Vortrag der Finanzdirektion an den Regierungsrat

betreffend

Weisung des Regierungsrates über Informationssicherheit und Datenschutz (ISDS)

1. Anlass

Mit RRB 1104/2003 hat der Regierungsrat das damalige Organisationsamt beauftragt, ein Expertengutachten erstellen zu lassen über die Weiterentwicklung der Sollvorgaben für die Informationssicherheit bei Datenschutzkonzepten. In diesem Gutachten wurde die **Überarbeitung der bestehenden Sollvorgaben für die Informationssicherheit** (RRB 4637/1992 „Mindestanforderungen an die Datensicherheit“) sowie des IT-Zonenplanes insbesondere in folgenden Punkten vorgeschlagen:

- die Verbesserung der Klassifizierung der Systeme und Anwendungen durch eine Erweiterung der Klassifizierungskriterien nach dem Vorbild der Weisung S02 über die Informatiksicherheit in der Bundesverwaltung;

- die verbindliche Festlegung von organisatorischen und technischen Massnahmen, die zur Gewährleistung eines ausreichenden Grundschutzes erforderlich sind, auf der Grundlage von so genannten Kontrollzielen und unter Berücksichtigung einer Best Practice, wie man sie in den anerkannten Standards zur Informationssicherheit findet;

- die Aufwertung der Risikoanalyse als Grundlage für die Identifikation der über den Grundschutz hinaus notwendigen organisatorischen und technischen Massnahmen.

Zudem wurde auch das Anbieten einer an den Belangen der Verwaltung orientierten **Ausbildung für Projektverantwortliche und Projektsachbearbeitende auf dem Gebiet der Informationssicherheit und des Datenschutzes** durch das Organisationsamt, in Zusammenarbeit mit der Datenschutzaufsichtsstelle, vorgeschlagen.

Die Kantonale Informatikkonferenz (KIK) nahm zu den Ergebnissen des Gutachtens und den geplanten Massnahmen an ihrer Sitzung vom 12. August 2004 Stellung und begrüsste die Vorgehensvorschläge. Der Regierungsrat nahm mit RRB 3104/2004 vom 13. Oktober 2004 Kenntnis vom Gutachten und vom Vortrag der Finanzdirektion und beauftragte diese, unter Einbezug der KIK und der kantonalen Datenschutzaufsichtsstelle die Projektarbeiten im Sinne der Ausführungen im Vortrag weiter zu führen und bis Ende 2005 abzuschliessen. In der Folge wurde indes seitens der Informatikverantwortlichen der Direktionen und der Staatskanzlei der Wunsch geäussert, die Überarbeitung der Informationssicherheits- und Datenschutzvorgaben sei auf die Gesamtrevision der Informatikstrategie abzustimmen. Diese wurde dem Regierungsrat am 5. Dezember 2007 in der Form des Informatikeinsatzkonzepts 2007 zum Entscheid vorgelegt.

Mit dem vorliegenden Beschluss und seinen Beilagen ist der vorerwähnte Auftrag der Finanzdirektion erfüllt. Die Beschlüsse und ihre Beilagen stellen den kantonalen Informatikverantwortlichen ein integriertes, modernes Regelwerk und umfassende Arbeitsunterlagen für die Bereiche Informationssicherheit und Datenschutz zur Verfügung.

Die Vorbereitungsarbeiten haben indes gezeigt, dass es angesichts der Bedeutung der vorliegenden Regelungen – namentlich allenfalls auch für Behörden im Sinne des Datenschutzgesetz vom 19. Februar 1986 (KDSG, BSG 152.04), denen gegenüber der Regierungsrat nicht direkt weisungsbefugt ist – angebracht ist, diese Materie auf Verordnungsebene zu regeln. Damit eine solche Verordnung die im vorliegenden Beschluss vorgesehene Regelung der technischen Einzelheiten auf Stufe Fachamt übernehmen kann, muss das KDSG angepasst werden, um diese Kompetenzsubdelegation zu erlauben (vgl. Art. 69 Abs. 3 der Verfassung des Kantons Bern vom 6. Juni 1993, BSG 101.1). Die Finanzdirektion wird diese Änderung – im Einvernehmen mit der Datenschutzaufsichtsstelle – im Rahmen der zurzeit anlässlich der Assoziierung an die Abkommen von Schengen und Dublin laufenden KDSG-Revision vorschlagen. Tritt diese Gesetzesänderung in Kraft, kann der vorliegende Beschluss in eine Verordnung überführt werden.

