Bericht 2014 der Datenschutzaufsichtsstelle des Kantons Bern

Datenschutzaufsichtsstelle des Kantons Bern
Münstergasse 2
3011 Bern
Telefon 031 633 74 10
Telefax 031 633 74 11
info.datenschutz@jgk.be.ch
www.be.ch/dsa

Inhaltsverzeichnis

		Seite
1.	Einleitung	1
2.	Aufgabenumschreibung, Prioritäten, Mittel	2
3.	Kontrollen von Informatikanwendungen, die im Betrieb stehen	3
4.	Videoüberwachung	4
5.	Vorabkontrollen von Informatikprojekten	4
6.	Ansichtsäusserungen, Praxis	6
7.	Gesetzgebung	7
8.	Aufsichts- und Justizentscheide	7
9.	Gemeinderechtliche Körperschaften	8
10.	Besonderes	8
11.	Berichtspunkte der Vorjahre	9
12.	Antrag	9
13.	Anhang	10

1 Einleitung

1.1 Auf einen Blick

Immer seltener betreiben Dienststellen ihre Informatikanwendungen selbständig und in ihrem alleinigen Einflussbereich. Zunehmend erfolgt der Betrieb arbeitsteilig. So übertrugen mehrere Dienststellen den Betrieb ihrer Informatikgrundversorgung dem kantonalen Amt für Informatik und Organisation (KAIO). Dieses lässt den Betrieb durch die kantonseigene BEDAG AG ausführen (Rechenzentrum). Andere Dienststellen schlossen direkt Verträge mit den Outsourcingpartnern ab. Bei beiden Vorgehensweisen werden damit in den Rechenzentren auch die zum Teil besonders schützenswerten Daten aus den diversen Geschäftsanwendungen bearbeitet.
Bevor diese Geschäftsanwendungen ursprünglich in Betrieb kamen, wurden in ISDS-Konzepten die Informatiksicherheitsvorgaben umschrieben, im Vorabkontrollverfahren geprüft und deren Umsetzung in der Verantwortung der Dienststellen überwacht.
Im Berichtsjahr hat die Aufsichtsstelle mehrmals festgestellt, dass die definierten Informatiksicherheitsvorgaben nach der Einführung der arbeitsteiligen Vorgehensweise

- entweder (bei direkt abgeschlossenen Verträgen) dem Outsourcingpartner nicht überbunden worden sind
- oder aber (bei einer Zwischenschaltung des KAIO) den Outsourcingpartner trotz Überbindungklauseln im Vertrag nicht zu den entsprechenden Vorkehrungen veranlasst haben.

Erfolgt die Auslagerung an die BEDAG AG, so sichert diese als ISO-zertifiziertes Rechenzentrum für ihre IT-Infrastruktur standardmässig einen Grundschutz nach ISO-2700x zu. Die Dienststellen wissen aber nicht, ob diese Massnahmen auch für ihre Anwendungen als Grundschutz genügen. Zudem sind für die Geschäftsanwendungen regelmässig über den Grundschutz hinausgehende Sicherheitsmassnahmen erforderlich. Die Dienststellen sind damit nicht mehr in der Lage, sicher zu stellen und zu dokumentieren, dass die für ihre Geschäftsanwendungen insgesamt erforderlichen Sicherheitsmassnahmen auch wirklich abgedeckt sind. Auf dieses „Entgleiten der Verantwortung“ stiess die Aufsichtsstelle sowohl bei aufsichtsrechtlichen Rückfragen, bei Vorabkontrollen wie auch bei einer Kontrolle. (s. 3,5,6).

Auch die Arbeit der Aufsichtsstelle wird überprüft. Gestützt auf die Übereinkommen von Schengen und Dublin evaluierte ein Expertengremium aus den Vertragsstaaten die Aufsichtsstelle. Es empfahl, dass die mit der Revision des Datenschutzgesetzes von 2008 eingeleiteten Massnahmen gefestigt und ausgebaut werden. (S. 1.3).

1.2 Zusammenarbeit mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und der Vereinigung der Schweizerischen Datenschutzbeauftragten (PRIVATIM)

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) koordiniert die Aufsicht über das Schengener-Informationssystem (SIS). 2014 fanden zwei Arbeitssitzungen statt. Mitarbeitende der Aufsichtsstelle wirkten in den PRIVATIM-Arbeitsgruppen ‚Information and Communication Technology‘ (ICT) und ‚Gesundheit‘ mit. Erstere veröffentlichte das Papier „Datenschutztechnische Anforderungen an Klinikinformationssysteme“.

Zu den Themen „Einführung in die Informatik(sicherheit) für Juristen“ und „juristische Weiterbildung anhand von Fallbeispielen“ führte PRIVATIM je einen eintägigen Kurs durch, welcher von den Mitarbeitenden der Aufsichtsstelle besucht wurde. (Zur neuen Ausgestaltung des Vertrags zum Einsatz von Microsoft Office 365 an den Schulen S. 9).

1.3 Schengen–Evaluation

Folgende Kommentare und Hinweise gab das Expertengremium der Vertragsstaaten, das neben den Bundesstellen auch die Kantone Jura, Neuenburg und Bern überprüfte, ab:
- Die im Datenschutzgesetz verankerte Unabhängigkeit der Aufsichtsstelle zur Budgetierung müsse noch verstärkt umgesetzt werden;
- gegenüber der Geschäftsprüfungskommission des Grossen Rates sei die verankerte Unabhängigkeit dahin zu verstehen, dass kein Einfluss auf Entscheide erfolgen dürfe;
- die Kontrolle der Abrufe der Kantonspolizei im SIS solle häufiger als bisher und periodisch erfolgen;
- künftig sei diese Kontrolle durch die Aufsichtsstelle selbst und nicht durch externe Beauftragte durchzuführen;
- ebenfalls seien die vom Polizeikommando in Zusammenarbeit mit der Aufsichtsstelle durchgeführten Kontrollen ein gutes Hilfsmittel, dürften jedoch nicht darüber hinwegtäuschen, dass es sich um eine ungenügende Selbstkontrolle handle;
- für den Beizug externer Kontrollbeauftragter sei in Zusammenarbeit mit der Schengener Koordinationsgruppe (s. 1.2) eine eigene gesetzliche Grundlage zu schaffen und die Unabhängigkeit der Kontrolleure gegenüber der kontrollierten Stelle müsse garantiert sein;

- eine Erhöhung des Personalbestandes der Aufsichtsstelle sei den zuständigen Instanzen vorzuschlagen;
- auf der Internetseite der Aufsichtsstelle seien Informationen über die Rechtsgrundlagen des SIS und Musterschreiben zur Ausübung des Auskunfts- und Berichtigungsrechts aufzunehmen. (S. 1.2; zu den Ressourcen 2.3).

