Bericht 2013 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

1 Einleitung

1.1 Auf einen Blick

Der Umgang mit vernetzten Grossdatenbanken bildete einen wichtigen Teil der Arbeit der Datenschutzaufsichtsstelle (Aufsichtsstelle) im vergangenen Jahr. Folgendes Beispiel dazu: Das Amt für Informatik und Organisation (KAIO) führt in der Datenbank GERES einen Zusammenzug der Einwohnerkontrolldaten aller Gemeinden. Eine Gemeinde wollte vom KAIO wissen, welchen Code sie muslimischen Glaubensangehörigen zuordnen solle. Dass nach den eidgenössischen und kantonalen Rechtsgrundlagen nur die vier staatlich anerkannten Religionsgemeinschaften erfasst werden dürfen, war ihr nicht bekannt. Das KAIO informierte die Aufsichtsstelle über die Anfrage. Für die Aufsichtsstelle war dies der Anlass, sich die in GERES verzeichneten Religionszugehörigkeiten darstellen zu lassen. Es zeigte sich, dass für mehr als 200‘000 Betroffene unzulässigerweise erfasst war, ob sie keine Religionszugehörigkeit hatten (Atheisten) oder ob sie einer nicht staatlich anerkannten Religionsgemeinschaft angehörten. Um welche Religionsgemeinschaft es im Einzelnen ging, war für die Mehrzahl der Einträge nicht ersichtlich. Einige Gemeinden hatten aber detaillierte Angaben zur Religionszugehörigkeit aufgenommen (insgesamt 24 Codes, zum Beispiel: Quäker). Die Aufsichtsstelle forderte die kommunalen Datenschutzaufsichtsstellen auf, für Abhilfe zu sorgen und allen nicht einer staatlich anerkannten Religionsgemeinschaft angehörenden Personen einen einheitlichen Code zuordnen zu lassen. Mit einschneidenden Folgen: Das auf GERES aufbauende Quellensteuersystem der Steuerverwaltung interpretierte bestimmte Codes als ungeklärte Fälle, die bis zur Klärung nicht nur für die Kirchensteuer sondern generell nicht besteuert werden durften. Das Bundesamt für Statistik beklagte den Verlust statistisch wichtiger Informationen. Gegenüber den Kindes- und Erwachsenenschutzbehörden (KESB) schliesslich war festzuhalten, dass ihr Gesuch um Zugriff auf die Religionszugehörigkeit in GERES schon deshalb abzulehnen sei, weil GERES die gewünschten Angaben künftig nicht mehr führen werde.

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). 2013 fand eine Arbeitssitzung statt. Mitarbeitende der Aufsichtsstelle wirkten in den PRIVATIM-Arbeitsgruppen ‚Information and Communication Technology‘ (ICT) und ‚Gesundheit‘ mit. Letztere erarbeitete im Berichtsjahr die Grundlagen für eine Broschüre zum Patientendossier (Krankengeschichte) und zu den Abklärungen, die zu treffen sind, um die Rechnungen der Spitäler für stationäre Behandlungen vom Kanton zu prüfen (gestützt auf die neue Spitalfinanzierung hat der Kanton 55% des gesamten Rechnungsbetrages zu bezahlen). Die Broschüre lässt sich auf die kantonalen Gegebenheiten anpassen. (Zum Versand des PRIVATIM-Merkblatts an die kommunalen Datenschutzaufsichtsstellen S. 6 und 9)

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:

- Subsidiarität des aufsichtsrechtlichen Handelns: Die Datenschutzgesetzgebung gibt den Betroffenen gute Abwehrrechte (Berichtigung, Vernichtung, Feststellen der Widerrechtlichkeit). Aufsichtsrechtliche Abklärungen haben zu 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.

- 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.

– 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.

– Vorabkontrollen: Verzicht auf inhaltliche Prüfung, verkürzte Prüfung: 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 hat dann zu 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).

– 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.

– Verzicht auf eigene Stellungnahmen zu Bundeserlassen: Im Gesetzgebungsverfahren stellen sich zu Bundeserlassen 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 den Mitarbeitenden nicht mehr möglich, die vorgegebenen Antwortzeiten einzuhalten (NEF-Leistungsziele) nehmen sie 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. Die Leitung der Aufsichtsstelle 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 Datenschutzaufsichtsstelle wird dann eine Erhöhung der Ressourcen auslösen, wenn zusätzliche Aufgaben, etwa nach Kantonalisierungen, dies erforderlich machen.

2.2 Eigenverantwortung der datenbearbeitenden Stellen

An den von den kommunalen Verbänden getragenen Ausbildungsveranstaltungen, beispielsweise an der Veranstaltung zur Umsetzung des Handbuchs „Informationsaustausch unter Behörden“, war ein sehr hohes Engagement der Kursteilnehmenden feststellbar.

Nur wenn Betroffene die zuständige Datenschutzaufsichtsstelle leicht auffinden können, ist es ihnen möglich, ihre Rechte zu wahren. Vorbildlich ist hierzu etwa die Ausgestaltung der Internetseite der Gemeinde Worb.

2.3 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Für die kantonale Verwaltung waren im Jahr 2013 49 Millionen CHF in Informatikmittel zu investieren. 157 Millionen CHF (davon 113 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 und 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 185'000 zur Verfügung (s. 2.4).

Sie verfügte über 4.7 Vollstellen (davon 0.7 für das Sekretariat). Weitere Angaben zu Budget, Rechnung, Erreichen der NEF-Ziele (Finanzzahlen) finden sich im Geschäftsbericht 2013 des Kantons Bern (Band I).