2. Terminologie und Übersicht der bestehenden Beschlüsse

2.1. Terminologie

Bei Diskussionen rund um den Datenschutz, um Datensicherheit, Informationssicherheit, IT-Security usw. zeigt sich immer wieder, dass die Begriffe nicht genau auseinander gehalten werden. Aus diesem Grund sollen die wichtigsten Begriffe an dieser Stelle kurz erläutert und zueinander in Beziehung gebracht werden.

Unter **Datenschutz** versteht man den Schutz der Persönlichkeitsrechte der Betroffenene beim Bearbeiten von Informationen über bestimmte oder bestimmbare natürliche und juristische Personen (Personendaten). Dies ist die Zielsetzung des Datenschutzrechts. Durch Vorschriften, wie Personendaten beschafft, gespeichert, genutzt und bekanntgegeben werden dürfen, sollen Verletzungen der verfassungsmässig geschützten Persönlichkeitsrechte nach Möglichkeit verhindert werden.

Sicherheit beinhaltet verschiedenste Aspekte, wie z.B. den physischen Schutz der Infrastruktur, die Verhinderung von Personenschäden sowie die Gewährleistung der Vertraulichkeit, der Verfügbarkeit und der Integrität von Informationen. Letzteres ist unter den Begriff der **Informationssicherheit** zu subsumieren. Mit Datensicherheit ist grundsätzlich die Informationssicherheit bei Personendaten gemeint. **Informatiksicherheit** oder IT-Security steht für die Sicherheit beim Bearbeiten von Informationen mit Hilfe der IT-Technologie.

Aus Abbildung 1 unten ist ersichtlich, dass es eine Überschneidung bei der Informationssicherheit und beim Datenschutz gibt. Datenschutz ohne Informationssicherheit funktioniert nicht. Ist zum Beispiel die Vertraulichkeit von Personendaten als Folge organisatorischer oder technischer Mängel nicht gewährleistet, so kann dies zu einer Beeinträchtigung der Persönlichkeitsrechte der betroffenen Personen führen. Art. 17 KDSG umfasst daher auch die Informationssicherheit.

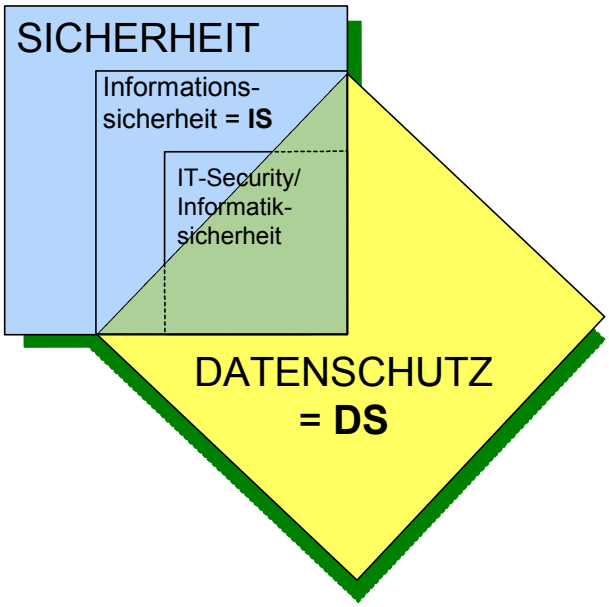

Abb. 1 - Sicherheit - Informationssicherheit - Datenschutz

Umgekehrt gilt aber, dass die Informationssicherheit nicht zwangsläufig datenschutzrelevant sein muss. Dies ist immer dann der Fall, wenn Informationen bearbeitet werden, die keinen Bezug zu einer bestimmten oder bestimmbaren Person haben (z.B. statistische oder anonymisierte Daten).

