Version SJSD - Vernehmlassung Herbst 2022

Reglement über die Informationssicherheit (ISR)

vom ...

Betroffene Erlasse (SGF Nummern):

Neu:	**???.???**
Geändert:	122.0.12 | 122.0.31 | 122.0.51 | 122.96.11 | 184.16
Aufgehoben:	17.15

Der Staatsrat des Kantons Freiburg

gestützt auf Artikel 118 der Verfassung des Kantons Freiburg vom 16. Mai 2004;

auf Antrag der Sicherheits-, Justiz- und Sportdirektion,

beschliesst:

I.

1 Allgemeine Bestimmungen

Art. 1 Gegenstand

[1] Dieses Reglement hat zum Zweck, die Sicherheit der Informationen und der Informationssysteme der Kantonsverwaltung zu gewährleisten.

[2] Zu diesem Zweck wird mit diesem Reglement:

a) eine Organisation für die Informationssicherheit eingeführt;

b) der oder die Delegierte für Informationssicherheit (der oder die IS-Delegierte) eingesetzt;

c) die Erarbeitung einer allgemeinen Informationssicherheitspolitik (AISP) für die Kantonsverwaltung vorgeschrieben;

d) ein Grundbestand von gemeinsamen Mindestregeln für die Informationssicherheit festgelegt;

e) eine Reihe von Grundsätzen für die Sicherheit der Informatikmittel aufgelistet, sofern diese der Informationssicherheit dienen.

Art. 2 Geltungsbereich

[1] Dieses Reglement gilt für alle Direktionen und Einheiten der Kantonsverwaltung sowie für Privatpersonen und Organe von privaten Institutionen, die öffentlich-rechtliche Aufgaben erfüllen.

[2] Es gilt ausserdem für die autonomen Einheiten nach Artikel 2 Abs. 2 der Verordnung über die Governance der Digitalisierung und der Informationssysteme des Staates. Diese legen ihre eigene Organisation fest und ernennen ihre eigenen Informationssicherheitsverantwortlichen.

[3] Dieses Reglement gilt für den Grossen Rat und für die Gerichtsbehörden, sofern eine Vereinbarung mit dem Staatsrat dies vorsieht.

[4] Eidgenössische und kantonale Spezialbestimmungen zur Informationssicherheit bleiben vorbehalten.

Art. 3 Gültigkeit für die Gemeinden

[1] Wenn Gemeinden auf kantonale Informationssysteme zugreifen, werden die dafür erforderlichen Sicherheitsmassnahmen in einer Vereinbarung definiert. Artikel 20 bleibt vorbehalten.

Art. 4 Begriffsbestimmung

[1] In diesem Reglement werden folgende Begriffe verwendet:

a) Informationssicherheit: Gesamtheit der Normen, Massnahmen, Verfahren, Strategien Richtlinien, Risikomanagement-Methoden, Handlungen, Schulungen, bewährten Methoden und Technologien, die darauf abzielen, die Sicherheit der Informationen, die sich im Besitz der Kantonsverwaltung befinden und von ihr bearbeitet werden, zu verstärken;

b) Informationssystem: organisierte Gesamtheit von Ressourcen zur Erzeugung, Beschaffung, Gruppierung, Klassifizierung, Bearbeitung und Verbreitung von Informationen mithilfe von Informatikmitteln;

c) Informatikmittel: Gesamtheit von Hardware- und Software-Ressourcen, die aus Informations- und Kommunikationstechnologien bestehen;

d) Protokollierung: Registrierung aller oder eines Teils der Aktivitäten, die auf einem Informatiksystem ausgeführt werden, zur Kontrolle oder Rekonstruktion;

e) Sicherheitsvorfall: ein oder mehrere unerwünschte oder unerwartete Ereignisse in Zusammenhang mit der Informationssicherheit, bei denen eine hohe Wahrscheinlichkeit besteht, dass sie die Zuverlässigkeit und die Qualität der von einer Verwaltungseinheit bearbeiteten Informationen beeinträchtigen, die Weiterführung ihrer Tätigkeit gefährden und/oder eine Bedrohung für Personen innerhalb oder ausserhalb der Kantonsverwaltung darstellen;

f) Abrufverfahren: automatisierter Datenbekanntgabemodus, bei dem die Empfängerin oder der Empfänger der Daten aufgrund einer Bewilligung des Verantwortlichen der Datensammlung / für die Bearbeitung selbst und ohne vorherige Kontrolle über den Zeitpunkt und den Umfang der Bekanntgabe entscheidet.

