Reglement über die Sicherheit der Personendaten (DSR)

vom 29.06.1999 (Fassung in Kraft getreten am 01.01.2022)

Der Staatsrat des Kantons Freiburg

gestützt auf den Artikel 22 des Gesetzes vom 25. November 1994 über den Datenschutz (DSchG);

nach Einsicht in die Stellungnahmen der kantonalen Datenschutzkommission und der Informatikkommission des Kantons;

auf Antrag der Justiz-, Polizei- und Militärdirektion,

beschliesst:

1 Allgemeine Bestimmungen

Art. 1 Gegenstand und Anwendungsbereich

[1] Dieses Reglement legt die allgemeinen Grundsätze und die Mindestanforderungen für die Sicherheit der Personendaten fest.

[2] Es gilt für jegliche Bearbeitung von Personendaten, die dem Gesetz über den Datenschutz (DSchG) unterstellt ist.

[3] Besondere Bestimmungen des Bundes oder des Kantons über die Sicherheit gewisser Anwendungen bleiben vorbehalten.

Art. 2 Definitionen

[1] In diesem Reglement bedeuten die folgenden Ausdrücke:

a) Informatiksicherheit: der Bereich der Informatik, der den physischen Schutz der Informationsbearbeitungsstellen und der Telekommunikationsinfrastrukturen, die Integrität der Basis- und der Anwendungssoftware sowie die Integrität, die Verfügbarkeit und die Vertraulichkeit der gespeicherten und der über das Netz transportierten Daten gewährleisten soll;

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

c) Abrufverfahren: ein automatisierter Datenbekanntgabemodus, bei dem die Empfängerin oder der Empfänger der Daten aufgrund einer Bewilligung des Verantwortlichen der Datensammlung selber und ohne vorherige Kontrolle über den Zeitpunkt und den Umfang der Bekanntgabe entscheidet.

[2] Im Übrigen gelten die Definitionen nach Artikel 3 DSchG.

2 Regeln für alle Formen der Datenbearbeitung

Art. 3 Allgemeine Grundsätze

[1] Die Personendaten müssen gegen jede Verletzung der Vertraulichkeit und gegen jede unerlaubte Bearbeitung geschützt werden.

[2] Der Schutz ist in allen Phasen der Datenbearbeitung, von der Beschaffung bis zur Vernichtung, sicherzustellen; er ist gegenüber jeder Person innerhalb und ausserhalb der Verwaltung sicherzustellen.

[3] Der Schutz muss auf die Massnahmen zur Sicherheit der Verwaltungsdokumente im Allgemeinen wie auch auf die Massnahmen zur Informatiksicherheit abgestimmt werden.

Art. 4 Verantwortung – Des öffentlichen Organs

[1] Das öffentliche Organ, das Personendaten bearbeitet, ist für ihre Sicherheit verantwortlich.

[2] Nach einer Beurteilung der Risiken, die für die in Erfüllung seiner Aufgaben bearbeiteten Daten bestehen (Art. 8 f.), ordnet es die geeigneten Massnahmen an, damit die Sicherheit gewahrt bleibt (Art. 10 f.).

[3] Es kontrolliert regelmässig die Anwendung der angeordneten Massnahmen durch die Benutzerinnen und Benutzer.

Art. 5 Verantwortung – Der Benutzerinnen und Benutzer

[1] Die Mitarbeiterinnen und Mitarbeiter, die Personendaten bearbeiten, sind verantwortlich für die Durchführung der Massnahmen, die vom Organ, dem sie angehören, angeordnet wurden.

[2] Sind die Benutzerinnen und Benutzer beauftragte Dritte, die den Bestimmungen dieses Reglements nicht unterstellt sind, so werden ihre Verantwortlichkeiten im Bereich der Sicherheit im Vertrag, der in Artikel 18 Abs. 2 DSchG vorgesehen ist, festgelegt.