3 Kontrollen von Informatikanwendungen, die im Betrieb stehen

Vier Prüfungen wurden im Berichtszeitraum durchgeführt:

- Grundschutzprüfung Universität Bern:

Die zentralen Informatikdienste stellen die IT-Grundversorgung der Universität Bern sicher (eMail, Internetdienste, Studierendenadministra-

tion, Ressourcenverwaltung usw.). Um künftige Vorabkontrollen effizienter zu gestalten, haben sich die Aufsichtsstelle und die IT-Leitung auf eine Grundschutzprüfung auf der Basis der Norm ISO 27000 geeinigt. Das Erstellen des entsprechenden Prüfkatalogs bedeutete für die Universität einen grossen Aufwand.
Die Prüfung vor Ort hat aufgezeigt, dass die zentralen Informatikdienste eine sehr komplexe und heterogene IT-Infrastruktur professionell betreiben. Die grosse Vielfalt macht die Aktualisierung und Dokumentation der Systeme aufwändig. Hier wurde Handlungsbedarf festgestellt.

- Busseninkassostelle:

Der Informationsfluss innerhalb des Inkassoprozesses geht über mehrere Systeme und Instanzen. Den Mitarbeitenden stehen - gemessen an der Inkassoaufgabe - unverhältnismässige Zugriffsrechte in die Daten der im Geschäftskontrollsystem der Gerichte Verzeichneten zu. Seit der Einführung des Systems wurde kein Eintrag gelöscht. Ein Löschkonzept oder eine Löschvorgabe fehlen. Prozessschwachpunkt ist das Fehlen aktiver Rückmeldungen über erfolgte Zahlungen von Säumigen.
2014 soll das Busseninkasso organisatorisch von der Justiz-, Gemeinde- und Kirchendirektion (JGK) zur Justizleitung übergehen. Die Justizleitung war bei der Vorstellung des Prüfberichts anwesend.

- Klinik Südhang:

Die Klinik Südhang betreut alkoholabhängige Personen. Als Stiftung erfüllt sie eine Aufgabe nach der Gesundheitsgesetzgebung. Mit den besonders schützenswerten Personendaten wird verantwortungsbewusst umgegangen. Die Leitung gibt klare Prozesse und Strukturen vor. Die interne Informatikinfrastruktur wird von einem eigenen Fachmann betreut. Diesem obliegt auch die Administration der Berechtigungen. Die Applikationen und Server betreibt ein externer Dienstleister. Mit diesem bestehen klar formulierte Leistungsvereinbarungen.
Mängel bestehen bei der Datenhaltung; weder wird zwischen aktiven und passiven Fällen unterschieden noch ist eine Löschung und Archivierung umgesetzt. Für den Mailverkehr muss eine Verschlüsselung eingerichtet werden, etwa durch den Einsatz des im Gesundheitswesen stark verbreiteten HIN-Mails.

- Wehrpflichtersatz:

Die Applikation WPEV (Wehrpflichtersatzverwaltung) wird von einer externen Firma betreut und in einem externen Rechenzentrum (Abraxas Informatik AG) betrieben. Erst nach einer engagierten Intervention der Amtsleitung erhielten die Prüfenden den notwendigen Zugang zu Applikation und Systemen. Die Prozesse sind gut eingespielt und die Verantwortlichen gehen sorgfältig mit den Daten um. Datenlöschung und Archivierung sind aber in WPEV nicht gelöst. Die direkte Abhängigkeit vom externen Dienstleister im Kerngeschäft bildet ein erhebliches Risiko. Mit ihm bestehen punkto Datenschutz und Informationssicherheit zu wenig klar formulierte Leistungsvereinbarungen. Ein Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept) fehlt und Passwort- und Protokollierungsvorgaben sind ungenügend umgesetzt.

- Nachbetreuungen früherer Kontrollen:
  - Spital STS AG, Thun

Die Feststellungen aus der Prüfung 2012 wurden mit der Aufsichtsstelle bereinigt und es wurde ein Massnahmen- und Terminplan erstellt. Erste Ergebnisse wurden präsentiert: So wurden ein ISDS-Beauftragter eingesetzt, die Risikoanalyse und weitere ISDS-Dokumente erstellt und z.T. bereits zur Umsetzung freigegeben.

- IV-Stelle

Die in der Prüfung 2012 gemachten Feststellungen wurden mit den Aufsichtsstellen derjenigen Kantone besprochen, die ebenfalls die Anwendung OSIV einsetzen. Diese haben daraufhin den Sachverhalt überprüft.

4 Videoüberwachung

In mehreren Vorabkontrollverfahren waren Kameras im Aussenbereich und im Innenbereich sowie Kameras mit und ohne Aufzeichnung zu prüfen. In der Regel konnte bei einer Aufzeichnung auf die gleichzeitige Echtzeitüberwachung verzichtet werden und umgekehrt (Ausgleichskasse und IV-Stelle Bern).

Videoaufzeichnungen gelten als schwere Eingriffe in das Grundrecht auf Datenschutz und benötigen eine formellgesetzliche Grundlage. In einer Ansichtsäusserung gegenüber der Kantonspolizei hielt die Aufsichtsstelle fest, dass dies auch für Aufzeichnungen in öffentlichen Gebäuden gilt, die nicht allgemein zugänglich sind.

Werden Eingänge eines öffentlichen Spitals überwacht, erfassen Aufzeichnungen immer auch Patientinnen und Patienten und unterstehen dem Berufsgeheimnis. Zwar darf im konkreten Fall (z.B. Diebstahl) nur die Kantonspolizei solche Aufzeichnungen auswerten. Damit sie das kann, müssten die Ärzte und das Pflegepersonals des Spitals aber von der Schweigepflicht befreit werden. Da das zuständige Kantonsarztamt keine generellen Befreiungen gewährt, verlangte das Polizeikommando den Verzicht auf eine Aufzeichnung (Spital Netz Bern AG, SNB AG).

In verschiedenen Gefängnissen und Vollzugseinrichtungen des Kantons Bern kommen zahlreiche Überwachungskameras zum Einsatz. Auf Anregung der Aufsichtsstelle verpflichtet das Amt für Freiheitsentzug und Betreuung seine Mitarbeitenden mit einem Merkblatt zum datenschutzkonformen Umgang mit Videoüberwachungsanlangen.

