Bericht 2016 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

Die von der Aufsichtsstelle beauftragten Prüfstellen sehen sich unterschiedlichen Informatikumgebungen gegenüber: So war in der Spitäler fmi AG das Berechtigungs- und Zugriffsmanagement der neusten Generation mit Nutzung mobiler Geräte und externen Zugängen zu prüfen. Das Ergebnis hat umfassend überrascht: Die eingesetzte Informatiklösung wird von den Mitarbeitenden gerade auch in Dringlichkeitssituationen als benutzerfreundliches Instrument wahrgenommen. Die hohen Ansprüche der medizinischen Betreuung werden erfüllt. Die Prüfenden erteilten der Informatiklösung aber auch mit Blick auf die Informatiksicherheit und auf den Persönlichkeitsschutz gute Noten (s. 4). Anders stellt sich die Situation bei den grossen Informatikprojekten für die Kantonsverwaltung dar: Zum künftigen kantonalen Informatikarbeitsplatz (KWP 2.0), zum Informatikprojekt EMM (Verwaltung der vom Kanton eingesetzten mobilen Geräte) und zum Geschäftsverwaltungs- und Archivierungssystem BE-GEVER hatte die Aufsichtsstelle gewichtige Vorbehalte. Zum Zeitpunkt der Berichterstattung war offen, ob es gelingt, sie auszuräumen (s. 5). Eine Erklärung für dieses Auseinanderklaffen liegt in der unterschiedlichen Beteiligung der Verantwortlichen für den Fachbereich: In der Spitäler fmi AG leitete ein Gremium aus Geschäftsleitung, Medizin und Informatik das Projekt. Die Mitglieder der Projektleitung tragen auch ausserhalb des Projektes Verantwortung für den korrekten Umgang mit den medizinischen Daten. Anders präsentiert sich die Situation für die Kantonsverwaltung: Für Projekte der gemeinsamen Grundversorgung wird die Projektleitungsarbeit im Rahmen der neuen Informatikstrategie unter der Leitung des Strategischen ICT-Ausschusses erheblich vom kantonalen Amt für Informatik und Organisation (KAIO) geprägt. Um den Datenschutzanliegen Rechnung zu tragen, sind auch bei Projekten der gemeinsamen Grundversorgung die Verantwortlichen der Fachbereiche verstärkt zu beteiligen (s. 8.7 zum Umgang mit Telefonieranddaten).

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). 2016 fanden zwei Arbeitssitzungen statt.

-Mitarbeitende der Aufsichtsstelle wirkten in den PRIVATIM-Arbeitsgruppen „Information and Communication Technology“ (ICT) und „Gesundheit“ mit. Die Arbeitsgruppe ICT hat sich intensiv mit „mobile computing“ befasst und dazu ein internes Arbeitspapier verfasst. Die Arbeitsgruppe „Gesundheit“ hat sich an ihren drei Sitzungen mit der Ausführungsgesetzgebung zum eidgenössischen Patientendossier befasst und eine Vernehmlassung eingereicht.
Der Kanton Bern stellt interessierten Privaten Grundbuchdaten elektronisch zur Verfügung. Der Betrieb der hierzu erforderlichen Infrastruktur ist gemeinsam mit anderen Kantonen an eine private Firma ausgelagert worden. Zu deren Beaufsichtigung gründeten die beteiligten Grundbuchämter den Verein TerrAudit. Beauftragte Dritte sollen für diesen Kontrollen durchführen. Auch Datenschutzaufsichtsstellen können dem Verein beitreten. Um ein Vermischen von verwaltungsunabhängigen und verwaltungsinternen Kontrollen zu vermeiden, hat die Aufsichtsstelle auf einen Beitritt verzichtet.

1.3 Änderungen im übergeordneten Recht

Eine Arbeitsgruppe der Konferenz der Kantonsregierungen war zum Zeitpunkt der Berichterstattung damit befasst, einen Leitfaden für die Kantone zu erarbeiten. Dieser soll den Anpassungsbedarf bei der kantonalen Datenschutzgesetzgebung aufzeigen. Auslösend ist die EU-Datenschutzreform sowie die Modernisierung der Europarats-Konvention 108. Berücksichtigung finden soll zudem der Vorentwurf zu einem totalrevidierten Bundesgesetz über den Datenschutz. Voraussichtlich unter der Federführung der Justiz-, Gemeinde- und Kirchendirektion (JGK) wird das kantonale Datenschutzgesetz zu überarbeiten sein. Anzustreben ist ein Inkrafttreten des überarbeiteten Erlasses auf Herbst 2018 hin.

2 Aufgabenumschreibung, Prioritäten, Mittel

2.1 Prioritäten

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

– Vorschalten der zuständigen Stelle: Die Beratung kommunaler und kantonaler Verwaltungsstellen hat durch die zuständigen kommunalen Datenschutzaufsichtsstellen bzw. Rechtsdienste der kantonalen Verwaltung zu erfolgen. Betroffene sind in kommunalen Fragen durch die kommunalen Datenschutzaufsichtsstellen zu beraten. Wer unmittelbar bei der Aufsichtsstelle anfragt, ist an die zuständigen Stellen zu verweisen. Diese Zuständigkeiten und die dadurch erfolgende Triage 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 gute Abwehrrechte (Berichtigung, Vernichtung, Feststellen der Widerrechtlichkeit). Aufsichtsrechtliche Abklärungen sollen unterbleiben, wenn solche Abwehrmöglichkeiten gegeben sind. Die Betroffenen sind auf ihre Abwehrrechte aufmerksam zu machen. Lassen die Hinweise Rückschlüsse auf Systemprobleme zu, ist diesen mit den entsprechenden Mitteln (z. B. Kontrollen) nachzugehen.

– Vorabkontrollen: Die Vorabkontrollvorgaben wollen die Projektleitungen 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 Personendaten).

– 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 (Direktionen) 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 (Leistungsziele), nehmen die Mitarbeitenden die eine Änderung der Priorisierung, allenfalls die Zuweisung an andere Mitarbeitende, den (Teil-)Verzicht auf eine 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.

2.2 Eigenverantwortung der datenbearbeitenden Stellen

An einer Weiterbildungsveranstaltung für das gesamte Personal der Salome Brunner-Stiftung für sprach- oder hörbehinderte Kinder und Jugendliche konnte die Aufsichtsstelle für Datenschutzanliegen sensibilisieren.
Eine Weiterbildungsveranstaltung führten auch die Schlichtungsbehörden für ihr Sekretariatspersonal durch.

2.3 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Berichtsjahr waren für die kantonale Verwaltung 39 Millionen CHF in Informatikmittel zu investieren. 164 Millionen CHF (davon 128 Millionen CHF für Drittdienstleister) sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). In diesen Zahlen sind die Aufwendungen der von der Aufsichtsstelle ebenfalls zu beaufsichtigen-

den 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 176'000 zur Verfügung (s. 3).

Sie verfügte 2016 über 5.15 Vollstellen (davon 0.2 für das Sekretariat). Weitere Angaben zu Budget, Rechnung, Erreichen der Ziele (Finanzzahlen) finden sich im Geschäftsbericht 2016 des Kantons Bern (Band I, s. 11.3).

3 Kontrollen von Informatikanwendungen, die im Betrieb stehen

Vier Kontrollen wurden im Berichtszeitraum durchgeführt:

- Klinikinformationssystem der Spitäler fmi AG (s. 1.1)

Die Verantwortlichen der Spitäler fmi AG haben in den letzten Jahren grosse Anstrengungen im Bereich Informationssicherheit und Datenschutz unternommen. So wurde u.a. das Berechtigungs- und Zugriffsmanagement professionalisiert und organisationsweit ausgerollt. Der Trend zur Nutzung mobiler Geräte verbunden mit externen Zugängen wurde rechtzeitig erkannt, in das Sicherheitskonzept integriert und notwendige Massnahmen wurden umgesetzt. Entsprechend zeigt die Prüfung, dass die fmi AG die Risiken im Bereich Informationssicherheit und Datenschutz ernst nimmt und ein guter Stand erreicht worden ist. Aufgedeckte Mängel wurden umgehend behoben oder in Projekten aufgenommen. Die Affinität zur Thematik und die hohe Fachkompetenz der Spitäler fmi AG haben wesentlich zu einem effizienten und erfolgreichen Audit beigetragen.