Weil es einen Datenschutz ohne Informationssicherheit nicht gibt, wird im Projekthandbuch HERMES 2003/2005 neu nicht von Datenschutz oder Informationssicherheit gesprochen, sondern es treten diese beiden Begriffe immer in der Kombination "Informationssicherheit und Datenschutz" auf und es wird dafür die Abkürzung ISDS verwendet.

2.2. Übersicht der bestehenden und neuen Regierungsratsbeschlüsse im Umfeld von Informationssicherheit und Datenschutz

Die bestehenden RRB sind abrufbar unter wwwin.kaio.fin.be.ch, Rubrik „Weisungen“. Diese Liste umfasst nicht RRB, die sich mit spezifischen Informatikvorhaben befassen.

RRB 4600/1992	vom 9. Dezember 1992 über die Informatikstrategie des Kantons Bern *Das Informatikeinsatzkonzept 2007 wird eine Woche vor der vorliegenden Weisung vorgelegt (vgl. Bemerkungen zu Art. 12)*
RRB 4637/1992	vom 9. Dezember 1992 über Mindestanforderungen an die Datensicherheit *mit der vorliegenden Weisung aufzuheben*
RRB 1347/1998	vom 17. Juni 1998 über Weisungen über den Umgang mit Passwörtern *bleibt unverändert*
RRB 3331/2001	vom 17. Oktober 2001 über allgemeine Geschäftsbedingungen zur Beschaffung von Informatikdienstleistungen *bleibt unverändert*
RRB 1103/2003	vom 9. April 2003 über Datenschutz bei Informatikanwendungen *mit der vorliegenden Weisung aufzuheben*
RRB 1104/2003	vom 9. April 2003 über Datenschutz bei Informatikprojekten *mit der vorliegenden Weisung aufzuheben*
RRB 1668/2004	vom 26. Mai 2004 über den Datenschutz, die periodische Prüfung von Informatikanwendungen und die Rahmenbedingungen für den Beizug externer Kontrollstellen *bleibt unverändert*
RRB ___/2007	vom X.X.2007 „Weisung des Regierungsrates über Informationssicherheit und Datenschutz (ISDS)“ *die vorliegende Weisung*

3. Bemerkungen zu den einzelnen Bestimmungen

Zum Ingress

Gemäss Artikel 38 KDSG erlässt der Regierungsrat die zum Vollzug des KDSG erforderlichen Bestimmungen. Artikel 17 KDSG bestimmt, dass wer Personendaten bearbeitet, auch für ihre Sicherung sorgt. Die Regelung der Informationssicherheit kann daher ebenfalls gestützt auf Art. 38 KDSG erfolgen. Zudem ist der Regierungsrat gemäss Artikel 23 Absatz 1 des Gesetzes über die Organisation des Regierungsrates und der Verwaltung (OrG, BSG 152.01) für die Führung der Verwaltung verantwortlich und kann somit Verwaltungsweisungen wie die vorliegende erlassen.

Zu Art. 1: Geltungsbereich

Der Geltungsbereich entspricht dem der aufzuhebenden RRB 4637/1992 und 4638/1992, die „für die ganze Staatsverwaltung inklusive Annexanstalten“ galten.[1]

Dagegen können auf Stufe Verwaltungsweisung die Gemeinden nicht in die Pflicht genommen werden. Wie bisher sind die Gemeinden (und damit auch die durch sie konstituierten oder beherrschten anderen Träger öffentlicher Aufgaben) dieser Weisung somit nicht unterstellt. Sie bleiben aber dem KDSG selbst unterstellt (Art. 2 Ziff. 5 Bst. a KDSG).