5 Vorabkontrollen von Informatikprojekten

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

- In der Vorabkontrolle des KIS (kiSro) muss die Spital Region Oberaargau AG (sro ag) darlegen, wie der Schutz exponierter Personen (VIP-Schutz) umgesetzt wird und wie die Protokollierung der Lesezugriffe erfolgen soll. Zudem ist ein Datenvernichtungs- und Archivierungskonzept auszuarbeiten (s. 8.4).

- Die intensiven Gespräche zum KIS des Inselspitals (i-pdos) wurden im Berichtsjahr weitergeführt. Es wurde eine differenzierte Lösung gefunden, welche die Datenschutzvorgaben für die Feldstechersuche und die Unterteilung zwischen aktiven und passiven Fällen erfüllt. Die Aufsichtsstelle erwartet die Umsetzungsbestätigung im Frühjahr 2014 (Verzögerungen aufgrund fehlender Benutzerfreundlichkeit der Suchmaske). Eingereicht wurden je ein Grobkonzept zur Leseprotokollierung und zum Archivieren und Löschen der Protokolldaten.

- Im Projekt KIS des Psychiatriezentrums Münsingen (PZM; ORBIS) wurden provisorische Lösungsvorschläge eingereicht. Eine definitive Beschreibung der geforderten Funktionalitäten ist noch ausstehend.

- Im Berichtsjahr erfolgte eine Besprechung zu den Kernpunkten des neu einzuführenden elektronischen Patientendossiers in den Universitären Psychiatrischen Dienste (UPD). Aufgrund von personellen Wechseln war die ISDS-Dokumentation im Berichtsjahr noch nicht prüfbereit.

- Die Aufsichtsstelle ist mit ihrer vierten Stellungnahme zu den überarbeiteten ISDS-Unterlagen und dem nachgelieferten Aufbewahrungs- und Löschkonzept zum KIS (PROKIS) der Spitäler Frutigen, Meiringen, Interlaken (fmi ag) in Verzug.

- Die Bereinigung der Zugriffsberechtigungen für das KIS der SNB AG ist erfolgt und die Patienten werden in der Patientenbroschüre auf die Möglichkeit der Sperrung eines abgeschlossenen Falls hingewiesen. Nach der Sperrung ist der Fall beim Wiedereintritt nicht mehr einsehbar. Der Aufbewahrungs- und Löschmechanismus ist weiterhin ein Diskussionspunkt.

- Zum KIS der Berner Klinik Montana konnte ein Vororttermin stattfinden und eine erste Stellungnahme abgegeben werden.

- Das eingereichte Archivierungs- und Löschkonzept zum Bildarchivierungssystem der fmi ag (Picture and Communication System, PACS) bildete den Abschluss der Vorabkontrolle. Erstmals wurde das sogenannte „organisatorische Löschen“ geprüft und umschrieben, unter welchen Voraussetzungen es dem „physischen Löschen“ gleichgesetzt werden kann: Eine Vernichtung im Sinne des Datenschutzgesetzes liegt dann vor, wenn durch das Löschen der Daten auf einem elektronischen Datenträger diese mit einem angemessenen technischen und organisatorischen Aufwand nicht mehr wieder lesbar gemacht werden können. Das rechtlich korrekte Datenvernichten kann gerade auch dadurch herbeigeführt werden, dass diejenigen Stellen, die zu einem erneuten Lesbarmachen der Daten in der Lage sind, rechtlich so eingebunden werden, dass sie ein Lesbarmachen von „vernichteten“ Daten grundsätzlich unterlassen. Die Aufsichtsstelle forderte daher, dass sicherzustellen ist, dass einmal gelöschte Daten gelöscht bleiben und nicht durch einen Datenrücksicherungsprozess (restore) wieder lesbar gemacht werden.

- Die datenschutzrechtlich geforderte Löschfunktion fehlte in der Patientenadministrationssoftware OPALE, welche in den drei psychiatrischen Kliniken des Kantons eingesetzt wird. Die Softwarelieferantin setzt die Anforderung für die UPD nun so um, dass sie den Personenbezug bei den gespeicherten Daten entfernt (Anonymisierung). Diese Funktionalität wird noch zu prüfen sein.

- Die Bestätigung des Ersatzes der Gruppen- durch Einzelkonten in den Psychiatrischen Diensten Biel-Seeland – Berner Jura (SPJBB) ist noch ausstehend.

- Die ISDS-Unterlagen zum System OPALE, wie es im PZM eingesetzt wird, liegen seit längerer Zeit vor und konnten aus Ressourcengründen noch nicht geprüft werden.

- Für das System zur Erfassung von Pflegedienstleistungen am PZM (tacs) wurde das Vorarchiv mit den eingeschränkten Zugriffsberechtigungen eingerichtet und die Umsetzung der Löschvorgaben bestätigt. Damit konnte die Vorabkontrolle abgeschlossen werden.

- Die Bernische Krebsliga führt mit der Applikation MC-SIS das Mammografie-Screening-Programm des Kantons Bern durch. Sobald die

noch offenen Punkte geklärt sind, wird die Aufsichtsstelle ihre erste Stellungnahme abgeben.

- Zu den ISDS-Unterlagen für die Applikation NICERStat des Bernischen Krebsregisters hat die Aufsichtsstelle einen Vorortttermin durchgeführt und eine erste Stellungnahme abgegeben.

- Beim Online-Patienten-Anmeldesystem (O-PAN) der Spitex Bern erfolgt lediglich eine Prüfung des Grundschutzes. Der Informatiksicherheitsverantwortliche des Kantons (IT-SIBE) hat mehrere Stellungnahmen abgegeben.

- Die Personalmanagementsoftware SAP HCM (Projektname PERSAP) des Inselspitals konnte nach der Prüfung des Archivierungs- und Löschkonzepts abgeschlossen werden.

- Zum Ersatz der Patienten-Medien-Terminal und zum Patientenidentifikationssystem der fmi ag wurde nach einem Vorortbesuch Stellung genommen.

