Bericht 2015 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	8
7.	Gesetzgebung	8
8.	Aufsichts- und Justizentscheide	9
9.	Polizei	10
10.	Besonderes	11
11.	Berichtspunkte der Vorjahre	11
12.	Antrag	11
13.	Anhang	12

1 Einleitung

1.1 Auf einen Blick

Die Projekte BE-Print (verwaltungsweit zur Verfügung stehende Druck-, Scan- und Kopierinfrastruktur) und HarmTel (Ablösen der Telefongeräte durch eine in den Informatikarbeitsplatz integrierte Kommunikationslösung) machen es augenfällig: Einzellösungen werden durch integrierte Systeme abgelöst (s. 5).

Die technische Integration der Systeme macht auch das Zusammenspiel von Leistungsbezüger und Leistungserbringer schwieriger. Zu verbessern ist vor allem die Kommunikation, nicht zuletzt bei Systemänderungen wie folgende Beispiele zeigen: Der Informatikdienst einer Direktion schaltete die technischen Massnahmen zum Erzwingen der Passwortvorgaben aus. Das so konfigurierte System übergab er an den Leistungserbringer der Informatikgrundversorgung. Bei den Leistungsbezügern (Anwendungsverantwortlichen), blieb die entstandene schwere Sicherheitslücke während Monaten unbemerkt (s. 10). Ähnliches zeigte die Kontrolle der Anwendung SUSA des Strassenverkehrs- und Schifffahrtsamtes: SUSA wird im Rechenzentrum Bedag im Auftrag betrieben. Die vom Strassenverkehrs- und Schifffahrtsamt sorgfältig nachgeführten Informatiksicherheits- und Datenschutzvorgaben trafen bei der Bedag aber nie ein (s. 3).

Zunehmend werden Daten auch auf mobilen Geräten wie Smartphones und Tabletts bearbeitet.

Die Prüfung des Managementsystems der mobilen Geräte (MDM) der Kantonspolizei hat gezeigt, dass ein angemessener Datenschutz auf diesen Geräten – etwa das Löschen der Daten nach einem Geräteverlust – unerlässlich ist. Andererseits kann die mit dem Managementsystem ermöglichte Kontrolle der mobilen Geräte auch zu einem unzulässigen Überwachen der Mitarbeitenden führen (s. 9.2).

Die Aufsichtsstelle hat die Aufgabe, das Grundrecht auf Datenschutz auch in dieser veränderten informatiktechnischen Umgebung einzufordern. Die Risikosituation ist neu zu beurteilen. Ein datenschutzkonformer Umgang mit den Daten der Bürgerinnen und Bürger ist zu sichern. Die technologischen Entwicklungen hin zu immer mehr Digitalisierung und Integration sind in diesem Sinne aktiv zu nutzen. Es braucht eine enge Zusammenarbeit mit den Projektauftraggebern, etwa um sichere Lösungen auch benutzerfreundlich auszugestalten. Gerade in den Vorabkontrollen von Informatikprojekten ist die Datenschutzaufsichtsstelle gefordert. Hier müssen die Sicherheits- und Datenschutzanforderungen rechtzeitig definiert und berücksichtigt werden.

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). 2015 fanden zwei Arbeitssitzungen, davon eine mit einem Besuch beim fedpol, statt.

- Die Beratungs- und Rehabilitationsstelle für Sehbehinderte und Blinde des Kantons Bern (BRSB) erfüllt eine vom Kanton und vom Bund finanzierte (Verbund-)Aufgabe. Ein Meinungsaustausch zeigte, dass die Datenschutzaufsicht dem EDÖB obliegt (s. zur Zuständigkeit für die IV-Stelle 8.2).
- Mitarbeitende der Aufsichtsstelle wirkten in den PRIVATIM-Arbeitsgruppen ‚Information and Communication Technology' (ICT) und ‚Gesundheit' mit. Letztere hat bei den kantonalen Gesundheitsbehörden eine Erhebung über die Rechnungskontrolle bei stationär erbrachten Leistungen durchgeführt (obligatorische Krankenpflegeversicherung; s. 13.3; sowie zur Patientenbroschüre s. 6).
- Zum Thema „Einführung in die Informatik(sicherheit) für Juristen" führte PRIVATIM einen eintägigen Kurs durch, welcher von Mitarbeitenden der Aufsichtsstelle besucht wurde.

1.3 Umsetzung der Schengen–Evaluation

Die Kommentare und Hinweise des Expertengremiums der Schengen-Vertragsstaaten, das 2014 den Kanton Bern überprüfte, wurden wie folgt umgesetzt:

- Die im Datenschutzgesetz verankerte Unabhängigkeit der Aufsichtsstelle zur Budgetierung wurde beim Ausarbeiten des Voranschlags 2016 respektiert: So verzichtete der Regierungsrat beispielsweise darauf, die im Voranschlag beantragte Stellenschaffung zu kommentieren.
- Die Geschäftsprüfungskommission des Grossen Rates unterstrich in ihren Gesprächen mit dem Datenschutzbeauftragten, dass auch sie die Unabhängigkeit der Aufsichtsstelle dahin versteht, dass kein Einfluss auf Entscheide erfolgen darf.
- Die Abrufe der Kantonspolizei im SIS wurden 2015 kontrolliert. Entsprechende Kontrollen sollen in Zukunft jährlich erfolgen. Die durchgeführte Kontrolle erfolgte durch das Polizeikommando in Zusammenarbeit mit der Aufsichtsstelle ohne den Beizug externer Prüfer. Um einer ungenügenden Selbstkontrolle entgegenzuwirken, wirkte die Aufsichtsstelle bei wichtigen Kontrollschritten unmittelbar mit, etwa beim Festlegen der Stichprobe der zu überprüfenden Abrufe.

- Die Schengener Koordinationsgruppe des EDÖB wurde über das Anliegen, für den Einsatz externer Kontrolleure eine eigene gesetzliche Grundlage zu schaffen und die Unabhängigkeit der Kontrolleure gegenüber der kontrollierten Stelle zu garantieren, informiert (s. 1.2).
- Der Grosse Rat bewilligte die Erhöhung des Personalbestandes der Aufsichtsstelle (s. 2.3).
- Auf der Internetseite der Aufsichtsstelle wurden Informationen über die Rechtsgrundlagen des SIS und Musterschreiben zur Ausübung des Auskunfts- und Berichtigungsrechts aufgeschaltet.

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, ist anhand folgender Kriterien zu entscheiden:

– Vorschalten der zuständigen Stelle: Die Beratung kommunaler und kantonaler Verwaltungsstellen hat durch die zuständigen kommunalen Datenschutzaufsichtsstellen bzw. Rechtsdienste/Kontaktstellen der kantonalen Verwaltung zu erfolgen. Betroffene Personen 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 sind 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 Personen 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 von der Aufsichtsstelle mit den entsprechenden Mitteln (z. B. Kontrollen) nachzugehen.

– Vorabkontrollen: Die Vorabkontrollvorgaben wollen die Projektleitungen zum Umsetzen 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

Vermehrt erhält die Aufsichtsstelle Anfragen für Referate. Vor Schulsozialarbeitenden hielt sie im Tandem mit dem Amt für Gemeinden und Raumordnung (AGR) einen Kurzvortrag zu den Grundprinzipien des Datenschutzrechts und den Aufbewahrungsvorschriften.
- Die Verantwortliche für den Datenschutz des Inselspitals hat gemeinsam mit einer Juristin des Rechtsdienstes in sämtlichen Kliniken (ca. 40) einen kurzen Datenschutzrundgang durchgeführt. Ziel des Rundganges war es den Mitarbeitenden die Kontaktpersonen für Fragen zum Thema Datenschutz bekanntzumachen, konkrete Verbesserungsvorschläge anzubringen und Informationsbroschüren zu verteilen.