Art. 5 Verantwortlichkeiten

[1] Jedes Organ, das über Informationen verfügt und diese bearbeitet, ist für deren Sicherheit und insbesondere für ihre Integrität, Verfügbarkeit, Vertraulichkeit, Nachvollziehbarkeit, langfristige Nutzbarkeit und Resilienz verantwortlich.

[2] Wenn mehrere Organe Informationen gemeinsam bearbeiten, wird die Aufteilung ihrer Verantwortlichkeiten in einer schriftlichen Vereinbarung festgehalten, sofern sie nicht ausdrücklich aus einer Gesetzesbestimmung hervorgeht.

[3] Im Übrigen ist das Amt für Informatik und Telekommunikation gemäss Artikel 13 für die Sicherheit der Informatikmittel verantwortlich.

2 Organisation

2.1 Strategische Organe

Art. 6 Staatsrat

[1] Der Staatsrat hat folgende Befugnisse:

a) Er legt die strategische Ausrichtung des Staates im Bereich Informationssicherheit fest.

b) Er erlässt die allgemeine Informationssicherheitspolitik des Staates.

c) Er schlägt im Rahmen des jährlichen Budgetverfahrens die für die Informationssicherheit benötigten Mittel vor.

d) Er genehmigt die Anstellung der oder des IS-Delegierten.

Art. 7 Sicherheits-, Justiz- und Sportdirektion (SJSD)

[1] Die SJSD hat folgende Befugnisse:

a) Sie ist Trägerin der Informationssicherheitsprojekte in der Kantonsverwaltung.

b) Sie nimmt zu Handen des Staatsrats Stellung zum Inhalt und zu späteren Änderungen der AISP.

c) Sie informiert den Staatsrat über alle wichtigen Geschäfte in Zusammenhang mit der Informationssicherheit.

d) Sie legt die Ausrichtung der empfohlenen Grundsätze oder Praktiken für die Informationssicherheit fest.

e) Sie erteilt der oder dem IS-Delegierten die Bewilligung für gezielte Aktionen, mit denen das Niveau der Informationssicherheit in der Kantonsverwaltung geprüft und/oder verbessert werden soll.

f) Sie genehmigt die Richtlinien, Empfehlungen und Leitlinien-Vorlagen, die der oder die IS-Delegierte erstellt.

g) Sie erteilt auf Empfehlung der oder des IS-Delegierten Aufträge an öffentliche oder private Dritte, damit diese das Niveau der Informationssicherheit in der Kantonsverwaltung prüfen.

Art. 8 Konferenz der Generalsekretäre (KGS)

[1] Die KGS hat folgende Befugnisse:

a) Sie koordiniert die Initiativen im Bereich Informationssicherheit innerhalb der Verwaltung und deren Umsetzung.

b) Sie nimmt Stellung zu den Budgeteingaben der Direktionen im Bereich Informationssicherheit.

c) Sie schlichtet bei allfälligen Meinungsverschiedenheiten zwischen der oder dem IS-Delegierten und einer Direktion.

[2] Die Person, die die SJSD in der KGS vertritt, sorgt für die Vor- und Nachbearbeitung der Dossiers im Bereich Informationssicherheit.

2.2 Operative Organe

Art. 9 Direktionen des Staatsrats

[1] Die Direktionen haben folgende Befugnisse:

a) Sie stellen sicher, dass die ihnen unterstellten Verwaltungseinheiten die Bestimmungen dieses Reglements und anderer, darauf beruhender Texte umsetzen.

b) Sie ermitteln ihren Budgetbedarf im Bereich Informationssicherheit.

c) Sie schlichten bei allfälligen Meinungsverschiedenheiten zwischen der oder dem IS-Delegierten und einer ihnen unterstellten Verwaltungseinheit.

d) Sie prüfen den Schulungs- und Sensibilisierungsbedarf des ihnen zugewiesenen Personals.