Die Bestimmung von Ziff. 1.4 von RRB 1104/2003, wonach jener RRB auch für Staatsbeiträge gelte, wird in Abs. 2 übernommen und konkretisiert.

Zu Art. 2: Verantwortlichkeiten

Die Verantwortlichkeitsregelung entspricht sinngemäss Ziffer 2 von RRB 4637/1992 und gibt die Verantwortlichkeitsregelung nach Art. 8 KDSG wieder.

Zu Art. 3: Pflichten der verantwortlichen Stelle

Die Auferlegung der allgemeinen Verantwortung für die Gewährleistung von ISDS entspricht, was die Informationssicherheit betrifft, Ziff. 3 des bisherigen RRB 4637/1992 und, was den Datenschutz betrifft, Art. 8 Abs. 1 KDSG und Ziff. 1.1 von RRB 1103/2003. Selbstverständlich bleibt die konkrete Wahrnehmung der auferlegten Verantwortung im Rahmen der Vorgaben der vorliegenden Weisung und seiner Ausführungsweisungen im Ermessen der verantwortlichen Stelle.

Fallengelassen wurde die Verpflichtung der Direktionen, eigene Sicherheitsstrategien zu erarbeiten. Der Spielraum zur Ausarbeitung solcher Strategien ist im Kontext der nun detaillierteren ISDS-Vorgaben nur noch beschränkt gegeben.

[1] Für RRB 4637/1992 galt dieser Geltungsbereich durch den Verweis auf die Informatikstrategie (RRB 4600/1992) im Ingress. Die Informatikstrategie legt den erwähnten Geltungsbereich in Absatz 2 von Teil A fest.

Zu Art. 4 bis 6: ISDS-Analyse und ISDS-Konzept, Unterlagen für die Bewilligung von Informatikprojekten und der entsprechenden Finanzmittel, Konsequenzen der Nichteinhaltung dieser Weisung

Die in der vorliegenden Weisung umrissene, mehrstufige Vorgehensweise bei Informatikprojekten mit ISDS-Analyse und, je nach deren Ergebnis, der Umsetzung der ISDS-Grundschutzmassnahmen oder der Erstellung eines ISDS-Konzepts wird in der ISDS-Wegleitung des KAIO detailliert erläutert. Sie löst die weniger differenzierte, unflexiblere Prozedur gemäss RRB 4637/1992 und RRB 1104/2003 ab. Das KAIO stellt zur Umsetzung dieses Vorgehens elektronische Vorlagen und Beratungsangebote zur Verfügung (vgl. Art. 11 Abs. 2). Die Regierung hat diesem Vorgehen in RRB 3104/2004, gestützt auf das jenem Beschluss beigelegte Expertengutachten, im Grundsatz bereits zugestimmt.

Die vorliegende Weisung und die ISDS-Wegleitung gehen vom Normalfall einer Anwendung aus, mit der Personendaten bearbeitet werden und die daher nicht nur informationssicherheits-, sondern auch datenschutzrelevant ist. Bei den wenigen Anwendungen, mit denen keine Personendaten bearbeitet werden, können ausschliesslich die IS-Teile der Unterlagen verwendet werden. In Bezug auf Art. 4 Abs. 3 Bst. d ist zu bemerken, dass nur spezifische gesetzliche Geheimhaltungsvorschriften erhöhte ISDS-Anforderungen begründen, nicht aber das allgemein geltende Amtsgeheimnis (Art. 320 StGB).