- KESB: Prüfung der Fachapplikation Klientendossier

Die Kindes- und Erwachsenenschutzbehörde (KESB) bearbeitet in hohem Mass besonders schützenswerte Personendaten. Die KESB ist im Kanton Bern regional in 11 Kreise aufgeteilt. Derzeit haben alle Mitarbeitenden einen Zugriff auf alle Dossiers in allen Kreisen (49‘000 Dossiers). Wohl besteht für diesen Zugriff eine gesetzliche Grundlage. Der Gesetzgeber macht jedoch Auflagen zur Verhältnismässigkeit. (So ist der Kreis der Zugriffsberechtigten z. B. auf Pikettfunktionen zu beschränken und die Zugriffe sind zu protokollieren.) Diese Auflagen sind jedoch nicht umgesetzt. Nicht umgesetzt ist auch die verlangte Verfügbarkeit: Im Notfall soll jederzeit auf ein Dossier zugegriffen werden können. Die Leistungsvereinbarungen mit dem Leistungserbringer verzichten u.a. aus wirtschaftlichen Gründen auf entsprechende Anforderungen.
Eigentümer der Klientendaten und Leistungsbezüger der IT-Dienstleistungen sind die Verantwortlichen der KESB-Kreise. Sie beziehen die Leistung von der IT-Abteilung der JGK. Diese bestellt die Leistungen für den Betrieb beim KAIO und für die Applikationen beim Softwarelieferanten. Das KAIO wiederum lagert den Betrieb in die Bedag aus. Diese Dienstleistungskette ist durch die KESB kaum zu beeinflussen oder zu kontrollieren, da ein aussagefähiges Leistungsreporting fehlt. Es stellt sich die Frage, inwiefern die KESB-Verantwortlichen ihre Verantwortung wahrnehmen können.
Das ISDS-Konzept hat Bestandteil der Leistungsbestellungen zu sein, damit die Leistungserbringer die ISDS-Anforderungen mit den entsprechenden Massnahmen umsetzen können. Das ISDS-Konzept der Fachapplikation Klientendossier war entgegen dieser Vorgabe nicht in die Leistungsbestellung eingeflossen. Für die Kommunikation der KESB mit anderen Stellen wird Briefpost, eMail und Fax eingesetzt. Je nach Adressat werden auch besonders schützenswerten Daten unverschlüsselt per Mail versendet. Fax wird vorwiegend als Empfangsgerät eingesetzt.

- Prüfung von Informatikanwendungen der Steuerverwaltung (SV)

Diese Prüfung wurde gemeinsam mit der Finanzkontrolle durchgeführt. Der Fokus richtete sich auf die Datenbearbeitung mit der Applikation zur Veranlagung natürlicher Personen (NESKO) unter Einbezug der organisatorischen und technischen Rahmenbedingungen beim Leistungsbezüger (SV), Leistungsbesteller (KAIO) und Leistungserbringer (Bedag). Die Aufsichtsstelle begutachtete die rechtlichen und vertraglichen Aspekte, während die Finanzkontrolle die applikatorischen und organisatorischen Anforderungen prüfte. Das in diesem Jahr überarbeitete und freigegebene ISDS-Konzept diente dabei als Grundlage. Der Auditbericht war zum Zeitpunkt der Berichterstattung in Bearbeitung.

- Prüfung von Informatikanwendungen der Mittelschulen ESCADA/EVENTO

Die Prüfung hat im Herbst stattgefunden. Zum Zeitpunkt der Berichterstattung wurden die Resultate verifiziert und ausgewertet. Der Bericht wird im 1. Quartal 2017 fertiggestellt.

Nachbetreuungen früherer Kontrollen:

- Datenschutzrechtliche Kontrolle Asyl Biel (ABR)

Die Geschäftsleitung hat aufgrund des Auditberichts umgehend die erforderlichen Schritte eingeleitet. Basierend auf der Norm ISO 2700x

liess sie ein ISDS-Konzept erarbeiten und die Risiken bewerten. Ergeben hat sich, dass der bestehende IT-Betrieb und die Infrastruktur den Anforderungen nicht genügen können und neu zu konzipieren sind. Das erforderliche Projekt wurde initiiert und steht kurz vor dem Abschluss.

- Grundschutzprüfung der Universität Bern

Im Berichtsjahr konnten alle nach dem ISDS-Audit noch offenen Massnahmen umgesetzt werden; das Audit ist somit abgeschlossen.

4 Videoüberwachung

- Auch 2016 waren mehrere Videoüberwachungsanlagen für kantonale Gebäude im Vorabkontrollverfahren zu prüfen. Darunter eine Anlage des Zentrums für Sport und Sportwissenschaften der Universität Bern und Anlagen im Inselspital. Die geplanten Überwachungen erwiesen sich als verhältnismässig. Da die Mitarbeitenden dem ärztlichen Berufsgeheimnis unterstehen, wurde das Inselspital verpflichtet, das Personal mit einem Merkblatt, einer Vereinbarung oder einer Weisung auf den datenschutzkonformen Umgang mit den Überwachungsbildern und auf das Berufsgeheimnis hinzuweisen. Diejenigen Kameras, die sich in nicht allgemein zugänglichen Gebäuden des Inselspitals befinden und die nicht der Sicherheit sondern der Logistik im Dienste der Patientinnen und Patienten dienen, konnten nicht gestützt auf das Polizeigesetz bewilligt werden. Die Echtzeitüberwachungen dürfen jedoch gestützt auf die gesetzliche Aufgabenerfüllung erfolgen. Als unzulässig erwiesen sich aber die geplanten Aufzeichnungen in den Gebäuden des Spitals, die während der Nachtzeit geschlossen sind. Videoüberwachungen mit Aufzeichnungen gelten als schwere Grundrechtseingriffe. Die für diese Überwachungen nötige formell-gesetzliche Grundlage für Spitäler fehlt.

- Die Tourismusorganisation des Berner Juras unterbreitete der Aufsichtsstelle Fragen zu geplanten Webcams mit Roundshot-Kameras. Die Webcams zeigen im Internet Bilder von öffentlichen Plätzen, Hauseingängen, privaten Vorplätzen usw., die gezoomt, individuell gespeichert, bearbeitet und weiter verwendet werden können. Erfasste Personen und Fahrzeuge werden damit bestimmbar. Die Personen müssten einerseits ihre Zustimmung zu solchen Aufnahmen und deren Veröffentlichung im Internet geben und andererseits dürften nur die nach Polizeigesetz zuständigen kommunalen Behörden öffentliche und allgemein zugängliche Orte aus Sicherheitsgründen mit Kameras so überwachen, dass Personen bestimmbar sind. Damit Webcams eingesetzt werden dürfen, müssen sie deshalb technisch so konfiguriert und örtlich installiert werden, dass mit ihnen weder Personen und Fahrzeugschilder erkennbar sind, noch über eine Bearbeitungsfunktion bestimmbar werden.

- Zum Aufsatz zu Kameras von Privatpersonen im öffentlichen Raum s. 11.3.

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:

- Zum Klinikinformationssystem des Spitals Emmental hat die Aufsichtsstelle im Berichtsjahr vier Stellungnahmen abgegeben. Die Prüfung beschränkte sich dabei auf die Verhältnismässigkeit der Ausgestaltung der Benutzerberechtigungen. Zurzeit fehlen u.a. noch Ausführungen zu einem allfälligen Umgehungs-/Notfallzugriff sowie zum Schutz exponierter Personen wie etwa Mitarbeitenden.

- Beim Klinikinformationssystem des Spitals Region Oberaargau hat die Aufsichtsstelle einen Vorortermin durchgeführt, um sich das System demonstrieren zu lassen und um offene Fragen zu klären. Im Anschluss daran hat sie ihre erste Stellungnahme dazu abgegeben. Die Aufsichtsstelle hat festgestellt, dass die Zugriffsberechtigungen zu weit ausgestaltet sind.

- Nach einer längeren Vorlaufzeit sind die formell vollständigen ISDS-Unterlagen zur Applikation MC-SIS des Mammografie-Screening-Programms für die Region Berner Jura, welches durch das Centre de dépistage du cancer du sein BEJUNE durchgeführt wird, eingetroffen. Die Prüfung der Unterlagen hat gezeigt, dass noch Einiges nachgebessert werden muss. U.a. sind eine ausführliche Beschreibung der Datenflüsse sowie ein detaillierteres Rollen- und Berechtigungskonzept nachzureichen. Auch ein Aufbewahrungs- und Löschkonzept fehlt.