2.3 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Berichtsjahr waren für die kantonale Verwaltung 32 Millionen CHF in Informatikmittel zu investieren. 160 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 190'000 zur Verfügung (s. 3).

Sie verfügte 2015 über 4.7 Vollstellen (davon 0.7 für das Sekretariat). Mit der digitalen Geschäftsverwaltung wurde bereits im Vorjahr auf die Wiederbesetzung einer 50%-Sekretariatsstelle verzichtet. Von August bis Dezember konnte mit den freistehenden Ressourcen eine 30%-Stelle einer wissenschaftlichen Mitarbeiterin besetzt werden. Zum Einarbeiten der neuen Sekretariatsmitarbeiterin (10%-Stelle) war das Sekretariat im Dezember doppelt besetzt (zusätzlich zur bisherigen 20%-Stelle). Mit dem Budget 2016 bewilligte der Grosse Rat eine neue 100%-Stelle (wissenschaftliche Mitarbeiterin). Auf diese Stelle sind die freigewordenen 55 Stellenprozente anzurechnen. Für 2016 verfügt die Aufsichtsstelle damit über insgesamt 5.15 Vollstellen. Der Grosse Rat beschloss über das gesamte staatliche Budget eine lineare Kürzung des Sachaufwandes. Der für die Prüfung von Informatikanwendungen durch externe Prüfstellen zur Verfügung stehende Betrag verringert sich dadurch um CHF 14'000. Weitere Angaben zu Budget, Rechnung, Erreichen der NEF-Ziele (Finanzzahlen) finden sich im Geschäftsbericht 2015 des Kantons Bern (Band I, s. 13.3).

3 Kontrollen von Informatikanwendungen, die im Betrieb stehen

Es wurden zwei (Doppel-)Prüfungen durchgeführt:

- Asylsozialhilfestelle Biel (ABR) und Migrationsdienst (MIDI):

Die beiden Prüfungen wurden auf die Kontrolle der Datenflüsse zwischen dem MIDI und der Asylsozialhilfestelle ABR fokussiert.
Die von der beigezogenen externen Prüfstelle zuerst durchgeführte Kontrolle bei ABR zeigte im Bereich des Datenschutzes wie auch der Informationssicherheit erhebliche Mängel. Technisch sind die Massnahmen zum Grundschutz und zum erhöhten Schutz in vielen Bereichen nicht umgesetzt. Besonders schützenswerte Daten werden mit Partnerinstitutionen weitgehend ohne die vorgegebenen Schutzmassnahmen ausgetauscht (s. auch 8.1). Organisatorisch fehlen klare Vorgaben und Richtlinien (Klassifizierung, Löschung, Archivierung). Damit fehlen auch die Rahmenbedingungen um Outsourcingpartner mit präzisen Verträgen genügend einzubinden.
Der MIDI bearbeitet seine Daten (Abrechnungen mit den Bundesstellen) u.a. mit der Applikation Asydata. Die im Jahr 2000 in Betrieb genommene Applikation genügt den heutigen ISDS-Anforderungen nicht. Da elementare Sicherheitsanforderungen nicht eingehalten werden, besteht dringender Handlungsbedarf. Die Applikation steuert einen geschäftskritischen Prozess. Im aktuellen Stand stellt sie für den MIDI ein erhebliches Risiko dar.

- Applikation SUSA des Strassenverkehrs- und Schifffahrtsamts (mit Applikationsbetrieb in der Bedag):

Diese Kontrolle wurde erstmals gemeinsam mit der Finanzkontrolle des Kantons Bern durchgeführt. Die beigezogene externe Prüfstelle hatte

den Auftrag, das Outsourcing des Betriebes einer Informatikanwendung im Rechenzentrum Bedag zu prüfen. (Wie werden die ISDS-Anforderungen des Auftraggebers und Dateneigentümers an den Outsourcingpartner übergeben und wie wird kontrolliert, ob sie eingehalten werden).
Die Verantwortlichen der Bedag unterstützten die Auditoren in konstruktiver Art und legten den Betrieb der Applikation SUSA im Detail offen. Dabei wurde festgestellt, dass technisch beim Grundschutz ein sehr guter Standard erreicht ist. Die Bedag betreibt ihre Anlagen nach eigenen Vorgaben, angelehnt an den Standard ISO 2700x. Die Prüfung der Maturität und Nachhaltigkeit der umgesetzten Massnahmen baut die Bedag noch auf.
Bei der vertraglichen Überbindung der ISDS-Anforderungen und Kontrolle der definierten Sicherheitsanforderungen durch den Auftraggeber ist die aktuelle Situation unbefriedigend. Wohl besteht ein ISDS-Konzept für die Applikation SUSA, das die Sicherheitsanforderungen beschreibt. Der Bedag wurde es jedoch nicht kommuniziert. Dies obwohl das bestehende Vertragswerk dies vorgibt.

- Nachbetreuungen früherer Kontrollen:
    - Audit der mobilen Infrastruktur (Smartphone) der Kantonspolizei:

(S. 9.2).

    - Spital Thun STS AG

Als Folge der Kontrolle des Klinikinformationssystems wurden Informationssicherheit und Datenschutz in das unternehmensweite Risikomanagementsystem aufgenommen. Die Geschäftsleitung stellte Ressourcen für Informationssicherheit und Datenschutz bereit und überarbeitete und optimierte die Prozesse. Das Audit ist abgeschlossen.

    - Spitalzentrum Biel SZB/CHB

Die noch offenen Pendenzen sollen bis Mitte 2016 erlediget werden.

4 Videoüberwachung

Mehrere Videoüberwachungsanlagen für kantonale Gebäude wurden im Vorabkontrollverfahren geprüft, darunter die Anlagen der Anstalten Thorberg, des Hochschulzentrums VonRoll der Universität Bern und der Gymnasien Biel-Seeland.

- Die Besichtigungen vor Ort führen oft zu Anpassungen der Bewilligungsgesuche an das Polizeikommando. So werden nicht eindeutig bewilligungsfähige Kameras gestrichen und die Unterlagen wo nötig mit Massnahmen zur Wahrung des Datenschutzes ergänzt. Beim Hochschulzentrum wurde u.a. auf die Arealkameras verzichtet und bei den Anstalten Thorberg auf Kameras in Besucherräumen. Für die Anstalten des Amtes für Freiheitsentzug und Betreuung sorgen neu eine „Weisung“ zur Benutzung der Kameras in Sicherheitszellen und ein „Merkblatt“ für Videoüberwachungen in Anstalten für die Wahrung der Verhältnismässigkeit im Umgang mit den Überwachungskameras. In Biel (Gymnasium) wurden die Unterlagen mit Bestimmungen über das Protokollieren der technischen Prüfung von Videoaufnahmen ergänzt.

- Das Tiefbauamt (TBA) unterbreitete der Aufsichtsstelle Fragen zu Webcams auf Grossbaustellen. Sobald Webcams eine Personenidentifikation ermöglichen, sind sie bewilligungspflichtige Kameras. Das ist der Fall, wenn Bilder der Webcams aus dem Internet abgerufen, gestoppt und vergrössert werden können und Fahrzeugnummern oder Personen erkennbar oder aus den Umständen bestimmbar werden. Das TBA hat die Bedenken und Verbesserungsvorschläge der Aufsichtsstelle berücksichtigt.