Zu Art. 7: ISDS bei bestehenden Anwendungen

Dem Anliegen einer durchgehenden Umsetzung von ISDS in der Kantonsverwaltung wird nur Genüge getan, wenn die neu definierten Standards konsequent auch auf die bestehenden Anwendungen angewendet werden. In diesem Sinne konkretisiert Art. 7 die Umsetzungsverantwortung der verantwortlichen Stellen weiter. Wegen des grossen Bestandes an bestehenden Anwendungen, deren Umsetzung von ISDS grossmehrheitlich auch im Lichte der neuen Vorgaben vollauf genügt, sowie wegen der knappen finanziellen und personellen Mittel der Verwaltungsinformatik wird aber auf konkrete zeitliche Vorgaben verzichtet.

Zu Art. 8: Periodische Prüfung der Informatikanwendungen

Art. 8 integriert im Wesentlichen unverändert den bestehenden RRB 1103/2003 vom 9. April 2003 über Datenschutz bei Informatikanwendungen. Angepasst wurde lediglich die Terminologie. So soll die Prüfung nun explizit nicht mehr nur die Anforderungen des Datenschutzes im engeren Sinne umfassen, also des Persönlichkeitsschutzes der Betroffenen, sondern (wie auch im Ausführungs-RRB 1668/2004, Ziff. 2.2.2 festgehalten) das ganze Kontinuum von Informationssicherheit und Datenschutz. Damit wird auch Artikel 17 KDSG Rechnung getragen (vgl. die Bemerkungen zum Ingress).

Es entfällt Ziffer 1.4 letzter Satz von RRB 1103/2003, der die Höhe für den Prüfplankredit 2004 bestimmte, und Ziffer 1.1, die grundsätzlich festhielt, dass alle Informatikanwendungen des Kantons den Anforderungen des Datenschutzes zu genügen hätten. Letzteres ergibt sich nun aus Art. 3 der vorliegenden Weisung. RRB 1103/2003 kann damit aufgehoben werden (Art. 12 der vorliegenden Weisung).

Zu Art. 9: Aufsicht

Gemäss Artikel 2 Absatz 6 KDSG ist die verwaltungsunabhängige Datenschutzaufsichtsstelle die kantonale Aufsichtsstelle für Datenschutz. Der vorliegende Beschluss, der wie erläutert gestützt auf Artikel 17 KDSG davon ausgeht, dass sich Informationssicherheit und Datenschutz in der Praxis nicht voneinander trennen lassen, erweitert diese Aufsicht nun explizit auf das ganze ISDS-Kontinuum.

Auch zur Aufsicht gehört die Pflicht der verantwortlichen Stelle, ihrem Kreditantrag eine Stellungnahme der Datenschutzaufsichtsstelle über die Einhaltung der ISDS-Bestimmungen beizulegen (Art. 5). Mit dieser Vorschrift wird die Ziff. 1.4 von RRB 1104/2003 sinngemäss übernommen. Weil die vorliegende Weisung vom Schwellenwert von CHF 100'000, der im erwähnten RRB für die Erstellung von ISDS-Unterlagen und die Vorlage an die Datenschutzaufsichtsstelle galt, Abstand nimmt, wird nun für die Vorlagepflicht an das Bestehen erhöhter ISDS-Anforderungen gemäss der Klassifizierungsvorgaben in der Wegleitung des KAIO angeknüpft (vgl. Art. 11 Abs. 1 Bst. a). Selbstverständlich ist auch die freiwillige Vorlage von Vorhaben, bei denen die Umsetzung des ISDS-Grundschutzes genügt, möglich.

Für spezifische, vor allem technische und organisatorische Aspekte der Informationssicherheit wurde im KAIO die Stelle einer oder eines Informationssicherheitsbeauftragten (IT-SIBE) geschaffen, die oder der die Datenschutzaufsichtsstelle bei der Aufsicht unterstützt und die verantwortlichen Stellen bei der Umsetzung der Informationssicherheit berät. Dem IT-SIBE wird die Aufsicht über die (vergleichsweise wenigen) Datenbearbeitungen zugestanden, die keine Personendaten betreffen und daher nicht unter die Aufsichtspflicht der Datenschutzaufsichtsstelle nach dem KDSG fallen.