2 Aufgabenumschreibung, Prioritäten, Mittel

2.1 Prioritäten

Neben anderem hat die Aufsichtsstelle die Datenbearbeitungen zu kontrollieren, für das Umsetzen der Datensicherheitsvorgaben zu sorgen, Verwaltung und Betroffene zu beraten, Informatikprojekte einer Vorabkontrolle zu unterziehen und generell für die Umsetzung der datenschutzrechtlichen Vorgaben zu sorgen. Das Datenschutzgesetz gibt diese Aufträge flächendeckend vor. Die zur Verfügung stehenden Ressourcen erlauben aber höchstens ein punktuelles Vorgehen. Ob eine Aktivität an die Hand genommen werden soll, in welcher Priorität und mit wie viel Mitteleinsatz dies erfolgen soll, ist anhand folgender Kriterien zu entscheiden:

– Vorschalten der zuständigen Stelle: Die Beratung kommunaler und kantonaler Verwaltungsstellen hat durch die zuständigen kommunalen Datenschutzaufsichtsstellen bzw. Rechtsdienste der kantonalen Verwaltung zu erfolgen. Betroffene sind in kommunalen Fragen durch die kommunalen Datenschutzaufsichtsstellen zu beraten. Wer unmittelbar bei der Aufsichtsstelle anfragt, ist an die zuständigen Stellen zu verweisen. Diese Zuständigkeiten und die dadurch erfolgende Triage ist in der Datenschutzverordnung verankert.

– FAQ: Erfolgen gleiche Anfragen von Betroffenen oder von Verwaltungsstellen gehäuft oder ist eine Häufung zu erwarten, ist die Antwort in einer frühen Phase in einer allgemeinen Form auf der Internetseite zu publizieren und bei weiteren Anfragen auf die Publikation zu verweisen.

– Unterschiedliche Qualitätsstandards: Einer betroffenen Person oder einer Milizbehörde wird als Antwort eine Handlungsanweisung ohne nähere rechtliche Begründung genügen. Für eine Stellungnahme an eine Justizinstanz ist dagegen ein umfassendes rechtliches „Abtiefen“ erforderlich. Der Qualitätsstandard ist vor Beginn der Arbeit festzulegen.

– Subsidiarität des aufsichtsrechtlichen Handelns: Die Datenschutzgesetzgebung gibt den Betroffenen gute Abwehrrechte (Berichtigung, Vernichtung, Feststellen der Widerrechtlichkeit). Aufsichtsrechtliche Abklärungen sollen unterbleiben, wenn solche Abwehrmöglichkeiten gegeben sind. Die Betroffenen sind auf ihre Abwehrrechte aufmerksam zu machen. Lassen die Hinweise Rückschlüsse auf Systemprobleme zu, ist diesen mit den entsprechenden Mitteln (z. B. Kontrollen) nachzugehen.

– Vorabkontrollen: Die Vorabkontrollvorgaben wollen die Projektleitungen zur Umsetzung der Datenschutzvorgaben im Projekt veranlassen. Diese Wirkung kann auch erreicht werden, wenn die Aufsichtsstelle nur formell das Einreichen der Unterlagen prüft, auf eine inhaltliche Prüfung aber ganz oder zum Teil verzichtet. Ein gesamthafter Verzicht soll dann erfolgen, wenn die gleiche Projektleitung wiederholt korrekte Unterlagen eingereicht hat, ein Projekt untergeordnete Bedeutung hat, aber auch, wenn die Gesamtbelastung der Aufsichtsstelle eine Prüfung nicht mehr erlaubt (Pufferfunktion). Teilkontrollen sind insbesondere dann am Platz, wenn über einzelne Bereiche Aussagen aus früheren Prüfungen möglich sind (z. B. zur Sicherheit der eingesetzten Informatikinfrastruktur) oder wenn Bereiche mit hohen Risiken bekannt sind (z. B. Zugriffsrechte auf besonders schützenswerte Daten).

– Verzicht auf eigene Stellungnahmen zu Bundeserlassen: Im Gesetzgebungsverfahren stellen sich aus Sicht aller Kantone regelmässig die gleichen Fragen. Die Aufsichtsstelle beschränkt sich darauf, die Stellungnahme von PRIVATIM weiterzugeben und allenfalls an dieser mitzuwirken.

Die Zuweisung der Aktivitäten auf die Mitarbeitenden erfolgt nach den Kriterien Region (Gemeinden), kantonale Organisationseinheit (Direktion) und Fachgebiet (z. B. Staatskirchenrecht). Die Mitarbeitenden setzen die Prioritäten nach den aufgezeigten Kriterien selbständig. Die Priorisierung von Vorabkontrollgeschäften erfolgt nach Eingang gemeinsam mit der Leitung der Aufsichtsstelle. Ist es nicht mehr möglich, die vorgegebenen Antwortzeiten einzuhalten (NEF-Leistungsziele) nehmen die Mitarbeitenden die Umpriorisierung, allenfalls die Zuweisung an einen andern Mitarbeitenden, den (Teil-)Verzicht auf Behandlung oder das Senken des Qualitätsstandards nach Rücksprache mit der Leitung der Aufsichtsstelle vor. Diese stellt dabei sicher, dass jedenfalls Kontrollen von Informatikanwendungen und Nachbetreuungen dieser Kontrollen stattfinden und dass trotz Verzichts auf Vorabkontrollen die „Selbststeuerung“ durch die Projektleitungen erhalten bleibt. Bei Beratungen und aufsichtsrechtlichen Interventionen liegen die Schwerpunkte auf den technischen Entwicklungen, die für die Persönlichkeitsrechte der Betroffenen besondere Folgen haben. Die Leitung der Aufsichtsstelle wird eine

Erhöhung der Ressourcen auslösen, wenn zusätzliche Aufgaben, etwa nach Kantonalisierungen, dies erforderlich machen oder wenn Kontrollinstanzen eine Erhöhung zur genügenden Aufgabenerfüllung für erforderlich halten. (S. 1.3).

2.2 Eigenverantwortung der datenbearbeitenden Stellen

Das KAIO hat mit der Hochschule Luzern eine CAS-Ausbildung zur Informatiksicherheit organisiert. Teilnehmer waren vorwiegend die (künftigen) IT-Sicherheitsverantwortlichen des Kantons Bern und Sicherheitsexperten des Bundes. Die Staatskanzlei thematisierte Datenschutzfragen an der jährlichen Weiterbildungsveranstaltung für die Übersetzungsdienste.

2.3 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Berichtsjahr waren fürdie kantonale Verwaltung 34 Millionen CHF in Informatikmittel zu investieren. 161 Millionen CHF (davon 117 Millionen CHF für Drittdienstleister) sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). In diesen Zahlen sind die Aufwendungen der von der Aufsichtsstelle ebenfalls zu beaufsichtigenden Spitäler inklusive des Inselspitals sowie der nicht zentral erfassten Fachanwendungen nicht enthalten.

Für die Prüfung von Informatikanwendungen durch externe Prüfstellen stand der Aufsichtsstelle der Betrag von CHF 182'000 zur Verfügung (s. 3).