- Bei einer ersten Kontrolle des Klinikinformationssystem KISIM des Spitalzentrums Biel (SZB) war das Fehlen aktueller ISDS-Unterlagen festgestellt worden. Zu den vom SZB inzwischen aktualisierten ISDS-Unterlagen gab die Aufsichtsstelle weitere Stellungnahmen ab.

Auch ausserhalb des Gesundheitsbereichs waren zahlreiche Vorabkontrollen durchzuführen:

- Die Vorabkontrolle der beiden Applikationen der Erziehungsdirektion StipBE-Online und Stipendienapplikation (erleichtertes Ausrichten von Ausbildungsbeiträgen) konnte bis auf das Löschkonzept abgeschlossen werden.

- Zur Applikation BISO-BE der Erziehungsdirektion zur Abwicklung der Berufs-, Studien- und Laufbahnberatung fand ein Vorortttermin statt. Im Anschluss hat die Aufsichtsstelle mehrere Stellungnahmen abgegeben. Im Herbst konnte die Vorabkontrolle abgeschlossen werden.

- Bis zum Abschluss der Grundschutzprüfung Universität Bern (s. 2.4) standen die Kontrollarbeiten an folgenden Projekten still: UNICARD, Kernsystem Lehre (KSL) und Studitracker (Studierendenadministration). Die noch ausstehenden Rückmeldungen der Universität zu UNICARD und KSL wurden eingefordert.

- Für die Fachapplikationen Escada (Lehrvertragsmanagement inklusiv Zuweisung von Prüfungsnoten) und Evento (Schulverwaltungssoftware für die Schulverwaltung, Kursadministration, Veranstaltungs- und Ressourcen-Planung) wurde ein gemeinsames ISDS-Konzept eingereicht. Die Aufsichtsstelle forderte eine aktualisierte Umsetzungsplanung für die noch nicht umgesetzten Grundschutzmassnahmen. Sie wird nun prüfen, ob ein ausreichend differenziertes Benutzerberechtigungs- sowie Datenarchivierungs- und Löschkonzept eingereicht und ob ein Prozess für die Verwaltung der Benutzeraccounts eingeführt wurde.

- Auf das Einverlangen von Strafregisterauszügen verzichtet die Berner Fachhochschule (BFH) nach einem Hinweis der Aufsichtsstelle (fehlende Rechtsgrundlage). Bereits elektronisch gespeicherte Auszüge wurden gelöscht. Das Studierenden-Administrationssystem IS-Academia der BFH wurde weiter ausgebaut (Schnittstellen und Einbindung weiterer Abteilungen), die angepasste ISDS-Dokumentation liegt der Aufsichtsstelle zur dritten Stellungnahme vor.

- Nach einer Vorbesprechung wurden die ISDS-Unterlagen für das Case Management Berufsbildung zur Prüfung eingereicht (CM-Online). Durch die Fallführung soll erreicht werden, dass Jugendlichen und jungen Erwachsenen mit Mehrfachproblematik eine erfolgreiche Berufslaufbahn bzw. der Einstieg ins Erwerbsleben gelingt.

- Für die Software zur Prüfung und Auszahlung von individuellen Leistungen durch das Alters- und Behindertenamt (ZERO) ist das Archivierungs- und Löschkonzept noch ausstehend.

- Der Workflow der Krankmeldungen untersteht bei kantonalen Verwaltungsstellen (Personalamt) dem kantonalen Datenschutzgesetz, beim Versicherer gelten die Datenschutzbestimmungen des Krankenversicherungsgesetzes und des Bundesdatenschutzgesetzes. Die vom Personalamt zur Vorabkontrolle unterbreitete Workflowlösung (Internetformular) erfüllt diese rechtlichen Vorgaben.

- Besonders schützenswerte Daten sind während eines Arbeitsverhältnisses in zwei Kategorien aufzuteilen: Die eine enthält Daten, die rollend nach 5 Jahren zu vernichten sind (wie einfache Arztzeugnisse), die andere solche, die 5 Jahre nach Beendigung des Arbeitsverhältnisses zu vernichten sind (z.B. Zeugnisse aus den Bewerbungsunterlagen). Das ergab die Prüfung des Projekts Webarchiv des Personalamts.

- Zum überarbeiteten ISDS-Konzept des kantonalen Finanzinformationssystems FIS bestehen noch offene Pendenzen (Zugriffsrechte, Archivierungskonzept, Ausführungen zu den integrierten Systemen).

- Gleiches gilt für das ebenfalls überarbeitete ISDS-Konzept zum Personalinformationssystem PERSISKA.

- Das Projekt elektronische Pensenmeldung (ePM) erfüllt die datenschutzrechtlichen Vorgaben. Ob das für den vorgesehenen Zugang über das neu in Betrieb stehende BE-Login Portal

auch gilt, ist offen. Die Vorabkontrollunterlagen zu BE-Login wurden der Aufsichtsstelle erst kurz, bevor das System der Bevölkerung zur Verfügung gestellt wurde, unterbreitet.

- Auch die ISDS-Unterlagen zum Fallbearbeitungssystem der 11 Kindes- und Erwachsenenschutzbehörden (KESB) gingen der Aufsichtsstelle verspätet zu. Anstelle des ISDS-Konzepts reichte die Projektleitung das für die Bundesverwaltung vorgegebene Bearbeitungsreglement ein. Die Angaben zur Informatiksicherheit zeigten zu wenig klar auf, welche Massnahmen noch zu treffen sind. Die Mitarbeitenden haben nicht nur auf die Daten ihrer Behörde sondern kantonsweit Zugriff. Das missachtet das Verhältnismässigkeitsgebot.

- Zur Grundschutz IT-Infrastruktur der Erziehungsdirektion fanden mehrere Sitzungen statt.

- Die Vorabkontrolle zu dem von der Kantonspolizei für alle Kantone (Konkordat) geführten System zum Verknüpfen von Gewaltdelikten (ViCLAS) schloss die Aufsichtsstelle erheblich verspätet ab. Im nun folgenden Betriebsbewilligungsverfahren wird zu berücksichtigen sein, dass das System vom Anbieter nicht mehr erneuert wird. Das führt zu Sicherheitsproblemen.

