gemeinden sowie bei den Trägern öffentlicher Aufgaben gewährleistet werden kann. Der Kanton übernimmt dabei nicht in erster Linie den Schutz der Informationen und der Informatikmittel der erwähnten Institutionen und Behörden, aber er kann mit einer kantonalen Cyber-Organisation dazu beitragen, dass mit Vernetzung, Informationsaustausch und Sensibilisierung auch ausserhalb der Verwaltungsgrenzen der Fokus vermehrt auf die Risikominimierung gelegt wird.

Die mit dem Gesetzesentwurf vorgeschlagene kantonale Cyber-Organisation (vgl. Kap. 7.5.2) richtet sich im Wesentlichen nach den Empfehlungen für die Umsetzung zur kantonalen Cyber-Organisation vom 12. Januar 2021 des Sicherheitsverbunds Schweiz (SVS). Die Notwendigkeit des Aufbaus einer kantonalen Cyber-Organisation, ist angezeigt und wurde im Austausch mit den zuständigen Stellen für die Cyber-Kriminalität (Kapo und Staatsanwaltschaft), mit der für die Informations- und Informatiksicherheit zuständigen Stellen (CISO und Leitung Informatik Aargau) sowie mit einer kritischen Infrastruktur (Swissgrid) erarbeitet.

6. Verhältnis zur mittel- und langfristigen Planung

6.1 Verhältnis zum Aufgaben- und Finanzplan (AFP)

Im AFP 2023–2026 ist ein Entwicklungsschwerpunkt betreffend die "Schaffung einer gesetzlichen Grundlage für die Informationssicherheit des Kantons" aufgenommen worden.

Die Bedrohungslage und mithin das Schadenspotenzial sind derart, dass der Regierungsrat den unmittelbaren Handlungsbedarf bereits angegangen ist und im Herbst 2023 den Auftrag erteilt hat, mittel- und langfristige Massnahmen vorzusehen, um die Organisationsform den Anforderungen an eine sichere Gewährleistung der Informations- und Cybersicherheit anzupassen und die notwendigen Ressourcen in finanzieller und personeller Hinsicht bereitzustellen beziehungsweise zu planen. Die entsprechenden finanziellen und personellen Ressourcen werden im AFP 2025–2028 eingestellt. Zudem wird im Aufgabenbereich 435 Informatik ein zusätzlicher Entwicklungsschwerpunkt zur Informationssicherheit aufgenommen.

6.2 Verhältnis zu Strategien des Regierungsrats

6.2.1 Strategie SmartAargau

Die im Kapitel 2.1.2 beschriebene Strategie SmartAargau orientiert sich auch daran, dass bei der Realisierung von E-Government-Vorhaben Informationssicherheit und Datenschutz gewährleistet werden. Der Gesetzesentwurf führt zu einer gewissen Vereinheitlichung in Bezug auf die Informationssicherheit zwischen Kanton und Gemeinden (vgl. insbesondere Kap. 5.1.1 und die Erläuterungen zu § 2 unter Kap. 7.2.2) und ist daher ganz im Sinne der Strategie SmartAargau.

6.2.2 Open Government Data Strategie 2017-2022

Zur Strategie: siehe Kapitel 2.1.5. Der Umsetzungsvorschlag verbessert insofern die zukünftige Umsetzung der OGD-Strategie Aargau, als die Wahrung der Unversehrtheit und Richtigkeit von Informationen (Schutzziel "Integrität") unter anderem für Informationen von Bedeutung ist, die zur Veröffentlichung oder Wiederverwendung bestimmt sind. Auch die Schutzziele "Verfügbarkeit" und "Nachvollziehbarkeit" der Informationssicherheit dienen selbstredend den Zielsetzungen von OGD. Derzeit laufen Vorarbeiten für das Projekt "Kantonale Datenstrategie und Erneuerung der OGD-Strategie sowie Masterplan zu deren Umsetzung; Etappe" (vgl. RRB Nr. 2022-001592). Die Entwicklungen in diesem Projekt werden bei den weiteren Arbeiten in vorliegendem Rechtssetzungsprojekt verfolgt.

6.2.3 Fachstrategie Informatik des Kantons Aargau 2020–2026

In der Fachstrategie Informatik des Kantons Aargau 2020–2026 wird im Kapitel 3.7 Informationssicherheit und Datenschutz folgendes ausgeführt:[6]

[6] Abrufbar unter: www.ag.ch / Verwaltung / Departement Finanzen und Ressourcen / Über uns / Organisation / Informatik Aargau (zuletzt besucht am: 10. August 2022).

"Der Kanton Aargau realisiert die Vorteile der wachsenden Durchdringung mit präventiver, gut organisierter IT-Sicherheit zum Schutz von IT-Infrastrukturen, Geräten und Informationen. Den wachsenden und zunehmend komplexer werdenden Bedrohungen durch Cyberkriminalität wird Rechnung getragen. Das Sicherheits- und Risikomanagement stellt sicher, dass vertrauliche und personenbezogene Daten entsprechend ihrer Klassifikation angemessen geschützt sind und die datenschutzrechtlichen Bestimmungen für deren Speicherung und Nutzung eingehalten werden."

Die vorgeschlagene Lösung entspricht in diesem Punkt vollumfänglich der IT-Governance der Fachstrategie Informatik. Weiter zielen insbesondere auch folgende strategischen Stossrichtungen der Fachstrategie in dieselbe Richtung wie der vorliegende Umsetzungsvorschlag:

- S12 Durchsetzung festgelegter Standards und Methoden;
- S13 Aufbau des Dateninventars sowie Sicherstellung einer hohen Verfügbarkeit unter Berücksichtigung der Datenklassifizierung ("Datenschutz");
- S19 Digitale Identitäten und Datenzugänge stehen organisations- und technologieübergreifend zur Verfügung;
- S30 Verstärkung von Sensibilität und Kompetenz der Mitarbeitenden im Bereich der Informationssicherheit.

6.3 Verhältnis zu anderen Rechtssetzungsprojekten

Auf kantonaler Ebene sind derzeit – mit Ausnahme der geplanten Änderung des PolG betreffend die PSP – keine direkten Abhängigkeiten zu anderen Rechtssetzungsprojekten ersichtlich.

Mit der vorgesehenen Änderung des PolG, dessen Inkrafttreten per 1. Juni 2024 geplant ist, soll unter anderem eine Grundlage für die PSP betreffend Angehörige der Kantonspolizei und Polizeikräfte der Gemeinden normiert werden. Weil das vorliegende Projekt "Schaffung rechtlicher Grundlagen für die Informationssicherheit" zeitlich im Vergleich zur vorliegenden Änderung des Polizeigesetzes verzögert ist und noch einige Zeit in Anspruch nehmen wird, macht es Sinn, wenn die Regelung der PSP von Angehörigen der Polizeikorps bereits im Rahmen der Änderung des PolG umgesetzt wird. Grundsätzlich wäre es erstrebenswert, die PSP generell, das heisst für alle Personalkategorien einheitlich zu normieren. Das PolG will aber unabhängig von der Frage der Informationssicherheit alle Mitarbeitenden der Polizei, namentlich auch diejenigen der Gemeinden, einer PSP unterziehen, weshalb es sich in seinem Zweck und im Geltungsbereich von der Regelung des InfoSiG unterscheidet. Folglich ist an der Spezialgesetzgebung des PolG festzuhalten. Die beiden Erlasse kommen dadurch nicht in Widerspruch zueinander, weil die Regelungen im Wesentlichen dieselben sind.

Im Zusammenhang mit der Durchführung einer PSP für die vom Volk gewählten Amtsträgerinnen und -träger ist die parallel laufende Umsetzung der Amtsenthebungsinitiative zu berücksichtigen. Hier besteht diesbezüglich Bedarf an einer Anpassung der zurzeit vorgeschlagenen Lösung in Hinblick auf die Möglichkeit einer Amtsenthebung bei negativem Ergebnis der PSP (vgl. Kap. 7.8).

Die kantonalen Rechtssetzungsprojekte und die Entwicklungen auf Bundesebene (z.B. Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise [E-ID-Gesetz, BGEID] oder Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben [EMBAG]) sind einerseits im Rahmen des vorliegenden Projekts stets im Auge zu behalten, andererseits ist das vorliegende Projekt auch bei den anderen kantonalen Rechtssetzungsprojekten sowie bei allfälligen Vernehmlassungen zum Bundesrecht zu beachten.

7. Erläuterungen zu den einzelnen Paragrafen

7.1 Ingress

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:

Die von der Cyberkriminalität ausgehende Bedrohung ist potenziell in der Lage, die öffentliche Sicherheit des Kantons zu gefährden, zum Beispiel ein Hackerangriff, der die kantonale Verwaltung und damit deren Serviceauftrag gegenüber der Bevölkerung über Tage oder gar Wochen lahmlegen würde. Da auch viele Personendaten, zum Teil auch besonders schützenswerte Personendaten der Bevölkerung in den Systemen der kantonalen Verwaltung liegen, kommen potenzielle Gefährdungen der Persönlichkeitsrechte zahlreicher Personen in Betracht. Es ist deshalb folgerichtig, § 27 Abs.1 der Kantonsverfassung als Delegationsnorm des InfoSiG aufzuführen. Weil das InfoSiG nicht zuletzt auch ein Organisationsgesetz ist, das eine verwaltungsinterne, behördenübergreifende und eine über die Grenzen der Verwaltung hinausgehende Organisation vorsieht, sind auch die §§ 86 Abs. 1, 94 Abs. 1 und 97 Abs. 1 der Kantonsverfassung, welche die Organisationsbestimmungen der drei Behörden darstellen, als Delegationsnormen des InfoSiG zu erwähnen.

7.2 Kapitel 1 Allgemeine Bestimmungen

7.2.1 § 1 Zweck

§ 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,

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.

Der Zweck des neuen Gesetzes ergibt sich grundsätzlich aus dem Begriff der Informationssicherheit. Bezweckt wird demnach der Schutz aller Informationen, für welche die kantonalen Behörden zuständig sind, ungeachtet des Umstands, ob sie diese selbst erstellen, von Dritten erhalten oder Dritten zur Bearbeitung weitergeben. Ebenso wie für die Herkunft der Informationen soll das Gesetz auch in Bezug auf die Art und Form der Informationen umfassend gelten und daher technologieneutral sein. Es spielt demnach keine Rolle, ob die Information textlicher, akustischer oder graphischer Natur ist und ob sie elektronisch oder beispielsweise auf einem Papierdokument verfügbar ist. Im Zentrum steht immer die Information und wie diese Information gewonnen, transportiert, verarbeitet und dann weiterbearbeitet wird, um daraus Wissen zu kreieren. Wissen, aus welchem man einen Mehrwert generieren oder aufgrund dessen man sich einen Vorteil verschaffen kann. Weiter soll das neue Gesetz auch sämtliche Informationstechnik erfassen, die von den kantonalen Behörden eingesetzt, auf welche zugegriffen wird oder deren Betrieb sie auslagern.

Der Schutz der Informationen und der Informatikmittel ist kein Selbstzweck, sondern dient bestimmten öffentlichen Interessen beziehungsweise Eigeninteressen des Kantons als Gemeinwesen. Im Gegensatz zum IDAG, das in Bezug auf Personendaten die Interessen Dritter (d.h. betroffener Personen) schützt, soll das Gesetz technologieneutral durch Gewährleistung einer sicheren Bearbeitung von Informationen, für die der Kanton zuständig ist, hohe eigene Interessen des Kantons, namentlich die innere Sicherheit (lit. a), die Entscheidungs- und Handlungsfähigkeit der Behörden und ihrer Verwaltungseinheiten (lit. b) und die Erfüllung der gesetzlichen und vertraglichen Verpflichtungen des Kantons zum Schutz von Informationen (lit. c) schützen. Der Schutz der öffentlichen Sicherheit

beinhaltet auch die Individualinteressen der Bevölkerung und von Unternehmen (Persönlichkeitsrechte und Geschäftsgeheimnisse) im Verkehr mit den Behörden.

7.2.2 § 2 Geltungsbereich

§ 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.

[3] Absatz 2 findet keine Anwendung, wenn die Gemeinden und andere Träger öffentlicher Aufgaben eine mindestens gleichwertige Informationssicherheit gewährleisten.

Die Vernetzung der Informatiksysteme der kantonalen Behörden nimmt untereinander laufend zu. Dadurch wird das Risiko erhöht, dass sich Angriffe sowie Bedrohungen gegen eine Behörde auf die Zuständigkeitsbereiche anderer beteiligter Behörden ausweiten könnten. Es ist daher unentbehrlich, dass die jeweiligen kantonalen Behörden gleichwertige Risikobeurteilungskriterien und -methoden anwenden und dass ihre organisatorischen, personellen, technischen und physischen Sicherheitsmassnahmen beim Einsatz von Informatikmitteln aufeinander abgestimmt werden. Mit Blick hierauf, aber auch aufgrund der im Handlungsbedarf (insbesondere unter Kapitel 4.3) aufgeführten Gründe soll das Gesetz für die Behörden des Kantons im Sinn von Kapitel 5 der Kantonsverfassung, mithin also der obersten Führungsverantwortung (Grosser Rat, Regierungsrat und Gerichte), sowie für die ihnen unterstellten Organisationen (Parlamentsdienste, kantonale Verwaltung und Justizverwaltung) gelten (Abs. 1). Gemäss § 94 der Kantonsverfassung sind die Anstalten, sowohl die unselbstständigen (Abs. 2) als auch die selbstständigen (Abs. 3), Teil der regierungsrätlichen Organisation, weshalb sie ebenfalls unter den Geltungsbereich des Gesetzes fallen. Nicht unter den Geltungsbereich des Gesetzes fallen hingegen alle weiteren Beteiligungen des Kantons, insbesondere auch diejenigen, an denen der Kanton eine Mehrheitsbeteiligung hat oder sogar Alleineigentümer ist. Es handelt sich hierbei um Rechtssubjekte des Privatrechts, denen gesetzliche Pflichten nicht auferlegt werden können. Wenn auch eine unmittelbare Anwendung der gesetzlichen Bestimmungen für Beteiligungen nicht in Betracht kommen, soll aber eine mittelbare Umsetzung einer genügenden Informationssicherheit mittels Aktionärsbefugnisse erreicht werden. Die Verpflichtung zur Umsetzung der Vorgaben zur Gewährleistung der Informationssicherheit trifft demnach die Behörden im Sinne der obersten Führungsverantwortung (vgl. § 5), wohingegen deren Verwaltungseinheiten schwergewichtig für die Umsetzung verantwortlich sind.

Fraglich ist, ob und inwieweit die Vorschriften des neuen Gesetzes auch für die Gemeinden und die anderen Träger öffentlicher Aufgaben (öffentlich-rechtliche Institutionen wie Körperschaften, Anstalten und Stiftungen; insbesondere auch öffentlich-rechtlich anerkannte kirchliche Körperschaften) gelten sollen. Der Kanton hat ein erhebliches Interesse daran, dass kantonale Daten, die von diesen bearbeitet werden, auch bei ihnen sicher sind. Aufgrund des Umstands, dass der (elektronische) Informationsaustausch zu den wesentlichen Elementen der Aufgabenerfüllung aller öffentlichen Organe unabhängig ihrer Staatsebene zählt und die jeweiligen Informationssysteme im Zuge der Digitalisierung zunehmend vernetzt betrieben werden, droht eine Erosion der Verantwortlichkeitszuweisungen für die Informationssicherheit. Dies hat zur Folge, dass sich Bedrohungen im eigentlichen Zuständigkeitsbereich einer Behörde auf die Bereiche anderer Beteiligter ausbreiten. Es wird daher vorgeschlagen, dass die entsprechenden Vorschriften des neuen Gesetzes – in Anlehnung an die Regelung des Bundes im Verhältnis zu den Kantonen – für Gemeinden und andere Träger öffentlicher Aufgaben zum Tragen kommen sollen, wenn sie klassifizierte Informationen des Kantons bearbeiten (Abs. 2 lit. a). Dasselbe soll auch gelten, wenn sie auf Informatikmittel des Kantons zugreifen

(Abs. 2 lit. b). Die Vorschriften des Kantons über klassifizierte Informationen und die Sicherheit beim Einsatz von Informatikmitteln (vgl. §§ 8-10, Kap. 7.3.4) sollen jedoch in Berücksichtigung des Subsidiaritätsprinzips nur dann zur Anwendung kommen, wenn die Vorschriften und Massnahmen der Gemeinden und anderer Träger öffentlicher Aufgaben den Sicherheitsanforderungen des Kantons nicht genügen. Das InfoSiG ist demnach nicht zu befolgen, soweit die Gemeinden und anderen Träger öffentlicher Aufgaben bereits mit einer eigenen, mit derjenigen des Kantons vergleichbaren Informationssicherheit ausgestattet sind. Dies ist der Fall, wenn der IKT-Minimalstandard des Bundes eingehalten wird. Dieser ist ein vom Bund als Empfehlung herausgegebener Branchenstandard und wird als «Ausdruck der Schutzverantwortung des Staates gegenüber den Bürgerinnen und Bürgern, der Wirtschaft, den Institutionen und der öffentlichen Verwaltung» bezeichnet. Der IKT-Minimalstandard richtet sich zwar insbesondere an die Betreiber von kritischen Infrastrukturen, er ist aber auch für jedes Unternehmen und auch für die öffentliche Hand auf allen Ebenen zur eigentlichen Richtschnur und zum gemeinsamen Nenner in Bezug auf das Sicherheitsniveau geworden. Aktuell ist der IKT-Minimalstandard 2023 (Version Mai 2023, mit Update NIST SP 800-53 Rev. 5 und ISO 27001:2022), der unter anderem auf die bewährten internationalen Standards NIST und ISO 27001 abstellt. Mithilfe eines Audits nach dem IKT-Minimalstandard kann der aktuelle Reifegrad des Sicherheitsdispositivs einer Organisation beurteilt werden. Dies erfolgt gestützt auf dem IKT-Tool, das den Reifegrad auf einer Skala von 0 bis 4 für jede einzelne Kontrolle und für die verschiedenen Funktionen von NIST (Identifizieren, Schützen, Detektieren, Reagieren, Wiederherstellen) misst. Der Reifegrad, der aktuell vom Bund zum IKT-Minimalstandard erklärt worden ist, hat den Wert 2.6.

Ein dynamischer Verweis auf den IKT-Minimalstandard im Gesetz kommt nicht in Betracht, weil ein gesetzlicher Verweis auf ein als "Empfehlung" qualifiziertes Dokument der Bundesverwaltung nicht in Betracht kommen kann. Das Dokument kann geändert aber auch aufgehoben werden beziehungsweise der IKT-Minimalstandard kann infolge veränderter Verhältnisse aufgrund der technologischen Entwicklung jederzeit und formlos durch einen passenderen Standard ersetzt werden. Diesfalls müsste das Gesetz angepasst werden, was bekanntlich einige Zeit in Anspruch nehmen würde.

7.2.3 § 3 Sicherheitsrelevanz

§ 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.

Der Bund sieht eine Bestimmung mit drei Begriffsdefinitionen vor, wovon zwei keiner Regelung bedürften, zumal allgemein verständlich ist, was Informatikmittel und kritische Infrastrukturen sind. Mit der dritten Begriffsdefinition legt er fest, was als sicherheitsrelevant zu gelten hat. Für das Verständnis der weiteren Bestimmungen des Gesetzesentwurfs ist es erforderlich zu definieren, was sicherheitsrelevante Informationen oder Tätigkeiten sind, denn dieser Begriff wird im Zusammenhang mit dem Schutz von Informationen und Informatikmitteln immer wieder aufgenommen. Damit wird insbesondere festgehalten, dass nicht alle klassifizierten Informationen beziehungsweise nicht alle Sicherheitsstufen für Informatikmittel als sicherheitsrelevant im Sinne dieses Gesetzes gelten. Die als "intern" klassifizierten Informationen (vgl. § 8 Abs. 2 lit. a; Kap. 7.3.4.1) und die Informatikmittel mit Sicherheitsstufe "Grundschutz" (§ 12 Abs. 3 lit. c; Kap. 7.4.1) sind von der Begriffsdefinition ausgenommen. Das heisst nicht, dass ihnen kein Schutz zukommen soll, jedoch wäre es mit unverhältnismässigem Aufwand verbunden, auch ihnen erhöhten Schutz zukommen zu lassen. Dies nicht zuletzt auch, weil der Schwellenwert dieses Schutzes eher tief ist. Der Schutz der Informationen und der Informatikmittel soll dort effizient ansetzen, wo das Schadenspotenzial als mögliche Folge einer Verletzung der Informationssicherheit hoch ist und soll dort eher vernachlässigt werden, wo das Schadenspotenzial gering ist (vgl. hierzu die Kap. 7.3.4.1 und 7.4.4.1). Es darf aber nicht ausser Acht gelassen

werden, dass selbst im Rahmen einer Bearbeitung von lediglich als "intern" klassifizierten Daten, konkrete Risiken bestehen. Zwar bleibt es beim geringen Schadenspotenzial als Folge einer Datenschutzverletzung dieser Datenkategorie, jedoch kann eine entsprechende Datenbearbeitung negative Wirkungen für das kantonale Informatiknetz haben. Ein denkbares Szenario ist beispielsweise, dass mit bewusstem oder unbewusstem Einspeisen einer Malware das ganze Informatiknetz unbemerkt mit hohem Schadenspotenzial infiziert werden könnte. Die Wahrscheinlichkeit des Eintritts eines solchen Schadens ist zwar gering, aber er kann nicht ganz ausgeschlossen werden. In der Praxis ist diesem Aspekt deshalb zumindest im Rahmen der vertraglichen Regelung durch spezifische Vorgaben Rechnung zu tragen.

7.2.4 § 4 Verhältnis zu anderen Gesetzen

§ 4 Verhältnis zu anderen Gesetzen

[1] Für Informationen, deren Schutz auch in anderen Gesetzen geregelt ist, finden die Bestimmungen dieses Gesetzes ergänzend Anwendung.

Im Verhältnis zu anderen Gesetzen, die ebenfalls den Schutz von Informationen vorsehen, soll das InfoSiG ergänzend Anwendung finden. Die spezialgesetzlichen Regelungen sollen nicht derogiert werden, ein Nebeneinander ist anzustreben. Dies gilt es im Verhältnis zum Öffentlichkeitsprinzip stets zu berücksichtigen. Das InfoSiG geht auch davon aus, dass im Grundsatz alle Informationen öffentlich sind, soweit sie nicht klassifiziert werden. In dieser Beziehung geht das Öffentlichkeitsprinzip dem InfoSiG vor. Bei Gesuchen um Zugang zu amtlichen Dokumenten gelten die Bestimmungen des Öffentlichkeitsprinzips (§§ 4 ff. IDAG). Dabei richtet sich eine entsprechende Interessenabwägung nach § 5 Abs. 3 lit. b IDAG. Insbesondere auch im Verhältnis zum Datenschutz muss klar hervorgehen, dass die beiden Disziplinen zwar eine gemeinsame thematische Schnittmenge haben, indem Personendaten auch Informationen sind, jedoch der Schutzzweck jeweils ein anderer ist. Der Datenschutz bezweckt den Schutz der Privatsphäre eines jeden Menschen. Die Datenschutzgesetzgebung legt unter anderem fest, dass Personendaten nur recht-, verhältnis- und zweckmässig sowie für die betroffenen Personen möglichst transparent bearbeitet werden dürfen (§§ 8, 9, 11 und 13 IDAG). Auch bei Inkrafttreten des neuen Gesetzes müssen Personendaten im Kanton weiterhin nach dem IDAG bearbeitet werden. Im Verhältnis zum neuen Informationssicherheitsgesetz wäre das IDAG demnach als Spezialgesetzgebung zu betrachten. Zu beachten ist indes, dass das IDAG selbst auch Anforderungen an den praktischen Schutz von Vertraulichkeit, Verfügbarkeit und Integrität der Daten stellt. So verlangt § 12 Abs. 1 IDAG, dass Personendaten durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Der Regierungsrat hat insbesondere in den §§ 4 und 5 VIDAG Anforderungen an den Schutz von Personendaten festgelegt. Die Vorschriften des neuen Gesetzes sollen auf die Bearbeitung von Personendaten gemäss IDAG und allfälligen anderen Erlassen, die den Schutz von Informationen separat regeln, als ergänzendes Recht angewendet werden. Personendaten gelten nämlich im Sinne des neuen Gesetzes (auch) als Informationen, welche die kantonalen Behörden hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit schützen müssen. In der Regel werden Personendaten als solche nicht formell (separat oder anders) klassifiziert. Die Ausführungsbestimmungen zum neuen Gesetz sollen allerdings Informationen und Daten je nach Schutzbedarf ein bestimmtes Schutzniveau in Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit zuweisen. Die Standardisierung der Massnahmen nach dem Stand von Wissenschaft und Technik, welche mit den jeweiligen Schutzniveaus verknüpft werden, wird auch dazu dienen, die Anforderungen der Datenschutzgesetzgebung an die Datensicherheit zu erfüllen und letztlich dazu beitragen, den Datenschutz beim Kanton zu erhöhen.