Sie verfügte über 4.7 Vollstellen (davon 0.7 für das Sekretariat). Nach der Umstellung auf eine digitale Geschäftsverwaltung wurde auf die Wiederbesetzung einer 50% Sekretariatsstelle verzichtet. Weitere Angaben zu Budget, Rechnung, Erreichen der NEF-Ziele (Finanzzahlen) finden sich im Geschäftsbericht 2014 des Kantons Bern (Band I).

3 Kontrollen von Informatikanwendungen, die im Betrieb stehen

Drei Prüfungen wurden im Berichtszeitraum durchgeführt:

- Grundschutzprüfung der IT-Infrastruktur der Erziehungsdirektion des Kantons Bern:

Die zentralen Informatikdienste (ID) stellen die IT-Grundversorgung der Erziehungsdirektion (ERZ) sicher (E-Mail, Internetdienste, Schuladministration, Ressourcenverwaltung usw.). Um künftige Vorabkontrollen effizienter zu gestalten, haben sich die Aufsichtsstelle und die ID-Leitung auf eine Grundschutzprüfung auf Basis der Norm ISO 27000 geeinigt. Die Prüfung vor Ort hat aufgezeigt, dass die zentralen Informatikdienste eine sehr komplexe und heterogene IT-Infrastruktur professionell betreiben. Handlungsbedarf wurde insbesondere in der Zusammenarbeit mit externen Dienstleistern festgestellt. So kann die ID-Leitung der ERZ die Konfiguration und Servicequalität der Firewall-Infrastruktur, die extern bereitgestellt wird und ein sicherheitsrelevantes Element der Netzwerksicherheit ist, nur marginal beurteilen oder gar kontrollieren (s. 1.1).

- Spitalzentrum Biel (SZB):

Unter professioneller Betreuung der Informatikabteilung und des Leiters Betriebe wurde das Klinikinformationssystem des SZB geprüft. Die Prüfung hat den schmalen Grat aufgezeigt, der zwischen einer optimalen Nutzung aller verfügbaren medizinischen Daten und der Einhaltung des Persönlichkeitsschutzes der Patienten liegt. Die Ergebnisse der Prüfung zeigen, dass der operative IT-Betrieb zuverlässig funktioniert und die Applikationen gut betreut werden. Ebenso ist die Sensibilität für Datenschutzanliegen bei den Hauptbeteiligten vorhanden. Aus technischer Sicht sind die Verantwortlichkeiten für die Betreuung der externen Dienstleister zu präzisieren und Richtlinien für die Durchführung der Wartungsprozesse zu überarbeiten. Die Massnahmen für die Umsetzung des Zugriffskonzeptes sind zeitnah umzusetzen.

- Audit der mobilen Infrastruktur (Smartphone) der Kantonspolizei:

Die Kontrolle der mobilen Infrastruktur der Kantonspolizei beinhaltete das Mobile Device Managementsystem (MDM) und die Smartphones. Zum Zeitpunkt der Berichtsverfassung war die Auswertung der Kontrolle noch nicht abgeschlossen.

- Nachbetreuungen früherer Kontrollen:
  - Grundschutzprüfung Universität Bern

Die Feststellungen aus der Prüfung 2013 wurden mit der Aufsichtsstelle bereinigt und ein Massnahmen- und Terminplan erstellt. Die ISDS-Verantwortlichen der Universität Bern haben die Umsetzung engagiert unterstützt und bereits eine Vielzahl von Massnahmen umgesetzt. Der Abschluss der Arbeiten ist per Mitte 2015 geplant.

  - Klinik Südhang

Dringende Massnahmen sind bereits realisiert worden. Am Löschkonzept wird gearbeitet.

  - Busseninkasso

Die Justizleitung hat zu den Fragen nach der anwendbaren Aufbewahrungsfrist und ob ein Abrufverfahren vorliege eine Stellungnahme abgegeben.

4 Videoüberwachung

Mehrere Videoüberwachungsanlagen für kantonale Gebäude wurden im Vorabkontrollverfahren geprüft, darunter die Anlagen der Kaserne Bern und der Polizeiwachen. Der Aufnahmebereich von Kameras, die unverhältnismässig viel vom Aussenbereich aufnehmen, wie etwa ein öffentliches Trottoir oder eine vorbeiführende öffentliche Strasse, wurde regelmässig korrigiert.

Das Gesetz über den Straf- und Massnahmenvollzug gibt vor, dass Überwachungskameras in Besucherräumen von Strafanstalten nur im Einzelfall „in begründeten Fällen“ und „offen“ (das heisst für die Betroffenen erkennbar) eingesetzt werden dürfen. Dies ergab die Analyse zu einer Anfrage. Weil diese Voraussetzungen nicht erfüllt waren, wurden die Kameras in den Besucherräumen der Anstalten Thorberg entfernt.

Beim KAIO Verwaltungsgebäude war eine Äusserung der Verantwortlichen in den Medien für die Aufsichtsstelle Anlass zu einer Nachfrage nach der nötigen Bewilligung. Dies veranlasste die Betreiber, den Sinn und Zweck der Anlage zu überdenken und auf den weiteren Einsatz der Kameras zu verzichten.

Mit der Kantonspolizei wurde das Vorgehen für die Umsetzung der 2015 einsetzenden Evaluationspflicht für Videoüberwachungsanlagen abgesprochen. Fünf Jahren nach Inbetriebnahme einer Anlage müssen die zuständigen Behörden bzw. Betreiber nach den Vorgaben der Videoverordnung eine Evaluation durchführen und einen Bericht darüber veröffentlichen. Die Kantonspolizei wird die kommunalen und kantonalen Behörden anweisen.

5 Vorabkontrollen von Informatikprojekten

Erneut betreute die Aufsichtsstelle eine hohe Anzahl von Anwendungen aus dem Gesundheitswesen, insbesondere Klinikinformationssysteme (KIS):

- Im Rahmen der Vorabkontrolle der Applikation MC-SIS des Mammografie-Screening-Programms des Kantons Bern, welches durch die Bernische Krebsliga durchgeführt wird, fand im Berichtsjahr ein zweiter Vorortttermin statt. Anschliessend erfolgten zwei Stellungnahmen. Aufgrund von Personalausfällen konnten die überarbeiteten ISDS-Unterlagen noch nicht eingereicht werden.

- Anfang Jahr erfolgten zur Applikation NICERStat des Bernischen Krebsregisters nochmals zwei Stellungnahmen der Aufsichtsstelle. Dank der guten Mitarbeit der Verantwortlichen konnte die Vorabkontrolle anschliessend abgeschlossen werden.

-Im Rahmen der Vorabkontrolle des KIS der Berner Klinik Montana hat die Aufsichtsstelle im Berichtsjahr mehrere Stellungnahmen abgegeben. Der datenschutzrechtliche Teil konnte abgeschlossen werden. Offen sind noch mehrere Punkte zur Informationssicherheit.