- Wiederholt fragten Gemeinden an, wie sie gegen Kameras von Privatpersonen vorgehen können, die im öffentlichen Raum Bilder aufnehmen. Zwar sind unbewilligte Videoüberwachungen im öffentlichen Raum durch Private unzulässig. Da jedoch Rechtsgrundlagen fehlen, muss eine Lösung im Gespräch, allenfalls unterstützt von einer Strafandrohung, und mit den Mitteln des eidgenössischen Datenschutzgesetzes (zivilrechtliche Klagen, Einschalten des EDÖB) gesucht werden.

- Die Polizei-und Militärdirektion (POM) publizierte die von ihren Ämtern verfassten Evaluationsberichte zu Videoüberwachungsanlagen, unter anderem auch denjenigen des Polizeikommandos (s. 13.3).

- (Zur Verhältnismässigkeit von Videoaufzeichnungen durch Institutionen, deren Mitarbeitende dem Berufsgeheimnis unterstehen: s. 8.4).

5 Vorabkontrollen von Informatikprojekten

Die Aufsichtsstelle befasste sich mit einer hohen Anzahl von Informatikprojekten, zahlreiche aus dem Gesundheitswesen, insbesondere Klinikinformationssysteme (KIS). Die nachfolgend aufgeführten Beispiele sind nicht abschliessend:

- Beim Klinikinformationssystem des Inselspitals (i-pdos) hat die Aufsichtsstelle das eingereichte Archivierungs- und Löschkonzept geprüft. Sie hat festgehalten, dass es im Sinne einer Minimallösung ausreichend ist, wenn jeder medizinische Fall nach einer festgelegten Dauer gelöscht wird. Einzuhalten sind die gesetzlichen Mindestaufbewahrungsfristen. Es liegt im Beur-

teilungsspielraum der verantwortlichen Gesundheitsfachpersonen, auf ein Verlängern der Aufbewahrungsfristen bei Fällen mit medizinischem Zusammenhang zu verzichten. Die Aufsichtsstelle ist jedoch der Ansicht, dass bei einem medizinischen Zusammenhang ein Verlängern der Aufbewahrungsfrist des vorbestehenden medizinischen Falles erfolgen soll — es sei denn, die benötigten Informationen des vorbestehenden Falles finden anderweitig im neuen Fall Eingang. Das medizinische Fachwissen sowie die entsprechende Verantwortung liegen jedoch nicht bei ihr. Die Feldstechersuche bei aktiven und abgeschlossenen Behandlungsfällen muss noch datenschutzkonform umgesetzt werden. Die Vorabkontrolle wurde damit abgeschlossen.

- Im Rahmen der Vorabkontrolle der Applikation MC-SIS (Mammografie-Screening-Programm des Kantons Bern, welches durch die Bernische Krebsliga durchgeführt wird) wurden die überarbeiteten ISDS-Unterlagen eingereicht. Diese ermöglichten es der Aufsichtsstelle, eine abschliessende Stellungnahme abzugeben und die Vorabkontrolle abzuschliessen.

- Beim Klinikinformationssystem der Berner Klinik Montana bestanden noch mehrere offene Punkte zur Informationssicherheit. Diese konnten mit den nachgebesserten ISDS-Unterlagen geklärt und die Vorabkontrolle abgeschlossen werden.

- Zum Klinikinformationssystem Cariatides der Psychiatrischen Dienste Biel-Seeland – Berner Jura (PDBBJ) hat die Aufsichtsstelle eine zweite Stellungnahme abgegeben. Da die Ausgestaltung der Zugriffsrechte komplex ist, war zusätzlich eine Demonstration vor Ort nötig. Diese hat gezeigt, dass es aus Verhältnismässigkeitsgründen noch einiger Änderungen bedarf. Diese sollten vorgenommen und in den überarbeiteten ISDS-Unterlagen dargelegt werden. Die vereinbarte Frist sowie die gewährte Nachfrist wurden von den PDBBJ bis Ende Berichtsjahr nicht eingehalten.

- Zwischen der Aufsichtsstelle und den Universitären Psychiatrischen Diensten Bern (UPD) fanden mehrerer Besprechungen zu den noch offenen Punkten ihres Klinikinformationssystems statt, insbesondere zur auftragsgesteuerten Berechtigungsvergabe bei den Querschnittsfunktionen, zur Rollen- und Berechtigungsmatrix sowie zur Patientensuche. Weiter erfolgte eine Demonstration der konkreten Ausgestaltung der Zugriffsrechte vor Ort. Die Aufsichtsstelle erwartet Anfang 2016 weitere schriftliche Erläuterungen und wird anschliessend eine weitere Stellungnahme abgeben können.

- Bei der Vorabkontrolle des Laborinformationssystems (LIS) des Psychiatriezentrums Münsingen (PZM) waren noch wenige Punkte des Grundschutzes offen. Diese konnten geklärt und die Vorabkontrolle abgeschlossen werden.

- Die Prüfung der ISDS-Unterlagen zur Applikation Acuraid zur Forschung im Bereich der Akupunktur des Instituts für Komplementärmedizin der Universität Bern führte zum Schluss, dass die Applikation nicht datenschutzkonform betrieben werden kann und somit nicht in Betrieb genommen werden darf.

- Zum Klinikinformationssystem der Regionalspital Emmental AG (RSE AG) erfolgte ein intensiver Austausch über die Benutzerberechtigungen. Es musste – wie bei Vorabkontrollen generell – geprüft werden, ob mit der Organisation der RSE AG bzw. der aktuellen Einstellung der Berechtigungen im KIS die datenschutzrechtlichen Spielräume lediglich ausgeschöpft oder überschritten werden. Die Aufsichtsstelle forderte in ihrer ersten Stellungnahme unter anderem eine eingeschränktere Suchfunktion und die erschwerte Suchabfrage für VIP-Patienten. Zudem muss ein Katalog mit spezifischen Fragen, welche sich aus der Durchsicht der Berechtigungsmatrix ergeben haben, beantwortet werden.

- Die Aufsichtsstelle ist im Verzug mit der Prüfung der verlangten Nachbesserungen für das Klinikinformationssystem der Spitäler Frutigen, Meiringen, Interlaken (fmi ag). Sie wird u.a. kontrollieren, ob die Anzeige der Psychiatriepatienten via Suchfunktion nun ausschliesslich den Psychiaterinnen und Psychiatern möglich ist.

- Nach zwei Stellungnahmen der Aufsichtsstelle zum Klinikinformationssystem des PZM sind nur noch zwei Punkte offen: Zum Aufbewahrungs- und Löschkonzept liegt eine Stellungnahme des Softwareherstellers zur Durchsicht vor, die geforderte Ergänzung des ISDS-Konzepts zur Datendrehscheibe (welche Daten fliessen über diese in das KIS und vom KIS weg, Schnittstellenspezifikation) ist hingegen noch ausstehend.

- Aufgrund eines personellen Wechsels innerhalb des Spitals Region Oberaargau (sro ag) und wegen des Ersatzes der Klinikinformationssoftware durch ein anderes Produkt kam es zu Verzögerungen in der Vorabkontrolle. Die eingereichten Überarbeitungen sind für eine weitere Überprüfung durch die Aufsichtsstelle noch unvollständig. So fehlen die Ausführungen zur (bemängelten) Informationssicherheit vollumfänglich.

- Zum Labor-Informationssystem des Instituts für Infektionskrankheiten (IFIK) der Universität Bern nahm die Aufsichtsstelle zwei Mal Stellung. Sie regte an, eine Forschungsdatenbank

mit pseudonymisierten Daten für das IFIK einzurichten und den Forschenden einen Zugriff nur auf diese Datenbank zu gewähren. Weiter noch offen ist u.a. die detaillierte Beschreibung des Zugriffsmanagements.