[2] Jede Direktion bezeichnet ausserdem mindestens eine Ansprechperson für Informationssicherheit. Die Ansprechperson für Informationssicherheit hat folgende Aufgaben:

a) Sie berät und unterstützt die Verwaltungseinheiten bei der Umsetzung ihrer Pflichten nach diesem Reglement.

b) Sie versichert sich bei den Verwaltungseinheiten, dass diese geeignete Sicherheitsmassnahmen ergriffen haben und dass die Massnahmen umgesetzt werden.

c) Sie ist in der Direktion Hauptansprechperson für alle Fragen zur Informationssicherheit.

d) Sie gehört dem Netzwerk der Ansprechpersonen für Informationssicherheit an.

[3] Die Funktion der Ansprechperson für Informationssicherheit kann der Person zugewiesen werden, die zur Ansprechperson für Datenschutz bestimmt wurde.

Art. 10 Delegierte/r für Informationssicherheit – Aufgaben

[1] Der oder die IS-Delegierte erfüllt seine oder ihre Aufgaben bereichsübergreifend für alle Direktionen.

[2] Er oder sie tut dies insbesondere wie folgt:

a) Er oder sie berät den Staatsrat sowie die Direktionen und Verwaltungseinheiten in Fragen der Informationssicherheit und der dafür erforderlichen Massnahmen.

b) Er oder sie erarbeitet die AISP und weitere Richtlinien im Bereich Informationssicherheit, sorgt für ihre Umsetzung und koordiniert ihre Ausführung.

c) Er oder sie erstattet der Sicherheits-, Justiz- und Sportdirektion regelmässig Bericht über den Stand der Informationssicherheit in der Kantonsverwaltung, über bekannte und neue Bedrohungen und über Massnahmen, die dagegen zu ergreifen sind.

d) Er oder sie organisiert im Rahmen seiner oder ihrer Kompetenzen Informationssicherheits-Audits.

e) Er oder sie beteiligt sich an der Konzipierung des Vorfallmanagementsystems.

f) Er oder sie organisiert gemeinsam mit der oder dem Datenschutzbeauftragten die Sitzungen des Netzwerks der Ansprechpersonen für Informationssicherheit und Datenschutz.

g) Er oder sie erfüllt die übrigen Aufgaben, die ihm oder ihr die SJSD im Bereich Informationssicherheit überträgt.

[3] Der oder die IS-Delegierte wird in das Generalsekretariat der SJSD integriert. Bei der Erfüllung der Aufgaben, die er oder sie für die gesamte Verwaltung erbringt, untersteht der oder die IS-Delegierte der Weisungsgewalt des Staatsrates. Artikel 51 Abs. 2 des Gesetzes über die Organisation des Staatsrates und der Verwaltung gilt sinngemäss.

Art. 11 Delegierte/r für Informationssicherheit – Zusammenarbeit

[1] Der oder die IS-Delegierte arbeitet bei der Erfüllung seiner oder ihrer Aufgaben mit folgenden Personen und Organen zusammen und tauscht mit ihnen Informationen aus:

a) mit der Konferenz der Generalsekretäre;

b) mit der oder den Personen, die beim Amt für Informatik und Telekommunikation (ITA) für die IT-Sicherheit verantwortlich sind;

c) mit den Informationssicherheitsverantwortlichen der Verwaltung und jenen der autonomen Einheiten nach Artikel 2 Abs. 2;

d) mit den Verantwortlichen der Datensammlung / für die Bearbeitung;

e) mit der oder dem Datenschutzbeauftragten in allen Fragen der sicheren Bearbeitung von Personendaten;

f) mit den übrigen Schweizer Behörden, die mit der Informationssicherheit beauftragt sind.

[2] Der oder die IS-Delegierte holt die für die Erfüllung seiner oder ihrer Aufgaben nötigen Informationen ein. Er oder sie kann namentlich Auskünfte oder das Vorlegen von Dokumenten verlangen, Inspektionen durchführen und sich Informationssysteme zeigen lassen. Das Amtsgeheimnis kann dem oder der IS-Delegierten nicht entgegengehalten werden.

