Verordnung über die Informationssicherheit (ISV)

vom 06.07.2023 (Fassung in Kraft getreten am 21.04.2026)

Der Staatsrat des Kantons Freiburg

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

gestützt auf Artikel 70 des Gesetzes vom 16. Oktober 2001 über die Organisation des Staatsrates und der Verwaltung (SVOG);

gestützt auf Artikel 6 Abs. 2 des Gesetzes vom 10. September 2015 über die Archivierung und das Staatsarchiv (ArchG);

gestützt auf die Artikel 12d, 12e und 22 des Gesetzes vom 25. November 1994 über den Datenschutz (DSchG);

gestützt auf das E-Government-Gesetz vom 18. Dezember 2020 (E-GovG);

auf Antrag der Sicherheits-, Justiz- und Sportdirektion,

beschliesst:

1 Allgemeine Bestimmungen

Art. 1 Zweck und Gegenstand

[1] Diese Verordnung regelt die Einführung einer Organisation für die Informationssicherheit in der Kantonsverwaltung.

[2] Zu diesem Zweck werden mit dieser Verordnung:

a) die von der Informationssicherheit betroffenen Organe bestimmt;

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

c) die Hauptzuständigkeiten der betroffenen Organe und der oder des IS-Delegierten festgelegt.

Art. 2 Geltungsbereich

[1] Diese Verordnung gilt für den Staatsrat, die Direktionen und die Staatskanzlei und ihre Verwaltungseinheiten einschliesslich der autonomen Einheiten im Sinne von Artikel 2 Abs. 2 der Verordnung vom 28. Juni 2021 über die Governance der Digitalisierung und der Informationssysteme des Staates.

[2] Die autonomen Einheiten nach Absatz 1 legen ihre eigene Organisation fest und ernennen ihre eigenen Informationssicherheitsverantwortlichen oder können in die Organisation der Direktion, der sie administrativ zugewiesen sind, oder in diejenige einer anderen autonomen Einheit integriert werden.

[3] Die eidgenössischen und kantonalen Spezialbestimmungen zur Informationssicherheit bleiben vorbehalten.

Art. 3 Begriffsbestimmung

[1] In dieser Verordnung werden folgende Begriffe verwendet:

a) Informationssicherheit: Gesamtheit der Normen, Massnahmen, Verfahren, Strategien, Richtlinien, Risikomanagement-Methoden, Handlungen, Schulungen, Best Practices 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;

c) Informatikmittel: Gesamtheit von Hardware-, Software- und Netzwerkressourcen, die von Informations- und Kommunikationstechnologien gebildet werden;

d) Protokollierung: Registrierung aller oder eines Teils der Aktivitäten, die in einem Informationssystem 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 einem öffentlichen Organ bearbeiteten Informationen beeinträchtigen, die Weiterführung ihrer Tätigkeit gefährden und/ oder eine Bedrohung für Personen innerhalb oder ausserhalb der Kantonsverwaltung darstellen;

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

Art. 4 Verantwortlichkeiten

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

[2] Wenn mehrere öffentliche 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 (ITA) gemäss Artikel 13 für die Sicherheit der Informatikmittel verantwortlich.

2 Organisation

2.1 Strategische Organe

Art. 5 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 (AISP) des Staates.

c) Er beantragt im Rahmen des jährlichen Budgetierungsverfahrens die für die Informationssicherheit benötigten Mittel.

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

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

Art. 6 Sicherheits-, Justiz- und Sportdirektion (SJSD)

[1] Die Sicherheits-, Justiz- und Sportdirektion (SJSD) hat folgende Befugnisse:

a) Sie ist Trägerin der Informationssicherheitsprojekte in der Kantonsverwaltung.

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

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

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

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

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

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

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

Art. 7 Konferenz der Generalsekretäre (KGS)

[1] Die Konferenz der Generalsekretäre (KGS) koordiniert die Initiativen im Bereich der Informationssicherheit innerhalb der Kantonsverwaltung und deren Umsetzung.

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

2.2 Operative Organe

Art. 8 Direktionen des Staatsrates

[1] Die Direktionen haben folgende Befugnisse:

a) Sie stellen sicher, dass die ihnen unterstellten Verwaltungseinheiten die Bestimmungen dieser Verordnung 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 ihrer Verwaltungseinheiten.

d) Sie prüfen den Schulungs- und Sensibilisierungsbedarf ihres Personals.

Art. 9 Direktionen – IS-Ansprechpersonen

[1] 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 dieser Verordnung.

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 (Art. 12) an.

[2] 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] Die oder der Delegierte für Informationssicherheit (die/der IS-Delegierte) erfüllt ihre oder seine Aufgaben bereichsübergreifend für alle Direktionen.

[2] Sie oder er tut dies insbesondere wie folgt:

a) Sie oder er berät den Staatsrat, die Direktionen, die Verwaltungseinheiten und die IS-Ansprechpersonen in Fragen der Informationssicherheit und zu den dafür erforderlichen Massnahmen.