Ein weiterer Erlass, der Informationssicherheitsbestimmungen, namentlich zur Personensicherheitsprüfung beinhaltet beziehungsweise beinhalten wird, ist das Gesetz über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG) vom 6. Dezember 2005 (SAR 531.200). Das Gesetz ist in

Revision, unter anderem werden gerade neue gesetzliche Grundlagen für die PSP geschaffen. Die Inkraftsetzung der Änderungen ist per 1. Juni 2024 vorgesehen. Das PolG will unabhängig von der Frage der Informationssicherheit alle Mitarbeitenden der Polizei einer PSP unterziehen, namentlich auch die Angehörigen der Regionalpolizeien, welche den Gemeinden unterstellt sind. Folglich ist an der Spezialgesetzgebung des PolG festzuhalten. Die beiden Erlasse kommen dadurch nicht in Widerspruch zueinander, vielmehr würden sie sich so ergänzen.

7.3 Kapitel 2 Führung und allgemeine Massnahmen

7.3.1 Führung

7.3.1.1 § 5 Führungsverantwortung

§ 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),

c) die Informatikmittel, die sie zur Erfüllung ihrer gesetzlichen Aufgaben einsetzen, vor Missbrauch und Störung geschützt werden.

Die Informationssicherheit dient dem Schutz der Informationen, welche das Gemeinwesen bearbeitet, das heisst, beschafft, aufbewahrt, verwendet, umarbeitet, bekannt gibt oder vernichtet (vgl. § 3 Abs. 1 lit. g IDAG). Dementsprechend erscheint es angezeigt, dass dasjenige Organ für die Sicherheit der Informationen verantwortlich ist, dessen Aufgabenerfüllung die Bearbeitung dieser Informationen dient. Es ist jenes Organ, das letztlich auch für die Kosten und die weiteren Folgen der zum Schutz der Informationen erforderlichen TOM aufkommen muss. Demnach erstaunt es nicht, dass etwa der Bundesrat und die Präsidentinnen und Präsidenten grosser Unternehmen die Informationssicherheit zur "Chefsache" erklärt haben. Demnach soll die oberste Führungsverantwortung nicht jener Instanz zugewiesen werden, welche über die Informatikmittel zur Bearbeitung der Informationen entscheidet, sondern derjenigen Instanz, der sie dient. Dies kann und wird oft dieselbe Instanz sein, muss es aber nicht. Es wird damit klargestellt, dass die Verantwortung für Informationssicherheit nicht delegiert oder ausgelagert werden kann. Die vorgeschlagene Lösung ist technologieneutral, da die Entwicklungen in diesem Bereich sehr rasch erfolgen. Sie vermeidet zudem eine zersplitterte Verantwortung zum Schutz eines Informationsbestands, welcher mit verschiedenen Mitteln gleichzeitig bearbeitet wird, und verfolgt überdies die Stossrichtung einer dezentralen Verantwortung für Informationssicherheit. So wird klargestellt, dass (richtigerweise) nicht der CISO oder sonst eine zentrale Stelle für die Informationssicherheit im Kanton verantwortlich ist, sondern die Behörden (Grosser Rat, Regierungsrat, Gerichte), die für ihre Zwecke Informationen bearbeiten oder bearbeiten lassen (Abs. 1). Das Gesetz hält die Aufgaben der Behörden verbindlich fest und stellt so sicher, dass diese in der Verwaltungshierarchie zuoberst angesetzt sind. Eine Delegation dieser Aufgaben ist nicht möglich. Bei einer Bearbeitung im Auftrag verbleibt die oberste Führungsverantwortung bei der beauftragenden Behörde.

Eine wesentliche Anforderung an die oberste Führungsverantwortung ist die laufende Prüfung und Beurteilung des Schutzbedarfs der Informationen in den verschiedenen Aufgabenbereichen (Abs. 2 lit. a). Zur Festlegung des Schutzbedarfs bedarf es einer nachvollziehbaren Methodik, welche in aller Regel von verschiedenen Schadensarten ausgeht. In Betracht kommen finanzielle Schäden,

Haftungsschäden oder auch Reputationsschäden, die ihrerseits in verschiedene Schadensklassen eingeteilt werden. Letztere sind pro Aufgabenbereich durch die zuständige Organisationseinheit spezifisch festzulegen und verbindlich zu verabschieden. Der Schutzbedarf kann je nach Objekt des Schutzbedarfs (IT-Systeme, Räume, Kommunikationsverbindungen) variieren.

Zur obersten Führungsverantwortung für die Gewährleistung der Informationssicherheit gehört auch das Ergreifen aller Massnahmen, mit denen die Vertraulichkeit, die Verfügbarkeit, die Integrität und die Nachvollziehbarkeit von Informationen gewährleistet sowie die Verfügbarkeit und die Integrität von Informatikmitteln geschützt werden können (Abs. 2 lit. b). Letztere gelten entsprechend den etablierten Normen (bspw. ISO 27001) als die vier generischen Sicherheitsziele der Informationssicherheit. Deren Schutz ist unabdingbar für eine effektive Gewährleistung der Informationssicherheit.

Vertraulichkeit: Das Ziel der Vertraulichkeit ist es, den Schutz von Informationen vor der Kenntnisnahme durch unbefugte Personen zu gewährleisten. Dies kann beispielsweise durch Zuweisung geeigneter Berechtigungen für den Zugriff auf Datenbestände oder die Zugriffssicherung von Dateien erreicht werden. Oder auch durch Verschlüsselung bei der Übertragung von Daten wie auch zur Absicherung von Beständen auf Speichermedien. Nicht zuletzt kann die Vertraulichkeit durch physische Massnahmen wie eine Zutrittssicherung gewährleistet werden.

Verfügbarkeit: Geschäftsprozesse und andere Vorgänge sind für ihren reibungslosen Ablauf darauf angewiesen, dass Daten, Soft- und Hardware in geeigneter Weise verfügbar sind. Verfügbarkeit setzt dabei voraus, dass die festgehaltenen Informationen lesbar, hörbar oder einsehbar sind beziehungsweise lesbar, hörbar oder einsehbar gemacht werden können. Für autorisierte Benutzer soll der Zugriff zu den geforderten Zeiten möglich sein. Auch hier ist es primäres Ziel, unbefugte Benutzer vom Zugriff auszuschliessen. Die Verfügbarkeit kann durch das Vorhalten redundanter Komponenten erhöht werden. Zu den einfachsten Schutzmassnahmen gehören deshalb Backups und Ersatzrechner. Wichtige Faktoren für eine Verbesserung der Verfügbarkeit sind auch die Qualitätssicherung von Software sowohl hinsichtlich Fehlervermeidung als auch bezüglich Lasttests. Eine Verfügbarkeit von 100%, also 24 Stunden am Tag, 7 Tage die Woche und 365 Tage im Jahr wäre wünschenswert, jedoch in der Praxis kaum zu erreichen, da Wartungsfenster, Migrationserfordernisse und ungeplante Systemausfälle zumindest zu kurzfristigen Ausfällen führen können. In der Praxis werden deshalb Verfügbarkeitskategorien und Prozentwerte definiert und auch vertraglich vereinbart.

Integrität: Beim Sicherheitsziel der Integrität geht es darum zu verhindern, dass Daten unbefugt verändert werden oder zumindest muss erkannt werden können, dass Veränderungen vorgenommen wurden. Massnahmen der Zugriffskontrolle und physische Sicherheitsmassnahmen können unbefugte Benutzer vom Zugriff ausschliessen, indem ihnen der Zugang und damit die Möglichkeit zur Manipulation zumindest erschwert wird. Mit spezifischen Massnahmen können auch nachträgliche Veränderungen an Daten erkannt werden.

Nachvollziehbarkeit: Informationen müssen ihren Quellen, Wegen und Bearbeitungszeitpunkten zugeordnet werden können. Es muss ersichtlich sein, wer wann welche Information bearbeitet hat. Die nachvollziehbare Bearbeitung der Informationen ist insbesondere für alle öffentlichen Verfahren (Strafverfahren, Beschwerdeverfahren usw.) von grosser Bedeutung, aber auch für die Erfüllung von Kontroll- und Aufsichtsaufgaben und das Vorgehen bei Missbräuchen.

Um die Gesamtheit aller Anforderungen und Massnahmen der Informationssicherheit gewährleisten zu können, muss insbesondere dem Schutzaspekt aller Informationen im Sinne ihrer langfristigen Erhaltung und Lesbarkeit (vor allem bei digitalen Informationen und Daten) Rechnung getragen werden. Dies gilt insbesondere für die Schutzziele Verfügbarkeit und Integrität. Mit entsprechenden technischen oder organisatorischen Massnahmen kann wesentlich zur Sicherstellung der mittel- bis langfristigen Handlungsfähigkeit der Behörden und ihrer Verwaltungseinheiten und damit letztlich zur Risikominimierung beigetragen werden. Es dient nicht zuletzt auch der Langzeitarchivierung von Informationen im Staatsarchiv, die nur möglich ist, wenn die verantwortliche Behörde angemessene

Massnahmen trifft, um die langfristige Erhaltung und Lesbarkeit von Informationen vor Abgabe ans Langzeitarchiv sicherzustellen.

Schliesslich gehört der Schutz der zur Aufgabenerfüllung eingesetzten Informatikmittel (Abs. 2 lit. c) ebenfalls zu den zentralen Aufgaben der obersten Führungsverantwortung.

7.3.2 Informationssicherheits-Risikomanagement

7.3.2.1 § 6 Implementierung

§ 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.

[2] Sie haben dabei den Grundsätzen der Zweckmässigkeit, der Wirtschaftlichkeit und der Benutzerfreundlichkeit Rechnung zu tragen.

Mit dem vorgeschlagenen Gesetzesentwurf werden die Behörden verpflichtet, mittels Implementierung eines Informationssicherheitsmanagementsystems (ISMS) zur Risikominimierung beizutragen (Abs. 1) und durch ihre Verwaltungseinheiten umzusetzen. Um von vornherein zu verhindern, dass Informationssicherheit lediglich ad hoc, zufällig oder punktuell betrieben wird, bedarf es eines angemessenen Managements, auch wenn dies mit einem gewissen Aufwand verbunden ist. In einem ISMS werden sämtliche Verfahren, Regeln, Massnahmen und Werkzeuge, die zur Organisation der Informationssicherheit in einem Unternehmen oder einer Verwaltungseinheit definiert werden, festgehalten.

Ein ISMS ist im Prinzip ein sich ständig wiederholender Prozess, der in unterschiedlich aufwändiger Ausgestaltung durchlaufen werden kann. Es gilt einerseits das Grundziel zu erreichen, nämlich Informationssicherheit strukturiert und systematisch zu betreiben und ständig zu verbessern. Dazu bedient sich ein ISMS in der Praxis folgender drei Sichtweisen:

- Governance-Sicht

  Die Governance-Sicht bezieht sich auf die Steuerungsaspekte des ISMS. Dazu gehören beispielsweise die enge Einbeziehung der Geschäftsleitung eines Departements beziehungsweise eines Unternehmens und seiner Verwaltungseinheiten, die Konsistenz zwischen den Geschäfts- und Informationssicherheitszielen, die effektive und zielgruppengerechte Kommunikationsstrategie sowie die angemessenen Regelwerke und Organisationsstrukturen.

- Risikomanagement-Sicht

  Die Risikomanagement-Sicht, die unter anderem als Basis für eine nachvollziehbare Entscheidungsfindung und Priorisierung von technischen und organisatorischen Massnahmen fungiert, ist eines der Kernelemente eines ISMS nach ISO/IEC 27001. Sie beinhaltet Vorgaben und Methoden für die Identifizierung, Analyse und Bewertung von Risiken im Kontext der Informationssicherheit, d.h. Risiken, die eine potenzielle Gefährdung für die Vertraulichkeit, Integrität und/oder Verfügbarkeit der Informationen, der für die Bearbeitung erforderlichen Infrastruktur und letztlich der davon abhängigen Geschäftsprozesse darstellen.

- Compliance-Sicht

  Die Compliance-Sicht umfasst einerseits die Definition der erforderlichen (Sicherheits-)Vorgaben. Andererseits bezieht sie sich auf die konkrete Erfüllung dieser Vorgaben, was durch eine regelmässige Kontrolle seitens der Informationssicherheitsverantwortlichen sowie durch interne Audits

sichergestellt werden muss. Eine angemessene Dokumentation und das vorhandene Sicherheitsbewusstsein von Mitarbeitenden und Führungskräften sind für die Compliance-Sicht ebenfalls von wesentlicher Bedeutung.

Wichtig ist, dass bezüglich des Managements der Informationssicherheit systematisch vorgegangen wird und die Informationssicherheit demnach systematisch definiert, gesteuert, kontrolliert, aufrechterhalten und fortlaufend verbessert wird. Die Grundprinzipien des Konzepts 'Informations- und Informatik-Risikomanagement', die bereits heute als Grundlage für das Informations- und Informatik-Risikomanagement der kantonalen Verwaltung und im Sinne einer Empfehlung für die Gerichte gelten, werden nunmehr in ein Gesetz im formellen Sinn überführt. Dies hebt die Wichtigkeit eines angemessenen Informations- und Informatik-Risikomanagements hervor und weitet auch den Geltungsbereich des Managementprozesses auf den Grossen Rat und die Gerichte aus, wodurch den Anliegen der Informationssicherheit zukünftig in angemessener Weise Rechnung getragen wird.

Bereits heute kann der Regierungsrat gestützt auf § 45 Abs. 4 GAF für alle Aufgabenbereiche Vorgaben zur Führung der Risikominimierung und des internen Kontrollsystems erlassen. Da diese Grundlage jedoch insbesondere infolge seiner Unbestimmtheit nicht als Grundlage für TOM mit Einschränkungen verfassungsmässiger Rechte genügt, ist es angezeigt für das Informationssicherheitsmanagement eine spezialgesetzliche Grundlage zu schaffen.

Zu einem angemessenen und wirkungsvollen Risikomanagement gehört die laufende Beurteilung der Risiken für die Informationssicherheit (Abs. 1 lit. a), das Treffen erforderlicher Massnahmen zur Vermeidung von Risiken oder zur Reduktion auf ein tragbares Mass (Abs. 1 lit. b). Ein wesentliches Element des ISMS ist zudem auch das Management der Restrisiken. Auch mit angemessenen TOM können Restrisiken im Bereich der Informationssicherheit nicht gänzlich verhindert werden. Das Management von Risiken ist zwar Bestandteil eines ISMS, dennoch erscheint es wichtig, dass die Behörden bestimmen, wie ihre unterstellten Organisationen mit Risiken umgehen sollen, welche Risiken sie ohne Weiteres tragen dürfen und welche Risiken der Behörde rapportiert werden müssen (Risikoakzeptanz; Abs. 1 lit. c). Auch wenn die meisten Risiken der Informationssicherheit auf der operativen Ebene (Departement, Amt oder sogar unterstellte Einheit) behandelt und getragen werden können, können bestimmte Risiken eine strategische Ausprägung haben. Solche Risiken sollen zumindest der betroffenen Behörde kommuniziert, wenn nicht gar durch diese getragen werden. Dies ist insbesondere der Fall bei Risiken in Zusammenhang mit Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz». Der gefällte Entscheid ist zudem regelmässig zu überprüfen. Nur so kann sichergestellt werden, dass die zuständige Organisationseinheit ihrer Verantwortung auch tatsächlich nachkommt und dies nicht faktisch an die ausführenden Stellen oder die Berater (CISO, Rechtsdienst etc.) delegiert. Zu beachten ist dabei selbstverständlich immer, dass auch betreffend das Management der Restrisiken der Schutzgedanke nicht die jederzeit alles überragende Leitlinie staatlichen Handelns sein soll. Vielmehr gilt es auch hier stets die Verhältnismässigkeit zu beachten.

Die Informationssicherheit soll künftig vermehrt mittels ISMS risikoorientiert, systematisch und im Rahmen eines Plan-Do-Check-Act-Zyklus angegangen werden. Die Risikoanalysen erlauben es, die Schutzobjekte und -ziele zu katalogisieren und entsprechende Massnahmen konkret zu definieren. Der kontinuierliche Evaluations- und Verbesserungsprozess schafft Verbindlichkeit und ermöglicht es, neue Herausforderungen und Schutzbedürfnisse rasch zu adressieren und Massnahmen entsprechend anzupassen.

Absatz 2 trägt der Tatsache Rechnung, dass die absolute Sicherheit ein unerreichbares Ideal ist. Der Aufwand für die Behebung verbleibender kleinerer Sicherheitslücken kann unverhältnismässig hoch werden. Die zuständigen Behörden müssen daher darauf achten, dass ihre Massnahmen risikoorientiert und effizient sind. Entsprechend ist bei der Verfolgung der Schutzmassnahmen von den übergeordneten Stellen eine Güterabwägung zwischen Sicherheitskosten und -nutzen vorzunehmen, indem die Grundsätze der Zweckmässigkeit, der Wirtschaftlichkeit und der Benutzerfreundlichkeit berücksichtigt werden. Schliesslich muss die Verwaltung operativ sein und darf sich nicht durch die

festgestellten Risiken paralysieren lassen. Auch das Funktionieren der Verwaltung stellt letztlich ein hohes Ziel dar. Damit ist auch immer eine Einschätzung der Bedrohungslage, der Risikolage und des objektiv einschätzbaren Schädigungsinteresses Dritter vorzunehmen.

7.3.3 Vorgehen bei Verletzungen der Informationssicherheit und Prävention

7.3.3.1 § 7 Früherkennung und Vorsorgeplanung

§ 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.
[4] Das Vorgehen bei Verletzungen der Informationssicherheit und das Ergreifen präventiver und prädiktiver Massnahmen zu deren Minimierung sind kontinuierlich zu üben beziehungsweise zu evaluieren.

Es kann nie gänzlich ausgeschlossen werden, dass es zu Vorfällen im Bereich der Informationssicherheit kommt. Es ist deshalb notwendig, einen einheitlichen und effektiven Ansatz für den Umgang mit solchen Vorfällen vorzusehen.

Die Behörden müssen die erforderlichen Massnahmen treffen, um Informationssicherheitsvorfälle überhaupt und frühzeitig identifizieren zu können (Abs. 1). Dies kann beispielsweise durch regelmässige Kontrollen, Sensoren, Alarmanlagen, Netzwerküberwachung sowie durch regelmässige Auswertung von Log-Files erfolgen. Sie müssen zudem ein Verfahren festlegen, welches anzuwenden ist, wenn Vorfälle oder Schwachstellen identifiziert werden, und zudem klare Zuständigkeiten für die Behandlung der Vorfälle zuweisen. Interne und externe Mitarbeitende müssen im Weiteren wissen, wie sie beim Eintreten eines Ereignisses zu reagieren haben, damit dessen Auswirkungen minimiert werden können. Die Behörden müssen zudem auch dafür sorgen, dass die Ursachen eines Vorfalls jeweils abgeklärt und ausgewertet werden, um daraus entsprechende Lehren für die Zukunft zu ziehen.

Die Behörden müssen darüber hinaus alle notwendigen Vorkehrungen treffen, damit sie ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen können (sog. Business-Continuity-Management, BCM; Abs. 2). Die Erfüllung aller Aufgaben der Behörden hängt unweigerlich vom zuverlässigen Einsatz der Informatikmittel ab. Daher ist es erforderlich, dass die Behörden die aus ihrer strategischen Sicht unverzichtbaren Aufgaben identifizieren und für den Fall einer schwerwiegenden Verletzung der Informationssicherheit (z.B. dauernder Ausfall eines Systems) Vorsorgeplanungen erstellen und auch entsprechende Übungen durchführen lassen. Weil sich die Risiken und die daraus folgenden Verletzungen der Informationssicherheit laufend ändern können, sind auch die Vorsorgeplanungen periodisch zu überprüfen und zu aktualisieren. Die Vorsorgeplanung sieht unter anderem die Bildung von Notfall-Teams, die Definierung von Meldewegen für die Störfall-Eskalation sowie die Bereitstellung von Ressourcen, die zur Bewältigung des Störfalls eingesetzt werden können, vor. Notfallpläne, Krisenmanagementpläne, Krisenvorsorgemassnahmen, Krisenkommunikationsvorbereitung sowie das Trainieren von möglichen Szenarien gehören heute zu einer zwingend notwendigen BCM-Kultur eines jeden Unternehmens.

Auch gute BCM-Massnahmen sind dem steten Wandel ausgesetzt, namentlich können sich Bedrohungen verändern, aber auch interne Prozesse und Strukturen können geändert werden. Die Absätze 3 und 4 konkretisieren das BCM deshalb insoweit, als dessen Prozesse und Massnahmen im Sinne einer ständigen Aufgabe kontinuierlich zu prüfen sind und bei Feststellung sicherheitsrelevanter Defizite entsprechende Massnahmen einzuleiten sind. Es gilt dabei, Wirksamkeit,

Angemessenheit und die Aktualität von Dokumenten zu überprüfen und Hinweise für Verbesserungsmöglichkeiten zu gewinnen. Zudem ist das spezifische Vorgehen bei sicherheitsrelevanten Vorfällen zu üben und die Massnahmen, die in einem solchen Fall zu ergreifen sind, kontinuierlich zu evaluieren, indem deren Aktualität hinterfragt und neue Entwicklungen erkundet werden.

Insbesondere das Vorgehen bei Verletzungen der Informationssicherheit ist kontinuierlich zu üben beziehungsweise zu evaluieren (Abs. 4). Die diesbezüglich zu ergreifenden Massnahmen sind einerseits präventiver Natur, mithin Massnahmen, die darauf abzielen, Risiken zu verringern oder schädliche Folgen abzuschwächen. Dies kann beispielsweise mittels Verschlüsselung oder durch Einsatz von Firewalls geschehen. Andererseits kommen auch sog. prädiktive Massnahmen zum Zug. Im Gegensatz zu den vorbeugenden Massnahmen versuchen prädiktive Massnahmen mit voraussagender beziehungsweiser vorausschauender Wirkung Verletzungen der Informationssicherheit zu verhindern. In diesem Kontext kann man die Methode der Anomalieerkennung erwähnen, die das Erkennen jeglicher Abweichung in einem Netzwerk von einem Standard bezweckt. Als weitere prädiktive Massnahmen kommen das SIEM (Ansatz zur zentralen Sammlung und Analyse von Daten aus verschiedenen Quellen in Echtzeit, das es ermöglicht, Bedrohungen schneller zu erkennen und zu reagieren, indem wichtige Informationen aus verschiedenen Quellen korrekt analysiert werden) und Penetrationstests durch sog. "gute" oder "ethische" Hacker in Betracht (sog. Bug Bounty-Programme). Selbstverständlich ist auch das Ergreifen dieser Massnahmen kontinuierlich zu üben und zu evaluieren.

