SJSD/Entwurf vom 11.10.2022

Erläuternder Bericht zum Entwurf des Reglements über die Informationssicherheit (ISR)

1 EINLEITUNG

Mit diesem Reglement wird auf der Grundlage von national und international anerkannten Standards eine einheitliche Rechtsgrundlage für die Informationssicherheit auf kantonaler Ebene geschaffen. Sein Schwerpunkt liegt auf der Einführung einer Organisation für die kantonale Informationssicherheit und auf der Erarbeitung einer allgemeinen Informationssicherheitspolitik als Werkzeuge für die Governance im digitalen Zeitalter. Eine Delegierte oder ein Delegierter für Informationssicherheit (IS-Delegierte/r) erhält den Auftrag, die Anwendung der gemäss Reglement vorgeschriebenen Standards umzusetzen, zu überwachen und zu koordinieren. Er oder sie wird insbesondere auch den Staatsrat und die Direktionen in Fragen der Informationssicherheit beraten und den öffentlichen Organen Werkzeuge und Unterstützung anbieten, damit sie die Sicherheit ihrer IT-Ressourcen optimal und gewissenhaft verwalten können. Der oder die IS-Delegierte wird in seiner/ihrer Funktion eng mit der kantonalen Behörde für Öffentlichkeit, Datenschutz und Mediation (ÖDSMB) und mit dem Amt für Informatik und Telekommunikation (ITA) zusammenarbeiten.

Mit der Annahme dieses Reglements wird das aktuelle und teilweise obsolet gewordene Reglement über die Sicherheit der Personendaten vom 29. Juni 1999 aufgehoben. Der Anwendungsbereich soll auf alle Informationen ausgeweitet werden, die von staatlichen Organen bearbeitet werden.

2 ALLGEMEINER KONTEXT DES REGLEMENTS

Cyber-Vorfälle nehmen weltweit zu und auch die Schweiz bleibt davon nicht verschont. Das Nationale Zentrum für Cybersicherheit (NCSC) erhält durchschnittlich über 300 Meldungen von erfolgreichen oder versuchten Cyber-Angriffen pro Woche. Solche Vorfälle werden im Kanton Freiburg sehr ernst genommen. Deshalb wurde im Herbst 2021 unter der Leitung der Finanzdirektion eine Arbeitsgruppe mit Vertretenden der Staatskanzlei, des ITA und des Amtes für Gesetzgebung

eingesetzt. Im Lauf des Jahres 2022 kam es bei der Erarbeitung des Regierungsprogramms 2022–2026 zu einer neuen Aufgabenverteilung, bei welcher der SJSD eine führende Rolle im Bereich Informationssicherheit zugewiesen wurde. Die Arbeitsgruppe wurde deshalb um Vertretende dieser Direktion erweitert, die ebenfalls zum vorgeschlagenen Text beigetragen haben.

Die Arbeitsgruppe begann damit, die auf kantonaler Ebene geltenden Standards für die Informationssicherheit zu überprüfen und mögliche Lücken zu identifizieren. Die Überprüfung ergab, dass für die Bearbeitung von Personendaten mit dem Gesetz vom 25. November 1994 über den Datenschutz (DSchG; SGF 17.1) und dem Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten (DSR; SGF 17.15) ein recht gut entwickeltes Regelwerk besteht. Für die Bearbeitung der übrigen Informationen durch die öffentliche Verwaltung gibt es hingegen bis jetzt keine spezifischen Bestimmungen, mit Ausnahme einiger verstreuter Normen aus bereichsspezifischen Erlassen.

Der Anwendungsbereich des DSR ist formell auf die Bearbeitung von Personendaten beschränkt. Dennoch wurde das Reglement in der Praxis am häufigsten auf die Bearbeitung nicht-personenbezogener Daten angewandt, wenn ein Schutzbedarf festgestellt wurde. Dies gilt auch für die Sicherheitspolitik für die Informationssysteme (SPIS) nach Artikel 14 DSR. Beim grössten Teil der Bestimmungen handelt es sich in Wirklichkeit nicht um Standards, die speziell auf die Sicherheit von Personendaten zugeschnitten sind. Vielmehr fallen sie in den breiteren Bereich der Informationssicherheit. Obwohl die beiden Bereiche natürlich miteinander verbunden sind, gibt es dennoch Unterschiede, die eine getrennte Behandlung rechtfertigen. Während sich die Datenschutzgesetzgebung nur auf Personendaten bezieht und allgemein darauf abzielt, Personen gegen die missbräuchliche Bearbeitung ihrer Daten zu schützen, geht es bei der Informationssicherheit darum, das Informationskapital der öffentlichen Hand insgesamt als strategische und für das Funktionieren der Verwaltung unverzichtbare Ressource zu schützen.

Das Fehlen einer Gesetzgebung zur Informationssicherheit stellt somit eine Lücke dar, die es zu schliessen gilt. Der Reglementsentwurf, der nun in Vernehmlassung geht, ist deshalb ein konsolidiertes Regelwerk zur Informationssicherheit, das für alle Informationen gelten soll, die von der öffentlichen Hand bearbeitet und aufbewahrt werden.

3 NOTWENDIGKEIT DES ENTWURFS UND GEPRÜFTE OPTIONEN

Das vorliegende Reglement wird vorgeschlagen, nachdem das Büro der Informatikkommission des Staatsrats (das 2020 durch die Delegation für die Digitalisierung und die Informationssysteme [DIS] ersetzt wurde) Ende 2018 beschlossen hat, die Bereiche Informationssicherheit und Sicherheit der Informatikmittel zu trennen.

Bisher waren diese Bereiche durch das DSR und die aufgehobene Verordnung vom 3. November 2015 über das Informatik- und Telekommunikationsmanagement in der Kantonsverwaltung generell dem ITA zugewiesen. Abgesehen vom Schutz der Personendaten, der einen eigenen, der ÖDSMB zugewiesenen Bereich darstellt, lässt sich also sagen, dass generell hauptsächlich das ITA für die Informationssicherheit in der Verwaltung verantwortlich war. Deshalb hatte der Staatsrat einem Mitarbeiter des ITA ein Pflichtenheft mit dieser Aufgabe zugewiesen.