- Die Vorabkontrolle Case Management Berufsbildung konnte mit zwei Bemerkungen abgeschlossen werden: Mutationslogs sind hauptdatengebunden und müssen so lange aufbewahrt werden, wie die Hauptdaten. Leseprotokollierungen müssen hingegen zwingend nach einem Jahr gelöscht werden. Zudem muss die verantwortliche Behörde dafür sorgen, dass die AGB ISDS unterzeichnet und eingehalten werden.

- Zum Kernsystem Lehre (KSL) der Universität Bern erfolgte eine weitere Stellungnahme der Aufsichtsstelle. Das Benutzerberechtigungskonzept wurde auf die Grundsätze der Rechtevergabe geprüft und einzelne Rollen per Stichprobe kontrolliert. Die ISDS-Dokumentation zur Archivierung und Löschung muss von der Universität noch eingereicht bzw. präzisiert werden.

- Für UNICARD fehlt die Umsetzungsbestätigung der Archivierung.

- Nach der Prüfung des sorgfältig ausgearbeiteten und differenzierten Archivierungs- und Löschkonzept des Studierenden-Administrationssystems IS-Academia der Berner Fachhochschule (BFH) konnte die Vorabkontrolle abgeschlossen werden.

- Im Rahmen der Vorabkontrolle des Finanzinformationssystems ESAP der BFH und der Pädagogischen Hochschule Bern (PHBern) erfolgte eine erste Stellungnahme. Die Aufsichtsstelle legte den Fokus dabei auf die datenschutzrechtlich heiklen Personaldatenbearbeitungen.

- Nach mehreren Fristverlängerungsgesuchen legte das Alters- und Behindertenamt (ALBA) der Aufsichtsstelle dar, weshalb die mit der Software zur Prüfung und Auszahlung von individuellen Leistungen (ZERO) geführten Daten gesamtheitlich aufbewahrt werden müssen und nicht rollend vernichtet werden können und stellte zwei datenschutzkonforme Löschvarianten vor. Die Vorabkontrolle konnte damit abgeschlossen werden.

- Für das neue Webanalyse-Tool „Adobe Analytics“ musste der Outsourcing-Vertrag geprüft werden. Der Vertrag regelt die nötigen datenschutzrechtlichen Vorgaben mit dem ausländischen Anbieter (wie die Geltung des schweizerischen bzw. kantonalen Datenschutzrechts und Gerichtsstands und die Auditmöglichkeiten). Die Datenschutzerklärung der kantonalen Website wurde unter „Rechtliches“ angepasst. Sie nennt die Daten, die bei einem Aufruf der Website anonym ausgewertet werden. Die Website gibt neu die Möglichkeit das Tracking zu deaktivieren (Opt-Out).

- Die Software-Lösung von ServiceNow soll der Abwicklung von Störungsmeldungen und Anliegen von IT-Benutzenden im täglichen Betrieb der IT-Infrastruktur des Kantons dienen. Die Applikation wird in den Rechnungszentren der Lieferfirma betrieben. Die Übertragung der Daten und Authentifizierungsmerkmale erfolgt verschlüsselt. Die Überprüfung der Aufsichtsstelle führte zur nötigen Abgrenzung, wozu ServiceNow nicht benutzt werden darf. Mit einem besonderen Prozess wird dafür gesorgt, dass keine besonders schützenswerten Daten oder Daten, für die eine besondere Geheimhaltungspflicht besteht, bearbeitet werden. Weil der Service von einem ausländischen Anbieter angeboten wird (amerikanisches Unternehmen mit Unternehmenssitz in Europa), war der Vertrag mit ServiceNow Netherlands besonders zu prüfen. Da ServiceNow ein U.S.-Swiss Safe Harbor zertifiziertes Unternehmen ist, stützt sich der Vertrag auf den Mustervertrag des EDÖB für Outsourcing-Verträge mit ausländischen Unternehmen. Für die Überprüfung war zudem der neue Entscheid des Europäischen Gerichtshofs zu berücksichtigen. Demnach bietet das Safe Harbor Abkommen keinen Schutz vor unverhältnismässigen US-Behördenzugriffen und erfüllt damit die Anforderungen an das „angemessene Datenschutzniveau“ der EU nicht. Der EDÖB kam zum Schluss, dass dies auch für das U.S.-Swiss Safe Harbor Framework und das schweizerische Datenschutzniveau gelte. Bis die Lage durch die EU geklärt ist und neue Datenschutzgarantien mit den USA vereinbart werden können, sollen sich die Vertragsparteien dazu verpflichten, betroffene Personen über mögliche US-Zugriffe zu informieren, ihnen wirksame Rechtsbehelfe einzuräumen und Urteile zu akzeptieren. Der Vertrag mit ServiceNow Netherlands verpflichtet ServiceNow u.a. zu einer umfassenden Geheimhaltung. Die Daten dürfen ausschliesslich in den schweizerischen Rechenzentren bearbeitet werden. Anwendbar ist schweizerisches Recht und es besteht ein schweizerischer Gerichtsstand. Mit den vertraglichen Sicherheiten kann der Service für „nicht heikle“ Daten datenschutzkonform betrieben werden.

- Die Software FTAPIs, der deutschen QSC AG, bietet eine Datenaustausch-Plattform mit einer besonders gesicherten Ende-zu-Ende-Verschlüsselung an. Die Plattform kann von der Bedag betrieben werden. Sie soll den Mitarbeitenden sowie den von ihnen eingeladenen „Gästen“ am Arbeitsplatz (PC) oder unterwegs auf mobilen Endgeräten zur Verfügung stehen. Die Prüfung der Aufsichtsstelle ergab, dass diese Plattform zurzeit nur von stationären Clients

(PCs) genutzt werden dürfte. Dafür muss die besondere Verschlüsselungslösung als sicher anerkannt werden und es muss mit technischen Mitteln möglich sein, den Gebrauch mobiler Endgeräte auszuschliessen. Für die mobilen Endgeräte (wie Smartphones, Tablets, Laptops, Netbooks etc.) kann die Plattform noch nicht eingesetzt werden. Die technischen Vorkehrungen zum Schutz der sensiblen Daten, insbesondere zur Trennung von privaten und beruflichen Daten, fehlen.

- Beim verwaltungsweiten Druckservice BE-Print hat die Aufsichtsstelle bereits frühzeitig davon abgeraten, im ISDS-Konzept ein reines Infrastrukturprojekt zu beschreiben und auf den Ersatz der bestehenden Drucker zu fokussieren. Zur Verfügung gestellt wird ein neuer Service, der sehr viel mehr beinhaltet als nur das Drucken. Funktionen wie Follow-me-Printing, Scan-to-mail, scan-to-folder etc. erfordern eine breite Palette von technischen Modulen und organisatorischen Vorkehrungen, die aufeinander abgestimmt sein müssen. Das System wird komplexer und somit steigen auch die Risiken. Die Verfügbarkeit ist nicht mehr von einem Endgerät abhängig sondern von einer Funktionskette, in der jedes Glied funktionieren muss: Anmeldung – Berechtigung – Transport – Verarbeitung – Ausgabe. Dadurch dass die einzelnen Module (Server, Netzwerke, Anmeldesystem) von verschiedenen Stellen und Dienstleistern betreut werden, wird die Komplexität zusätzlich erhöht (s.1.1).
Bei den Print- und Scan-Funktionen kommt hinzu, dass Anmeldedaten am Multifunktionsgerät eingegeben werden müssen, wo der Komfort einer gewohnten Tastatur weitgehend fehlt. Ein korrektes Passwort manuell einzugeben wird damit benutzerunfreundlich. Da beim Scannen auch besonders schützenswerte Daten übertragen werden, ist ab Scanner eine Verschlüsselung der Daten vorzusehen.
Ein ISDS-Konzept für den Fax-Betrieb wird das KAIO erst noch einreichen.

