

## Bericht 2010 der Datenschutzaufsichtsstelle

### 1 Einleitung

#### 1.1 Auf einen Blick

Rechtsauskünfte, Gesetzgebungsprojekte, aufsichtsrechtliche Eingaben und Kontrollen von bereits in Betrieb stehenden Informatikanwendungen beanspruchten die Aufsichtsstelle 2010. Ein beträchtlicher Teil der Mittel der Aufsichtsstelle floss jedoch in Vorabkontrollen von Informatiksystemen. Informatiksysteme bilden das Datenversorgungssystem der Verwaltung. Ihre technischen Möglichkeiten sind umfassend geworden. Klinikinformationssysteme etwa können Patienten gläsern machen. Regelmässig holen sich Projektverantwortliche mehr Lob, wenn sie die Systembenutzer grosszügig mit Daten eindecken. Nicht selten werden vorgesehene Einschränkungen für die Systemeinführung zusätzlich fallen gelassen. Schranken setzen hier die Datenschutzvorgaben. Dem Grundrecht auf Datenschutz dient es daher, wenn die Aufsichtsstelle künftige Informatiksysteme konsequent in den Blick nimmt.

Bei der Vorabkontrolle der Staatsschutzdatenbank hat sich dies bestätigt: Die im Sommer von der Geschäftsprüfungsdelegation der Eidgenössischen Räte auf Bundesebene festgestellten Strukturprobleme zeigten sich auf kantonaler Ebene bereits bei der Vorabkontrolle vom Frühjahr. Der Nachrichtendienst des Bundes liess das Polizeikommando allerdings im Nachhinein wissen, den Kantonen stehe für ihre Staatsschutzdatenbanken ein Vorabkontrollrecht gar nicht zu. Verkannt wird damit, dass die Vorabkontrolle ein Aufsichtsinstrument ist und das Bundesrecht die kantonalen Aufsichtsrechte ausdrücklich vorbehält.

#### 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 Schengen-Informationssystem. Ergebnisse der Überprüfung des Umgangs der Kantonspolizei mit diesem System (s. 2.4) konnten in den Koordinationssitzungen eingebracht werden. Zum Vertrag mit dem Bund über die von der Kantonspolizei bei Demonstrationen vom Bundeshaus aus eingesetzte Videoüberwachungsanlage holte der EDÖB bei der kantonalen Aufsichtsstelle eine Stellungnahme ein.

PRIVATIM informierte seine Mitglieder u.a. über die Datenerhebung für die Volkszählung 2010 bei Kollektivhaushalten (z.B. Heime und Straf- und Massnahmevollzugseinrichtungen), über neue Entwicklungen im Europarecht und deren Auswirkungen auf das Datenschutzrecht in der Schweiz sowie über die bewährte Praxis bei Vorabkontrollen (s. 4). Für die lateinischsprachigen Kantone wurde eine neue Arbeitsgruppe gebildet. Dieser gehört auch der Kanton Bern an.

Mitarbeiter der Datenschutzaufsichtsstelle wirkten in der Arbeitsgruppe Gesundheit und in der Arbeitsgruppe Information and Communication Technology mit. Letztere dient

## Rapport d'activité 2010 du Bureau pour la surveillance de la protection des données

### 1 Introduction

#### 1.1 2010 en bref

Renseignements juridiques, projets législatifs, requêtes relevant du droit de la surveillance et contrôle d'applications informatiques d'ores et déjà opérationnelles ont mobilisé le Bureau en 2010. Une part considérable des ressources a aussi été consacrée aux contrôles préalables de systèmes informatiques. Les possibilités techniques de ces pourvoyeurs de données administratives sont devenues immenses. Ainsi, un système d'informations cliniques peut rendre les patients transparents. Les responsables de projets décrochent davantage de louanges s'ils fournissent généreusement les utilisateurs en données. Il n'est pas rare non plus que des restrictions prévues soient abandonnées au moment de l'introduction du système. Un examen minutieux par le Bureau ne peut donc que renforcer la garantie du droit fondamental à la protection des données.

Le cas de la banque de données de la protection de l'Etat l'a confirmé: les problèmes structurels que la Délégation des commissions de gestion des Chambres fédérales a relevés durant l'été avaient déjà été constatés au printemps lors du contrôle préalable au niveau cantonal. Le Service de renseignement de la Confédération a toutefois indiqué a posteriori au Commandement de la police que les cantons n'avaient pas le droit de soumettre leurs banques de données de la protection de l'Etat à un tel contrôle. Ce faisant, il a ignoré le fait que le contrôle préalable est un instrument de surveillance et que la législation fédérale réserve expressément le droit des cantons à exercer une surveillance.

#### 1.2 Collaboration avec le préposé fédéral à la protection des données et à la transparence et les commissaires suisses à la protection des données (PRIVATIM)

Le préposé fédéral à la protection des données et à la transparence (PFPDT) coordonne la surveillance du Système d'information Schengen. Les résultats du contrôle portant sur les modalités d'utilisation de ce système par la Police cantonale (cf. ch. 2.4) ont pu être exposés lors des séances de coordination.

Le PFPDT a demandé aux autorités cantonales de surveillance de prendre position sur le contrat passé avec la Confédération à propos de l'installation de vidéosurveillance exploitée depuis le Palais fédéral par la Police cantonale lors de manifestations.

PRIVATIM a informé ses membres sur divers sujets comme la collecte de données destinées au recensement de 2010 auprès de ménages collectifs (p. ex. foyers, établissements d'exécution des peines et des mesures), les derniers développements du droit européen et leurs répercussions sur le droit de la protection des données en Suisse, ou encore la pratique éprouvée des contrôles préalables (cf. ch. 4). Un nouveau groupe de travail a par ailleurs été constitué pour les cantons latins, dont le canton de Berne fait également partie.

dem Austausch zwischen den Informatik-Spezialisten. Ausserdem werden ausgewählte technische Themen aufbereitet. Die Aufsichtsstelle hat sich in dieser Arbeitsgruppe aktiv an der Ausarbeitung einer Checkliste ‚Mobile Security‘ beteiligt. In der Arbeitsgruppe Gesundheit wurde gemeinsam mit dem EDÖB das Merkblatt Austritts- und Operationsberichte überarbeitet.

Im Dezember hat der Bundesrat einen Bericht zum Postulat Lustenberger verabschiedet (Erleichterter Datenaustausch zwischen Bundes- und Kantonsbehörden in ausgewählten Bereichen, insbesondere mit Blick auf den Sozialhilfemissbrauch). Diesen Bericht erstattete eine vom Bund eingesetzte Arbeitsgruppe. Die Aufsichtsstelle vertrat in dieser PRIVATIM. Die Arbeitsgruppe kam zum Schluss, dass der Datenschutz den behördlichen Datenaustausch nicht behindert und bei der Missbrauchsbekämpfung gut ausgebildetes Personal genau so wichtig ist wie der Datenabgleich. Der Bundesrat prüft nun verschiedene Massnahmen wie die Einrichtung einer Datenbank über Sozialversicherungsleistungen.

## **2 Aufgabenumschreibung, Prioritäten, Mittel**

### **2.1 Prioritäten**

Für das Bearbeiten der Geschäfte gilt unverändert folgende Prioritätenfolge: 1. ISDS-Konzepte für Informatikprojekte (Vorabkontrollen), 2. Betreuung beigezogener externer Kontrollstellen, 3. Allgemeine Gesetzgebung vor Spezialerlassen, 4. Generelle Weisungen vor Einzelfällen, 5. Beratung und Instruktion und 6. Einzelprobleme mit vielen Betroffenen vor solchen mit wenig Betroffenen und geringer Wiederholungswahrscheinlichkeit.

Die Informatiksicherheits- und Datenschutzvorgaben (ISDS-Weisungen, Regierungsratsbeschluss 2127/07; s. 3) führen dazu, dass auch für einen Grossteil der in Betrieb stehenden Informatikanwendungen neue ISDS-Konzepte gemacht werden müssen. Nach der Polizeigesetzgebung gilt Gleiches für bestehende Videoüberwachungsanlagen. Es gelang im Berichtsjahr nicht, alle aus dem Vorjahr übernommenen offenen Geschäfte abzuschliessen.

### **2.2 Eigenverantwortung der datenbearbeitenden Stellen**

Bei auffällig vielen Forschungsprojekten gelangten die Verantwortlichen bereits in der Initialisierungsphase an die Aufsichtsstelle. Gleiches gilt für Informatikprojekte (z.B. elektronisches Baubewilligungsverfahren des Amtes für Gemeinden und Raumordnung oder kantonales Krebsregister des Kantonsarztamtes).

Auf deren Initiative hin fand sowohl für die Juristinnen und Juristen der Regierungstatthalterämter als auch für die Mitarbeitenden der Gemeinde Muri-Gümligen eine Datenschuttschulung statt.

Des collaborateurs du Bureau sont membres des groupes de travail "Santé" et "Technologies de l'information et de la communication". Ce dernier est une plate-forme d'échange entre spécialistes de l'informatique qui traite en outre certaines questions techniques de manière approfondie. Le Bureau a participé activement, dans ce contexte, à l'élaboration d'une liste de contrôle "Sécurité mobile". Le groupe de travail "Santé" a quant à lui remanié le feuillet thématique "Lettres de sorties et rapports opératoires" en collaboration avec le PFPDT.

En décembre, le Conseil fédéral a adopté le rapport d'un groupe de travail sur le postulat Lustenberger (échange de données facilité entre autorités fédérales et cantonales dans certains domaines, en particulier sous l'angle des abus de l'aide sociale). Le groupe de travail institué par la Confédération, au sein duquel le Bureau représentait PRIVATIM, était parvenu à la conclusion que la protection des données n'empêche pas les échanges entre autorités et que dans la lutte contre les abus, la qualification du personnel est tout aussi importante que l'harmonisation des données. Le Conseil fédéral examine différentes mesures comme la création d'une banque de données sur les prestations des assurances sociales.

## **2 Description des tâches, priorités, moyens à disposition**

### **2.1 Priorités**

Les dossiers continuent à être traités en fonction des priorités suivantes: 1) les concepts SIPD concernant des projets informatiques (contrôles préalables), 2) le suivi des sociétés d'audit externes mandatées, 3) la législation générale plutôt que la législation spéciale, 4) les directives générales plutôt que les cas particuliers, 5) les conseils et l'instruction, 6) les problèmes concernant un grand nombre de personnes plutôt que ceux touchant quelques rares individus et risquant peu de se reproduire.

L'instruction concernant la sûreté de l'information et la protection des données (consignes SIPD, arrêté du Conseil exécutif 2127/07; cf. ch. 3) requiert l'élaboration de nouveaux concepts SIPD pour la plupart des applications informatiques utilisées. La législation sur la police énonce la même exigence par rapport aux installations de vidéosurveillance existantes. Dans ce domaine, il n'a été possible de liquider qu'une partie des affaires reprises de l'exercice précédent.

### **2.2 Responsabilité propre des services traitant les données**

Il est frappant de constater que les responsables de nombreux projets de recherche se sont adressés au Bureau dès la phase initiale de leurs travaux. Il en est allé de même dans le domaine informatique (p. ex. procédure électronique d'octroi du permis de construire de l'Office des affaires communales et de l'organisation du territoire ou registre cantonal des tumeurs de l'Office du médecin cantonal).

Les juristes des préfectures et le personnel de la commune de Muri-Gümligen ont pu suivre, à leur demande, un cours sur la protection des données.

Solche Schritte zeigen das eigenverantwortliche Bemühen um einen korrekten Umgang mit Personendaten.

### 2.3 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Jahr 2010 waren 43,3 Millionen CHF in Informatikmittel zu

investieren. 190,2 Millionen CHF (davon 97,2 Mio. CHF für Drittdienstleister) sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). In diesen Zahlen sind die Aufwendungen der von der Aufsichtsstelle ebenfalls zu beaufsichtigenden Spitalzentren und des Inselfspitals nicht enthalten.