-Im Berichtsjahr hat die Aufsichtsstelle mehrere Stellungnahmen zum KIS der Universitären Psychiatrischen Dienste Bern (UPD) abgegeben. Weiter haben Sitzungen mit den Verantwortlichen stattgefunden. Noch offene Punkte sind u.a. die auftragsgesteuerte Berechtigungsvergabe bei den Querschnittsfunktionen, die Bereinigung der Rollen- und Berechtigungsmatrix sowie die Patientensuche.

- Die Vorabkontrolle des Laborinformationssystems (LIS) des Psychiatriezentrums Münsingen (PZM) konnte bis auf einige wenige Punkte des Grundschutzes abgeschlossen werden.

- Zum Klinikinformationssystem der Psychiatrischen Dienste Biel-Seeland – Berner Jura (SPJBB) sind die ISDS-Unterlagen eingetroffen. Inzwischen hat die Aufsichtsstelle eine erste Stellungnahme abgegeben. Eine zweite Stellungnahme wird in Kürze erfolgen.

- Zur Patientenadministrationssoftware OPALE der SPJBB erfolgte Ende Jahr die Bestätigung des Ersatzes der Gruppen- durch Einzelkonten. Dies ermöglichte den Abschluss der Vorabkontrolle.

- Die noch fehlende Löschfunktion in der Patientenadministrationssoftware OPALE UPD wurde implementiert. Die Aufsichtsstelle konnte die Vorabkontrolle damit abschliessen.

- Im KIS des Inselspitals (i-pdos) konnte die gefundene Lösung zur datenschutzkonformen Umsetzung der Feldstechersuche und der Unterteilung zwischen aktiven und passiven Fällen aufgrund von erneut aufgetretenen Anwendungsproblemen noch nicht eingeführt werden. Der Aufsichtsstelle wurde im Berichtsjahr ein Archivierungs- und Löschkonzept eingereicht. Diesem fehlt der erforderliche Detaillierungsgrad. Es liefert insbesondere keine Lösung, wie mit den sich aufgrund der hohen jährlichen Fallzahlen anhäufenden Datenmengen umgegangen wird (Verlängerung der Aufbewahrungsdauer von früheren Behandlungsfällen bei Neueintritt).

- Zu den überarbeiteten ISDS-Unterlagen und dem nachgelieferten Aufbewahrungs- und Löschkonzept zum KIS (PROKIS) der Spitäler Frutigen, Meiringen, Interlaken (fmi ag) hat die Aufsichtsstelle eine Stellungnahme abgegeben.

Mit den erforderlichen Nachbesserungen ist die fmi ag in Verzug.

- Im Berichtsjahr erfolgte ein intensiver Austausch mit dem Psychiatriezentrum Münsingen (PZM) zum Klinikinformationssystem (ORBIS). Im Frühjahr wurde das überarbeitete ISDS-Konzept eingereicht und dazu von der Aufsichtsstelle eine Stellungnahme abgegeben. Das daraufhin überarbeitete Konzept liegt der Aufsichtsstelle zur erneuten Durchsicht vor. Sie wird unter anderem prüfen, ob die geforderte datenschutzkonforme Löschfunktion entwickelt wurde und implementiert werden kann.

- Patiententerminal fmi ag: Dieses Projekt stellt den Patientinnen und Patienten verschiedene Steuerfunktionen zur Verfügung wie Internet, TV, Licht etc. Es werden keine Patientendaten auf dem Terminal dargestellt. Die Vorabkontrolle wurde erfolgreich abgeschlossen

- Identity-Management fmi ag: Mit der eingesetzten Technologie werden die Prozesse zur Bewirtschaftung der Benutzeraccounts und der Berechtigungen unterstützt. Dass Projekt ist wegweisend für ähnliche Anwendungsfälle, da damit kritische Risiken bei der Berechtigungsvergabe und -rücknahme eliminiert werden können und die Vergabe von Applikationsberechtigungen standardisiert und zentral überwacht werden kann.

- Die Prüfung der Applikation ZAPSAP der Bau-, Verkehrs- und Energiedirektion, welche für das Baukostenmanagement, das Auftrags- und Zeitmanagement sowie das kaufmännische Immobilienmanagement eingesetzt wird, erfolgte summarisch. Es fand ausserdem eine Sitzung mit den Verantwortlichen statt. Die datenschutzrechtliche Prüfung konnte im Berichtsjahr abgeschlossen werden. Zum Grundschutz gibt es noch offene Punkte (s. 1.1).

- Zum Studierendenverwaltungssystem Studitracker der Universität Bern erfolgte eine verkürzte Vorabkontrolle. Die Grundschutzprüfung erfolgte bereits im Rahmen der Prüfung der IT-Grundversorgung der zentralen Informatikdienste durch die Aufsichtsstelle.

- Für die Software zur Prüfung und Auszahlung von individuellen Leistungen durch das Alters- und Behindertenamt (ZERO) haben die Verantwortlichen erste Lösungsansätze für eine Löschung der Daten eingereicht. Die dazu gestellten Rückfragen der Aufsichtsstelle sind bis Ende des Berichtsjahres unbeantwortet geblieben.

- BE-Print: Im Infrastrukturprojekt BE-Print wird die bestehende Druckerinfrastruktur mit in den Kommunikationsnetzen eingebundenen Multifunktionsgeräten ersetzt. Das vorgelegte ISDS-Konzept hat das Bearbeiten von Personendaten mittels dieser Infrastruktur nicht berücksichtigt und wurde von der Aufsichtsstelle zurückgewiesen (s. 1. 1).

- HarmTel: Das vorgelegte ISDS-Konzept zur Harmonisierung der Telefonie und Einführung von Microsoft Lync weist aus Sicht der Aufsichtsstelle gravierende Lücken auf. So wurde die Nutzung mobiler Geräte nicht berücksichtigt. Dies gegen den aktuellen und unaufhaltsamen Trend der „Konsumerisierung“ der IT. Ungenügend abgeklärt wurde auch die Frage, ob die Anwesenheits-Statusanzeige in bestimmten Konstellationen nicht zu einer unzulässigen Mitarbeiterüberwachung führen kann und wie mit den anfallenden Randdaten umzugehen ist.

- DMS OSIV: Die Vorabkontrolle des Dokumentenmanagementsystems zur Verwaltung der Dokumente der Invalidenversicherung Bern wurde erfolgreich abgeschlossen.

- KWP 2010: Die sichere Konfiguration der Clients setzt ein ISDS-Konzept voraus. In der Mehrzahl der Direktionen fehlt dies. Die Finanzdirektion stellt ihr ISDS-Konzept den interessierten Direktionen zur Verfügung (s. 1.1).

- Steuerverwaltung AMA-Nesko: Wie bereits bei anderen Vorabkontrollen im Umfeld von Nesko, konnte nicht klar dargelegt werden, wie die ISDS-Anforderungen bei den Outsorcingpartnern letztendlich konkret umgesetzt werden. Die Steuerverwaltung bestellt ihre Leistungen beim KAIO und nicht direkt beim Leistungserbringer. Die Aufsichtsstelle fordert die Herstellung von Transparenz (s. 1.1).