- Bei der Vorabkontrolle der Applikation Optinomic des Kompetenzzentrums für Mensch und Sucht, Südhang, hat ein Vorortermin stattgefunden. Nebst einer Demonstration der Applikation konnten auch Unklarheiten und das weitere Vorgehen besprochen werden. Im Anschluss daran hat das Kompetenzzentrum nachgebesserte ISDS-Unterlagen eingereicht. Von der Aufsichtsstelle gefordert waren u.a. eine Aktualisierung der Unterlagen auf die neue Version von Optinomic, eine ausführlichere und verständlichere Zugriffsmatrix, sowie ein Aufbewahrungs- und Löschkonzept.

- Per 1. Januar 2017 wurden die drei psychiatrischen Kliniken verselbständigt. Sie unterstehen ungeachtet ihrer neuen Rechtsform (Aktiengesellschaft) aber weiterhin dem kantonalen Datenschutzgesetz. Aus technischer Sicht bedeutet dies, dass die kantonalen IT-Dienstleistungen, wie z. B. eMail und Web, aber auch betriebskritische Rechenzentrumsdienste nicht mehr zur Verfügung stehen und dafür die eigene IT-Infrastruktur auf- resp. ausgebaut werden muss. Aus rechtlicher Sicht wird die Mehrzahl der Infrastrukturen und Applikationen der Vorabkontrollpflicht unterstehen, da die in diesem Umfeld bearbeiteten Daten in der Regel besonders schützenswerte Personendaten sind. Die Aufsichtsstelle hat vorgeschlagen für alle Standorte ein gemeinsames ISDS-Konzept zu erstellen, welches auf die besonderen Risiken des psychiatrischen Umfeldes abgestimmt ist und einen angemessenen Grundschutz beschreibt. Dies würde den Aufwand für die Vorabkontrolle der Applikationen wesentlich verringern. Die Institutionen entschieden jedoch ein ISDS-Konzept pro Standort zu erstellen. Bis zum Berichtszeitpunkt haben die Psychiatrischen Dienste Biel-Seeland – Berner Jura (PDBBJ) ein ISDS-Konzept zur Prüfung eingereicht. Mit den anderen beiden Kliniken steht die Aufsichtsstelle in Kontakt.
Die psychiatrischen Kliniken verfügen seit ihrer Verselbständigung auch über eigene Personaldatensysteme. Auf Anfrage des Personalamtes prüfte die Aufsichtsstelle eine Vereinbarung, welche die Voraussetzungen, den Umfang und den Zeitraum regelt (zwei Jahre), unter denen den Institutionen weiterhin ein Zugriff auf Daten des Personalinformationssystem des Kantons gewährt wird. Dieser Zugriff setzt voraus, dass die Institutionen ihre Personalinformationssysteme einer Vorabkontrolle zuführen und ihre Personaldatensammlungen im Register der Datensammlungen anmelden (s. 6 und 8.3).
Bei der Vorabkontrolle des Personalinformationssystems (PIS) des Psychiatriezentrums Münsingen (PZM) liegt bereits eine erste Stellungnahme der Aufsichtsstelle vor.

- An das PZM erfolgte zum KIS eine Rückmeldung zur geplanten physikalischen Löschung. Bis diese umgesetzt werden kann, behilft sich das PZM mit einer Zwischenlösung. Es gilt zu klären, welche Inhalte für einen sicheren Nachweis einer durchgeführten Datenlöschung notwendig sind. Erfolgt die Protokollierung unter Nennung des Namens des Patienten, verhindert das Protokoll, dass dem Recht auf Vergessen der Betroffenen Genüge getan wird.

- Zum Klinikinformationssystem Cariatides der PDBBJ hat die Aufsichtsstelle eine dritte Stellungnahme abgegeben. Diese klammerte die Zugriffsrechte aus, da diese erst mit der neuen Version des Systems datenschutzkonform ausgestaltet und umschrieben werden können.

- Im Berichtsjahr kam es zwischen der Aufsichtsstelle und den Universitären Psychiatrischen Diensten Bern (UPD) wiederum zu einem mehrmaligen Austausch zu noch offenen Punkten des Klinikinformationssystems wie z.B. der Löschfunktion. Die UPD haben die Ausgestaltung der Zugriffsrechte überprüft und der Aufsichtsstelle nebst dem überarbeiteten ISDS-Konzept eine neue Berechtigungsmatrix eingereicht. Dazu hat die Aufsichtsstelle wiederum eine Stellungnahme abgegeben und Rückfragen gestellt.

- Bei der Vorabkontrolle des Abrechnungssystems IBAS für Menschen mit Behinderungen (Weblösung, Ausführungskredit von 3.2 Millionen CHF), des Alters- und Behindertenamtes (ALBA) sind die ISDS-Unterlagen eingereicht worden.

- Nach mehrmaligem schriftlichen Austausch und einer Sitzung vor Ort zur Besprechung von Unklarheiten hat die Universität Bern zu den Applikationen des Kreditorenworkflows ein vereinfachtes ISDS-Konzept bei der Aufsichtsstelle eingereicht.

- Die Universität Bern hat die ISDS-Konzepte von zwei IT-Projekten (eForms und ZundL) zur Vorabkontrolle eingereicht. Einerseits wurden elektronische Formulare für die Administration implementiert und andererseits die Zeit- und Leistungserfassung eingeführt. Beide Applikationen werden auf der Infrastruktur der Informatikdienste betrieben. Dies vereinfachte die Vorabkontrolle erheblich, da die IT-Infrastruktur im Jahr zuvor erfolgreich einer Grundschutzprüfung unterzogen wurde (s. 3). Beide Prüfungen sind abgeschlossen.

- Die geforderten Präzisierungen zum Archivieren und Löschen im Kernsystem Lehre (KSL, Gesamtapplikation für die elektronische Prüfungsverwaltung, das elektronische Vorlesungsverzeichnis und die Hörraumverwaltung) wurden von der Universität Bern eingereicht.

- Für UNICARD (elektronische Legitimationskarte für Studierende und Mitarbeitendenkarte, mit Chip) steht noch die Bestätigung aus, dass die Archivierungsvorgaben umgesetzt sind.

- Das Berner Institut für Hausarztmedizin benutzt eine Webapplikation zur Verwaltung (insbesondere für die Zuteilung und Abrechnung) der für Medizinstudierende obligatorischen Hausarztpraktika. Die Aufsichtsstelle hat die eingereichten Unterlagen summarisch geprüft. Die eingeforderten Verträge mit den Outsourcingpartnern müssen noch punktuell überprüft werden. Auf eine Prüfung der Informationssicherheitsaspekte verzichtete die Aufsichtsstelle.

- Im Rahmen der Vorabkontrolle der Applikation CASEnet für die Abwicklung des Case Managements für Lehrpersonen der Pädagogischen Hochschule Bern (PHBern) hat die Aufsichtsstelle eine erste Stellungnahme abgegeben. Die geforderten Nachbesserungen in den ISDS-Unterlagen hat die PHBern fristgerecht eingereicht. Da zum Rollen- und Berechtigungskonzept noch einige Unklarheiten bestanden, waren mündliche Klärungen nötig.

- Mit dem Informatikprojekt BEKOS (Koordination der kantonalen pädagogischen und sozialpädagogischen Institutionen) der Gesundheits- und Fürsorgedirektion (GEF) sollen die IT-Infrastruktur inkl. Kommunikation und die Basissoftware für den Unterrichtsbetrieb und die Administration harmonisiert werden. Bei der Vorabkontrolle wurden erhebliche konzeptionelle wie auch technische Lücken aufgedeckt. Das Projekt wurde inzwischen den Informatikdiensten der Erziehungsdirektion (ERZ) übergeben.

- Im Rahmen der Vorabkontrolle des Finanzinformationssystems ESAP der Berner Fachhochschule (BFH) und der PHBern erfolgte eine zweite Stellungnahme. Noch ausstehend ist ein Archivierungskonzept, in welchem aufzuzeigen ist, welche Daten in der jeweiligen Phase wie lange im System bleiben und wer jeweils darauf Zugriff hat.