Für die Prüfung von Informatikanwendungen durch externe Prüfstellen stand der Datenschutzaufsichtsstelle der Betrag von CHF 150'000 zur Verfügung (s. 2.4). Sie verfügte über 3,6 Vollstellen (davon 0,7 für das Sekretariat). Dies nachdem der stellvertretende Datenschutzbeauftragte mit Abschluss seiner Ausbildung zum zertifizierten Informationssystem-Auditor (CISA) seinen Beschäftigungsgrad von 80% auf 90% erhöht hat.

Die für das Aufgabenfeld des IT-Sicherheitsbeauftragten des Kantons vorgesehene Stellenaufstockung begrüsst die Aufsichtsstelle. Auch mit dem neuen Inhaber der Stelle erfolgte - etwa bei der Beurteilung von ISDS-Konzepten - eine gute Zusammenarbeit.

(Zu dem durch das Spitalversorgungsgesetz entstehenden Ressourcenbedarf s. 6.3)

### 2.4 Kontrollen von Informatikdatenbearbeitungen

Vier Prüfungen wurden im Berichtszeitraum ausgelöst:

- In Schulen stellen sich vielseitige Datenschutzfragen. Sie reichen vom Umgang mit Noten, Krankheitsfällen, Wissen über das persönliche Umfeld von Schülern über Website-Angebote bis hin zu Fragen der Informatiksicherheit von Fachanwendungen oder von Rechnern in Arbeitsräumen oder Computerpools. Exemplarisch wurde deshalb das Gymnasium Neufeld für eine Überprüfung ausgewählt. Etwa 40 Verbesserungsmassnahmen wurden vorgeschlagen. Lediglich der fehlende IT-Notfallplan war mit hoher Priorität zu beheben.

- Das von der Kantonspolizei Bern betriebene System ViCLAS (Violent Crime Linkage Analysis System) dient den angeschlossenen Polizeicorps zur Erstellung von psychologischen Täterprofilen. Auch bei scheinbar nicht zusammenhängenden Straftaten kann dank ViCLAS durch übereinstimmende psychologische Täterprofile ein Zusammenhang erkannt werden. Überprüft wurde sowohl die Sicherheit des Informationssystems als auch die Rechtmässigkeit der gespeicherten Datensätze (Stichprobe für den Kanton Bern). Während die Sicherheit des Systems in zahlreichen Punkten verbesserungsfähig war, gab es zur Rechtmässigkeit der gespeicherten Datensätze keine Beanstandungen.

- Die Steuerverwaltung setzt in grosser Zahl Fachapplikationen ein. Um die ISDS-Vorgaben für alle Applikationen in effizienter Weise erfüllen zu können, wurde ein Gesamt-ISDS-Konzept erstellt. Dieses soll alle gemeinsamen Teile der Fachapplikationen abdecken. Ob die verfolgte Methode

De telles démarches attestent d'une volonté d'utiliser les données de manière correcte et responsable.

### 2.3 Rapport entre moyens informatiques et moyens mis à la disposition de la protection et de la sécurité des données

Le budget attribuait CHF 43,3 millions aux investissements dans le domaine informatique, et CHF 190,2 millions à l'exploitation (dont CHF 97,2 mio destinés à des tiers prestataires de services). Ces chiffres ne concernent pas les centres hospitaliers ni l'Hôpital de l'île, également placés sous la surveillance du Bureau.

Pour le contrôle des applications informatiques par des services externes (cf. ch. 2.4), la somme prévue était de CHF 150 000. Le Bureau a disposé de 3,6 postes à temps complet (dont 0,7 pour le secrétariat), le délégué suppléant ayant fait passer son taux d'occupation de 80 à 90 pour cent dès l'obtention de son certificat dans le domaine de l'audit informatique (CISA).

Le Bureau salue l'étoffement de l'effectif prévu dans le domaine relevant du délégué cantonal à la sécurité informatique. Il a pu collaborer de manière fructueuse avec le nouveau titulaire du poste également, en particulier lors de l'évaluation de concepts SIPD.

(Cf. ch. 6.3: nouvelles ressources requises par la loi sur les soins hospitaliers).

### 2.4 Contrôle du traitement de données informatiques

Quatre audits ont été demandés en 2010:

- La question de la protection des données est omniprésente dans les écoles: notes, maladies, informations sur l'entourage personnel des élèves, offres de sites Internet, mais aussi sécurité informatique d'applications spécialisées, présence d'ordinateurs dans les locaux de travail ou encore salles informatiques. Considéré comme représentatif, le gymnase du Neufeld a fait l'objet d'un audit au terme duquel quelque 40 mesures d'amélioration ont été proposées. Seule l'absence de plan d'urgence informatique a toutefois nécessité une intervention immédiate.

- Le système ViCLAS d'analyse des crimes violents exploité par la Police cantonale permet au corps de police de dresser des profils psychologiques de criminels et, partant, d'établir des liens entre des infractions a priori distinctes. L'audit a porté tant sur la sécurité du système d'information que sur la légalité des enregistrements de données (contrôle par sondage pour le canton de Berne). Si ce second aspect n'a pas suscité de remarque particulière, de nombreuses améliorations ont en revanche été proposées dans le but de renforcer la sécurité du système.

- L'Intendance des impôts recourt abondamment à des applications spécialisées. Elle a fait établir un concept SIPD global recouvrant les parties communes à toutes ces applications afin d'être en mesure de satisfaire efficacement aux consignes SIPD pour chacune d'elles. L'audit vise à déterminer si la méthode choisie respecte les prescriptions légales. Il ne s'achèvera toutefois qu'en 2011.

mit den rechtlichen Vorgaben vereinbar ist, ist Gegenstand einer Überprüfung. Diese wird jedoch erst 2011 abgeschlossen.

- Die Überprüfung des Klinikinformationssystems der Spitalzentrum Biel AG musste ins Jahr 2011 verschoben werden. Grund ist die verspätete Einführung des Systems. Zu den Prüfungen im Jahr 2009 (Schengener-Informationssystem SIS, BEWAN-Anmeldeinformationen, Lebensmittelkontrollanwendung Limsophy-Lims, Experten-Notebooks Steuerverwaltung) wurde die Umsetzung der in den jeweiligen Prüfberichten geforderten Massnahmen verfolgt. In allen Fällen wurden die angezeigten Massnahmen umgesetzt oder eingeleitet.

## 2.5 Register der Datensammlungen

Das revidierte Datenschutzgesetz beauftragt die Aufsichtsstelle, ein Internet-Register der Datensammlungen zu führen. Zweck dieses Registers ist es, der Bevölkerung einen Überblick über die behördlichen Datensammlungen zu geben. Das entsprechende Projekt wurde im Berichtsjahr gestartet. Die Erfassung der Datensammlungen in der Register-Applikation wird im ersten Halbjahr 2011 erfolgen, so dass etwa Mitte 2011 mit der Veröffentlichung des Registers gerechnet werden kann.

## 3 Informatiksicherheits-Vorgaben

Das kantonale Amt für Informatik und Organisation (KAIO) hat die Arbeit an einer Direktionsverordnung ISDS, die den bisherigen Regierungsratsbeschluss ablösen soll, vorangetrieben. Widersprüche zwischen dem bisherigen Regierungsratsbeschluss und der revidierten Datenschutzgesetzgebung wurden beseitigt. Die Direktionsverordnung wird im April 2011 in Kraft treten.

## 4 Vorabkontrollen von Informatikprojekten

Die Aufsichtsstelle unterzieht die Methode zur Prüfung der umfangreichen ISDS-Dokumentation von Informationssystemen einer ständigen Optimierung. Neu wurden daher die Kontakte zu den Daten bearbeitenden Stellen durch Besuche vor Ort intensiviert. Die Dokumente werden zudem stets in Zweier-Teams bearbeitet.

Folgende Projekte wurden betreut:

- Das Smartcard-Management-System des KAIO (Verwaltung von Datenträgern zur Identifizierung) wird ersetzt. Die entsprechenden ISDS-Unterlagen konnten einer ersten Prüfung unterzogen werden.
- Das System GELAN ist das Agrarsystem der Kantone Bern, Freiburg und Solothurn. In einer ersten Besprechung der ISDS-Unterlagen wurden diverse Fragen aufgeworfen, die zunächst beantwortet werden müssen. Sobald die Angaben vorliegen, kann die Detailprüfung in Angriff genommen werden.
- Von den Anwendungen der Steuerverwaltung wurden Konzepte eingereicht zu E-VAS GG (Ersatz Veranlagungssystem Grundstückgewinnsteuer) und VA-NP (Veranlagung Natürliche Personen). Die Unterlagen zu E-VAS GG wurden geprüft. Zu beachten war bei diesen Prüfungen stets auch das ISDS-Konzept NESKO. Es wurde

- L'examen du système d'informations cliniques du Centre hospitalier Bienne SA a dû être reporté à 2011 suite aux retards intervenus lors de l'introduction de celui-ci.

La mise en œuvre des mesures exigées dans les rapports des audits effectués en 2009 (Système d'information Schengen [SIS], transmission d'informations sur la connexion au moyen de BEWAN, application Limsophy Lims pour le contrôle des denrées alimentaires, ordinateurs portables des experts fiscaux de l'Intendance des impôts) a donné lieu à une vérification: toutes les mesures ont été réalisées ou sont en voie de l'être.

## 2.5 Registre des fichiers

La loi révisée sur la protection des données charge le Bureau de tenir un registre des fichiers à jour sur Internet. Le but de ce registre est de fournir au public une vue d'ensemble de tous les fichiers établis par les autorités. Le projet a été lancé en 2010, et la saisie des fichiers dans l'application interviendra au cours du premier semestre de 2011, en vue d'une publication au début de l'été.

## 3 Consignes de sécurité informatique

L'Office cantonal d'informatique et d'organisation (OIO) a poursuivi l'élaboration d'une ordonnance de Direction SIPD destinée à remplacer l'arrêté du Conseil-exécutif ad hoc. Les contradictions entre ce dernier et la législation révisée sur la protection des données ont été éliminées, et l'ordonnance doit entrer en vigueur en avril 2011.

## 4. Contrôle préalable de projets informatiques

Le Bureau ne cesse d'optimiser sa méthode d'examen de la vaste documentation SIPD afférente à chaque système informatique. Ainsi, il a récemment intensifié ses contacts avec les services traitant les données en organisant des visites sur place. De plus, les documents sont toujours examinés par une équipe de deux personnes.

Le Bureau a suivi les projets ci-dessous:

- Le système de gestion des cartes à puce de l'OIO (administration de supports de données à des fins d'identification) doit être remplacé. Le dossier SIPD a fait l'objet d'un premier examen.
- GELAN est un système d'information agricole commun aux cantons de Berne, de Fribourg et de Soleure. Diverses questions ont été soulevées lors d'un premier entretien consacré au dossier SIPD. L'examen de détail pourra débuter une fois que les précisions requises auront été apportées.
- Deux concepts concernant des applications de l'Intendance des impôts ont été soumis au Bureau: E-VAS GG (remplacement du système de taxation de l'impôt sur les gains immobiliers) et VA-NP (taxation des personnes physiques). Le Bureau a examiné les documents concernant E-VAS GG, en relation avec le concept SIPD de NESKO.

