Bericht 2017 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 Erziehungsberatung mit 13 Regionalstellen bearbeitet in erheblichem Mass besonders schützenswerte Daten. Das von ihr bisher eingesetzte Geschäftsverwaltungssystem kontrollierte die Aufsichtsstelle bereits vor einiger Zeit. 2017 wurde das System ersetzt. Die Erziehungsberatung unterbreitete das neue System zur Vorabkontrolle. Eher zufällig stellte die Aufsichtsstelle dabei fest, dass die Erziehungsdirektion die Arbeitsplatzumgebung der Erziehungsberatung – ohne Vorabkontrollverfahren – migriert hatte. Das Umstellen von der bisherigen zur neuen technologischen Umgebung umfasste neben einem Wechsel des Betriebssystems zu Windows 10 auch den Wegfall der bis anhin sicheren, verschlüsselten Netzwerkverbindung. Vom Arbeitsplatzrechner in der Regionalstelle zum Applikationsserver in der Erziehungsdirektion und zurück wurden die Daten damit neu unverschlüsselt übertragen. Weder der Erziehungsberatung noch der Erziehungsdirektion war dies bewusst. Erst auf Intervention der Aufsichtsstelle hin sorgte die Erziehungsdirektion für Abhilfe.

Der Vorfall illustriert, womit sich die Aufsichtsstelle immer wieder konfrontiert sieht: Mit dem Blackbox-Prinzip: Für die Erziehungsberatung sind der Informatikarbeitsplatz und dessen Fähigkeit, Daten-Verbindungen herzustellen (Konnektivität), eine Blackbox. Sie weiss kaum, was in dieser Blackbox geschieht, und sie kann es nur schwer beeinflussen. Die Blackbox ist für sie zudem Zwangskonsum. Das Gleiche gilt für die Informatiklösungen, die den Amtsstellen im Rahmen der IT-Grundversorgung zur Verfügung gestellt werden. Das kantonsweite Geschäftsverwaltungssystem GEVER mit digitaler Archivierung (DGA), die Drucklösung BE-Print, aber auch der kantonale Workplace KWP 2.x oder die Drahtlos-Netzwerk-Lösung sind Beispiele, mit denen sich die Aufsichtsstelle auseinandergesetzt hat. Die Haltung der Amtsstellen zum Blackbox-Prinzip ist unterschiedlich: Während die einen sich von anspruchsvollen Aufgaben entlastet sehen, realisieren die anderen ihren Herrschaftsverlust.

Das Datenschutzgesetz weist die Verantwortung für den Umgang mit den Daten den Amtsstellen zu: Verantwortlich ist diejenige Stelle, die die Daten für ihre Aufgabenerfüllung bearbeitet. Das künftige, an die europäischen Vorgaben angepasste Datenschutzrecht verlangt von den Amtsstellen, dass sie den datenschutzkonformen Ist-Zustand ihrer Datenbearbeitungen nachweisen können. Das wird bedingen, dass den Amtsstellen das Wissen für einen solchen Nachweis auch im Falle einer Blackbox-Lösung zur Verfügung steht.

Die inzwischen mit der neuen ICT-Verordnung getroffene Regelung ist mit diesen Vorgaben unvereinbar: Neu soll die Aufsichtsstelle ihre begründeten Empfehlungen einzig an das für die IT-Grundversorgung zuständige Kantonale Amt für Informatik und Organisation (KAIO) richten. Dies dann, wenn die technische oder organisatorische Ausgestaltung der IT-Grundversorgung Grund für die Empfehlung ist. Die betroffene Amtsstelle sei gar nicht in der Lage, von der Aufsichtsstelle verlangte Anpassungen auszulösen, wird zur Begründung angeführt. Deutlicher könnten die unterschiedlichen Auffassungen zwischen den Befürwortern einer zentralen ICT-Aufgabenerfüllung und der Aufsichtsstelle nicht umschrieben werden.

Das Blackbox-Prinzip ist nicht nur kantonsintern feststellbar: Die Aufsichtsstelle stellt es auch fest, wenn staatliche Stellen ihre Informatikaufgaben in hohem Umfang an externe Dienstleister auslagern, so etwa die Polizei an Swisscom.

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

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) koordiniert die Aufsicht über das Schengener-Informationssystem (SIS). 2017 fand eine Arbeitssitzung statt. Die Aufsichtsstelle führte eine Überprüfung der SIS-Abfragen von 319 Zugriffsberechtigten der Regionalpolizei Berner Oberland durch. Die stichprobenbasierte Kontrolle ergab, dass die Zugriffe rechtmässig waren.

Mitarbeitende der Aufsichtsstelle wirkten in den PRIVATIM-Arbeitsgruppen „Information and Communication Technology“ (ICT), „Gesundheit“ und „Digitale Verwaltung“ mit. Die Arbeitsgruppe Gesundheit befasste sich intensiv mit Fragen des Datenschutzes und der Sicherheit des elektronischen Patientendossiers (EPD). Die vorgesehenen Opt-Out-Bestimmungen (die betroffene Person muss aktiv werden, um eine Datenbekanntgabe zu verhindern) sind problematisch. Sie gewähren den Gesundheitsfachpersonen einen Zugriff auf Daten, obwohl diese für das Erfüllen ihrer Aufgabe nicht nötig sind. Das EPDG verlangt, dass Gesundheitsfachpersonen in Spitälern bis 2020 und in Pflegeheimen bis 2022 über die technische Infrastruktur verfügen um Dokumente im EPD zu lesen. Für die übrigen Gesundheitsfachpersonen und für die Patientinnen und Patienten ist die Verwendung des EPD freiwillig. Ein weiteres Schwerpunktthema war die Qualitätssicherung und -kontrolle im Gesundheitswesen. Verschiedene

Gesundheitsregister werden zu diesem Zweck geführt und aus den gleichen Patientenstammdaten gespeist. Dabei besteht die Gefahr der Verknüpfung ihrer Inhalte. Auch interprofessionelle Peer Reviews können zur Qualitätssicherung und -kontrolle eingesetzt werden. Aufgrund der ungenügenden rechtlichen Grundlage äusserte sich PRIVATIM hierzu kritisch. Die Mitglieder tauschten sich über die nationale Studie zur Durchimpfung von Kindern aus. Der Kanton Bern hatte dazu Vorarbeiten geleistet.
Die Arbeitsgruppe Digitale Verwaltung will ein Arbeitspapier „Digitale Beziehung Einwohnende – Staat“ ausarbeiten.

1.3 Änderungen im übergeordneten Recht, Umsetzung der Motion „Lockerungen im Datenschutz - für Regelungen mit Augenmass“

Auch das kantonale Recht ist an die EU-Datenschutzreform sowie die Modernisierung der Europarats-Konvention 108 anzupassen. Berücksichtigung finden soll zudem der Entwurf zu einem totalrevidierten Bundesgesetz über den Datenschutz. Eine Arbeitsgruppe der Konferenz der Kantonsregierungen erarbeitete einen Leitfaden für die Kantone. Unter der Federführung der Justiz-, Gemeinde- und Kirchendirektion (JGK) erarbeitete eine interne Arbeitsgruppe aus Vertretern der Polizei- und Militärdirektion, der Justizleitung und der Datenschutzaufsichtsstelle eine gesetzesvertretende Verordnung, die auf den 1. August 2018 hin in Kraft treten soll. Die Anliegen der vom Grossen Rat angenommenen Motion 224-2016 Vogt „Lockerungen im Datenschutz - für Regelungen mit Augenmass“ sollen in der folgenden Überarbeitung des Datenschutzgesetzes aufgenommen werden.