Der Bereich Informationssicherheit im engeren Sinne (Bearbeitung von Fachdaten) betrifft jedoch Aspekte, die nicht im Handlungsbereich des ITA liegen und auf die es wenig Einfluss hat. Aus diesem Grund hat der Staatsrat mit der Annahme der Verordnung vom 28. Juni 2021 über die Governance der Digitalisierung und der Informationssysteme des Staates (SGF 122.96.11) entschieden, den Bereich Informationssicherheit formell aus den Aufgaben des ITA herauszulösen. Das ITA soll sich in Zukunft auf die Sicherheit der Informatikmittel konzentrieren, die zu seinen Kernaufgaben

gehört (zum Unterschied zwischen den beiden Bereichen siehe Definitionen in Artikel 4 des Reglements). Aufgrund dieser Änderung musste die Frage der Informationssicherheit in der Verwaltung umfassender überdacht werden.

Zu Beginn wollte die Arbeitsgruppe eine Organisationsverordnung erstellen. Diese hätte sich darauf beschränkt, die Verantwortung für die Informationssicherheit neu auf die verschiedenen Ebenen und auf die verschiedenen Fachstellen der Verwaltung zu verteilen. Diese Option wurde jedoch verworfen. Stattdessen entschied man sich für ein neues konsolidiertes Reglement über die Informationssicherheit, das nicht nur eine neue Organisation etabliert, sondern auch eine Reihe von Regeln aufstellt, mit denen in der Verwaltung ein angemessenes Sicherheitsniveau erreicht werden soll. In diesem Zusammenhang entstand die Idee, das DSR zu aktualisieren, indem es in ein neues Reglement über die Informationssicherheit (ISR) integriert wird, damit es in Bezug auf bestehende Standards dem neusten Stand entspricht und sein Anwendungsbereich alle Informationen im Besitz der öffentlichen Hand umfasst.

Es stellte sich jedoch die Frage, ob das ISR nicht ebenso wie das neue Bundesgesetz über die Informationssicherheit (ISG) die die Form eines Gesetzes annehmen sollte. Die Arbeitsgruppe hat diese Idee jedoch verworfen, einerseits aus Effizienzgründen und andererseits, weil die vorgesehenen Bestimmungen hauptsächlich Organisationsnormen sind, die gemäss Artikel 188 KV in die Kompetenz des Staatsrats fallen. Es handelt sich zudem um einen hoch technischen Bereich, für den sich die Zuständigkeit des Staatsrats besser eignet als jene des Grossen Rates, zumal er sich rasch wandelt und deshalb schnelle Anpassungen erfordern kann. Im Übrigen haben auch andere Kantone die Form eines Reglements gewählt.

4 ALLGEMEINER ÜBERBLICK ÜBER DAS REGLEMENT

Mit dem neuen Reglement sollen die Zuständigkeiten im Bereich Informationssicherheit mit einem Paradigmenwechsel geklärt und neu verteilt werden. So soll der Bereich Informationssicherheit im weiteren Sinne, der hauptsächlich unter der Aufsicht der oder des zukünftigen IS-Delegierten und der entsprechenden Organisation stehen wird, von der Sicherheit der Informatikmittel getrennt werden, die in der Zuständigkeit des ITA verbleibt. Als eine der Hauptneuerungen des Reglements wird eine Stelle für einen oder eine IS-Delegierte geschaffen (vgl. Art. 10). Um dieser Person die Arbeit zu erleichtern, sieht das Reglement vor, dass in der Verwaltung Ansprechpersonen für Fragen der Informatiksicherheit und des Datenschutzes eingesetzt werden (vgl. Art. 9 Abs. 2 und 12).

Diese Organisation wird in den Kommentaren zu den einzelnen Artikeln erläutert.

5 UMSETZUNG SOWIE FINANZIELLE UND PERSONELLE AUSWIRKUNGEN

Die finanziellen und personellen Auswirkungen, die mit der Umsetzung des Reglements für die Verwaltungseinheiten einhergehen, sind nicht unerheblich. Die Kosten sollten jedoch auch nicht überbewertet werden: Zum einen formalisiert die Verordnung lediglich weitgehend unbestrittene Ziele, deren Unverzichtbarkeit niemand ernsthaft in Frage stellen kann und die im Wesentlichen bereits im aktuellen DSR enthalten waren. Zum anderen sind die dabei entstehenden Kosten unendlich viel geringer als jene von Sicherheitsvorfällen, die die Arbeit einer oder mehrerer Verwaltungseinheiten lahmlegen und/oder die Grundrechte der Einwohnerinnen und Einwohner des Kantons gefährden würden.

Wie dem auch sei, der oder die zukünftige IS-Delegierte, dessen oder deren Stelle mit Inkrafttreten des Reglements eigens geschaffen würde, wird den grössten Teil der Arbeit zu übernehmen haben. Angesichts der umfangreichen Aufgabe (vgl. Art. 10 ff.) müssten für die Funktion 1–2 VZÄ

bereitgestellt werden, wobei die Schaffung des 2. VZÄ derzeit geprüft wird. Diese VZÄ werden der Direktion zugewiesen, die für die Informationssicherheit verantwortlich ist, d. h. der SJSD. Das ITA, das bisher für die Informationssicherheit verantwortlich war, wird in der Praxis von diesen Aufgaben entlastet. Da der Staatsrat einem Mitarbeiter des ITA ein Pflichtenheft für diese Aufgabe zugewiesen hat, muss die Umlagerung der Stelle vom ITA zur SJSD geprüft werden.

Wie oben erwähnt, wird das ITA von seinen Aufgaben in Zusammenhang mit der Informationssicherheit im weiteren Sinne entlastet, damit es sich besser auf die Sicherheit der Informatikmittel konzentrieren kann. Es wird jedoch bei vielen Aufgaben regelmässig eng mit dem oder der IS-Delegierten zusammenarbeiten. Im Übrigen ist es weiterhin dafür zuständig, die beschlossenen technischen Sicherheitsmassnahmen konkret auf die Informatikmittel der Verwaltung anzuwenden und ihre Wirksamkeit zu überwachen. In dieser Hinsicht verpflichtet das Reglement das ITA dazu, gestützt auf die Sensibilität der Informationssysteme und der bearbeiteten Informationen verschiedene Sicherheitsstufen einzuführen und spezifische Massnahmen für die als kritisch eingestuften Infrastrukturen und Ressourcen zu ergreifen. Zum jetzigen Zeitpunkt ist es allerdings schwierig, wenn nicht gar unmöglich, die Kosten der technischen Massnahmen zu beziffern, die für die Verbesserung der Sicherheit der verwaltungseigenen Informationssysteme getroffen werden müssen. Mit Verweis auf die Rechtsprechung des Bundesgerichts wird jedoch darauf hingewiesen, dass diese Art von Ausgaben in der Regel als gebundene Ausgaben betrachtet werden und deshalb nicht den Regeln des Finanzreferendums unterliegen (Entscheid des BGer 1P.722/2000 vom 12. Juni 2001, E. 3b).