- mehrfach mit der Steuerverwaltung besprochen und bildete auch Gegenstand einer Prüfung durch eine externe Kontrollstelle (s. 2.4).
- Das Projekt eRecruiting von beco und der Berner Fach Hochschule sieht eine elektronische Unterstützung aller Schritte einer Stellenbesetzung vor. Die Vorabkontrolle ergab einen positiven Gesamteindruck und lediglich Detailanmerkungen.
  - Die ISDS-Unterlagen zu Persiska (Gehalt auszahungssystem) wurden aktualisiert. Darin integriert wurden die Unterlagen zu den elektronischen Unfallmeldungen.
  - Die Prüfung des Dokumentenmanagementsystems des Personalamts und des KAIO konnte dank dem Engagement der Verantwortlichen in verhältnismässig kurzer Zeit abgeschlossen werden. Offen sind – wie auch in anderen Projekten - noch Fragen der elektronischen Archivierung.
  - Insgesamt vier Informatikprojekte der Universität befanden sich in unterschiedlichen Prüfphasen: Für das System UNICARD erging eine erste, für das Kernsystem Lehre (KSL) eine zweite Stellungnahme mit Nachbesserungsvorschlägen. Die überarbeiteten ISDS-Unterlagen eines Krankheitsregisters des Instituts für Sozial- und Präventivmedizin lagen für eine zweite Stellungnahme vor. Zum IDES Implantatregister (Forschungsprojekt) des Instituts für Evaluative Forschung in der orthopädischen Chirurgie konnte die Aufsichtsstelle einen abschliessenden Prüfbericht abgeben.
  - Die Vorabkontrolle des System PACS (Bildarchivsystem) der SRO AG (Spital Region Oberaargau) konnte abgeschlossen werden.
  - Auf Antrag der SRO AG erging im (Teil-)Vorabkontrollverfahren für das Klinikinformationssystem kiSro eine begründete Empfehlung zum Benutzerberechtigungskonzept. Die SRO AG lehnte diese im Dezember mit Verfügung ab. Ob die Aufsichtsstelle gegen diese Verfügung bei der Gesundheits- und Fürsorgedirektion Beschwerde erhebt, war im Berichtszeitraum noch offen.
  - Zum Informatikprojekt ELA\_DMS (elektronisches Archiv) der Spitäler fmi ag (Frutigen, Meiringen, Interlaken) erging eine erste Stellungnahme. Eine spitalinternen Dokumentenspermmöglichkeit für Patienten muss noch geschaffen und die endgültige Löschung der elektronischen Archivdaten umgesetzt werden.
  - Die 92'444 Datenfeldzuordnungen umfassende Berechtigungsmatrix des Klinikinformationssystems des Inselspitals (i-pdos) konnte aufgrund ihres Umfangs nicht vollständig überprüft werden. Die Aufsichtsstelle beschränkte sich auf eine Prüfung der Gruppierungsmethoden und untersuchte besonders exponierte Stellen genauer. Die ersten Prüfungshandlungen ergaben insbesondere, dass der Suchverlauf zu offen gestaltet ist und dass die abgeschlossenen Fälle nicht inaktiv gesetzt werden können. Zudem blieben Fragen zur Rollenvergabe offen. Diese Punkte müssen bis Mitte 2011 nachgebessert werden.
  - Die Spitalnetz Bern AG nahm ihr Klinikinformationssystem ungeachtet der Hinweise der Aufsichtsstelle auf die deutlich zu weit gehenden Zugriffsmöglichkeiten in Betrieb. Zu weit waren die Zugriffe in dem aus mehreren Spitälern zusammengesetzten Spitalnetz sowohl mit Blick auf die Funktion, die Organisationseinheiten (klinikübergreifende
- Plusieurs entretiens ont eu lieu avec l'Intendance des impôts, et ce concept a pour sa part également fait l'objet d'un audit externe (cf. ch. 2.4).
  - Le projet eRecruiting du beco et de la Haute école spécialisée bernoise prévoit un soutien électronique tout au long des étapes de recrutement. L'impression générale était positive au terme du contrôle préalable, et seules quelques remarques de détail ont été formulées.
  - Le dossier SIPD concernant PERSISKA (système de versement des traitements) a été actualisé. Il inclut désormais la documentation relative aux déclarations électroniques d'accident.
  - Grâce à l'engagement des responsables, le système de gestion des documents de l'Office du personnel et de l'OIO a pu être examiné dans un laps de temps assez bref. Comme pour d'autres projets, certaines questions relatives à l'archivage électronique subsistent toutefois.
  - Quatre projets informatiques de l'Université ont été examinés, à des stades divers. Le Bureau a remis une première prise de position au sujet du système UNICARD et une deuxième à propos de l'application Kernsystem Lehre (KSL), toutes deux assorties de propositions d'amélioration. Il s'apprête à préavisser pour la deuxième fois le dossier SIPD remanié concernant le registre des maladies de l'Institut de médecine sociale et préventive, et a pu rendre un rapport d'examen complet sur le registre des implants IDES (projet de recherche) de l'Institut de recherche évaluative en chirurgie orthopédique.
  - Le contrôle préalable du système PACS d'archivage des images du centre hospitalier régional de Haute-Argovie (CHR SRO AG) a pu être achevé.
  - A la demande du CHR SRO AG, le Bureau a formulé, dans le cadre d'un contrôle préalable partiel, des recommandations motivées sur le concept des autorisations du système d'informations cliniques kiSro. Le CHR SRO AG les a toutefois rejetées par voie de décision en décembre. La question d'un éventuel recours du Bureau devant la Direction de la santé publique et de la prévoyance sociale était encore en suspens à la fin de l'année.
  - Le projet informatique ELA\_DMS (archivage électronique) du CHR Spitalier FMI AG (Frutigen, Meiringen et Interlaken) a fait l'objet d'une première prise de position. Il y a encore lieu d'offrir aux patients une possibilité de blocage interne et de prévoir la radiation définitive des données archivées sous forme électronique.
  - Il n'a pas été possible de procéder à l'examen intégral de la matrice des droits d'accès au système d'informations cliniques DEP de l'Hôpital de l'Île, qui attribue pas moins de 92 444 champs de données aux utilisateurs. Le Bureau s'est contenté d'examiner les méthodes de regroupement, et s'est par ailleurs concentré sur les points particulièrement sensibles. Il s'est d'ores et déjà avéré que les possibilités de recherche sont trop larges, et que les dossiers clos ne peuvent pas être désactivés. De plus, des questions relatives à l'attribution des rôles sont restées en suspens. Toutes les corrections requises doivent être apportées d'ici à la mi-2011.
  - Le Spitalnetz Bern (SNB) AG – qui regroupe plusieurs hôpitaux – a commencé à exploiter son système d'informations cliniques sans tenir compte de la mise en garde

Zugriffe) als auch die Spitäler (standortübergreifende Zugriffe). Die Aufsichtsstelle wies darauf hin, dass derart weit gefasste Zugriffsrechte auch strafrechtlich relevant sein können (Verletzung des Amts- und des Berufsgeheimnisses). Die SNB AG ist nun daran, die Zugriffsrechte datenschutzkonform einzugrenzen. Damit konnte auch die zweite Tranche des vom Grossen Rat bewilligten Beitrags freigegeben werden.

- Die ISDS-Unterlagen der Patientenverwaltungslösung OPALÉ der Psychiatrischen Dienste Biel-Seeland – Berner Jura Bellelay liegen vor.
- Zur Prüfung stehen auch die ISDS-Unterlagen der Systeme IBI-Care (Leistungserfassungssystem, erste Kontrollhandlungen wurden vorgenommen) und Polypoint (Ressourcen- und Rapportverwaltung) der Universitären Psychiatrischen Dienste an.
- Nach der ersten Prüfung des Verwaltungssystems der Pädagogischen Hochschule (VSPH) zeigte sich, dass die Risikoanalyse überarbeitet und ein Löschkonzept nachgereicht werden muss.
- Die Berner Fachhochschule reichte zwei Informatikprojekte zur Vorabkontrolle ein: Noch offen ist die Prüfung der BFH Card (Multifunktionskarte) sowie des Studierenden-Administrationssystems OPROAD.
- Die Vorabkontrolle zur Anwendung OPTIMO (Optimierung der Mobilisierung) der Kantonspolizei konnte abgeschlossen werden.
- Ein Besuch vor Ort zeigte, dass für das an mehreren fixen Standorten nur temporär eingesetzte Verkehrskontrollsystem VKS (Abstands- und Geschwindigkeitsmessungen auf Autobahnabschnitten) der Kantonspolizei keine Vorabkontrolle erforderlich ist.

(Zu den ebenfalls einer Vorabkontrolle unterstellten Informatikprojekten zur Videoüberwachung s. 6.4; zu E-Voting für AuslandschweizerInnen 6.3; zur Staatsschutzdatenbank 8 und 1.1)

## 5 Ansichtsäusserungen, Praxis

Aus den zahlreichen Anfragen an die Datenschutzaufsichtsstelle sind die folgenden Sachverhalte erwähnenswert:

- Google Analytics ist ein Instrument um Besuche auf Internetseiten auszuwerten. Seine Verwendung auf kantonalen und kommunalen Webseiten war sehr kritisch zu beurteilen. Inzwischen hat Google eine Funktion „\_anonymizelp()“ eingebaut, mit der sich zentrale Datenschutzfragen lösen lassen. Der Einsatz des verwandten Tools Google Urchin erfüllt jedoch den gleichen Zweck und lässt sich aus Sicht des Datenschutzes unbedenklich betreiben.
- Die Handhabung des in einem Netzwerk freigegebenen Outlook-Kalenders kann datenschutzrechtliche Probleme aufwerfen. Private Termine müssen als privat markiert und damit für Dritte nicht einsehbar gemacht werden.

du Bureau s'agissant des possibilités d'accès nettement trop étendues. Cette remarque valait aussi bien pour les fonctions et unités organisationnelles (accès aux données d'une autre clinique) que pour les sites (accès aux données d'un autre hôpital). Le Bureau a relevé que des droits d'accès aussi vastes pouvaient avoir des implications pénales (violation du secret de fonction et du secret professionnel). Le SNB s'emploie désormais à les limiter de façon à respecter les exigences de la protection des données. Dès lors, la seconde tranche de la subvention accordée par le Grand Conseil a pu être débloquée.

- Le dossier SIPD de l'application de gestion administrative des patients OPALÉ des Services psychiatriques Jura bernois–Bienne–Seeland à Bellelay est disponible.
- De même, les dossiers SIPD des systèmes IBI-Care (saisie des prestations), pour lequel de premiers contrôles ont été effectués, et Polypoint (gestion des ressources et des rapports) des Services psychiatriques universitaires ont été remis au Bureau pour examen.
- Une première vérification du système administratif (VSPH) de la Haute école pédagogique a révélé la nécessité de remanier l'analyse des risques et de prévoir une procédure d'effacement.
- La Haute école spécialisée bernoise a demandé le contrôle préalable de deux projets informatiques: la carte multifonctionnelle HESB-Card et le système d'administration des étudiants OPROAD.
- Le contrôle préalable de l'application OPTIMO (optimisation de la mobilisation) de la Police cantonale a pu être achevé.
- Une visite sur place a permis de constater que le système de contrôle de la circulation VKS (détermination de la vitesse et de la distance par rapport au véhicule qui précède sur une section d'autoroute) utilisé temporairement en plusieurs endroits fixes par la Police cantonale ne requiert pas de contrôle préalable.

(D'autres projets informatiques ont été soumis au Bureau en vue d'un contrôle préalable: cf. ch. 6.4: vidéosurveillance; ch. 6.3: vote électronique des Suisses et Suissesses de l'étranger; ch. 8 et 1.1: banque de données de la protection de l'Etat).

## 5 Avis exprimés, pratique

Le Bureau est appelé à traiter de nombreuses demandes, et sa pratique permet de dégager les points essentiels suivants:

- Google Analytics est un instrument d'évaluation des visites de sites Internet. Son utilisation par rapport aux sites cantonaux et communaux a donné lieu à une appréciation très critique. Depuis lors, Google a ajouté une fonction intitulée "\_anonymizelp()" permettant de résoudre des questions essentielles de protection des données. Il existe toutefois un outil similaire, Google Urchin, dont l'utilisation ne suscite aucune réserve du point de vue de la protection des données.
- L'utilisation d'un calendrier Outlook partagé à l'intérieur d'un réseau peut soulever des problèmes de protection des données. Les rendez-vous privés doivent être inscrits

Ebenso müssen Termine wie ‚Bewerbungsgespräch mit Herrn Mustermann‘ als privat markiert werden, weil andernfalls eine unzulässige Datenbekanntgabe erfolgt. Vorsicht ist bei Dokumentenanhängen zu Besprechungsanfragen geboten: Wenn die Besprechungsanfrage von Dritten einsehbar ist, dann sind es auch die angehängten Dokumente. Grundsätzlich stellt sich die Frage, ob eine weite Kalenderfreigabe überhaupt notwendig ist, weil die Funktion ‚Terminplanung‘ es unabhängig von Kalenderfreigaben erlaubt, die Verfügbarkeit anderer Nutzer abzuklären.