- Nachdem die Kantonspolizei einen Strategiewechsel prüft, erledigte sich das ebenfalls verspätete Vorabkontrollverfahren zum Protokollsystem OboraNew der Kantonspolizei von selbst.

- Soll die Polizei mit einer Abrufmöglichkeit auf die Daten der Gefängnisverwaltung überprüfen können, ob sich eine angehaltene Person in Haft befindet, ist hierzu eine Grundlage in einem Gesetz erforderlich. Darauf wies die Aufsichtsstelle das Amt für Freiheitsentzug und Betreuung schon vor längerer Zeit hin. Nachdem die erforderliche Rechtsgrundlage immer noch fehlt, durfte die Teilanwendung Police-Tool nicht in Betrieb genommen werden. Auf eine ablehnende Verfügung gegen diese Stellungnahme der Aufsichtsstelle verzichtete das Amt.

Die Ressourcensituation hat es der Aufsichtsstelle nicht erlaubt, die bei den Vorabkontrollen bestehenden erheblichen Rückstände abzubauen. Weitgehend geglückt ist es dagegen, neu eingehende Projekte in angemessenen Fristen zu behandeln. Der Umgang einzelner Projektleitungen mit den Vorabkontrollvorgaben führte zum Eindruck, es werde eine Taktik des Minimierens angestrebt. Vorgelegt wurden mit minimstem Aufwand erstellte Pro-forma-Unterlagen mit inneren Widersprüchen. Die Aufsichtsstelle weist solche Unterlagen zur Verbesserung zurück und macht die Projektleitungen darauf aufmerksam, dass die Vorabkontrollunterlagen ein Instrument sind, das es in erster Linie ihnen erlaubt, datenschutzkonforme Datenbearbeitungen sicher zu stellen.

(Zu den ebenfalls einer Vorabkontrolle unterstellten Videoüberwachungen s. 4, zum Beschwerdeverfahren im Vorabkontrollverfahren eines Klinikinformationssystems s. 8.4).

6 Ansichtsäusserungen, Praxis

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

- Mit DHCP-Logs kann in Verbindung mit weiteren Elementen unter anderem festgestellt werden, welche Mitarbeitenden eine bestimmte Internetseite besucht haben. Um technische Fehler festzustellen, dürfen sie 4 bis 6 Wochen aufbewahrt werden. Will eine Dienststelle die DHCP-Logs länger aufbewahren, damit sie eine missbräuchliche Internetverwendung durch Mitarbeitende feststellen kann, benötigt sie hierzu eine Rechtsgrundlage in einem Gesetz. Dies hielt die Aufsichtsstelle entgegen der von der Finanzdirektion und dem KAIO vertretenen Auffassung fest.

- Will eine Dienststelle Fotos von Personen auf ihrer Internetseite publizieren, ist eine rechtliche Grundlage in einem Gesetz erforderlich. Wird zusätzlich die Einwilligung der betroffenen Person eingeholt, genügt eine Verordnungsbestimmung. In einem hierzu veröffentlichten Merkblatt hat die Aufsichtsstelle nebst diesen Voraussetzungen zur Publikation auch die Rechte von Dritten und Mitarbeitenden aufgezeigt. Hauptsächlich geht es um Abwehrrechte wie etwa um Löschbegehren gegen widerrechtlich publizierte Fotos.

- Mit Microsoft 365 (MS365) wird das Microsoft-Office Paket und Speicherplatz in der Cloud zu günstigen Konditionen zur Verfügung gestellt. Das Angebot spricht insbesondere Schulen an, da damit Wartung und Support weitgehend entfallen. Aus Sicht des Datenschutzes ist problematisch, dass die Daten im Ausland bearbeitet werden. Der Gerichtsstand im Ausland verbietet es den Schulen diese Lösung einzusetzen (erschwerte Rechtsdurchsetzung). Das war gegenüber interessierten Schulverantwortlichen festzuhalten. Ein Merkblatt von PRIVATIM enthält Erläuterungen dazu. Die Aufsichtsstelle leitete das Merkblatt an die kommunalen Aufsichtsstellen weiter. Der Trend zu solchen Diensten scheint aber unaufhaltsam. Moderne Kommunikationsplattformen nutzen sie nicht selten automatisch [z. B. Synchronisation über die iCloud (Apple) oder die Mediaplattform von Google+].

- Mehrere Anfragen betrafen die Auskunftspflicht gegenüber den Steuerbehörden. Die Auf-

sichtsstelle bestätigte, dass sowohl die Einsicht in Krankheitsrechnungen wie auch in Firmenkundendaten unter die Auskunfts- bzw. Mitwirkungspflicht nach Steuergesetz fallen.

- Wiederholt wurden die detaillierten Fragebögen für Wochenaufenthalter zum Festlegen des Steuerdomizils beanstandet. Die Fragebögen wurden überarbeitet und datenschutzsensibler ausgestaltet. Angaben zu besonders schützenswerten Personendaten, wie zu politischen, religiösen oder weltanschaulichen Aktivitäten, sind freiwillig.

- Arbeitgeber können von der Regionalen Arbeitsvermittlungsstelle (RAV) den Lebenslauf von stellensuchenden Personen erhalten. Ein Lebenslauf darf aber nur gestützt auf eine gesetzliche Grundlage oder auf eine schriftliche Zustimmung im Einzelfall weitergegeben werden. Den Betroffenen war nicht immer bewusst, dass sie mit dem Ankreuzen der „Freischaltung" in der Wiedereingliederungsvereinbarung ihre Zustimmung dazu geben. In Zukunft werden sie ausdrücklich auf die Tragweite dieser Bestimmung hingewiesen.

- Regelmässig werden die Möglichkeiten und Fristen für die Vernichtung von Daten und Akten von Strafverfahren, von polizeilichen Ermittlungsverfahren und von Strafregistereinträgen nachgefragt. Die Fristen dafür sind je nach Sachverhalt und Stand des Verfahrens unterschiedlich. Sie lassen sich den eidgenössischen und kantonalen Gesetzesbestimmungen (Strafrecht, Strafprozessrecht, kantonale Einführungsgesetzgebung) entnehmen. Bevor ein Vernichtungsgesuch gestellt wird, ist um Auskunft und Einsicht zu ersuchen.