Die Direktionen müssen aus ihren Reihen mindestens eine Ansprechperson für Fragen der Informationssicherheit bezeichnen, die ihr Generalsekretariat und die untergeordneten Verwaltungseinheiten in der ersten Phase berät. Diese Aufgabe kann jedoch mit jener der Ansprechpersonen für Datenschutz kombiniert werden, die mit dem Vorentwurf des revidierten DSchG eingeführt werden. Die Ansprechpersonen werden in einem eigens dafür eingerichteten Netzwerk entsprechend geschult und können sich in diesem Rahmen direkt an die/den IS-Delegierte/n und an die/den Datenschutzbeauftragte/n wenden. Da sich die beiden Funktionen sehr ähneln, können sie von ein und derselben Person ausgeübt werden.

Die Mehrarbeit, die mit der Einführung einer Ansprechperson für Informationssicherheit entsteht, wird auf 0,5 VZÄ pro Direktion sowie für die Staatskanzlei und die Gerichtsbehörden geschätzt.

Gleichzeitig steht fest, dass bei Inkrafttreten des Reglements Informations- und Schulungsveranstaltungen nötig sein werden. Dieser Aufwand wird zwischen dem oder der zukünftigen IS-Delegierten, dem ITA, der ÖDSMB und dem Amt für Personal und Organisation (POA) aufgeteilt.

6 ÜBEREINSTIMMUNG MIT ÜBERGEORDNETEM RECHT UND EUROPARECHT

Die Bestimmungen des Reglements beziehen sich im Wesentlichen auf den Bereich der Organisation, für den die Bundesverfassung die Autonomie der Kantone anerkennt (vgl. Art. 47 Abs. 2 BV). Die Kantonsverfassung sieht ihrerseits vor, dass solche Regeln generell in die Zuständigkeit des Staatsrats fallen (vgl. Art. 118 KV). Das Reglement ist somit aus organisationsrechtlicher Sicht mit der Bundesverfassung und der Kantonsverfassung vereinbar.

Die geplanten Regeln stehen nicht im Widerspruch zu den Datenschutzregeln auf europäischer Ebene, sondern präzisieren und ergänzen sie. Auch die Unabhängigkeit der Datenschutzbehörde wird durch das Reglement nicht in Frage gestellt, denn diese behält alle ihre Vorrechte in Bezug auf die Bearbeitung von Personendaten. Es besteht also keine Unvereinbarkeit mit den internationalen Verpflichtungen der Schweiz.

7 KOMMENTAR ZU DEN EINZELNEN ARTIKELN

Artikel 1 Gegenstand

Aus Artikel 1 Abs. 1 geht hervor, dass sich das ISR nicht nur auf die Sicherheit der Informationen als solche bezieht, sondern auf sämtliche Prozesse und Mittel mit denen diese Informationen bearbeitet werden.

Der Begriff der Informationssicherheit beruht im Allgemeinen auf anerkannten Standards. Informationssicherheit umfasst daher alle technischen und organisatorischen Massnahmen, mit denen die Integrität, Verfügbarkeit, Vertraulichkeit, Nachvollziehbarkeit, langfristige Nutzbarkeit und Resilienz von Informationen geschützt wird (vgl. Art. 5 Abs. 1). Die Massnahmen können sich sowohl auf die Sicherheit der Bearbeitung als auch auf die Sicherheit der dafür erforderlichen Mittel beziehen. Die Informationssicherheit betrifft alle Bearbeitungsverfahren, ob elektronisch oder analog, und umfasst auch die Sicherheit von Personendaten im Sinne von Artikel 22 DSchG oder anderer Gesetze, die den Schutz von Informationen vorschreiben.

Informationssicherheit ist kein Selbstzweck. Sie dient der Fähigkeit der öffentlichen Hand, Entscheidungen zu treffen, zu handeln und die Aufgaben auszuführen, zu denen sie gemäss Verfassung und Gesetz verpflichtet ist, was die in Absatz 2 genannten Massnahmen rechtfertigt.

Artikel 2 Geltungsbereich

Idealerweise sollte der Geltungsbereich des Reglements so breit wie möglich sein, um sicherzustellen, dass das Sicherheitsniveau bei allen Informationen, die zur Erfüllung einer öffentlichen Aufgabe benötigt werden, unabhängig von der bearbeitenden Person gleich hoch ist. Dies betrifft in erster Linie die Organe der Kantonsverwaltung sowie Privatpersonen und Organe privater Institutionen, die öffentlich-rechtliche Aufgaben wahrnehmen. Damit deckt sich der Geltungsbereich mit jenem des DSchG.

Im Reglement werden allerdings einige Besonderheiten berücksichtigt:

- Es gibt beim Staat einige Institutionen, die ihre IT selbständig verwalten. Diese Institutionen werden die im Reglement vorgesehenen materiellen Regelungen zur Informationssicherheit und die AISP anwenden müssen, während sie ihre Organisationsautonomie behalten. Sie sind jedoch verpflichtet, eine Organisation für die Informatiksicherheit festzulegen und eine/n Informationssicherheitsverantwortliche/n zu ernennen (Abs. 2).
- Da es sich um einen Erlass des Staatsrats handelt, kann das Reglement dem Grossen Rat oder den Gerichtsbehörden aus Gründen der Gewaltentrennung eigentlich nicht auferlegt werden. Grundsätzlich liesse sich dies nur mit einem vom Grossen Rat verabschiedeten Gesetz erreichen (zum Entscheid für ein Reglement, s. Kap. 3 *in fine*). Da das Thema Informationssicherheit jedoch alle drei Gewalten gleichermassen betrifft, geht der Staatsrat davon aus, dass die betreffenden Organe die Regelungen freiwillig ganz oder teilweise übernehmen werden. Dies wird in Form von Vereinbarungen mit der Exekutive geschehen (Abs. 3).

Absatz 4 begründet einen Vorbehalt, mit dem der Geltungsbereich des Reglements aufgrund anderer kantonaler oder eidgenössischer Gesetze erweitert oder eingeschränkt werden kann.

Artikel 3 Gültigkeit für die Gemeinden

Um die Autonomie der Gemeinden zu wahren und ihnen gleichzeitig die Möglichkeit zu geben, die vom Staat bereitgestellten Ressourcen zu nutzen, sollen solche Fälle in einer Vereinbarung mit den

Gemeinden geregelt werden. Im Übrigen können sich die Gemeinden jederzeit auf die AISP beziehen, die frei verfügbar sein wird (s. Art. 18 Abs. 3).