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. Administrative Aufgaben kommen dazu. In allen Organisationseinheiten umzusetzende administrative Aufgaben, wie etwa das Ablösen des aktuellen Geschäftsverwaltungs- und Archivierungssystems, oder das Mitwirken in der Betriebskommission binden in einer Kleinstdienststelle einen überproportional grossen Anteil an Personalressourcen. Das Datenschutzgesetz gibt seine 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 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 notwendige Triage sind in der Datenschutzverordnung verankert.

– FAQ: Kommen 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 gewährt 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 Vorgaben wollen die Projektleitungen zum Umsetzen des Datenschutzes im Projekt veranlassen. Dieselbe Wirkung kann erzielt 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 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 von der Kirchlichen Kontaktstelle für Flüchtlingsfragen organisierten Weiterbildungsveranstaltung konnten sich Mitarbeitende der Asylsozialhilfestellen zu Datenschutzanliegen informieren.
Eine Weiterbildungsveranstaltung führten auch die Zivilgerichte für ihr Sekretariatspersonal durch.
Auf Anfrage nahm die Aufsichtsstelle an einer halbjährlichen Sitzung der Vereinigung Berner Kirchenverwalter teil und beantwortete aktuelle Datenschutzfragen.

2.3 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Für die kantonale Verwaltung waren 39 Millionen CHF in Informatikmittel zu investieren. 164 Millionen CHF (davon 128 Millionen CHF für Drittdienstleister) sollte der Betrieb der Informatikmittel kosten (Budgetzahlen 2016). 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 2017 der Betrag von CHF 176'000 zur Verfügung (s. 3).

Sie verfügte über 5.15 Vollstellen (davon 0.2 für das Sekretariat). Ausfälle führten dazu, dass während mehr als 8 Monaten eine 100%-Stelle unbesetzt blieb. Weitere Angaben zu Budget, Rechnung, Erreichen der Ziele (Finanzzahlen) finden sich im Geschäftsbericht 2017 des Kantons Bern (Band I).

3 Kontrollen von Informatikanwendungen, die im Betrieb stehen

Drei Kontrollen wurden im Berichtszeitraum durchgeführt:

- BE-Print; Prüfung der Drucker- und Scannerinfrastruktur

Ein Service der IT-Grundversorgung stellt den Direktionen und der Staatskanzlei die Druckerinfrastruktur zur Verfügung. Technisch umfasst dies Multifunktionsgeräte zum Drucken und Scannen von Dokumenten, sowie die Kommunikationsverbindungen und die Server für den Betrieb der benötigen Applikationen. Mit dem „follow-me-printing“ werden alle Druckaufträge an den in der Bedag gelegenen Printserver geschickt, der diese dann an dasjenige Gerät weitersendet, an dem sich der Benutzende anmeldet und den Druckauftrag auslöst. Beim Scannen wird nach dem Anmelden am Multifunktonsgerät das digitalisierte Dokument an den Scanserver geschickt, der dieses in einen Ordner des Benutzenden ablegt oder an dessen Mailpostfach weiterleitet. Die Prüfung zeigte, dass die vorgegebene verschlüsselte Datenübertragung nicht genügend umgesetzt war. Über das Prüfungsergebnis wurden neben dem Leistungserbringer KAIO auch die betroffenen Direktionen und die Staatskanzlei informiert.

- Grundschutz-Prüfung der IT-Infrastruktur der Kantonspolizei

Bei der komplexen IT-Infrastruktur der Kantonspolizei wurde geprüft, ob die Grundschutzvor-

gaben umgesetzt sind. Die Prüfung soll den Status der ISDS-Konformität für den Betrieb zeigen und somit den Aufwand für künftige Vorabkontrollen verkleinern. Derzeit wird der Auditbericht verfasst und mit der Kantonspolizei abgestimmt.

- Prüfung von Informatikanwendungen der Mittelschulen ESCADA/EVENTO

Die Prüfung hat bereits im Herbst 2016 stattgefunden. Sie hat erhebliche Mängel im Benutzermanagement aufgedeckt. So waren Konten ausgetretener Mitarbeitender immer noch aktiv. Auch die an die Benutzenden zugeteilten Berechtigungen waren nicht korrekt nach dem „need-to-know"-Prinzip vergeben. Dies führt etwa dazu, dass Mitarbeitende einer Schule auf die Schülerdossiers von anderen Schulen Zugriff haben. Nicht umgesetzt waren Datenlöschung und Archivierung. Vorgaben fehlten.

- Prüfung der Cloudanwendungen MS 365 in der Erziehungsdirektion

Die geplante Prüfung musste wegen Verzögerungen beim Erstellen des ISDS-Konzeptes auf Anfang 2018 verschoben werden.

Nachbetreuungen früherer Kontrollen:

- Asyl Biel (ABR)

Die Geschäftsleitung hat aufgrund des Auditberichtes die notwendigen technischen und administrativen Massnahmen eingeleitet. Alle Beteiligten haben einen grossen Effort geleistet um das ambitiöse ISDS-Projekt 2017 abzuschliessen. ABR ist heute in der Lage, die besonders schützenswerten Daten im Migrationsbereich datenschutzkonform zu bearbeiten.

- Klinik Südhang

Die Umsetzung der ausstehenden Pendenzen soll mit der anstehenden Migration erledigt werden. Dies betrifft insbesondere den sicheren Fernzugriff auf Daten.

4 Videoüberwachung

- Mehrere Anlagen des Inselspitals sowie eine Anlage des Betreibungs- und Konkursamtes Bern-Mittelland waren im Vorabkontrollverfahren zu prüfen. Die geplanten Überwachungen erwiesen sich als verhältnismässig. Die Aufsichtsstelle wies das Inselspital und das Kantonsarztamt darauf hin, dass vor einer Auswertung von Bildern mit Patientinnen und Patienten durch die Kantonspolizei das Kantonsarztamt um Entbindung von den Geheimhaltungspflichten zu ersuchen ist. Erneut waren auch Kameras zu beurteilen, die nicht Sicherheitszwecken, sondern logistischen Zwecken oder der medizinischen Überwachung von Patientinnen und Patienten dienen. Solche Überwachungen regelt das Polizeigesetz nicht. Sie dürfen - soweit es die Aufgabenerfüllung erfordert - ausschliesslich als Echtzeitüberwachungen erfolgen. Ausserhalb des Geltungsbereiches des Polizeigesetzes fehlt für Aufzeichnungen eine formellgesetzliche Grundlage. Das Gleiche gilt für Kameras, die zwar aus Sicherheitsgründen, aber nicht „in allgemein zugänglichen" Gebäuden bzw. Räumlichkeiten eingesetzt werden. Das Inselspital verzichtete deshalb auf die geplante Aufzeichnung in einem abends und an den Wochenenden abgeschlossenen Raum.
Die Überwachung des Betreibungs- und Konkursamtes bot Anlass, die Kennzeichnungspflicht zu präzisieren: So sind nur jene Räume mit Hinweisen auf die Videoüberwachung zu versehen, die auch tatsächlich überwacht werden. Da der Gebäudelift überwacht wird, sind zusätzlich zum überwachten Stockwerk sämtliche Lifteingänge mit Kamerahinweisen zu versehen, nicht aber der nicht überwachte Haupteingang.

-Kamera zur Überwachung von Rauchemissionen

Der Einsatz von Überwachungskameras zur Aufzeichnung von möglicherweise unerlaubten Rauchemissionen benötigt eine ausdrückliche gesetzliche Grundlage. Da die Betroffenen dem Einsatz der Kameras zustimmen, genügt eine Ergänzung der kantonalen Lufthygieneverordnung.

