Datenschutzverordnung

Vom 20. Mai 2003 (Stand 7. Mai 2006)

Der Regierungsrat,

gestützt auf die Artikel 8, 22 und 24 des Gesetzes vom 5. Mai 2002 über den Schutz von Personendaten (Datenschutzgesetz)[1)],

beschliesst:

1. Datensicherheit

Art. 1 *Grundsätze*

[1] Die organisatorischen und technischen Massnahmen zur Gewährung der Datensicherheit richten sich nach dem Zweck, der Art sowie dem Umfang der Datenbearbeitung und berücksichtigen die möglichen Gefährdungen der Persönlichkeitsrechte betroffener Personen sowie die wirtschaftliche Tragbarkeit.
[2] Sie sind in angemessenen Zeitabständen von den verantwortlichen Stellen auf ihre Tauglichkeit zu überprüfen und nötigenfalls durch bessere Mittel zu ersetzen. Der Regierungsrat kann Richtlinien für verbindlich erklären.
[3] Die Wirksamkeit von Massnahmen der Datensicherheit muss jederzeit gewährleistet sein.

Art. 2 *Verantwortlichkeiten*

[1] Die öffentlichen Organe sind für die Einhaltung der Vorschriften über die Datensicherheit selber verantwortlich.
[2] Sie beurteilen die Risiken, ermitteln die Schutzziele und realisieren die Schutzmassnahmen. Die kantonalen öffentlichen Organe sprechen sich dabei in Bezug auf elektronisch geführte Datensammlungen mit der Fachstelle Informatik/EDV ab.
[3] Wird eine Datensammlung von mehreren öffentlichen Organen gemeinsam angelegt oder genutzt, haben sie vorgängig die Verantwortlichkeiten mittels Vereinbarung zu regeln; vorbehalten bleibt Artikel 6 Absatz 1 des Datenschutzgesetzes. Können sie sich nicht einigen, unterbreiten die kantonalen öffentlichen Organe die Angelegenheit dem Regierungsrat oder der Verwaltungskommission der Gerichte zum Entscheid.

---

1) GS I F/1

Art. 3 *Risikobeurteilung*

[1] Die öffentlichen Organe prüfen für ihre Informatiksysteme und sonstigen Sammlungen von Personen- und anderen Daten jeweils Art und Umfang der Gefährdung, insbesondere durch zufällige oder unbefugte Zerstörung, durch zufälligen Verlust (insbesondere wegen technischer Mängel an Geräten und Gebäuden sowie infolge von Feuer und Elementarereignissen) sowie durch unbefugten Zugang, unbefugte Veränderung oder unbefugtes Bekanntgeben.
[2] Sie berücksichtigen die Eintretenswahrscheinlichkeit des Risikos und beurteilen die drohenden Schadenfolgen.

Art. 4 *Schutzziele*

[1] Entsprechend den Ergebnissen der Risikobeurteilung legen die öffentlichen Organe die Schutzziele fest, namentlich im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit.

Art. 5 *Massnahmen*

[1] Die Schutzmassnahmen können der Verkleinerung des Risikos oder der Milderung der Schadenfolgen dienen.
[2] Zur Gewährleistung der Datensicherheit können insbesondere die folgenden Massnahmen in Erwägung gezogen werden:

a. Zugangskontrollen, indem nur berechtigte Personen freien Zugang zu Räumlichkeiten haben, in denen sich Datensammlungen oder Informatik-Geräte befinden;
b. Benutzerkontrollen, indem unbefugten Personen die Benutzung von Informatik-Geräten, mit denen Daten bearbeitet werden, verwehrt wird;
c. Datenträgerkontrollen, indem unbefugten Personen das Lesen, Kopieren, Verändern, Zerstören oder Entfernen von Datenträgern verwehrt wird;
d. Zugriffskontrollen gemäss Artikel 6;
e. Bearbeitungskontrollen, indem das unbefugte Bearbeiten (Lesen, Kopieren, Verändern, Löschen usw.) von Daten verhindert wird;
f. Eingabekontrollen, indem bei der Eingabe, Veränderung und Löschung von Daten die Identität der eingebenden Person und der Zeitpunkt festgehalten wird;
g. Transportkontrollen, indem beim Transport von Datenträgern oder bei der Bekanntgabe von Daten das unbefugte Lesen, Kopieren, Verändern oder Löschen verhindert wird;
h. Empfängeridentifikation, damit der Empfänger von Personendaten identifiziert werden kann;