- Die Applikation Electronic Monitoring (EM) erlaubt es, gestützt auf Bundesrecht freiheitsentziehende strafrechtliche Sanktionen für Erwachsene und Jugendliche sowie ambulante Massnahmen (wie z.B. Hausarrest) elektronisch zu überwachen. Im Kanton Bern ist heute eine beschränkte Anzahl Überwachungsgeräte im Einsatz. Für die Zukunft soll die Überwachung jedoch schweizweit ausgebaut werden. Auf 2017 hin soll der Kanton Bern an das EM des Kantons Zürich angeschlossen werden. Die erhobenen Daten sind besonders schützenswert. Die Vorabkontrolle ergab, dass das zuständige Amt zwar zahlreiche nötige ISDS-Massnahmen getroffen hat, dass aber auch bei einem Anschluss an das Zürcher EM noch weitere ISDS-Fragen und -Aspekte geklärt werden müssen. Der Kanton Bern bleibt für Datenbearbeitungen durch Dritte verantwortlich. Als Outsourcingpartner unterstehen Dritte den Bestimmungen des Datenschutzrechts des Kantons Bern. Offen ist beispielsweise, ob die Anwendung des GPS-Trackings auf das Notwendige beschränkt wird. Zu konkretisieren sind die Kriterien für eine mögliche aktive (Echtzeit-) Überwachung, die Aufbewahrung und Vernichtung der Tracking-Daten sowie die Beschränkung des Zugriffs des externen Softwarelieferanten auf die erhobenen Daten.

- Das Agrarinformationssystem GELAN 2015 löst GELAN 2011 ab. Es ist eine Webanwendung, mit der die Kantone Bern, Freiburg und Solothurn ihre bunderechtlichen Agrardaten, insbesondere sämtlich Berechnungsdaten und administrativen Sanktionen erfassen. Die Benutzenden werden mit einem Merkblatt auf ihre Verantwortung für das Einhalten von Datenschutz und Datensicherheit hingewiesen. GELAN 2015 erfüllt die ISDS-Anforderungen. Die Vorabkontrolle konnte bis auf das Archivierungs- und Löschkonzept abgeschlossen werden.

- Mit dem „E-Recruiting des Kantons Bern“ wurde der Aufsichtsstelle ein elektronisches Bewerbungsmanagementsystem zur Vorabkontrolle eingereicht. Das ausgewählte Produkt ist bei verschiedenen öffentlich-rechtlichen Kunden im Einsatz, u.a. beim Bund und bei anderen Kantonen. Wenn der Kanton ein Kommunikations- und Datenbearbeitungssystem anbietet, ist er umfassend für die Datensicherheit verantwortlich. Fragen zum Anbieter der externen Informatikplattform und zur Datensicherheit konnten geklärt werden. Der Anbieter ist vertraglich verpflichtet die AGB ISDS des Kantons Bern einzuhalten. Die Bewerberinnen und Bewerber werden mit einer Datenschutzerklärung über den Umfang und die Sicherheit der Datenbearbeitungen informiert.

- Mit dem Zeugnismanagementsystem wird den Personaldiensten und Vorgesetzten ein gesichertes System mit Funktionalitäten für die Generierung von Arbeitszeugnissen zur Verfügung gestellt. Das System wird von der Bedag entwickelt und betrieben. Die Zeugnisse werden nicht in diesem System aufbewahrt. Im Personaldossier wird eine Kopie hinterlegt.

- Das KAIO reichte die neue Web-Formularlösung zur Vorabkontrolle ein. Mit ihr wird der Verwaltung eine einheitliche Lösung für das Erstellen von Webformularen zur Verfügung gestellt. Sie bietet insbesondere eine verschlüsselte Datenübertragung und einen gesicherten Zugang nur für berechtigte Personen. Auch hier wurde vertraglich das Einhalten der AGB ISDS sichergestellt.

- Die Prüfung des Umfragetools Scoppo führte zu folgendem vorläufigem Ergebnis: Vorausgesetzt, dass die rechtliche Grundlage für die jeweilige Datenbearbeitungen vorhanden ist, kann das Tool für nicht besonders schützenswerte Daten nur dann eingesetzt werden, wenn der Grundschutz nach den AGB ISDS vertraglich vereinbart und die Vernichtung der Daten nach Abschluss einer Umfrage gesichert ist. Für besonders schützenwerte Daten müssen zusätzlich die ISDS-Schutzmassnahmen für den erhöhten Schutz vereinbart und ihre Umsetzung in

einem ISDS-Konzept nachgewiesen werden. Zurzeit fehlt bereits die Möglichkeit, solche Daten verschlüsselt zu übertragen. Für anonyme Umfragen könnte das Tool erst eingesetzt werden, wenn die Anonymisierung gewährleistet ist.

- Mit der Software Octosam war ein Lizenzverwaltungssystem für die kantonale Verwaltung zu prüfen. Die Vorabkontrolle ergab, dass mit den aufgezeichneten Daten gleichzeitig umfangreiche Mitarbeiterdaten anfallen würden. Kantonsweit wäre nachweisbar, wer (IP-Adresse), mit welcher lizenzierten Software, wann und wie lange gearbeitet hat. Das Erfassen solcher umfassender Daten zum Arbeitsverhalten wäre ein schwerer Eingriff in die Grundrechte der Mitarbeitenden. Er wäre nur gestützt auf eine ausdrückliche formell-gesetzlich Grundlage zulässig.

- Die Vorabkontrolle des Projektes zur Realisierung eines Enterprise Mobility Management (EMM) zur Verwaltung mobiler Geräte erwies sich als anspruchsvoll. Das Projekt hat für die Aufsichtsstelle wegweisenden Charakter, da der Einsatz mobiler Mittel längst Alltag ist und es umsetzbare, zukunftsweisende Lösungen zu finden gilt. Die mobile Infrastruktur muss gesetzeskonform und benutzerfreundlich betrieben werden können. Genau darin besteht die Herausforderung: Informationssicherheitsmassnahmen werden nur dann umgesetzt, wenn sie benutzerfreundlich sind. Thematisiert wurden die Trennung von privaten und geschäftlichen Daten und Apps, die Nutzung privater Geräte (Bring your own device BYOD), das Bearbeiten besonders schützenswerter Personendaten auf den Geräten, die sichere Authentisierung der Benutzenden, die Konfiguration und Überwachung der Geräte (Virenschutz, Sperrung usw.) sowie die Geräte- und Systemvielfalt. Die Vorabkontrolle konnte noch nicht abgeschlossen werden (s. 1.1).

- das Projekt BE-GEVER gehört zur gemeinsamen Grundversorgung (s.1.1). Wie bei EMM sollen die Organisationseinheiten künftig mit diesem zentral betriebenen Geschäftsverwaltungs- und Archivierungssystem arbeiten. In der Vorabkontrolle erwiesen sich vorab zwei Aspekte als problematisch: - Im Unterschied etwa zum Bund wird für die digital abgelegten Unterlagen („papierloses Büro“) weder eine digitale Unterschrift noch eine Zwei-Faktoren-Authentifizierung für die Systemanmeldung verlangt. Das führt zur Situation, dass das System Änderungen an den Unterlagen protokolliert und geänderte Unterlagen versioniert, aber nicht mit genügender Sicherheit nachweisen kann, wer die entsprechenden Änderungen vorgenommen hat. Das staatliche Handeln muss nachweisbar sein. Dies garantiert letztlich das willkürfreie Handeln. Ohne genügende Authentifizierung gelingt es nach einem Verzicht auf Papierakten aber nicht mehr, genügend beweisfeste Unterlagen vorzulegen. Wird dieser Mangel nicht behoben, genügt BE-GEVER unter dem Aspekt der Datenrichtigkeit den Datenschutzansprüchen nicht. – Die Mandanten (Organisationseinheiten der Direktionen) sollen ihre Daten autonom klassifizieren und die Zugriffsberechtigungen zuteilen können. Um die Zusammenarbeit zu fördern, ermöglicht das System den mandantenübergreifenden Dokumentenaustausch, resp. eine gemeinsame Ablage von Dossiers. Sollen Sicherheitslücken vermieden werden, setzt dies allerdings voraus, dass alle Beteiligten, also auch solche ausserhalb der eigenen Organisationseinheit, denselben Klassifizierungsmassstab anwenden. Wie das, nachdem der Kanton im Unterschied zum Bund ausser für Regierungsratsbeschlüsse keine kantonsweite Klassifizierungsvorgabe kennt, umzusetzen ist, konnte im Vorabkontrollverfahren nicht aufgezeigt werden.