Natürlich bleiben die besonderen Aufsichtskompetenzen der Finanzkontrolle nach Massgabe des Gesetzes über die Finanzkontrolle vom 1. Dezember 1999 (KFKG, BSG 622.1) vorbehalten.

Zu Art. 10: Kontaktpersonen der Datenschutzaufsichtsstelle und des IT-SIBE

Mit der Einführung neuer ISDS-Regeln ist voraussichtlich wenigstens in den ersten Jahren ein erhöhter Informations- und Beratungsbedarf verbunden. Damit die Datenschutzaufsichtsstelle und der IT-SIBE diesen decken können, sind sie darauf angewiesen, über mindestens eine Kontaktperson in ISDS-Fragen pro Direktion zu verfügen. Die entsprechenden Kontaktangaben sind der Datenschutzaufsichtsstelle und dem IT-SIBE mitzuteilen.

Zu Art. 11: Weisungen des Amtes für Informatik und Organisation

Mit Artikel 11 wird dem KAIO als zuständigem Querschnittamt (vgl. Art. 11 Bst. a der Verordnung vom 18. Oktober 1995 über die Organisation und die Aufgaben der Finanzdirektion, OrV FIN, BSG 152.221.171) die Weisungsbefugnis delegiert bzw. die bestehende Weisungsbefugnis konkretisiert (vgl. Art. 11 Bst. c OrV FIN), um die erforderlichen Ausführungsbestimmungen zu erlassen. Dies hat nach Konsultation der Direktionen, der Staatskanzlei, der kantonalen Datenschutzaufsichtsstelle und des relevanten intrakantonalen Koordinationsgremiums, der Kantonalen Informatikkonferenz (KIK) zu erfolgen. Die KIK hat einer materiell gleichlautenden Fassung der vorliegenden Weisung und der ersten Fassung der ISDS-Wegleitung an ihrer Sitzung vom 21. September 2006 zugestimmt.

Die ISDS-Wegleitung legt das zu beachtende Grundschutzniveau fest und bestimmt Inhalt und Form der ISDS-Analyse und -Klassifizierung sowie des ISDS-Konzepts. Sie umfasst in einem Anhang auch neue kantonale Allgemeine ISDS-Geschäftsbedingungen (AGB ISDS), die in Ergänzung der Allgemeinen Geschäftsbedingungen der Schweizerischen Informatikkonferenz (AGB SIK) gemäss RRB 3331/2001 für die vertragliche Regelung der Leistungen Dritter im Zusammenhang mit Informatikprojekten zum Einsatz kommen sollen.

Die AGB ISDS konkretisieren die eher rudimentären ISDS-Bestimmungen der AGB SIK unter Bezugnahme auf die im Projekt erarbeiteten ISDS-Grundlagen. Damit wird sichergestellt, dass der kantonale Auftraggeber und seine externen Outsourcing- oder Dienstleistungspartner vom selben ISDS-Schutzniveau ausgehen und die Einhaltung von ISDS auch im kantonsexternen Bereich gewährleistet ist. Nach Art. 11 Abs. 1 Bst. d richtet sich die Verpflichtung zum Einbezug der AGB ISDS im Einzelnen nach der ISDS-Wegleitung. Diese sieht vor, dass der Einbezug der AGB ISDS für alle Informatikdienstleistungen obligatorisch ist, die die Bearbeitung von Daten des Leistungsbezügers beinhalten.

Zu Art. 12: Aufhebung und Anpassung von Regierungsratsbeschlüssen

Mit dem Inkrafttreten der vorliegenden Weisung, welche die bestehenden Verwaltungsweisungen im ISDS-Bereich zusammenfasst und aktualisiert, können ihre Vorgängerbeschlüsse (RRB 4637/1992, 1103/2003 und 1104/2003) aufgehoben werden. Die materiellen IS-Bestimmungen von RRB 4637/1992 sind nun in der ISDS-Wegleitung untergebracht, ebenso wie die Bestimmungen von RRB 1104/2003 über das bei Informatikprojekten zu erstellende Datenschutzkonzept. RRB 1103/2003 wurde in Art. 8 der vorliegenden Weisung wiedergegeben (vgl. die Bemerkungen zu jener Bestimmung).