i. Kontinuitätskontrollen, indem Vorkehrungen getroffen werden, damit bei einem Ausfall von Informatik-Systemen wichtige Funktionen möglichst rasch weiter erfüllt werden können;

k. Generationenfolgekontrollen, indem verhindert wird, dass Daten infolge technologischen Wandels bei den Betriebssystemen oder Programmen nicht mehr dauerhaft erschlossen und erhalten werden können.

Art. 6 *Zugriffskontrollen*

[1] Es dürfen nur berechtigte Personen Zugriff auf die Informatik-Systeme und die Datensammlungen haben.
[2] Die Zugriffe von berechtigten Personen sollen auf diejenigen Personendaten beschränkt werden, die sie für die Erfüllung ihrer dienstlichen Aufgaben benötigen. Ist die Beschränkung des Zugriffs auf bestimmte Daten technisch nicht möglich oder wirtschaftlich nicht tragbar, müssen die Zugriffe bei elektronisch geführten Datensammlungen protokolliert werden.
[3] Der Zugang zu Informatik-Systemen und Datensammlungen ist mindestens von der Benützung von Passwörtern abhängig zu machen, die periodisch zu wechseln und geheim zu halten sind. Bei Personalabgängen sind die entsprechenden Passwörter unverzüglich zu sperren.

Art. 7 *Sicherung*

[1] Programme und Daten sind periodisch auf Datenträgern zu sichern sowie dezentralisiert und sicher aufzubewahren.

Art. 8 *Öffentliche Netze*

[1] Der Datenaustausch über öffentliche Netze soll wenn immer möglich verschlüsselt und über gesicherte Zugangspunkte erfolgen.
[2] Zugriffe von aussen auf das kantonsinterne Netz müssen grundsätzlich über die bereitgestellten gesicherten Netzwerkübergänge erfolgen.

Art. 9 *Informatikarbeitsplätze ausserhalb der ordentlichen Amtsräumlichkeiten*

[1] Die Zulässigkeit der Bearbeitung von Personendaten ausserhalb der Amtsräume, der Verwendung von Programmen des Arbeitgebers auf privaten Geräten sowie von privaten Programmen und privater Peripherie auf Geräten des Arbeitgebers ist in den Benützungsreglementen zu regeln.
[2] Die öffentlichen Organe treffen geeignete Massnahmen, damit es bei Wartungsarbeiten durch Dritte nicht zu Verletzungen der Vertraulichkeit oder zu unerlaubten Bearbeitungen von Daten kommt. Wenn möglich sollen dabei speziell überwachte Accounts eingerichtet sowie anonymisierte oder pseudonymisierte Testdaten verwendet werden.

Art. 10 *Instruktion des Personals*

[1] Die öffentlichen Organe beziehungsweise die Verwaltungsstellen instruieren ihr Personal über die für sie geltenden Vorschriften betreffend die Datensicherheit und über die möglichen Konsequenzen bei deren Missachtung.
[2] Das Personal hat dem Leiter oder der Leiterin der Verwaltungsstelle unterschriftlich zu bestätigen, dass es ein Benützungsreglement ausgehändigt erhalten hat.