7.3.4 Klassifizierung

7.3.4.1 § 8 Grundzüge der 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,

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.

Die Klassifizierung von Informationen beziehungsweise die Einstufung von Informatikmitteln bildet einen wesentlichen Grundstein für die Umsetzung des ISMS. Sie dient der bedarfsgerechten Ausrichtung der TOM. Heute findet sich die Grundlage zur Klassifizierung von Informationen und zur Feststellung des Schutzbedarfs in der Informationssicherheitsstrategie und die Details im von der Informatikkonferenz am 9. Juni 2021 beschlossenen Standard "Datenklassifikation des Kantons Aargau" (vgl. hierzu auch Kapitel 4.1). Bei der Klassifizierung wird der Schutzbedarf von Informationen hinsichtlich einer Beeinträchtigung der zu schützenden Interessen beurteilt. Sie bildet die Basis für die weiteren Massnahmen zum Schutz der Informationssicherheit (TOM). Die Grundzüge, das Verfahren und die Zuständigkeiten der Klassifizierung von Informationen sind einerseits mit Blick auf die Wichtigkeit der Klassifizierung für die Informationssicherheit in einem Gesetz im formellen Sinn zu regeln.

Das Ziel, dass bei allen kantonalen Behörden und den ihnen unterstellten Organisationen die Klassifizierung von Informationen einheitlich erfolgt, kann nur durch eine formell-gesetzliche Grundlage erreicht werden. Zu den Grundzügen der Klassifizierung gehören dabei neben der Klärung der Frage, welche Informationen überhaupt zu klassifizieren sind (Abs. 1), insbesondere auch Regelungen

betreffend die Klassifizierungsstufen (Abs. 2), die Zuständigkeiten (§ 9), mithin auch die Zuständigkeit zur Änderung von Klassifizierungen und den Zugang zu klassifizierten Informationen (§ 10).

Zur Klärung der Frage, welche Informationen überhaupt zu klassifizieren sind, nimmt § 8 direkten Bezug auf die in § 1 Abs. 2 lit a und b umschriebenen und durch Klassifizierung zu schützenden öffentlichen Interessen. Der Verweis auf diese Interessen ist jedoch ausdrücklich eingeschränkt, zumal der Schutz der öffentlichen Interessen gemäss Litera c keinen eigenen Grund zur Klassifizierung darstellt. Mit dem Schutz dieses Interesses soll nämlich die rechtmässige Bearbeitung von Informationen sichergestellt werden, deren Schutz in anderen Gesetzen vorgesehen oder mit Dritten durch Vertrag vereinbart wird. Personendaten, welche bereits durch die Datenschutzgesetzgebung oder Vertragsinhalt, das durch das Geschäfts-, Fabrikations- oder Berufsgeheimnis geschützt sind, werden demnach grundsätzlich nicht klassifiziert, es sei denn, dass einzelne Informationen zum Schutz eines Interesses gemäss § 1 Abs. 2 lit. a und b klassifiziert werden müssen. Dasselbe gilt für Informationen, die bei den Gerichten oder Staatsanwaltschaften im Rahmen ihrer ordentlichen Verfahren bearbeitet werden. Die Mehrheit dieser Informationen sind Personendaten, die zwar schützenswert sind, die aber aufgrund des vorliegenden Gesetzes nicht klassifiziert werden müssen. Hingegen können die besonderen Massnahmen, die zum Schutz solcher Informationen getroffen werden, klassifiziert werden (zum Beispiel ein Informationssicherheitskonzept).

In der Praxis geht man generell von vier Klassifizierungsstufen aus (öffentlich, intern, vertraulich und geheim), die jeweils unterschiedliche Regelungen und Bedingungen mit sich bringen. Angesichts des geltenden Öffentlichkeitsprinzips kann auf die Klassifizierungsstufe "öffentlich" verzichtet werden. Der Öffentlichkeitsgrundsatz bildet eine wesentliche Voraussetzung für eine wirksame Kontrolle der staatlichen Behörden. Gestützt darauf sind Informationen grundsätzlich öffentlich, wenn dem nicht überwiegende öffentliche oder private Interessen entgegenstehen. Ist folglich eine Information nicht klassifiziert, ist sie automatisch als öffentlich einzustufen. Gesetzlich soll demnach ein dreistufiges Klassifikationsschema implementiert werden (Abs. 2). Die Klassifizierungsstufe hängt von der Sensibilität der Informationen ab. So sind interne Informationen von mittlerer Sensibilität, es geht mithin um Dateien und Daten, die zwar nicht öffentlich zugänglich sein sollen, bei denen eine Datenverletzung zwar das öffentliche Interesse gemäss § 1 Abs. 2 lit. a und b beeinträchtigen könnte (lit. a), jedoch kein gravierendes Risiko darstellen würde. Hier sind wie bei den hoch sensiblen Daten Zugriffskontrollen notwendig, aber eine grössere Zahl an Nutzern haben Zugriff. Dagegen müssen vertrauliche und geheime Informationen mit einer hohen Sensibilität besonders geschützt und getrackt werden, um sie vor Bedrohungen zu schützen, weil eine Datenverletzung das öffentliche Interesse gemäss § 1 Abs. 2 lit. a und b erheblich (lit. b) beziehungsweise auf schwerwiegende Art und Weise (lit. c) beeinträchtigen könnte. Die Zahl der Nutzer, die auf Informationen mit solch strengen Zugriffskontrollen zugreifen können, sollte zwingend reduziert werden, bei geheimen Informationen auf das absolut notwendige Minimum.

Die erwähnten Qualifizierungen stellen unbestimmte Rechtsbegriffe dar, die unter Berücksichtigung der in der Praxis vorkommenden Risiken noch zu konkretisieren sind. Zudem muss nebst dem Kriterium der Schwere der potenziellen Beeinträchtigung der Interessen gemäss § 1 Abs. 2 lit. a und b auch eine vernünftige kausale Verbindung zwischen der unberechtigten Kenntnisnahme der Information und der potenziellen Beeinträchtigung der geschützten Interessen vorliegen. Erforderlich ist somit, dass auch die Eintrittswahrscheinlichkeit des Schadens berücksichtigt wird. Die Klassifizierung einer Information entspricht also dem Ergebnis einer Risikobeurteilung und soll somit den tatsächlichen Schutzbedarf dieser Information wiedergeben.

Eine Beeinträchtigung der öffentlichen Interessen gemäss § 1 Abs. 2 lit. a und b ist nicht einfach vernachlässigbar, sondern kann vielmehr zu einem spürbaren Schaden führen. Bei Informationen kann der Schwellenwert für die Klassifizierung "intern" relativ rasch erreicht werden. Zu denken ist beispielsweise an Sicherheitsunterlagen zu Informatikmitteln oder interne Mitberichte. Der Ausdruck "erhebliche" Beeinträchtigung geht von einem beträchtlichen, gewichtigen potenziellen Schaden aus. Das ist der Fall, wenn dem Kanton ein erheblicher finanzieller Schaden entstehen kann, die freie

Meinungs- und Willensbildung der Behörden vorübergehend oder die Erfüllung bestimmter Aufgaben über längere Zeit erheblich erschwert werden. Mit "schwerwiegender" Beeinträchtigung wird ein maximales Schadenspotenzial mit katastrophalen Folgen für den Kanton definiert. Dies kann der Fall sein bei einer Behörde, die über längere Zeit entscheidungs- und handlungsunfähig ist, wenn Leib und Leben der Bevölkerung oder von Bevölkerungsgruppen gefährdet sind, das Erbringen unverzichtbarer Dienstleistungen durch kritische Infrastrukturen nicht mehr gewährleistet ist oder wenn der Kanton einen schwerwiegenden finanziellen Schaden erleiden würde.

Bei der Beurteilung des Schutzbedarfs von Informationen politischer Natur ist besondere Zurückhaltung geboten. In einer modernen Demokratie gehört es zur normalen Regierungstätigkeit, dass politische Ideen, Vorschläge, Konzepte und Entscheide in der Öffentlichkeit besprochen und gegebenenfalls (auch heftig) kritisiert werden. Die Klassifizierung darf also nicht dazu dienen, bestimmte Sachverhalte der öffentlichen Debatte zu entziehen, wenn kein überwiegendes öffentliches Interesse dafür besteht.

Wie bereits erwähnt, sollte aufgrund des Öffentlichkeitsprinzips die Öffentlichkeit der Informationen der Norm entsprechen. Die Klassifizierung von Informationen ist zwar zu deren Schutz notwendig, jedoch soll sie eben nur bei effektivem Schutzbedarf vorgenommen werden. Eine Klassifizierung ist deshalb auf die tiefste erforderliche Klassifizierungsstufe, auf das Notwendige zu beschränken und wenn immer möglich auch in zeitlicher Hinsicht zu beschränken (Abs.3). Der Schutzbedarf von Informationen nimmt mit der Zeit oftmals ab oder erübrigt sich nach einem bestimmten Ereignis wie die Veröffentlichung eines Berichts. Eine Klassifizierung erübrigt sich in einem solchen Fall. Es muss sichergestellt sein, dass Informationen nicht unnötig klassifiziert bleiben. Spätestens im Zeitpunkt des Anbietens an das Staatsarchiv hat eine Überprüfung des Schutzbedarfs zu erfolgen.

7.3.4.2 § 9 Zuständigkeiten

§ 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.

Gesetzlich wird lediglich festgehalten, dass Informationen zu klassifizieren beziehungsweise einer Klassifizierungsstufe gemäss § 8 Abs. 2 lit. a-c zuzuweisen sind (Abs. 1). Die Zuständigkeit zur Klassifizierung sollte in aller Regel derjenigen Stelle überlassen sein, die schutzwürdige Informationen in irgendeiner Form festhält oder herausgibt. Nebst dem Verfassen eines Dokuments können auch auf Bild- und Tonträger festgehaltene Informationen klassifizierungswürdig sein. Die in Absatz 1 definierte Stelle vermag den Schutzbedarf der Informationen sowie allfällige Risiken am besten einzuschätzen. Die Behörden können aber im Rahmen des Erlasses von Ausführungsbestimmungen vorsehen, dass die Klassifizierung beispielsweise durch die Behördenleitung, durch eine zentrale zuständige Stelle oder ausschliesslich durch die Linie zu erfolgen hat.

Die Klassifizierung ist grundsätzlich verbindlich. Ist eine Information klassifiziert, wird sie auf ihrem weiteren Weg von dieser Klassifizierung begleitet. Wer Zugang zu einer solchen Information erhält, muss die Vorgaben einhalten, die mit der Klassifizierung verbunden sind. Eine Änderung oder Aufhebung der Klassifizierung darf im Grundsatz nur von derjenigen Stelle vorgenommen werden, welche die Klassifizierung festgelegt hat. Es versteht sich aber, dass auch hier der Dienstweg, die Dienstaufsicht und die entsprechenden Weisungsbefugnisse der vorgesetzten Stellen beziehungsweise der Aufsichtsbehörden zum Tragen kommen (Abs. 2). Letztere können Entscheide der klassifizierenden Stelle gegebenenfalls korrigieren.

7.3.4.3 § 10 Zugang zu klassifizierten Informationen

§ 10 Zugang zu klassifizierten Informationen

[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.

Absatz 1 umschreibt die Voraussetzungen für den Zugang zu klassifizierten Informationen, der wiederum Voraussetzung für das Bearbeiten der entsprechenden Informationen ist. Der Grundsatz "Kenntnis nur, wenn nötig" gilt für jede einzelne klassifizierte Information. Es besteht also kein allgemeines Recht, Zugang zu allen klassifizierten Informationen zu haben. Die Regelung des Zugangs zu klassifizierten Informationen umfasst auch den Zugang zu den Systemen, in denen sich die Informationen befinden. "Gewähr bieten" für einen sachgerechten Umgang setzt voraus, dass die Personen, die klassifizierte Informationen bearbeiten sollen, entsprechend ausgebildet wurden. Ferner müssen sie gegebenenfalls den Nachweis für die Fähigkeit erbringen, die erforderlichen technischen und physischen Sicherheitsmassnahmen einhalten zu können. Für als "vertraulich" oder "geheim" klassifizierte Informationen kann zudem die Durchführung einer PSP eine weitere Bearbeitungsvoraussetzung darstellen (vgl. Erläuterungen zu § 18 Abs. 2, Kap. 7.4.4.2.1). Die Bestimmung richtet sich an alle, die zur Aufgabenerfüllung ermächtigt sind, sei es infolge gesetzlicher Vorgaben (alle in einem Anstellungs- oder Beamtenverhältnis stehenden und die in ein kantonales Gremium gewählten Personen), sei es aufgrund der Vergabe eines öffentlichen Auftrags mittels privatrechtlichen Vertrags oder der Auslagerung einer öffentlichen Aufgabe mittels Leistungsvertrags. In den Ausführungsbestimmungen sind die Modalitäten des Zugangs noch zu regeln.

Absatz 2 statuiert einen – an sich ohnehin zum Tragen kommenden Vorbehalt – wonach in besonderen Verfahren die Spezialgesetzgebung anwendbar bleibt. Es geht um den Zugang zu klassifizierten Informationen des Grossen Rats und der Parlamentsdienste sowie der Gerichtsbehörden und der Staatsanwaltschaft. Hier besteht ein gesetzlich statuiertes hohes, in aller Regel überwiegendes Interesse am Zugang zu einer klassifizierten Information. Das Interesse kann ein solches der parlamentarischen Oberaufsicht sein und damit die Gewaltenteilung betreffen oder aber der Strafverfolgung oder der Durchsetzung des materiellen Rechts dienen. Im Einzelfall wird jeweils eine Interessenabwägung zwischen dem Interesse an der Informationssicherheit und den von den zuständigen Stellen geltend gemachten öffentlichen Interessen durchgeführt werden, soweit dies von der Spezialgesetzgebung vorgesehen ist.

Auch der Inhalt von Absatz 3 hat nicht normativen, sondern rein informativen Charakter. Es ist aber aufgrund des engen Zusammenhangs wichtig rechtsetzerisch klarzustellen, dass klassifizierte Informationen unter die Archivierungsgesetzgebung fallen, sobald sie archiviert worden sind, mithin dieses als lex specialis dem InfoSiG vorgeht. Die Klassifizierung gemäss InfoSiG ist demnach in eine entsprechende Klassifizierung nach den unterschiedlichen Schutzfristen und Einsichtnahmemöglichkeiten gemäss § 46 – 48 IDAG zu überführen. Es bedarf folglich einer Regelung des Übergangs der klassifizierten Informationen ans Staatsarchiv und dessen Modalitäten. Aus diesem Grund wird in Analogie zur bundesrechtlichen Regelung von Art. 12 Abs 3 ISG ein neuer Absatz 4 vorgesehen, der den Regierungsrat ermächtigt, die Entklassifizierung von Archivgut zu regeln.

7.3.5 Vertragliche Überbindung und Kontrolle

7.3.5.1 § 11 Zusammenarbeit mit Dritten

§ 11 Zusammenarbeit mit Dritten

[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.

Die Verwaltung ist im Rahmen ihrer Aufgabenerfüllung häufig auf Leistungen Dritter angewiesen. Als Dritte gelten nach diesem Gesetz Organisationen und Personen des öffentlichen oder privaten Rechts, die nicht zu den Behörden nach diesem Gesetz und deren Verwaltungsorganisationen zu zählen sind und deshalb selbstständig handeln. Es gilt diesbezüglich zwischen der Vergabe eines öffentlichen Auftrags, die zum Abschluss eines privatrechtlichen Vertrags führt, und der Auslagerung öffentlicher Aufgaben, die mittels Abschlusses eines öffentlich-rechtlichen Leistungsvertrags vorgenommen wird, zu unterscheiden. Die auftragserteilenden Stellen haben in beiden Fällen dafür zu sorgen, dass bei der Auftragserteilung und -ausführung die gesetzlich vorgesehenen Massnahmen eingehalten werden. Die einzuhaltenden Sicherheitsmassnahmen werden in aller Regel vertraglich festgehalten, die Drittparteien sind mithin vertraglich zu verpflichten, die Anforderungen und Massnahmen gemäss InfoSiG einzuhalten. Grundsätzlich sollten Beauftragte erst dann Zugang zu Informationen oder zu ICT-Mitteln der Verwaltung erhalten, wenn sie selbst die erforderlichen Massnahmen umgesetzt haben. Entscheidend ist aber auch, dass die auftragserteilenden Stellen die Umsetzung der Massnahmen angemessen (d.h. risikoorientiert) überprüfen. Dies kann zum Beispiel mittels schriftlicher Bestätigung durch eine unabhängige Drittpartei erfolgen, aber unter Umständen auch im Rahmen eines Besuchs vor Ort. Soweit der Auftrag die Ausübung einer sicherheitsempfindlichen Tätigkeit vorsieht, drängt sich für die dienstleistungserfüllenden Personen die Durchführung einer PSP auf (vgl. Erläuterungen zu § 18 Abs. 2, Kap. 7.4.4.2.1).

7.4 Kapitel 3 Technische und organisatorische Massnahmen (TOM)

Kapitel 3 des Gesetzesentwurfs widmet sich den technischen und organisatorische Massnahmen, den sog. TOM. Sie umfassen alle in der Praxis zu treffenden Vorkehrungen zur Gewährleistung der Sicherheit der Informationen und der eingesetzten Informatikmittel. Die Behörden, in deren Aufgabenbereich Informationen bearbeitet werden, sind verpflichtet, die erforderlichen Massnahmen zu treffen, um Risiken zu vermeiden oder auf ein tragbares Mass zu reduzieren. Dabei geht es um dem festgestellten Informationssicherheitsrisiko angemessene organisatorische und technische Massnahmen. Konkret handelt es sich um die zweite Phase des ISMS, um die eigentliche Risikobehandlung. Ziel ist es, in den Grundzügen zu formulieren, was in Bezug auf die konkreten Risiken zu unternehmen ist, um den Anliegen der Informationssicherheit angemessen Rechnung zu tragen. Eine komplementäre Regelung findet sich in § 12 Abs. 1 IDAG, wonach Personendaten – d.h. Daten von natürlichen Personen (vgl. § 3 Abs. 1 lit. d IDAG) – durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten zu schützen sind.

Nebst der Sicherheit beim Einsatz von Informatikmitteln (Kap. 7.4.1) werden physische Massnahmen (Kap. 7.4.2), das Identitäts- und Zugriffsmanagement (Kap. 7.4.3), personelle Massnahmen (Kap. 7.4.4), namentlich die sorgfältige Auswahl, risikogerechte Identifizierung und funktionsgerechte Aus- und Weiterbildung von Personen mit Zugang zu klassifizierten Informationen, Informatikmitteln oder Räumlichkeiten und die Möglichkeit der Verwendung biometrischer Verifikationsmethoden oder der AHV-Versichertennummer (Kap. 7.4.4.1), die PSP (Kap. 7.4.4.2) sowie die sicherheitsspezifische Eignungsprüfung von Unternehmen (Kap. 7.4.5) geregelt. Letztere schafft eine Grundlage, welche die Vergabestellen verpflichtet, im Rahmen von sicherheitsempfindlichen Vergaben die Eignung der Anbietenden in Bezug auf die Informationssicherheit zu prüfen. Alle anderen Massnahmen sind

gängige und wirkungsvolle Instrumente zur Gewährleistung der Informationssicherheit und leiten sich unmittelbar von den internationalen Standards ab.

7.4.1 Sicherheit beim Einsatz von Informatikmitteln

7.4.1.1 § 12 Sicherheitsverfahren

§ 12 Sicherheitsverfahren

[1] Die Behörden legen ein Verfahren zur Gewährleistung der Informationssicherheit beim Einsatz von Informatikmitteln fest.

[2] Das Sicherheitsverfahren umfasst insbesondere

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

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.

Ebenso wie die Klassifizierung von Informationen ist auch die Sicherheit in Bezug auf die zur Verarbeitung von Informationen verwendeten Informatikmittel entscheidend für die Sicherstellung der Informationssicherheit. Hierbei handelt es sich nicht um eine rein technische Angelegenheit, vielmehr ist die überwiegende Mehrheit der Sicherheitsvorkehrungen im Informatikbereich organisatorischer Natur. Jedoch besteht für die kantonale Verwaltung kein gesetzlicher Rahmen, welcher den Einsatz von Informatikmitteln bestimmt und dabei spezifische Verfahren sowie Zuständigkeiten festlegt. Eine solche Regelung ist notwendig, damit weitere Massnahmen im Bereich Informationssicherheit ergriffen werden können (zum Beispiel der Ausbau der PSP oder für den Einsatz von Identitätsverwaltungs-Systemen [Identity and Access Management; IAM]). Dabei gilt es den Wandel in Bezug auf den Betrieb der Informatikmittel zu berücksichtigen. Die Verwaltung bezieht inzwischen sehr oft ihre Informatikleistungen bei hochspezialisierten externen Unternehmen. Dadurch ist eine organisatorische Trennung zwischen Einsatz und Betrieb von Informatikmitteln entstanden, die auch wesentliche Auswirkungen auf die Sicherheit hat.

Das Gesetz legt im Grundsatz fest, welche Aufgaben die leistungsbeziehenden Behörden erfüllen müssen, um ihre Verantwortung in Bezug auf die Sicherheit wahrzunehmen. Die Behörden haben diese Aufgaben in einem sogenannten Sicherheitsverfahren näher zu umschreiben (Abs. 1). Allfällig bereits vorhandene Verfahren müssen systematisiert und wo nötig ergänzt werden. Die wichtigsten Verfahrensetappen müssen auf Verordnungsebene behördenübergreifend vereinheitlicht werden. Das Sicherheitsverfahren muss insbesondere die sicherheitsmässigen Aufgaben, Kompetenzen und Verantwortungen derjenigen Stellen festlegen, die den Einsatz von Informatikmitteln planen und beschliessen. Absatz 2 führt einige Eckpunkte des Verfahrens auf:

- Lit.a: Informatikmittel werden für bestimmte Zwecke und für eine geplante Lebensdauer eingesetzt. Der erste Schritt in Bezug auf die Umsetzung der Informationssicherheit besteht darin, bei der Bestimmung des Einsatzzwecks des Informatikmittels die Geschäftsprozesse zu bestimmen, die mit dem einzusetzenden Informatikmittel unterstützt werden sollen, sowie die Informationen zu identifizieren, die damit bearbeitet werden sollen. Zu diesem Zeitpunkt, noch in der Planungsphase, müssen der Schutzbedarf der Informationen gemäss § 5 Abs. 2 lit. a beurteilt und die möglichen Auswirkungen einer Störung oder eines Missbrauchs des einzusetzenden Informatikmittels in Relation zu den Interessen gemäss § 1 Abs. 2 abgeschätzt werden. Es handelt sich dabei grundsätzlich um eine sogenannte Business-Impact-Analyse, die zwingend von der für den Geschäftsprozess verantwortlichen Stelle durchgeführt werden muss. Im Rahmen der Beurteilung des Schutzbedarfs muss auch berücksichtigt werden, dass Informatikmittel in der Regel in einer bestimmten technischen und logischen Umgebung (sog. Architektur) vernetzt und betrieben werden. Die frühzeitige Identifizierung von Vernetzungen und Abhängigkeiten hilft auch, die Massnahmen dort umzusetzen, wo sie am wirksamsten sind.