- Gibt ein Mitarbeiter Daten – etwa aus seinem Notizbuch –niemandem bekannt, kann es sich um ein persönliches Arbeitsmittel handeln. Für dieses gilt das Datenschutzgesetz nicht. Geht es um Daten von Dritten, besteht für diese damit kein Einsichtsrecht. Auch der Berichtigungs- und Vernichtungsanspruch fehlt. Notizen können auch mit technischen Mitteln erfolgen (PC, Handy). Vereinzelt haben sich Polizeimitarbeitende daher auf den Standpunkt gestellt, mit ihrem Handy gemachte Bildaufnahmen (z. B. von Wohnungsinnenräumen oder von Prostituierten) seien ebenfalls als persönliche Arbeitsmittel einzustufen. Das ist jedenfalls dann unzulässig, wenn das Polizeirecht das ordentliche, unter dem Geltungsbereich des Datenschutzgesetzes stehende Erheben dieser Daten nicht zulässt.

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.
Entgegen dem Antrag des Regierungsrats verpflichtete der Grosse Rat mit einer Motion zum Nachrichtendienstgesetz den Regierungsrat, sich im Vernehmlassungsverfahren für das Beibehalten der kantonalen Oberaufsicht durch das Parlament einzusetzen. Er setzte damit ein Zeichen, dass ein Ausschalten der kantonalen Aufsichtsrechte in diesem auch datenschutzrechtlich äusserst heiklen Bereich nicht angeht.
Zum Bundesgesetz über die Registrierung von Krebserkrankungen gab die Aufsichtsstelle zu bedenken, dass für das Erheben von Mindestdaten eine hinreichend bestimmte formellgesetzliche Grundlage genügt, bei Zusatzdaten jedoch am Erfordernis der Einwilligung des Betroffenen festzuhalten ist. Weiter regte sie an, dass die übermittelten Originaldaten nach dem Registrierungsvorgang und der Qualitätssicherung durch die nationale Krebsregistrierungsstelle vernichtet werden müssen, da sie nicht mehr benötigt werden. Im Übrigen verwies sie auf die Stellungnahme von PRIVATIM.
Ein Zweck des online abrufbaren Registers über Gesundheitsfachpersonen ist der Schutz und die Information von Patientinnen und Patienten. Der datenschutzrechtliche Verhältnismässigkeitsgrundsatz erfordert ein Minimieren auf das Notwendige: Zum Schutz der Patientinnen und Patienten genügt es, wenn ersichtlich ist, ob eine Gesundheitsfachperson auf der Liste der Gesundheitsfachpersonen mit anerkannten Ausbildungsabschlüssen figuriert (und dort wo notwendig, eine Berufsausübungsbewilligung besitzt). Ob ein Eintrag früher bestand, ist nicht aufzuführen. Dies hielt die Aufsichtsstelle zum Revisionsvorschlag zur Interkantonalen Vereinbarung über die Anerkennung von Ausbildungsabschlüssen fest.

7.2 Kantonale Erlasse

Zum Gesetz über die Finanzkontrolle wurde der Vorschlag der Aufsichtsstelle, den abrufähnlichen Zugriff auf Daten aus dem Finanzinformationssystem FIS abzustützen, in erster Lesung vom Grossen Rat verabschiedet.

Raumbezogene Daten können durch Verknüpfungen/Kombinationen leicht zu Daten mit Personenbezug werden. Etwa durch ein Verbinden mit der Adresse kann jede Angabe über eine zunächst nicht bestimmbare Person einen Personenbezug erhalten. Die Kombinationsmög-

lichkeiten sind unbegrenzt. Das bringt (Daten-) Grundlagen für Planung und Forschung, birgt aber auch Risiken. Die Aufsichtsstelle wurde bereits zu den Vorarbeiten zum neuen Kantonalen Geoinformationsgesetz beigezogen. Im Mitbericht gab sie weitere Hinweise. So wies sie etwa darauf hin, dass die Haftung des Kantons für unrichtige Geodaten mit Personenbezug nicht ausgeschlossen werden kann.

Zur Einführungsverordnung zum Konkordat über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen verwies die Aufsichtsstelle auf den Vorbehalt der Regelung der Videoüberwachung im Polizeigesetz. Für die Pflicht für urteilende Strafbehörden, Strafurteile an die Polizei zu melden, verlangte sie eine formellgesetzliche Grundlage.

Verschiedene Stellungnahmen betrafen Ergänzungen der Verordnung über die Harmonisierung amtlicher Register. Fragen stellen sich regelmässig zur Verhältnismässigkeit des Umfangs der Zugriffe. Erhält eine Stelle etwa neu einen Zugriff auf GERES (Zusammenzug der Einwohnerkontrolldaten aller Gemeinden), so ist ihr der vorbestehende Zugriff auf die Zentrale Personenverwaltung (ZPV) zu entziehen, soweit damit der gleiche Informationsbedarf abgedeckt werden kann. In diesem Zusammenhang zeigte sich, dass auch das Grundstück-Dateninformationssystem GRUDIS auf die ZPV Zugriffe gewährt. Sie waren aber nicht auf Personen mit einem Bezug zu Grundstücken beschränkt, sondern umfassten alle Daten der ZPV. Korrekturen wurden eingeleitet.

Die Aufsichtsstelle gab zwei Hinweise zur Totalrevision der Spitalversorgungsverordnung ab. Die Gesundheits- und Fürsorgedirektion bestätigte, dass das Spitalamt für die Berechnung des Ausbildungspotentials nur eine Datensammlung zu statistischen Zwecken (ohne Bezug zu den betroffenen Mitarbeitern) führen wird.