Artikel 4 Begriffsbestimmung

Mit der Begriffsbestimmung werden Fachbegriffe, die im Reglement mehrmals verwendet werden, definiert. Es handelt sich um anerkannte Standards aus dem Bereich Informationssicherheit. Trotz kleiner Abweichungen entsprechen die Definitionen inhaltlich jenen der Normen-Reihe zum Management der Informationssicherheit (ISO 27000 ff.).

Artikel 5 Verantwortlichkeiten

Diese Bestimmung verankert den Grundsatz, wonach jedes Organ für die Informationen, über die es verfügt und die es bearbeitet, verantwortlich ist (Abs. 1). Dies schliesst jedoch nicht aus, dass speziell für dieses Thema eine Managementorganisation geschaffen wird, mit der Aufgaben unter den strategischen, operativen und ausführenden Organen aufgeteilt werden.

Es kommt immer öfter vor, dass mehrere Organe Informationen gemeinsam bearbeiten und für diese eine geteilte Verantwortung haben. In Übereinstimmung mit der Gesetzgebung über den Datenschutz (s. Art. 17 Abs. 2 und 19 Abs. 2 Bst. e DSchG) muss die Verteilung der Verantwortlichkeiten in einer Vereinbarung der beteiligten Parteien geregelt werden, sofern sie nicht bereits aus dem Gesetz hervorgeht. In der Vereinbarung wird insbesondere definiert, wer in welchem Umfang und in welcher Phase für welche Bearbeitungsschritte verantwortlich ist.

Ein Fall, in dem die Verteilung der Verantwortung feststeht und somit keine Vereinbarung erfordert, ist die Zusammenarbeit zwischen dem Fachorgan, das Informationen sammelt und bearbeitet, und dem ITA, das IT-Ressourcen zur Verfügung stellt, damit die Informationen aufbewahrt und verwendet werden können (Abs. 3). Da diese Ko-Verantwortung praktisch die gesamte Informationsverarbeitung der Kantonsverwaltung betrifft, schien es angebracht, sie direkt im Reglement zu verankern (vgl. auch Kommentar zu Art. 13).

Artikel 6 Staatsrat

Die Artikel 6–17 des Reglements sind der Schaffung einer eigenen Organisation für die Informationssicherheit gewidmet. An der Spitze dieser Organisation steht der Staatsrat, der in diesem Bereich eine strategische Rolle innehat.

Er wird dafür zuständig sein, die Hauptausrichtung im Bereich Informationssicherheit und die dafür bereitgestellten Mittel festzulegen (Abs. 1 Bst. a und c). Des Weiteren wird er die AISP (s. Kommentar zu Art. 18) beschliessen, die die meisten Regeln für den Bereich Informationssicherheit enthält (Bst. b).

Da der Status des oder der zukünftigen IS-Delegierten mit dem eines zentralen Dienstes vergleichbar ist, wird der Staatsrat schliesslich auch seine oder ihre Anstellung genehmigen (s. Art. 8 Abs. 1 Bst. d des Staatspersonalgesetzes; StPG).

Artikel 7 Sicherheits-, Justiz- und Sportdirektion

Diese Bestimmung nennt die Aufgaben der SJSD im Bereich Informationssicherheit, da diese Direktion die Zuständigkeit für das Thema übernimmt. Sie gewährleistet in Absprache mit der Konferenz der Generalsekretäre den Hauptkontakt zum Staatsrat.

Artikel 8 Konferenz der Generalsekretäre (KGS)

Als transversales Verwaltungsorgan ist die KGS am besten dafür geeignet, in Fragen der Informationssicherheit für eine gute Koordination mit der übrigen Verwaltung zu sorgen. Sie kann bei Meinungsverschiedenheiten im Bereich Informationssicherheit zwischen der oder dem IS-Delegierten und einer Direktion auch die Schlichtungsrolle übernehmen.

Artikel 9 Direktionen des Staatsrats

Mit dem heutigen DSR wurden die Direktionen bisher wenig in die Informationssicherheit einbezogen. Das vorliegende ISR sieht für sie namentlich die Pflicht vor, bei sich ein Kompetenzzentrum einzurichten, das als erste Anlaufstelle fungiert und für die Einhaltung der Sicherheitsvorschriften durch die unterstellten Einheiten und für den Schulungsbedarf der Angestellten zuständig ist. Weiter müssen die Direktionen ihren Budgetbedarf für die Informationssicherheit planen und allfällige Meinungsverschiedenheiten mit einer unterstellten Einheit oder der/dem IS-Delegierten ausräumen (Abs. 1).

Für die Schaffung des Kompetenzzentrums als erste Anlaufstelle müssen die Direktionen mindestens eine Ansprechpersonen für alle Fragen des Datenschutzes und der Informationssicherheit bezeichnen (Abs. 2). Diese Funktion kann mit derjenigen der Ansprechperson für Datenschutz kombiniert werden, die im Prinzip im Rahmen der Totalrevision des DSchG eingeführt wird. Die Ansprechpersonen erhalten eine besondere Ausbildung in einem Netzwerk, das unter dem Vorsitz der oder des IS-Delegierten steht, und dürfen sich direkt an den oder die IS-Delegierte bzw. an den oder die Datenschutzbeauftragte wenden.

Artikel 10 Delegierte/r für Informationssicherheit – Aufgaben

Mit dem Reglement wird die neue Funktion einer/eines Delegierten für Informationssicherheit (IS-Delegierte/r) eingeführt. Es handelt sich um eine anspruchsvolle Funktion, die gleichzeitig Vertrautheit mit technischen Werkzeugen und kommunikative, strategische, Audit-, Schulungs-, Management- und Koordinationskompetenzen erfordert. Grundkenntnisse über den rechtlichen Rahmen werden ebenfalls verlangt.

Der Reglementsentwurf beschreibt einige der Hauptaufgaben, die der oder die zukünftige IS-Delegierte zu erfüllen hat (Abs. 2). In der Praxis ist allerdings mit einem weit umfangreicheren Pflichtenheft zu rechnen. Vereinfacht kann gesagt werden, dass der oder die IS-Delegierte in der Lage sein muss, nicht nur die AISP zu verfassen und nachzuführen, sondern auch neue Risiken zu erkennen, die Kontrolle der Umsetzung vorgeschriebener Präventions-, Erkennungs- und Korrekturmassnahmen zu planen und sicherzustellen, um (allfällige) Sicherheitsvorfälle zu bewältigen, und vor allem alle Akteure auf allen Verwaltungsebenen zu beraten und zu sensibilisieren, sei es mit der Veröffentlichung von Richtlinien oder mit Aktionen direkt vor Ort, damit alle die richtigen Verhaltensweisen verinnerlichen.