  Die Bestimmung bezweckt die Gewährleistung der Informationssicherheit beim Einsatz der vom Kanton beschafften Informatikmittel. Selbstverständlich dürfen die Beurteilung des Schutzbedarfs und die Analyse möglicher Auswirkungen einer Störung oder eines Missbrauchs der einzusetzenden Informatikmittel aber nicht erst vorgenommen werden, wenn deren Einsatz bevorsteht. Vielmehr sind Prüfung und Analyse bereits im Rahmen des Beschaffungsverfahrens erforderlich. Das sollte zwar klar sein, wird aber mit einem entsprechenden textlichen Einschub noch verbindlich präzisiert.

- Lit. b: Informatikmittel werden je nachdem, wie schädlich eine Verletzung der Sicherheit der mit ihnen bearbeiteten Informationen ist, in Sicherheitsstufen eingeteilt (vgl. Ausführungen zu Absatz 3 nachfolgend). Für jede Sicherheitsstufe werden risikoangemessene standardisierte Sicherheitsmassnahmen festgelegt, beispielsweise zum Anmeldeverfahren, zur Verschlüsselung und zum Umgang mit Datenträgern oder Geräten.

- Lit. c: Die Behörden haben festzulegen, welche Massnahmen umgesetzt werden müssen und wie die Umsetzung dieser Massnahmen zu prüfen ist. Grundsätzlich sollen standardisierte Massnahmen zur Anwendung kommen. Die Überprüfung der Umsetzung der Massnahmen ist in diesem Zusammenhang besonders wichtig. So sollte die zuständige Behörde oder Organisation vor dem Einsatz eines Informatikmittels einen Beleg dafür haben, dass das Sicherheitsverfahren rechtmässig stattgefunden hat und die erforderlichen Massnahmen tatsächlich umgesetzt wurden (Konformität).

- Lit. d: Mit der Sicherheitsfreigabe soll sichergestellt werden, dass die zuständige Organisationseinheit vor dem Einsatz eines Informatikmittels die identifizierten Restrisiken kennt und auch bereit ist, diese zu tragen. Ist sie der Meinung, die Restrisiken seien noch zu hoch, kann sie die Freigabe verweigern und die Umsetzung ergänzender risikomindernder Massnahmen verlangen.

- Lit. e: Informationssicherheit verändert sich kontinuierlich. Die Behörden müssen deshalb ein Vorgehen festlegen, um eine Veränderung der Risiken bei bereits eingesetzten Informatikmitteln zu berücksichtigen.

Die Sicherheitseinstufung gemäss Absatz 3 dient zur Identifizierung des Schadenspotenzials eines bestimmten Informatikmittels in Bezug auf die öffentlichen Interessen gemäss § 1 Abs. 2. Das Schadenspotenzial wird von der Schwere des Schadens abgeleitet, der verursacht werden kann, wenn die Informationen, die mit dem betroffenen Informatikmittel bearbeitet werden, oder das Informatikmittel selber missbraucht oder gestört werden. Für die Beurteilung der Schwere des Schadens kann auf die Erläuterungen zu den Klassifizierungsstufen in Kapitel 7.3.4.1, 5. und 6. Abschnitt, verwiesen werden.

- Die Sicherheitsstufe "Grundschutz" gilt für alle Informatikmittel, die keine besonderen Schutzanforderungen aufweisen, und erlaubt die Bearbeitung von Informationen bis und mit der Klassifizierung "intern". Grundschutz gilt demzufolge auch für die öffentlichen Informationen.
- Die Sicherheitsstufe "hoher Schutz»" ist für Informatikmittel mit erhöhtem Schadenspotenzial vorgesehen und erlaubt die Bearbeitung von Informationen bis und mit der Klassifizierung "vertraulich".
- Die Sicherheitsstufe "sehr hoher Schutz" ist für Informatikmittel mit sehr hohem Schadenspotenzial vorgesehen und erlaubt die Bearbeitung von Informationen bis und mit der Klassifizierung "geheim".

Die Zuständigkeit für die Durchführung des Sicherheitsverfahrens obliegt derjenigen Verwaltungseinheit, welche die Informatikmitteln beschafft (Abs. 4). Das gilt auch für gemeinsame Beschaffungen mehrerer Behörden. In aller Regel wird in solchen Fällen eine zentrale Beschaffung durch die IT AG in Betracht kommen. Die Zuständigkeit in der kantonalen Verwaltung obliegt folglich der IT AG für die ICT-Grundversorgung des Kantons und den jeweiligen Abteilungen oder Ämtern für deren Fachapplikationen. Die für den Leistungsbezug verantwortliche Verwaltungseinheit ist letztlich für die Geschäftsprozesse sowie für die Umsetzung der Sicherheitsanforderungen verantwortlich. Sie muss deshalb dem leistungserbringenden Unternehmen ihre Geschäfts- und Sicherheitsanforderungen klar kommunizieren und ihm die Anforderungen und Massnahmen nach diesem Gesetz vertraglich überbinden und deren Umsetzung angemessen überprüfen (vgl. § 11). Damit ist es auch klar, dass die Hauptverantwortung für die Sicherheit im Betrieb von Informatikmitteln auch bei Auslagerung bei der zuständigen Verwaltungseinheit verbleibt. Beauftragte Unternehmen sind ihrerseits dafür zuständig, im Rahmen des Betriebs der kantonalen Informatikmittel die Sicherheit nach dem Stand der Wissenschaft und Technik zu gewährleisten. Sie haben die ihnen vertraglich überbundenen Anforderungen und Massnahmen nach diesem Gesetz zu berücksichtigen und umzusetzen.

7.4.2 Physische Massnahmen

7.4.2.1 § 13 Grundsatz

§ 13 Grundsatz

[1] Die Behörden sorgen in ihrem Zuständigkeitsbereich für einen angemessenen physischen Schutz der Informationen und Informatikmittel.

Die physische Sicherheit ist bei der Erstellung von Schutzzonenkonzepten eine der wichtigsten Verteidigungslinien. Insofern ist die physische Sicherheit für ein umfassendes Verständnis der Informationssicherheit – nicht zuletzt aus dem Blickwinkel der IT-Sicherheit – ein unerlässlicher Baustein. Im Vordergrund der physischen Sicherheit steht in der Regel die Sicherheit von Personen, Gebäuden und materiellen Werten. Zu letzteren gehören heutzutage meist in grossem Umfang Datenbestände, die auf Systemen und Datenträgern innerhalb der eigenen (oder fremder) Gebäude gespeichert, verarbeitet und schliesslich vernichtet werden.

Beim heutigen Betrieb informationsverarbeitender Systeme müssen vielfältige Bedrohungen bedacht werden. Das Spektrum reicht dabei von fahrlässiger oder vorsätzlicher Beschädigung durch Mitarbeitende und Dienstleister über externe Bedrohungen wie Einbrüche und Spionage bis hin zu Naturkatastrophen und Umwelteinflüssen. Als Schadensursachen kommen dabei die Unterbrechung von Versorgungsdiensten (Energie), Umwelteinflüsse (Hitze, Kälte, Feuchtigkeit, Staub, Vibrationen, etc.), Fahrlässigkeit (Aufhalten zu verschliessender Türen durch Mülleimer) oder Vorsatz (Diebstahl, Spionage, Einbruch, Abhören, Vandalismus, Sabotage, Terrorismus, etc.) in Betracht.

Bei den physischen Massnahmen geht es darum, die Risiken durch die dargestellten Bedrohungen zu reduzieren. § 13 legt den Grundsatz fest, dass die Behörden für einen angemessenen physischen Schutz ihrer Informationen und Informatikmittel sorgen müssen. Insbesondere ist der unberechtigte

Zugang zu den Informationen oder Informatikmitteln etwa durch Zugangskontrollen, Videokameras, Schliesssysteme, Sicherheitsbehältnisse, Aktenvernichtungsgeräte usw. zu verhindern. Gegen Elementarschäden werden beispielsweise Brandmeldeanlagen und automatische Löschanlagen eingesetzt. Die Massnahmen des physischen Schutzes betreffen sowohl Informationen und Informatikmittel, die sich in Räumlichkeiten der Verwaltung befinden als auch solche, die öffentlich zugänglich sind. Es handelt sich beim zweiten Fall einerseits um Informationen und Informatikmittel, die von ihrem üblichen Standort (Büro) mitgenommen werden und die anschliessend – ausserhalb des üblichen Sicherheitsperimeters (z.B. Homeoffice) – geschützt werden müssen. Es handelt sich aber auch um Informationen und Einrichtungen, Verkabelungen und Versorgungsleitungen, die nicht unter ständiger Kontrolle stehen. Besondere Aufmerksamkeit muss beispielsweise Zugangspunkten wie Anlieferungs- und Ladezonen geschenkt werden.

Physische Sicherheitsmassnahmen müssen regelmässig mithilfe von Risikoanalysen auf ihre Wirksamkeit überprüft werden.

7.4.2.2 § 14 Sicherheitszonen

§ 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,
c) Taschen- und Personenkontrollen durchführen zu lassen,
d) unangemeldet Raumkontrollen, auch in Abwesenheit der Angestellten, durchführen zu lassen.

Die Ausscheidung bestimmter Räume beziehungsweise Bereiche als Sicherheitszone stellt eine physische Massnahme der Informationssicherheit dar, die bereits heute beispielsweise bei der Kantonspolizei ergriffen wird. Aber auch dort, wo es um den Schutz von Serverräumen (Rechenzentrum) geht, sind entsprechende Massnahmen unabdingbar. Eine Sicherheitszone muss vordefiniert werden, identifizierbar sein und entsprechend geschützt werden. Die Massnahmen in den Sicherheitszonen der jeweiligen Stufen sind risikogerecht auszugestalten. Über ihre tatsächliche Einrichtung entscheidet die Behörde nach einer Risikobeurteilung. Klar ist, dass Sicherheitszonen nur für Informationen und Informatikmittel der höchsten Klassifizierungs- beziehungsweise Sicherheitsstufe gelten soll (Abs. 1 lit. a und b). Steht das Sicherheitsbedürfnis von Gebäuden, Teilen von Gebäuden oder Räumlichkeiten in keinem direkten oder überwiegenden Zusammenhang mit der Informationssicherheit, stehen mithin andere Gründe im Vordergrund, liegt keine Sicherheitszone gemäss § 14 InfoSiG vor (z.B. JVA) und das Ergreifen von Massnahmen lässt sich nicht mit dieser Bestimmung legitimieren.

Absatz 2 regelt die besonderen Befugnisse derjenigen Verwaltungseinheit, die eine Sicherheitszone einrichtet. Die Massnahmen müssen selbstverständlich verhältnismässig sein.

- Das Mitführen bestimmter Gegenstände in eine Sicherheitszone kann eingeschränkt werden, namentlich das Mitführen von Bild- oder Tonaufnahmegeräten (inkl. Smartphones oder Notebooks mit entsprechenden Funktionen) ist in der Regel nur mit besonderer Bewilligung erlaubt.
- Bereiche der Sicherheitszone, die für die Informationssicherheit besonders wichtig sind (z.B. die Zutrittszone zu einem besonderen Serverraum, der Administratorarbeitsplatz oder der Archivraum mit "geheim" klassifizierten Informationen), können mittels Videoaufnahmegeräten überwacht werden.

- Beim Ein- oder Ausgang können Taschen- oder Personenkontrollen durchgeführt werden. Damit soll verhindert werden, dass Personen ohne Bewilligung Geräte in die Sicherheitszone mitnehmen oder Informationen (z.B. mit einem USB-Memorystick) entwenden.
- Auch Bürokontrollen sollen im Bereich der Sicherheitszonen möglich sein. Dabei geht es um die Überprüfung der Einhaltung der sogenannten Clean Desk Policy (es dürfen keine schutzwürdigen Informationen auf dem Schreibtisch oder anderswo herumliegen, der PC muss gesperrt oder ausgeschaltet sein, Datenträger müssen unter Verschluss gehalten werden, die Schubladen müssen geschlossen sein, der Abfallkorb darf keine klassifizierten Informationen enthalten, usw.). Die Kontrolle darf auch in Abwesenheit der betroffenen Personen, beispielsweise während der Nacht, stattfinden.

Die Aufzählung ist nicht abschliessend. So könnte auch der Betrieb einer störenden Fernmeldeanlage nach dem Fermeldegesetz (FMG) vom 30. April 1997 (SR 784.10) in Betracht kommen, wenn die Sicherheitszone besonders kritisch ist und das Bundesrecht den Betrieb zulässt.

7.4.3 Identitäts- und Zugriffsmanagement

7.4.3.1 § 15 Identitätsverwaltungssysteme

§ 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.

Das Identitäts- und Zugriffsmanagement (oder auch Berechtigungsmanagement) will sicherstellen, dass stets mit allen Benutzerinnen und Benutzern und deren Daten sicher und bewusst umgegangen wird. Als Basis hierfür dient ein solides Berechtigungs- und Rollenkonzept, das bereits in der Planungsphase konzipiert werden sollte. Ebenso wichtig ist auch eine geregelte Administration des Identitäts- und Zugriffsmanagements, zudem die Ausbildung der Administratorinnen und Administratoren über ein Administrationskonzept und eine Kontrollinstanz, um sicherzustellen, dass Benutzerinnen und Benutzer tatsächlich nur diejenigen Rechte erhalten, die sie effektiv benötigen. Aufgabe eines Identitäts- und Zugriffsmanagements ist es, zum einen die Vielzahl an Identitäten und Berechtigungsprofilen eines Benutzers gegen Missbrauch zu sichern, zum andern sollen die Benutzerdaten für die verschiedenen Anwendungen konsistent, ständig verfügbar und verlässlich bereitgehalten werden, um einen reibungslosen Betrieb zu ermöglichen.

Absatz 1 sieht vor, dass die Behörden für die zentrale Kontrolle von Personen, Maschinen und Systemen, die Zugang zu sicherheitsrelevanten Informationen und Informatikmitteln sowie zu Sicherheitszonen haben, ein solches Identitätsverwaltungssystem betreiben können. Dabei wird absichtlich offengelassen, wie viele solcher zentralen Identitätsverwaltungssysteme eingesetzt werden. Da es den Behörden überlassen ist, wie viele solcher Systeme sie betreiben und wie sie sich organisieren, kann eine Konkretisierung erst im Rahmen der Ausführungsbestimmungen erfolgen. Für jedes System muss jedenfalls eine verantwortliche Stelle bezeichnet werden (Abs. 3).

Absatz 2 beschreibt die Funktionsweise der zentralen Identitätsverwaltungssysteme. Danach wird das Resultat der Prüfung an die angeschlossenen Informationssysteme übermittelt, damit diese die Berechtigungen ermitteln können.

7.4.3.2 § 16 Datenaustausch und -abgleich

§ 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.

Eine wichtige Voraussetzung für das Funktionieren eines Identitätsverwaltungssystems ist die Gewährleistung der Erfassung aller erforderlichen Daten. Zu diesem Zweck ist der Datenaustausch und -abgleich mit anderen Identitätsverwaltungssystemen zu ermöglichen (Abs. 1). Dabei sind Austausch und Abgleich auf Daten zu begrenzen, die im jeweiligen System bearbeitet werden dürfen (Abs. 2). Ein Austausch kommt beispielsweise beim Aufbau eines neuen Identitätsverwaltungssystems zum Tragen. Die dafür notwendigen Identitätsdaten werden diesfalls aus den Personal- und Benutzerverzeichnissen bezogen. Auch beim Anschluss einer Fachapplikation, die bisher die Authentifizierung der Benutzerinnen und Benutzer selbstständig durchgeführt hat, ist ein Austausch möglich. In diesem Fall werden die für die Authentifikation verwendeten Daten an das zentrale Identitätsverwaltungssystem übertragen und dort in die bestehenden Daten eingetragen. Zu diesem Zeitpunkt sind auch die Anforderungen nach Absatz 2 zu überprüfen. Die weiteren Mutationen an den Benutzerdaten werden normalerweise von der Fachanwendung an das Identitätsverwaltungssystem gemeldet. Je nach konkreter organisatorischer Ausgestaltung ist aber für bestimmte Benutzerkreise auch eine zentrale Benutzerverwaltung denkbar. Die häufigste Übermittlung von Daten im Sinne eines Austausches erfolgt jedoch im laufenden Betrieb bei jeder Anmeldung (Login) einer Benutzerin oder eines Benutzers. Das Identitätsverwaltungssystem authentifiziert die Benutzerin oder den Benutzer, komplettiert die von der Fachanwendung verlangten Identitätsdaten aus seinem Verzeichnis (z.B. die Zugehörigkeit zu einem Departement oder Amt) oder aus externen Quellen (z.B. die Funktion als Rechtsanwalt) und stellt diese Daten der Fachanwendung in Form von Bestätigungen zur Verfügung, damit diese über die konkreten Zugriffsberechtigungen befinden kann.

7.4.4 Personelle Massnahmen

7.4.4.1 Auswahl, Instruktion und Berechtigungen

7.4.4.1.1 § 17 Voraussetzungen für den Zugang zu Informationen und Informatikmitteln

§ 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,
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 nach Art. 50c des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) vom 20. Dezember 1946 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.
[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.

Mit der Statuierung von § 17 soll verhindert werden, dass Unbefugte auf Daten lesend oder ändernd zugreifen oder unberechtigt Funktionen in IT-Systemen nutzen. Die sorgfältige Auswahl, die risikogerechte Identifikation, eine optimale, zielgerichtete Instruktion im Sinne einer funktionsgerechten Aus- und Weiterbildung und eine Verpflichtung zur Geheimhaltung und zu besonderer Sorgfalt (Abs. 1 lit. a-d) sind unabdingbare Voraussetzungen für eine Gewährleistung der Informationssicherheit in personeller Hinsicht. Es liegt in der Verantwortung der Anstellungsbehörden beziehungsweise der Verwaltungseinheiten bei Vergaben öffentlicher Aufträge oder bei Auslagerung öffentlicher Aufgaben dafür zu sorgen, dass diesen Anforderungen im Rahmen der Aufgabenerfüllung nachgelebt wird. Bei einer Aufgabenerfüllung durch Dritte ist dies durch vertragliche Überbindung sicherzustellen (vgl. Erläuterungen zu § 11; Kap. 7.3.5.1).

- Bei der Auswahl der anzustellenden oder zu beauftragenden Personen müssen die Auswahlkriterien dem Schutzbedarf der Informationen beziehungsweise der Sicherheitsstufe der Informatikmittel entsprechen. Die Anstellungsbehörden und die Vergabestellen sind für ihre Personalentscheide beziehungsweise für ihre Vergabeentscheide verantwortlich. Auch die Unterstellung einer Person unter die PSP entbindet sie nicht von dieser Verantwortung.
- Da die Verwaltung des Zugangs zu Informationssystemen und Sicherheitszonen zunehmend elektronisch erfolgt, müssen sich Personen, die auf die Infrastruktur des Kantons zugreifen wollen, elektronisch identifizieren lassen (Authentisierung), damit über ihre Zugangsberechtigung entschieden werden kann. Je nach Schutzbedarf der Informationen beziehungsweise Sicherheitsstufe der Informatikmittel sind stärkere oder schwächere Authentisierungssysteme eingesetzt. Beispielsweise kann zusätzlich zu einem Passwort die Überprüfung eines biologischen Merkmals (Fingerabdruck, Augenscan, usw.) verlangt werden.
- Die Aus- und Weiterbildung der Angestellten und die Instruktion und vertragliche Überbindung der Anforderungen nach diesem Gesetz an beauftragte Unternehmen ist für die Informationssicherheit wesentlich. Im Bereich der Informationssicherheit genügt eine einmalige Ausbildung nicht. Die Angestellten müssen regelmässig geschult und sensibilisiert werden. Und besondere Aufmerksamkeit ist der Schulung der Vorgesetzten sowie derjenigen Personen zu schenken, die eine sicherheitsempfindliche Tätigkeit ausüben.
- Die Angestellten müssen ausdrücklich auf die Folgen einer Amtsgeheimnis- oder einer Datenschutzverletzung aufmerksam gemacht werden. Bei Vergaben öffentlicher Aufträge müssen die Geheimhaltungspflicht und die Pflicht zur Einhaltung des Datenschutzes vertraglich überbunden werden. Bereits heute werden Datenschutzrevers von allen mit sicherheitsrelevanten Dienstleistungen beauftragten Personen unterzeichnet. Bei der Auslagerung öffentlicher Aufgaben ist im Leistungsvertrag darauf hinzuweisen, dass die Vertragspartner im Rahmen ihrer Aufgabenerfüllung amtliche Funktionen ausüben und folglich dem Amtsgeheimnis unterstehen. Sie fallen deshalb unter den Anwendungsbereich von Art. 320 StGB. Dies wurde mit der Revision von Artikel 320 StGB, welche mit dem ISG erfolgte, klargestellt.

Die Verwendung von biometrischen Verifikationsmethoden zur Authentisierung von Personen kann zusätzliche Sicherheit bringen. Dabei geht es nicht darum, eine Person aus einer beliebigen Anzahl Personen zu identifizieren, sondern nur darum zu prüfen, ob eine bestimmte Person, die Zugang zu Ressourcen des Kantons verlangt, wirklich diejenige ist, die sie zu sein behauptet. Die Behörden sollen von dieser Möglichkeit für den Zugang zu ihren Ressourcen Gebrauch machen können (Abs. 2). Bereits heute werden verschiedentlich biometrische Verfahren zur Authentifikation eingesetzt, zum Beispiel für den Zugang zu Hochsicherheitstrakten in Vollzugseinrichtungen. Die Zugangsdaten (Sicherheitsrisiko "Kennwort") stellen praxisgemäss eine grosse Schwachstelle eines jeden IT-Systems dar und werden daher regelmässig Ziel von Cyberangriffen. Mittels einer Multifaktor-Authentifizierung, insbesondere unter Verwendung von Biometrie, Gesichtserkennung und Gerätepasswörter, soll sichergestellt werden, dass eine Benutzerin oder ein Benutzer des Systems auch wirklich die Person ist, die sie zu sein vorgibt. Daher werden während des Anmeldevorgangs mehrere Faktoren

eingesetzt, um die Identität einer Person, die Zugriff auf das System erhalten möchte, zu ermitteln. Je mehr Faktoren im Rahmen der Identifizierung zur Anwendung gelangen, umso grösser ist das Vertrauen in deren Echtheit. Eine Zwei-Faktor-Authentifizierung ermöglicht dabei einen flexiblen und umfassenden sicheren Netzwerkzugriff auf besonders sensible Daten und Unterlagen im Büro, unterwegs an einer externen Sitzung oder im Home-Office. Aus Datenschutzgründen sind die biometrischen Daten nach Wegfall der Zugangsberechtigung zwingend zu vernichten.

Absatz 3 schafft zudem die Möglichkeit zur systematischen Verwendung der AHV-Versichertennummer als Personenidentifikator für den Zugang zu Informationen und Informatikmitteln. Für ein Identitätsverwaltungssystem ist es unumgänglich, dass die zu erfassenden Personen fehlerfrei identifiziert werden. Keine Person darf wegen der Übereinstimmung von Erkennungsmerkmalen mit einer anderen verwechselt oder gar – im Bereich der Daten – zusammengeführt werden. Es darf aber auch keine Person wegen nicht erkannter Übereinstimmung doppelt geführt werden. Es ist unbestritten, dass die AHV-Versichertennummer ein sehr gutes Personenidentifikationsinstrument für eine fehlerfreie Identifizierung darstellt.