Die Direktionsverordnung über die Verwaltung und Archivierung von Unterlagen der öffentlichrechtlichen Körperschaften und deren Anstalten soll die bisherige Weisung des Amtes für Gemeinden und Raumordnung ablösen. Die Aufsichtsstelle wurde in einer frühen Phase beigezogen. Sie äusserte sich zu Grundsatzfragen der Archivierung und zu Detailfragen über Aufbewahrungsfristen.

8 Aufsichts- und Justizentscheide

8.1 Verweigerung der Einsicht in einen Supervisionsbericht

In einer kantonalen Einrichtung gab es Probleme in der Teamzusammenarbeit, weshalb eine Supervision angeordnet wurde. Ein von der Supervision betroffener Mitarbeiter verlangte Einsicht in den entsprechenden Bericht. Laut Polizei- und Militärdirektion wurde ihm die Zustellung einer Fotokopie des vollständigen Berichts zu Recht verweigert. Soweit der Bericht Personendaten anderer Mitarbeiter enthalte, die in Zusammenhang mit seinen eigenen Personendaten stehen, stünden überwiegende öffentliche aber auch besonders schützenswerte private Interessen einer Einsicht entgegen. Ohne eine Geheimhaltung wäre das Ziel der Supervision – die funktionierende Teamzusammenarbeit und somit eine Wiederherstellung des geordneten Verwaltungshandelns - wohl nicht zu erreichen. Zudem hätten die Mitarbeitenden ein Interesse, frei von Befürchtungen negativer Konsequenzen ihre Befindlichkeiten im Rahmen einer Teamsupervision darzulegen.

8.2 In ein Polizeijournal ist Einsicht zu gewähren

Die Beschwerdeführerin verlangte Einsicht in die sie betreffenden Daten eines Polizeijournals. Dies wurde ihr von der Kantonspolizei verweigert. Sie erhielt lediglich eine zusammengefasste Darstellung der Einträge. Die Polizei- und Militärdirektion hielt hierzu fest, dass eine solche Zusammenfassung von Polizeijournaleinträgen lediglich in Frage komme, wenn das durch überwiegende öffentliche oder Drittinteressen gerechtfertigte Abdecken zur Unleserlichkeit des Textes führen würde. Dies sei nicht der Fall. Es hätten der Beschwerdeführerin die Einträge im Polizeijournal daher zugestellt werden müssen. Die Polizei- und Militärdirektion hält jedoch fest, es sei rechtmässig, gewisse Passagen abzudecken. So seien polizeitaktische Angaben - insbesondere die genauen Einsatzzeiten - aus überwiegenden öffentlichen Interessen abzudecken.

8.3 Register der Datensammlungen

Ein Spitalzentrum muss seine Datensammlungen im Register der Datensammlungen erfassen und nachführen. Es erbringt die durch die Spitalliste definierten und ihm übertragenen Leistungen und nimmt somit eine öffentliche Aufgabe wahr. Insoweit ist das Spitalzentrum dem kantonalen Datenschutzgesetz unterworfen und hat seine Datensammlungen anzumelden. Zudem verneint das Verwaltungsgericht eine Teilnahme am wirtschaftlichen Wettbewerb, soweit das Spitalzentrum in Erfüllung der ihm vom Kanton übertragenen Aufgaben handelt. Damit bestätigt das Verwaltungsgericht den Entscheid der Vorinstanz (Gesundheits- und Fürsorgedirektion).

8.4 Vorabkontrollverfahren eines Klinikinformationssystems

Die Aufsichtsstelle führte im Rahmen der Einführung des Klinikinformationssystems eines Spitalzentrums beim Verwaltungsgericht Beschwerde gegen die durch die Gesundheits- und Fürsorgedirektion als Vorinstanz abgewiesenen Punkte. Das Verwaltungsgericht stützte in seinem Urteil den Entscheid der Gesundheits- und Fürsorgedirektion, dass neueintretende Patienten nicht darüber zu informieren sind, dass das Klinikinformationssystem auch Zugriff auf Krankengeschichten derjenigen Spitäler gibt, die vor dem Zusammenschluss zum neuen Spitalzentrum selbständig waren. Auch müssen abteilungsübergreifende Lesezugriffe bei den hier gegebenen Grössenordnungen nicht protokolliert werden. Die von der Vorinstanz vertretene Auffassung, Daten exponierter Patienten (etwa eigener Mitarbeitender) müssten nicht besonders geschützt werden, korrigierte das Verwaltungsgericht.

8.5 Vorabkontrollpflicht für eine Datendrehscheibe

Ersetzt eine psychiatrische Klinik bestehende Schnittstellen zwischen einer Vielzahl von Datenbearbeitungssystemen durch eine Datendrehscheibe (JCAPS), hat sie dies der Aufsichtsstelle zur Vorabkontrolle zu unterbreiten. Aufzuzeigen ist für alle Datenfelder, dass die Datenschutzvorgaben auch nach dem Drehscheibeneinsatz in allen verbundenen Datenbearbeitungssystemen eingehalten werden. Dies hielt die Aufsichtsstelle in einem begründeten Antrag (Aufsichtsrecht) fest.

9 Gemeinderechtliche Körperschaften

Mitteilungen der Datenschutzaufsichtsstelle
Erstmals wandte sich die Aufsichtsstelle im Berichtsjahr zu Fragen von aktuellem und wiederkehrendem Interesse mit Mitteilungen an die Datenschutzaufsichtsstellen der Gemeinden. Die Mitteilungen stehen im Dienst einer effektiven und einheitlichen Umsetzung des Datenschutzrechtes durch die kommunalen Aufsichtsstellen. Sie betrafen die Publikation von nichtständigen Mitgliedern von Abstimmungs- und Wahlausschüssen (April 2013), die Einführung der elektronischen Geschäftsverwaltung GEVER (Juli 2013), unzulässige Daten über die Religionszugehörigkeit in der Einwohnerkontrolle (August 2013, s. 1) und den Einsatz von Microsoft Office 365 an den Schulen (November 2013, s. 6). Die Mitteilungen sind auf der Website der Datenschutzaufsichtsstelle publiziert.