- Die Diffamierung – beispielsweise von Lehrern – in Facebookgruppen ist differenziert zu beurteilen. Es gibt offene, geschlossene und geheime Facebook-Gruppen. Eine Diffamierung in einer geschlossenen oder geheimen Facebook-Gruppe ist nicht mit einer öffentlichen Kundgabe auf einer gewöhnlichen Internetseite ohne Zugangsschutz gleich zu setzen. Sie entspricht eher einer E-Mail-Mitteilung, die mehreren, einander bekannten Personen versendet wird. Das war zuhause einer Schule festzuhalten, die den für die Diffamierungen verantwortlichen Schüler zur Rechenschaft ziehen wollte.
- Patientinnen und Patienten haben einen Anspruch auf Herausgabe ihrer Krankengeschichte. Es ist zulässig, die Herausgabe der Behandlungsdokumentation an eine ausdrückliche Befreiung von der gesetzlichen Aufbewahrungspflicht und an einen Verzicht auf haftpflichtrechtliche Ansprüche zu knüpfen, soweit sich das Spital ohne die Unterlagen nicht mehr zur Wehr setzen kann. Für Blut und Blutprodukte gilt jedoch eine bundesrechtliche Aufzeichnungs- und Aufbewahrungspflicht (20 Jahre), die weder eine Herausgabe noch eine Löschung zulässt.
- Holt eine erkrankte Person eine Zweitmeinung ein, darf die angefragte Gesundheitsfachperson nur mit ausdrücklicher Einwilligung des Patienten mit dem Verfasser der Erstmeinung Rücksprache nehmen.
- Das Datenschutzgesetz ist seit 2008 auch im erstinstanzlichen Verwaltungsverfahren anwendbar. Stellt eine von einem Polizeieinsatz betroffene Person Haftungsansprüche und verlangt sie in diesem Verfahren Einsicht in eine Videoaufzeichnung der Polizei, so ist es zum Schutz der aufgezeichneten Drittpersonen zulässig, die Sichtung allein unter der Aufsicht des beauftragten Anwaltes zuzulassen und das Erstellen von Kopien zu verbieten.
- Weist eine anfragende Person ein entsprechendes Interesse nach, hat das Regierungsstatthalteramt zu bestätigen, dass eine Erbschaft ausgeschlagen worden ist. Ist die Erbschaft angenommen worden, ist ein beim Regierungsstatthalteramt anfragender Gläubiger an die Einwohnergemeinde des Erblassers weiterzuleiten. Diese hat – soweit zum Einbringen einer Forderung erforderlich – über den Liquidator, den Erbschaftsvertreter oder die Erben Auskunft zu erteilen.
- Im nicht öffentlichen Raum ist eine Überwachung mit technischen Geräten grundsätzlich strafbar. Soll in einem Forschungsprojekt der Einfluss des Umfelds auf das Verhalten auffälliger Kinder überprüft werden, ist es bereits aus diesem Grund unzulässig, die Kinder Kamerabrillen tragen zu lassen.
- Ohne Grundlage in einem formellen Gesetz ist es nicht

comme tels afin que des tiers ne puissent pas prendre connaissance des détails. Il en va de même de rendez-vous dont l'objet est par exemple "entretien d'embauche avec M. Candidat", faute de quoi on est en présence d'une communication illicite de données. La prudence est de mise lorsque des fichiers sont joints à une demande de réunion: si la demande peut être lue par des tiers, il en va de même des pièces jointes. D'une manière générale, la question de l'opportunité de partager un calendrier avec un grand nombre de personnes se pose, dès lors que la fonction "Organiser une réunion" informe sur la disponibilité des autres utilisateurs même sans partage de calendrier.

- La diffamation sur Facebook – à l'endroit de membres du corps enseignant par exemple – doit être appréciée de manière différenciée, selon qu'elle a lieu au sein d'un groupe ouvert, fermé ou secret. La diffusion de propos diffamatoires à l'intérieur d'un groupe fermé ou secret n'a pas la même portée que la publication de tels propos sur une page Internet ordinaire, accessible à tout un chacun. Elle s'apparente plutôt à l'envoi d'un courriel à plusieurs personnes se connaissant entre elles. Le Bureau a expliqué cette distinction à une école qui entendait prendre des mesures disciplinaires contre des élèves auteurs de propos insultants.
- Les patients et patientes ont le droit d'obtenir leur anamnèse. Il est admissible de faire dépendre la remise d'un dossier médical d'une déclaration expresse de libération de l'obligation légale d'archiver et de renonciation à toute prétention en dommages-intérêts, dans la mesure où l'hôpital – privé des documents – n'a plus la possibilité de se défendre. Dans le cas des opérations en rapport avec du sang ou des produits sanguins toutefois, le droit fédéral impose une obligation d'enregistrer et d'archiver pendant 20 ans qui n'autorise aucune remise ni radiation.
- Un professionnel ou une professionnelle de la santé dont une personne malade sollicite un second avis a besoin de l'accord exprès de celle-ci pour prendre contact avec l'auteur du premier avis.
- Depuis 2008, la loi sur la protection des données est également applicable aux procédures administratives de première instance. Si une personne concernée par une intervention policière qui invoque des prétentions en dommages-intérêts demande à consulter un enregistrement vidéo de la police dans le cadre de la procédure, il est admissible de ne permettre le visionnement que sous la surveillance de l'avocat mandaté et d'interdire l'établissement de copies afin de protéger les tiers qui ont été simultanément filmés.
- La préfecture doit confirmer la répudiation d'une succession à une personne qui invoque un intérêt à l'obtention de cette information. Si la succession a été acceptée, la préfecture doit adresser le créancier qui l'a sollicitée aux autorités de la commune du défunt. Celles-ci sont alors tenues de lui donner des renseignements sur le liquidateur, le représentant de la succession ou les héritiers dans la mesure où le recouvrement de la créance le requiert.
- Dans l'espace non public, la surveillance au moyen d'appareils techniques est punissable. Cette seule raison suffit à interdire de faire porter des lunettes caméra à des en-

zulässig, dass eine im Bereich Suchtmittelmissbrauch tätige Stelle ihren Leistungsempfängern zur Eingangskontrolle einen Ausweis abgibt. Soll mit dem Ausweis sichergestellt werden, dass nur in einem bestimmten Gebiet wohnhafte Personen die Leistung beziehen, so ist der Einsatz eines Ausweises auch mit gesetzlicher Grundlage nur geeignet, wenn durch Meldungen oder mit periodischen Rückfragen sichergestellt wird, dass der Ausweis-träger nicht umgezogen ist.

## 6 Gesetzgebung

### 6.1 Datenschutzgesetz

Vor zwei Jahren wurde das Datenschutzgesetz an die Übereinkommen von Schengen und Dublin angepasst. In der Personalverordnung wurde der vorgegebenen unabhängigen Stellung des Datenschutzbeauftragten mit einer Neuregelung des Gehaltsaufstiegs und der Ersteinreihungszuständigkeit Rechnung getragen. Nach wie vor haben sich die neuen Regelungen bewährt. Das kann nun auch für die begründete Empfehlung, gegen die sich die betroffene Stelle mit einer ablehnenden Verfügung zur Wehr setzen kann und für die danach der Aufsichtsstelle zustehende Beschwerdemöglichkeit gesagt werden. (Vgl. hierzu 4 [kiSro]; 7.1 und zur unabhängigen Stellung kommunaler Datenschutzaufsichtsstellen 10).

### 6.2 Bundeserlasse

Die Vereinigung der Schweizerischen Datenschutzbeauftragten (PRIVATIM) nimmt zu Bundeserlassen nur noch vereinzelt Stellung. Hat sich PRIVATIM geäußert oder Stellungnahmen seiner Mitglieder vermittelt, schliesst sich die kantonale Datenschutzaufsichtsstelle - wenn nicht spezifisch bernische Gegebenheiten zu berücksichtigen sind - an. Unter anderem vermittelte PRIVATIM Stellungnahmen zum Bundesgesetz über die polizeilichen Aufgaben des Bundes und zur Totalrevision des Bundesgesetzes betreffend die Überwachung des Fernmeldeverkehrs.

### 6.3 Kantonale Erlasse

Folgende Gesetzgebungsarbeiten sind aus Datenschutzsicht erwähnenswert:

- Den Gerichts- und Verwaltungsbehörden wird im revidierten Spitalversorgungsgesetz neu eine Meldepflicht auferlegt. Sie müssen Vorfälle melden, welche auf eine Verletzung betrieblicher Pflichten hindeuten. Das kann zu einem erheblichen Eingriff in das Grundrecht auf Datenschutz führen. Die Aufsichtsstelle forderte deshalb dazu auf, diese betrieblichen Pflichten im Gesetz näher zu umschreiben. Bis anhin der Aufsicht des EDÖB unterstehende Privatspitäler, welche auf der Spitalliste figurieren, sollen neu unter die kantonale Aufsicht fallen. Ein solcher Systemwechsel bedingt bei der Aufsichtsstelle eine Ressourcenerhöhung.
- Die Aufsichtsstelle wiederholte zur Teilrevision des Sozi-

fants präsentant des troubles dans un projet de recherche visant à étudier l'influence de l'environnement sur leur comportement.

- Sans base légale formelle, un service actif dans le domaine de l'abus de stupéfiants ne saurait délivrer une carte de légitimation aux bénéficiaires de ses prestations afin de faciliter le contrôle à l'entrée des locaux. Si la carte doit garantir que seules les personnes domiciliées dans un certain secteur aient accès au service, elle ne se prête à cette utilisation, même avec une base légale, que si un système d'annonce ou un contrôle périodique permet de s'assurer que son détenteur ou sa détentrice n'a pas démenagé.

## 6 Législation

### 6.1 Loi sur la protection des données

La loi sur la protection des données a été adaptée, voici deux ans, aux accords de Schengen/Dublin. L'ordonnance sur le personnel tient désormais compte de l'indépendance du délégué à la protection des données, avec une nouvelle réglementation relative à la progression des traitements et aux compétences en matière de fixation du traitement de départ. Les nouvelles dispositions légales continuent à faire leurs preuves. Tel est notamment le cas de celles qui permettent au Bureau de formuler des recommandations motivées, puis de recourir le cas échéant contre une décision de rejet émanant du service concerné (cf. à cet égard ch. 4: kiSro, 7.1, et 10: indépendance des autorités communales de surveillance de la protection des données).

### 6.2 Législation fédérale

L'association des commissaires suisses à la protection des données (PRIVATIM) ne prend plus que sporadiquement position sur des actes législatifs fédéraux. Si elle l'a fait ou a répercuté des prises de position de ses membres, le Bureau se rallie à l'avis exprimé, à moins qu'il y ait lieu de tenir compte de spécificités bernoises. PRIVATIM a en particulier diffusé des prises de position relatives à la loi fédérale sur les tâches de police de la Confédération ainsi qu'à la révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication.