- Auch beim Projekt zur Harmonisierung der Telefonie (HarmTel) handelt es sich, wie bei BE-Print, nicht um eine Ersatzbeschaffung für Telefone, sondern um eine komplexe Investition in die modernen Kommunikationsmöglichkeiten. Mit dem Umstellen der analogen Systeme auf digitale Systeme (Voice over IP) wird die Telefonie-Infrastruktur in die digitale Datenwelt integriert. Dies bedeutet, dass nun mehrere Systeme und damit auch mehrere Datenquellen miteinander eine neue Kommunikationsplattform bilden (Collaboration). Das herkömmliche Telefon wird zum Endgerät und gewährt Zugriff auf alle Daten, die für einen Benutzer freigeschaltet sind, und zwar nicht nur auf eigene, sondern auch auf freigegebene Daten anderer Mitarbeitender. Es brauchte einige Arbeitszyklen und Zugeständnisse aus dem Projekt, bis dieses von der Aufsichtsstelle als datenschutzkonform beurteilt werden konnte. Diese Beurteilung ist allerdings an klare Bedingungen geknüpft: Bei den mobilen Geräten ist nur die Ablösung der DECT-Geräte zulässig, alle anderen Systeme sind nicht erlaubt. Ein Zugriff von mobilen Geräten ist untersagt, bis diese über ein Verwaltungssystem (EMM) geschützt sind und den Datenschutzanforderungen genügen (laufendes Projekt zur Verwaltung der mobilen Endgeräte). Um einen Anruf über die Microsoft-Lync/Skype-Plattform (Basis von HarmTel) anzunehmen, muss das Gerät entsperrt sein. Dies entspricht nicht den Vorgaben des Grundschutzes. Wird jedoch ein nach der Passwortweisung ordnungsgemässes Passwort (8 Zeichen, Sonderzeichen, Gross-/Kleinbuchstaben) eingerichtet, so ist die Eingabe zur Freischaltung zu umständlich. Die Lösung dieses Problems ist noch offen. Sicherzustellen war ausserdem, dass die Präsenzstatusanzeige nicht zu einer Mitarbeiterüberwachung führt: Die Mitarbeitenden können zum einen die Statusanzeige selbst steuern, sodann sollen in der Personalverordnung Vorgaben für die Vorgesetzten zum Umgang mit diesem Instrument verankert werden. Telefonie-Randdaten (wer hat wann, wie lange, mit wem kommuniziert) stehen nach der Einführung von HarmTel zwar unter der Verfügungsmacht, nicht aber unter der Datenherrschaft des KAIO. Verlangt – etwa die Staatsanwaltschaft – solche Randdaten, dann hat nicht das KAIO sondern der Datenherr zu bestimmen, ob eine solche Herausgabe erfolgen soll. Das KAIO hat dies nicht nur gegenüber anderen Direktionen sondern insbesondere auch gegenüber dem Grossen Rat und den Gerichten zu respektieren. Randdaten sind höchstens während zehn Tagen aufzubewahren (s. 1.1).

- Die Software BVM-Tool unterstützt die IV-Stelle bei der Bekämpfung des Versicherungsmissbrauchs. Entsprechend dem Zweck werden sehr sensible Daten darin verwaltet. Die Erfahrungen aus früheren Kontrollen und die gute Zusammenarbeit zwischen IV-Stelle und Aufsichtsstelle haben wesentlich zu einer effizienten Vorabkontrolle beigetragen.

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).

6 Ansichtsäusserungen, Praxis

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

- Patienten stehen zahlreiche Datenschutzrechte zu. Ihr Recht auf Einsicht in das Patientendossier sowie das Recht auf Kopien ist dabei das Wichtigste. Weiter können sie grundsätzlich bestimmen, wer welche Inhalte aus dem Patientendossier erfahren darf. Die Aufsichtsstelle hat im Berichtsjahr eine Broschüre zu diesem Thema herausgegeben. Diese basiert auf Grundlagen von PRIVATIM (s. 1.2).

- Die Aufsichtsstelle hat festgestellt, dass die komplexen Wechselwirkungen von (vermehrt eingesetzten) Datendrehscheiben zu wenig beachtet werden. Sie hielt fest, dass die entsprechenden Prozesse (Datenflüsse) für alle über eine Datendrehscheibe verbundenen Systeme in der Vorabkontrolldokumentation festgehalten sein müssen, um die Datenintegrität sicher zu stellen.

- Auskünfte am Telefon oder am Empfang eines Spitals an Behörden sind heikel, da mit der Antwort auch die Mitteilung einhergeht, dass sich eine Person zurzeit in Behandlung befindet. Diese Information untersteht der Schweigepflicht und ist auch strafrechtlich geschützt. Gesundheitsfachpersonen und ihre Hilfspersonen (z.B. Personen am Empfang) dürfen solche Auskünfte nur erteilen, wenn eine ausdrückliche gesetzliche Grundlage dafür besteht oder wenn entweder die Einwilligung der betroffenen Person oder eine Entbindung vom Berufsgeheimnis vom Kantonsarztamt vorliegt. Die Aufsichtsstelle hält jedoch eine Ausnahme für reine Kontaktaufnahmen mit den Patienten für datenschutzrechtlich vertretbar, wenn folgende drei Voraussetzungen gesamthaft gegeben sind: 1. Die anfragende Behörde hat sichere Kenntnis vom Klinikaufenthalt des Patienten. 2. Der Patient hat keine andere Anordnung getroffen. 3. Es werden lediglich Auskünfte verlangt, die es der Behörde erlauben, mit dem Patienten Kontakt aufzunehmen während der Patient vor Ort ist.

- Da die Kirchgemeinden über keine Einwohnerkontrollen verfügen, ist das Musterdatenschutzreglement des AGR im Bereich der Listenauskünfte nicht auf sie übertragbar. Kirchgemeinden führen Mitgliederdaten, die als Daten über die Religionsangehörigkeit zu den besonders schützenwerten Daten gehören. Listenauskünfte zu besonders schützenswerten Daten sind an Private weder nach der Datenschutz- noch nach der Informationsgesetzgebung zulässig.

- Wann müssen Kirchenaustrittsschreiben vernichtet werden? Der Austritt aus einer Landeskirche ist in der Kirchengesetzgebung geregelt. Die gesetzlich verlangte schriftliche Austrittserklärung wird von der Archivgesetzgebung nicht als archivwürdig eingestuft. Sie ist deshalb nur so lange aufzubewahren als dies zu Beweiszwecken für Steuerforderungen der Kirchgemeinden nötig ist. Die maximal zulässige Frist hat sich an der Rechtskraft der Kirchensteuerveranlagung im Einzelfall zu orientieren und beträgt maximal 3 Jahre. Spätestens nach Eintritt der Rechtskraft der Veranlagung wird die Austrittserklärung nicht mehr benötigt und ist zu vernichten.

- Darf das Evaluations-Tool des US-amerikanischen Unternehmens SurveyMonkey eingesetzt werden? Mit der Zustimmung zur Datenschutzrichtlinie des Unternehmens erklären sich die Nutzenden des Tools damit einverstanden, dass die erhobenen Daten auch zu Datenverarbeitern in Länder weitergeleitet werden können, die das europäische bzw. schweizerische Datenschutzniveau nicht erfüllen. Und weiter, dass SurveyMonkey die Datenschutzrichtlinie jederzeit einseitig ändern darf. Beides widerspricht den Anforderungen des Datenschutzgesetzes. Datenbearbeitungen in solchen Ländern sind nur zulässig, wenn ein angemessenes Datenschutzniveau vertraglich sichergestellt werden kann. Ein solcher Vertrag kann mit SurveyMonkey offensichtlich nicht abgeschlossen werden. Die Nutzung des Tools ist deshalb nicht zulässig.