- Webcams

Nach einer Petition unterbreitete eine Gemeinde der Aufsichtsstelle Fragen zu der von ihr auf dem Schulhaus installierten Webcam. Auf Hinweise der Aufsichtsstelle hin wurde die Webcam neu so eingestellt, dass sich die Bilder von öffentlichen Strassen und Plätzen, von Hauseingängen, Fenstern, privaten Vorplätzen verpixelt präsentierten. Sie konnten nur beschränkt gezoomt und nicht individuell bearbeitet werden. An einer öffentlichen Veranstaltung sicherten die Gemeindeverantwortlichen zudem zu, dass jederzeit zusätzliche Verbesserungswünsche zum Schutz der Privatsphäre berücksichtigt würden.

5 Vorabkontrollen von Informatikprojekten

Die Aufsichtsstelle prüfte erneut eine hohe Anzahl von Informatikprojekten. Im Folgenden werden in nicht abschliessender Aufzählung Beispiele laufender und erledigter Vorabkontrollen des Berichtsjahres aufgeführt.

5.1 Laufende Vorabkontrollen

-TREE2, Informatikanwendung der Universität Bern für ein sozialwissenschaftliches Forschungsprojekt, das die Transitionen Jugendli-

cher von der obligatorischen Schule in die nachobligatorische Ausbildung und ins Erwerbsleben untersucht. In einer ersten Stellungnahme der Aufsichtsstelle wurden die Verantwortlichen aufgefordert, die nötigen Anpassungen in den einzelnen Prüfbereichen des ISDS-Konzepts anzubringen bzw. umzusetzen.

-Axioma Erziehungsberatung: Oft vermittelt die (zu einem späten Zeitpunkt des Vorabkontrollverfahrens mögliche) Vorführung einer Anwendung vor Ort gegenüber der reinen Dokumentenprüfung der Aufsichtsstelle einen besseren Überblick, so auch in diesem Projekt. Noch zu bereinigende Diskussionspunkte ergaben sich in der Frage, ob die Kontaktdaten aller in die Beratungsprozesse involvierten Personen kantonsweit allen Erziehungsberatungsstellen offen stehen dürfen, sowie betreffend Nachvollziehbarkeit des Verwaltungshandelns, wenn die Dossiers nur elektronisch, also „papierlos“ geführt werden. (s. 1. 1)

-BEJUNE, Applikation zur Datenbearbeitung in der krebsdiagnostischen Früherkennung (Mammografie) im Berner Jura sowie in den Kantonen Jura und Neuenburg: Nach einer ersten Stellungnahme der Aufsichtsstelle im Jahr 2016 befinden sich die nachgebesserten ISDS-Unterlagen für letzte Klärungen in einer weiteren Vorabkontroll-Phase.

-IBAS, Abrechnungssystem der GEF im Bereich Menschen mit Behinderung: Die Inbetriebnahme des Systems ist für Anfang 2019 geplant. Nach einer ersten Stellungnahme wurde der Aufsichtsstelle mitgeteilt, dass die ISDS-Dokumente nach dem Zuschlag für die Realisierung des Projekts an die betreffende Firma nochmals überarbeitet und die bereits erteilten Hinweise der Aufsichtsstelle einbezogen würden.

-Die BFH aktualisierte ihr Betriebssystem auf Windows 10 und installierte Microsoft Office 365 lokal. Die Funktionsweise des cloudbasierten Office 365 bzw. die Prüfung, ob die ISDS-Vorgaben eingehalten werden, setzt hohes Fachwissen voraus und ist ressourcenintensiv. Es erfolgte eine erste, auf Informationssicherheitsaspekte fokussierte Prüfung der Unterlagen durch die Aufsichtsstelle. Die BFH muss zahlreiche Informationen wie Aussagen über die Transportverschlüsselung, Authentisierung, Integrität und Löschung in die ISDS-Unterlagen einarbeiten.

-Der beantwortete Fragekatalog zur Funktionsweise des KIS der UPD liegt der Aufsichtsstelle zur Prüfung vor. Ebenso die komplett überarbeitete Dokumentation der Grundsätze für das Rollen- und Berechtigungskonzept. Der Handlungsbedarf betreffend Einsehbarkeit der Leseprotokollierung (Rückbau auf die hierzu Berechtigten mit Kontrollaufgaben) wird noch adressiert werden.

-Die Ausgestaltung der Benutzerberechtigungen der Assistenzärzte, gab Anlass zum Meinungsaustausch mit der RSE AG. Sie leisten in beiden RSE-Spitälern (Nacht-)Dienste und verfügen deshalb über äusserst breite Berechtigungen. Die datenschutzrechtlich gebotene Einschränkung muss nun geprüft werden, zusammen mit den Rückmeldungen zum Handling der Daten über exponierte Personen (VIP).

-Auch beim KIS der fmi ag ist der Umgang mit VIP noch datenschutzrechtlich zu beurteilen. An einer Vorortbesprechung im Spital Interlaken (fmi ag) wurde zudem intensiv über die auftragsgesteuerte Berechtigungsvergabe für Querschnittsdisziplinen (wie etwa die Physiotherapie oder die Ernährungsberatung) diskutiert. Die fmi ag lieferte in der Folge einen Lösungsvorschlag mittels „Alerts“ (Warnhinweisen). So soll die Krankengeschichte eines Patienten für die Ernährungsberaterin erst abrufbar sein, nachdem die behandelnde Ärztin ein „Alert“ ausgelöst hat, d.h. die Alertfunktion ist so etwas wie eine Anmeldung, welche die Krankengeschichte für die Ernährungsberaterin freischaltet. Eine globale Berechtigung der Ernährungsberaterin auf alle Daten von Patientinnen und Patienten des Spitals läuft dem Grundsatz der Verhältnismässigkeit zuwider, da sie nur bei einem Bruchteil der hospitalisierten Personen tätig werden muss.

-Die Verantwortlichen der SRO AG haben nach einem Personalwechsel die ISDS-Dokumentation des KIS grundsätzlich überarbeitet. Im Berichtsjahr fand deshalb erneut eine Besprechung der noch offenen Punkte inklusive Demonstration statt und die daraufhin überarbeiteten Dokumente liegen zur Prüfung vor. Mit Nachdruck hat die Aufsichtsstelle die Erledigung der bisher unbearbeitet gebliebenen informationssicherheitsrelevanten Pendenzen eingefordert.

-ERP strategische Grundsatzentscheide

Die Aufsichtsstelle hat beim Entscheid zu den strategischen Grundsatzfragen und zur Freigabe der Konzepthase für das Projekt Enterprise Resource Planning (ERP) zur Kenntnis genommen, dass das nötige ISDS-Konzept in der Konzeptphase erarbeitet wird.

- Electronic Monitoring EM

Gestützt auf Bundesrecht ermöglicht die Applikation Electronic Monitoring (EM), freiheitsentziehende strafrechtliche Sanktionen für Erwachsene und Jugendliche sowie ambulante Massnahmen (wie bspw. Hausarrest) elektronisch zu überwachen. Sämtliche erhobenen Daten sind

besonders schützenswert. Der Kanton Bern hat sich inzwischen der Lösung des Kantons Zürich angeschlossen. Ergebnisse der ersten Vorabkontrolle von 2016 wurden für das Überarbeiten der Unterlagen berücksichtigt. Nach wie vor offen sind u.a. die verhältnismässige Anwendung des GPS-Trackings, die Kriterien für eine mögliche Echtzeitüberwachung, die Aufbewahrung und Vernichtung der erhobenen Daten sowie die Beschränkung des Zugriffs des externen Softwarelieferanten.