Art. 12 Netzwerk der Ansprechpersonen für Informationssicherheit und Datenschutz

[1] Das Netzwerk ist ein interdisziplinärer Ausschuss, der wenn möglich Rechts-, Technik- und Managementkompetenzen vereint.

[2] Das Netzwerk hat folgende Aufgaben:

a) Es fördert den harmonisierten Vollzug dieses Reglements und der AISP in der Kantonsverwaltung.

b) Es beteiligt sich am Austausch von Informationen, namentlich über das Risikomanagement, über bewährte Methoden sowie über Probleme und Vorfälle im Bereich Informationssicherheit und Datenschutz;

c) Es unterstützt den oder die IS-Delegierte bei der Erarbeitung der verschiedenen Dokumente, die er oder sie gemäss diesem Reglement verfassen muss.

[3] Das Netzwerk steht unter dem Vorsitz der oder des IS-Delegierten und besteht aus der oder dem Datenschutzbeauftragten und mindestens einer Vertreterin oder einem Vertreter pro Direktion. Informationssicherheitsverantwortliche der autonomen Einheiten nach Artikel 2 Abs. 2 und der Gemeinden können ihm ebenfalls angehören.

2.3 Spezialisierte Organe

Art. 13 Amt für Informatik und Telekommunikation

[1] Das ITA ist für die Sicherheit der Informatikmittel, die es verwaltet und der Kantonsverwaltung zur Verfügung stellt, verantwortlich.

Art. 14 Amt für Personal und Organisation

[1] Das Amt für Personal und Organisation organisiert Schulungen für das Staatspersonal, um die Kompetenzen der Kantonsverwaltung im Bereich Informationssicherheit zu erweitern und zu festigen.

[2] Es wird bei dieser Aufgabe von der oder dem IS-Delegierten, von der oder dem Datenschutzbeauftragten und vom ITA unterstützt.

Art. 15 Behörde für Öffentlichkeit, Datenschutz und Mediation

[1] Die Beratungs- und Kontrollkompetenzen der Behörde für Öffentlichkeit, Datenschutz und Mediation im Bereich Schutz der Personendaten bleiben vorbehalten.

2.4 Fachorgane

Art. 16 Verwaltungseinheiten

[1] Die Verwaltungseinheiten nehmen für ihre Informationssysteme eine Beurteilung der relevanten Risiken vor und ergreifen geeignete Mittel, um deren Sicherheit gemäss diesem Reglement und der AISP zu gewährleisten.

[2] Sie sorgen für die Schulung ihres Personals und überprüfen regelmässig die Umsetzung der vorgeschriebenen Massnahmen durch ihre Mitarbeitenden.

[3] Artikel 5 Abs. 3 bleibt vorbehalten.

Art. 17 Nutzerinnen und Nutzer

[1] Die Mitarbeitenden, die vom Staat bereitgestellte Informationssysteme nutzen, sind für die Umsetzung der vorgeschriebenen Massnahmen nach diesem Reglement verantwortlich.

[2] Wenn es sich bei den Nutzerinnen und Nutzern um Auftragnehmende handelt, für die die Bestimmungen dieses Reglements nicht gelten, werden ihre Verantwortlichkeiten im Bereich Sicherheit in einem Vertrag festgelegt.

[3] Nutzerinnen und Nutzer, die bei der Erfüllung ihrer Aufgaben Mängel bei der Informationssicherheit entdecken, informieren ihre Vorgesetzten. Diese treffen geeignete Massnahmen.

3 Allgemeine Informationssicherheitspolitik des Staates

Art. 18 Grundsätze

[1] Der Staat definiert eine allgemeine Informationssicherheitspolitik.

[2] Die AISP umfasst folgende Grundsätze:

a) Risikomanagement

b) Schutz des Informationskapitals des Staates

c) Schutz der materiellen und immateriellen Ressourcen

d) Sicherstellung der Tätigkeiten der Kantonsverwaltung

e) Anwendung und Kontrolle der gesetzlichen und reglementarischen Bestimmungen, namentlich im Bereich Schutz der Personendaten

f) Abstimmung mit den Bedürfnissen der Kantonsverwaltung

[3] Die AISP wird auf der Website des Staates veröffentlicht.