- Bewerbungsunterlagen enthalten besonders schützenswerte Daten. Solche Daten müssen verschlüsselt übertragen werden. Das ist mit der Standardlösung myCareer nicht möglich. Der Kanton muss aber eine sichere Übertragung bzw. ein sicheres Datenkommunikationsnetz zur Verfügung stellen. Deshalb darf er myCareer nicht einsetzen und muss eine andere Lösung suchen.

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). Für die Vernehmlassung zur Totalrevision des Bundesgesetzes über genetische Untersuchungen beim Menschen (GUMG) übermittelte die Aufsichtsstelle die Stellungnahme von PRIVATIM.

7.2 Kantonale Erlasse

Mit der Revision des Arbeitsmarktgesetzes wurde die nötige kantonale gesetzliche Grundlage für den Datenaustausch in der Interinstitutionel-

len Zusammenarbeit (IIZ) auf der Grundlage des Arbeitslosenversicherungsrechts des Bundes und für eine elektronische Plattform geschaffen. Da verschiedene, voneinander unabhängige Institutionen im Rahmen der IIZ auf diese Daten zugreifen, handelt es sich um ein Abrufverfahren, für das eine formell-gesetzliche Grundlage nötig ist. Sämtliche Hinweise der Aufsichtsstelle waren berücksichtigt worden. Der Regierungsrat ist verpflichtet, die konkreten datenschutzrechtlichen Anforderungen an die Datenbearbeitung und den Datenaustausch in einer Verordnung zu regeln. Die Plattform unterliegt als Informatikprojekt der Vorabkontrolle.

- In der Praxis hat sich gezeigt, dass vielfach unklar ist, was mit Anonymisierung gemeint ist. Die Aufsichtsstelle hat deshalb bei der Änderung des Sozialhilfegesetzes angeregt, im Vortrag eine Definition einzufügen.

- Mit der 6. Revision der Verordnung über die Harmonisierung amtlicher Register (RegV) haben neben den Steuerbehörden des Kantons und der Gemeinden noch zehn Ämter mit steuerrechtlichen Aufgaben (bzw. deren Systeme automatisiert) Zugriff auf die Zentrale Personenverwaltung (ZPV). Alle anderen Behörden, die den ZPV-Zugriff verlieren, erhalten neu Zugriff auf die GERES-Plattform. Die Aufsichtsstelle prüfte jene Zugriffe auf ihre Datenschutzkonformität, die gegenüber dem bestehenden ZPV-Zugriff neu waren. Die RegV legte bisher für die ZPV fest, dass die Gemeinden nur Zugriff auf die Daten ihrer Einwohner haben. Die Praxis missachtete diese Vorgabe und gewährte den ZPV-Zugriff kantonsweit. Die Gemeinden beantragten daher einen kantonsweiten Zugriff auf sämtliche GERES-Daten. Die Aufsichtsstelle und die kommunalen Aufsichtsstellen der vier grössten Gemeinden wiesen darauf hin, dass ein solcher Zugriff unverhältnismässig sei und eine Gefahr für die Privatsphäre – insbesondere von exponierten Persönlichkeiten – darstelle. Der Regierungsrat erteilte den Gemeinden mit der Revision in einem zusätzlichen separaten Profil einen kantonsweiten Zugriff auf eine beschränkte Anzahl Merkmale. Diese sollen den korrekten Nachvollzug der Zu- und Wegzüge erleichtern. Die Lesezugriffe sollen protokolliert aber nur bei Verdacht überprüft werden. Die nötigen Schutzmassnahmen für gefährdete Personen sollen noch getroffen werden. Unbestritten war der neue gemeindeübergreifende Zugriff der regionalen Sozialdienste auf die Einwohnerkontrolldaten der angeschlossenen Gemeinden. Die Aufsichtsstelle überprüfte mit dem KAIO die gesetzliche Abstützung für sämtliche Merkmale, die in der GERES-Plattform geführt werden. Gewisse Zugriffe wurden bereinigt. So wird neu kein Zugriff mehr auf die „Berufsmerkmale“ gegeben, weil es für sie keine Melde- bzw. Erfassungspflicht gibt. Es ist deshalb nicht gewährleistet, dass sie richtig und vollständig sind. Bereinigt wurden die umfangreichen Personendaten-Historisierungen: Nach den Vorgaben des Registerharmonisierungsgesetzes soll die GERES-Plattform den aktuellen Personendatenstand wiedergeben und nicht umfassende Rückverfolgungen zulassen. Daten von Personen, die aus dem Kanton weggezogenen oder verstorbenen sind, sind auf der GERES-Plattform spätestens nach fünf Jahren zu entfernen. Die Bereinigung ist noch nicht abgeschlossen.

- Bei der Änderung der Spitalversorgungsverordnung äusserte sich die Aufsichtsstelle zum Inhalt und Umfang der benötigten Personendaten in der Spitalseelsorge. Sie hielt fest, dass den Mitarbeitenden der Spitalseelsorge nur zu denjenigen Angaben über den Gesundheitszustand der Patienten Zugriff gewährt werden darf, die sie für die Spitalseelsorge benötigen. Sie wies darauf hin, dass die technische Umsetzung bei einem Zugriff mittels Klinikinformationssystem anspruchsvoll ist.

8 Aufsichts- und Justizentscheide

8.1 Aufsichtsrechtliche Aufforderung, unverzüglich die verschlüsselte Mailübertragung einzusetzen

Bei allen Mitarbeitenden des MIDI ist BE-Mail secure installiert. Diese kantonale Lösung zur sicheren Mail-Übertragung erlaubt es auch gegenüber Stellen, die nicht über diese Lösung verfügen, Mails verschlüsselt zuzustellen und von ihnen zu empfangen. Während des Audits einer Asylsozialhilfestelle und des MIDI (s. 3) erhielt die Aufsichtsstelle Kenntnis von zwei Mailzusendungen. In beiden wurden besonders schützenswerte Daten (neben Foto und Name Angaben zu Ethnie, Religion, strafrechtlichen Verurteilungen und Haftangaben) unverschlüsselt per Mail übertragen. Vor dieser offensichtlichen Gefährdung schutzwürdiger Interessen der Betroffenen forderte die Aufsichtsstelle das vorgesetzte Amt für Migration und Personenstand (MIP) auf, unverzüglich dafür zu sorgen, dass das sichere Mailsystem eingesetzt wird. Die Geschäftsleitung des MIP erliess eine entsprechende Weisung innert Tagesfrist.