Seit dem 1. Januar 2022 dürfen die Einheiten der Kantons- und Gemeindeverwaltungen die AHV-Nummer zwar systematisch verwenden, soweit sie zur Erfüllung ihrer gesetzlichen Aufgabe erforderlich ist (Art. 153c Abs. 1 Bst. a Ziff. 3 AHVG) und das anwendbare Recht dies nicht ausdrücklich ausschliesst (Art. 153c Abs. 2 AHVG). Damit braucht es grundsätzlich keine spezialgesetzliche Erlaubnisnorm für jeden einzelnen Verwendungszweck und jeden einzelnen Verwender. Soll die AHV-Nummer systematisch als Personenidentifikator im Bereich der Informationssicherheit verwendet werden, ist dies gemäss Art. 134ter Abs. 1 der Verordnung über die Alters- und Hinterlassenenversicherung (AHVV) vom 31. Oktober 1947 (SR 831.101) der Zentralen Ausgleichsstelle (ZAS) zu melden. Die Meldung muss insbesondere die gesetzliche Grundlage für die systematische Verwendung der AHV-Nummer und die Angabe der gesetzlichen Aufgaben, deren Erfüllung diese systematische Verwendung erfordert, enthalten (vgl. Art. 134ter Abs. 2 Bst. b AHVV).

Es ist fraglich, ob die eher generische Ermöglichung der systematischen Verwendung der AHV-Versichertennummer als Personenidentifikator für den Zugang zu Informationen und Informatikmitteln, wie es Absatz 3 vorsieht, den Voraussetzungen der AHV-Gesetzgebung zu genügen vermag. Es ist zudem fraglich, ob damit die gesetzliche Aufgabe genügend umschrieben ist. Es ist daher eine entsprechende gesetzliche Grundlage für die Verwendung der AHV-Versichertennummer als Personenidentifikator zu schaffen. Eine gesetzliche Grundlage ist ohnehin notwendig, damit nebst der Kantonsverwaltung auch der Grosse Rat und die Gerichte die AHV-Nummer systematisch als Personenidentifikator verwenden können. Im Gegensatz zu Einheiten der Kantonsverwaltung ist für die systematische Verwendung der AHV-Nummer durch Organisationen und Personen des öffentlichen oder privaten Rechts, die nicht der Kantonsverwaltung zugerechnet werden können und die durch Bundesrecht, kantonales Recht oder kommunales Recht oder durch Vertrag mit Verwaltungsaufgaben betraut sind, weiterhin eine spezialgesetzliche Grundlage erforderlich (Art. 153c Abs. 1 Bst. a Ziff. 4 AHVG).

Absatz 4 stellt einen zentralen Grundsatz der Informationssicherheit auf, wonach mit Berechtigungen restriktiv umzugehen ist. Das Prinzip der Datensparsamkeit (so viele Daten wie nötig, so wenige wie möglich) ist auf die Berechtigungen analog anzuwenden. Wer für den Kanton arbeitet oder einen Auftrag ausführt, braucht zur Aufgabenerfüllung unter Umständen einen Zugang zu bestimmten Informationen, Informatikmitteln oder Sicherheitszonen. Sie sollen jedoch nur diejenigen Berechtigungen erhalten, die sie zur Erfüllung ihrer Aufgaben tatsächlich benötigen. Das Risiko eines Missbrauchs kann wesentlich reduziert werden, wenn eine Person nicht ohne Grund Informationen eines anderen Bereichs bearbeiten kann.

Es kommt vor, dass ehemalige Angestellte oder Auftragnehmerinnen und Auftragnehmer nach Beendigung des Arbeitsverhältnisses, des Vertrags oder einer besonderen Aufgabe nicht aufgefordert werden, ihren Schlüssel oder Badge zurückzugeben, oder dass ihr Benutzerkonto nicht gesperrt

wird. Solche ungültigen Berechtigungen könnten in der Folge benutzt werden, um gegen die Interessen des Arbeit- oder Auftraggebers zu handeln. Wenn eine Anstellung, ein Vertrag oder eine Aufgabe beendet ist, müssen die entsprechenden Berechtigungen entzogen werden (Abs. 5, Satz 1). Besteht Grund zur Annahme, dass eine Gefährdung der Informationssicherheit vorliegt, müssen die Berechtigungen sofort gesperrt oder entzogen werden (Abs. 5, Satz 2). Beide Massnahmen sollen insbesondere dazu beitragen, das Risiko einer sog. Innentat zu reduzieren.

7.4.4.2 Personensicherheitsprüfung (PSP)

7.4.4.2.1 § 18 Gegenstand und Voraussetzungen

§ 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.

[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.

[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.

Mit der Regelung der Personensicherheitsprüfung (PSP; §§ 18 ff.) wird eine ausdrückliche gesetzliche Grundlage dafür geschaffen, um die Vertrauenswürdigkeit anzustellender oder bereits angestellter Mitarbeitenden, zu wählender oder bereits gewählter Beamtinnen und Beamten oder Personen in kantonale Gremien sowie zu beauftragender oder beauftragter Dritter zu überprüfen, die sicherheitsrelevante Tätigkeiten oder wichtige Funktionen ausüben (z.B. Systemadministratorinnen und -administratoren, Personen mit Zugang zu Sicherheitszonen, Richterinnen und -richter). Die Behörden können so namentlich feststellen, ob eine Person wegen Vorstrafen als weniger vertrauenswürdig erscheint oder wegen Schulden potenziell erpressbar ist. Mit dieser organisatorischen Massnahme können die Behörden das Risiko, dass Sicherheitslücken durch vorsätzliches Fehlverhalten der eigenen Mitarbeitenden entstehen, reduzieren.

Absatz 1 umschreibt den Prüfzweck. Die PSP ist eine vorbeugende Massnahme zum Schutz vor sog. Innentäterinnen und Innentätern. Sie soll das Risiko einer Beeinträchtigung der Interessen gemäss § 1 Abs. 2 identifizieren, das mit der Ausübung einer sicherheitsrelevanten Tätigkeit durch eine bestimmte Person verbunden sein könnte. Es geht also um die Einschätzung der Wahrscheinlichkeit einer vorsätzlichen oder fahrlässigen Verletzung der Informationssicherheit des Kantons durch eine bestimmte Person.

In Absatz 2 geht es um die Voraussetzungen für die Durchführung einer PSP. Die Durchführung ist möglich, wenn die PSP eine dem Sicherheitsrisiko, das mit dem Einsatz der geprüften Person in Zusammenhang steht, angemessene Schutzmassnahme ist. Damit wird klargestellt, dass die Anordnung einer PSP verhältnismässig sein muss. Die entsprechende Risikobeurteilung ist von der verantwortlichen Behörde im Rahmen ihres Risikomanagements vorzunehmen. Sie entscheidet letztlich, ob

sie ein allfälliges erhöhtes Risiko tragen, ob sie dieses mit bestimmten Auflagen reduzieren oder ob sie es beispielsweise durch Nichtanstellung oder Kündigung vermeiden will. Die Anwendungsfälle von lit. a-c sind lediglich beispielhaft und nicht abschliessend: eine PSP ist demnach möglich, wenn die geprüfte Person bei ihrer Tätigkeit häufig oder in grossem Umfang Zugang zu sicherheitsrelevanten Informationen (lit. a), weitreichenden Einblick in wichtige politische oder sicherheitsrelevante Geschäfte (lit. b) oder regelmässig oder unbegleitet Zugang zu Sicherheitszonen gemäss § 14 (lit. c) hat. Es kommen selbstverständlich weitere Gründe in Betracht.

Gleichzeitig wird in Absatz 2 festgehalten, dass es für die Durchführung eines Antrags einer hierfür zuständigen Stelle oder eines wahlvorbereitenden Gremiums bedarf. Ausgehend von den in § 19 Abs. 1 lit. a-c vorgesehenen Anwendungsfällen (Angestellte, Beamtinnen und Beamte, Mitglieder eines kantonalen Gremiums sowie Dritte im Auftrag oder in Erfüllung einer öffentlichen Aufgabe), werden die in Frage kommenden zuständigen Stellen und Gremien ausdrücklich erwähnt. Im Falle einer Anstellung von Kantonspersonal ist die PSP von der Anstellungsbehörde einzuleiten, die dann auch mit dem Ergebnis der PSP (§ 22) über die Anstellung entscheidet. Anders die Ausgangslage bei den Beamtinnen und Beamten, die vom Regierungsrat gewählt werden. Der Antrag hat hier vom wahlvorbereitenden Departement auszugehen, wohingegen der Entscheid selbstredend der Wahlbehörde, dem Regierungsrat, obliegt. Bei der Wahl von Beamtinnen und Beamte durch den Grossen Rat und von Personen in kantonale Gremien geht der Antrag vom wahlvorbereitenden Gremium aus und der Entscheid obliegt der Wahlbehörde. Bei Wahlen des Grossen Rats erfolgt die Wahlvorbereitung durch eine Kommission. Bei der Durchführung einer PSP mit privaten Dritten ist zu unterscheiden, ob es sich um die Auslagerung einer öffentlichen Aufgabe oder um die Vergabe eines öffentlichen Auftrags handelt. Die PSP im Zusammenhang mit der Vergabe ist von der Vergabestelle einzuleiten und auch der Entscheid obliegt der Vergabestelle, zumal der Entscheid im Rahmen eines Vergabeverfahrens gefällt wird. Bei der Beauftragung Dritter aufgrund der Auslagerung einer öffentlichen Aufgabe hat die Einleitung der PSP durch dasjenige Departement zu erfolgen, das die Aufgabe auslagern möchte. Der Entscheid wird dann schliesslich durch den Regierungsrat im Rahmen des Entscheids über die Auslagerung gefällt, zumal der Regierungsrat gemäss § 9 des Organisationsgesetzes für die Übertragung von Teilen des Vollzugs öffentlicher Aufgaben an Dritte zuständig ist.

In Absatz 3 wird der Prüfungsinhalt der PSP festgehalten, mithin die Frage beantwortet, welche Daten zur Beurteilung des Risikos bearbeitet werden dürfen. Erfahrungsgemäss hat eine Gefährdung oder Verletzung der Informationssicherheit durch eine bestimmte Person einen Ausgangspunkt, der zeitlich zurückliegt und auf bestimmte persönliche Umstände zurückzuführen ist. Es sind in der Regel persönliche, insbesondere finanzielle Schwierigkeiten oder verheimlichte Beziehungen, die Situationen schaffen können, die dem Kanton erheblichen Schaden zufügen. Deshalb wird im Rahmen der PSP die Lebensführung der zu prüfenden Person unter die Lupe genommen. Die in Absatz 3 aufgeführten persönlichen Umstände über die Lebensführung (enge persönliche Beziehungen und familiäre Verhältnisse, Straffälligkeit und finanzielle Lage) sind dabei nicht abschliessend.

Die Durchführung der PSP erfordert grundsätzlich die ausdrückliche Einwilligung der betroffenen Person. Gleichzeitig hat sie aber bei Einwilligung auch eine Mitwirkungspflicht (Abs. 4). Danach hat die zu prüfende Person an der Sachverhaltserhebung mitzuwirken. Nebst der Auskunftserteilung anlässlich der Befragung sind weiterführende und für den Zweck der PSP hilfreiche Unterlagen einzureichen. Insbesondere notwendig ist die Mitwirkung zur Abklärung der persönlichen Umstände und Verhältnisse, die ohne Mitwirkung nicht ohne weiteres erkennbar sind. Die befragte Person muss ihre Antworten wahrheitsgemäss erteilen. Die ganze Sicherheitsprüfung wäre illusorisch, wenn Fragen nach Alkohol- oder Betäubungsmittelmissbrauch, nach persönlichen Schulden, nach Nebenbeschäftigungen und ähnlichem unter Berufung auf die Grundrechte nicht beantwortet werden müssten und entsprechende Erkenntnisse aufgrund dessen nicht in die Beurteilung des Sicherheitsrisikos einfliessen würden. Zwar ist es der zu prüfenden Person insbesondere anlässlich der Befragung unbenommen, bestimmte Fragen nicht beantworten zu wollen. Es ist dann aber Aufgabe der Behörden,

die Auskunftsverweigerung oder auch die Verweigerung der Einreichung weiterer Dokumente entsprechend zu würdigen.

Wenn für die betroffene Person bereits eine PSP in den letzten zwei Jahren durchgeführt worden ist, soll aus Gründen der Wirtschaftlichkeit keine neue Prüfung durchgeführt werden (Abs. 5). Es besteht zwar eine Wahrscheinlichkeit, dass sich die Verhältnisse im Laufe der Zeit ändern können und ein Sicherheitsrisiko nach erfolgter PSP entstehen kann. Aus diesem Grund wird ein kurzes Zeitfenster von zwei Jahren gewählt, innert dem ein Verzicht auf die PSP möglich ist.

Im Rahmen des Erlasses von Ausführungsbestimmungen gilt es zu prüfen, ob es mehrerer oder zumindest zweier Prüfstufen bedarf. Ist die für die Reinigung der Räumlichkeiten einer Sicherheitszone zuständige Person der gleichen Prüfung zu unterziehen wie das obere Kader, das regelmässig Zugang zu sicherheitsrelevanten Informationen und Einblick in wichtige politische Geschäfte hat? Massgebend für den Entscheid, ob mehrere Prüfstufen erforderlich sind und folglich eingeführt werden sollen, ist zum einen die tatsächliche Sicherheitsrelevanz der betroffenen Funktion, zum andern die Verhältnismässigkeit einer erhöhten Prüfung. Die Verhältnismässigkeit ist jedenfalls spezifisch zu beachten. Dies ergibt sich aus der Formulierung, wonach nur die "notwendigen und in einem engen Zusammenhang zur Aufgabenerfüllung" stehenden Daten erhoben werden dürfen (vgl. § 21 Abs. 1). Diese Formulierung gibt der Fachstelle PSP eine klare Leitlinie, um die Datenerhebung jeweils fallbezogen vorzunehmen, was auf den ersten Blick eher gegen eine Statuierung mehrerer oder zumindest zweier Prüfstufen spricht.

7.4.4.2.2 § 19 Personenkreis

§ 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.

[2] Von Abs. 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.

Absatz 1 legt fest, wer sich einer PSP unterziehen muss und zu welchem Zeitpunkt (Abs. 1 lit. a-c). Der Personenkreis umfasst die Angestellten und die Beamtinnen und Beamten der Kantonsverwaltung (lit. a) und Personen, die sich zur Wahl in ein Amt oder in ein kantonales Gremium stellen (lit. b). Diesbezüglich kommen nicht nur Volkswahlen, sondern auch Wahlen durch den Grossen Rat und den Regierungsrat in Betracht. Bei Privaten kommt eine PSP bei der Auslagerung öffentlicher Aufgaben und bei der Vergabe öffentlicher Aufträge zum Tragen (lit. c).

In Bezug auf den Zeitpunkt ist eine PSP jeweils immer vor Antritt einer Stelle oder vor einer Wahl oder vor Erteilung eines Auftrags beziehungsweise vor Auslagerung einer Aufgabe durchzuführen. Selbstverständlich muss aber auch die Möglichkeit bestehen, während der Anstellungs- oder Amtsdauer oder während der Aufgabenerfüllung eine PSP zu beantragen, wenn Anlass dazu besteht (vgl. hierzu die Erläuterungen zu § 23 Abs. 2 unter Kap. 7.4.4.2.6).

Von der Regelung von lit. b sollen die politischen Behörden Grosser Rat und Regierungsrat ausgenommen sein, auch wenn diese Personen im Rahmen ihrer Funktion oft Einblick in überaus sicherheitsempfindliche Informationen erhalten, sowie die Richterinnen und Richter. Dies entspricht der Regelung des Bundes, der ebenfalls die Mitglieder des Parlaments, des Bundesrats und des Bundesgerichts ausnimmt. Eine Ausnahme rechtfertigt sich, weil Politikerinnen und Politiker im Brennpunkt der Öffentlichkeit stehen. Deren Leben und Wirken wird von den Medien durchleuchtet, sodass die Wählerinnen und Wähler sich ein Bild von den Kandidierenden machen können. Bei den Mitgliedern der Justiz rechtfertigt sich eine Ausnahme aufgrund deren institutioneller Stellung und folglich aus Gleichbehandlungsgründen zu den anderen Behörden. Dazu kommt, dass die überwiegende Mehrheit der Informationen, die bei den Gerichten im Rahmen ihrer Aufgabenerfüllung bearbeitet werden, schützenswerte Personendaten und folglich nicht klassifizierte Daten sind. Der Schutz dieser Informationen wird durch das Amtsgeheimnis, das Datenschutzgesetz sowie generell in den Prozessgesetzen geregelt. Das legitime öffentliche Interesse nach vertrauenswürdigen und integren Personen in der Justiz ist ausreichend durch die geltenden Bestimmungen im GOG abgedeckt.

Die Behörden müssen für ihren Bereich eine Liste derjenigen Funktionen erlassen, welche die Ausübung einer sicherheitsrelevanten Tätigkeit erfordern und deren Funktionsträgerinnen und Funktionsträger somit geprüft werden müssen. Diese Liste ist periodisch zu aktualisieren (Abs. 3).

Mit Absatz 4 wird klargestellt, dass Kantonspersonal von Bundesrechts wegen einer PSP des Bundes unterstehen kann, wenn es klassifizierte Informationen des Bundes bearbeitet oder auf Informatikmittel des Bundes zugreift. In diesen Fällen sind die Bestimmungen des ISG auch für Mitarbeitende des Kantons anwendbar.

7.4.4.2.3 § 20 Zentrale Fachstelle für PSP

§ 20 Zentrale Fachstelle für PSP

[1] Die Kantonspolizei führt als zentrale Fachstelle PSP durch.

[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.

Für die Durchführung der PSP ist eine zentrale Fachstelle zu bezeichnen (Abs. 1). Es ist wichtig, dass die Stelle, welche die PSP durchführt, das Risiko für die Informationssicherheit möglichst objektiv, mithin gestützt auf die erhobenen Daten sowie nach dem Stand der Wissenschaft und Rechtsprechung beurteilen können muss. Entsprechend darf sich die Führungslinie nicht in das Prüfverfahren einmischen, ansonsten die Gefahr besteht, dass die PSP für persönliche oder politische Zwecke missbraucht wird. Die Fachstelle PSP muss demzufolge in ihrer Beurteilung unabhängig, weisungsungebunden sein. Durch eine zentrale Fachstelle kann dieses Ziel viel eher erreicht werden als durch eine dezentrale Lösung. Die Kompetenzstellenlösung führt zudem auch zu einer Bündelung von Know-how und trägt zu einer einheitlichen Praxis bei. Bereits heute werden PSP zum Teil zentral durch Spezialistinnen und Spezialisten der Kantonspolizei durchgeführt. Dazu kommt, dass ein Zugriff gemäss § 21 Abs. 1 lit. c und d ohnehin nur den Polizeikräften zusteht. Da auf die Möglichkeit des Zugriffs auf die entsprechenden Quellen nicht verzichtet werden sollte, kommt einzig die Kantonspolizei als zentrale Fachstelle für PSP ernsthaft in Betracht. Aus diesem Grund soll deren Zuständigkeit gesetzlich festgehalten werden.

Wie in § 18 Abs. 2 klargestellt, braucht es für die Durchführung der PSP stets eines Auftrags einer Stelle oder eines Gremiums (vgl. Kapitel 7.4.4.2.1, 4. Abschnitt). Die Fachstelle PSP kann nicht von sich aus eine PSP einleiten und durchführen.

Mit Absatz 2 wird der Fachstelle gesetzlich die Möglichkeit eingeräumt, zur Durchführung der PSP ein Informationssystem zu betreiben. In diesem dürfen besonders schützenswerte Personendaten und das Profiling von Personen bearbeitet werden können, wenn dies zur Beurteilung des

Sicherheitsrisikos erforderlich ist. Selbstverständlich kommen hierbei die Vorgaben der Datenschutzgesetzgebung zum Tragen.

7.4.4.2.4 § 21 Datenerhebung

§ 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,
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),
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,
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.

Absatz 1 regelt die Möglichkeit der Datenerhebung, indem die verschiedenen Quellen, aus denen Daten zur PSP erhoben werden können, aufgeführt werden. Es handelt sich dabei um eine Kann-Vorschrift, zumal die Fachstelle nicht zwingend auf alle verfügbaren Mittel zugreifen muss, um das Risiko zu beurteilen. Auch hier ist der Grundsatz der Verhältnismässigkeit spezifisch zu beachten. Dies ergibt sich aus der Formulierung, wonach nur die "notwendigen und in einem engen Zusammenhang zur Aufgabenerfüllung" stehenden Daten erhoben werden dürfen. Bei der Datenerhebung geht es um Erkenntnisse zur Vertrauenswürdigkeit, insbesondere zu einer allfälligen strafrechtlichen Vorbelastung, zur Beurteilung der finanziellen Situation und daraus folgend zur Beurteilung einer möglichen Bestechlichkeit. Die Befragung der zu prüfenden Person (lit. h) und auch Dritter bei Zustimmung der zu prüfenden Person (lit. i) dienen im Sinne einer erweiterten Prüfung dazu, Sachverhalte anzusprechen, die aus den Registerabfragen nicht oder nur unklar hervorgehen und folglich offen und unbeantwortet sind. Es sei darauf hingewiesen, dass im Rahmen der PSP aus dem Strafregister (lit. a) lediglich die Informationen aus dem Privatauszug und allenfalls aus dem Sonderprivatauszug (einzuholen durch die zu überprüfende Person) zur Verfügung stehen. Die Behördenauszüge, die weitere Informationen wie hängige Strafverfahren enthalten, können von Bundesrechts wegen nicht beigezogen werden. In Bezug auf das Einholen von Auskünften und Akten über hängige und abgeschlossene Strafverfahren bei den Strafbehörden (lit. b) ist anzumerken, dass Auskünfte und insbesondere Akten aus Strafverfahren nur unter sehr engen Voraussetzungen herausgegeben werden können. Die Herausgabe von Informationen aus laufenden Strafverfahren setzt voraus, dass das Verfahren nicht gefährdet wird. Informationen aus abgeschlossenen Verfahren sind bei derjenigen Instanz einzuholen, bei der das Strafverfahren rechtskräftig abgeschlossen wurde.

Werden bei der Datenerhebung auch Daten Dritter ermittelt, weil sie in einem engen Konnex mit den Daten der zu prüfenden Person stehen, dürfen diese nur bearbeitet werden, wenn dies für die Beurteilung des Sicherheitsrisikos unerlässlich ist (Abs. 2). Dies ist beispielsweise der Fall bei Bankkontenauszügen einer verheirateten Person. Der Aufwand, der mit dem Einholen der Einwilligung der Drittperson zur Datenbearbeitung verbunden wäre, wäre für die Fachstelle unverhältnismässig. Aber auch hier gilt der Grundsatz der Datensparsamkeit. Es sollen nur Daten für die Prüfung erhoben und verwendet werden, die unabdingbar für eine Sicherheitsbeurteilung sind. Bei Daten Dritter, die mit den Daten der zu prüfenden Person verknüpft sind, dürfte dies selten der Fall sein. Es ist deshalb Zurückhaltung in der Datenbearbeitung zu üben. Aus Transparenzgründen hat die Fachstelle die betroffenen Drittpersonen über die beabsichtigte Datenbearbeitung zu informieren (Abs. 2, 2. Satz).