Art. 19 Inhalt

[1] In Anwendung der Grundsätze soll die AISP namentlich:

a) den Steuerungs-, Bezugs- und Kohärenzrahmen für die Kantonsverwaltung setzen;

b) mit den geltenden Gesetzen und Reglementen übereinstimmen;

c) sich auf bewährte Methoden und anerkannte internationale Normen stützen;

d) die Verantwortlichkeiten beim Management der Informationssicherheit klären;

e) Regeln für die Erkennung, Bearbeitung und Behebung von Sicherheitsvorfällen definieren;

f) einen Kontinuitätsplan mit den Tätigkeiten, die für das Funktionieren des Staats bei einem Sicherheitsvorfall unverzichtbar sind, enthalten;

g) den Schulungs- und Sensibilisierungsbedarf des Personals berücksichtigen.

[2] In der AISP werden auch Regeln für ihre Umsetzung und Kontrolle definiert.

[3] Die AISP wird regelmässig nachgeführt.

Art. 20 Gültigkeit für die Gemeinden

[1] Die AISP gilt für die Gemeinden, wenn diese Informationssysteme der Kantonsverwaltung nutzen.

Art. 21 Sektorspezifische Richtlinien zur Informationssicherheit

[1] Die Direktionen und die autonomen Einheiten verfassen ihre eigenen Richtlinien zur Informationssicherheit und zum Datenschutz für die Sektoren, in denen es ihnen notwendig erscheint.

[2] Eine sektorspezifische Richtlinie kann in bestimmten Punkten von der AISP abweichen.

[3] Der oder die IS-Delegierte und der oder die Datenschutzbeauftragte werden bei der Erarbeitung einer sektorspezifischen Richtlinie einbezogen.

Art. 22 Leitlinie zur Informationssicherheit

[1] Verwaltungseinheiten, die grosse Datenmengen bearbeiten, können eine Leitlinie zur Informationssicherheit verfassen. Sie beziehen die für sie zuständige Ansprechperson für Informationssicherheit und/oder Datenschutz ein.

4 Mindestsicherheitsregeln

4.1 Allgemeine Grundsätze

Art. 23 Risikobeurteilung

[1] Das öffentliche Organ beurteilt das Risiko für die von ihm bearbeiteten Informationen in Bezug auf deren Verfügbarkeit, Integrität, Vertraulichkeit, Nachvollziehbarkeit, langfristige Nutzbarkeit und Resilienz.

[2] Das öffentliche Organ berücksichtigt in seiner Risikobeurteilung menschliche, technische und juristische Faktoren.

Art. 24 Festlegen von Massnahmen

[1] Das öffentliche Organ legt je nach Ausmass der Risiken und der Vertraulichkeitsstufe der Daten die geeigneten organisatorischen und technischen Massnahmen für eine Minimierung des Risikos fest; die Massnahmen können sowohl Prozesse, Personen und Räumlichkeiten als auch Material und die Sicherheit der Informatikmittel betreffen.

[2] Die Massnahmen müssen den Umständen angemessen, technisch geeignet, wirtschaftlich tragbar und praktisch umsetzbar sein.

Art. 25 Konzeption und Weiterentwicklung

[1] Die Anforderungen der Informationssicherheit, namentlich ihre Kosten, sind bei der Konzeption und bei der Weiterentwicklung von Informationssystemen zu berücksichtigen.

Art. 26 Restrisiken

[1] Das öffentliche Organ weist Risiken, die nicht oder nur ungenügend reduziert werden können (Restrisiken), aus und dokumentiert sie.

[2] Der Entscheid darüber, ob bekannte Restrisiken in Kauf genommen werden, obliegt der oder dem Verantwortlichen des betreffenden öffentlichen Organs. Bei Bedarf wird er mit der zuständigen Direktion besprochen.