Art. 6 Verantwortung – Bei gemeinsamer Bearbeitung

[1] Bearbeiten mehrere öffentliche Organe zusammen Daten, so muss die Verteilung der Verantwortlichkeiten im Bereich der Sicherheit zwischen dem Verantwortlichen der Datensammlung und den daran Beteiligten in der Anmeldung der Datensammlung geregelt werden (Art. 19 Abs. 2 Bst. e DSchG).

Art. 7 Verantwortung – Vorbehalt

[1] Die besonderen Verantwortlichkeiten des Amtes für Informatik und Telekommunikation (das Amt) oder des zuständigen Informatikdienstes im Bereich der Informatiksicherheit bleiben vorbehalten.

Art. 8 Risikobeurteilung – Im Allgemeinen

[1] Das öffentliche Organ beurteilt für jede Datensammlung, wie hoch das Risiko ist, dass die Vertraulichkeit der Daten verletzt wird und dass die Daten unerlaubt bearbeitet werden; je nach Bedarf beurteilt es auch die Risiken einer Verletzung der Integrität und der Verfügbarkeit der Daten.

[2] Solche Risiken sind insbesondere:

a) das Risiko der Fälschung, des Diebstahls oder der widerrechtlichen Verwendung;

b) das Risiko des unbefugten Änderns, Kopierens oder Zugreifens;

c) das Risiko des zufälligen Verlusts oder technischer Fehler.

Art. 9 Risikobeurteilung – Zuweisung einer Vertraulichkeitsstufe

[1] Das öffentliche Organ weist jeder Datensammlung eine Vertraulichkeitsstufe zu. Es gilt die folgende Skala:

a) Stufe 1: öffentlich zugänglich;

b) Stufe 2: für internen Gebrauch;

c) Stufe 3: vertraulich oder geheim.

[2] Das Organ stützt sich dabei auf die Art der bearbeiteten Personendaten, den Zweck, den Umfang und die Formen der Bearbeitung sowie die Nachteile, die eine missbräuchliche Verwendung der Daten für die Betroffenen haben kann.

[3] Wenn nötig, kann auch bestimmten Daten oder Datenkategorien eine Vertraulichkeitsstufe zugewiesen werden.

Art. 10 Bestimmung der Massnahmen – Zugriffsberechtigung

[1] Das öffentliche Organ bestimmt aufgrund ihrer Aufgaben, welche Personen Zugriff auf die Datensammlungen haben wie auch den Umfang ihres Zugriffs.

[2] Eine Zugriffsberechtigung kann auch für bestimmte Daten oder Datenkategorien erteilt werden, insbesondere bei einer automatisierten Bearbeitung der Daten.

Art. 11 Bestimmung der Massnahmen – Organisatorische und technische Massnahmen

[1] Das öffentliche Organ bestimmt aufgrund des Ausmasses der Risiken und der Vertraulichkeitsstufe der Daten die geeigneten organisatorischen und technischen Massnahmen; diese können sowohl Personen und Räume als auch das Material und die Informatiksicherheit betreffen.

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

Art. 12 Periodische Überprüfung

[1] Das öffentliche Organ überprüft periodisch die Risiken und die getroffenen Massnahmen, vor allem in Bezug auf neue technische Möglichkeiten.

Art. 13 Archivierung und Vernichtung

[1] Die Sicherheit der Personendaten im Zwischenarchiv muss gewährleistet werden.

[2] Die Dokumente und anderen Träger von Personendaten, die nicht dem Archiv abzuliefern sind, müssen auf geeignete Weise vernichtet werden. Jede Möglichkeit einer Wiederherstellung der als vertraulich oder geheim klassifizierten Daten ist auszuschliessen.

3 Besondere Regeln für die automatisierte Datenbearbeitung

Art. 14 Wahrung der Informatiksicherheit

[1] Die Informatiksysteme, -anwendungen und -netzwerke, die der Bearbeitung von Personendaten dienen, müssen den Standardanforderungen der Informatiksicherheit genügen.

[2] Diese Anforderungen werden durch die Sicherheitspolitik für die Informationssysteme festgesetzt, das in den Bestimmungen über Planung und Anwendung der Informatik beim Staat vorgesehen ist.