- Die Arbeitsplätze der Verwaltung sollen mit neuen Informatikarbeitsgeräten (Clients) ausgerüstet werden (Projekt KWP 2.0, s. 1.1). Als Betriebssystem soll Windows 10 Einsatz finden. Stationäre und mobile Geräte sollen zum Einsatz kommen. Nach einer ersten Prüfung des ISDS-Konzepts hat die Aufsichtsstelle u.a. festgestellt, dass die Geräte erhöhte ISDS-Anforderungen erfüllen müssen damit standardmässig besonders schützenswerte Personendaten bearbeitet werden dürfen, dass die Konnektivität der Geräte an die Kommunikationsnetze einzubeziehen ist, dass standardisierte Gerätekonfigurationen nach „Best practices“ festzulegen und umzusetzen sind und ein Überwachen der Einhaltung dieser Einstellungen möglich sein muss. Die Prozesse für die Installation von Sicherheits- und Supportupdates sind zu dokumentieren und umzusetzen. Die Vorabkontrolle war zum Zeitpunkt der Berichterstattung noch offen.

Die Ressourcensituation hat es der Aufsichtsstelle nicht erlaubt, die bei den Vorabkontrollen bestehenden erheblichen Rückstände genügend abzubauen. Das noch offene Vorabkontrollverfahren zum Geschäftsverwaltungssystem AXIOMA der KESB konnte mit dem durchgeführten Audit zum Abschluss gebracht werden (s. 3). Die Mehrzahl der neu eingegangenen Projekte konnten behandelt werden. Die angestrebten Reaktionszeiten wurden jedoch in der Mehrzahl der Antworten überschritten.

(Zu den ebenfalls einer Vorabkontrolle unterstellten Videoüberwachungen s. 4).

6 Ansichtsäusserungen, Praxis

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

- Wenn ein Krankenversicherer bei einem Spital eine Wirtschaftlichkeitsprüfung durchführen will und dabei ausführlichere medizinische Unterlagen zur retrospektiven Stichprobenprüfung anfordert, ist dies grundsätzlich datenschutzrechtlich zulässig. Das Vorgehen ist durch eine genügende gesetzliche Grundlage abgestützt und durch die bundesgerichtliche Rechtsprechung bestätigt. Der Versicherer kann alle Angaben herausverlangen, welche objektiv erforderlich und geeignet sind, die Wirtschaftlichkeit der Leistungen überprüfen zu können. Dies bedeutet umgekehrt jedoch, dass das Spital nur diejenigen Dokumente einreichen darf und muss, welche für die Prüfung der Wirtschaftlichkeit geeignet und erforderlich sind. Der Versicherer muss das Herausgabebegehren nicht näher begründen und kann seine Prüfung anhand von Stichproben vornehmen. Das Spital ist jedoch berechtigt, die eingeforderten Zusatzangaben an den vertrauensärztlichen Dienst des Versicherers anstatt dem Versicherer direkt weiterzuleiten. Auch die versicherten Personen können eine Herausgabe an den Vertrauensarzt verlangen. Der Versicherer muss die versicherten Personen über diese Wahlmöglichkeit informieren.

- Werden Institutionen mit öffentlicher Aufgabe aufgelöst, stellt sich die Frage nach der weiteren Aufbewahrung der Personendaten. Häufig werden im Auflösungsakt die Aufbewahrungspflichten an den Rechtsnachfolger übergeben. Gibt es keine Nachfolgeinstitution, muss ein Träger für die Aufbewahrung gefunden werden. Regelmässig wird das „Mutter-Gemeinwesen", also diejenige juristische Person, zu der die aufgelöste Behörde gehörte, als Träger eingesetzt. Fehlt auch ein „Mutter-Gemeinwesen“, wird das Einsetzen eines gleichartigen Aufgabenträgers zugelassen. Fehlt es auch an einem gleichartigen Aufgabenträger, ist selbst für Gemeinden eine Übergabe an das Staatsarchiv zulässig.

- Die Aufsichtsstelle fragte bei der GEF nach, ob im Zusammenhang mit der Fusion der Spital Netz Bern AG und des Inselspitals zur Inselgruppe AG der Umgang mit dem Berufsgeheimnis thematisiert worden sei. Sie regte an, die Öffentlichkeit über den Umgang mit der Behandlungsdokumentation zu informieren. Es besteht Übereinstimmung darin, dass die Behandlungsdokumentation von der erstellenden Institution nur mit Zustimmung der behandelten Person an eine neue (d.h. fusionierte) Institution weitergegeben werden darf und dass sich dieses Erfordernis in einer entsprechenden Ausgestaltung der Zugriffsrechte im KIS der Nachfolgeinstitution auszuwirken hat.

- Zeigt eine ehemalige Mitarbeiterin angebliche Missstände einer Kita beim Kantonalen Jugendamt (KJA) als Aufsichtsbehörde an, stellt sich die Frage, wie der Leiterin dieser Kita beim KJA Einsicht in ihre Akten zu gewähren ist. Datenschutzrechtlich ist sichergestellt, dass der Kitaleiterin für sich und für die Kita (juristische Person) Einsicht zu gewähren ist. Zu prüfen sind jedoch überwiegende öffentliche Interessen oder besonders schützenswerte Interessen Dritter, welche der Einsicht entgegenstehen könnten. Zu klären war, ob die Anzeigerin bekannt gegeben werden durfte oder ob besonders schützenswerte Interessen der Bekanntgabe entgegenstanden. Die Gerichtspraxis verneint eine Bekanntgabe dann, wenn erstens an der Anzeige ein öffentliches Interesse besteht, zweitens der Inhalt der Anzeige zutreffend ist und drittens der Anzeigerin Nachteile drohen. Nachteile wären beispielsweise die Ausübung von Gewalt oder Sachbeschädigungen. Kommt man zum Schluss, dass die Anzeigerin nicht bekannt gegeben werden darf, ist zu prüfen, ob ein Schwärzen des Namens ausreichend ist, um ihre Identität zu schützen oder ob ein Schwärzen gewisser Passagen vorgenommen werden muss.

- Eine Privatperson veranlasste die Aufsichtsstelle zu prüfen, ob die kantonale Arbeitslosenkasse für ihre Briefpost an Versicherte Couverts ohne „sprechende Absenderadresse“ verwenden sollte. Die Aufsichtsstelle kam zum Schluss, dass es Situationen gibt, in denen unberechtigte Dritte durch eine Absenderadresse von der Arbeitslosigkeit einer Person erfahren können. Sachverhalte im Bereich der Sozialversicherungen stehen unter dem Sozialversicherungsgeheimnis. Unter diesen Schutz fällt auch die Angabe, dass eine Person arbeitslos ist. Auf Empfehlung der Aufsichtsstelle beschloss die kantonale Arbeitslosenkasse ein neutrales Amtscouvert einzusetzen.

- Privatpersonen reichten verschiedentlich bei der Aufsichtsstelle Einsichtsgesuche in eigene Daten ein. In solchen Fällen ist es Aufgabe der Aufsichtsstelle die gesuchstellenden Personen darauf hinzuweisen, ihre Gesuche direkt bei derjenigen kantonalen, kommunalen oder eidgenössischen Behörden einzureichen, welche die fraglichen Daten bearbeiten. Praktische Hilfe dafür bieten die Musterformulare auf der Website der Aufsichtsstelle und des EDÖB.

- Auf Anfrage der Steuerverwaltung war zu klären, ob für Auskunftsgesuche, die umfangreiche Kopien zur Folge haben, Gebühren erhoben werden dürfen. Die Materialien zur Daten-

schutzgesetzgebung ergaben, dass der Gesetzgeber 2008 keine Ausnahme von der Gebührenfreiheit wollte. Ein rechtsmissbräuchliches Auskunftsgesuch wäre – ohne Gebühr - abzuweisen.

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 zu den Ausführungserlassen zum Bundesgesetz über das elektronische Patientendossier (EPDG) übermittelte die Aufsichtsstelle die Stellungnahme von PRIVATIM.

