Reglement

vom 29. Juni 1999

über die Sicherheit der Personendaten (DSR)

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. KAPITEL

Allgemeine Bestimmungen

Gegenstand und Anwendungsbereich

Artikel 1. [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.

Definitionen

Art. 2. [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. KAPITEL

Regeln für alle Formen der Datenbearbeitung

Allgemeine Grundsätze

Art. 3. [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.

Verantwortung
a) Des öffentlichen Organs

Art. 4. [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.

b) Der Benutzerinnen und Benutzer

Art. 5. [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.

c) Bei gemeinsamer Bearbeitung

Art. 6. 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).

d) Vorbehalt

Art. 7. Die besonderen Verantwortlichkeiten des Informatikzentrums der Kantonsverwaltung Freiburg (Informatikzentrum) oder des zuständigen Informatikdienstes im Bereich der Informatiksicherheit bleiben vorbehalten.

Risikobeurteilung
a) Im Allgemeinen

Art. 8. [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.

b) Zuweisung einer Vertraulichkeitsstufe

Art. 9. [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.

Bestimmung der Massnahmen
a) Zugriffsberechtigung

Art. 10. [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.

b) Organisatorische und technische Massnahmen

Art. 11. [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.

Periodische Überprüfung

Art. 12. Das öffentliche Organ überprüft periodisch die Risiken und die getroffenen Massnahmen, vor allem in Bezug auf neue technische Möglichkeiten.

Vorarchivierung und Vernichtung

Art. 13. [1] Die Sicherheit der Personendaten in Vorarchivierungsdossiers muss sichergestellt werden.

[2] Die Dokumente und andere 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. KAPITEL

Besondere Regeln für die automatisierte Datenbearbeitung

Wahrung der Informatiksicherheit

Art. 14. [1] Die Informatiksysteme, -anwendungen und -netzwerke, die der Bearbeitung von Personendaten dienen, müssen den Standardanforderungen der Informatiksicherheit genügen.

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

[3] Das Informatiksicherheitskonzept wird den Gemeinden zur Verfügung gestellt. Es ist für alle Gemeindesysteme verbindlich, die an das Netz der kantonalen Verwaltung angeschlossen sind.

Unterstützung und Beratung

Art. 15. [1] Bei einer automatisierten Datenbearbeitung berät und unterstützt das Informatikzentrum die Dienststellen und Anstalten der kantonalen Verwaltung in allen Fragen im Zusammenhang mit der Sicherheit der Personendaten. Die besonderen Befugnisse des Informatikdienstes der Universität bleiben vorbehalten.

[2] Bei allen Fragen im Zusammenhang mit der Anwendung des Informatiksicherheitskonzepts können auch die Gemeinden das Informatikzentrum zur Beratung und Mithilfe beiziehen. Dieses kann die daraus entstehenden Kosten in Rechnung stellen.

[3] Das Informatikzentrum und der Informatikdienst der Universität arbeiten in diesem Bereich mit der kantonalen Aufsichtsbehörde für Datenschutz zusammen.

Anwendungen und Datensammlungen
a) Konzept

Art. 16. [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.

b) Authentifikation und Zugriffskontrolle

Art. 17. [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.

c) Protokollierung

Art. 18. Gewährleisten die präventiven Massnahmen die Sicherheit der Personendaten nicht hinreichend, so muss die Datenbearbeitung protokolliert werden.

d) Ausübung der Rechte der Betroffenen

Art. 19. 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).

Netze und Übermittlung

a) Vertrauliche oder geheime Daten

Art. 20. [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.

b) Abrufverfahren

Art. 21. [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.

c) Internet und Intranet

Art. 22. [1] Die Bestimmungen dieses Kapitels gelten auch für die Bearbeitung von Daten über ein Netz wie Internet oder Intranet.

[2] Im Einvernehmen mit der kantonalen Aufsichtsbehörde für Datenschutz sorgen das Informatikzentrum 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.

Periphere Geräte und Wartung

Art. 23. 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.

Protokollierungsverfahren

Art. 24. [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. KAPITEL

Aufsicht

Kontrolle durch die vorgesetzte Behörde

Art. 25. Die vorgesetzte Behörde kontrolliert die Anwendung der Bestimmungen dieses Reglements durch die öffentlichen Organe, die ihr unterstehen.

Art. 26. [1] Die zuständige Aufsichtsbehörde für Datenschutz übt die externe Kontrolle gemäss den Artikeln 29 ff. DSchG aus. Kontrolle durch die Aufsichtsbehörde

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

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

Art. 28. 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. Zufällige Feststellungen

5. KAPITEL

Übergangs- und Schlussbestimmungen

Art. 29. 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. Übergangsrecht

Art. 30. 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: Änderung bisherigen Rechts

Art. 3 Abs. 1 Bst. e

[[1] Das Informatikzentrum hat insbesondere folgende Aufgaben:]

e) es wacht über die Anwendung der Massnahmen zur Informatiksicherheit und erfüllt die Aufgaben, für die es aufgrund der Bestimmungen über die Sicherheit der Personendaten zuständig ist;

Art. 6 Randtitel und Abs. 2

Informatikpolitik
a) Im Allgemeinen

[2] *Den Ausdruck* «der Sicherheit der Daten und des Datenschutzes» *durch* «der Informatiksicherheit» *ersetzen.*

Art. 6a (neu). b) Informatiksicherheitskonzept

[1] Das Informatiksicherheitskonzept legt die Standardanforderungen für die Informatiksicherheit fest. Es enthält insbesondere:

a) eine Umschreibung der Verantwortlichkeiten für die Sicherheit der Informatiksysteme, -anwendungen und -netze;

b) eine allgemeine Liste der Massnahmen, die für die Sicherheit der Systeme, der Netzwerke, der Anwendungen und der Daten nötig sind;

c) Weisungen für die verschiedenen Sicherheitsverfahren, vor allem für die Verwaltung von Zugriffsberechtigungen, die Identifikationsverfahren, die Verwaltung von Passwörtern, die Datenverschlüsselung, die Verwaltung von Protokolldateien und die Vernichtung der Daten.

[2] Es berücksichtigt die Sicherheitsanforderungen für den Schutz der Personendaten und wird der kantonalen Datenschutzkommission zur Stellungnahme vorgelegt.

[3] Es wird regelmässig nachgeführt und den Benutzern in geeigneter Form zur Kenntnis gebracht.

Inkrafttreten und Veröffentlichung

Art. 31. [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.

Vom Staatsrat beschlossen in Freiburg am 29. Juni 1999.

Der Präsident: M. PITTET

Der Kanzler: R. AEBISCHER