-Geschäftsverwaltungssystem BE-GEVER DGA

Das Projekt BE-GEVER DGA bildet Teil der IT-Grundversorgung. In der Vorabkontrolle des Konzernkonzeptes (Bericht 2016) 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. Hierzu hat die Aufsichtsstelle gegenüber der Staatskanzlei (Pilotbetrieb) eine begründete Empfehlung abgegeben. Die ablehnende Verfügung der Staatskanzlei hat sie mit Verwaltungsgerichtsbeschwerde angefochten (8.1). Gleiches gilt für den ohne Vorabkontrollverfahren aufgenommenen Betrieb von BE-GEVER DGA im Generalsekretariat der Finanzdirektion, in der Finanzverwaltung, der Steuerverwaltung und im Personalamt.

-Die Mandanten (Direktionen oder deren Organisationseinheiten) sollen die Zugriffsberechtigungen - auch direktionsübergreifend - zuteilen können. Sollen Sicherheitslücken vermieden werden, setzt dies eine kantonsweit gültige Klassifizierung voraus. Wie sich deren Fehlen auswirkt, wird bei der Behandlung der inzwischen eingereichten ersten Mandantenkonzepte zu prüfen sein. Die Ausgestaltung der internen Zugriffsrechte und die Aufbewahrungsdauer für Dokumente und Logfiles werden einen weiteren Hauptschwerpunkt der Prüfung bilden.

-Arbeitsplatz KWP 2.x

Die Verwaltung soll mit neuen Arbeitsplätzen (Clients) ausgerüstet werden, basierend auf dem Betriebssystem Windows 10. Es werden stationäre und vor allem mobile Geräte zum Einsatz kommen. Nach einer ersten Prüfung des ISDS-Konzeptes hat die Aufsichtsstelle u.a. festgestellt,

-dass die Geräte erhöhte Anforderungen erfüllen müssen, damit besonders schützenswerte Personendaten bearbeitet werden dürfen, und

-dass die Konnektivität der Geräte einzubeziehen ist.

Die Gerätekonfigurationen müssen in „Standardimages“ festgelegt, umgesetzt und überwacht werden können. Hierzu ist ein Standard festzulegen (best practices). Die Prozesse für die Installation von Sicherheits- und Supportupdates sind zu dokumentieren und umzusetzen. Die Aufsichtsstelle hat ihre Empfehlungen an das KAIO weitergegeben. Die Vorabkontrolle konnte noch nicht abgeschlossen werden, da das KAIO das Projekt erweitert hat.

-BEKOS

Das Informatikprojekt zur Koordination der kantonalen pädagogischen und sozialpädagogischen Institutionen der GEF beinhaltet die Harmonisierung der IT-Infrastruktur inkl. Kommunikation und Basissoftware für Unterrichtsbetrieb und Administration. Bei der Vorabkontrolle der eingereichten ISDS-Unterlagen wurden erhebliche konzeptionelle und technische Lücken aufgedeckt. Obschon die Aufsichtsstelle das Erstellen eines prüfbaren ISDS-Konzeptes aktiv unterstützt hat, wurde bis anhin kein ISDS-Konzept zur Prüfung vorgelegt.

-Verselbständigung der Psychiatrischen Kliniken:

Per 1. Januar 2017 wurden die drei Psychiatrischen Kliniken verselbständigt. Sie unterstehen ungeachtet ihrer neuen Rechtsform aber weiterhin dem Datenschutzgesetz. Aus technischer Sicht bedeutet die Verselbständigung, dass die kantonalen IT-Dienstleistungen, wie z. B. Mail und Web, aber auch betriebskritische Rechenzentrumsdienste, nicht mehr zur Verfügung stehen und dafür die eigene IT-Infrastruktur aufresp. ausgebaut werden muss. Entgegen dem Vorschlag der Aufsichtsstelle entschieden sich die Kliniken, ein ISDS-Konzept pro Standort zu erstellen. Dieses muss auf die besonderen Risiken des psychiatrischen Umfeldes abgestimmt sein und einen angemessenen Grundschutz beschreiben. Damit soll der Aufwand für die Vorabkontrolle der Applikationen wesentlich verringert werden. Bis zum Berichtszeitpunkt haben die SPJBB ein ISDS-Konzept zur Prüfung eingereicht.

5.2 Abgeschlossene Vorabkontrollen

Folgende Vorabkontrollverfahren konnten abgeschlossen werden:

- GELAN 2015, neues Agrarinformationssystem der Kantone Bern, Freiburg und Solothurn;
- PERSISKA Update, zentrales Personalinformationssystem des Kantons Bern;
- Snagit, Konzernapplikation des KAIO zur Erstellung und Verbesserung von Screenshots (Bildschirmfotos und Videos);
- Optinomic, Applikation des Kompetenzzentrums für Mensch und Sucht, Südhang;
- Kreditorenworkflow Universität Bern;
- CASEnet PH Bern, Applikation für die Abwicklung des Case Management für Lehrpersonen der Pädagogischen Hochschule Bern;

- PIS PZM, Informatiksystem für das Personal- und Gehaltswesen des Psychiatriezentrums Münsingen;
- KSL, Kernsystem Lehre der Universität Bern, Gesamtapplikation für die elektronische Prüfungsverwaltung, das elektronische Vorlesungsverzeichnis und die Hörraumverwaltung;
- BIHAM Universität Bern, Webapplikation zur Verwaltung der Hausarztpraktika (summarische datenschutzrechtliche Prüfung, Verzicht auf Informationssicherheitsprüfung);
- Beratungs- und Reportingtool MVB BE, Digitalisierung der Geschäftsprozesse (Personal- und Adressverwaltung, Stammdaten, Kundenberatung) der Mütter- und Väterberatung;
- KSML Portal, kantonale Stellenmarkt-Applikation für Lehrerinnen und Lehrer (summarische datenschutzrechtliche Prüfung).
- Die Vorabkontrolle zum KIS der PZM AG konnte nach der Bestätigung des Softwareanbieters, dass Löschprotokolle keine personenbezogenen medizinischen Daten des Patienten enthalten (andernfalls wird das Recht auf Vergessen verletzt), abgeschlossen werden. Bei der Löschprotokollierung handelt es sich damit aufgrund der Persönlichkeitsrechtsüberlegungen nicht um ein im technischen Sinn detailliertes Protokoll, sondern eher um ein „Plausibilitäts-Löschprotokoll". Anders ausgedrückt darf das Löschprotokoll (oder „dahinterliegende Tabellen") nicht so detailliert sein (d.h. Patientendaten enthalten), dass damit das Löschen unterlaufen wird.
- Enterprise Mobility Management EMM (der IT-Grundversorgung und der Kantonspolizei)
Die Vorabkontrolle des Projektes zur Realisierung eines Enterprise Mobility Management (EMM) zur Verwaltung mobiler Geräte wurde abgeschlossen. Der Betrieb der Verwaltungssoftware wurde an die Swisscom AG ausgelagert. Die Kantonspolizei hat ein ähnliches Projekt vorabkontrollieren lassen.
- OSIV der IV-Stelle
Hält sich eine Verwaltungsstelle für unzuständig, leitet sie das Geschäft an die zuständige Stelle weiter. Da das Datenschutzrecht des Bundes kein dem Vorabkontrollverfahren entsprechendes Verfahren kennt, war ein Weiterleiten an den EDÖB nicht möglich. Dies nachdem die IV-Stelle erste Aktivitäten zur Durchführung eines Vorabkontrollverfahren ihres zu erneuernden Geschäftsverwaltungssystems OSIV eingeleitet hatte. Die schwankende Rechtsprechung des Bundesgerichts zur Zuständigkeitsfrage verbietet es der Aufsichtsstelle, Ressourcen dort einzusetzen, wo ihr – insbesondere mit Blick auf eine begründete Empfehlung – ihre Unzuständigkeit entgegengehalten werden kann.