[3] Die Sicherheitspolitik für die Informationssysteme wird den Gemeinden zur Verfügung gestellt. Sie ist für alle Gemeindesysteme verbindlich, die an das Netz der kantonalen Verwaltung angeschlossen sind.

Art. 15 Unterstützung und Beratung

[1] Bei einer automatisierten Datenbearbeitung berät und unterstützt das Amt die Dienststellen und Anstalten der kantonalen Verwaltung in allen Fragen im Zusammenhang mit der Sicherheit der Personendaten. Die besonderen Befugnisse der Universität und der zur Fachhochschule Westschweiz gehörenden Hochschulen im Informatikbereich bleiben vorbehalten.

[2] Bei allen Fragen im Zusammenhang mit der Umsetzung der Sicherheitspolitik für die Informationssysteme können auch die Gemeinden das Amt zur Beratung und Mithilfe beiziehen. Diese kann die daraus entstehenden Kosten in Rechnung stellen.

[3] Das Amt, die Universität und die zur Fachhochschule Westschweiz gehörenden Hochschulen arbeiten in diesem Bereich mit der kantonalen Behörde für Öffentlichkeit, Datenschutz und Mediation zusammen.

Art. 16 Anwendungen und Datensammlungen – Konzept

[1] Die Anforderungen für die Sicherheit der Personendaten müssen bereits beim Konzipieren der Anwendungen und der Datensammlungen berücksichtigt werden.

[2] Die entsprechenden Kosten müssen in die Finanzplanung der Anwendungen einbezogen werden.

Art. 17 Anwendungen und Datensammlungen – Authentifikation und Zugriffskontrolle

[1] Der Zugriff auf Informatiksysteme, mit denen Personendaten bearbeitet werden können, muss durch folgende Vorkehrungen geschützt werden:

a) ein Authentifikationsverfahren, das mindestens die Identifikation der Benutzerinnen und Benutzer sowie das Eingeben eines Passwortes beinhaltet;

b) ein Zugriffskontrollsystem, das auf einer Bestimmung individueller Zugriffsberechtigungen beruht.

[2] Der Zugriff auf Anwendungen und/oder Datensammlungen ist ebenfalls durch diese Massnahmen zu schützen, wenn:

a) als vertraulich oder geheim klassifizierte Daten bearbeitet werden, oder

b) die zuständige Aufsichtsbehörde für Datenschutz dies verlangt.

[3] Die Verantwortlichen für das System, die Anwendung oder die Datensammlungen bestimmen die individuellen Zugriffsberechtigungen aufgrund der Aufgaben, die die Benutzerinnen und Benutzer erfüllen müssen. Sie bezeichnen ein Organ, das unter ihrer Verantwortung die Zugriffsberechtigungen verwaltet und die Einzelheiten des Authentifikationsverfahrens regelt.

Art. 18 Anwendungen und Datensammlungen – Protokollierung

[1] Gewährleisten die präventiven Massnahmen die Sicherheit der Personendaten nicht hinreichend, so muss die Datenbearbeitung protokolliert werden.

Art. 19 Anwendungen und Datensammlungen – Ausübung der Rechte der Betroffenen

[1] Die Anwendungen und Datensammlungen müssen es den betroffenen Personen ermöglichen, ihr Auskunftsrecht über sie betreffende Daten (Art. 23–25 DSchG) wie auch ihre Rechte bei unrechtmässiger Bearbeitung auszuüben (Recht auf Berichtigung oder Vernichtung der Daten oder Recht auf Anbringen eines entsprechenden Vermerks, Art. 26 DSchG).

Art. 20 Netze und Übermittlung – Vertrauliche oder geheime Daten

[1] Die als vertraulich oder geheim klassifizierten Personendaten müssen bei der Übertragung und bei der Speicherung durch Verschlüsselung oder andere geeignete Massnahmen geschützt werden.