Der oder die zukünftige IS-Delegierte wird direkt in das Generalsekretariat der SJSD integriert. Es ist jedoch der Staatsrat, der ihm Weisungen für die Ausübung seiner Funktion erteilt. Die SJSD wird also im Bereich Informatiksicherheit die Rolle eines zentralen Dienstes übernehmen.

Artikel 11 Delegierte/r für Informationssicherheit – Zusammenarbeit

Der oder die zukünftige IS-Delegierte soll nicht ein neues Kontroll- oder Aufsichtsorgan im eigentlichen Sinn werden, wie dies beispielsweise bei der ÖDSMB der Fall ist, der das DSchG solche

Aufgaben überträgt. Die betreffende Person wird deshalb keine Entscheidungskompetenz haben. Ebenso wenig ist es vorgesehen, dass sie Empfehlungen abgeben kann, die eine gerichtliche Kontrolle erlauben, wie dies beim aktuellen DSchG der Fall ist.

Der oder die IS-Delegierte wird jedoch den Auftrag haben, mit allen Verwaltungsebenen zusammenzuarbeiten und Informationen auszutauschen. Wenn er oder sie bei einer Verwaltungseinheit informationssicherheitstechnische Mängel feststellt und diese nicht freiwillig Massnahmen zu ihrer Behebung ergreift, so kann der oder die IS-Delegierte die betroffene Direktion darüber informieren (s. Art. 9).

Um der oder dem IS-Delegierten die Arbeit zu erleichtern, sieht das Reglement vor, dass er oder sie von den Verantwortlichen der Datensammlung / für die Bearbeitung und von den übrigen Organen der Verwaltung alle für die Erfüllung ihrer/seiner Aufgabe notwendigen Informationen verlangen kann, ohne dass ihm/ihr das Amtsgeheimnis entgegengehalten werden könnte. Damit erhält der oder die IS-Delegierte eine Untersuchungsbefugnis, die für seine oder ihre Tätigkeit erforderlich ist.

Artikel 12 Netzwerk der Ansprechpersonen für Informationssicherheit und Datenschutz

Obwohl jede Organisation ihre eigenen Besonderheiten aufweist, lässt sich ein homogenes Sicherheitsniveau in der Verwaltung nur mit der Entwicklung eines gemeinsamen Verständnisses und gemeinsamer Praktiken erreichen. Die Ansprechpersonen des Netzwerks werden sich dank ihres Status mit der Situation und den Problemen der Informationssicherheit in ihrem Zuständigkeitsbereich gut auskennen, namentlich was die Anwendbarkeit und die Wirksamkeit von Vorschriften und Massnahmen betrifft. Das Netzwerk wird sich hauptsächlich damit befassen, den Vollzug und die Evaluation der vorgeschlagenen Normen zu koordinieren. Es kann auch zur Risikoerkennung und zur Ermittlung der nötigen Präventionsmassnahmen beitragen.

Das Netzwerk wird unter dem Vorsitz der oder des zukünftigen IS-Delegierten stehen.

Artikel 13 Amt für Informatik und Telekommunikation

Nach Annahme des ISR wird sich das ITA auf die Sicherheit der Informatikmittel konzentrieren, die es verwaltet und/oder die es den Leistungsempfängerinnen und Leistungsempfängern zur Verfügung stellt. Konkret bedeutet dies, dass das ITA für die Sicherheit der Server, der internen und externen Netzwerke der Verwaltung sowie der Anwendungen und Geräte (vor, während und nach ihrer Inbetriebnahme) verantwortlich ist, aber nur in Bezug auf das (materielle oder immaterielle) Produkt und seine Komponenten selbst. Das ITA trägt grundsätzlich keine Verantwortung für die Bearbeitungsschritte, die die Leistungsempfängerinnen und Leistungsempfänger dieser Produkte ausführen.

Artikel 14 Amt für Personal und Organisation

Das Amt für Personal und Organisation (POA) spielt als zentraler Dienst der Kantonsverwaltung bei der Digitalisierung eine wichtige Rolle: Einerseits begleitet und berät es die Verwaltungseinheiten bei ihrer Transformation, andererseits konzeptualisiert und koordiniert es die Entwicklung der erforderlichen Kompetenzen.

Artikel 15 Behörde für Öffentlichkeit, Datenschutz und Mediation

Die ÖDSMB ist die kantonale Fachbehörde für den Schutz von Personendaten. Das vorliegende Reglement hat keinerlei Einfluss auf die Zuständigkeiten und Rechte dieser Behörde. Diese bleiben

unangetastet. Abgesehen von der Integration des DSR in das ISR besteht die Hauptänderung darin, dass die ÖDSMB mit der oder dem IS-Delegierten eine bevorzugte Ansprechperson erhält. Die Beteiligung der oder des Datenschutzbeauftragten am Netzwerk der Ansprechpersonen für Informationssicherheit und Datenschutz wird im Übrigen auch im revidierten DSchG vorgeschrieben.

Artikel 16 Verwaltungseinheiten

Trotz seiner Ansiedlung am Ende der Sicherheitskette ist in erster Linie das Organ, das die Informationen bearbeitet, für deren Sicherheit verantwortlich, das heisst hauptsächlich der staatliche Dienst oder die autonome Einheit. Vereinbarungen über die Verantwortlichkeiten bei gemeinsamer Datenbearbeitung bleiben vorbehalten (s. Art. 5 Abs. 2).

In den Absätzen 1 und 2 werden die Konsequenzen dieser Verantwortung erläutert: Das verantwortliche Organ muss eine Risikobeurteilung vornehmen, geeignete technische und organisatorische Massnahmen gemäss den Artikeln 23–27 und der AISP vorschreiben, die Umsetzung dieser Massnahmen kontrollieren und das Personal schulen.

Artikel 17 Nutzerinnen und Nutzer

Die Nutzerinnen und Nutzer als letztes Glied in der Sicherheitskette müssen sich bei der Bearbeitung der Informationen, auf die sie zugreifen können, vorbildlich verhalten.