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

6 Ansichtsäusserungen, Praxis

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

- Um allfällige Ansprüche des Konkubinatspartners der Verstorbenen prüfen zu können, verlangte ein Sozialdienst vom Erbschafts- und Siegelungsdienst der Gemeinde die Herausgabe der relevanten Stellen des Testaments. In ihrer Ansichtsäusserung gegenüber der kommunalen Aufsichtsstelle gelangte die Aufsichtsstelle zum Schluss, das Sozialhilfegesetz biete eine hinreichende gesetzliche Grundlage für diese Bekanntgabe.

- Mitarbeitende von Trägerschaften, denen per Leistungsauftrag oder -vereinbarung öffentliche Aufgaben übertragen worden sind, unterstehen dem Amtsgeheimnis. Dies auch dann, wenn die betreffenden Institutionen neu privatrechtlich konstituiert worden sind. Entscheidend für die Qualifikation als Beamter im Sinn des Strafgesetzbuches ist das Ausüben bestimmter Funktionen im Dienst der Öffentlichkeit, nicht die personalrechtliche Ausgestaltung des Dienstverhältnisses.

- Die kantonale GERES-Datenbank wird von den Gemeinden gespeist und vom KAIO gestützt auf das Registerharmonisierungsgesetz betrieben. Die ursprünglich von der Bedag für den Kanton Bern entwickelte GEmeindeREegisterSoftware (GERES) wird seit 2015 vom Verein „GERES-Community", dem 16 Kantone angehören, weiterentwickelt. Sowohl die zuständige Stelle des KAIO als auch Datenschutzbehörden anderer Kantone stellten der Aufsichtsstelle wiederholt rechtliche Fragen zum aktuellen Betrieb und zur Einführung des neuen eCH-Schnittstellenstandards. Die Aufsichtsstelle wies darauf hin, dass in der GERES-Datenbank nur jene Daten bearbeitet werden dürfen, für die eine gesetzliche Grundlage besteht, dass die Zugriffsrechte, insbesondere auf Historisierungen, datenschutzkonform ausgestaltet sein müssen und dass Daten, die von den Gemeinden als nicht mehr registerpflichtig gemeldet werden, innert fünf Jahren zu vernichten sind.

- Ein Coach ersuchte die Aufsichtsstelle, die Wahrung der Vertraulichkeit im Rahmen von arbeitsmarktlichen Massnahmen (AMM) zu prüfen. Er arbeitete als Coach im Auftrag eines privaten Unternehmens, das seinerseits im Auftrag des beco arbeitsmarktliche Massnahmen zur Wiedereingliederung arbeitsloser Personen anbietet. Seine Hinweise veranlassten die Aufsichtsstelle, dem beco Fragen und Verbesse-

rungsvorschläge zur Wahrung der Vertraulichkeit zu unterbreiten. Dies führte zu folgenden Klärungen und Verbesserungen: Ein Einsitz zur Qualitätssicherung erfolgt ausschliesslich bei Bewerbungscoachings (und nicht mehr bei Stabilisierungscoachings) und nur mit vorgängiger Zustimmung der Versicherten. Das Formular für den Schlussbericht enthält neu den Hinweis, dass der Umfang auf das Nötige, für die Wiedereingliederung Zweckmässige zu beschränken ist. Die betroffenen Personen werden von Anfang an über die Berichterstattung an ihre RAV-Personalberatung informiert. Sie können zum Schlussbericht Stellung nehmen und erhalten anschliessend eine Kopie. Mails mit besonders schützenswerten Daten werden neu verschlüsselt übertragen oder die Daten werden auf dem Postweg zugestellt. Die AMM-Anbieter müssen darüber hinaus über ein eigenes Datenschutzreglement und einen Datenschutzverantwortlichen verfügen. Die Anforderungen sind Bestandteil der Verträge des beco mit den Anbietern.

- Ein Hinweis einer Privatperson veranlasste die Aufsichtsstelle zu prüfen, ob die Couverts, welche die Finanzverwaltung des Kantons Bern für das Busseninkasso verwendet, den datenschutzrechtlichen Anforderungen genügen. Dritte konnten der Adressierung entnehmen, dass es sich um ein Busseninkasso handelt. Auf Empfehlung der Aufsichtsstelle wurde die Versandpraxis angepasst und die Couverts mit einem kantonsinternen Kürzel versehen.

- Wiederholt stellten Private Fragen zur Löschung von Einträgen in Polizeiinformationssystemen. Die Fristen dafür sind je nach Sachverhalt und Stand des Verfahrens sehr unterschiedlich und ergeben sich aus den eidgenössischen und kantonalen Gesetzesbestimmungen. Löschungen erfolgen auch in Konstellationen, die für die Betroffenen nachteilige Auswirkungen haben können, - etwa nach einem Freispruch - einzig auf Gesuch hin. Die Aufsichtsstelle klärt jeweils über das Vorgehen und die Rechte auf. Ein Gesuch um Datenvernichtung bedingt regelmässig, dass vorgängig ein Gesuch um Auskunft und Einsicht gestellt wird.

- In einer Gemeinde wehrten sich mehrere hundert Personen mit einer Petition gegen den Bau einer Masthalle. Die Gemeinde gab die Unterschriften den am Bau Interessierten weiter. Die Unterzeichner wurden danach massiv persönlich angegangen. Eine betroffene Person fragte die Aufsichtsstelle deshalb um Rat. Die verfassungsrechtlich garantierte Petitionsfreiheit gibt jeder Person das Recht, Petitionen an Behörden zu richten „ohne Nachteile zu erleiden“. Das Bundesgericht bestätigte, dass die Petitionsfreiheit beinhaltet, „ungehindert Bitten, Vorschläge, Kritiken oder Beschwerden an die Behörden zu richten ohne deswegen Belästigungen oder Rechtsnachteile irgendwelcher Art befürchten zu müssen“. Die Gemeinde ist deshalb verpflichtet, die Angaben vertraulich zu behandeln. Sie darf sie auch nicht für Kontaktaufnahmen verwenden. Als Ausdruck eines politischen Engagements sind die Angaben zudem besonders schützenswerte Daten, die nur gestützt auf eine formell-gesetzliche Grundlage weitergegeben werden dürften. Die Datenweitergabe war somit auch eine Datenschutzverletzung.

- Ein Gastgewerbebetrieb fragte die Aufsichtsstelle, ob Ausweisdokumente von Hotelgästen statt kopiert auch eingescannt werden dürfen. Das Gastgewerbegesetz und die zugehörige Weisung der Volkswirtschaftsdirektion regeln die Gästekontrolle. Die Angaben, welche von den Übernachtungsgästen erhoben werden müssen, sind abschliessend aufgezählt. Es sind dies: Name und Vorname, Wohnadresse, Geburtsdatum und Nationalität. Für die Gästekontrolle dürfen die Gastgewerbebetriebe somit Ausweisdokumente weder kopieren noch scannen. Ob dies im Rahmen des privatrechtlichen Beherbergungsvertrags erlaubt ist, hätte der EDÖB zu klären.

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.