Absatz 3 regelt die Dauer der Aufbewahrung der Daten beziehungsweise hält in sinngemässer Konkretisierung von § 21 IDAG fest, dass die erhobenen Daten so lange, wie die betreffende Person die sicherheitsrelevante Tätigkeit ausübt, auch benötigt werden. Im Rahmen der Personensicherheitsprüfung werden aber besonders schützenswerte Personendaten erhoben, für deren Bearbeitung erhöhte gesetzliche Anforderungen gelten. Gestützt auf § 8 Abs. 2 IDAG bedarf es zur rechtmässigen Bearbeitung besonders schützenswerter Daten einer gesetzlichen Grundlage (lit. a) oder der Erfüllung einer klar umschriebenen gesetzlichen Aufgabe (lit. b). Werden Personendaten nicht mehr zur Erfüllung einer gesetzlichen Aufgabe sowie zu Sicherungs- und Beweiszwecken nach § 21 Abs. 1 IDAG benötigt, sind sie zu vernichten beziehungsweise gemäss § 45 IDAG dem Staatsarchiv zur Langzeitaufbewahrung anzubieten. Es braucht folglich noch eine Frist, innert welcher die erhobenen Daten noch längstens aufzubewahren sind. In Anlehnung an die Bundesregelung wird eine 10-Jahresfrist vorgesehen. Nach Ablauf dieser Maximalfrist kann die Aufbewahrung der Daten aus der Sicherheitsprüfung nicht mehr als notwendig angesehen werden, weshalb eine längere Aufbewahrung weder recht- noch verhältnismässig wäre. Werden die erhobenen Daten aber nicht mehr benötigt, weil das PSP-Verfahren eingestellt wird, eine geprüfte Person die Stelle nicht antritt oder den Auftrag ablehnt, müssen sie gelöscht werden. Dies hat innert einer angemessenen Frist zu geschehen. Der Gesetzgeber räumt der Fachstelle diesbezüglich eine Frist von maximal drei Monaten ein, innert der die definitive Löschung der Daten zu erfolgen hat (Abs. 4).

7.4.4.2.5 § 22 Ergebnis der PSP

§ 22 Ergebnis der PSP

[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:

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.

Nach der Datenerhebung und Beurteilung der PSP hat die Fachstelle das Ergebnis zu begründen und schriftlich festzuhalten (Abs. 1). Dabei gibt es drei mögliche Szenarien: es besteht kein Sicherheitsrisiko (lit. a) oder es besteht eines (lit. c) beziehungsweise es besteht ein Sicherheitsrisiko, das mit Auflagen auf ein tragbares Mass reduziert werden kann (lit. b). Allfällige Auflagen sind durch die Fachstelle vorzuschlagen. Hingegen ist es nicht Aufgabe der Fachstelle PSP, die Verantwortung für Personalentscheide zu übernehmen, sondern lediglich die entscheidende Behörde über ein allfälliges Risiko zu informieren. Vor ihrem Entscheid muss die entscheidende Stelle beziehungsweise das entscheidende Gremium von der Erklärung der Fachstelle PSP Kenntnis nehmen, denn nur dann kann sie ihren Entscheid unter Berücksichtigung der allfälligen Risiken treffen.

Absatz 2 umschreibt, wann ein Sicherheitsrisiko vorliegt. Selbstverständlich ist es nicht einfach, das Risiko in Bezug auf menschliche Handlungen oder Unterlassungen einzuschätzen. Die für die Unterstellung unter die PSP massgebende Formulierung 'sicherheitsrelevante Tätigkeit' enthält in seiner Bedeutung die Auswirkungen, deren Eintreten vermieden werden soll. Es handelt sich dabei um eine erhebliche beziehungsweise schwerwiegende Beeinträchtigung der Interessen gemäss § 1 Abs. 2. Wenn die zu prüfende Person die Aufgaben, die ihr zugewiesen werden sollen, vorschriftskonform und sachgemäss erfüllt, kann der Schaden nicht eintreten. Das zu vermeidende Ereignis ist also im Umkehrschluss die vorschriftswidrige oder unsachgemässe Ausübung der sicherheitsempfindlichen Tätigkeit durch die betroffene Person. Sie muss in diesem Fall für die Tätigkeit als ungeeignet betrachtet werden. Ein Sicherheitsrisiko muss somit angenommen werden, wenn die Wahrscheinlichkeit hoch ist, dass die geprüfte Person die sicherheitsrelevante Tätigkeit vorschriftswidrig oder unsachgemäss ausüben wird, mithin für die sicherheitsrelevante Tätigkeit nicht geeignet ist und dadurch die Interessen gemäss § 1 Abs. 2 mindestens erheblich beeinträchtigen wird.

Die Fachstelle hat sich bei ihrer Beurteilung einzig an der Eintrittswahrscheinlichkeit des Ereignisses zu halten. Dabei wird es sich bei einer solchen Wahrscheinlichkeit zwangsläufig immer um eine Prognose über ungewisse künftige Sachverhalte handeln, die stets mit Unsicherheiten behaftet sind, weil es in der Natur der Sache liegt, dass sie nicht nur auf harten Fakten beruhen und dass es sich bei den aus den erhobenen Daten gezogenen Schlussfolgerungen auch um Annahmen und Vermutungen handeln kann. Grundlage für diese Prognose bildet die Gesamtheit aller Umstände wie beispielsweise die Persönlichkeit der betroffenen Person, ihr Vorleben und ihre Lebensverhältnisse, soweit diese Rückschlüsse auf ihr künftiges Verhalten zulassen.

In Absatz 3 werden deshalb die Risikofaktoren konkretisiert, die zur Annahme einer hohen Wahrscheinlichkeit für eine Beeinträchtigung führen. Es werden persönliche Eigenschaften umschrieben, die besonders risikoträchtig sind. Die Aufzählung orientiert sich inhaltlich an der Rechtsprechung des Bundesverwaltungsgerichts und des Bundesgerichts. Die Umschreibungen zielen zwar im Grundsatz auf möglichst objektiv feststellbare Eigenschaften ab, doch können diese häufig nur aus Indizien oder aus dem Kontext abgeleitet werden. Mit Integrität und Vertrauenswürdigkeit (lit. a) werden der Charakter sowie die Gewohnheiten und Beziehungen einer Person zu ihrem Umfeld anvisiert. Diese Eigenschaften sind bei der Ausübung einer sicherheitsempfindlichen Tätigkeit die Eignungserfordernisse schlechthin. Liegen diese Eigenschaften vor, kann mit hoher Wahrscheinlichkeit darauf vertraut werden, dass die mit einer solchen Tätigkeit betraute Person die geforderten Sicherheitsinteressen wahrt. Als besonders risikoträchtige Eigenschaften werden weiter Erpressbarkeit und Bestechlichkeit (lit. b) sowie ein beeinträchtigtes Urteils- oder Entscheidungsvermögen (lit. c) betrachtet. Welche der Indizien und Zusammenhänge die fehlende Vertrauenswürdigkeit einer Person, ihre mutmassliche Erpressbarkeit oder Bestechlichkeit oder ihr beeinträchtigtes Urteils- und Entscheidungsvermögen belegen, kann rechtsatzmässig nicht spezifiziert, sondern muss letztlich in jeder einzelnen Beurteilung ermittelt und dargelegt werden.

Der geprüften Person soll in jedem Fall das Recht eingeräumt werden, Einsicht in die Unterlagen der PSP zu nehmen (Abs. 4). Dieses Einsichts- und Korrekturrecht ist Ausfluss des rechtlichen Gehörs gemäss Art. 29 Abs. 2 BV und zwingend zu gewähren. Insbesondere die Möglichkeit der Berichtigung allfällig falsch erhobener Daten ist ein wichtiger Aspekt des Persönlichkeitsschutzes.

Nicht gesetzlich zu regeln sind die aus der PSP fliessenden Konsequenzen, weil sich diese ohnehin im Sinne der Durchsetzung des InfoSiG aufdrängen und im Rahmen des gesetzlich bereits zur Verfügung stehenden personalrechtlichen, disziplinarischen und vertraglichen Instrumentariums zu treffen sind. Die PSP wird ja gerade mit dem Zweck durchgeführt festzustellen, ob eine Person die Eigenschaften mitbringt, um angestellt oder in ein Amt beziehungsweise in ein Gremium gewählt zu werden. Bei externen Zulieferern dient die PSP auch zur Feststellung, ob ein Auftrag an ein bestimmtes Unternehmen vergeben werden kann. Zudem besteht die Möglichkeit, auch im Rahmen laufender Anstellungs- und Beamtenverhältnisse, einer laufenden Amtsperiode oder eines laufenden öffentlichen Auftrags eine PSP durchzuführen, wenn Anlass besteht anzunehmen, dass seit der letzten Prüfung neue Risiken entstanden sein könnten (§ 23 Abs. 2). Wird im Rahmen einer PSP festgestellt, dass die erforderliche Befähigung nicht gegeben ist, muss entsprechend gehandelt werden. Das heisst, die geprüfte Person darf nicht angestellt oder zur Wahl vorgeschlagen beziehungsweise gewählt werden. Und es darf keine Vergabe an ein Unternehmen erfolgen, dessen Personal die PSP nicht bestanden hat. Und laufende Anstellungsverhältnisse und auf eine bestimmte Dauer begründete Ämter sowie vertragliche Beziehungen sind zu beenden. Eine Nichtanstellung beispielsweise ist ohnehin nicht zu begründen. Und eine Kündigung der Anstellung würde gestützt auf den Tatbestand der mangelnden Eignung ordentlich (§ 10 Abs. 1 lit. b PersG) mit der Möglichkeit der Freistellung und in besonders schwerwiegenden Fällen fristlos (§ 11 Abs. 1 PersG) vorgenommen werden können. Eine fristlose vertragliche Beendigung wäre bei nicht mehr gegebener Eignung in Bezug auf die Gewährleistung der öffentlichen Interessen gemäss § 1 Abs. 2 sicherlich möglich. Dies gestützt auf die vertragliche Regelung, subsidiär aber gestützt auf den privatrechtlichen Grundsatz, wonach eine Kündigung aus wichtigen Gründen immer möglich ist, soweit einem Vertragspartner die Weiterführung des Vertragsverhältnisses nicht zumutbar ist.

Auch die Beendigung einer laufenden Amtsdauer ist grundsätzlich möglich. Soweit der Grosse Rat oder der Regierungsrat Wahlbehörden sind, obliegt ihnen auch die Beendigung des mit der Wahl begründeten Rechtsverhältnisses. Schliesslich kann auch eine durch Volkswahl begründete Amtsdauer durch Amtsenthebung beendet werden. Dies ist für die Richterinnen und Richter gemäss § 11 des Gerichtsorganisationsgesetzes (GOG) vom 06. Dezember 2011 (SAR 155.200) bereits vorgesehen, unabhängig davon, ob das Rechtsverhältnis durch Volkswahl oder Wahl durch eine kantonale Behörde vorgenommen wurde. Jedoch lässt sich die Folge des Nichtbestehens der PSP nicht unter einen der Tatbestände von § 25 Abs. 4 lit. a-d GOG subsumieren. Gemäss § 25 Abs. 4 lit. b GOG ist die Amtsenthebung zulässig, wenn die Richterin oder der Richter die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat. Eine Berufung auf diese Bestimmung kommt aber nicht in Betracht, weil sie auf Fälle von Krankheit abzielt. Aus der Formulierung (die Fähigkeit, das Amt auszuüben, auf Dauer verloren) geht hervor, dass es auch Fälle geben kann, in denen diese Fähigkeit zwar eingeschränkt ist, das Amt aber weiterhin ausgeübt werden kann. Dies ist typischerweise bei Krankheitsfällen der Fall. Im Rahmen der Umsetzung der Amtsenthebungsinitiative werden zurzeit in Anlehnung an § 25 Abs. 4 GOG entsprechende Rechtsgrundlagen für eine Amtsenthebung geschaffen. Dabei geht es um Änderungen des Schul- und des Kulturgesetzes hinsichtlich einer allfälligen Amtsenthebung von Schul- und Erziehungsräten sowie von Mitgliedern des Kuratoriums. Es braucht folglich eine spezielle Bestimmung, damit als Folge einer PSP mit dem Ergebnis 'Sicherheitsrisiko' eine Amtsenthebung zulässig ist (vgl. Kap. 7.8).

7.4.4.2.6 § 23 Wiederholung

§ 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.

Absatz 1 schreibt einen festen ordentlichen Wiederholungsintervall vor, indem er die Pflicht zur Wiederholung von PSP spätestens nach 5 Jahren statuiert. Bei Personen in einer Funktion mit Amtsdauer soll eine Wiederholung jeweils vor der Wiederwahl erfolgen, in aller Regel alle 4 Jahre. Der Bund schreibt keinen festen Wiederholungsintervall fest, weil eine Wiederholung aus seiner Sicht vermehrt dem tatsächlichen Sicherheitsbedarf entsprechend erfolgen soll. Dies hört sich zwar nach flexibler Handhabung an, ist aber in seiner Effektivität fraglich, weil diese letztlich von der Initiative irgendwelcher Personen, welche den Sicherheitsbedarf beurteilen müssen, abhängt. Eine institutionalisierte Wiederholung der PSP mag zwar banal anmuten, trägt aber zur Sicherheit bei, weil die PSP periodisch wiederholt werden muss, ohne dass eine subjektive Einschätzung über den Prüfungsbedarf entscheidet. Es ist selbstredend, dass eine solche Einschätzung per se risikobehaftet ist. Wichtig ist aber, dass im Rahmen der festgelegten fünfjährigen Wiederholungsdauer die Möglichkeit besteht, die PSP ausserordentlich zu wiederholen, wenn aufgrund veränderter Umstände Anlass zur Annahme besteht, dass neue Risiken bei der betroffenen Person entstanden sein könnten, die einen Bezug zur sicherheitsrelevanten Tätigkeit aufweisen (Abs. 2).

7.4.5 Sicherheitsspezifische Eignungsprüfung von Unternehmen

7.4.5.1 § 24 Befähigungsnachweis

§ 24 Befähigungsnachweis

[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
e) einen Nachweis der Zertifizierung der Informationssicherheitsprozesse oder zumindest des Vorliegens eines dem Vorhaben angemessenen ISDS-Konzepts.

Wie in Kapitel 5.2.3.1 'Betriebssicherheitsverfahren' bereits ausgeführt, soll von einem Leistungsbezug beim Bund, der ein umfangreiches Betriebssicherheitsverfahren implementiert, abgesehen werden. Das vom Bund vorgesehene Verfahren soll einerseits der Prüfung der Vertrauenswürdigkeit der zu beauftragenden Unternehmen dienen. Andererseits soll es ermöglichen, die notwendigen Massnahmen zur Wahrung der Informationssicherheit während der Ausführung von sicherheitsempfindlichen Aufträgen zu kontrollieren und durchzusetzen. Aus der Verordnung über das Betriebssicherheitsverfahren (VBSV), geht hervor, wie die Datenerhebung erfolgen soll und welche Daten erhoben werden sollen. Gemäss Art. 9 Abs. 3 VBSV wird lediglich eine Selbstdeklaration der Betriebe eingefordert, die "wahrheitsgemäss Auskunft erteilen" müssen. Dabei geht es (nicht abschliessend) um Daten über die Eigentumsverhältnisse, die Zusammensetzung der Unternehmensführung, allfällige Interessenbindungen des obersten Kaders und von Mitgliedern der Unternehmensführung, die Solvenz, die Bezahlung der Steuern und Sozialabgaben sowie Referenzen aus früheren Beschaffungsverfahren. Ein Mehrwert gegenüber der Eignungsprüfung im Rahmen des Vergabeverfahrens ist nicht zu erkennen, zumal die Befähigung zur Gewährleistung von Informationssicherheit und Datenschutz bereits heute im Rahmen der Eignungsprüfung durch die Vergabestellen geprüft wird. Der vom Bund betriebene Aufwand erscheint als nicht verhältnismässig in Relation zum Resultat, zumal dasselbe Ergebnis ohne weiteres im Vergabeverfahren erzielt werden kann. Dies aber mit dem entscheidenden Vorteil, dass keine Sistierung des Vergabeverfahrens notwendig ist, weil die Prüfung durch eine Bundesstelle ausserhalb des Vergabeverfahrens vorzunehmen ist. Danach müsste das

Resultat wieder ins kantonale Vergabeverfahren eingespeist werden und die Vergabestelle hätte bei entsprechendem Resultat der Prüfung den Ausschluss eines oder mehrerer Unternehmen zu verfügen. Es muss davon ausgegangen werden, dass die Vergabeverfahren dadurch tendenziell länger würden, was in vergaberechtlicher Hinsicht nicht anzustreben ist. Vielmehr soll neu gesetzlich eine Verpflichtung zur spezifischen Eignungsprüfung bei sicherheitsrelevanten Vergaben öffentlicher Aufträge aber auch bei der Übertragung von öffentlichen Aufgaben an Private, die in aller Regel ebenfalls nach vergaberechtlichen Kriterien erfolgt, statuiert werden (Abs. 1). In diesen Fällen muss die Informationssicherheit zwingend berücksichtigt werden und darf nicht dem Ermessen der Vergabestellen anheimgestellt bleiben. Im Grundsatz ist dies eine submissionsrechtliche Thematik, jedoch rechtfertigt sich eine Regelung im InfoSiG, da es ganz spezifisch um die Wahrung der mit dem InfoSiG verfolgten öffentlichen Interessen geht.

Die Prüfung der Eignung in sicherheitstechnischer Hinsicht entspricht einer Risikobeurteilung. Die erforderlichen Daten werden im Wesentlichen beim Betrieb selbst mit dessen Einverständnis erhoben. So sollen die Unternehmen zur Beurteilung des Risikos durch gezielte Abfrage, welche die Eigenheiten der spezifischen Vergabe beziehungsweise der Übertragung der öffentlichen Aufgabe berücksichtigt, aufgefordert werden Daten zu liefern, die für die Beurteilung ihrer Eignung in sicherheitsbezogener Hinsicht notwendig sind (Abs. 2). Dies entspricht grundsätzlich der Datenerhebung im Rahmen der Eignungsprüfung im Vergabeverfahren mit dem Unterschied, dass in Absatz 2 lit. a-e ausschliesslich Kriterien zur Beurteilung des Sicherheitsrisikos vorgegeben werden. Daten über die Eigentumsverhältnisse und die Solvenz, letztere durch Einsicht in allfällige hängige Pfändungs- und Konkursverfahren oder mittels Nachweises der Bezahlung von Steuern und Sozialabgaben, sind bewährte Kriterien in allen wesentlichen Vergabeverfahren zur Ermittlung der finanziellen und wirtschaftlichen Befähigung zur Aufgabenerfüllung. Spezifisch informationssicherheitsrelevant ist vor allem Absatz 2 lit. e, wonach durch die Unternehmen der Nachweis der Zertifizierung der Informationssicherheitsprozesse (ISO/IEC 27001) oder zumindest des Vorliegens eines dem Vorhaben angemessenen ISDS-Konzepts erbracht werden muss. Die vorgeschlagene Formulierung des zweiten Teilsatzes von lit. e ist bewusst offen formuliert und eröffnet so die Möglichkeit, die Anforderungen spezifisch auf das konkrete Vorhaben und das jeweilige Schadenspotenzial anzupassen, so dass auch im Einzelfall der Aufwand in einem vernünftigen Verhältnis zum Nutzen steht. Sind gewichtige oder komplexe Aufträge oder öffentliche Aufgaben zu vergeben beziehungsweise auszulagern, ist auf ein ISDS-Konzept abzustellen, das den anerkannten Standards (z.B. NIST Cybersecurity Framework) zu genügen vermag. Bei weniger umfassenden oder komplexen Aufträgen oder Auslagerungen öffentlicher Aufgaben, namentlich im Sozial-, Bildungs- oder Gesundheitsbereich, reicht ein dem Vorhaben angemessenes ISDS-Konzept. Der durch die Dritten zu erbringende Aufwand muss in einem adäquaten Verhältnis zur Auftragsvergabe beziehungsweise zur Auslagerung der öffentlichen Aufgabe stehen, ansonsten vermehrt mit Auftragsverweigerungen zu rechnen sein wird.

7.5 Kapitel 4 Organisation

7.5.1 Verwaltungsinterne Organisation

7.5.1.1 § 25 Fachstelle für Informationssicherheit

§ 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,

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,
i) Erlass von technischen Weisungen und Standards.

[3] Administrativ ist die Fachstelle für Informationssicherheit dem Departement Finanzen und Ressourcen beigeordnet.

Die Fachstelle für Informationssicherheit soll departements- und behördenübergreifend tätig sein und über entsprechende Weisungs- und Durchsetzungsbefugnisse verfügen, welche die Vollzugsautonomie der Behörden tangieren können. Aber die Gefährdung der öffentlichen Interessen, die durch eine Verletzung der Informationssicherheit einher gehen kann, rechtfertigt es, dass die Fachstelle gesetzlich bestimmte Aufsichts- und Kontrollkompetenzen erhält wie beispielsweise die autonome Durchführung von Überprüfungen aber auch die Möglichkeit des Ergreifens von Massnahmen, wenn Verletzungen der Informationssicherheitsvorgaben (Gesetz, Verordnung, Weisungen, Standards) festgestellt werden sollten (Abs. 2 lit. c). Der Fachstelle steht deshalb vorerst ein Antragsrecht zu. Sie erstattet dabei Bericht an die betroffenen Stellen und beantragt, die festgestellten Mängel innerhalb einer bestimmten Frist zu beheben. Je dringender das Anliegen, desto kürzer wird die Frist ausfallen. Selbstverständlich steht es den betroffenen Stellen zu, zum Antrag Stellung zu beziehen und auf allfällige Unzulänglichkeiten in den Feststellungen der Fachstelle zwecks Bereinigung hinzuweisen.

Bleibt der Antrag stehen und handelt die betroffene Stelle danach nicht oder versäumt sie es, innert der gesetzten Frist Massnahmen zu ergreifen, ist die Fachstelle befugt, mittels Durchgriffs die notwendigen Massnahmen im Sinne einer Ersatzvornahme, mithin auf Kosten der betroffenen zuständigen Stelle zu ergreifen (Abs. 2 lit. d). Dies beinhaltet auch, dass wo Gefahr in Verzug ist beziehungsweise keine Möglichkeit zur Fristgewährung zur Behebung einer Sicherheitslücke besteht, die Fachstelle unmittelbar, auch ohne Antrag und Fristgewährung, zur Anordnung beziehungsweise Ergreifung von Massnahmen befugt ist. Die Ergreifung von Massnahmen hat dabei in Zusammenarbeit mit den betroffenen Stellen zu erfolgen. Wenn die Fachstelle nur auf Antrag der Behörden tätig werden und blosse Empfehlungen abgeben kann, ist die Gefahr erheblich, dass die öffentlichen Interessen gemäss § 1 Abs. 2 verletzt werden könnten. Eine Fachstelle ohne Durchsetzungsmöglichkeit ist keine wirksame Option im Hinblick auf eine möglichst risikofreie Informationssicherheit und besonders im Kampf gegen Cyberbedrohungen. Jedoch soll die Durchgriffsbefugnis beschränkt sein auf Situationen besonderer Gefahrensituationen. Ein Durchgriff ist dann nicht notwendig, wenn die Verletzung von Vorgaben zu keiner ernsthaften Gefährdung führt. Nur wenn eine unmittelbare Gefahr für die Informationssicherheit droht oder mit negativen Auswirkungen auf weite Teile der kantonalen Informatikinfrastruktur zu rechnen ist, soll das Durchgriffsrecht zum Tragen kommen. Diese Einschränkung ist durch das Verhältnismässigkeitsprinzip geboten und trägt der Vollzugsautonomie Rechnung. Wenn sich die dezentralen Fachstellen nicht an die Vorgaben halten, haben sie diese Risiken für sich zu verantworten. Dies gilt aber nur, solange damit keine schwerwiegenden Folgen für die öffentlichen Interessen beziehungsweise keine Kompromittierung anderer Informatiksysteme verbunden ist. Auch das Ergreifen von Massnahmen in präventiver Hinsicht gehört dazu. So soll bei neu aufgetretenen Gefahren und Bedrohungen sowie bei Entdeckung neuer Schwachstellen und Lücken die Information aller Beteiligten rasch, zielgerichtet und behördenübergreifend erfolgen. Schliesslich ist es auch in operationeller Hinsicht erforderlich, dass es in der Verwaltungspraxis departements- und behördenübergreifend zu einer Vereinheitlichung in Bezug auf den Vollzug der Informationssicherheitsgesetzgebung kommt. Dazu kann das Wirken einer zentralen Fachstelle mit entsprechenden Befugnissen beitragen.