Der Geltungsbereich des Reglements beschränkt sich im Wesentlichen auf die Organe und das Personal der Verwaltung. Wenn externe Dritte einen Auftrag erhalten und auf die Informationssysteme des Staates zugreifen, muss der oder die Verantwortliche der Datensammlung / für die Bearbeitung mit einem Vertrag sicherstellen, dass sie die geltenden Sicherheitsregeln einhalten (Abs. 2). Bei Bedarf kann der oder die IS-Delegierte Vertragsvorlagen erstellen.

Artikel 18 Allgemeine Informationssicherheitspolitik des Staates – Grundsätze

Die AISP soll auf Kantonsebene zum wichtigsten Instrument der Informationssicherheit werden. Sie wird die wichtigsten Verhaltensregeln im Bereich Informationssicherheit enthalten, an die sich die Verwaltungseinheiten und die Staatsangestellten gemäss den genannten Grundsätzen zu halten haben (Abs. 2). Obwohl die AISP kein Erlass ist, wird ihr Inhalt mit der Annahme durch den Staatsrat für alle Organe, die der Exekutivgewalt des Staatsrats unterstellt sind, obligatorisch. Vorbehalten bleiben die nach Artikel 21 erlaubten Ausnahmen. Die AISP kann auch in besonderen, im Reglement vorgesehenen Einzelfällen (z. B. Art. 20) oder wenn es ein Vertrag vorsieht für obligatorisch erklärt werden. Sie wird allen Organen des Staates und allen Staatsangestellten zur Verfügung gestellt und im Internet veröffentlicht (Abs. 3).

Artikel 19 Allgemeine Informationssicherheitspolitik des Staates – Inhalt

Mit dieser Bestimmung werden die Leitlinien für den Inhalt der AISP (Abs. 1 und 2) festgelegt, allerdings mit dem Hinweis, dass es sich nicht um ein starres Instrument handelt. Die zukünftigen Änderungen der AISP werden von der oder dem zukünftigen IS-Delegierten vorgeschlagen (s. Art. 10 Abs. 2 Bst. b), von der Sicherheits-, Justiz- und Sportdirektion geprüft (s. Art. 7 Abs. 1 Bst. b) und schliesslich vom Staatsrat erlassen (s. Art. 6 Abs. 1 Bst. b).

Artikel 20 Allgemeine Informationssicherheitspolitik des Staates – Gültigkeit für die Gemeinden

Damit Lücken in der Sicherheitskette vermieden werden können, muss die AISP unbedingt auch für jene Gemeinden gelten, die auf die Informationssysteme des Staates zugreifen.

Artikel 21 Sektorspezifische Richtlinien zur Informationssicherheit

Es kann vorkommen, dass es in bestimmten Sektoren notwendig ist, für die Informationssicherheit und den Datenschutz spezifischere Regeln festzulegen. In diesem Fall dürfen die Direktionen und die autonomen Einheiten in einer Richtlinie ihre eigenen Regeln erlassen (Abs. 1). Zu erwähnen sind hier beispielsweise die Richtlinien der EKSD (heute BKAD) vom 28. März 2018 über die Internetnutzung und den Gebrauch digitaler Technologien in den Schulen oder die Richtlinien der SJD (heute SJSD) vom 27. April 2009 über die Dauer der Aufbewahrung und die Beseitigung der Polizeidaten. Bei Bedarf dürfen solche Richtlinien in bestimmten Punkten von der AISP abweichen (Abs. 2). Bei der Erarbeitung einer sektorspezifischen Richtlinie müssen der oder die IS-Delegierte und der oder die Datenschutzbeauftragte zwingend einbezogen werden (Abs. 3). Dies gilt nur für Richtlinien, die eine Direktion für ihre unterstellten Einheiten erlässt, und nicht für die internen Richtlinien einer Verwaltungseinheit.

Artikel 22 Leitlinie zur Informationssicherheit

Verwaltungseinheiten, die dies für notwendig erachten, können für ihr Personal Leitlinien zur Informationssicherheit und zum Datenschutz erlassen. Der oder die zukünftige IS-Delegierte wird entsprechende Vorlagen bereitstellen. Diese Leitlinien dürfen jedoch nicht von den Regeln abweichen, die in der AISP oder in einer sektorspezifischen Richtlinie festgelegt wurden.

Artikel 23 Risikobeurteilung

Die Risikobeurteilung besteht darin, für jeden relevanten Risikofaktor (Verfügbarkeit, Integrität, Vertraulichkeit, Nachvollziehbarkeit, langfristige Nutzbarkeit und Resilienz) die tiefer liegenden Schwachstellen und ihre möglichen Konsequenzen zu identifizieren, um die geeignetsten Korrekturen vornehmen zu können. Überdies soll die Risikobeurteilung den Verantwortlichen der Datensammlung / für die Bearbeitung dabei helfen, die Art ihres Informationskapitals, ihre Arbeitsprozesse und ihre kritischen technologischen Ressourcen besser einzuschätzen. Der oder die zukünftige IS-Delegierte wird eine Standardmethode für die Risikobeurteilung empfehlen.

Artikel 24 Festlegen von Massnahmen

Gestützt auf die Risikobeurteilung legt der Verantwortliche der Datensammlung / für die Bearbeitung an seine Tätigkeit und an die Sensibilität der bearbeiteten Informationen angepasste Sicherheitsmassnahmen fest (Abs. 1). Eine Liste der möglichen Massnahmen und die Art ihrer Umsetzung werden in der AISP ausgeführt. Wie die Bestimmung sagt, kann es sich dabei um technische, organisatorische, digitale oder analoge Massnahmen handeln. Für gewöhnlich wird unterschieden zwischen Massnahmen, die Risiken für einen Vorfall minimieren (Präventionsmassnahmen), und Massnahmen, mit denen die Folgen eines Vorfalls gemildert werden (Korrekturmassnahmen).

Artikel 25 Konzeption und Weiterentwicklung

Der Grundsatz der sicheren Softwareentwicklung «*Security by Design*» bedeutet, dass Verantwortliche der Datensammlung / für die Bearbeitung, die eine neue Datenbearbeitung etablieren wollen, die Sicherheitsaspekte ab der ersten Phase der Einführung dieser Bearbeitung berücksichtigen müssen. Dies umfasst insbesondere die Kosten, die mit den Sicherheitsmassnahmen verbunden sind.

Artikel 26 Restrisiken

Manche Risiken können selbst dann nicht oder nur ungenügend beseitigt werden, wenn sie bekannt sind. Sie können jedoch aufgrund einer umfassenden Interessenabwägung in Kauf genommen werden. Diese Bestimmung legt das Verfahren für solche Fälle fest. Sie wurde grösstenteils aus Artikel 14d Abs. 2 und 3 der Cyberrisikenverordnung des Bundes (CyRV; SR 120.73) übernommen.