Art. 11 *Kontrollaufgaben*

[1] Die öffentlichen Organe überprüfen periodisch die Einhaltung der Schutzmassnahmen.
[2] Die kantonale Aufsichtsstelle sowie die Abteilung Informatik können in die Prüfungsberichte von kantonalen öffentlichen Organen Einsicht nehmen und die Durchführung von Überprüfungen anregen oder auf Gesuch hin vornehmen.
[3] Die Fachstelle Informatik/EDV ist verpflichtet, die technischen Veränderungen im Bereich der Datensicherheit zu verfolgen sowie die kantonalen öffentlichen Organe über Neuerungen zu orientieren und Verbesserungen der Schutzmassnahmen vorzuschlagen. Sie kann dem Regierungsrat oder der Verwaltungskommission der Gerichte den Erlass von Richtlinien oder Weisungen beantragen.

Art. 12 *Gemeinden*

[1] Ist eine Gemeinde an das Informatiknetz der kantonalen Verwaltung angeschlossen, sind die für die kantonalen öffentlichen Organe geltenden Vorschriften und Richtlinien über die Datensicherheit auch für sie verbindlich.

2. Ausführende Bestimmungen zur Bearbeitung von Personendaten

Art. 13 *Videoüberwachung*

[1] Die durch öffentliche Organe veranlasste präventiv-beobachtende Videoüberwachung ist zulässig zur Erreichung eines in einem erheblichen öffentlichen Interesse begründeten Zweckes, namentlich zum Schutz von Polizeigütern, sowie unter Beachtung der allgemein für die Bearbeitung von Personendaten geltenden Grundsätze.
[2] Die aufgenommenen Bilder sind innert Wochenfrist zu vernichten, soweit sie nicht für den Überwachungszweck ausgewertet und aufbewahrt werden müssen.
[3] Die polizeiliche Videoüberwachung zur Beschattung einer tatverdächtigen Person richtet sich nach den strafprozessualen Vorschriften.

Art. 14 *Aufbewahrungsfristen*

[1] Die öffentlichen Organe legen in Absprache mit den verantwortlichen Personen des zuständigen Archivs die Aufbewahrungsfristen fest, soweit sie nicht spezialrechtlich geregelt sind. Die Aufbewahrungsfrist begrenzt die Dauer, während der die Personendaten zu Beweis- und Sicherungszwecken im Archiv aufzubewahren sind.
[2] Nach Ablauf der Aufbewahrungsfrist entscheiden die verantwortlichen Personen des Archivs, ob die Personendaten vernichtet oder für die wissenschaftliche Forschung oder archivische Weiterverwendung weiterhin erhalten werden sollen.

3. Kantonale Aufsichtsstelle, Gebühren, Inkrafttreten

Art. 15 *Aufsichtsstelle*

[1] Die kantonale Aufsichtsstelle (Datenschutzbeauftragte oder Datenschutzbeauftragter) ist administrativ der Staatskanzlei angegliedert; in fachlicher Hinsicht erfüllt sie ihre Aufgaben unabhängig und selbstständig.
[2] Liegt ein Ausstandsgrund vor, so bezeichnet der Regierungsrat auf Antrag der befangenen Aufsichtsstelle im Einzelfall einen Stellvertreter oder eine Stellvertreterin.

Art. 16 *Gebühren*

[1] Soweit die Behandlung eines Gesuches unter die Gebührenpflicht im Sinne von Artikel 22 Absatz 2 des Datenschutzgesetzes fällt, erheben die kantonalen öffentlichen Organe 60 bis 80 Franken pro Stunde Aufwand.

Art. 17 *Schlussbestimmungen und Inkrafttreten*

[1] Die öffentlichen Organe realisieren die Sicherheitsmassnahmen innert drei Jahren ab Inkrafttreten des Gesetzes.
[2] Einfach umzusetzende und kostengünstige Sicherheitsmassnahmen, vor allem solche organisatorischer Natur, sind möglichst schon vorher zu realisieren.
[3] Diese Verordnung tritt auf den 1. Juli 2003 in Kraft.