Haben alle ergriffenen präventiven Massnahmen nicht zum Ziel geführt und werden Systeme des Kantons angegriffen, ist die Fachstelle für Informationssicherheit zuständig für die behördenübergreifende Bewältigung von Cybervorfällen in der Verwaltung (Abs. 2 lit. e). Selbstverständlich erfolgt die Bewältigung unter Beizug der betroffenen Stellen.

Im Weiteren ist die Fachstelle für Informationssicherheit allgemein zuständig für die fachliche Beratung und Unterstützung der Behörden und ihrer Verwaltungseinheiten (Abs. 2 lit. a). Die Fachstelle fungiert somit als verwaltungsinternes Kompetenzzentrum für die Informationssicherheit. Sie ist in operativer Hinsicht zuständig für den Aufbau, Betrieb und die Weiterentwicklung eines Informationssicherheits-Managementsystems (lit. b), wohingegen dessen Implementierung in strategischer Hinsicht in der Verantwortung der Behörden liegt (§ 5). Die Fachstelle beurteilt zudem die mit dem Einsatz neuartiger Technologien für die Informationssicherheit entstehenden Risiken (Abs. 2 lit. f). Im Bereich der Technik kommen regelmässig neuartige Technologien zum Einsatz. Die Risiken, die mit dem Einsatz solcher neuartigen Mittel (Hard- und Software) verbunden sind, sind oft unklar. Insbesondere für Technologien, die einen breiten Anwendungsbereich und Auswirkungen auf die ganze Verwaltung haben können, soll die Fachstelle eine Beurteilung vornehmen und die Risiken analysieren können. Die damit verbundenen Risiken sind zu gross, als dass eine Einbindung der Fachstelle auf Gutdünken und Antrag der Behörden beschränkt sein soll. Eine weitere Aufgabe der Fachstelle Informationssicherheit ist die Teilnahme bei wichtigen behördenübergreifenden Projekten und in allen mit der Umsetzung der Informationssicherheit betrauten Gremien (Abs. 2 lit. g). Es ist wichtig, dass die Fachstelle die für den Vollzug wichtigen Informationen aus erster Hand erhält und ihr Know-how in kantonalen Projekten einbringen kann. Die Fachstelle legt jährlich Rechenschaft ab über ihr Wirken, indem sie dem Regierungsrat Bericht erstattet (Abs. 2 lit. h). Der Regierungsrat muss regelmässig über den Stand der Informationssicherheit informiert werden, damit er deren Wirksamkeit und Wirtschaftlichkeit beurteilen kann. Schliesslich ist die Fachstelle zuständig für den Erlass von technischen Weisungen und Standards (Abs. 2 lit. i). Das fachliche Know-how der Fachstelle hat in diese normativen Instrumente einzufliessen und dabei müssen die aktuellen Erkenntnisse über die Abwehr von Gefahren und Bedrohungen und der aktuelle Stand der technischen Möglichkeiten zum Schutz der Informationssicherheit berücksichtigt werden. Es ist wichtig, dass diese Grundlagen, beispielsweise Sicherheits-Standards, schnell den aktuellen Bedürfnissen angepasst werden können. Der Erlass durch die zentrale Fachstelle gewährleistet eine einheitliche, behördenübergreifende Anwendung von Konzepten und Standards in der Verwaltung.

Die aufgeführten Aufgaben der Fachstelle für Informationssicherheit können in Berührung kommen, kollidieren aber nicht mit dem Aufgabenbereich der ÖDB, deren Aufgabenerfüllung mit dem Ziel des Grundrechts- und Persönlichkeitsschutzes gemäss IDAG selbstverständlich vorbehalten bleibt. Zum Zusammenspiel von Informationssicherheit und Datenschutz sei auf die Erläuterungen zu § 4 (Kap. 7.2.4) verwiesen.

Heute ist der CISO und seine Organisation der Informatik Aargau des Departements Finanzen und Ressourcen unterstellt. Im Vollzug hat sich diese Organisation grundsätzlich bewährt. Jedoch bringt es die Ausstattung mit weitreichenden Kompetenzen, namentlich der Möglichkeit eines departements- und behördenübergreifenden Durchgriffs im Sinne der Massnahmenergreifung bei festgestellter Gefährdung der Informationssicherheit (Abs. 2 lit. c) mit sich, dass die Fachstelle in Bezug auf die Informatik funktional unabhängig tätig sein muss. Sollten die Interessen der IT beziehungsweise der IT-Sicherheit und der Informationssicherheit nicht deckungsgleich sein, hat der Leiter IT heute eine Interessenabwägung vorzunehmen. Diese kann nicht restlos unbefangen erfolgen, was einer wirksamen Durchsetzung der Informationssicherheit abträglich sein könnte. Um das hohe Risikominimierungsziel erreichen zu können und folglich zur uneingeschränkten Durchsetzung der Informationssicherheit braucht es diesbezüglich funktionale Unabhängigkeit. Das ist ein allgemeines Gebot der Good Governance, das in organisatorischer Hinsicht immer zu berücksichtigen ist. Aufgrund der durch die Verbundenheit und Nähe zur zentralen IT entstehenden Synergien ist aber eine administrative Verortung in der Abteilung Informatik des Departements Finanzen und Ressourcen (Abs. 3)

jedoch unabdingbar. Die Aufgaben lassen sich einfacher erfüllen, wenn sich die entsprechenden Befugnisse infolge der funktionalen Unabhängigkeit sowie der Direktunterstellung beim Regierungsrat legitimieren lassen. Die Fachstelle für Informationssicherheit soll deshalb als Stabsstelle direkt dem Regierungsrat unterstellt sein (Abs. 1) und diesem auch Bericht erstatten. Der Regierungsrat hat zudem in eigener Kompetenz auch die weitere verwaltungsinterne Organisation im Bereich der Informationssicherheit zu regeln, namentlich in Bezug auf die Befugnisse der Informationssicherheitsbeauftragten in den Departementen sowie zu einer gemeinsamen Konferenz derselben zur Förderung des einheitlichen Vollzugs, der Standardisierung der Anforderungen und Massnahmen und zum Informationsaustausch im Zusammenhang mit dem Informationssicherheits-Risikomanagement sowie mit auftretenden Problemen und Vorfällen im Bereich der Cybersicherheit.

7.5.2 Verwaltungsübergreifende Organisation

7.5.2.1 § 26 Kantonale Cyber-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

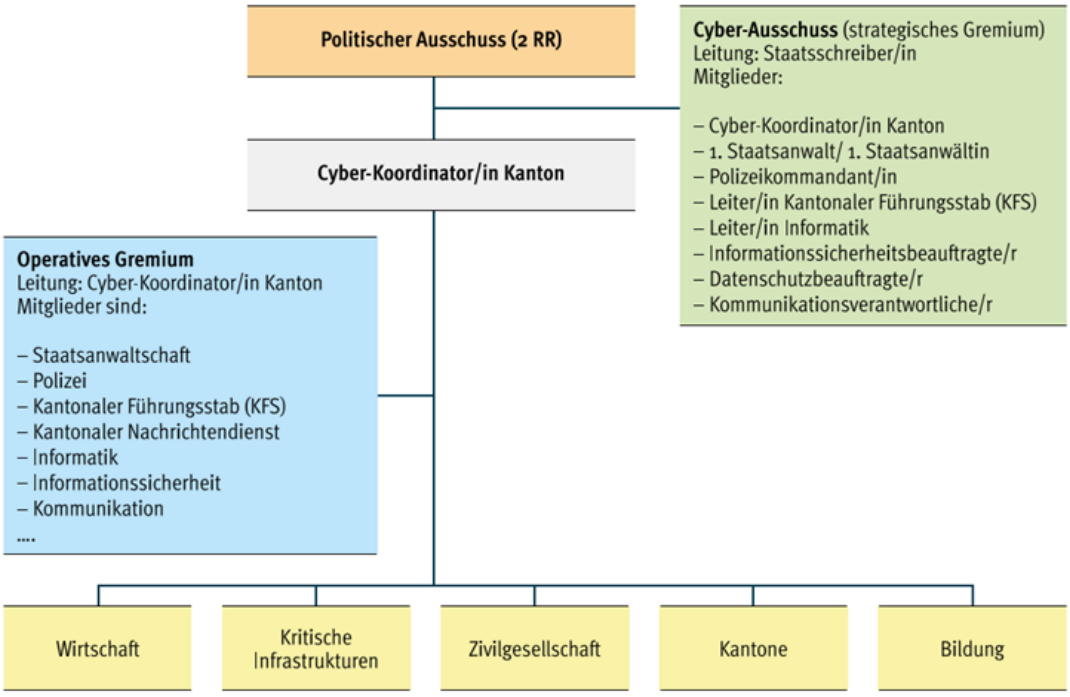
b) Cyber-Koordinationsstelle

c) Kerngruppe Cyber

[3] Der Regierungsrat regelt die organisatorischen Belange durch Verordnung.

Die mit dem Gesetzesentwurf vorgeschlagene kantonale Cyber-Organisation (§§ 26 ff.) richtet sich im Wesentlichen nach den Empfehlungen für die Umsetzung zur kantonalen Cyber-Organisation vom 12. Januar 2021 des Sicherheitsverbunds Schweiz (SVS). Danach sieht die Organisationstruktur wie folgt aus:

Abbildung 7: Vom SVS empfohlene kantonale Cyber-Organisation

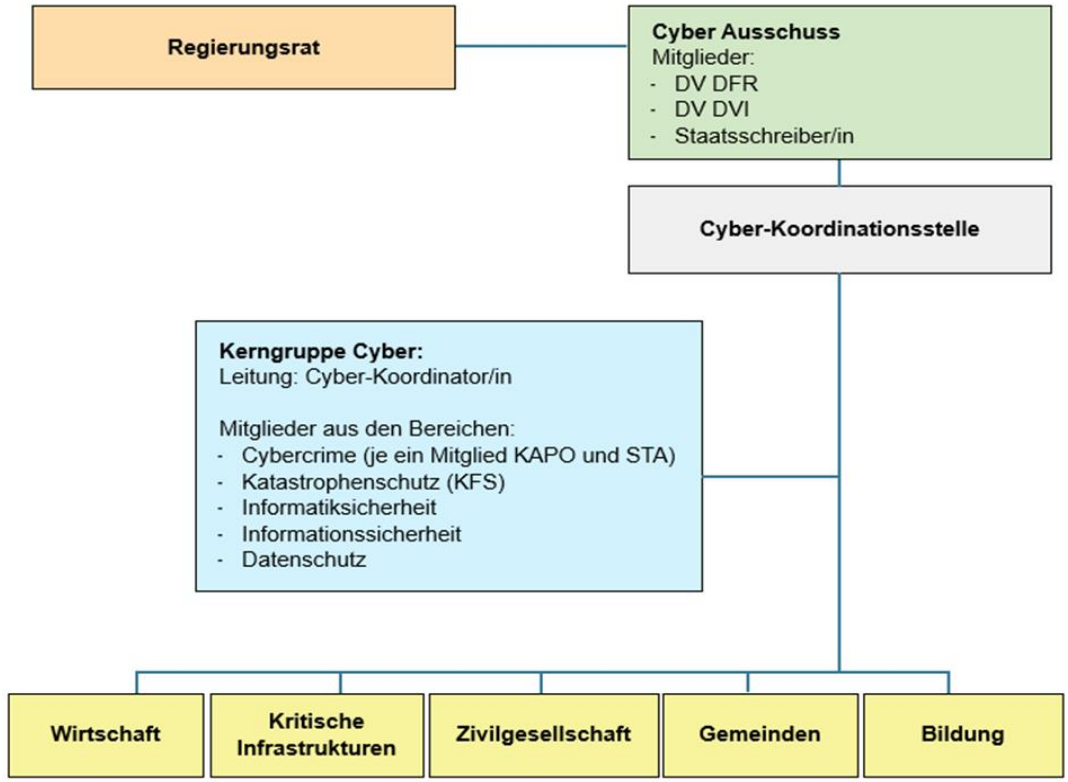


Die im Entwurf vorgeschlagene Lösung verzichtet auf die Schaffung eines politischen und zusätzlich eines strategischen Ausschusses, wie es die Empfehlungen des SVS vorsehen. Es macht wenig Sinn neben der politischen Ebene, der ohnehin strategische Funktion zukommt, organisatorisch noch eine spezifisch strategische Ebene vorzusehen. Um allfällige Abgrenzungsprobleme zwischen den beiden Aufgabenbereichen zu vermeiden, sollte vielmehr darauf verzichtet werden, einen strategischen Ausschuss zu schaffen. Die strategischen Befugnisse lassen sich ohne weiteres im politischen Ausschuss verankern.

Ziel ist es, eine möglichst wirksame Cyber-Organisation mit klaren Kompetenzen aufzubauen, um die Gefahr zu vermeiden, dass dadurch Doppelspurigkeiten oder Kompetenzüberschneidungen entstehen könnten. Die im Entwurf vorgeschlagene Cyber-Organisation entspricht folglich der vom SVS empfohlenen Organisation (vgl. Abb. 5) mit Ausnahme des Verzichts auf die zusätzliche Schaffung eines strategischen Ausschusses. Die Organisation soll aus einem (politisch-strategischen) Cyber-Ausschuss (Abs. 2 lit. a) bestehen, dem zwei Regierungsrätinnen oder -räte sowie die Staatsschreiberin oder der Staatsschreiber angehören. Dabei ist es naheliegend, dass aufgrund der Nähe zum Thema 'Cyber' die Vorsteherin oder der Vorsteher der Departemente Volkswirtschaft und Inneres sowie Finanzen und Ressourcen diese Funktion von Amtes wegen einnehmen sollen. Die Cyber-Koordinationsstelle (Abs. 2 lit. b) soll als Single Point of Contact mit dem Ziel der Koordination und des Informationsaustausches zwischen den staatlichen und privaten Akteuren sowie zur Stärkung der Resilienz in Verwaltung, Wirtschaft und Bevölkerung fungieren. Schliesslich wird die Schaffung einer Kerngruppe Cyber vorgeschlagen (Abs. 2 lit. c), die operativ die Cyber-Koordinationsstelle unterstützt und das Cyber-Know-how der darin vertretenen Spezialistinnen und Spezialisten aus den Bereichen Informations- und Informatiksicherheit, Datenschutz, Cyberkriminalität und Katastrophenschutz einbringt.

Das Organigramm der vorgeschlagenen kantonalen Cyber-Organisation sieht demnach wie folgt aus:

Abbildung 8: Vorgeschlagene kantonale Cyber-Organisation



Gemäss Empfehlungen des SVS erfordert die Wahrnehmung der in § 28 aufgeführten Aufgaben der Cyber-Koordinationsstelle personelle Ressourcen im geschätzten Umfang von einer Vollzeitstelle mit einer administrativen Unterstützung. Da die Koordinationsstelle von einer Person geleitet werden soll, ist eine Stellvertretung erforderlich, um allfällige Ausfälle auffangen zu können. Die Stellvertretung könnte von einem Mitglied der Kerngruppe übernommen werden, erfordert jedoch ebenfalls personelle Ressourcen. Der vorliegende Entwurf hält sich diesbezüglich an die Empfehlungen des SVS.

Die kantonale Cyber-Organisation, wie sie im Entwurf vorgeschlagen wird, wurde im Austausch mit den zuständigen Stellen für die Cyber-Kriminalität (Kapo und Staatsanwaltschaft), mit der für die Informations- und Informatiksicherheit zuständigen Stellen (CISO und Leitung Informatik Aargau) sowie mit dem CISO einer kritischen Infrastruktur (Swissgrid) erarbeitet.

7.5.2.2 § 27 Cyber-Ausschuss

§ 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.

Der Cyber-Ausschuss soll aus zwei Vorsteherinnen oder Vorstehern bestehen. Da, wie oben unter Kap. 7.5.2.1 bereits ausgeführt, in den Departementen Volkswirtschaft und Inneres sowie Finanzen und Ressourcen aufgrund der Berührungspunkte und Nähe zum Thema "Cyber" in ihren Aufgabenbereichen (Cyber Crime, CISO, IT AG) das Know-how vorhanden ist, um die Aufgaben dieses Ausschusses zu erfüllen, sind die entsprechenden Vorsteherinnen oder Vorsteher von Amtes wegen gesetzlich für diese Funktion vorzusehen (Abs. 1). Zudem soll auch die Staatsschreiberin oder der Staatsschreiber diesem Gremium angehören. Der Cyber-Ausschuss fungiert dabei in politisch-strategischer Hinsicht als verlängerter Arm des Regierungsrats. Ihm soll die Aufsichtsfunktion über die kantonale Cyber-Organisation zukommen (Abs. 2 lit. a). Im Weiteren übernimmt er die Wahlvorbereitung und schlägt dem Regierungsrat die Cyber-Koordinatorin oder den Cyber-Koordinator zur Wahl vor (Abs. 2 lit. b). Er genehmigt die Ziele und prüft deren jährliche Erreichung (Abs. 2 lit. c) und entscheidet im Sinne eines Eskalationsgremiums über Differenzen, falls es in den verschiedenen Gremien der kantonalen Cyber-Organisation zu Ungereimtheiten kommen sollte (Abs. 2 lit. d). Schliesslich lässt er relevante Cybervorfälle im Nachgang analysieren, beurteilt deren Bewältigung (Abs. 2 lit. e) und sorgt dafür, dass daraus entsprechende Lehren gezogen beziehungsweise gestützt darauf allfällige Massnahmen ergriffen werden. Der Cyber-Ausschuss hat die Möglichkeit, die Cyber-Koordinatorin oder den Cyber-Koordinator sowie Mitglieder der Kerngruppe Cyber zu dessen Sitzungen einzuladen, soweit zur Aufgabenerfüllung entsprechendes Know-how notwendig sein sollte.

7.5.2.3 § 28 Cyber-Koordinationsstelle

§ 28 Cyber-Koordinationsstelle

[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,
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.

Für eine erfolgreiche Bewältigung der Cyberbedrohungen braucht es ein gemeinsames, koordiniertes Vorgehen. Deshalb wird eine Stelle geschaffen, die mit der Koordination und dem Informationsaustausch zwischen den staatlichen und privaten Akteuren sowie der Stärkung der Widerstandsfähigkeit (oder Reslilienz) in Verwaltung, Wirtschaft und Bevölkerung betraut wird (Abs. 1). Gemäss den Empfehlungen des SVS liegt der Mehrwert einer solchen Stelle in ihrer Funktion als Single Point of Contact (SPoC) für Fragen zur Informationssicherheit innerhalb des Kantons (Abs. 2 lit. a). Die Cyber-Koordinationsstelle ist das zentrale Koordinationsorgan der kantonalen Cyber-Organisation. Sie stellt die Vernetzung im Kanton zwischen den verschiedenen staatlichen und privaten Akteuren sicher und nach aussen zu den Behörden auf nationaler Ebene und zu anderen Kantonen (Abs. 2 lit. b). Soweit im Rahmen der Anpassung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) die Umsetzung von Massnahmen notwendig wird, übernimmt die Cyber-Koordinationsstelle die Koordination der Umsetzung im Kanton (Abs. 2 lit. c). Die Cyber-Koordinatorin oder der Cyber-Koordinator übernimmt gleichzeitig die Leitung der mit Spezialistinnen und Spezialisten aus den Bereichen Informations- und Informatiksicherheit, Datenschutz, Cyberkriminalität und Katastrophenschutz konstituierten Kerngruppe Cyber (Abs. 2 lit. d). In operativer Hinsicht ist die Cyber-Koordinationsstelle befugt, Empfehlungen abzugeben, wenn sie innerhalb der kantonalen Cyber-Organisation Risiken für die Informationssicherheit entdeckt (Abs. 2 lit. e) und sie soll Übungen koordinieren (Abs. 2 lit. f). Dies namentlich mit dem KFS und den kritischen Infrastrukturen. Die Aufzählung ist bewusst nicht abschliessend, weil es denkbar ist, dass solche Übungen auch mit der Wirtschaft und mit der Armee oder mit anderen Organisationen durchgeführt werden könnten. Erreicht ein Cyber-Vorfall das Ausmass einer Katastrophe im Sinne von § 2 Abs. 1 des Gesetzes über den Bevölkerungsschutz und den Zivilschutz im Kanton Aargau (Bevölkerungsschutz- und Zivilschutzgesetz Aargau, BZG-AG) vom 4. Juli 2006 (SAR 515.200) beziehungsweise einer Notlage im Sinne von § 2 Abs. 2 BZG-AG, obliegt gemäss § 4 Abs. 1 BZG-AG die Führung dem KFS. Das KFS kann bei einem solchen Ereignis die Kerngruppe Cyber zur Unterstützung beiziehen. Übungen sind in präventiver Hinsicht unabdingbar, weil sie die Zusammenarbeit zwischen den für einen Cyber-Vorfall zuständigen Akteuren verbessern und zur Klärung der im Ernstfall einzuhaltenden Abläufe beitragen.

Der Cyber-Koordinationsstelle obliegen auch Förderungs-, Schulungs- und Sensibilisierungsaufgaben. So soll die Cyber-Koordinationsstelle für die Stärkung der sog. Awareness, des Bewusstseins hinsichtlich des richtigen Verhaltens in Bezug auf die latenten Cyber-Bedrohungen durch Beratung und Unterstützung von Projekten zur Förderung der Informationssicherheit (Abs. 2 lit. g), Erstellen von Ausbildungsunterlagen und Durchführung von Schulungen (Abs. 2 lit. h), Sensibilisierung von Verwaltung, Wirtschaft und Bevölkerung (Abs. 2 lit. i) und durch Planung und Durchführung von Präventionskampagnen (Abs. 2 lit. j) sorgen. Für die Erfüllung dieser Aufgaben sind der Cyber-Koordinationsstelle entsprechende finanzielle Ressourcen zur Verfügung zu stellen.

Die Cyber-Koordinationsstelle hat dem Regierungsrat jährlich Bericht zu erstatten (lit. k). Gestützt auf § 26 Abs. 3 wird der Regierungsrat kraft seiner Verordnungskompetenz die Verortung der Cyber-Koordinationsstelle innerhalb der Verwaltung zu beschliessen haben.

7.5.2.4 § 29 Kerngruppe Cyber

§ 29 Kerngruppe Cyber

[1] Zur operativen Unterstützung der Cyber-Koordinationsstelle ist eine Kerngruppe Cyber einzusetzen.

[2] Sie hat insbesondere folgende Aufgaben:

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.

Die Kerngruppe Cyber unterstützt die Cyber-Koordinatorin oder den Cyber-Koordinator in operativer Hinsicht (Abs. 1). Es ist notwendig, dass in diesem Gremium Spezialistinnen und Spezialisten vertreten sind, die in ihrem beruflichen Alltag mit der Gewährleistung der Informationssicherheit beziehungsweise mit der Abwehr von Cyberrisiken betraut sind. Aus diesem Grund gibt der Gesetzgeber vor, aus welchen Bereichen sich die Kerngruppe zumindest zusammensetzen muss. Er erwähnt ausdrücklich die Bereiche Informations- und Informatiksicherheit, Datenschutz, Cyberkriminalität und Katastrophenschutz (Abs. 2 lit. a). Folglich setzt sich die Kerngruppe im Sinne des gesetzlich geforderten Minimums (der Regierungsrat kann in den Ausführungsbestimmungen auch weitere Mitglieder aus anderen Bereichen vorsehen) konkret zusammen aus je einem Vertreter der Staatsanwaltschaft und der Kantonspolizei (Cyberkriminalität), des KFS (Katastrophenschutz), der Informatik (Informatiksicherheit), aus dem CISO beziehungsweise künftig aus dem Leiter der Fachstelle Informationssicherheit (Informationssicherheit) sowie aus der beauftragten Person für Öffentlichkeit und Datenschutz (Datenschutz).