7.2 Kantonale Erlasse

- Durch das revidierte Personal- und Spitalversorgungsgesetz werden die Haftungsfälle der Listenspitäler, Listengeburtshäuser und Rettungsdienste unter die Zivilgerichtsbarkeit gestellt. Das erhöht das Kostenrisiko für Personen, die eine Staatshaftung aufgrund eines Datenschutzverstosses geltend machen, massiv. Die Aufsichtsstelle geht davon aus, dass Patienten dadurch von einer Klage absehen. Deshalb hat sie angeregt, in diesen Fällen auf einen Parteikostenersatz zu verzichten.

- Zum Entwurf zu einem neuen Landeskirchengesetz unterstützte die Aufsichtsstelle in der Expertengruppe und im Mitbericht eine Einführung eigener unabhängiger Datenschutzaufsichtsstellen für die Landeskirchen. Zur vorgesehenen Datenbekanntgabe über Spitalpatienten an Geistliche der eigenen Landeskirche verlangte sie eine ausnahmslose Zustimmung vor der Bekanntgabe (Opt-In). Die Kirchgemeinden erhalten um-fangreiche Daten über ihre Mitglieder aus den Einwohnerregistern (auch zu Lebenspartner und Kindern). Damit können sie eine Mitgliederverwaltung führen. Die zusätzliche Bekanntgabe von Klassenlisten durch die Schulen, die auch Nicht-Konfessionsangehörige enthalten, ist damit unverhältnismässig.

- Zum Entwurf für ein Justizvollzugsgesetz konnte die Aufsichtsstelle zahlreiche Fragen zu Datenbekanntgaben, Videoüberwachungen, GPS-Anwendungen und Abrufverfahren klären und Präzisierungen insbesondere zur nötigen formell-gesetzlichen Grundlage für Abrufverfahren, zur Beachtung der besonderen Geheimhaltungspflichten und zu Anforderungen an Videoüberwachungen einbringen. Die vorgesehene generelle Überwachung der Besuchsräume ist unverhältnismässig und kollidiert mit anderen Grundrechten. Eine Überwachung darf wie bis anhin nur in begründeten Fällen nach vorgängiger Information erfolgen.

- Der Entwurf zum Polizeigesetz sieht in notstandsähnlichen Fällen eine umfassende Datenübermittlung zwischen Behörden sowie mit Privaten vor. Die Aufsichtsstelle wies auf die Unverhältnismässigkeit und die Gefahr, dass besondere Geheimhaltungspflichten untergraben werden, hin. Schränken polizeiliche Massnahmen – etwa Überwachungen – das Grundrecht auf Datenschutz ein, hat der Rechtsschutz auch im polizeilichen Umfeld sinngemäss den Vorgaben der Strafprozessordnung zu genügen. Für Personensicherheitsprüfungen gegenüber Mitarbeitenden sind die erforderlichen Rechtsgrundlagen zu schaffen. Der vorgesehene Verzicht auf eine Zustimmung des Polizeikommandos zu Videoüberwachungen für kantonale und kommunale Gebäude ist ein Rückschritt. Wirksame Abwehrmittel für die Gemeinden gegen unzulässige Videoüberwachungen durch Private im öffentlichen Raum fehlen nach wie vor. Das systematische Abgleichen elektronisch erfasster Daten über Hotelübernachtungen ist unverhältnismässig.

- Aus dem Präsenzstatus der neuen kantonsweiten Kommunikationslösung Skype for Business können je nach Einstellung Rückschlüsse über das Verhalten der Mitarbeitenden gezogen werden. Die Finanzdirektion stellte im Vorabkontrollverfahren in Aussicht, in der nächsten Revision der Personalverordnung Leitplanken und Rahmenbedingungen aufzunehmen. Mit der Revision 2016 wurde diesem Anliegen noch nicht Rechnung getragen.

8 Aufsichts- und Justizentscheide

8.1 Einsicht in die Watch-Liste

Der Vorsteher des Amts für Justizvollzug (AJV) führte als Bestandteil des internen Risikomanagements eine sog. Watch-Liste. Sämtliche verwahrten Täter sowie andere Risikotäter, die sich zum Zeitpunkt des Delikts, der Gerichtsverhandlung oder bei Vorfällen im Vollzug mit einer ausserordentlichen öffentlichen bzw. medialen Aufmerksamkeit konfrontiert sahen, figurierten darauf. Wer auf der Liste geführt wurde, erhielt Vollzugslockerungen nur mit Zustimmung des Vorstehers.
Ein Betroffener wollte nicht nur Einsicht in seine eigenen Daten sondern in die vollständige, aber anonymisierte Watch-Liste. Nach dem Beschwerdeentscheid der Polizei- und Militärdirektion (POM) muss die Einsicht in fremde, besonders schützenswerte Personendaten gesetzlich vorgesehen sein, bedarf der ausdrücklichen Zustimmung der betroffenen Personen oder muss in deren Interesse liegen. Bei überwiegenden öffentlichen oder besonders schützenswerten

privaten Interessen muss die Bekanntgabe verweigert, eingeschränkt oder mit Auflagen verbunden werden. Ein blosses Abdecken der Namen der Betroffenen reicht zur Verschleierung ihrer Identität nicht aus. Mit den verbleibenden Daten z.B. mit den Tatbeständen der Delikte oder mit den verhängten Sanktionen wäre es möglich, auf die Identität der Betroffenen zu schliessen – insbesondere weil diese in den Medien in Erscheinung traten. Die Watch-Liste hat Auswirkungen darauf, wer in den Entscheid betreffend Vollzugslockerungen eingebunden werden muss und ist kein Arbeitsmittel zum ausschliesslich persönlichen Gebrauch.

8.2 Modalitäten und Umfang des Auskunfts- und Einsichtsrechts

Ein Student der Universität Bern hat Einsicht in sämtliche ihn betreffende Akten der Universität beantragt ohne genauer zu bezeichnen, welche Datensammlungen damit angesprochen sind und wo sich diese befinden. Die Universität verwehrte die Einsicht in gewisse Daten u.a. weil es der Universitätsleitung weder bekannt noch mit zumutbarem Aufwand möglich sei, ausfindig zu machen, welche Korrespondenzen zwischen dem Beschwerdeführer und den einzelnen Organisationseinheiten der Universität bestehen würden.
Nach dem angerufenen Verwaltungsgericht bezieht sich das Auskunfts- und Einsichtsrecht auf Daten, welche in einer Datensammlung bearbeitet werden. Eine Datensammlung ist ein Bestand an Personendaten mehrerer Personen, der so aufgebaut ist, dass die Daten mit vernünftigem Aufwand auffindbar sind. Keine Rolle spielen die Wahl des Speichermediums, die Zweckbestimmung, die Dauerhaftigkeit, die Strukturierung oder die Speichermodalitäten. Auch als Datensammlungen zu qualifizieren sind Datenbestände, die nicht als Datensammlungen angelegt wurden und keine eigene erkennbare Zweckbestimmung aufweisen, die aber nach Personen erschlossen werden können. Eine Datensammlung in diesem Sinn ist auch die Korrespondenz einer Behörde mit einer bestimmten Person.
Ausserdem hat sich die verantwortliche Behörde so zu organisieren, dass sie auch wenig konkretisierten Auskunftsbegehren nachkommen kann. An Auskunfts- oder Einsichtsbegehren sind grundsätzlich keine hohen Anforderungen zu stellen. Insbesondere brauchen sie nicht begründet zu werden und Interessierte können pauschal Auskunft über bzw. Einsicht in alle über sie in den Datensammlungen einer Behörde vorhandenen Daten verlangen. Es ist ausreichend, dass ersichtlich ist, wer die gesuchstellende Person ist und dass sie Auskunft über oder Einsicht in ihre Daten wünscht, die in einer Datensammlung bearbeitet werden. Die gesuchstellende Person ist indes aufgrund des Grundsatzes von Treu und Glauben verpflichtet, soweit möglich und zumutbar konkretisierende Angaben zu machen, welche die Auffindbarkeit der Datensammlungen erleichtern.
Der teilunterlegene Beschwerdeführer hat gegen das Urteil Beschwerde beim Bundesgericht erhoben. Dieses hat die Beschwerde abgewiesen, soweit es darauf eingetreten ist.