7.2 Kantonale Erlasse

- Im Mitberichtsverfahren zum Baugesetz zur Einführung des elektronischen Baubewilligungs- und Plangenehmigungsverfahren (eBUP) stellte die Aufsichtsstelle fest, dass im Kanton Bern, im Gegensatz zu anderen Kantonen, welche dieses Instrument bereits eingeführt haben, auch das öffentliche Auflageverfahren mit der Publikation aller relevanten Baugesuchsunterlagen im Internet erfolgen soll. Dabei können sich datenschutzrechtliche Fragen ergeben, namentlich wenn die zu veröffentlichenden Personendaten in die Kategorie der besonders schützenswerten Daten fallen. Da die Gesuchstellenden inskünftig keine Wahl mehr zwischen der elektronischen Eingabe und der Papierform haben, sollte die Möglichkeit geschaffen werden, dass bestimmte Gesuchsunterlagen von der Publikation im Internet ausgenommen bzw. durch Unkenntlichmachung der betreffenden Stellen vor einer unbeschränkten Einsichtnahme geschützt werden können.

- Durch eine erste Änderung des Personalgesetzes sollen Haftungsstreitigkeiten bei privaten Organisationen, die im Auftrag des Kantons Leistungen erbringen, neu ausschliesslich der Zivilgerichtsbarkeit unterstellt werden. Die Aufsichtsstelle schlug vor, den Anspruch auf Parteikostenersatz in Haftungsstreitigkeiten nach Datenschutzgesetz bei Listenspitälern, Listengeburtshäusern und Rettungsdiensten im Sinne einer „Gegenausnahme“ auszuschliessen. Dies weil andernfalls das Kostenrisiko für Personen, die eine Staatshaftung aufgrund eines Datenschutzverstosses geltend machen, massiv erhöht wird, so dass diese in vielen Fällen auf Klagen verzichten.

- Die Aufsichtsstelle äusserte sich auch zur zweiten geplanten Revision des Personalgesetzes. Mit dieser sollen die Grundlagen für den Umgang mit Personendaten, die bei der Nutzung der elektronischen Infrastruktur der Verwaltung anfallen, geschaffen werden, beispielswiese bei der Telefonie und beim Gebrauch des Informatikarbeitsplatzes. Die Aufsichtsstelle hatte hierzu mehrfach eine klare Rechtsgrundlage verlangt, etwa bei der Vorabkontrolle zum Projekt zur Harmonisierung der Telefonie. Sie befasste sich mit dem Umstand, dass mit der Aufzeichnung und Auswertung solcher Daten immer auch besonders schützenswerte Daten bearbeitet werden, Personenprofile entstehen und Rückschlüsse auf das Arbeitsverhalten ermöglicht werden. Dies in zunehmend umfangreicherem Mass. Sie prüfte, ob der Entwurf Inhalt, Zweck und Umfang für die damit verbundenen schweren Eingriffe in das Grundrecht auf Datenschutz hinreichend bestimmt regelt und ob die Verhältnismässigkeit gewahrt bleibt.

- Die Aufsichtsstelle wirkte in der Arbeitsgruppe für das Erarbeiten eines neuen Gesetzes über zentrale Personendatensammlungen mit. Das Gesetz soll einerseits das bestehende Gesetz über die Harmonisierung amtlicher Register ablösen und andererseits eine Rechtsgrundlage für den Einbezug weiterer zentraler Personendatensammlungen schaffen. Besonderes Augenmerk widmete die Aufsichtsstelle den Anforderungen an die gesetzliche Grundlage, die für Datenbearbeitungen von besonders schützenswerten Daten im Abrufverfahren erfüllt sein müssen. Die Gesetzgebungsarbeiten werden 2018 weitergeführt.

- Die Aufsichtsstelle wies im Mitberichtsverfahren zur Revision des Gesetzes über die Sozialhilfe darauf hin, dass der Begriff der Anonymisierung bei der Lieferung von Sozialhilfedaten der Trägerschaften und Leistungserbringer an die GEF im Vortrag zu klären sei.

- Mit der Revision der kantonalen Tierseuchenverordnung, werden die Gemeinden Registrierstelle für die Kennzeichnung der Hunde und für ihre Halterinnen und Halter. Die Verordnung regelt den Datenzugriff für Behörden und Private. Sie bestimmt, dass die Liste der Tierschutzorganisationen, Tierheime, Tierärztinnen und Tierärzte mit Einsichts- und Abfragerechten im Internet veröffentlicht wird.

- Die Aufsichtsstelle äusserte sich zur geplanten Verordnung über die Informations- und Telekommunikationstechnik der Verwaltung (ICT-V), welche sich mit der Steuerung und Verantwortung für die IT-Grundversorgung befasst (s. 1.1)

8 Aufsichts- und Justizentscheide

8.1 Begründete Empfehlungen betreffend BE-GEVER DGA Axioma

Das die ganze Kantonsverwaltung betreffende Informatikprojekt BE-GEVER DGA steht seit Frühjahr 2016 bei der Aufsichtsstelle im Vorabkontrollverfahren (s. 5.1). Neben dem sogenannten Konzernkonzept wurden der Aufsichtsstelle auch Muster für künftige Mandanten (Ämter oder Direktionen), unterbreitet. Die Staatskanzlei führte BE-GEVER DGA als Teilprojekt vorzeitig ein. Mit der Einführung erfolgte der Wechsel zum papierlosen Büro. Den digitalen Unterlagen fehlt jedoch ohne Zwei-Faktoren-Authentifizierung und ohne digitale Unterzeichnung die nötige Beweiskraft zum Nachweis des staatlichen Handelns. Die Staatskanzlei lehnte eine begründete Empfehlung der Aufsichtsstelle zur Behebung dieses Mangels ab. Die Aufsichtsstelle erhob dagegen Verwaltungsgerichtsbeschwerde.
Im Berichtsjahr entnahm die Aufsichtsstelle den Newslettern des KAIO, dass die Finanzdirektion als erste Direktion GEVER DGA in allen Ämtern eingeführt habe. Im Wesentlichen mit der gleichen Begründung wie gegenüber der Staatskanzlei formulierte die Aufsichtsstelle zu Handen dieser Ämter (ausser KAIO) als verantwortliche Behörden Empfehlungen mit dem Antrag, die erforderlichen ISDS-Unterlagen innert Frist einzureichen, raschmöglichst dafür zu sorgen, dass die Anmeldung an BE GEVER über eine dem Stand der Technik genügende Zwei-Faktoren-Authentifizierung erfolge, umgehend und bis zur Einführung einer Zwei-Faktoren-Authentifizierung alle Unterlagen, die in BE GEVER eingebunden werden, als digital signierte Unterlagen einzubinden und, soweit den Mitarbeitenden die für ein digitales Signieren erforderlichen technischen Mittel fehlen, bis zur Einführung der Zwei-Faktoren-Authentifizierung ihr Handeln weiterhin papiergebunden zu dokumentieren. Die Finanzdirektion zog die Verfahren an sich, gab den Empfehlungen, soweit es um das Einreichen der ISDS-Unterlagen ging, statt und schob den Entscheid im Übrigen bis

zum rechtskräftigen Urteil des Verwaltungsgerichts zum Teilprojekt GEVER DGA der Staatskanzlei auf. Die Aufsichtsstelle legte auch gegen diese Verfügungen Verwaltungsgerichtsbeschwerden ein.