- Die Überarbeitungen der ISDS-Konzepte des kantonalen Finanzinformationssystems FIS und des Personalinformationssystems PERSISKA sind noch nicht abgeschlossen.

- Die Überprüfung von BE-Login führte zu notwendigen Anpassungen: Unter anderem werden die Passwortanforderungen erhöht (Länge, Wechsel etc.) und vor der Anbindung von Fachapplikationen wird geprüft, ob die Drittservices mit einer eigenen Identifikations- bzw. Registrierungsstelle die Datensicherheit gewährleisten (s.1.1).

- Für die statistische Auswertung der kantonalen Webseiten wird neu das Webanalyse-Tool „Adobe Analytics“ eingeführt. Die Daten der Nutzerinnen und Nutzer, die beim Aufrufen der Website anfallen, werden unmittelbar nach deren Erfassung mit technischen Massnahmen anonymisiert. Die Nutzerinnen und Nutzer werden über die statistische Auswertung orientiert und können die Erfassung ihrer Daten unterbinden. Da die Auswertung der Daten durch Dritte in London erfolgt, müssen die datenschutzrechtlichen Aspekte in einem Outsourcingvertrag un-

ter Einschluss der AGB ISDS des Kantons Bern geregelt werden. Der Vertrag wird der Aufsichtsstelle noch vorgelegt.

- Die Vorabkontrolle für das Analyse-System der Polizei zum Verknüpfen von Gewaltdelikten ViCLAS konnte 2013 abgeschlossen werden. Noch immer fehlt aber die vom Regierungsrat zu erteilende Betriebsbewilligung.

Die Ressourcensituation hat es der Aufsichtsstelle erneut nicht erlaubt, die bei den Vorabkontrollen bestehenden erheblichen Rückstände abzubauen. Die Mehrzahl der neu eingehenden Projekte konnten dagegen in angemessenen Fristen behandelt werden.

(Zu den ebenfalls einer Vorabkontrolle unterstellten Videoüberwachungen s. 4, zum begründeten Antrag im Vorabkontrollverfahren zum Aufbewahrungs- und Löschkonzept für ein Klinikinformationssystem s. 8.1).

6 Ansichtsäusserungen, Praxis

Folgende Sachverhalte geben einen Eindruck über die zahlreichen Anfragen an die Aufsichtsstelle:

- Der Einsatz privater Kommunikationsmittel in Verbindung mit frei verfügbaren IT-Anwendungen für die Speicherung, Synchronisation und Bearbeitung von Daten führt - zum Beispiel in Schulen - zu einer Vermischung von privaten und geschäftlichen Daten. Zudem besteht das Risiko, dass durch einfaches Synchronisieren der privaten Geräte via public Cloud–Dienste wie iCloud und Skydrive auch geschäftliche Daten mit transferiert werden. Der Bund hält in seiner Weisung zum IKT-Grundschutz in der Bundesverwaltung fest, dass keine besonders schützenswerten Daten auf privaten mobilen Geräten gespeichert werden dürfen. Zulässig ist dies nur auf Geräten, die zum Zweck der verschlüsselten Mobilkommunikation beschafft oder konfiguriert worden sind.

- Die Rückmeldung an die Vorgesetzten im Mitarbeitergespräch (MAG) ist nicht Teil der Leistungs- und Verhaltensbeurteilung. Sie hat einen persönlich-vertraulichen Charakter und dient der Qualitätsentwicklung. Sie gehört deshalb ins Dossier der Vorgesetzten. Das Personalamt wird das MAG-Formular mittelfristig so anpassen, dass die Rückmeldung nicht mehr automatisch ins administrative Personaldossier aufgenommen wird.

- Die Beratungsgespräche der Ansprechstelle des Personalamts (ASP) stehen unter dem Schutz des Amtsgeheimnisses. Angaben etwa zu Suchtkrankheiten sind durch die zugesicherte Vertraulichkeit geschützt. Solche Angaben gehören zu den besonders schützenswerten Personendaten und dürfen nur gestützt auf eine klare gesetzliche Grundlage weitergegeben werden. Eine solche Grundlage fehlt für die Mitarbeitenden der ASP. Ohne ausdrückliche und freiwillige Zustimmung der betroffenen Personen dürfen deshalb keine Mitteilungen an die Linienvorgesetzten erfolgen.

- Steuerstatistiken von Gemeinden dürfen nur so veröffentlicht werden, dass keine Rückschlüsse auf bestimmte Personen möglich sind. Für kleinere Gemeinden ist zu prüfen, ob dies dadurch sichergestellt werden kann, dass mehrere Gemeinden oder die Einkommensklassen statistisch zusammengefasst werden.

- Verschiedene Anfragen betrafen die Zulässigkeit von Outsourcingverträgen. Grundsätzlich dürfen Behörden des Kantons Bern Datenbearbeitungen durch Dritte vornehmen lassen, wenn dies nicht ausgeschlossen ist und die Datensicherung unter Einschluss der AGB ISDS vertraglich sichergestellt wird. Ein Auftragnehmer untersteht dem Datenschutzgesetz und muss alle technischen und organisatorischen Vorkehrungen treffen, die für die Datensicherung nötig sind. Bei einer Auslagerung der Datenbearbeitung ins Ausland sind zusätzliche Anforderungen und die Schranken des Datenschutzgesetzes zu beachten.

- Die Chatnutzung von XING kommt für eine kantonale Fachgruppe nicht in Frage. Mit XING werden Daten durch Dritte im Ausland bearbeitet. Die Anforderungen des Datenschutzgesetzes u.a. an die Vertraulichkeit und Verfügbarkeit und zur Datenbekanntgabe ins Ausland müssen beachtet werden. Je nach Art und Schutzbedarf der Daten, sind unterschiedliche Sicherheitsanforderungen zu erfüllen. Die Durchsetzung der Datenschutzrechte, wie die jederzeitige Auskunft, Berichtigung und Löschung, muss gewährleistet sein (schweizerischer Gerichtsstand). XING macht geltend, dass Mitgliederdaten ausschliesslich in Deutschland gespeichert werden und dass die Datenströme mit einer SSL-Verschlüsselung gesichert werden. Mit dem Dienstleister Akamai (USA) liege ein Auftragsdatenverarbeitungsvertrag vor, der u.a. den EU-rechtlichen Vorgaben entspreche. Diese Darlegungen sind jedoch nicht nachprüfbar. Die tatsächliche Vereinbarkeit mit dem kantonalen Datenschutzrecht und die Orte der Datenbearbeitungen bleiben unklar.

- Eine private Institution, die Aufgaben nach der Sozialhilfegesetzgebung erfüllt, darf ihre Daten nicht im Cloud-Dienst Wuala speichern. Wohl erfüllt Wuala mehrere Datenschutzvorgaben für Cloud-Dienste. Für einen zulässigen Einsatz fehlt es in den Geschäftsbedingungen und in der Datenschutzrichtlinie jedoch vor allem an

verankerten Kontrollrechten des Auftraggebers. Zudem schliesst Wuala die Haftung weitgehend aus. Erschwerend für eine Rechtdurchsetzung ist auch das Englische als Prozesssprache. Wohl verschlüsselt Wuala, der Cloudanbieter verfügt aber unter Umständen temporär über den Schlüssel.