Eine Schulungsveranstaltung für die Aufsichtsstellen der Gemeinden konnte mangels Anmeldungen nicht durchgeführt werden. (Zur vorbildlichen Internetseite der Gemeinde Worb und zum hohen Interesse der Kursteilnehmenden s. 2.2, zur Ablösung der Archivweisung 7.2).

10 Berichtspunkte der Vorjahre

(3: Nachbetreuungen zu den 2012 vorgenommenen Kontrollhandlungen, 5: weitergeführte Vorabkontrollen, 8.3: Register der Datensammlungen, Beschwerden, 8.4: Beschwerdeverfahren im Vorabkontrollverfahren zu einem Klinikinformationssystem, 8.5 Begründete Empfehlung im Vorabkontrollverfahren JCAPS).

11 Antrag

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

24. Januar 2014

Der Datenschutzbeauftragte: *Siegenthaler*

12 Anhang

12.1 Abkürzungen, Bezeichnungen

A: Anhang
Apple: Amerikanisches Unternehmen mit Hauptsitz im kalifornischen Cupertino, das Computer und Unterhaltungselektronik sowie Betriebssysteme und Anwendungssoftware herstellt (nach Wikipedia)
Applikation: Informatikanwendung
BFH: Berner Fachhochschule
BFHCard: Chipunterstützte Multifunktionskarte der BFH, welche als Identifikations- und Zahlungsmittel eingesetzt werden kann
Clinical Trial Unit: Teil des Departments für Klinische Forschung der Universität Bern, führt patientengestützte klinische Studien durch
Case Management Berufsbildung: Informatiklösung um Massnahmen zu koordinieren und um Jugendliche und junge Erwachsene, deren Integration ins Erwerbsleben gefährdet ist, stufenübergreifend zu unterstützen.
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
DHCP: Dynamic Host Configuration Protocol, DHCP-Log-Dateien erlauben es neben anderem, das Verhalten eines Computerbenutzers nachzuverfolgen
EDÖB: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
ePM: elektronische Pensenmeldung von Schulleitungen an das Personalamt
FAQ: Frequently Asked Questions, englisch für häufig gestellte Fragen
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
Google+: Soziales Netzwerk von Google Inc., weltweit zweitgrösste soziale Netzwerk (nach Wikipedia)
iCloud: Von Apple angebotener Cloud-Dienst
ICT: Information and Communication Technology, deutsch: Informations- und Kommunikationstechnologie
i-pdos: Integriertes Patientendossier Inselspital (Klinikinformationssystem)
ISO: Internationale Organisation für Normung
IT: Informationstechnologie
IS-Academia: Studierenden-Administrationssystem
ISDS: Informationssicherheit und Datenschutz
IV: Invalidenversicherung
JCAPS: Java Composite Application Platform Suite: Softwareprodukt, das die Integration verteilter Dienste in der Anwendungslandschaft eines Unternehmens unterstützt (nach Wikipedia).
KAIO: Kantonales Amt für Informatik und Organisation
KIS: Klinikinformationssystem(e)
KSL: Kernsystem Lehre: Informatikprogramm der Universität
Log: Ereignisprotokoll; englisch, automatisch geführtes Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem (nach Wikipedia)
NEF-Ziele: Im Rahmen der neuen Verwaltungsführung für jede Verwaltungseinheit festzulegende Leistungs- und Wirkungsziele (im Voranschlag und Geschäftsbericht des Kantons Bern aufgeführt)
NICER: National Institute for Cancer Epidemiology and Registration: Institution zur Krebsforschung
OboraNew: Erneuerung der elektronischen Rapportierungslösung der Kantonspolizei
OPALE: Patientenverwaltungslösung
OSIV: Open System IV, Informatikanwendung mehrerer IV-Stellen
PACS: Picture Archiving and Communication System: Bildarchivierungs- und Kommunikationssystem in der Medizin
PERSISKA: Personal- und Informationssystem des Kantons Bern
PERSAP: Projekt zur Ablösung des elektronischen Personalverwaltungssystems des Inselspitals
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.
SNB: Spitalnetz Bern AG (Spitäler Aarberg, Münsingen, Riggisberg, Tiefenau und Ziegler, Spital und Altersheim Belp, Pflegezentrum Elfenau)
SPJBB: Psychiatrische Dienste Biel-Seeland – Berner Jura Bellelay
SRO: Spital Region Oberaargau
STS: Spitäler Thun Simmental AG
SZB: Spitalzentrum Biel
tacs: Leistungserfassungssystem für Spitäler
UNICARD: Informatiksystem der Universität Bern zur Ausstellung und Verwaltung der elektronischen Legitimationskarte mit Chip
UPD: Universitäre Psychiatrische Dienste Bern

ViCLAS: Violent Crime Linkage Analysis System: Analyse-System zum Verknüpfen von Gewaltdelikten
WPEV: Wehrpflichtersatzverwaltung
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

12.2 Referenznummern der in Ziffer 8 aufgeführten Aufsichts- und Justizentscheide

8.1: Entscheid der Polizei- und Militärdirektion BD 121/12 vom 2. April 2013
8.2: Entscheid der Polizei- und Militärdirektion BD 158/11 vom 8. April 2013
8.3: Urteil des Verwaltungsgerichts VGE 100.2012.118 vom 4. Februar 2013
8.4: Urteil des Verwaltungsgerichts VGE 100.2012.330 vom 15. August 2013
8.5: Begründeter Antrag der Aufsichtsstelle 42.50-12.5652 vom 17. September 2013

12.3 Internetadressen

2.3: Geschäftsbericht: http://www.fin.be.ch/fin/de/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html
3: HIN-Mail: http://www.hin.ch/
8.3: Register der Datensammlungen: http://www.jgk.be.ch/jgk/de/index/aufsicht/datenschutz/register_der_datensammlungen.html
9: Mitteilungen an kommunale Datenschutzaufsichtsstellen: http://www.jgk.be.ch/jgk/de/index/aufsicht/datenschutz/kommunaler_datenschutz/mitteilungenetc.html