Art. 27 Regelmässige Überprüfung

[1] Die Massnahmen, die im Bereich Informationssicherheit umgesetzt werden, müssen regelmässig, jedoch spätestens bei jeder Revision der AISP überprüft werden, um sie an die juristischen, organisatorischen und technologischen Änderungen und an die Entwicklung der Gefahren und Risiken anzupassen.

4.2 Klassifikation der Informationen

Art. 28 Grundsatz

[1] Das öffentliche Organ klassifiziert die Informationen, für die es verantwortlich ist, nach ihrer Vertraulichkeit und nach folgender Abstufung:

a) nicht klassifiziert;

b) interner Gebrauch;

c) vertraulich;

d) geheim.

[2] Die Klassifikation berücksichtigt die Art der bearbeiteten Informationen, ihren Wert, ihre Sensibilität und den Schaden, den eine unerlaubte Bekanntgabe für den Staat oder für die Personen, auf die sich die Informationen beziehen, verursachen könnte.

[3] Die Bestimmungen zum Auskunftsrecht aus dem Gesetz über die Information und den Zugang zu Dokumenten bleiben vorbehalten.

Art. 29 Vertrauliche oder geheime Informationen

[1] Als vertraulich oder geheim klassifizierte Informationen müssen bei der Übermittlung und bei der Aufbewahrung mit verstärkten Sicherheitsmassnahmen geschützt werden.

[2] Im Übrigen bestimmt das öffentliche Organ anhand der zu erfüllenden Aufgaben, welche Personen auf die vertraulichen oder geheimen Informationen zugreifen dürfen und in welchem Umfang.

4.3 Besondere Sicherheitsmassnahmen

Art. 30 Authentifizierung und Zugriffskontrolle

[1] Der Zugriff auf die Informationssysteme der Kantonsverwaltung ist mindestens mit den folgenden Massnahmen zu schützen:

a) einem Authentifizierungsverfahren, das mindestens die Identifizierung der Nutzerinnen und Nutzer und die Eingabe eines Passworts oder eines anderen Verifizierungsmittels beinhaltet;

b) einem Zugriffskontrollsystem, das auf der Festlegung individueller Zugriffsrechte beruht.

Art. 31 Protokollierung

[1] Wenn die Präventionsmassnahmen nicht ausreichen, um die Sicherheit der Informationen zu garantieren, so ist für ihre Bearbeitung ein Protokollierungsverfahren erforderlich.

[2] Für die Protokolldateien gelten die Regeln des Datenschutzes, insbesondere was die Anmeldung der Datensammlungen nach Artikel 19 des Gesetzes vom 25. November 1994 über den Datenschutz (DSchG) betrifft.

[3] Für das Aufbewahren, Verwenden und Vernichten der Protokolldateien gelten die Weisungen der AISP.

Art. 32 Abrufverfahren

[1] Bei der Einführung eines Abrufverfahrens im Sinne von Artikel 10 Abs. 2 DSchG werden die individuellen Zugriffsberechtigungen im Einvernehmen mit den Empfängerinnen und Empfängern der Daten vom Verantwortlichen der Datensammlung / für die Bearbeitung gemäss DSchG festgelegt.

[2] Der Verantwortliche der Datensammlung / für die Bearbeitung sorgt dafür, dass die Empfängerinnen und Empfänger die Daten weder ändern noch neue eingeben können und dass sie nur auf Daten zugreifen können, für die sie eine Zugriffsberechtigung haben.

[3] Das Abrufverfahren muss in einem Benutzerreglement dokumentiert werden, das insbesondere Folgendes präzisiert: die Personen, die Zugriff auf die Daten haben, die verfügbaren Daten, die Abfragehäufigkeit, das Authentifikationsverfahren, die weiteren Sicherheitsmassnahmen sowie die Kontrollmassnahmen. Eine Kopie des Reglements wird der zuständigen Aufsichtsbehörde für Datenschutz zugestellt.

Art. 33 Private Geräte

[1] Es sind besondere Massnahmen zu ergreifen, um zu verhindern, dass es bei der Verwendung privater Geräte zu Vertraulichkeitsverletzungen oder zu einer unerlaubten Bearbeitung kommt.