7 Gesetzgebung

7.1 Bundeserlasse und Konkordate

PRIVATIM nimmt zu Bundeserlassen nur noch vereinzelt Stellung. Hat sich PRIVATIM geäussert oder Stellungnahmen seiner Mitglieder vermittelt, schliesst sich die Aufsichtsstelle – wenn nicht spezifisch bernische Gegebenheiten zu berücksichtigen sind – an (s. 2.1). PRIVATIM verfasste eine Stellungnahmen zum Bundesgesetz über die Informationssicherheit. Zur Änderung des Bundesgesetzes über die Ausländerinnen und Ausländer und weiterer ausländerrechtlicher Erlasse verzichtete PRIVATIM auf eine Stellungnahme.

7.2 Kantonale Erlasse

Die Revision des Arbeitsmarktgesetzes schafft die nötige Rechtsgrundlage für die Bearbeitung und den Austausch besonders schützenswerter Personendaten im Rahmen der interinstitutionellen Zusammenarbeit IIZ. Klärenden Bemerkungen zu den berechtigten Behörden und zur Datenbearbeitung fanden Eingang ins revidierte Gesetz.

Der gegenseitige Zugriff der Kindes- und Erwachsenenschutzbehörden auf ihre Daten bedarf einer gesetzlichen Grundlage. Mit der Revision des Gesetzes über den Kindes- und Erwachsenenschutz wird dieser von der Aufsichtsstelle in der Vorabkontrolle des Geschäftsverwaltungssystems gemachten Feststellung Rechnung getragen. Geschaffen wird auch eine Rechtsgrundlage für Fallkonferenzen. Mit einer indirekten Änderung des Datenschutzgesetzes wird festgehalten, dass in Gemeindereglementen künftig nicht mehr vorgesehen werden darf, dass die Einwohnerkontrolle Auskünfte über die Handlungsfähigkeit erteilt.

Mehrere Stellungnahmen betrafen Ergänzungen der Verordnung über die Harmonisierung amtlicher Register. Unter anderem sollen bisherige Zugriffe auf die Zentrale Personenverwaltung ZPV aus organisatorischen Gründen durch Zugriffe auf GERES ersetzt werden. GERES ist ein Zusammenzug der Einwohnerkontrolldaten aller Gemeinden. Das war Anlass auch die Erforderlichkeit der vorbestehenden Zugriffe zu prüfen.

Im Rahmen der Teilrevision der Personalverordnung wurde auch die Personaldatenbekanntgabeverordnung geändert. Die Aufsichtsstelle hat sich zweimal geäussert. Sie regte an, den Anwendungsbereich weiterhin auf die Bekanntgabe von Personaldaten mit elektronischen Mitteln, das heisst auf Abrufverfahren (insbesondere via Internet oder Intranet), zu beschränken. Die Publikation von Bildern in gedruckten Medien ist bereits durch die Rechtsgrundlage zur Aufgabenerfüllung der Behörde abgedeckt. Zur Frage der stillschweigenden Zustimmung hat sich die Aufsichtsstelle dahingehend geäussert, dass diese nicht in jedem Fall ungenügend ist. In der Regel muss jedoch die ausdrückliche Zustimmung eingeholt werden. Nur so ist sichergestellt ist, dass die betroffene Person sich des Ausmasses der Bekanntgabe bewusst ist und sich auch über die Ablehnungsmöglichkeit im Klaren ist.

Die Direktionsverordnung über die Verwaltung und Archivierung von Unterlagen der Öffentlichrechtlichen Körperschaften und deren Anstalten löst die bisherige Weisung Gemeindearchive / Aktenaufbewahrung in der Gemeinde des Amts für Gemeinden und Raumordnung ab. Die Aufsichtsstelle setzte sich für verhältnismässige Aufbewahrungsfristen ein. Sie fand nicht überall Gehör. Absehbar ist, dass nicht zuletzt Änderungen im übergeordneten Recht regelmässig zu Anpassungen führen werden.

8 Aufsichts- und Justizentscheide

8.1 Aufbewahrungs- und Löschkonzept eines Spitals

Ein Spital reichte im Rahmen der Vorabkontrolle zu seinem Klinikinformationssystem ein Aufbewahrungs- und Löschkonzept bei der Aufsichtsstelle ein. Darin war vorgesehen, dass die Aufbewahrungsfrist der vorbestehenden Behandlungsfälle mit jedem neuen Behandlungsfall verlängert wird. Das Spital begründete dieses Vorgehen unter anderem damit, dass das Behandlungsdossier eines Patienten eine vollständige Einheit darstelle und dass jeder medizinische Entscheid auf der Kenntnis der älteren Fälle beruhe. Die Behandlung eines Patienten sei erst abgeschlossen, wenn er das Spital nicht mehr aufsuche, beziehungsweise der letzte Fall abgeschlossen sei. Daher beginne die Aufbewahrungsfrist erst mit Abschluss der letzten Behandlung zu laufen.
Die Aufsichtsstelle bezeichnete dieses geplante Vorgehen in ihrer darauffolgenden begründeten Empfehlung als mit den datenschutzrechtlichen Vorgaben nicht vereinbar. Eine Aufbewahrung ist pro medizinischen Behandlungsfall vorzusehen und somit muss die jeweilige Aufbewahrungsfrist für jeden einzelnen medizinischen Behandlungsfall separat laufen. Ist ein medizinischer Zusammenhang gegeben, darf die Auf-

bewahrungsfrist eines alten, noch nicht gelöschten Behandlungsfalles verlängert werden. Für bestimmte Spezialabteilungen kann ein medizinischer Zusammenhang zwischen alten und neuen Fällen derselben Abteilung vermutet werden. In den übrigen Fällen obliegt die Beurteilung, ob ein medizinischer Zusammenhang gegeben ist, der Gesundheitsfachperson, welche den aktuellen Fall führt.

8.2 Vernichtung und Archivierung von Personendaten

Das Verwaltungsgericht teilte der ERZ zur Information ein nicht anonymisiertes Urteil im Zusammenhang mit dem Nichtbestehen einer Anwaltsprüfung mit (Kenntnis der Rechtsprechung im Bereich Bildung/Prüfung). Die betroffene Person verlangte von der ERZ daraufhin die Vernichtung sämtlicher im Zusammenhang mit dieser Urteilsmitteilung bearbeiteter Personendaten. Zusätzlich verlangte sie, dass auch das gesamte Dossier zu ihrem Gesuch um Datenvernichtung nach Verfahrensabschluss vernichtet werde.
Das angerufene Verwaltungsgericht hält dazu fest, dass für die Mitteilung des nicht anonymisierten Urteils eine gesetzliche Grundlage gefehlt habe. Diese Mitteilung sei damit rechtswidrig gewesen. Die im Rahmen des anschliessenden Gesuchsverfahrens durch die ERZ gemachten Datenbearbeitungen seien zwar rechtmässig erfolgt, jedoch eine direkte Folge der widerrechtlichen Datenbearbeitung durch das Verwaltungsgericht gewesen. Da das Datenschutzgesetz auch einen Anspruch auf Beseitigung der Folgen einer widerrechtlichen Datenbearbeitung einräume, sei die Aufbewahrung und Archivierung des Gesuchsdossiers eingeschränkt. Der Archivierungsvorbehalt gelte damit nicht und das Gesuchsdossier sei zu vernichten.