RRB 4637/1992 war Anhang 1 von RRB 4600/1992 über die Informatikstrategie des Kantons Bern. RRB 4638/1992 (Anhang 2) ist infolge der Einführung der Neuen Verwaltungsführung NEF obsolet geworden. Der Regelungsgegenstand von Anhang 3 und 4 der Informatikstrategie ist inzwischen im IT-Zonenplan des KAIO (Weisungen Nr. 01-7-1 und 01-7-2 des Organisationsamts) geregelt. Die Anhänge der Informatikstrategie sind damit aufgehoben oder obsolet geworden. Gleichzeitig mit der vorliegenden Weisung wird dem Regierungsrat eine Totalrevision der Informatikstrategie (neu: Informatikeinsatzkonzept 2007) vorgelegt, die die alte Strategie aufhebt und für die ISDS integral auf die vorliegende Weisung verweist.

Weitergelten kann auch RRB 1668/2004, der in Ausführung von RRB 1103/2003 (jetzt Art. 8 der vorliegenden Weisung) die Rahmenbedingungen für den Beizug externer Kontrollstellen definiert. In RRB 1668/2004 wurde die Weiterentwicklung auf dem Gebiet der ISDS-Vorgaben bereits antizipiert (Ziff. 2.2.2 und 5). Dennoch wird der Klarheit halber festgehalten, dass Verweise auf nicht mehr geltende Bestimmungen im Bereich der Informationssicherheit und des Datenschutzes als Verweise auf die aktuellen ISDS-Bestimmungen zu lesen sind.

Ebenfalls weitergelten können vorerst RRB 1347/1998 vom 17. Juni 1998 über Weisungen über den Umgang mit Passwörtern und die gestützt darauf erlassene Weisung des Organisationsamts (nun des KAIO) Nr. 03-01 vom 12. Juni 2003, welche durch die ISDS-Grundschutzbestimmungen nur in Einzelpunkten tangiert werden. Diese Weisun-

gen werden im Rahmen der Gesamtüberarbeitung der ICT-Weisungen gemäss dem Informatikeinsatzkonzept 2007 anzupassen sein.

Absatz 2, der die punktuelle Anpassung von RRB 0330/2001 vom 24. Januar 2001 über die Betriebsbewilligung des Regierungsrats für das Informationssystem der Kantonspolizei regelt, wurde der formellen Vollständigkeit halber mit nur terminologischen Anpassungen aus dem aufzuhebenden RRB 1103/2003 übernommen.

4. Personelle und finanzielle Auswirkungen, Auswirkungen auf die Volkswirtschaft und auf die Gemeinden

Da die Weisung mit den Vorgaben, die Einhaltung von Informationssicherheit und Datenschutz zu gewährleisten und dies im Projekt und später anlässlich von Prüfungen zu dokumentieren, materiell nichts Neues regelt, sind insoweit keine zusätzlichen personellen und finanziellen Auswirkungen zu erwarten. Auch die rückwirkende Anwendung der neuen Standards soll möglichst ohne Zusatzaufwand bzw. im Rahmen des Möglichen abgewickelt werden, weshalb auf eine zeitliche Befristung verzichtet wurde (s. oben zu Art. 7). Der Umsetzungsaufwand ist nach den Erfahrungen der FIN gering, soweit die Anwendungen sauber dokumentiert sind und die altrechtlichen Datenschutzvorgaben eingehalten wurden. Allfällige Belastungsspitzen können durch eine zweckmässige zeitliche Planung der Umsetzung aufgefangen werden.