8.2 Watch-Liste

Ein Strafgefangener verlangte umfassende Einsicht in eine Liste über verwahrte Straftäter sowie „Risikotäter", die eine überdurchschnittliche mediale Aufmerksamkeit auslösten. Der Vorsteher des Amts für Justizvollzug (AJV) führte diese seit 2013. Der Eintrag in der „Watch-Liste" hatte insbesondere zur Folge, dass Vollzugslockerungen nur mit Zustimmung des Vorstehers AJV gewährt werden durften. Dem Gesuchsteller wurde in Bezug auf seine persönlichen Daten Einsicht gewährt, nicht jedoch in anonymisierte Daten anderer Personen, die ebenfalls auf der Liste figurieren. Er gelangte mit der Rüge ans Bundesgericht, die Verweigerung der Einsicht in die Daten der übrigen Gefangenen sei willkürlich.
Das Bundesgericht wies die Beschwerde ab. Die Vorinstanz habe kein Bundesrecht verletzt, indem sie die öffentlichen Interessen am Schutz jener Daten stärker gewichtete als den Informationsanspruch des Beschwerdeführers. Eine Anonymisierung der Namen reiche nicht aus, da aufgrund der Angaben auf der Liste auf die entsprechenden Personen geschlossen werden könne, was insbesondere dem Beschwerdeführer, der sich mit mehreren dieser Personen im Vollzug befinde, möglich wäre. Die Rechtmässigkeit der Watch-Liste brauche nicht geprüft zu werden, da dies ausserhalb des Streitgegenstands liege.
In zwei weiteren Fällen verlangten Gefangene, dass ihre Namen von der Liste gestrichen würden, da die mediale Resonanz nichts über die Gefährlichkeit eines Täters aussage. Das Obergericht entschied hier, die Watch-Liste sei ungeeignet, nicht erforderlich und damit unverhältnismässig. Diese Beurteilung deckte sich im Wesentlichen mit derjenigen der Datenschutzaufsichtsstelle (vgl. Bericht 2016, S. 9f). Die Unterscheidung zwischen Tätern, die ein gewisses Medieninteresse auslösten, und solchen, von denen die Öffentlichkeit keine Kenntnis nehme, sei nicht nachvollziehbar, erkannte das Obergericht. In der Folge schaffte die POM die Liste ab.

8.3 Meldung fehlender Fahrfähigkeit an die Strassenverkehrsbehörde

Zweifelt die IV-Stelle, dass die versicherte Person über die körperliche oder geistige Leistungsfähigkeit verfügt, die zum sicheren Führen von Motorfahrzeugen notwendig ist, kann sie die betreffende Person der zuständigen kantonalen Strassenverkehrsbehörde melden. Die gleiche Befugnis kommt aufgrund des Devolutiveffekts im Verwaltungsbeschwerdeverfahren dem angerufenen Gericht zu. Dies insbesondere in Fällen, in denen sich entsprechende Anzeichen erstmals im Gerichtsverfahren ernsthaft konkretisieren. Die Meldung erfolgte im konkreten Fall durch Zustellung des Urteils an das Strassenverkehrs- und Schifffahrtsamt des Kantons Bern, nachdem die Beschwerdeführerin laut einem Spitalbericht geäussert habe, sie wolle sich oder jemanden anderes schwer verletzen, um Ruhe finden zu können. Innere Stimmen würden ihr u.a. sagen, sie solle im Dunkeln beim Autofahren das Licht ausschalten.

8.4 Einsicht ins Steuerregister

Vom Bundesgericht wie zuvor bereits vom Verwaltungsgericht bekam die Gesuchstellerin Recht, welche Einsicht in die Steuerregisterdaten wohlhabender, aufwandbesteuerter Personen im Berner Oberland verlangte. Beide Instanzen gelangten zum Schluss, dass die bis Ende 2015 geltende Bestimmung des Steuergesetzes anwendbar und im Sinn einer vorbehaltlosen und uneingeschränkten Öffentlichkeit der Steuerregister auszulegen sei. Eine von den betroffenen Personen erwirkte Datensperre entfalte keine Wirkung, zumal die Steuerbehörde zur Bekanntgabe der Daten gesetzlich verpflichtet sei. Zudem handle es sich bei den nachgesuchten Auskünften nicht um besonders schützenswerte Personendaten, weshalb der mit der Bekanntgabe verbundene Eingriff als leicht zu qualifizieren sei. Erst mit dem revidierten Steuergesetzesartikel habe sich der Kanton Bern dafür entschieden, den Auskunftsanspruch künftig vom Nachweis eines wirtschaftlichen Interesses abhängig zu machen.

8.5 Begründete Empfehlung gegen den Zugriff der UPD AG auf Personaldaten

Seit der rechtlichen Verselbständigung per 1. Januar 2017 hat die psychiatrische Institution UPD AG gestützt auf eine Vereinbarung mit dem Kanton Bern einen On-line-Zugriff auf vorbestehende Daten des Personalinformationssystem PERSISKA.Auskunft des Kantons. Der Zugriff ist auf Gehaltsdaten beschränkt, die bis fünf Jahre zurückliegen. Die UPD AG stellte sich nach der Verselbständigung gestützt auf ein Gutachten auf den Standpunkt, dass sie nicht dazu verpflichtet sei, ihre Personaldatensammlung für das Register der kantonalen Datensammlungen anzumelden und ihr Personalinformationssystem einer Vorabkontrolle zuzuführen. Dies weil das Datenschutzgesetz des Bundes zur Anwendung gelange. Der automatisierte elektronische Zugriff auf PERSISKA.Auskunft durch ein privates Unternehmen ist ein Abrufverfahren. Da PERSISKA.Auskunft auch besonders schützenswerte Daten enthält,

darf ein solches Abrufverfahren ausschliesslich gestützt auf eine formell-gesetzliche Grundlage gewährt werden, die hier fehlt. Hinzu kommt, dass das Ausüben der Datenschutzrechte (wie Berichtigen und Vernichten) für die Mitarbeitenden nach dem Datenschutzgesetz des Bundes deutlich erschwert wird, da im Streitfall Zivilgerichte zuständig sind – mit entsprechenden Kostenrisiken. Damit stehen einem weiteren On-line-Zugriff überwiegende öffentliche und private Interessen entgegen. Nach kantonalem Datenschutzgesetz ist die datenbekanntgebende Behörde bei dieser Konstellation verpflichtet, den On-line-Zugriff durch Auskünfte im Einzelfall zu ersetzen. Die Aufsichtsstelle erliess deshalb eine begründete Empfehlung gegenüber dem Personalamt mit einem entsprechenden Antrag.

8.6 Elektronisches Zustellen von Verfügungen der Steuerverwaltung, Entscheid der Finanzdirektion

Seit 2016 ist es für Steuerpflichtige nicht mehr möglich, nur die E-Rechnungen ins E-Banking Portal zu erhalten, die Veranlagungsverfügung sowie Entscheide aber auf dem Postweg. Die Aufsichtsstelle hatte die Steuerverwaltung darauf hingewiesen, dass diese Praxis mit den datenschutzrechtlichen Anforderungen nicht vereinbar sei. Für die elektronische Zustellung der Rechnungen sowie der Verfügungen und Entscheide sei je eine separate freiwillige Zustimmung nötig. Sie ersuchte die Steuerverwaltung mit einer begründeten Empfehlung, eine datenschutzkonforme Wahlmöglichkeit einzuräumen.
Die Steuerverwaltung wies diesen Antrag ab. Dagegen reichte die Aufsichtsstelle bei der Finanzdirektion Verwaltungsbeschwerde ein. Diese wies die Beschwerde ab. Die dagegen von der Aufsichtsstelle erhobene Verwaltungsgerichtsbeschwerde ist hängig.