8.2 Für die IV-Stelle zuständige Datenschutzaufsichtsstelle

Ein denunzierter Versicherter ersuchte die IV-Stelle Vevey um Bekanntgabe des Namens des Denunzianten. Die IV-Stelle wies das Einsichtsgesuch ab. Der Versicherte gelangte mit Beschwerde ans Sozialversicherungsgericht des Kantons Waadt. Dieses erachtete sich als unzuständig und überwies den Fall ans Bundes-

verwaltungsgericht. Dieses bejahte seine Zuständigkeit, wies aber die Beschwerde ab. Das daraufhin angerufene Bundesgericht stützte seinen Entscheid auf eine Stellungnahme des EDÖB, wonach die IV-Stelle wohl Bundesrecht vollziehe aber ein kantonales Organ sei. Das Bundesgericht erwog, die IV-Stelle sei kein Teil der Bundesverwaltung und werde auch nicht in den Organisationserlassen des Bundes aufgeführt. Kantonale Behörden würden nicht unter das Bundesdatenschutzrecht fallen. Die IV-Stellen seien durch Vereinbarungen zwischen dem Bund und den Kantonen ausdrücklich als kantonale Stelle errichtet worden. Das Bundesgericht hiess die Beschwerde gut und wies den Fall an das von Anfang an zuständige kantonale Verwaltungsgericht zurück. Es bejahte damit für alle kantonalen IV-Stellen die Zuständigkeit der kantonalen Aufsichtsstellen. Nach dem Urteil des Bundesverwaltungsgerichts hatte die Aufsichtsstelle eine offene Aufsichtssache an den EDÖB überwiesen (Ausgestaltung der Zugriffsrechte in der Informatikanwendung OSIV der IV-Stelle Bern). Das den Kanton Waadt betreffende Bundesgerichtsurteil klärte auch diese im Kanton Bern aktuelle Zuständigkeitsfrage abschliessend.

8.3 Berichtigung und Vernichtung von Akten der Kantonspolizei

Zu einem Eintrag im Journal der Kantonspolizei verlangte ein Betroffener eine Berichtigung. Die Kantonspolizei wies das Berichtigungsgesuch ab. Auf Beschwerde erwog die Polizei- und Militärdirektion, dass Werturteile und umstrittene Tatsachendarstellungen der Berichtigung oder Vernichtung nicht offen stehen. In solchen Fällen könne der Betroffene einzig eine angemessene Gegendarstellung aufnehmen lassen. Gleiches gelte für Rechtsverhältnisse, insbesondere zwischen Bürger und Staat, die im Streit liegen und entsprechend kontrovers dargestellt würden. Die Richtigkeit der umstrittenen Ausführungen könne in dem sich allenfalls anschliessenden formellen Verfahren (Justizverfahren) geprüft werden.

8.4 Videoüberwachung in Echtzeit oder mit Aufzeichnung: Verhältnismässigkeit; Bedeutung des Berufsgeheimnisses

Gegenüber einer gemeinderechtlichen Körperschaft bewilligte das Polizeikommando einzig eine Echtzeitüberwachung. Videoaufzeichnungen liess es nicht zu. Im Gebäude, dessen Zugangsbereich überwacht werden sollte, waren neben anderen Mietern auch medizinische Einrichtungen untergebracht. Videoaufzeichnungen dürften deshalb nur nach einer Befreiung vom ärztlichen Berufsgeheimnis ausgewertet werden. Im Bewilligungsverfahren für ein Spital habe das Polizeikommando in Erfahrung gebracht, dass das Kantonsarztamt eine generelle Befreiung jedoch verweigere. In ihrem Entscheid wies die Polizei- und Militärdirektion darauf hin, dass die Herrschaft über die Aufzeichnungen der gemeinderechtlichen Körperschaft und nicht einer Medizinalperson zukomme. Eine Befreiung vom Berufsgeheimnis sei deshalb für ein Auswerten der Aufzeichnungen in der Regel nicht erforderlich. Eine dissuasive Videoüberwachung mit Aufzeichnung sei verhältnismässig und die Beschwerde der gemeinderechtlichen Körperschaft gutzuheissen.

9 Polizei

9.1 ViCLAS-Betriebsbewilligung

Der Regierungsrat erteilte der schweizweit betriebenen Schwerstkriminellen-Datenbank ViCLAS gestützt auf die im Vorabkontrollverfahren gemachten Hinweise der Aufsichtsstelle die sowohl nach dem Polizeigesetz als auch nach dem ViCLAS-Konkordat erforderliche Betriebsbewilligung. Dies auf fünf Jahre befristet. Grund für die Befristung ist der Umstand, dass die kanadische Polizei als Lizenzgeberin das Programm zurzeit nicht mehr der informatiktechnischen Entwicklung anpasst.

9.2 Audit mobile Telefonie MDM

Neben zahlreichen Informatiksicherheitsproblemen erwies sich vorab das Potenzial zur Mitarbeiterüberwachung als erheblich. So stellte die eingesetzte externe Prüfstelle fest, dass die Mitarbeitenden ungenügend über den Umfang der Datenerhebung informiert wurden. So fehlte etwa eine Information darüber, dass beim Polizeikommando Roaminginformationen anfallen, gänzlich. Das Polizeikommando kann über das MDM aber auch feststellen, welche Apps ein Mitarbeiter auf seinem Gerät (das er auch zu privaten Zwecken nutzen darf) installiert hat. Zudem ist es möglich festzustellen, innerhalb welcher Sende-Ellipse sich ein Handy zurzeit befindet (Echtzeit). Da die Mitarbeitenden angehalten sind, für die Alarmierung die ihnen abgegebenen Handys auch in der Freizeit eingeschaltet zu lassen, ist eine Ortung auch ausserhalb der Dienstzeit möglich. Die für einen derart schweren Eingriff in das Grundrecht auf Datenschutz erforderliche formell-gesetzliche Grundlage fehlt. Zumindest bei iPhones mit älteren Betriebssystemen kann zudem jedenfalls keine Rede davon sein, die Mitarbeitenden würden der Überwachungsmöglichkeit zustimmen, indem sie die Ortung nicht ausschalteten. Mit

einem Ausschalten würde nämlich die vom Polizeikommando zu Recht verlangte Möglichkeit entfallen, die auf dem Handy gespeicherten dienstlichen Daten bei Diebstahl über das MDM zu löschen. Macht ein Mitarbeiter mit seinem Handy Fotos zu dienstlichen Zwecken, ist eine Synchronisation auf seinem privaten PC – und damit via iTunes eine Speicherung in der Cloud – nicht auszuschliessen. Eine Containerlösung, welche die Trennung von dienstlichen und privaten Bildern erlauben würde, fehlt. Das Polizeikommando hat vorab mit organisatorischen Massnahmen für Abhilfe gesorgt. Mit der Anschaffung neuer iPhones stellt es zudem sicher, dass auf diesen auch die aktualisierten iOS Betriebssysteme installiert werden können. Vollständige Vorabkontrollunterlagen wurden der Aufsichtsstelle aber noch nicht eingereicht. Das Audit hat gezeigt, dass der Betrieb eines MDM-Systems anspruchsvoll ist und mit ihm ein grosses Potenzial zur Verletzung von Datenschutzrechten einhergeht. Gezeigt hat das Audit allerdings auch, wie notwendig es ist, mobile Geräte, auf denen Daten zur staatlichen Aufgabenerfüllung bearbeitet werden, mit einem MDM-System zu verwalten und zu schützen. Das Polizeikommando hat diese Problematik als einzige Dienststelle erkannt und nach einer Lösung gesucht. Mobile Geräte stehen aber in der gesamten Staatsverwaltung flächendeckend im Einsatz. Das nun angelaufene Projekt für ein verwaltungsweites MDM-System (s. 5: Hinweis zu HarmTel) kommt spät.

9.3 IMSI-Catcher

Gegenüber der Polizei- und Militärdirektion wies die Aufsichtsstelle darauf hin, dass die Anschaffung eines IMSI-Catchers ein vorabkontrollpflichtiges Informatikprojekt darstellt.

(Zu den Videoüberwachungen der Kantonspolizei s. 4, zu Berichtigungen 8.3).