[2] Ist es unmöglich, die netzwerkbedingten Risiken auf ein vertretbares Mass zu senken, so muss der Datenverkehr durch Schaffung eines vom Hauptnetz getrennten virtuellen Netzes oder eine andere geeignete Massnahme isoliert werden.

Art. 21 Netze und Übermittlung – Abrufverfahren

[1] Wird ein Abrufverfahren eingerichtet, so werden die individuellen Zugriffsberechtigungen vom Verantwortlichen der Datensammlung und von der Empfängerin oder dem Empfänger der Daten im gegenseitigen Einvernehmen festgelegt.

[2] Der Verantwortliche der Datensammlung sorgt dafür, dass die Empfängerin oder der Empfänger die Daten nicht verändern und keine neuen Daten hinzufügen kann und nur zu den Daten Zugriff hat, für die sie oder er zugriffsberechtigt ist.

[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. 22 Netze und Übermittlung – Internet und Intranet

[1] Die Bestimmungen dieses Abschnitts gelten auch für die Bearbeitung von Daten über ein Netz wie Internet oder Intranet.

[2] Im Einvernehmen mit der kantonalen Behörde für Öffentlichkeit, Datenschutz und Mediation sorgen das Amt und der Informatikdienst der Universität dafür, dass den Benutzerinnen und Benutzern eines solchen Netzes eine allgemeine Information über die damit verbundenen Risiken abgegeben wird, insbesondere was die E-Mail betrifft; diese Information wird auch den Gemeinden zugestellt.

Art. 23 Periphere Geräte und Wartung

[1] Es sind besondere Massnahmen zu ergreifen, um zu vermeiden, dass es bei der Datenausgabe auf peripheren Geräten und bei Wartungsarbeiten zu Verletzungen der Vertraulichkeit oder zu einer unerlaubten Bearbeitung kommt.

Art. 24 Protokollierungsverfahren

[1] Wird ein Informatiksystem oder eine Informatikanwendung mit einem Verfahren zur Protokollierung der Vorgänge ausgerüstet, so unterliegen die Protokolldateien den Datenschutzbestimmungen, insbesondere was die Anmeldung nach Artikel 19 DSchG betrifft.

[2] Für die Aufbewahrung, die Auswertung und die Vernichtung der Protokolldateien werden im Informatiksicherheitskonzept, das in den Bestimmungen über Planung und Anwendung der Informatik beim Staat vorgesehen ist, Weisungen erlassen.

4 Aufsicht

Art. 25 Kontrolle durch die vorgesetzte Behörde

[1] Die vorgesetzte Behörde kontrolliert die Anwendung der Bestimmungen dieses Reglements durch die öffentlichen Organe, die ihr unterstehen.

Art. 26 Kontrolle durch die Aufsichtsbehörde

[1] Die zuständige Aufsichtsbehörde für Datenschutz übt die externe Kontrolle gemäss den Artikeln 29 ff. DSchG aus.

[2] Das kontrollierte öffentliche Organ arbeitet mit der Aufsichtsbehörde zusammen und liefert ihr sämtliche nötigen Angaben, vor allem diejenigen für die Risikobeurteilung, die Festlegung der Zugriffsberechtigungen, die Bestimmung der organisatorischen und technischen Massnahmen und die durchgeführten Überprüfungen.

Art. 27 Befugnisse des Amtes

[1] Die Befugnisse des Amtes oder gegebenenfalls des zuständigen Informatikdienstes bei der Kontrolle der Informatiksicherheit bleiben vorbehalten.

[2] Wenn die durchgeführten Kontrollen Lücken in der Sicherheit der Personendaten zutage bringen, so erstattet das Amt oder der zuständige Informatikdienst der oder dem direkten Vorgesetzten sowie der zuständigen Aufsichtsbehörde für Datenschutz Meldung.