Artikel 27 Regelmässige Überprüfung

Bei der Sicherheit der Informationstechnologien besteht ein konstanter Überprüfungsbedarf.

Artikel 28 Klassifikation der Informationen – Grundsätze

Im Bereich Informationssicherheit ist es Standard, die verschiedenen Kategorien gespeicherter Informationen einer Vertraulichkeitsstufe zuzuordnen. Die Zuweisung betrifft in der Regel ein Dossier als Ganzes. Es ist aber auch möglich, in einem Dossier verschiedene Vertraulichkeitsstufen anzuwenden, wenn sich der Schutzbedarf der einzelnen Dokumente unterscheidet.

Die vorgeschlagene Klassifizierung richtet sich generell nach den in diesem Bereich anerkannten Standards. Die gewählte Lösung basiert auf dem Grundsatz, wonach alle Informationen im Besitz von Behörden schutzwürdig sind. Der Vorschlag, standardmässig die Kategorie «nicht klassifiziert» zu verwenden bedeutet demnach nicht unbedingt, dass die so klassifizierten Informationen öffentlich zugänglich wären.

Die Vertraulichkeitsstufe hat insbesondere einen Einfluss auf die Festlegung der technischen und organisatorischen Massnahmen (Art. 29 Abs. 1 und 39 Abs. 1) sowie der Zugriffsberechtigungen (Art. 29 Abs. 2; Art. 30 Abs. 1 Bst. b und 32 Abs. 1) und auf die Vorkehrungen im Fall der Vernichtung (Art. 35 Abs. 2).

Artikel 29 Vertrauliche oder geheime Informationen

Im Bereich Informationssicherheit haben die Begriffe vertraulich und geheim eine eigene Bedeutung, die nicht unbedingt mit derjenigen des Datenschutzgesetzes oder anderer Geheimhaltungsvorschriften übereinstimmt (vgl. Art. 13 ISG). Ausschlaggebend für die Einstufung, die in der AISP näher erläutert wird, ist das Schadenspotenzial, das bei einem unbefugten Zugriff besteht.

Bei den vorgesehenen verstärkten Sicherheitsmassnahmen handelt es sich in Absatz 1 hauptsächlich um die Datenverschlüsselung und in Absatz 2 um die Festlegung der Zugriffsberechtigungen.

Artikel 30 Authentifizierung und Zugriffskontrolle

Die Sicherheit der Informationssysteme des Staates und der einzelnen Anwendungen wird durch Kontrollen bei der Zulassung gewährleistet. Erstens müssen die Nutzerinnen und Nutzer «authentifiziert» werden (Abs. 1 Bst. a) und zweitens müssen ihre Zugriffsrechte auf die Anwendungen und Daten beschränkt werden, die sie für die Erfüllungen ihrer Aufgabe benötigen (Abs. 1 Bst. b). In

manchen Fällen kann es notwendig sein, ein zusätzliches Zugriffskontrollsystem auf der Ebene der einzelnen Dossiers vorzusehen. Konkret wird dabei festgelegt, welche Subjekte oder Systeme Zugriff auf welche Objekten haben, und zwar in welchem Umfang, unter welchen Bedingungen, wann und wie lange.

Artikel 31 Protokollierung

Die Protokollierung der Datenbearbeitung ist eine Sicherheitsmassnahme, mit der die Operationen, die vor einem Sicherheitsvorfall ausgeführt wurden, rekonstruiert werden können. Mit dieser Massnahme wird also eher die Sicherheit der Informationssysteme und Anwendungen gewährleistet als die Vertraulichkeit von Informationen. Die Protokollierung kann auch angeordnet werden, um die Massnahmen zum Schutz der Vertraulichkeit von Daten durch eine nachträgliche Kontrolle der Datenbearbeitung in einem Informationssystem zu verstärken. Der Umfang und die Häufigkeit der Protokollierung hängen von den Umständen ab.

Weiter ist zu beachten, dass die Protokollierung eine Bearbeitung von Personendaten darstellt, die möglicherweise die Rechte der Nutzerinnen und Nutzern verletzt. Aus diesem Grund wird auf das DSchG verwiesen und an die Anmeldung der Bearbeitung/Datensammlung erinnert (Abs. 2). Die AISP wird zusätzliche Weisungen enthalten, namentlich zur Frage des Datenschutzes (Abs. 3).

Artikel 32 Abrufverfahren

Artikel 21 DSR über das Abrufverfahren (s. Artikel 4 Abs. 1 Bst. f) ist praktisch die einzige Bestimmung des Reglements, die sich ausschliesslich auf den Schutz von Personendaten bezieht. Deshalb dürfte sie eigentlich nicht in das vorliegende Reglement über die Informationssicherheit integriert werden. Da das DSR jedoch aufgehoben werden soll, wurde dies dennoch provisorisch getan. Sobald die Ausführungsgesetzgebung zum DSchG vorliegt, wird dieser Artikel aus dem ISR gestrichen und in den neuen Erlass verschoben.

Artikel 33 Private Geräte

Da die Nutzung privater Geräte für berufliche Zwecke immer mehr zunimmt, besteht in diesem Bereich ein klarer Regelungsbedarf. Da die Massnahmen zu spezifisch sind, werden sie in der AISP (s. Art. 18 und 19) oder auch in sektorspezifischen Richtlinien (s. Art. 21) festgelegt.

Artikel 34 Transversale und öffentlich zugängliche Informationssysteme

Das Sicherheitsaudit, von dem die Rede ist, kann entweder intern oder extern erfolgen. Dies hängt von den verfügbaren Kompetenzen und Ressourcen und/oder von der Kritikalität der betroffenen Informationssysteme ab.

Artikel 35 Archivierung und Vernichtung

Informationen, die zu nicht mehr laufenden Fällen gehören und vorarchiviert werden (Laufendes Archiv und Zwischenarchiv im Sinne der Gesetzgebung über die Archivierung), müssen weiterhin gesichert und geschützt werden (Abs. 1). Da diese Informationen von den staatlichen Diensten und autonomen Einheiten aufbewahrt werden, bleiben diese für ihre Sicherheit verantwortlich.