8.3 Falsche Zeugnisnoten im Informatiksystem

Die Gewerblich-Industrielle Berufsschule Bern (GIBB) hat Zeugnisnoten mehrere Jahre, nachdem sie in Rechtskraft erwachsen waren, abgeändert ohne ein formelles Verfahren der Wiederaufnahme eingeleitet zu haben. Dies führte zum Nichtbestehen der Lehrabschlussprüfung. Als Grund für die Abänderung gab die GIBB technische Probleme mit der Schulapplikationssoftware „Evento“ an, was zur Ausweisung von angeblich falschen Zeugnisnoten geführt habe.
Das vom Betroffenen angerufene Verwaltungsgericht hielt fest, dass in Rechtskraft erwachsene Zeugnisnoten verbindlich seien und nur mit einem Wiederaufnahmeverfahren abgeändert werden dürfen. Dafür wären entschuldbare Gründe – vorliegend das nachträgliche Auffinden von erheblichen Tatsachen oder Beweismitteln – erforderlich gewesen. Die Probleme mit „Evento“ und falsch ausgestellten Zeugnisnoten seien jedoch bereits im Zeitpunkt der erstmaligen Ausstellung der Zeugnisnoten bekannt gewesen. Die GIBB habe somit nicht damit rechnen dürfen, dass die Noten in den Zeugnissen korrekt ausgewiesen sind. Sie hätte die Lehrkräfte anweisen müssen, zumindest die ungenügenden Noten auf Übereinstimmung mit denjenigen in „Evento“ zu prüfen, was laut Verwaltungsgericht ein vertretbarer Aufwand gewesen wäre. Es verneinte somit entschuldbare Gründe und liess ein Zurückkommen auf die rechtskräftig eröffneten Zeugnisnoten nicht zu.

9 Gemeinderechtliche Körperschaften

- Im Vorjahr hatte die Aufsichtsstelle alle Aufsichtsstellen der Gemeinden informiert, der Vertrag zum Einsatz von Microsoft Office 365 an den Schulen genüge den Datenschutzvorgaben nicht und dürfe nicht unterzeichnet werden. In Verhandlungen mit Microsoft erreichte PRIVATIM nun eine datenschutzkonforme Ausgestaltung des Vertragswerks (das einen Bundesordner füllt und teilweise in englischer Sprache gehalten ist). Das wurde den Aufsichtsstellen der Gemeinden mitgeteilt.
- Mit einer neuen BSIG-Weisung gibt die Justiz-Gemeinde- und Kirchendirektion den Gemeinden vor, welche Religionszugehörigkeiten sie in der Einwohnerkontrolle mit welchen Codes einzutragen haben. Damit kann den im Vorjahr festgestellten unkorrekten Einträgen entgegengewirkt werden.
- Die Aufsichtsstelle wirkte bei Ausbildungsveranstaltungen für Gemeindemitarbeitende mit. Eine solche Veranstaltung fand auch in französischer Sprache statt. (Zur Ablösung der Archivweisung s. 7.2).

10 Besonderes:

10.1 Google Street View

Ein Urteil des Bundesgerichts verpflichtet Google, in seinem Produkt „Street View“ im Bereich von sensiblen Einrichtungen eine vollständige Anonymisierung von Personen und Autokennzeichen vorzunehmen. Der Aufwand für eine lückenlose manuelle Anonymisierung sei vor dem Hintergrund der auf dem Spiel stehenden Persönlichkeitsschutzinteressen hier nicht übermässig. Für den Kanton Bern unterbreitete Google der Staatskanzlei eine 39 Seiten lange Liste. Dies mit dem Hinweis, die Staatskanzleikönne Google allfällig erforderliche Ergänzungen innert Monatsfrist mitteilen. Die Liste war unsorgfältig redigiert. Offenbar wurde in einem Adress- oder Telefonverzeichnis nach bestimmten Suchbegriffen gesucht. Eine Suche nach

Sozialdiensten und Vormundschaftsbehörden (heute Kindes- und Erwachsenenschutzbehörden) war entgegen den bundesgerichtlichen Vorgaben nicht erfolgt. Auch scheint eine Nachbearbeitung durch Google kaum durchgeführt worden zu sein. Das erklärt etwa, dass Google nicht nur vorschlug, die im Verzeichnis enthaltenen Kinderkrippen als sensible Einrichtungen einzustufen, sondern auch die Adressen von Personen mit dem Namen „Krippendorf“. Mit seinem Vorgehen wollte Google seinen Aufwand zur Wahrung der Persönlichkeitsrechte der Betroffenen gering halten und erreichen, dass der Kanton diesen Aufwand übernimmt. Das widerspricht dem Bundesgerichtsurteil und der Kanton hat dazu nicht Hand geboten.

11 Berichtspunkte der Vorjahre

(3: Nachbetreuungen zu den 2013 vorgenommenen Kontrollhandlungen, 5: Weitergeführte Vorabkontrollen, 7.2: Gestützt auf das Merkblatt der Aufsichtsstelle geschaffene Rechtsgrundlage für die Publikation von Fotos auf Internetseiten, 8.1: Begründeter Antrag im Vorabkontrollverfahren zur Datenaufbewahrung in einem Klinikinformationssystem; 9: BSIG-Weisung zum Eintrag von Konfessionsangehörigkeiten).

12 Antrag

Dem Regierungsrat und dem Grossen Rat wird nach Artikel 37 des Datenschutzgesetzes beantragt, vom Bericht Kenntnis zu nehmen.