Für die Umsetzung der neuen Pflichten bei der Abwicklung von Informatikprojekten wird dank der benutzerfreundlichen elektronischen Ausgestaltung der Vorlagen des KAIO und gestützt auf die ersten Erfahrungen mit den neuen Hilfsmitteln ebenfalls erwartet, dass der personelle Aufwand nicht höher ist als derjenige für die pflichtgemässe Umsetzung der bisherigen Vorgaben. Zwar sind nun potenziell auch – anders als unter RRB 1104/2003 – Informatikprojekte mit einer Investitionssumme von weniger als CHF 100'000.– betroffen. Dafür kann das Erarbeiten eines ISDS-Konzepts neu auch bei teuren Projekten entfallen, wenn gemäss Klassifikation keine erhöhten ISDS-Anforderungen bestehen.

Unabhängig vom vorliegenden Beschluss wurde wegen der steigenden Komplexität der technischen und organisatorischen Aspekte der Informationssicherheit die Stelle eines oder einer Informationssicherheitsbeauftragten (IT-SIBE) im KAIO bereits geschaffen. Als kantonale Fachstelle für Informationssicherheit wird der IT-SIBE die IT-Verantwortlichen in der Verwaltung beraten und die Datenschutzaufsichtsstelle bei ihrer Aufsicht unterstützen können (vgl. die Bemerkungen zu Art. 11).

Die Vorlage hat keine Auswirkungen auf die Volkswirtschaft oder die Gemeinden.

5. Ergebnis des Mitberichtsverfahrens

Das Mitberichtsverfahren wurde im September und Oktober 2006 für den vorliegenden Beschluss und für die ICT-Strategie 2007 (jetzt Informatikeinsatzkonzept 2007) zusammen durchgeführt. Die BVE wurde zudem im September 2007 zur Abgabe eines zweiten Mitberichts zum vorliegenden Geschäft eingeladen.

Die Direktionen und die Staatskanzlei äusserten sich zustimmend oder verzichteten auf Bemerkungen; teils brachten sie Änderungsvorschläge zu einzelnen Punkten an. Nicht umgesetzt wurden die folgenden Anliegen der POM und BVE:

- Die POM beantragt, die JGK habe geeignete **Fachstellen für Audits** zu bezeichnen (Art. 8 Abs. 3). Dies kann nicht umgesetzt werden, weil das Beschaffungsrecht das Führen ständiger Anbieterlisten verbietet (Art. 17 ÖBV).

- Der Meinung der POM, die neuen Vorgaben lösten bedeutenden **Mehraufwand** aus, was im Vortrag auszuweisen sei, kann nicht gefolgt werden. Die Umsetzung der ISDS-Weisung führt nach den Erfahrungen der FIN nicht zu mehr Aufwand als die richtige Umsetzung des geltenden Rechts.

- Der Antrag der POM, die Direktionen einen *oder mehrere* **IT-SIVE bzw. IT-BDS** bezeichnen zu lassen, würde dem Zweck der entsprechenden Regelung – die Schaffung einer einzigen Anlaufstelle auf Stufe DIR/STA und damit die eindeutige Zuweisung der Verantwortlichkeit – zuwiderlaufen.

- Die **Beschränkung der Rückwirkung** der neuen Weisung auf „strategische Fachanwendungen“, wie sie die BVE beantragt, würde nach Meinung der FIN den Schutzerfolg der vorliegenden Weisung ernsthaft in Frage stellen.

- Der von der BVE vorgeschlagene Erlass (und damit auch die laufende Nachführung) der sehr technischen **Ausführungsbestimmungen** durch den Regierungsrat erscheint nicht stufengerecht.

6. Antrag

Die Finanzdirektion beantragt dem Regierungsrat, den beiliegenden Beschlussesentwurf zu genehmigen.

Bern, 6. Dezember 2007 KAIO

DER FINANZDIREKTOR

Urs Gasche
Regierungspräsident

Beilage: – Beschlussesentwurf