8.3 Auf Personaldatensammlungen anwendbares Datenschutzrecht

Auf das Gesuch eines Spitals um Entfernung des Eintrags seiner Personaldatensammlung aus dem Register der Datensammlungen konnte die Aufsichtsstelle aus formellen Gründen nicht eintreten. Dem Gesuch fehlte eine rechtsgültige Unterzeichnung.
Grund des Gesuchs war, dass das Spital gestützt auf ein Gutachten (s. 11.3) der Meinung war, auf das Bearbeiten von Mitarbeiterdaten sei das Bundesdatenschutzgesetz anwendbar. Die Aufsichtsstelle hielt hierzu fest, dass in diesem Fall datenschutzrechtliche Auseinandersetzungen vor den Zivilgerichten auszutragen wären. Etwa bei einem Begehren um Löschung oder Berichtigung von Daten würden sich die Mitarbeitenden neu dem Risiko einer Parteikostenersatzpflicht gegenübersehen. Der Rechtsschutz für arbeitsrechtliche Datenschutzanliegen würde damit umfassend verschlechtert werden. Betroffen wären nicht nur die Mitarbeitenden des Spitals, sondern auch die übrigen Arbeitnehmenden von privatrechtlich organisierten Trägern öffentlicher Aufgaben.

8.4 Zuständige Aufsichtsstelle für die IV-Stelle

Anders als noch im letzten Jahr hielt die sozialrechtliche Abteilung des Bundesgerichts in einem Fall zur Anwendung des Öffentlichkeitsprinzips im Kanton Zürich fest, die IV-Stellen seien der Aufsicht des EDÖB unterstellt. Die Aufsichtsstelle geht nach wie vor von ihrer Zuständigkeit für die IV-Stelle des Kantons Bern aus. Die schwankende Rechtsprechung erschwert jedoch das aufsichtsrechtliche Handeln.

8.5 Aufsichtsrechtliche Überprüfung der Aufzeichnungen von Lesezugriffen auf Steuerdaten

Der Fachbereich Wehrpflichtersatz der kantonalen Wehrpflichtersatzverwaltung hat Zugriff auf die Daten der Steuerverwaltung. Die Zugriffe sind nicht auf die Daten beschränkt, die der Fachbereich für seine Aufgabenerfüllung benötigt. Jedem berechtigten Mitarbeitenden stehen die Daten aller Steuerpflichtigen offen. Abgerufen werden dürfen diese Daten aber nur, wenn die Aufgabenerfüllung dies verlangt. Weil der

Zugriff nicht präventiv beschränkt werden kann, muss die Steuerverwaltung die Zugriffe, bzw. Abrufe der Daten protokollieren. Damit können die Zugriffe im Nachhinein überprüft und bei Missbrauch Massnahmen getroffen werden. Dies kann unter Umständen zum Entzug der Zugriffberechtigung führen.
Die Prüfung der Logdateien ergab, dass ein Mitarbeiter der kantonalen Wehrpflichtersatzverwaltung ohne dienstlichen Anlass auf die Steuerdaten eines ehemaligen Mitarbeiters zugegriffen hatte. Das zuständige Amt für Bevölkerungsschutz, Sport und Militär vernahm den Betroffenen und verwarnte ihn. Zudem wird es die Mitarbeitenden im Rahmen des internen Kontrollsystems erneut auf die Problematik einer sachfremden Nutzung der Fachapplikationen der Steuerverwaltung aufmerksam machen.

8.6 Elektronische Zustellung von Verfügungen der Steuerverwaltung, begründete Empfehlung

Seit dem 1. Januar 2016 erhalten Steuerpflichtige, die sich für die elektronische Zustellung der Rechnungen registrieren, zusammen mit den Steuerrechnungen auch die Veranlagungsverfügungen und -entscheide auf elektronischem Weg. Neu ist, dass die Steuerpflichtigen zwingend auch Veranlagungsverfügungen und Entscheide ins E-Banking-Portal erhalten. Es ist nicht mehr möglich nur die E-Rechnungen auf diesem Weg zu erhalten, die Veranlagungsverfügung (mit Schlussabrechnung) und Entscheide aber auf dem Postweg. Die Aufsichtsstelle wies die Steuerverwaltung darauf hin, dass diese Praxis mit den datenschutzrechtlichen Anforderungen nicht vereinbar ist. Für die elektronische Zustellung der Rechnungen sowie der Verfügungen und Entscheide ist eine je separate freiwillige Zustimmung nötig. Die Aufsichtsstelle ersuchte die Steuerverwaltung mit einer begründeten Empfehlung, eine datenschutzkonforme Wahlmöglichkeit einzuräumen. Eine kombinierte Zustellung von Rechnungen und Verfügungen ohne eine separate Zustimmung ist nur mit einer klaren rechtlichen Grundlage zulässig. Die Steuerverwaltung wies den Antrag mit einer Verfügung ab. Dagegen reichte die Aufsichtsstelle anfangs Mai 2016 bei der Finanzdirektion Verwaltungsbeschwerde ein. Zum Zeitpunkt der Berichterstattung war diese noch hängig.

8.7 Zulässigkeit der Speicherung von Telefonie-Randdaten

Mit Blick auf das Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs hielt das Bundesverwaltungsgericht fest, dieses Gesetz stelle eine genügend bestimmte gesetzliche Grundlage dar, um den durch die Randdatenspeicherung entstehenden erheblichen Grundrechtseingriff zuzulassen (Wer hat an welchem Datum zu welcher Zeit wie lange mit wem telefoniert). Das Urteil befasst sich mit der Randdatenspeicherung durch Anbieterinnen von Fernmeldedienstleistungen. Der Kanton Bern speicherte im Berichtsjahr neu Telefonie-Randdaten in erheblichem Umfang. Dies als Folge einer Standardkonfiguration des Kommunikationssystems Skype for Business. Durch diese wurden die Randdaten automatisch in einem Ordner in der Mailablage der Benutzenden abgespeichert. Weder die für die Anbieterinnen von Fernmeldedienstleistungen vorgegebene Höchstaufbewahrungsdauer von sechs Monaten wurde beachtet, noch bestand eine gesetzliche Grundlage. Dass den mit den Vorgaben zur Randdatenerhebung vertrauten Strafverfolgungsbehörden die Unzulässigkeit dieses Vorgehens zuerst auffallen musste, liegt auf der Hand. Als Datenherrin über die Telefonie-Randdaten der Justiz intervenierte die Justizleitung denn auch beim KAIO. Dieses sollte bei künftigen Projekten aber auch bei allfälligen Konfigurationsänderungen von im Betrieb stehenden Anwendungen der gemeinsamen Grundversorgung die Sicht der für die Datenbearbeitung verantwortlichen Stellen verstärkt einbeziehen.

8.8 Anschaffung eines IMSI-Catchers, begründete Empfehlung

Nicht zuletzt den Ausschreibungsunterlagen war zu entnehmen, dass die Kantonspolizei die Anschaffung eines IMSI-Catchers für CHF 750'000 beabsichtigte. Mit einer begründeten Empfehlung verlangte die Aufsichtsstelle, dass die beabsichtigten Datenbearbeitungen der Aufsichtsstelle zur Vorabkontrolle unterbreitet werden. Aus finanzpolitischen Überlegungen verzichtete die POM daraufhin auf die Anschaffung. Eine ablehnende Verfügung zur begründeten Empfehlung erliess sie nicht.

9 Berichtspunkte der Vorjahre

(3: Nachbetreuungen zu den 2015 vorgenommenen Kontrollhandlungen, 5: Weitergeführte Vorabkontrollen. Auch 2016 ergab eine aufsichtsrechtliche Rückfrage bei einer Direktion, dass nach fünf Fehlversuchen entgegen der 2016 überarbeiteten Passwortweisung keine Sperrung der Eingabemöglichkeit erfolgte.)