30. Januar 2015

Der Datenschutzbeauftragte: *Siegenthaler*

13 Anhang

13.1 Abkürzungen, Bezeichnungen

A: Anhang
Adobe Analytics: Werkzeug für Anbieter von Internetseiten, das Statistiken über Seitenbesucher, deren Wohnregion und besuchte Inhalte führt
AGB ISDS: Vom KAIO für den Umgang mit Outsourcingpartnern herausgegebene, allgemeine Geschäftsbedingungen zu Informatiksicherheit und Datenschutz
Akamai: Einer der weltweit grössten Anbieter für die Auslieferung und Beschleunigung von Online-Anwendungen und –Inhalten mit Sitz in Cambridge, Massachusetts, USA (nach Wikipedia)
AMA-Nesko: Ablösung Mainframe (Ablösung des Grossrechnersystems)
Apple: Amerikanisches Unternehmen mit Hauptsitz im kalifornischen Cupertino, das Computer und Unterhaltungselektronik sowie Betriebssysteme und Anwendungssoftware herstellt (nach Wikipedia)
Applikation: Informatikanwendung
ASP: Ansprechstelle des Personalamts (Beratungs- und Auskunftsangebot für Mitarbeitende und Führungsverantwortliche der kantonalen Verwaltung)
BE-Login: kantonsweites Einstiegsportal zur Nutzung von elektronischen Diensten
BSIG: Bernische Systematische Information Gemeinden
CAS: Certificate of Advanced Studies: Studiengang zur beruflichen Weiterbildung
Cloud: Nach Wikipedia: Rechnen in der Wolke: umschreibt den Ansatz, abstrahierte IT-Infrastrukturen (z. B. Rechenkapazität, Datenspeicher, Netzwerkkapazitäten oder auch fertige Software) dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung zu stellen
DMS: Dokumentenmanagement-System
EDÖB: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
ERZ: Erziehungsdirektion
FAQ: Frequently Asked Questions, englisch für häufig gestellte Fragen
FIS: Finanzinformationssystem
fmi ag: Spitäler Frutigen, Meiringen, Interlaken
GEF: Gesundheits- und Fürsorgedirektion
GERES: Informatiklösung zur Verwaltung und Harmonisierung von Personendaten, im Kanton Bern zum Zusammenzug aller Einwohnerkontrolldaten
GIBB: Gewerblich-Industrielle Berufsschule Bern
Google StreetView: Ist ein Zusatzdienst zu Googles Kartendienst Google Maps und dem Geoprogramm Google Earth. Es werden Ansichten in 360-Grad-Panoramabildern aus der Straßenperspektive dargestellt (nach Wikipedia)
iCloud: Von Apple angebotener Cloud-Dienst
ICT: Information and Communication Technology, deutsch: Informations- und Kommunikationstechnologie
ID: Informatikdienste
IIZ: Interinstitutionellen Zusammenarbeit
IKT: Informations- und Kommunikationstechnologie
i-pdos: Integriertes Patientendossier Inselspital (Klinikinformationssystem)
ISO: Internationale Organisation für Normung
ISO 2700x: Normenreihe von Standards der IT-Sicherheit (nach Wikipedia)
IT: Informationstechnologie
ISDS: Informationssicherheit und Datenschutz
IV: Invalidenversicherung
KAIO: Kantonales Amt für Informatik und Organisation
KIS: Klinikinformationssystem(e)
Konsumerisierung: Trend, dass Mitarbeitende ihre privaten mobilen Geräte mit an den Arbeitsplatz bringen und diese Geräte auch beruflich nutzen wollen (nach DSiN-Blog)
LIS: Labor-Informationssystem
MAG: Mitarbeitergespräch
MC-SIS: Multi Cancer Screening Information System, gängige Software für Brustkrebs-Früherkennungsprogramme
MDM: Mobile-Device-Management (deutsch: Mobilgeräteverwaltung)
Microsoft Lync: Anwendung von Microsoft, die verschiedene Kommunikationsmedien (unter anderem IP-Telefonie, Videokonferenz Voicemail) in einer einheitlichen Anwendungsumgebung zusammenfasst. Andern Kommunikationsteilnehmern werden Verfügbarkeitsinformationen gegeben (Anwesenheit, während einer bestimmten Zeit unterbleibende Eingaben auf Tastatur und Maus)
Microsoft Office 365: Eine Kombination bestehend aus Office-Webanwendungen, Serviceleistungen und einem Office-Software-Abonnement (nach Wikipedia)
NEF-Ziele: Im Rahmen der neuen Verwaltungsführung für jede Verwaltungseinheit festzulegende Leistungs- und Wirkungsziele (im Voranschlag und Geschäftsbericht des Kantons Bern aufgeführt)
Nesko: Neues Steuerkonzept
NICER: National Institute for Cancer Epidemiology and Registration: Institution zur Krebsforschung
OPALE: Patientenverwaltungslösung
OSIV: Open System IV, Informatikanwendung mehrerer IV-Stellen
PERSISKA: Personal- und Informationssystem des Kantons Bern
PRIVATIM: Vereinigung der Schweizerischen Datenschutzbeauftragten
PZM: Psychiatriezentrum Münsingen
RAV: Regionale Arbeitsvermittlungsstelle

s: siehe
SIS: Schengener Informationssystem: Europaweite elektronische Fahndungsdatenbank der Schengener Staaten. Darin können Fahndungen nach Sachen und Personen innert kürzester Zeit im gesamten Schengen-Raum ausgeschrieben und abgefragt werden.
SkyDrive: Online-Datenspeicherungs-Dienst von Microsoft (heute OneDrive) (nach Wikipedia)
SPJBB: Psychiatrische Dienste Biel-Seeland – Berner Jura Bellelay
SSL: Secure Sockets Layer, die alte Bezeichnung für Transport Layer Security, ein Netzwerkprotokoll zur sicheren Übertragung von Daten (nach Wikipedia)
SZB: Spitalzentrum Biel
UPD: Universitäre Psychiatrische Dienste Bern
ViCLAS: Violent Crime Linkage Analysis System: Analyse-System zum Verknüpfen von Gewaltdelikten
Wuala: ist ein Cloud-Speicher-Dienst aus der Schweiz, der Daten zentral auf den europäischen Servern der amerikanisch dominierten LaCie AG speichert (nach Wikipedia)
XING: Soziales Netzwerk, in dem Mitglieder vorrangig ihre beruflichen und/oder privaten Kontakte zu anderen Personen verwalten und neue Kontakte finden können (nach Wikipedia)
ZAPSAP: Anwendung für das Baukostenmanagement, das Auftrags- und Zeitmanagement und das kaufmännische Immobilienmanagement der BVE
ZERO: Zur Prüfung und Auszahlung von individuellen Leistungen durch das Alters- und Behindertenamt der GEF eingesetztes Programm
ZPV: Zentrale Personenverwaltung: Datenbank der Steuerverwaltung mit Angaben zu natürlichen und juristischen Personen

13.2 Referenznummern der in Ziffer 8 aufgeführten Aufsichts- und Justizentscheide

8.1: Begründeter Antrag der Aufsichtsstelle 42.72-13.5952 vom 19. Juni 2014
8.2: Urteil des Verwaltungsgerichts VGE 100.2013.156 vom 15. April 2014
8.3: Urteil des Verwaltungsgerichts VGE 100.2014.99U vom 13. Oktober 2014

13.3 Internetadressen

2.3: Geschäftsbericht:
http://www.fin.be.ch/fin/de/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html

9: Mitteilungen an kommunale Datenschutzaufsichtsstellen:
http://www.jgk.be.ch/jgk/de/index/aufsicht/datenschutz/kommunaler_datenschutz/mitteilungenetc.html