Die Kerngruppe Cyber dient in erster Linie dem Informationsaustausch (Abs. 2 lit. e) zwischen den Mitgliedern des Gremiums, die zum einen zu den Cyberspezialistinnen und -spezialisten zu zählen sind, zum andern aus Mitgliedern anderer Bereiche wie dem Datenschutz und dem Katastrophenschutz besteht. Es werden Informationen, aber auch Erfahrungen ausgetauscht sowie die neuesten Entwicklungen in der Abwehr von Cyber-Bedrohungen besprochen. Für die Praxis wesentlich ist insbesondere der Austausch zwischen dem CISO beziehungsweise dem künftigen Leiter der Fachstelle Informationssicherheit und den Vertreterinnen und Vertretern der Cybercrime-Organisationen. Im Interesse einer wirkungsvollen und raschen Strafverfolgung ist eine enge Zusammenarbeit erforderlich, weshalb ein periodischer Austausch sehr wichtig ist. Erforderlich ist auch die gemeinsame Beurteilung der Bedrohungslage (Abs. 2 lit. b), die nicht durch eine Stelle erfolgt, sondern objektiviert durch das Zusammenwirken im Gremium. Die Kerngruppe Cyber vereint das gebündelte Cyber-Know-how des Kantons sowie weiteres in diesem Zusammenhang wesentliches Know-how in sich. Die Kerngruppe Cyber beaufsichtigt im Weiteren die Bewältigung erheblicher Cybervorfälle innerhalb der Verwaltung (Abs. 2 lit. c). Dies bedeutet, dass sie bei Cyber-Vorfällen in der Verwaltung, die Auswirkungen auf die Bevölkerung und auf die Wirtschaft haben können, beizuziehen ist. Deren Mitglieder, namentlich die Spezialistinnen und Spezialisten des Cybercrime, können punktuell auch zur Bewältigung von Cyber-Vorfällen im Kanton beigezogen werden, soweit deren Beizung hilfreich sein könnte. Selbstverständlich sind im Rahmen des periodischen Austausches Cyber-Vorfälle und deren Bewältigung zu analysieren sowie vor allem auch Lehren daraus zu ziehen (Abs. 2 lit. d). Nur aus einer minuziösen Aufbereitung der Bewältigung von Cybervorfällen - aus verschiedenen Gesichtspunkten betrachtet – können die erforderlichen Schlussfolgerungen gezogen sowie Verbesserungen in Bezug auf die zu ergreifenden Massnahmen und die definierten Prozesse vorgenommen werden.

7.6 Kapitel 5 Vollzug

7.6.1 § 30 Ausführungsbestimmungen

§ 30 Ausführungsbestimmungen

[1] Die Behörden erlassen die für den Vollzug dieses Gesetzes erforderlichen Ausführungsbestimmungen durch Dekret, Verordnung bzw. Reglement.
[2] Soweit der Grosse Rat und die Gerichte keine eigenen Ausführungsbestimmungen erlassen haben, gelten für sie die Verordnungen und Weisungen des Regierungsrats sinngemäss.

Der Gesetzgeber sieht die oberste Führungsverantwortung für die Informationssicherheit bei den Behörden (vgl. § 4 Abs. 1). Sie haben gestützt darauf konsequenterweise auch die für den Vollzug des Gesetzes erforderlichen Ausführungsbestimmungen für ihre Bereiche zu erlassen (Abs. 1). Dies findet darin seine Rechtfertigung, dass so die Eigenheiten der verschiedenen Behörden am besten berücksichtigt werden können. Es stellt auch kein eigentliches Problem dar, da auch der Grosse Rat und die Gerichte über eine eigene Rechtsetzungskompetenz verfügen. So erlässt der Grosse Rat Ausführungsbestimmungen in Form des Dekrets, der Regierungsrat in Form der Verordnung und die Gerichte in Form des Reglements. Das Gesetz soll aber eine rechtsetzerische Ausweichklausel vorsehen, die es dem Grossen Rat und den Gerichten erlaubt, auf eine eigene Regelung zu verzichten. In diesem Fall sind die Verordnungen und Weisungen des Regierungsrats, für den die Klausel nicht gilt und der dazu verpflichtet ist, Ausführungsbestimmungen zu erlassen, sinngemäss für die beiden Behörden anwendbar. Dies soll einen möglichst einheitlichen Vollzug ermöglichen.

7.7 Kapitel 6 Schlussbestimmungen

7.7.1 § 31 Übergangsbestimmung

§ 31 Übergangsbestimmung

[1] Die Klassifizierung der im Zeitpunkt dieses Gesetzes vorhandenen Informationen hat spätestens bis 5 Jahre nach Inkrafttreten dieses Gesetzes zu erfolgen.

Im Rahmen des Projekts 'Strategische Entwicklung Daten' ist unter anderem geplant, Informationen und Datenbestände zu klassifizieren. Es ist aber davon auszugehen, dass zum Einführungszeitpunkt des InfoSiG nicht alle Informationen und Datenbestände klassifiziert sein werden. Insofern ist zum jetzigen Zeitpunkt von einem Klassifizierungsbedarf an Informationen und Datenbeständen auszugehen, die im Zeitpunkt des Inkrafttretens dieses Gesetzes noch nicht klassifiziert sind. Es braucht folglich eine Übergangsbestimmung, die zum Zwecke der vollständigen Klassifizierung eine angemessene Vollzugsfrist einräumt. Der Regierungsrat erachtet aufgrund der geschätzten Datenbestände eine Frist von 5 Jahren ab Inkrafttreten des Gesetzes als angezeigt.

7.7.2 § 32 Inkrafttreten

§ 32 Inkrafttreten

[1] Der Regierungsrat bestimmt den Zeitpunkt des Inkrafttretens.

Die Inkraftsetzung soll voraussichtlich auf den 1. Juli 2026 erfolgen.

7.8 Fremdänderungen des Schulgesetzes und des Kulturgesetzes

Im Rahmen der Umsetzung der Amtsenthebungsinitiative werden zurzeit verschiedene Amtsenthebungstatbestände geschaffen. Es betrifft dies verschiedene Behörden, namentlich den Grossen Rat, den Regierungsrat, Gemeindebehörden, Schulbehörden (Schulrat und Erziehungsrat) sowie das Ku-

ratorium. Die Regelungen lehnen sich dabei an die im GOG bereits geregelten Amtsenthebungstatbestände an (§ 25 Abs. 4 lit. a-d). Gemäss § 19 Abs. 1 lit. b E InfoSiG kommt eine PSP in Betracht bei Personen, die in ein Amt oder als Mitglied eines kantonalen Gremiums gewählt werden sollen. Gemäss Abs. 2 sind von der Regelung von Abs. 1 lit. b die Mitglieder des Grossen Rats und des Regierungsrats ausgenommen. Da der Geltungsbereich des InfoSiG die Gemeinden nicht allgemein mitumfasst, ist die Amtsenthebung von Gemeindebehörden in diesem Kontext kein Thema. Eine PSP kommt aber für die Schul- und Erziehungsräte sowie für die Mitglieder des Kuratoriums in Betracht, weshalb eine entsprechende Anpassung der noch zu schaffenden Regelungen vorzusehen ist.

§ 76b Abs. 1 lit. d (neu) Schulgesetz; Amtsenthebung

In Anlehnung an die Neuregelung von § 25 Abs. 4 lit. e GOG ist eine neue Bestimmung zu schaffen, wonach eine Amtsenthebung als Folge einer PSP mit dem Ergebnis 'Sicherheitsrisiko' zulässig ist.

§ 79b Abs. 1 lit. d (neu) Schulgesetz; Amtsenthebung

In Anlehnung an die Neuregelung von § 25 Abs. 4 lit. e GOG ist eine neue Bestimmung zu schaffen, wonach eine Amtsenthebung als Folge einer PSP mit dem Ergebnis 'Sicherheitsrisiko' zulässig ist.

§ 15b Abs. 1 lit. d (neu) Kulturgesetz; Amtsenthebung

In Anlehnung an die Neuregelung von § 25 Abs. 4 lit. e GOG ist eine neue Bestimmung zu schaffen, wonach eine Amtsenthebung als Folge einer PSP mit dem Ergebnis 'Sicherheitsrisiko' zulässig ist.

8. Auswirkungen

8.1 Personelle und finanzielle Auswirkungen auf den Kanton

Mit dem Inkrafttreten des InfoSiG ergeben sich unmittelbare Auswirkungen in personeller und finanzieller Hinsicht aufgrund der Schaffung der Cyber-Koordinationsstelle und aufgrund der zusätzlich notwendigen PSP durch die Kantonspolizei. Da die entsprechende Aufgabenerfüllung mit den derzeitigen Ressourcen nicht zu bewältigen ist, bedarf es aus heutiger Sicht mindestens zweier Vollzeitstellen. Die Stellen werden unter Berücksichtigung des Anhörungsergebnisses im Rahmen des AFP 2026–2029 im Stellenplan eingestellt werden.

Die Bedrohungslage und mithin das Schadenspotenzial haben in einem Ausmass zugenommen, dass in Bezug auf die Informationssicherheit der unmittelbare Handlungsbedarf angegangen werden muss, ohne das Inkrafttreten des InfoSiG abzuwarten. Neben der Schaffung der gesetzlichen Grundlagen gemäss der vorliegenden Anhörungsvorlage hat der Regierungsrat deshalb bereits notwendige Massnahmen beschlossen. Um das angestrebte Sicherheitsniveau erreichen zu können, sind substanzielle Investitionen in technische und organisatorische Massnahmen zu tätigen sowie in personeller Hinsicht zusätzliche Stellen zu schaffen. Nebst der angemessenen Verstärkung der Fachstelle für Informationssicherheit bedarf es zusätzlicher Ressourcen für die mit ihr eng verbundenen Stellen innerhalb der Informatik Aargau, welche mit der Wahrnehmung von informationssicherheitsspezifischen Aufgaben (Cybersecurity-Engineering, sicherheitsrelevante Stellen im Rahmen von Entwicklung, Bereitstellung und Betrieb von Applikationen, Plattformen und Infrastrukturen) betraut sind und für die Rolle der Informationssicherheitsbeauftragten Personen (ISBP) in den Departementen, der Staatskanzlei und den Gerichten Kanton Aargau. Die benötigten personellen und finanziellen Ressourcen werden im AFP 2025–2028 eingestellt. Für die Massnahmen, die gemäss § 24 Abs. 1 GAF einen Verpflichtungskredit in der Kompetenz des Grossen Rats bedingen, wird dem Grossen Rat parallel zum Start der Anhörung eine entsprechende Botschaft unterbreitet. Das anvisierte Zielniveau für die Informationssicherheit sowie die dazu notwendigen Massnahmen werden in einem neuen Entwicklungsschwerpunkt "Informationssicherheit" im AFP 2025–2028 (Aufgabenbereich 435 'Informatik') aufgenommen werden.

Grundsätzlich ist zu erwähnen, dass die finanziellen Auswirkungen vom Sicherheitsniveau abhängen, das erreicht werden soll und auch davon, wie die technologische Entwicklung weitergeht. Die Planung des Regierungsrats sieht deshalb ein abgestuftes Vorgehen vor. Zunächst soll bis Ende 2026 der IKT-Minimalstandard des Bundes erreicht werden. Als strategische Zielsetzung wird mittelfristig ein Reifegrad angestrebt, der eine Zertifizierung nach ISO/IEC 27001 erlaubt. Der IKT-Minimalstandard unterstützt die vom Bund vorgegebenen Ziele zur Erreichung seiner Informationssicherheitsvorgaben und ist zwingend zu erreichen. Die mit dem Entwicklungsschwerpunkt "Massnahmen Informationssicherheit" assoziierten Kosten tragen zur Erreichung des Minimalstandards bei. Erst auf der Basis einer entsprechenden Analyse und des daraus ermittelten Handlungsbedarfs lässt sich evaluieren, ob eine Zertifizierung nach ISO/IEC 27001 überhaupt sinnvoll ist und welche Kosten mit deren Erfüllung verbunden wären.

8.2 Auswirkungen auf die Wirtschaft und die Gesellschaft

Dritte sind von der Wirkung des Gesetzes erfasst, wenn sie im Rahmen eines öffentlichen Auftrags oder der Auslagerung einer öffentlichen Aufgabe mit Informationen oder IKT-Mitteln des Kantons in Berührung kommen. Im Rahmen dieser Zusammenarbeit sollen den Unternehmen die Anforderungen und Massnahmen nach diesem Gesetz vertraglich überbunden und deren Umsetzung angemessen überprüft werden, soweit die Auftrags- beziehungsweise Aufgabenerfüllung sicherheitsrelevant ist (§ 11). Und Unternehmen, die an sicherheitsrelevanten Vergabeverfahren teilnehmen oder öffentliche Aufgaben des Kantons übernehmen wollen, müssen künftig eine sicherheitsspezifische Eignungsprüfung durchlaufen (§ 24). Neu ist nur die gesetzliche Statuierung dieser Pflicht, in der Praxis werden solche Massnahmen schon seit einigen Jahren ergriffen. Insbesondere bei sicherheitsrelevanten Vergaben werden bereits heute die Anforderungen an den Datenschutz und die Informationssicherheit in den Ausschreibungsunterlagen als Eignungskriterien formuliert und auch im Vertrag festgehalten. Es ergeben sich folglich durch die Neuregelung keine zusätzlichen Hürden für die Unternehmen, zumal für sie die Erfüllung der Anforderungen in der Regel auch kein Problem darstellt.

Im Übrigen wird ausdrücklich festgehalten, dass die neuen Regelungen zur Informationssicherheit Digitalisierungsvorhaben, die der Wirtschaft dienen, nicht behindern, sondern fördern sollen. Dies ist insofern selbstverständlich beziehungsweise systemimmanent, als die Informationssicherheit eine erfolgreiche Digitalisierung erst möglich macht.

Für die Gesellschaft bringt die vorgeschlagene Lösung Verbesserungen. Vorab wird Transparenz und damit Rechtssicherheit durch ausdrückliche Normen für die Informationssicherheit geschaffen. Dies stärkt das Vertrauen in das Funktionieren des Staats, da mit einer verbesserten Informationssicherheit auch die Erfüllung der Staatsaufgaben besser sichergestellt wird. Gleichsam dürfte sich auch das Vertrauen in den Staat insofern erhöhen, als die Gesellschaft im Umstand bestärkt wird, dass der Kanton mit Informationen und Daten verantwortungsvoll umgeht und diese sachgerecht schützt. Schliesslich profitiert die Gesellschaft auch von der verbesserten Zusammenarbeit zwischen Bund, Kanton und Gemeinden, welche aus der Umsetzung des vorliegenden Vorschlags resultieren sollte. Insbesondere die Schaffung einer verwaltungsübergreifenden Cyber-Organisation kann dazu beitragen, dass mit Vernetzung, Informationsaustausch und Sensibilisierung auch ausserhalb der Verwaltungsgrenzen, in Wirtschaft und Gesellschaft, der Fokus vermehrt auf die Risikominimierung und auf die Resilienz des Standorts Aargau gelegt wird (vgl. Kap. 5.2.4.2).

8.3 Auswirkungen auf die Umwelt und das Klima

Das neue Gesetz hat keine Auswirkungen auf die Umwelt und das Klima.

8.4 Auswirkungen auf die Gemeinden

Gemäss Geltungsbereich sollen die Vorschriften des neuen Gesetzes für Gemeinden nur zum Tragen kommen, wenn sie klassifizierte Informationen des Kantons bearbeiten und auf Informatikmittel

des Kantons zugreifen (§ 2 Abs. 2 lit. a und b). Die Vorschriften des Kantons über klassifizierte Informationen und die Sicherheit beim Einsatz von Informatikmitteln sollen jedoch in Berücksichtigung des Subsidiaritätsprinzips nur dann zur Anwendung kommen, wenn die Vorschriften und Massnahmen der Gemeinden den Sicherheitsanforderungen des Kantons nicht genügen. Das InfoSiG ist demnach nicht zu befolgen, soweit die Gemeinden bereits mit einer eigenen, mit derjenigen des Kantons vergleichbaren Informationssicherheit ausgestattet sind (§ 2 Abs. 3). Der vorliegende Gesetzesentwurf definiert, was dieses gleichwertige Sicherheitsniveau konkret bedeutet, weil es ansonsten für die Gemeinden nicht nachvollziehbar ist, was sie im Hinblick auf die Zielerreichung vorkehren müssen. Die Gemeinden müssen den IKT-Minimalstandard des Bundes erfüllen, der auch für den Kanton als Minimalstandard gilt, wenn sie im Rahmen der Bearbeitung von klassifizierten Informationen oder beim Zugriff auf Informatikmittel des Kantons nicht unter den Anwendungsbereich des InfoSiG fallen wollen. Mit § 2 wird demnach ein Mindestsicherheitsstandard für Gemeinden (und andere Träger öffentlicher Aufgaben) vorgegeben. Die Gemeinden sind mit zahlreichen kantonalen Systemen verbunden. Aufgrund der vielschichtigen Verbindungen der Gemeindeverwaltungen mit kantonalen Systemen muss sichergestellt werden, dass die Gemeinden die Einhaltung eines Mindestsicherheitsstandards hinsichtlich Sicherheit beim Einsatz von Informatikmitteln gewährleisten können. Ansonsten besteht das Risiko, dass sie zum Einfallstor für Angriffe auf kantonale Systeme werden (vgl. Erläuterungen zu § 2, Kap. 7.2.2).

Es ist demzufolge von Mehrkosten für die Gemeinden für die Gewährleistung der Sicherheit der mit dem Kanton gemeinsam betriebenen Applikationen beziehungsweise bei Nutzung der Systeme oder Bearbeitung von klassifizierten Informationen des Kantons auszugehen. Dieser Bedarf an erhöhter Informationssicherheit besteht für die Gemeinden jedoch unabhängig von der kantonalen Rechtsetzung. Auch sie bearbeiten klassifizierte Informationen und betreiben Informatiksysteme, die den beschriebenen Bedrohungen ausgesetzt sind. Deshalb ist es für die Gemeinden unabdingbar, gestützt auf die internationalen Standards den Schutz von Informationen und Informatikmitteln zu gewährleisten und zur Risikominimierung beizutragen. Wie auch die Wirtschaft und die Gesellschaft profitieren die Gemeinden aber von der Schaffung einer verwaltungsübergreifenden Cyber-Organisation. Mit der Cyber-Koordinationsstelle wird auch den Gemeinden eine Austauschpartnerin zur Verfügung stehen, deren Know-how genutzt werden, die offene Fragen beantworten, zur Vernetzung der öffentlichen und privaten Ebenen beitragen und mit gezielten Kampagnen zur Sensibilisierung für die Cyber-Bedrohungen und zur Stärkung der Resilienz beitragen kann.

Eine Information hat im Rahmen der Sitzung des Konsultationsgremiums Kanton-Gemeinden (KKG) vom 14. März 2024 stattgefunden. Die Gemeindevertretungen haben sich zu den Auswirkungen dahingehend geäussert, dass es ihnen bewusst sei, dass ein akuter Bedarf an Informations- und Cybersicherheit zum Schutz der Informationen und der Informatikmittel der Gemeinden - unabhängig von den Auswirkungen des kantonalen Gesetzesprojekts - bestehe. Sie äusserten den Wunsch, der Kanton möge sie unterstützen, indem er entsprechende Strukturen schaffe.

Dieses Anliegen ist in verschiedener Hinsicht problematisch. Der Kanton regelt die Sicherheit der ihm anvertrauten Informationen und seiner Informatikmittel. Die Gemeinden als autonome Staatsgebilde sind ihrerseits für die Sicherheit der ihnen anvertrauten Informationen und ihrer Informatikmittel zuständig. Es ist mithin ihre Aufgabe, diesen Schutz zu gewährleisten. Sie können diese ihnen durch die Verfassung zugewiesene Zuständigkeit nicht gegen Entgelt an den Kanton delegieren, weil sie dadurch gegen die staatsrechtliche Ordnung verstossen und die Gemeindeautonomie aushöhlen würden. Dem Kanton wäre es auch aufgrund des Gebots der staatlichen Wettbewerbsneutralität nicht gestattet, die Gemeinden gegen Entgelt zu unterstützen. Es gibt genügend Know-how auf dem freien Markt, der den Gemeinden zur Verfügung stünde. Der Kanton darf private Unternehmen nicht konkurrenzieren. Hier würde man gegenüber der Wirtschaft ein falsches Signal aussenden. Die Gemeinden haben sich selbst zu organisieren und sollten über die Zusammenarbeit erreichen, dass Synergien in Bezug auf die anfallenden Kosten erzielt werden können. Der Kanton ist bereit, die

Gemeinden auf ihrem Weg zu unterstützen durch enge Zusammenarbeit in den bestehenden Gremien und durch Erfahrungsaustausch.

8.5 Auswirkungen auf die Beziehungen zum Bund und zu anderen Kantonen

Die Beziehungen zum Bund vereinfachen sich, da eine weitgehende, aber stufengerechte Angleichung an das ISG erfolgt. Insbesondere sollen die Begriffe im Sinne des Bundesrechts verwendet werden, was zu einem gemeinsamen Verständnis führt, und die Zusammenarbeit vereinfacht. Nennenswerte Auswirkungen auf die Beziehungen zu anderen Kantonen sind nicht ersichtlich.

9. Wirkungskontrolle

Eine Wirkungskontrolle dieses Gesetzes gemäss § 50 Abs. 4 lit. l des Gesetzes über die Organisation des Grossen Rates und über den Verkehr zwischen dem Grossen Rat, dem Regierungsrat und der Justizleitung (Geschäftsverkehrsgesetz, GVG) vom 19. Juni 1990 (152.200) ist nicht zielführend. Die neu im Gesetz festgeschriebenen Sicherheitsvorkehrungen und Massnahmen werden bereits heute zu einem relevanten Teil angewendet beziehungsweise ergriffen. Die Gesetzgebung ist in diesem Sinne weitgehend lediglich verfassungsmässig bedingter Nachvollzug der heute gelebten Praxis. Im Nachhinein kann aber kaum festgestellt werden, ob mit den derzeit angewendeten Massnahmen und eingesetzten Systemen ein unter dem neuen Gesetz erfolgter Angriff hätte abgewehrt werden können oder nicht. Eine entsprechende Aussage hätte eine bloss theoretische Bedeutung. Um eine aussagekräftige Analyse vornehmen zu können, müssten zudem bereits die heutigen Sicherheitsvorkehrungen auf ihre Wirksamkeit hin geprüft werden. Ohne Wirkungskontrolle des Status quo ist eine Prüfung der durch die neue Gesetzgebung erzielten Wirkung nicht möglich beziehungsweise nur mit einem unverhältnismässigen Aufwand, weshalb darauf verzichtet werden soll.

10. Weiteres Vorgehen

Anhörung	8. Mai bis 16. August 2024
Verabschiedung Botschaft 1. Beratung	1. Quartal 2025
1. Beratung im Grossen Rat	2. Quartal 2025
Verabschiedung Botschaft 2. Beratung	4. Quartal 2025
2. Beratung Grosser Rat, inkl. Redaktionslesung	1. Quartal 2026
Referendumsfrist	2. Quartal 2026
Inkrafttreten	1. Juli 2026

Was allfällige Ausführungsbestimmungen des Grossen Rats (§ 30 Abs. 1) betrifft, wird die Dekretsgebung im Zeitplan nicht berücksichtigt. Diese kann gestützt auf § 30 Abs. 2 auch nach Inkrafttreten dieses Gesetzes erfolgen.

Beilagen

- Beilage 1: Synopse E-InfoSiG
- Beilage 2: Synopse Fremdänderung Schulgesetz
- Beilage 3: Synopse Fremdänderung Kulturgesetz
- Beilage 4: Begriffe Informationssicherheit