10 Antrag

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

30. Januar 2017

Der Datenschutzbeauftragte: *Siegenthaler*

11 Anhang

11.1 Abkürzungen, Bezeichnungen

ABR: Asyl-Bienne-Région (Verein)
AGB ISDS: Vom KAIO für den Umgang mit Outsourcingpartnern herausgegebene, allgemeine Geschäftsbedingungen zu Informatiksicherheit und Datenschutz
ALBA: Alters- und Behindertenamt
Applikation: Informatikanwendung
AXIOMA: Geschäftsverwaltungslösung der CMI Informatik AG
Bedag: Bedag Informatik AG: Die Bedag wurde 1990 gegründet und befindet sich im Eigentum des Kantons Bern
BFH: Berner Fachhochschule
BE-GEVER: Projektname zur Einführung eines Geschäftsverwaltungssystems mit papierloser Geschäftsführung
BEJUNE: Vertragliche Zusammenarbeitsformen zwischen den Kantonen Bern, Jura und Neuenburg
BEKOS: Name des Informatikprojekts zur Koordination der kantonalen pädagogischen und sozialpädagogischen Institutionen der GEF
BYOD: Bring Your Own Device: Bezeichnung dafür, private mobile Endgeräte wie Laptops, Tablets oder Smartphones in die Netzwerke von Unternehmen … zu integrieren (Wikipedia)
Case Management: Fallbetreuung
EDÖB: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
eForms: interaktive Formulare (Informatiklösung der Universität)
EM: Electronic Monitoring: elektronisch überwachte Form des „Hausarrests“ oder des Rayonverbots
EMM: Enterprise Mobility Management (siehe auch MDM)
EPDG: Bundesgesetz über das elektronische Patientendossier
E-Rechnung: elektronische Rechnung
E-Recruiting: Elektronisches Bewerbungsverfahren
ESAP: Projektname für das Projekt zur Ablösung des Finanz- und Personalsystems der BFH und der PH
ESCADA/EVENTO: Projektname der Schulverwaltungslösung der Mittelschulen
EU-Datenschutzreform: Am 14. April 2016 hat das Europäische Parlament der Datenschutzreform zugestimmt. Am 4. Mai 2016 wurden die Datenschutz-Grundverordnung [Verordnung (EU) 2016/679] und die Datenschutz-Richtlinie für Polizei und Strafjustiz [Richtlinie (EU) 2016/680] im Amtsblatt der EU veröffentlicht. Die EU-Mitgliedstaaten haben zwei Jahre Zeit, die Bestimmungen der Richtlinie in nationales Recht umzusetzen (Wikipedia)
Europarats-Konvention 108: Im Jahr 2016 überarbeitetes Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten
FAQ: Frequently Asked Questions, englisch für häufig gestellte Fragen
fmi ag: Spitäler Frutigen, Meiringen, Interlaken
GEF: Gesundheits- und Fürsorgedirektion
GELAN: Abkürzung von Gesamtlösung EDV Landwirtschaft und Natur: Von den Kantonen Bern, Freiburg und Solothurn gemeinsam betriebenes umfassendes Agrarinformationssystem.
GPS-Tracking: Global Positioning System; Tracking: Erfassen des zurückgelegten Wegs
IBAS: Individueller Bedarf Abrechnungs-System
ICT: Information and communications technology: Informations- und Kommunikationstechnik
IMSI-Catcher: IMSI-Catcher sind Geräte, mit denen die auf der Mobilfunkkarte eines Mobiltelefons gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt werden kann. Auch das Mithören von Mobilfunktelefonaten ist möglich (Wikipedia)
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
KESB: Kindes- und Erwachsenenschutzbehörde
KIS: Klinikinformationssystem(e)
Kita: Kindertagesstätte
KWP 2.0: Projektname für das Projekt zur Ablösung der Informatikarbeitsplätze der Kantonsverwaltung (ursprünglich HCP, danach KWP 2017)
MC-SIS: Multi Cancer Screening Information System, gängige Software für Brustkrebs-Früherkennungsprogramme
Mobile computing: Eine Technologie, welche es erlaubt, mittels eines Computers oder anderen kabellosen Geräte, Daten, Stimmen oder Bilder zu übermitteln ohne physisch angeschlossen sein zu müssen. Mobile computing beinhaltet hauptsächlich mobile Kommunikation und mobile Hardware (Wikipedia)
MDM: Mobile-Device-Management: Mobilgeräteverwaltung
NESKO: Neues Steuerkonzept: elektronische Datenverarbeitung auf dem Gebiet der Steuerfestsetzung und des Steuerbezuges
Octosam: OctoSAM Inventory: Softwarewerkzeug der Firma Octosoft, das Computer im Netzwerk inventarisiert und die Nutzung der installierten Softwareprodukte aufzeichnet
Opt-In: von englisch to opt (for something) „optieren“, „sich für etwas entscheiden“ ist ein aus-

drückliches Zustimmungsverfahren aus dem Permission Marketing, bei dem der Endverbraucher Werbekontaktaufnahmen vorher – meist durch eMail, Telefon oder SMS – explizit bestätigen muss (Wikipedia)
Optinomic: Softwarelösung der Optinomic GmbH zum Erfassen, Visualisieren und Analysieren von Daten, die während laufender (Therapie-)Prozesse erhoben werden
PDBBJ: Psychiatrischen Dienste Biel-Seeland – Berner Jura
PHBern: Pädagogische Hochschule
PIS: Personalinformationssystem
PRIVATIM: Vereinigung der Schweizerischen Datenschutzbeauftragten
PZM: Psychiatriezentrum Münsingen
Roundshot-Kamera: Kamera, die 360° Panorama-Bilder liefert
RSE: Regionalspital Emmental AG
Salome Brunner-Stiftung: Sprachheilschulen Wabern, Biel und Langenthal sowie die Heilpädagogische Schule Wabern, rund 150 Mitarbeitende
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
Skype for Business: Nachfolgebezeichnung für die Microsoft Lync Plattform: Anwendung von Microsoft, die verschiedene Kommunikationsmedien (unter anderem IP-Telefonie, Videokonferenz, Voicemail) in einer einheitlichen Anwendungsumgebung zusammenfasst. Anderen Kommunikationsteilnehmern werden Verfügbarkeitsinformationen gegeben (Anwesenheit, während einer bestimmten Zeit unterbleibende Eingaben auf Tastatur und Maus); die Einführung für die Kantonsverwaltung erfolgte unter dem Projektnamen HarmTel
SV: Steuerverwaltung
TerrAudit: Von den Grundbuchbehörden der Kantone Bern, Solothurn, Graubünden und Tessin gegründeter Verein zur interkantonalen und behördenübergreifenden Koordination der Kontrollen von Datenplattformen im Grundbuchbereich
Unicard: Elektronischer Ausweis im Kreditkartenformat, dient Studierenden und Mitarbeitenden als Ausweis. Kann auch als Bibliotheksausweis, Zahlungsmittel oder als Zugangs-Badge eingesetzt werden
UPD: Universitäre Psychiatrische Dienste Bern
ZundL: Zeit- und Leistungserfassung

11.2 Referenznummern der in Ziffer 8 aufgeführten Aufsichts- und Justizentscheide

8.1: Entscheid der Polizei- und Militärdirektion vom 7. September 2016 – BD 260/15 Ho
8.2: Urteil des Verwaltungsgerichts vom 18. April 2016 – 100.2015.204U; Urteil des Bundesgerichts vom 12. August 2016 – 1C_200/20161
8.3: Verfügung der Datenschutzaufsichtsstelle des Kantons Bern vom 27. Januar 2016
8.4: Urteil des Bundesgerichts vom 16. Februar 2016 – 9C_36/2016
8.5: Aufsichtsrechtliche Rückfrage vom 10. März 2016 – 42.72-13.6362
8.6: Verwaltungsbeschwerde vom 4. Mai 2016 – 42.72-15.6279
8.7: Urteil des Bundesverwaltungsgerichts vom 9. November 2016 – A-4941/2014

11.3 Internetadressen und Literaturnachweise

1.3: Medienmitteilung des Bundesrats zur Revision des Bundesdatenschutzgesetzes und zu den Reformen auf europäischer Ebene: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-56764.html
2.3: Geschäftsbericht: http://www.fin.be.ch/fin/de/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html
4: Liz Fischli-Giesser: Private Videoüberwachungen im kommunalen öffentlichen Raum, KPG-Bulletin 3/2016
8.3: Prof. Dr. Astrid Epiney, Zur Abgrenzung des Anwendungsbereichs des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetze, Jusletter vom 2.3.2015: http://doc.rero.ch/record/256921/files/Aufsatz146.pdf