### 6.3 Législation cantonale

Les travaux législatifs suivants ont des incidences en matière de protection des données:

- La loi sur les soins hospitaliers révisée impose une obligation d'informer aux autorités judiciaires et administratives, qui sont tenues d'annoncer sans retard les faits susceptibles de constituer une violation du devoir de diligence lié à l'entreprise. Une telle disposition peut entraîner de graves atteintes au droit fondamental à la protection des données. Le Bureau a par conséquent demandé que la loi précise la notion de "devoir de diligence lié à l'entreprise". Les établissements privés inscrits sur la liste des hôpitaux, placés jusqu'ici sous la surveillance du PFPDT, doivent désormais relever du Bureau. Ce changement de système implique une augmentation des ressources.
- Le Bureau a réitéré ses critiques sur le devoir particulier



alihilfegesetzes ihre Kritik an der Einführung des besonderen Sozialhilfegeheimnisses. Dieses wird durch die vorgesehenen Datenbekanntgabeerleichterungen seines Gehalts gerade wieder entleert. Die Präzisierungsvorschläge für Gesetz und Vortrag wurden nur teilweise übernommen.

- Daten über Prostituierte sind besonders schützenswert. Das war zum Gesetz über die Ausübung der Prostitution festzuhalten. Werden Salonbetreiber verpflichtet ein Register über die beschäftigten Prostituierten zu führen, so sind diese Daten nach Aufgabe der Tätigkeit rasch zu vernichten. Meldeermächtigungen sind präzise zu fassen. Das gilt auch für die Regelungen des Informatiksystems über die Salonbetreiber.
- Der vom Kanton Bern eingeschlagene Weg, den Einsatz der Versichertennummer mit einer Globalermächtigung im Registerharmonisierungsgesetz zuzulassen, erachten der EDÖB, das Bundesamt für Sozialversicherungen und die Aufsichtsstelle als bundesrechtswidrig. Im Vorabkontrollverfahren des Projektes E-Voting für AuslandschweizerInnen (elektronische Stimmabgabe) stellte die Aufsichtsstelle den vorgesehenen Nummerneinsatz fest. Sie regte deshalb zum Gesetz über die politischen Rechte an, den Nummerneinsatz für Wahlen und Abstimmungen ausdrücklich vorzusehen.
- Zum Einführungsgesetz zum Kindes- und Erwachsenenschutzrecht regte die Datenschutzaufsichtsstelle u.a. an, eine Regelung zu treffen, die Betreuungs- und Klinikeinrichtungen zum vertraulichen Umgang mit Unterbringungsanfragen verpflichtet. Auf den entsprechenden Regelungsbedarf war die Aufsichtsstelle von den Regierungsverantwortlichen hingewiesen worden.
- Das Gesetz über Freiheitsbeschränkungen im Jugendstraf- und Massnahmenvollzug und in der stationären Jugendhilfe sieht als Sanktion den Einzug von elektronischen Geräten vor. Die Aufsichtsstelle hielt fest, dass diese Rechtsgrundlage nicht auch zur Kenntnisnahme der auf dem Gerät gespeicherten Daten ermächtigt.
- Zweimal nahm die Aufsichtsstelle zur Revision des Polizeigesetzes Stellung. Mit dem Inkrafttreten der Schweizerischen Strafprozessordnung entfallen die bisherigen Rechtsgrundlagen zur präventivpolizeilichen Observation und zur präventivpolizeilichen verdeckten Ermittlung. Es ist unzulässig, im Polizeigesetz Ersatzregelungen in einem verkürzten Verfahren ohne Vernehmlassungsmöglichkeit zu schaffen. Unter welchen Voraussetzungen die präventivpolizeilichen Eingriffe zulässig sein sollen, ist in Regelungen von hoher Bestimmtheit zu umschreiben. Zur präventiven Überwachung von Chaträumen ist eine verdeckte Fahndung und nicht eine präventive Observation erforderlich. Die Regelung fällt in die Bundeskompetenz. Ausgeschlossen ist eine rückwirkende Inkraftsetzung.
- Die Finanzdirektion hatte den Erlass einer ‚Verordnung über die Aufzeichnung und Auswertung der Personendaten über die Nutzung der ICT-Infrastruktur‘ geplant. Damit sollte das Logging für alle elektronischen Geräte im Prinzip erlaubt werden und die Auswertung für viele Fälle ebenfalls zulässig erklärt werden. Die Aufsichtsstelle hat grundlegende Bedenken zur Regelung derart weiter Eingriffe in Persönlichkeitsrechte auf Verordnungsstufe gel-

de Discretion des personnes chargées de l'aide sociale prévu par la révision partielle de la loi sur l'aide sociale, qui est vidé de sa substance par les exceptions prévues. Ses propositions de précision de la loi et du rapport n'ont été que partiellement reprises.

- Les données concernant les personnes prostituées sont particulièrement dignes de protection, comme le Bureau s'est vu amené à le relever au sujet de la loi sur l'exercice de la prostitution. Dès lors que les exploitants de salons de massage doivent tenir un registre des travailleurs et travailleuses du sexe qu'ils emploient, il importe que ces données soient rapidement détruites en cas de cessation de l'activité. Les autorisations de communiquer des données doivent être prévues avec précision, tout comme les règles relatives au système informatique sur les tenanciers de salons.
- La solution privilégiée par le canton de Berne, consistant à autoriser de manière générale l'utilisation du numéro d'assuré dans la loi sur l'harmonisation des registres officiels, est considérée comme contraire au droit fédéral par le PFPDT, l'Office fédéral des assurances sociales et le Bureau. C'est lors du contrôle préalable portant sur le projet E-voting de vote électronique pour les Suisses et Suissesses de l'étranger que le Bureau a relevé l'utilisation de ce numéro. Il a donc proposé qu'elle soit expressément prévue dans la loi sur les droits politiques pour les élections et les votations.
- Le Bureau a demandé que la loi portant introduction du droit de la protection de l'enfant et de l'adulte soit en particulier complétée par une disposition obligeant les institutions d'accueil et de prise en charge médicale sollicitées en vue d'un placement à traiter la demande de manière confidentielle. Ce sont les préfetures qui avaient attiré son attention sur la nécessité d'une telle réglementation.
- La loi sur les mesures restreignant la liberté des mineurs dans le cadre de l'exécution des peines et des mesures et de l'aide à la jeunesse prévoit comme sanction le retrait d'appareils électroniques. Le Bureau a relevé que cette base légale n'autorisait toutefois pas la consultation des données enregistrées dans ces appareils.
- Le Bureau a pris position à deux reprises au sujet de la révision de la loi sur la police. Suite à l'entrée en vigueur du code de procédure pénale suisse, il n'existe plus de bases légales permettant l'observation et l'investigation secrète à titre préventif. Il n'est toutefois pas admissible de réintroduire de telles bases dans la loi sur la police au moyen d'une procédure abrégée, sans consulter les milieux intéressés. En effet, les conditions d'une intervention préventive de la police doivent être réglementées avec une extrême précision. La surveillance préventive de salons de cyberbavardage requiert non pas une observation, mais une recherche secrète, et il appartient à la Confédération de légiférer en la matière. Une entrée en vigueur rétroactive est en tous les cas exclue.
- La Direction des finances avait prévu l'édiction d'une ordonnance sur l'enregistrement et l'évaluation des données personnelles relatives à l'utilisation de l'infrastructure TIC autorisant en principe la journalisation pour tous les appareils électroniques de même qu'une évaluation dans de nombreux cas. Le Bureau a de sérieuses réserves par

tend gemacht. Der Verordnungsentwurf wurde zurück gestellt.

## **7 Aufsichts- und Justizentscheide**

### **7.1 Unzulässige Generalvollmacht in der Sozialhilfe**

Erstmals seit der Einführung des Beschwerderechts für die Aufsichtsstellen hatte sich eine Justizbehörde mit einer solchen Beschwerde zu befassen. Es ging um die umfassende Sozialhilfевollmacht der Stadt Biel. Für die Abklärung ihrer finanziellen Leistungsfähigkeit sollten Betroffene es der Abteilung für Soziales ermöglichen, Informationen bei rund 20 teilweise nicht näher bezeichneten Stellen einzuholen. Die Sozialhilfebehörde lehnte es mit Verfügung ab, dem begründeten Antrag der kommunalen Aufsichtsstelle zu folgen und auf die Einführung der beanstandeten (General-)Vollmacht zu verzichten. Daraufhin erhob die kommunale Aufsichtsbehörde Beschwerde. Der Regierungsrat von Biel holte bei der kantonalen Aufsichtsstelle einen Amtsbericht ein. Er stützte sich in wesentlichen Punkten auf diesen Amtsbericht und hiess die Beschwerde gut. Er entschied, dass die Vollmacht in ihrem Wortlaut als kombinierte Einwilligung in eine Datenbekanntgabe durch alle aufgeführten Stellen gelten muss und der Vollmachtgeber nicht genügend in der Lage ist, einzuschätzen, welche Daten zu welchem Zweck von seiner Einwilligung betroffen sind und welche Auswirkungen seine Einwilligung gegenüber den betroffenen Stellen hat.

### **7.2 Videoverordnung; Zulässigkeit der Echtzeitüberwachung**

Gestützt auf das Polizeigesetz durfte der Regierungsrat in der Videoverordnung die Echtzeitüberwachung öffentlicher Plätze und zum Schutz öffentlicher Gebäude vorsehen. Der Wortlaut des Polizeigesetzes lässt eine Echtzeitüberwachung zu. Unklarheiten in der grossrätlichen Debatte ändern daran nichts. Der Regierungsrat hat bei seinem Vorgehen auch die Vorgaben zur Gewaltenteilung respektiert. Das hielt das Bundesgericht in einem gegen die Videoverordnung gerichteten Beschwerdeverfahren fest. Es unterstrich aber, dass auch die Echtzeitüberwachung einer rechtlichen Grundlage bedarf.

### **7.3 Recht auf Einsicht in die Namensliste der für eine Gewaltstudie befragten Schlüsselpersonen**

Das Bundesgericht hiess eine Beschwerde gegen den Gemeinderat Burgdorf gut. Dieser hielt die Namen der von ihm zur Befragung für eine Gewaltstudie bestimmten Schlüsselpersonen unter Verschluss. Der Beschwerdeführer berief sich auf das Grundrecht auf Information und erhielt Recht: Im Gegensatz zu den Vorinstanzen befand das Bundesgericht, einer Einsichtnahme würden weder private noch öffentliche Interessen (auch nicht Forschungsinteressen) entgegenstehen. Insbesondere werde aus der Studie nicht ersichtlich, wer sich wie geäussert habe.

rapport à l'adoption au niveau d'une ordonnance de dispositions portant pareillement atteinte aux droits de la personnalité. Les travaux relatifs à l'ordonnance ont été reportés.

## **7 Surveillance et décisions de justice**

### **7.1 Inadmissibilité d'une procuration générale dans le domaine de l'aide sociale**

Pour la première fois depuis l'introduction du droit de recours des autorités de surveillance, une autorité de justice a été saisie d'un tel recours. Celui-ci avait pour objet la procuration générale prévue par la ville de Bienne dans le domaine de l'aide sociale. Les personnes concernées devaient autoriser le Département des affaires sociales à recueillir des informations auprès d'une vingtaine de services – pas tous nommément désignés – afin de déterminer leurs capacités financières. L'autorité sociale a rejeté, par voie de décision, la proposition motivée de renoncer à l'introduction d'une telle procuration formulée par l'autorité communale de surveillance de la protection des données. Celle-ci a alors formé recours devant le préfet de Bienne, qui a sollicité un rapport officiel du Bureau. Le préfet a ensuite admis le recours en se fondant, à propos de divers points essentiels, sur ce rapport. Il a estimé que pour les personnes concernées, signer une telle procuration équivalait à donner leur accord à la communication combinée de données par tous les services concernés, alors qu'elles n'étaient pas suffisamment en mesure d'évaluer quelles données seraient utilisées par ces services, à quelles fins et avec quelles conséquences.