8.7 Aufsichtsrechtliche Rückfrage zur Weiterverwendung einer Benutzeridentität

Eine Rückfrage bei der Bedag zeigte, dass unter dem Benutzerkürzel eines seit längerer Zeit pensionierten Mitarbeiters eines Amtes noch regelmässig Aktivitäten stattfanden. Auf eine aufsichtsrechtliche Rückfrage hin setzte die Amtsleitung diesem Vorgehen ein Ende. Mit der Berechtigung war es möglich gewesen auf dem Host spezialisierte Auswertungen vorzunehmen. Die dazu erforderliche Ausgestaltung der Zugriffsrechte hatte sich als schwierig erwiesen. Die Zugriffsrechte wurden daher nicht auf die nachfolgenden Personen übertragen. Diese arbeiteten vielmehr unter der Identität des Vorgängers weiter und nahmen auch unter dieser Identität die vom System verlangten Passworterneuerungen vor.

9 Gemeinderechtliche Körperschaften

(s. 2.2, 4, 6, 7, 8.4).

10 Berichtspunkte der Vorjahre

(3: Nachbetreuungen zu den 2016 vorgenommenen Kontrollhandlungen, 5: weitergeführte Vorabkontrollen, 8.2: Gerichtsentscheide zur Zulässigkeit der Watch-Liste 8.6: Entscheid der Finanzdirektion zur Verwaltungsbeschwerde über das elektronische Zustellen von Steuerveranlagungsverfügungen).

11 Antrag

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

12. Januar 2018

Der Datenschutzbeauftragte: *Siegenthaler*

12 Anhang

12.1 Abkürzungen, Bezeichnungen

ABR: Asyl-Bienne-Région (Verein)
AJV: Amt für Justizvollzug
AMM: Arbeitsmarktliche Massnahmen, z. B. Entwickeln und Umsetzen von individuellen Bewerbungsstrategien
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
BE-Print: Vom KAIO als Service der IT-Grundversorgung angebotene Druck- und Scaninfrastruktur
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
DGA: Digitale Archivierung
eCH-Standard: Dokument, das vom Verein eCH angenommen wurde, und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt. Es fallen darunter unter anderem technische Interoperabilitätsstandards, Verfahrensstandards, konzeptionelle Datenmodelle, Format- und Datendefinitionen, Präzisierungen von bestehenden internationalen Standards, Beschreibung von ‚Best Practices', welche neuen eGovernment-Projekten von Nutzen sein können
EDÖB: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EM: Electronic Monitoring: elektronisch überwachte Form des „Hausarrests" oder des Rayonverbots
EMM: Enterprise Mobility Management
EPD: Elektronisches Patientendossier: Sammlung von behandlungsrelevanten Informationen der Patientinnen und Patienten
EPDG: Bundesgesetz über das elektronische Patientendossier
E-Rechnung: elektronische Rechnung
E-Recruiting: Elektronisches Bewerbungsverfahren
ERP: Enterprise Resource Planning: bezeichnet eine Softwarelösung zur Ressourcenplanung eines Unternehmens bzw. einer Organisation
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
follow-me-printing: Druck von Dokumenten, wobei alle Druckaufträge an den Printserver geschickt werden, der diese dann an dasjenige Gerät weitersendet, an dem sich der Benutzende anmeldet und das Drucken auslöst
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
GERES: Informatiklösung zur Verwaltung und Harmonisierung von Personendaten, im Kanton Bern zum Zusammenzug aller Einwohnerkontrolldaten
IBAS: Individueller Bedarf Abrechnungs-System
ICT: Information and communications technology: Informations- und Kommunikationstechnik
IT: Informationstechnologie
ISDS: Informationssicherheit und Datenschutz
IV: Invalidenversicherung
KAIO: Kantonales Amt für Informatik und Organisation
KIS: Klinikinformationssystem(e)
Konnektivität: (engl. Connectivity); in der Informatik für die Art und Weise einer Verbindung, die Fähigkeit, eine Verbindung herzustellen, bzw. die Verbindungsdichte im Netzwerk (nach Wikipedia)
KSL: Kernsystem Lehre: Informatikprogramm der Universität
KSML: Kantonaler Stellenmarkt für Lehrerinnen und Lehrer
KWP 2.x: Projektname für das Projekt zur Ablösung der Informatikarbeitsplätze der Kantonsverwaltung (ursprünglich HCP, danach KWP 2017)

MVB BE: Mütter- und Väterberatung Kanton Bern
Mobile Geräte (computing): Eine Technologie, welche es erlaubt, mittels eines Computers oder anderen kabellosen Geräten, Daten, Stimmen oder Bilder zu übermitteln ohne physisch angeschlossen sein zu müssen. Mobile computing beinhaltet hauptsächlich mobile Kommunikation und mobile Hardware (Wikipedia)
Migration: Umstellung von einer bisherigen zu einer neuen technologischen Umgebung (nach Wikipedia)
MS 365: Eine Kombination bestehend aus Office-Webanwendungen, Serviceleistungen und einem Office-Software-Abonnement (nach Wikipedia)
Opt-In(Out): von englisch to opt (for something) „optieren", „sich für etwas entscheiden" ist ein ausdrückliches Zustimmungsverfahren aus dem Permission Marketing, bei dem der Endverbraucher Werbekontaktaufnahmen vorher – meist durch eMail, Telefon oder SMS – explizit bestätigen muss (Wikipedia). (Beim Opt-Out wird das passive Verhalten des Betroffenen als Zustimmung verstanden. Erst wenn der Betroffene sich aktiv gegen die Datenbearbeitung entscheidet, wird diese aufgegeben.)
Optinomic: Softwarelösung der Optinomic GmbH zum Erfassen, Visualisieren und Analysieren von Daten, die während laufender (Therapie-)Prozesse erhoben werden
OSIV: Open System IV, Informatikanwendung mehrerer IV-Stellen
PHBern: Pädagogische Hochschule
PIS: Personalinformationssystem
PRIVATIM: Konferenz der Schweizerischen Datenschutzbeauftragten
PZM AG: Psychiatriezentrum Münsingen (seit dem 1.1. 2017 als Aktiengesellschaft verselbstständigt)
RAV: Regionales Arbeitsvermittlungszentrum
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
SPJBB: Services psychiatriques Jura bernois - Bienne – Seeland (seit dem 1.1. 2017 als Réseau santé mentale SA verselbständigt)
SV: Steuerverwaltung
TREE2: Hier: Informatikanwendung der Universität Bern für ein sozialwissenschaftliches Forschungsprojekt
UPD AG: Universitäre Psychiatrische Dienste Bern (seit dem 1.1. 2017 als Aktiengesellschaft verselbstständigt)
VIP: Very Important Person, (Prominente), in Verbindung mit Klinikinformationssystemen sind besonders exponierte Personen gemeint, also etwa auch Mitarbeitende der Klinik, die sich dort behandeln lassen

12.2 Referenznummern der in Ziffer 8 aufgeführten Aufsichts- und Justizentscheide

8.1: Begründete Empfehlung vom 9. Januar 2017 42 2016 6365
8.2: Entscheid des Bundesgerichts 1C_111.2017 vom 1. Mai 2017 Beschluss der 2. Strafkammer des Obergerichts vom 10. November 2017: SK 17 228
8.3: Urteil des Verwaltungsgerichts vom 20. Januar 2017 VGE 200.2016.468
8.4: Entscheid des Bundesgerichts 1C-447-449/2016 vom 31. August 2017
8.5: Begründete Empfehlung vom 1. Dezember 2017 42.50-16.6462
8.6: Entscheid des stellvertretenden Finanzdirektors vom 4. April 2017 1301.07.00/16.000063/16.001643/Ca

12.3 Internetadressen und Literaturnachweise

1.3: Motion Vogt 224-2016: http://www.gr.be.ch/gr/de/index/geschaefte/geschaefte/suche/geschaeft.gid-94567e2995974f9c82bfde6720219d41.html
2.3: Geschäftsbericht: http://www.fin.be.ch/fin/de/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html
8.5: 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