10 Besonderes:

10.1 Passwortvorgaben während Monaten missachtet

Seit Juli 2014 und bis März 2015 wurde die für den ganzen Kanton gültige Passwortweisung für die Anmeldung am elektronischen Arbeitsplatz für alle Mitarbeitenden der Justiz-, Gemeinde- und Kirchendirektion (JGK) nicht korrekt umgesetzt (Ausschalten der entsprechenden Schutzmechanismen). Die gleiche Systemkonfiguration lässt sich auch im Mai 2013 nachweisen. Entgegen der Passwortweisung erlaubte es das System, triviale Passwörter (zum Beispiel zweimal die aktuelle Jahreszahl) einzugeben. Zudem beschränkte es die Anzahl der Fehlversuche nicht. (Die kantonale Passwortrichtlinie erlaubt drei Fehlversuche, das System war auf 999 Fehlversuche eingestellt). In korrekter Weise wurde dagegen ein Passwortwechsel nach 30 Tagen verlangt. Zu lösen war das Problem auf technischer Ebene im März 2015 nicht mehr durch die JGK, sondern durch den Leistungserbringer KAIO. Das KAIO bietet die gemeinsame Grundversorgung (GGV) an, in welche die JGK ihre Anwendungen seit 2014 überführt hat. Das korrekte Umsetzen der Passwortverwaltung hatte im System für die Benutzenden zu Anmeldeproblemen geführt. Der Informatikdienst der JGK entschied sich daher, die Vorgaben der Passwortrichtlinie zu missachten. Damit konnte die Verfügbarkeit der von den Dienststellen der JGK betriebenen Anwendungen aufrechterhalten werden.
Das Beispiel zeigt, wie wichtig es in hoch integrierten Systemen ist, die Verantwortung über die gesamte Dienstleistungskette wahrzunehmen: Gefährdet war die Vertraulichkeit der von den Dienststellen bearbeiteten Daten. Für diese Vertraulichkeit hat die Geschäftsleitung der Dienststelle zu sorgen. Das bedeutet einmal, dass sie sowohl gegenüber dem Informatikdienst der Direktion als auch gegenüber zentralen Anbietern von Informatikdienstleistungen (Grundversorgung) sicherzustellen hat, dass diese Leistungserbringer zu einer ordnungsgemässen Aufgabenerfüllung befähigt sind (Auswahl). Mit Instruktionen sind die Leistungserbringer zudem in die Lage zu versetzen das Richtige zu tun. Sie sind jedenfalls zu verpflichten, die Anwendungsverantwortlichen (Leistungsbezüger) über Veränderungen der Systeme, vorab über solche mit Auswirkungen auf die Sicherheit, zu informieren. Das entbindet die Leistungsbezüger aber nicht von der Pflicht - etwa im Rahmen von Führungsrapporten institutionalisiert - nachzufragen, ob die gesetzlichen Rahmenbedingungen eingehalten werden und damit den sicheren und datenschutzkonformen Betrieb der Gesamtinformatiklösungen sicherzustellen (Kontrolle).

11 Berichtspunkte der Vorjahre

(3: und 9.2: Nachbetreuungen zu den 2014 vorgenommenen Kontrollhandlungen, 5: Weitergeführte Vorabkontrollen).

12 Antrag

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

29. Januar 2016

Der Datenschutzbeauftragte: *Siegenthaler*

13 Anhang

13.1 Abkürzungen, Bezeichnungen

ABR: Asyl-Bienne-Région (Verein)
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
Applikation: Informatikanwendung
ASP: Ansprechstelle des Personalamts (Beratungs- und Auskunftsangebot für Mitarbeitende und Führungsverantwortliche der kantonalen Verwaltung)
Bedag: Bedag Informatik AG: Die Bedag wurde 1990 gegründet und befindet sich im Eigentum des Kantons Bern
BRSB: Beratungs- und Rehabilitationsstelle für Sehbehinderte und Blinde des Kantons Bern
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
EDÖB: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EMM: Enterprise Mobility Management (siehe auch MDM)
ESAP: Projektname für das Projekt zur Ablösung des Finanz- und Personalsystems der Berner Fachhochschule und der Pädagogische Hochschule
FAQ: Frequently Asked Questions, englisch für häufig gestellte Fragen
fedpol: Bundesamt für Polizei
fmi ag: Spitäler Frutigen, Meiringen, Interlaken
FTAPI: Die FTAPI Software GmbH (File Transfer Application Platform for Integration) ist ein Münchner Unternehmen, das hochsichere Lösungen zum geschäftlichen Datentransfer, sowie zur Datenspeicherung entwickelt und vertreibt (nach Wikipedia)
GEF: Gesundheits- und Fürsorgedirektion
GERES: Informatiklösung zur Verwaltung und Harmonisierung von Personendaten, im Kanton Bern zum Zusammenzug aller Einwohnerkontrolldaten
IFIK: Institut für Infektionskrankheiten der Universität Bern
IIZ: Interinstitutionellen Zusammenarbeit
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)
LIS: Labor-Informationssystem
MC-SIS: Multi Cancer Screening Information System, gängige Software für Brustkrebs-Früherkennungsprogramme
MIP: Amt für Migration und Personenstand
MDM: Mobile-Device-Management (deutsch: Mobilgeräteverwaltung)
Microsoft Lync/Skype Plattform: 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)
NEF-Ziele: Im Rahmen der neuen Verwaltungsführung für jede Verwaltungseinheit festzulegende Leistungs- und Wirkungsziele (im Voranschlag und Geschäftsbericht des Kantons Bern aufgeführt)
OSIV: Open System IV, Informatikanwendung mehrerer IV-Stellen
PDBBJ: Psychiatrischen Dienste Biel-Seeland – Berner Jura
PRIVATIM: Vereinigung der Schweizerischen Datenschutzbeauftragten
PZM: Psychiatriezentrum Münsingen
QSC AG: Die QSC AG (QSC ist ein Eigenname) mit Sitz in Köln-Ossendorf ist ein deutscher IT-Dienstleister sowie ein Netzbetreiber und Anbieter von Internet- und Telekommunikationsprodukten (nach Wikipedia)
RSE: Regionalspital Emmental AG
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.
SUSA: Fachlösung für Strassenverkehrs- und Schifffahrtsämter
SZB: Spitalzentrum Biel
SRO: Spital Region Oberaargau
UPD: Universitäre Psychiatrische Dienste Bern
ViCLAS: Violent Crime Linkage Analysis System: Analyse-System zum Verknüpfen von Gewaltdelikten
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: Aufforderung der Aufsichtsstelle vom 2. Dezember 2015 an das MIP zum unverzüglichen Anordnen der erforderlichen Massnahmen: 42.52-6250
8.2: BGer 1C_125/2015 vom 17. Juli 2015
8.3: Entscheid der Polizei-und Militärdirektion vom 20. Februar 2015 – BD 123/13 Sn
8.4: Entscheid der Polizei-und Militärdirektion vom 28. Juli 2015 –BD 238/14 Ho

13.3 Internetadressen

1.2: PRIVATIM: Über die Rechnungskontrolle durch die Kantone bei stationär erbrachten Leistungen im Bereich der obligatorischen Krankenpflegeversicherung: http://www.privatim.ch/files/layout/downloads_de/15_0071_07-DE_privatim-Umfrage_Rechnungspruefung_Ergebnisse_20150213.pdf
2.3: Geschäftsbericht: http://www.fin.be.ch/fin/de/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html
4: Evaluationsberichte zu den Videoüberwachungsanlagen des Polizei- und Militärdirektion: http://www.pom.be.ch/pom/de/index/direktion/ueber-die-direktion/publikationen.html
6: Datendrehscheiben: http://www.jgk.be.ch/jgk/de/index/aufsicht/datenschutz/informatiksicherheit.assetref/dam/documents/JGK/DS/de/DS_Datendrehscheiben_Dokumentation%20in%20der%20Vorabkontrolle%20nach%20Art.%2017a%20KDSG_de.pdf