### **7.2 Ordonnance sur la vidéosurveillance: admissibilité de la surveillance en temps réel**

La teneur de la loi sur la police permet la surveillance en temps réel – et le flottement lors des débats parlementaires n'y change rien. Le Conseil-exécutif l'a donc prévue dans l'ordonnance sur la vidéosurveillance pour les places publiques et la protection des bâtiments publics. Ce faisant, il a respecté le principe de la séparation des pouvoirs, comme l'a relevé le Tribunal fédéral dans une procédure de recours dirigée contre l'ordonnance tout en soulignant la nécessité d'une base légale pour la surveillance en temps réel égale-ment.

### **7.3 Droit de consulter la liste de noms des personnes-clés interrogées dans le cadre d'une étude sur la violence**

Le Tribunal fédéral a admis un recours contre le conseil communal de Berthoud qui conservait en un endroit inaccessible les noms des personnes-clés qu'il avait désignées en vue d'une étude sur la violence. Le recourant, qui invoquait son droit fondamental à l'information, a obtenu gain de cause: contrairement aux instances précédentes, le Tribunal fédéral a estimé qu'aucun intérêt privé ni public (et aucun intérêt lié à la recherche) ne s'opposait à la consultation de telles données. L'étude ne révélait notamment pas qui s'était exprimé et en quels termes.

#### **7.4 Keine Umgehung des Öffentlichkeitsprinzips durch behördliche Zusicherung der Geheimhaltung**

Gestützt auf das Öffentlichkeitsprinzip verlangte derselbe Beschwerdeführer Einsicht in die Listen der im Projekt ‚Aufgabendialog Kanton Bern‘ interviewten Experten. Weil das federführende Generalsekretariat der Finanzdirektion die Einsicht verweigerte, erhob er (erfolglos) Beschwerde bei der Finanzdirektion. Als nächste Instanz urteilte das Verwaltungsgericht. Es hielt fest weder der Schutz der Forschung noch die Vertraulichkeitszusicherung der Finanzdirektion bilde ein dem Einsichtsrecht entgegenstehendes überwiegendes öffentliches Interesse und hiess die Beschwerde gut.

#### **7.5 Datenaustausch im Aufnahmeverfahren für Berufsmaturitätsschulen**

Die Gesetzgebung über Berufsmaturitätsschulen schliesst es nicht aus, dass Interessierte die Anmeldeverfahren für mehrere Schulen durchlaufen. Es fehlen damit auch Rechtsgrundlagen, die es einem Schulleiter der einen Schule erlauben würde, die andere Schule über ein erfolgloses Aufnahmeverfahren zu informieren. Erst recht fehlen Rechtsgrundlagen, die die Interessierten zu entsprechenden Mittelungen an die Schule verpflichten. Darauf machte die Aufsichtsstelle einen Schulleiter auf aufsichtsrechtliche Eingabe hin aufmerksam.

#### **7.6 Amtshilfe: kein Vorrang der Datenbeschaffung bei der betroffenen Person**

Eine späte Abmeldung für die Tagesschule veranlasste eine Gemeindeschreiberin das Anmeldedatum zweier schulpflichtiger Kinder direkt bei der Privatschule abzuklären, welche die Kinder schliesslich besuchten. Die Abklärung sollte es erlauben, den trotz unterbliebenem Besuch der Tagesschule geschuldeten Beitrag in Rechnung zu stellen. Zu Unrecht rügten die betroffenen Eltern, die Auskunft hätte nur bei ihnen erfragt werden dürfen (Vorrang der Datenbeschaffung bei der betroffenen Person). Dieser Vorrang gilt nur bei Datenbeschaffungen bei Privaten. Die Privatschule erfüllte aber eine öffentliche Aufgabe (Volksschulstufe) und war damit eine Behörde, die Amtshilfe zu leisten hatte. Zum gleichen Schluss kam ein zum Sozialhilfegesetz eingeholtes Rechtsgutachten. Die Aufsichtsstelle hielt dies im Sinne einer Rechtsauskunft zu einer Aufsichtsanzeige fest. Diese war nicht an die Hand zu nehmen, da für die vorgebrachten Rügen Rechtsmittel offen standen.

#### **7.7 Rechtswidrige Handhabung des Einsichtsrechts bei der IV-Stelle**

Verlangten Betroffene Einsicht in ihre Invalidenversiche-

#### **7.4 La garantie de la confidentialité par une autorité ne permet pas de contourner le principe de la publicité**

Se fondant sur le principe de la publicité, le même recourant demandait à pouvoir consulter les listes des experts interviewés dans le cadre du projet "Dialogue sur les prestations du canton de Berne". Suite au refus d'accéder à sa demande opposé par le Secrétariat général de la Direction des finances, responsable du projet, il a formé (sans succès) un recours devant cette même Direction. L'affaire a ensuite été portée devant le Tribunal administratif, qui a admis le recours au motif que ni la protection de la recherche, ni la garantie de la confidentialité donnée par la Direction des finances ne constituaient un intérêt public prépondérant s'opposant à la consultation.

#### **7.5 Echange de données dans la procédure d'admission aux écoles de maturité professionnelle**

La législation sur les écoles de maturité professionnelle n'exclut pas les inscriptions multiples. Dans ce contexte, il n'existe pas de base légale permettant à la direction d'une école d'informer une autre école d'un échec lors d'une procédure d'admission. Et surtout, il manque une base légale imposant un devoir d'information aux personnes intéressées. Telles sont les constatations que le Bureau a adressées au directeur d'une école suite à une requête relevant du droit de la surveillance.

#### **7.6 Entraide administrative: aucune primauté de l'acquisition des données auprès de la personne intéressée**

Suite à une désinscription tardive à l'école à journée continue, une secrétaire communale a demandé directement à l'école privée fréquentée en fin de compte par les deux enfants en âge de scolarité concernés la date de leur inscription. Cette information devait lui permettre d'établir la facture de la contribution due malgré tout par les parents. Ces derniers ont émis le grief – infondé – selon lequel un tel renseignement n'aurait dû être demandé qu'à eux seuls (primauté de l'acquisition des données auprès de la personne intéressée). La règle de la primauté ne s'applique en effet qu'à la collecte de données auprès de personnes privées. Or, l'école privée accomplit en l'espèce une tâche publique (école obligatoire). Dès lors, elle est assimilée à une autorité, et partant tenue de fournir une entraide administrative. Une expertise juridique demandée au sujet de la loi sur l'aide sociale a abouti aux mêmes conclusions. Le Bureau l'a précisé, sous forme d'avis de droit, en réponse à une dénonciation à l'autorité de surveillance qu'il n'a pas eue à traiter du fait de l'existence de voies de recours pour les griefs en question.

#### **7.7 Pratique illégale de l'Office AI en matière d'octroi du droit de consultation**

L'Office AI avait pour habitude de n'accorder aux personnes

rungsunterlagen, gewährte die IV-Stelle ihnen diese mit dem Hinweis, vom Inhalt dürfe weder durch Weitergabe noch in Form von Auszügen, Fotokopien oder auf andere Weise Dritten Kenntnis gegeben werden.

Will eine Behörde Einsicht gewähren, hat sie stets zu prüfen, ob dieser Einsicht überwiegende Drittinteressen entgegenstehen. Die IV-Stelle unterliess eine solche Prüfung. Der Hinweis sollte den Schaden für die Dritten verkleinern. Ein Einsichtsberechtigter hat aber im Rahmen der Rechtsordnung das Recht, über die ihm offen gelegten Informationen frei zu verfügen. Insbesondere darf er sie einem Anwalt unterbreiten. Die IV-Stelle verletzte mit ihrem Vorgehen damit sowohl die Rechtsansprüche der Dritten als auch diejenigen der Einsichtsberechtigten. Auf einen aufsichtsrechtlichen Hinweis der Aufsichtsstelle hin beschied die IV-Stelle nach mehreren Monaten, sie werde die entsprechenden Formulare überarbeiten.

## 8 Staatschutz

Im Vorabkontrollbericht zur Staatsschutzdatenbank hielt die Aufsichtsstelle Ende März fest, die kantonale Staatsschutzdatenbank müsse eine Vorabkontrolle durchlaufen, dem Regierungsrat zu einer Betriebsbewilligung nach Polizeigesetz unterbreitet werden und es sei für sie eine Betriebsordnung zu erstellen, die das Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) zu genehmigen habe. Neben Hinweisen zur Ausgestaltung der Datenfelder und der Löschungen ergab die Vorabkontrolle das Fehlen einer genügenden Rechtsgrundlage im kantonalen Recht und die fehlende Umschreibung der kantonalen Kontrollmechanismen. Zu diesen fand im Juli eine Besprechung mit dem Kontrollorgan des Nachrichtendienstes des Bundes (NDB) statt. Dies, nachdem die Geschäftsprüfungsdelegation der Eidgenössischen Räte kurz vorher ihren Bericht zu der ‚Datenbearbeitung im Staatsschutzinformationssystem ISIS‘ veröffentlicht hatte und zum Schluss kam, der NDB bearbeite Daten ohne Staatsschutzrelevanz und die Kontrollmechanismen über die Datenbearbeitungen hätten bisher ungenügend gewirkt. Im November unterbreitete das Polizeikommando der Aufsichtsstelle den Entwurf für eine Betriebsordnung zur Stellungnahme. Es wies auf die Ansicht des NDB hin, wonach eine kantonale Staatsschutzdatenbank nur die vom VBS zu genehmigende Betriebsordnung benötige. Weder eine Betriebsbewilligung des Regierungsrates noch eine Vorabkontrolle durch die Aufsichtsstelle sei zulässig. Einer kantonalen gesetzlichen Grundlage bedürfe es nicht. Ob sich die Polizei- und Militärdirektion dieser Haltung anschliesst, ist im der Berichtszeitraum offen geblieben. Die Aufsichtsstelle teilt die Auffassungen des NDB nicht: Sowohl die Betriebsbewilligung des Regierungsrats als auch die Vorabkontrolle sind Aufsichtsinstrumente des kantonalen Rechts. Das Bundesrecht behält diese ausdrücklich vor. Es geht sodann nicht um eine Geschäftskontrolldatenbank, die allenfalls durch das Bundesrecht abgedeckt sein könnte. Die Staatsschutzdatenbank ist vielmehr im Staatsschutzumfeld ein selbständiges präventivpolizeiliches Instrument, das zu schweren Eingriffen in das Grundrecht auf Datenschutz der Betroffenen

invalides le droit de consulter leur dossier d'assurance qu'à la condition qu'elles ne le transmettent pas à des tiers et que son contenu ne soit pas non plus porté à la connaissance de tiers sous forme d'extrait, de photocopie ou d'une autre manière.

Avant de permettre la consultation de données, une autorité doit toujours vérifier qu'aucun intérêt prépondérant de tiers ne s'y oppose. L'Office AI omettait de le faire, au motif que les conditions dont était assortie la consultation réduisaient le risque pour les tiers. Pourtant, une personne habilitée à consulter son dossier a le droit de disposer librement des informations mises à sa disposition dans le respect des dispositions légales en vigueur. Elle peut en particulier les soumettre à un avocat. Ainsi, l'Office AI violait aussi bien les prétentions juridiques de tiers que celles des personnes directement concernées. Plusieurs mois après y avoir été invité par le Bureau, l'office AI a décidé de modifier ses formulaires ad hoc.