Art. 28 Zufällige Feststellungen

[1] Stellen Mitarbeiterinnen oder Mitarbeiter bei der Erfüllung ihrer Aufgaben Lücken bei der Sicherheit der Personendaten eines anderen öffentlichen Organs als ihres eigenen fest, so informieren sie ihre Dienstchefin oder ihren Dienstchef; diese beziehungsweise dieser erstattet dem für die Daten verantwortlichen Organ Meldung.

5 Übergangs- und Schlussbestimmungen

Art. 29 Übergangsrecht

[1] Gemeinden mit alter Hardware und Software, die sich nur schwer an die Anforderungen der Informatiksicherheit anpassen lassen, können sich bis zum Auswechseln ihrer Hardware und Software mit physischen Massnahmen zur Gewährleistung der Sicherheit der Personendaten bei der automatisierten Bearbeitung begnügen.

Art. 30 Änderung bisherigen Rechts

[1] Der Beschluss vom 22. Dezember 1987 über die Planung und Anwendung der Informatik in der Kantonsverwaltung, im Unterrichtswesen und in den kantonalen Anstalten (SGF 122.96.11) wird wie folgt geändert:

...

Art. 31 Inkrafttreten und Veröffentlichung

[1] Dieses Reglement tritt am 1. Januar 2000 in Kraft.

[2] Es wird im Amtsblatt veröffentlicht, in die Amtliche Gesetzessammlung aufgenommen und im Sonderdruck herausgegeben.

Änderungstabelle – Nach Beschlussdatum

Beschluss	Berührtes Element	Änderungstyp	Inkrafttreten	Quelle (ASF seit 2002)
29.06.1999	Erlass	Grunderlass	01.01.2000	BL/AGS 1999 f 216 / d 219
14.11.2002	Art. 7	geändert	01.01.2003	2002_120
14.11.2002	Art. 15	geändert	01.01.2003	2002_120
14.11.2002	Art. 22	geändert	01.01.2003	2002_120
14.11.2002	Art. 27	geändert	01.01.2003	2002_120
03.12.2002	Art. 15	geändert	01.01.2003	2002_132
03.12.2002	Art. 22	geändert	01.01.2003	2002_132
14.12.2010	Art. 15	geändert	01.01.2011	2010_144
14.12.2010	Art. 22	geändert	01.01.2011	2010_144
03.11.2015	Art. 14	geändert	03.11.2015	2015_111
03.11.2015	Art. 15	geändert	03.11.2015	2015_111
04.06.2019	Art. 13	Titel geändert	01.07.2019	2019_043
04.06.2019	Art. 13 Abs. 1	geändert	01.07.2019	2019_043
31.01.2022	Art. 15 Abs. 3	geändert	01.01.2022	2022_010
31.01.2022	Art. 22 Abs. 2	geändert	01.01.2022	2022_010

Änderungstabelle – Nach Artikel

Berührtes Element	Änderungstyp	Beschluss	Inkrafttreten	Quelle (ASF seit 2002)
Erlass	Grunderlass	29.06.1999	01.01.2000	BL/AGS 1999 f 216 / d 219
Art. 7	geändert	14.11.2002	01.01.2003	2002_120
Art. 13	Titel geändert	04.06.2019	01.07.2019	2019_043
Art. 13 Abs. 1	geändert	04.06.2019	01.07.2019	2019_043
Art. 14	geändert	03.11.2015	03.11.2015	2015_111
Art. 15	geändert	14.11.2002	01.01.2003	2002_120
Art. 15	geändert	03.12.2002	01.01.2003	2002_132
Art. 15	geändert	14.12.2010	01.01.2011	2010_144
Art. 15	geändert	03.11.2015	03.11.2015	2015_111
Art. 15 Abs. 3	geändert	31.01.2022	01.01.2022	2022_010
Art. 22	geändert	14.11.2002	01.01.2003	2002_120
Art. 22	geändert	03.12.2002	01.01.2003	2002_132
Art. 22	geändert	14.12.2010	01.01.2011	2010_144
Art. 22 Abs. 2	geändert	31.01.2022	01.01.2022	2022_010
Art. 27	geändert	14.11.2002	01.01.2003	2002_120