Art. 34 Transversale und öffentlich zugängliche Informationssysteme

[1] Alle transversalen oder öffentlich zugänglichen Informationssysteme müssen vor ihrer Inbetriebnahme ein Sicherheitsaudit durchlaufen.

Art. 35 Archivierung und Vernichtung

[1] Die Sicherheit der Informationen in den Zwischenarchiven muss sichergestellt sein.

[2] Informationen, die nicht für eine Archivaufnahme bestimmt sind, werden auf geeignete Weise vernichtet. Als vertraulich oder geheim klassifizierten Informationen wird besondere Beachtung geschenkt, um die Möglichkeit einer Wiederherstellung auszuschliessen.

Art. 36 Schutz von Räumlichkeiten und Informatikmitteln

[1] Alle Räume, in denen nicht öffentlich zugängliche Informationen aufbewahrt werden, müssen abgeschlossen oder überwacht werden.

[2] Der Schutz der Informatikmittel richtet sich nach den Bestimmungen der AISP, die diesbezüglich auf anerkannten Empfehlungen und Normen basiert.

Art. 37 Sicherheitsvorfälle

[1] Der oder die IS-Delegierte verfasst eine Richtlinie über das Sicherheitsvorfallmanagement. Bei Fragen, die die Sicherheit der Informatikmittel betreffen, arbeitet er oder sie bei dieser Aufgabe mit dem ITA zusammen.

[2] Die Richtlinie behandelt insbesondere die folgenden Punkte:

a) die Prozesse zur Erkennung, Meldung und Beurteilung von Vorfällen in Zusammenhang mit der Informationssicherheit;

b) die Interventions- und Bearbeitungsmassnahmen bei einem Vorfall;

c) die Verteilung der Rollen und Zuständigkeiten;

d) den Austausch und die Koordination mit dem oder der Datenschutzbeauftragten;

e) die Information der Öffentlichkeit.

[3] Die ÖDSMB wird bei der Erarbeitung der Richtlinie über den Umgang mit Sicherheitsvorfällen einbezogen.

5 Sicherheit der Informatikmittel

Art. 38 Richtlinie über die Sicherheit der Informatikmittel

[1] Das ITA verfasst eine Richtlinie über die Sicherheit der Informatikmittel.

[2] Die Richtlinie definiert mindestens:

a) die Mindeststandards und -normen für die Sicherheit der Informatikmittel;

b) die Einzelheiten für die Umsetzung der Sicherheitsmassnahmen und ihre Kontrolle.

[3] Das ITA wendet die Richtlinie über die Sicherheit der Informatikmittel an. Wenn nötig gibt es den zuständigen Organen Anweisungen.

Art. 39 Sicherheitsstufen

[1] Die Sicherheitsstufe der Informatikmittel hängt von der Klassifikation der bearbeiteten Informationen ab.

[2] Standardmässig wird die Sicherheitsstufe Standard angewandt.

[3] Eine erhöhte Sicherheitsstufe wird angewandt, wenn:

a) eine Verletzung der Vertraulichkeit, der Verfügbarkeit, der Integrität, der Nachvollziehbarkeit, der langfristigen Nutzbarkeit oder der Resilienz der Informationen den höheren Interessen des Staates schaden könnte; oder

b) der Missbrauch der Informationen oder ihre Beeinträchtigung den höheren Interessen des Staates schaden könnte.

[4] Für die Sicherheit der kritischen Infrastrukturen und Anwendungen gelten besondere Regeln, die vom Staatsrat genehmigt werden.

Art. 40 Technische Sicherheitsmassnahmen

[1] Das ITA legt die technischen Anforderungen fest, die für die Sicherheitsstufen nach Artikel 39 gelten.

[2] Das ITA stellt sicher, dass die technischen Sicherheitsmassnahmen für die erhöhte Sicherheitsstufe regelmässig kontrolliert werden.

Art. 41 Verfahren bei Uneinigkeit

[1] Sind das zuständige Organ und das ITA uneinig über die anzuwendende Sicherheitsstufe, so entscheidet die Delegation des Staatsrats für die Digitalisierung und die Informationssysteme.

[2] Der oder die IS-Delegierte wird angehört.