## 8 Protection de l'Etat

Dans son rapport de contrôle préalable sur la banque de données cantonale de la protection de l'Etat, le Bureau a relevé fin mars que cette dernière devait bel et bien subir un tel contrôle, obtenir du Conseil-exécutif une autorisation d'exploitation au sens de la loi sur la police et faire l'objet d'un règlement d'exploitation soumis à l'approbation du Département fédéral de la défense, de la protection de la population et des sports (DDPS). Le rapport formulait des remarques sur la conception des champs de données et sur la radiation, tout en relevant l'insuffisance des bases légales cantonales et l'absence d'une description des mécanismes cantonaux de contrôle. Ces derniers ont été évoqués en juillet lors d'un entretien avec l'organe de contrôle du Service de renseignement de la Confédération (SRC). Peu avant, la Délégation des Commissions de gestion des Chambres fédérales avait publié son rapport intitulé "Traitement des données dans le système d'information relatif à la protection de l'Etat ISIS", dans lequel elle parvenait à la conclusion que le SRC traitait des données sans pertinence du point de vue de la protection de l'Etat et que les mécanismes de contrôle du traitement des données n'avaient jusque-là pas été suffisamment efficaces. En novembre, le Commandement de la police a remis un projet de règlement d'exploitation au Bureau afin qu'il puisse prendre position, en relevant que de l'avis du SRC, une banque de données cantonale de la protection de l'Etat n'avait besoin que d'un règlement d'exploitation approuvé par le DDPS. Ainsi, selon le SRC, il n'est pas admissible que le Conseil-exécutif délivre une autorisation d'exploitation ni que le Bureau procède à un contrôle préalable, et aucune base légale cantonale n'est nécessaire. Pendant la période couverte par le rapport, la Direction de la police et des affaires militaires n'a pas indiqué si elle se ralliait à cette opinion. Quant au Bureau, il n'est pas d'accord avec le SRC: tant l'autorisation d'exploitation du Conseil-exécutif que le contrôle préalable sont des instruments de surveillance du droit cantonal, expressément réservés par le droit fédéral. En effet, il ne s'agit pas en l'espèce d'une banque de données de contrôle des affaires, qui pourrait éventuellement relever du seul

führt. Die Aufsichtsstelle wird sich nach dem Berichtszeitpunkt zu den von den zuständigen Stellen eingeleiteten Schritten zu äussern haben. Erhebliche Bedeutung kommt dabei der Ausgestaltung des polizeiinternen Kontrollorgans zu.

Die Bundesregelungen lassen für alle kantonalen Kontrollstellen Einsichtnahmen in die Daten nur mit Zustimmung des NDB zu. Bisher hat die Aufsichtsstelle keine solchen Kontrollhandlungen vorgenommen.

(s. auch 1.1; 4)

## 9 Videoüberwachung

Will eine kantonale Stelle eine Videoüberwachung einrichten, hat sie das Vorabkontrollverfahren zu durchlaufen und die Zustimmung des Polizeikommandos einzuholen. Das Polizeikommando trifft seinen Zustimmungsentscheid gestützt auf den Vorabkontrollbericht der Aufsichtsstelle. Liegt die Zustimmung des Polizeikommandos vor, hat die zuständige Stelle den Einsatz der Videoüberwachung zu verfügen. Betroffenen und der Aufsichtsstelle kommt ein Beschwerderecht gegen diese Einsatzverfügung zu. Auch bereits in Betrieb stehende Überwachungsanlagen müssen dieses Verfahren durchlaufen. Zahlreiche Stellen unterbreiteten der Aufsichtsstelle daher Vorabkontrollunterlagen, so etwa das Amt für Freiheitsentzug und Betreuung, das Obergericht, das Inselspital (auch für das von ihm betriebene Parkhaus), die Berner Fachhochschule, das Untersuchungsrichteramt Berner Oberland und mehrere regionale Arbeitsvermittlungsstellen. Fehlende Eignung der gesamten Überwachungsanlage, unnötige Datenaufzeichnungen, zu weit gefasste Kamerafelder (etwa wenn neben dem interessierenden Einfahrtsbereich auch die vorbeiführende Strasse erfasst wird), fehlende Gesichtsausfilterung oder ungenügende Sicherung der Datenübertragung waren im Vorabkontrollverfahren Kritikpunkte. Das Polizeikommando beurteilte die Anlagen in allen Fällen gleich. Es führt zu den bewilligten Videoüberwachungsanlagen eine im Internet verfügbare Karte.

Videoüberwachungsanlagen von Gemeinden sind den kommunalen Aufsichtsstellen zur Vorabkontrolle zu unterbreiten. Die kantonale Aufsichtsstelle hat mehrere kommunale Aufsichtsstellen hierzu beraten.

(s. zu der vom Bundeshaus aus betriebenen Videoüberwachungsanlage 1.2; zur Vorabkontrolle vorbestehender Videoüberwachungsanlagen 2.1; zum Forschungsprojekt Kamerabrille: 5; zum Bundesgerichtsentscheid zur Videoverordnung: 7.2)

## 10 Gemeinderechtliche Körperschaften

Nicht alle Gemeinden gestalten ihre Datenschutzaufsichtsstelle so unabhängig aus, wie es das Datenschutzgesetz nach der Anpassung an die Vorgaben von Schengen/Dublin verlangt. So geht es nicht an, dass der Gemeindeschreiber in der aus drei Mitgliedern bestehenden Datenschutzaufsichtsstelle Mitglied ist.

droit fédéral, mais bien d'un instrument policier de prévention qui, dans le contexte de la protection de l'Etat, peut porter gravement atteinte au droit fondamental à la protection des données des personnes concernées. Le Bureau devra encore prendre position sur les démarches entreprises par les services compétents, en accordant une importance particulière aux spécificités de l'organe de contrôle interne à la police.

Les prescriptions fédérales n'autorisent les organes de contrôle cantonaux à consulter les données qu'avec l'accord du SRC. A ce jour, le Bureau n'a effectué aucun contrôle.

(Cf. aussi ch. 1.1 et 4.)

## 9 Vidéosurveillance

Tout service cantonal qui entend installer une vidéosurveillance doit suivre la procédure de contrôle préalable et demander l'accord du Commandement de la police. Ce dernier statue en se fondant sur le rapport de contrôle préalable du Bureau. Une fois l'accord obtenu, le service compétent doit rendre une décision sur l'installation de la vidéosurveillance, décision que les personnes concernées et le Bureau peuvent attaquer au moyen d'un recours. La même procédure doit être respectée pour les installations qui sont déjà en exploitation. En conséquence, de nombreux services ont soumis des dossiers pour contrôle préalable au Bureau, comme l'Office de la privation de liberté et des mesures d'encadrement, la Cour suprême, l'Hôpital de l'île (également pour le parking qu'il exploite), la Haute école spécialisée bernoise, le Service de juges d'instruction de l'Oberland bernois, ainsi que plusieurs services régionaux de placement. Parmi les points critiqués par le Bureau, on peut citer l'inadéquation de l'installation dans son ensemble, l'enregistrement inutile de données, la largeur excessive du champ de caméra (p. ex. lorsque la route adjacente est filmée en même temps que l'entrée devant être surveillée), l'absence de système de floutage des visages, ou encore la sécurité insuffisante lors du transfert des données. Le Commandement de la police a apprécié toutes les installations de la même manière que le Bureau. Il publie sur Internet une carte de l'ensemble des installations de vidéosurveillance autorisées.

Les installations des communes doivent être soumises au contrôle préalable des autorités communales de surveillance. Le Bureau a prodigué des conseils à plusieurs d'entre elles.

(Cf. ch. 1.2: installation de vidéosurveillance exploitée depuis le Palais fédéral, ch. 2.1: contrôle préalable d'installations de vidéosurveillance existantes, ch. 5: projet de recherche recourant à des lunettes caméra et ch. 7.2: arrêt du Tribunal fédéral relatif à l'ordonnance sur la vidéosurveillance).

## 10 Collectivités de droit communal

Les autorités de surveillance des communes ne satisfont pas toutes aux exigences d'indépendance telles qu'elles sont énoncées par la loi sur la protection des données adaptée aux accords de Schengen/Dublin. Il n'est en particulier pas acceptable qu'un secrétaire communal fasse partie d'une telle autorité composée de trois membres.

Gemeinderechtliche Körperschaften geben auf ihren Internetseiten auch Personendaten bekannt. Das Amt für Gemeinden und Raumordnung (AGR) hat hierzu eine Musterverordnung erstellt.

(Vgl. zur Ausbildungsveranstaltung der Gemeinde Muri-Gümligen 2.2; zum Einsatz von Google Analytics und zur Auskunftserteilung bei Erbschaften 5; zur Überarbeitung des vorab durch gemeinderechtliche Körperschaften anzuwendenden Sozialhilfegesetzes 6.3; zur Beschwerdeführung der kommunalen Datenschutzaufsichtsstelle von Biel gegen die unzulässige Generalvollmacht in der Sozialhilfe 7.1; zum Einsichtsrecht in die Liste der für eine kommunale Studie befragten Schlüsselpersonen 7.3; zur Informationsbeschaffung durch eine Gemeindeschreiberin bei einer Privatschule 7.6; zur Zuständigkeit der kommunalen Aufsichtsstellen für die Vorabkontrollen von Videoüberwachungsanlagen 9).

## 11 Berichtspunkte der Vorjahre

(2.4: Nachkontrolle, ob die 2009 bei den Kontrollen von Informatikdatenbearbeitungen festgelegten Massnahmen umgesetzt worden sind; 3: Erlass der Direktionsverordnung ISDS; 4: weitergeführte Vorabkontrollen; 6.3: Sozialhilfe: Ausgestaltung des Sozialhilfegesetzes; 7.1: begründete Empfehlung der Datenschutzaufsichtsstelle Biel; 7.2: Videoverordnung: Bundesgerichtsurteil über die Zulässigkeit der Echtzeitüberwachung).

## 12 Antrag

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

25. Januar 2011

Der Datenschutzbeauftragte: *Siegenthaler*

Les collectivités de droit communal publient également des données personnelles sur Internet. L'Office des affaires communales et de l'organisation du territoire (OACOT) a élaboré un modèle d'ordonnance à cet égard.

(Cf. ch. 2.2: cours pour le personnel de la commune de Muri-Gümligen; ch. 5: utilisation de Google Analytics et communication de renseignements relatifs aux successions; ch. 6.3: révision de la loi sur l'aide sociale, dont la mise en œuvre relève pour l'essentiel des communes; ch. 7.1: recours de l'autorité de surveillance de la protection des données de la ville de Bienne contre la procuration générale illégale prévue dans le domaine de l'aide sociale; ch. 7.3: droit de consulter la liste des personnes-clés interrogées dans le cadre d'une étude communale; ch. 7.6: obtention de données auprès d'une école privée par une secrétaire communale; ch. 9: compétence des autorités communales de surveillance pour procéder au contrôle préalable concernant les installations de vidéosurveillance).

## 11 Points abordés dans le rapport précédent

(2.4: vérification de la mise en œuvre des mesures fixées lors des contrôles du traitement de données informatiques en 2009; 3: édicton de l'ordonnance de Direction SIPD; 4: contrôles préalables effectués; 6.3: prescriptions de la loi sur l'aide sociale; 7.1: recommandations motivées de l'autorité de surveillance de la protection des données de la ville de Bienne; 7.2: ordonnance sur la vidéosurveillance – arrêt du Tribunal fédéral relatif à l'admissibilité de la surveillance en temps réel).

## 12 Proposition

Il est proposé au Conseil-exécutif et au Grand Conseil de prendre connaissance du présent rapport conformément à l'article 37 de la loi sur la protection des données.