Für die Vernichtung von Dokumenten, die vertrauliche oder geheime Informationen enthalten, gelten nicht nur dann besondere Regeln, wenn die Dokumente in Papierform vorliegen (Notwendigkeit eines Aktenvernichters), sondern auch und vor allem, wenn es sich um Dokumente auf

Datenträgern handelt: Mit dem blossen Löschen der Daten lässt sich oft nicht ausschliessen, dass diese wiederhergestellt werden können. Deshalb sind zusätzliche Massnahmen vorzusehen (Abs. 2). Einzelheiten dazu sollen in der AISP ausgeführt werden.

Artikel 36 Schutz von Räumlichkeiten und Informatikmitteln

Die Informationssicherheit beschränkt sich nicht auf den IT-Bereich, sondern betrifft auch die physische und analoge Welt.

Artikel 37 Sicherheitsvorfälle

Diese Bestimmung betrifft nur Vorfälle, die die festgelegten Kriterien erfüllen. Kleinere Vorfälle, die keine wirklichen Auswirkungen auf die Tätigkeit einer Verwaltungseinheit haben, sind ausgeschlossen (s. Definition in Artikel 4 Abs. 1 Bst. e).

Ziel des Vorfallmanagements ist die Erkennung und Bearbeitung von Vorfällen vor, während und nach ihrem Auftreten. Weitere wichtige Elemente sind die Dokumentation (Reporting) und die Auswertung (Bilanz). Dies wird in einer entsprechenden Richtlinie festgelegt (s. Abs. 1 und 2).

Der Einbezug der ÖDSMB bei der Erarbeitung der Richtlinie (s. Abs. 3) soll eine Abstimmung mit dem DSchG sicherstellen, das diese Frage im Prinzip ebenfalls behandeln sollte.

Artikel 38 Richtlinie über die Sicherheit der Informatikmittel

Das ITA, das für die Sicherheit der Informatikmittel verantwortlich und in der Verwaltung deren Hauptlieferant ist, wird eine Richtlinie verfassen, in der die anwendbaren Mindeststandards und -normen sowie deren Umsetzung und Kontrolle für die gesamte Verwaltung festgelegt werden (Abs. 1 und 2). Falls die Verantwortlichen der Datensammlung / für die Bearbeitung bestimmte Operationen selbst ausführen müssen, weil sie sofort auf die Informatikmittel zugreifen können, wenn sie sich in ihrem Besitz befinden, wird das ITA den verantwortlichen Personen die nötigen Anweisungen geben (Abs. 3).

Artikel 39 Sicherheitsstufen

Bei den Informatikmitteln gibt es in der Regel zwei Sicherheitsstufen: Standard und erhöht. Auf jeder Stufe wird automatisch eine Reihe von vordefinierten Sicherheitsmassnahmen angewendet. Welche Sicherheitsstufe zur Anwendung kommt, hängt von verschiedenen Kriterien ab. Diese berücksichtigen einerseits den Schutzbedarf in Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität, Nachvollziehbarkeit, langfristige Nutzbarkeit und Resilienz der Informationen und andererseits die Kritikalität eines geordneten und verzögerungsfreien Ablaufs der Arbeitsprozesse, die vom betroffenen Informatikmittel unterstützt werden.

Die Sicherheitskategorie «Standardschutz» gilt für Informatikmittel, die keine besonderen Schutzanforderungen erfüllen müssen. Die überwiegende Mehrheit der Informationssysteme der Kantonsverwaltung dürfte in diese Sicherheitskategorie fallen. Mit Informatikmitteln dieser Kategorie können Personendaten, als «intern» klassifizierte Informationen und Informationen, deren Vertraulichkeit geschützt werden muss, ohne dass sie einen besonders hohen Schutz erfordern, bearbeitet werden.

In die Kategorie «erhöhter Schutz »werden Informatikmittel eingestuft, wenn der Missbrauch der Informationen, die mit ihnen bearbeitet werden, oder der Missbrauch des Informatikmittels selbst einen erheblichen Schaden verursachen kann, indem er die höheren Interesse des Staates gefährdet.

Betroffen sind Informatikmittel, mit denen Informationen der Kategorien «vertraulich» oder «geheim» bearbeitet werden. Wenn ein Informatikmittel einen Arbeitsprozess unterstützt, dessen Ausfall oder Störung den Handlungsspielraum einer Behörde erheblich beeinträchtigen kann, sollte das Informatikmittel ebenfalls dieser Kategorie zugeordnet werden.

Absatz 3 behält kritische Infrastrukturen und Anwendungen vor; die entsprechende Liste wird vom Staatsrat geführt. Diese Bestimmung sieht eine Art dritte Sicherheitsstufe in Form von «massgeschneiderten» Sicherheitsmassnahmen für die besonderen Bedürfnisse dieser Systeme vor.

Artikel 40 Technische Sicherheitsmassnahmen

Die Festlegung der standardisierten Sicherheitsmassnahmen für den Standardschutz und den erhöhten Schutz gehört zum Fachbereich des ITA und liegt deshalb in dessen Zuständigkeit und Verantwortung (Abs. 1). Die Massnahmen gelten für alle Verwaltungseinheiten des Staates mit Ausnahme der kritischen Infrastrukturen und Anwendungen (s. Art. 39 Abs. 4).

Das ITA muss künftig dafür sorgen, dass regelmässig überprüft wird, ob die Sicherheitsmassnahmen für die Sicherheitsstufe «erhöhter Schutz» immer noch dem neusten Stand der Technik entsprechen (Abs. 2 mit Verweis auf Art. 27).

Artikel 41 Verfahren bei Uneinigkeit

Das Reglement sieht ein Verfahren für Fälle vor, in denen sich das leistungsempfangende Organ und das ITA nicht über die Sicherheitsstufe einigen können, die einem Informationssystem oder einer Anwendung zuzuordnen ist. Solche Uneinigkeiten können direkt der DIS zum Entscheid vorgelegt werden.

Artikel 42 Zusammenarbeit im Bereich Informationssicherheit

Der Austausch von Informationen und Erfahrungen ist für die Informationssicherheit von entscheidender Bedeutung. In der Schweiz gibt es in diesem Bereich mehrere Kompetenzzentren, sowohl auf Kantons- wie auch auf Bundesebene. Es ist wichtig, dass sich auch der Kanton Freiburg an den Diskussionen in diesen Strukturen beteiligen kann.

Übrige Änderungen

Der Vollständigkeit halber sei hier noch erwähnt, dass die Verordnung über die Zuständigkeitsbereiche der Direktionen des Staatsrats und der Staatskanzlei (ZDirV) geändert werden muss, weil die SJSD die Informationssicherheit in ihren Zuständigkeitsbereich aufnimmt.

Bei den übrigen Änderungen handelt es sich um terminologische Anpassungen.