6 Zusammenarbeit mit dem Bund und den anderen Kantonen

Art. 42 Zusammenarbeit im Bereich Informationssicherheit

[1] Der oder die IS-Delegierte und das ITA arbeiten bei den verschiedenen Aspekten der Informationssicherheit und der Sicherheit der Informatikmittel mit dem Bund und den anderen Kantonen zusammen.

[2] Sie dürfen in diesem Rahmen Informationen und Personendaten mit den Fachstellen des Bundes und der Kantone austauschen.

II.

1.
Der Erlass SGF 122.0.12 (Verordnung über die Zuständigkeitsbereiche der Direktionen des Staatsrats und der Staatskanzlei (ZDirV), vom 12.03.2002) wird wie folgt geändert:

Art. 3 Abs. 1

[1] Der Zuständigkeitsbereich der Sicherheits-, Justiz- und Sportdirektion umfasst:

r) *(neu)* die Informationssicherheit.

und die weiteren Aufgaben, die ihr zugewiesen werden.

2.
Der Erlass SGF 122.0.31 (Reglement der Konferenz der Generalsekretäre, vom 11.12.1990) wird wie folgt geändert:

Art. 1 Abs. 2

[2] Die Konferenz nimmt, insbesondere im Hinblick auf die Planung, die Koordination und die Realisierung, Stellung zu Vorhaben und Fragen im Zusammenhang mit:

b1) *(neu)* der Informationssicherheit;

3.
Der Erlass SGF 122.0.51 (Verordnung über die Information über die Tätigkeit des Staatsrats und der Kantonsverwaltung (InfoV), vom 14.12.2010) wird wie folgt geändert:

Art. 34 Abs. 3 *(geändert)*

[3] Sie entsprechen den Anforderungen in Sachen Informationssicherheit und Schutz der Personendaten.

Art. 36 Abs. 2

[2] Das Amt für Informatik und Telekommunikation übernimmt die Verantwortung, die sich aus seiner Stelle als Fachdienst des Staates für Informatik ergibt; insbesondere:

c) *(geändert)* achtet es auf die Einhaltung des Richtplans und des Leitplans der Digitalisierung und der Informationssysteme gemäss den hierfür geltenden Bestimmungen;

4.
Der Erlass SGF 122.96.11 (Verordnung über die Governance der Digitalisierung und der Informationssysteme des Staates, vom 28.06.2021) wird wie folgt geändert:

Art. 4 Abs. 1

[1] Der Staatsrat hat insbesondere folgende Aufgaben:

b) *(geändert)* Er legt den politischen und reglementarischen Rahmen für die Entwicklung der Digitalisierung und der Informationssysteme des Staates fest und achtet dabei besonders auf die Informationssicherheit und auf die Sicherheit der Informatikmittel;

Art. 21

Sicherheit der Informatikmittel und Datenschutz *(Artikelüberschrift geändert)*

Art. A7-3 Abs. 1

[1] Die IKInfra hat folgende besondere Aufgaben:

a) *(geändert)* Sie nimmt Stellung zum Gesamtkonzept des ITA zu den Infrastrukturen der Digitalisierung und der Informationssysteme des Staates, sorgt für Kohärenz und für die Nutzung aller möglichen Synergien und achtet besonders auf die Sicherheit der Informatikmittel und die mit der technologischen Veralterung verbundenen Risiken.

5.

Der Erlass SGF 184.16 (Verordnung über das kantonale Bezugssystem von Daten von Personen, von Organisationen und von Verzeichnissen (Pilotprojekt), vom 24.06.2019) wird wie folgt geändert:

Art. A5-1 Abs. 1 *(geändert)*

[1] Der Schutz der Daten des kantonalen Bezugssystems wird mit den Massnahmen für die allgemeine Informationssicherheit harmonisiert. Die Massnahmen für die Sicherheit der Informatikmittel werden vom ITA, entsprechend den existierenden Risiken und Technologien, beantragt und umgesetzt.

III.

Der Erlass SGF 17.15 (Reglement über die Sicherheit der Personendaten (DSR), vom 29.06.1999) wird aufgehoben.

IV.

Dieses Reglement tritt am 00 Monat 0000 in Kraft.

[Signaturen]