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

c) Sie oder er erstattet der SJSD regelmässig Bericht über den Stand der Informationssicherheit in der Kantonsverwaltung, über bekannte und neue Bedrohungen und über Massnahmen, die dagegen zu ergreifen sind.

d) Sie oder er organisiert im Rahmen ihrer oder seiner Kompetenzen Informationssicherheits-Audits.

e) Sie oder er beteiligt sich an der Konzipierung des Systems zum Management der Sicherheitsvorfälle.

f) Sie oder er organisiert die Sitzungen des Netzwerks der Ansprechpersonen für Informationssicherheit.

g) Sie oder er erfüllt die übrigen Aufgaben, welche die SJSD ihr oder ihm im Bereich Informationssicherheit überträgt.

[3] Die oder der IS-Delegierte wird in das Generalsekretariat der SJSD integriert. Bei der Erfüllung der Aufgaben, die sie oder er für die gesamte Kantonsverwaltung erbringt, untersteht sie oder er der Weisungsgewalt des Staatsrates. Artikel 51 Abs. 2 des Gesetzes vom 16. Oktober 2001 über die Organisation des Staatsrates und der Verwaltung gilt sinngemäss.

Art. 11 Delegierte/r für Informationssicherheit – Zusammenarbeit

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

a) mit der KGS;

b) mit den Präsidentinnen und Präsidenten der Fachkommissionen für die kantonale Informatik gemäss Artikel 15 der Verordnung über die Governance der Digitalisierung und der Informationssysteme des Staates (GDISV);

c) mit der oder den Personen, die beim ITA für die IT-Sicherheit verantwortlich sind;

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

e) mit den Verantwortlichen für die Bearbeitung;

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

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

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

Art. 12 Netzwerk der Ansprechpersonen für Informationssicherheit

[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 dieser Verordnung und der AISP in der Kantonsverwaltung.

b) Es beteiligt sich am Austausch von Informationen, namentlich über das Risikomanagement, über Best Practices sowie über Probleme und Vorfälle im Bereich Informationssicherheit.

c) Es unterstützt die IS-Delegierte oder den IS-Delegierten bei der Erarbeitung der verschiedenen Dokumente, die sie oder er gemäss dieser Verordnung 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 (IS-Ansprechperson). Informationssicherheitsverantwortliche der autonomen Einheiten nach Artikel 2 Abs. 2 GDISV und der Gemeinden können ihm ebenfalls angehören.

2.3 Fachorgane

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 und vom ITA unterstützt.

Art. 15 Behörde für Öffentlichkeit, Datenschutz und Mediation

[1] Die Beratungs- und Kontrollkompetenzen der Behörde für Öffentlichkeit, Datenschutz und Mediation (ÖDSMB) gemäss der Gesetzgebung über den Datenschutz bleiben vorbehalten.

2.4 Sachlich zuständige Organe

Art. 16 Verwaltungseinheiten

[1] Die Verwaltungseinheiten nehmen für ihre Informationssysteme eine Beurteilung der relevanten Risiken vor und ergreifen geeignete Mittel, um deren Sicherheit gemäss dieser Verordnung 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 4 Abs. 2 bleibt vorbehalten.

Art. 17 Benutzerinnen und Benutzer

[1] Die Mitarbeitenden, die vom Staat bereitgestellte Informationssysteme nutzen, achten auf die Umsetzung der vorgeschriebenen Massnahmen gemäss dieser Verordnung.

[2] Wenn es sich bei den Benutzerinnen und Benutzern um Auftragnehmende handelt, für welche die Bestimmungen dieser Verordnung nicht gelten, werden ihre Verantwortlichkeiten im Bereich Sicherheit in einem Vertrag festgelegt.

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

3 Zusammenarbeit mit dem Bund und den anderen Kantonen

Art. 18 Zusammenarbeit im Bereich Informationssicherheit

[1] Die oder der 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.

4 Gültigkeit

Art. 19 Geltungsdauer

[1] Diese Verordnung gilt bis zum Inkrafttreten des Gesetzes über die Informationssicherheit und dessen Ausführungsbestimmungen.

Änderungstabelle – Nach Beschlussdatum

Beschluss	Berührtes Element	Änderungstyp	Inkrafttreten	Quelle (ASF seit 2002)
06.07.2023	Erlass	Grunderlass	01.08.2023	2023_062
21.04.2026	Art. 11 Abs. 1, b)	geändert	21.04.2026	2026_035
21.04.2026	Art. 12 Abs. 3	geändert	21.04.2026	2026_035

Änderungstabelle – Nach Artikel

Berührtes Element	Änderungstyp	Beschluss	Inkrafttreten	Quelle (ASF seit 2002)
Erlass	Grunderlass	06.07.2023	01.08.2023	2023_062
Art. 11 Abs. 1, b)	geändert	21.04.2026	21.04.2026	2026_035
Art. 12 Abs. 3	geändert	21.04.2026	21.04.2026	2026_035