25 janvier 2011

Le délégué à la protection des données: *Siegenthaler*

### Anhang:

#### 1. Abkürzungen, Bezeichnungen

AGR: Amt für Gemeinden und Raumordnung  
 Applikation: Informatikanwendung  
 Aufbieten von Polizei- und Wehrdienstorganisationen  
 beco: Berner Wirtschaft  
 BEWAN: Weitbereichsnetzwerk des Kantons Bern  
 BFH: Berner Fachhochschule  
 BFHCard: Chipunterstützte Multifunktionskarte der BFH,

### Annexe:

#### 1. Abréviations et désignations

AI: assurance-invalidité  
 beco: Economie bernoise  
 BEWAN: réseau cantonal de communications longues distances  
 Cf.: confer (voir)  
 CISA: Certified Information Systems Auditor  
 DDPS: Département fédéral de la défense, de la protection

welche als Identifikations- und Zahlungsmittel eingesetzt werden kann

Chatraum: elektronische Kommunikation in Echtzeit über das Internet, die für die Teilnehmer zu einer ähnlichen Situation wie in einem Plauderraum führt

CISA: Certified Information Systems Auditor

EDÖB: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

ELA\_DMS: elektronische Archivierung und Dokumenten-Management-System (der Spitäler fmi ag: Spitäler Frutigen, Meiringen, Interlaken)

ePUB: Elektronische Prüfungsadministration der Universität Bern

ERZ: Erziehungsdirektion

E-VAS GG: Ersatz des Veranlagungssystems Grundsteuergewinnsteuer

E-Voting: elektronisches Wahl- und Abstimmungsverfahren (das Projekt umfasst zur Zeit allein die Stimmabgabe der Auslandschweizer)

eVUB: Elektronisches Vorlesungsverzeichnis der Universität Bern

Facebook: Internetapplikation zur Pflege sozialer Beziehungen und zum Austausch von persönlichen Informationen

fmi ag: Spitäler Frutigen, Meiringen, Interlaken

GELAN: Gesamtlösung EDV Landwirtschaft; Agrarinformationssystem der Kantone Bern, Freiburg und Solothurn

Google Analytics („\_anonymizelp()"): Applikation zur Erfassung des Nutzerverhaltens auf Webseiten. Mit der Funktion \_anonymizelp() kann die Internet-Adresse der Nutzer anonymisiert werden

Google Urchin: Applikation zur Erfassung des Nutzerverhaltens auf Webseiten. Die erhobenen Daten werden im Gegensatz zu Google Analytics zu keinem Zeitpunkt an die Firma Google übertragen

Google: Internetsuchmaschine des US-Unternehmens Google Inc. mit Marktanteilen von mehr als 80 Prozent aller weltweiten Suchanfragen

IBI-Care: Elektronisches Erfassungssystem der Universitären Psychiatrischen Dienste für die an den Patienten erbrachten Leistungen

ICT: Information and Communication Technology (zu Deutsch: Informations- und Kommunikationstechnologie)

IDES: International Documentation and Evaluation System: Am Institut für evaluative Forschung in der orthopädischen Chirurgie entwickeltes mehrsprachiges Orthopädie-Implantatregister

i-pdos: Integriertes Patientendossier Insele Spital

ISDS: Informationssicherheit und Datenschutz

ISIS: Informatisiertes Staatsschutz-Informationssystem, wird vom Nachrichtendienst des Bundes betrieben

IT-(Sicherheitsbeauftragter): Informationstechnologie (auch NewIT)

IV: Invalidenversicherung

KAIO: Kantonales Amt für Informatik und Organisation

kiSro: Klinikinformationssystem der SRO AG (elektronische Behandlungsdokumentation)

KSL: Kernsystem Lehre: Informatikprogramm der Universität

Limsophy-Lims: Informatikprogramm zur Unterstützung von Lebensmittelkontrollen

de la population et des sports

DEP: dossier électronique du patient (Hôpital de l'île)

ELA\_DMS: archivage électronique et système de gestion des documents (du CHR Spitaler FMI AG: hôpitaux de Frutigen, Meiringen et Interlaken)

ePUB: système d'administration électronique des examens de l'Université de Berne

E-VAS GG: remplacement du système de taxation de l'impôt sur les gains immobiliers

E-voting: projet de procédure de vote électronique qui ne concerne pour l'instant que les Suisses et Suissesses de l'étranger.

eVUB: répertoire électronique des cours de l'Université de Berne

Facebook: réseau social sur Internet qui permet d'échanger des informations personnelles.

FMI AG: hôpitaux de Frutigen, Meiringen et Interlaken

GELAN: système d'information agricole commun aux cantons de Berne, de Fribourg et de Soleure

Google Analytics („\_anonymizelp()"): application permettant d'évaluer le comportement des visiteurs de sites Internet. La fonction "\_anonymizelp()" empêche l'identification de l'adresse Internet de l'utilisateur.

Google Urchin: application permettant d'évaluer le comportement des visiteurs de sites Internet; contrairement à ce qui se passe avec Google Analytics, les données collectées ne sont à aucun moment transmises à la société Google.

Google: moteur de recherche sur Internet de l'entreprise étasunienne Google Inc. qui, à l'échelle mondiale, détient plus de 80 pour cent des parts de marché.

HESB: Haute école spécialisée bernoise

HESB-Card: carte à puce multifonctionnelle de la HESB (légitimation, comptabilisation des frais)

IBI-Care: système de saisie électronique des prestations fournies aux patients par les Services psychiatriques universitaires

IDES (International Documentation and Evaluation System): projet multilingue de registre des implants de l'Institut de recherche évaluative en chirurgie orthopédique

INS: Direction de l'instruction publique

ISIS: système d'information relatif à la protection de l'Etat exploité par le Service de renseignement de la Confédération

Journalisation: tenue d'un procès-verbal de l'état d'un système d'information (enregistrement du comportement des utilisateurs)

kiSro: système d'informations cliniques du CHR SRO AG (dossiers médicaux électroniques)

KSL: programme informatique de l'Université de Berne

Limsophy Lims: programme informatique pour le contrôle des denrées alimentaires

NESKO: système informatique de l'Intendance des impôts, servant à la taxation et à la perception

OACOT: Office des affaires communales et de l'organisation du territoire

OIO: Office cantonal d'informatique et d'organisation

OPALE: application de gestion administrative des patients des Services psychiatriques Jura bernois–Bienne–Seeland à Bellélay

OPROAD: projet informatique de la HESB visant à optimiser

Logging: Protokollierung von Informationen über den Zustand eines Informationssystems (Aufzeichnung des Benutzerverhaltens)

Mobile Security: Sicherheit von tragbaren, elektronischen Geräten, z.B. von Mobiltelefonen

NDB: Nachrichtendienst des Bundes (für den Staatsschutz zuständige Organisationseinheit des VBS)

NESKO: Neues Steuerkonzept: Gesamtheit der Steuerveranlagungs- und Steuerbezugsapplikationen

Observation: Beobachtung durch die Polizei

OPALE: Patientenverwaltungsinformatikprojekt der Psychiatrischen Dienste Biel-Seeland – Berner Jura Bellelay

OPROAD: Informatikprojekt der BFH zur Prozessoptimierung in der Studierendenadministration

OPTIMO: Optimierung der Mobilisierung im Kanton Bern, von der Kantonspolizei betriebene Informatikanwendung für das

Outlook (Kalender): Kalenderfunktion der Applikation Microsoft Outlook (E-Mail, Kontakte, Aufgaben, gemeinsame Kalender)

PACS: Picture Archiving and Communication System: Bildarchivierungs- und Kommunikationssystem in der Medizin

Persiska: Personal- und Informationssystem des Kantons Bern

Polypoint: Informatiklösung für Spitäler, mit Funktionalitäten zu Codierung, Leistungserfassung, Auftragsmanagement und elektronischer Krankengeschichte

präventivpolizeilich: Polizeiliches Handeln zur Gefahrenabwehr

PRIVATIM: Vereinigung der Schweizerischen Datenschutzbeauftragten

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.

Smartcard-Management-System: System zur Verwaltung von kreditkartenähnlichen Datenträgern, die Authentifizierungsinformation enthalten

SNB: Spitalnetz Bern AG (Spitäler Aarberg, Münsingen, Riggisberg, Tiefenau und Ziegler, Spital und Altersheim Belp, Pflegezentrum Elfenau)

SRO: Spital Region Oberaargau

UNICARD: Informatiksystem der Universität Bern zur Ausstellung und Verwaltung der elektronischen Legitimationskarte mit Chip

VA NP: Veranlagung Natürliche Personen; System der Steuerverwaltung

VBS: Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport

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

VKS: Verkehrskontrollsystem

VSPH: Informatiksystem der Pädagogischen Hochschule, welches der elektronischen Unterstützung der Geschäftsprozesse der Verwaltung dient

## 2. Referenznummern der in Ziffer 7 aufgeführten Justizentscheide; Hinweis auf Rechtsgutachten

les processus d'administration des étudiants

OPTIMO: optimisation de la mobilisation dans le canton de Berne (application de la Police cantonale pour la mobilisation des forces de police et des services de défense)

Outlook (calendrier): agenda de l'application Microsoft Outlook (courrier, contacts, tâches, calendrier partagé)

PACS (Picture Archiving and Communication System): système permettant de gérer les images médicales grâce à des fonctions d'archivage

PERSISKA: Système d'information sur le personnel du canton de Berne

PFPDT: préposé fédéral à la protection des données et à la transparence

Polypoint: solution informatique pour hôpitaux, avec des fonctionnalités telles que le codage, la saisie des prestations, la gestion des mandats et l'anamnèse électronique

PRIVATIM: association des Commissaires suisses à la protection des données

Salon de cyberbavardage: lieu de rencontre virtuel qui permet de converser en temps réel.

Sécurité mobile: sécurité d'appareils électroniques portables, p. ex. de téléphones

SIPD: sûreté de l'information et protection des données

SIS (Système d'information Schengen): système des Etats de Schengen grâce auquel les données d'objets ou de personnes recherchés peuvent être notifiées et interrogées très rapidement dans tout l'espace Schengen.

SNB: Spitalnetz Bern AG (réseau constitué des hôpitaux d'Aarberg, de Münsingen et de Riggisberg, des hôpitaux Tiefenau et Ziegler, de l'hôpital et foyer pour personnes âgées de Belp et du centre de soins d'Elfenau)

SRC: Service de renseignement de la Confédération (service du DDPS compétent en matière de protection de l'Etat)

SRO: centre hospitalier régional de Haute-Argovie

Système de gestion de cartes à puce: système d'administration de supports de données semblables aux cartes de crédit qui contiennent des informations d'authentification.

TIC: technologies de l'information et de la communication

UNICARD: système informatique de l'Université de Berne servant à l'établissement et à la gestion des cartes de légitimation à puce

VA-NP: taxation des personnes physiques, système de l'Intendance des impôts

VICLAS: Violent Crime Linkage Analysis System – système d'analyse des crimes violents devant servir à l'identification des criminels en série

VKS: système de contrôle de la circulation

VSPH: système informatique de la Haute école pédagogique destiné au soutien des processus administratifs

## 2. Numéros de référence des décisions de justice mentionnées au chiffre 7; références d'avis de droit



- 7.1: Entscheid des Regierungsstatthalters von Biel vom 9.7.2010: vbv 327/2010
- 7.2: BGE vom 13.10.2010: 1C\_315/2009 (VidV BE);
- 7.3: BGE vom 29.10.2010: 1C\_284/2010 (Gewaltstudie)
- 7.4: VGE vom 29.06.2010: 100.2008.23415U (Aufgabendi-  
alog)
- 7.6: Prof. Dr. iur. Thomas Gächter: Informationsaustausch  
im Umfeld der Sozialhilfe, Rechtsgutachten zuhanden  
der Gesundheits- und Fürsorgedirektion des Kantons  
Bern; abrufbar unter [www.be.ch/gef](http://www.be.ch/gef)

### 3. Internetadresse der Karte der bewilligten Video- überwachungsanlagen

- 9: [www.geoportal.sites.be.ch/site/bve\\_geo\\_karte\\_video](http://www.geoportal.sites.be.ch/site/bve_geo_karte_video)

- 7.1: Décision sur recours du préfet de Bienne du 9.7.2010:  
vbv 327/2010
- 7.2: ATF du 13.10.2010: 1C\_315/2009 (ordonnance sur la  
vidéosurveillance);
- 7.3: ATF du 29.10.2010: 1C\_284/2010 (étude sur la vio-  
lence)
- 7.4: JTA du 29.06.2010: 100.2008.23415U (dialogue sur les  
prestations)
- 7.6: Avis de droit sur l'échange d'informations dans le  
contexte de l'aide sociale rédigé par le professeur Tho-  
mas Gächter à l'attention de la Direction de la santé  
publique et de la prévoyance sociale, disponible (en al-  
lemand) à l'adresse: [www.be.ch/gef](http://www.be.ch/gef)

### 3. Adresse Internet de la carte des installations de vi- déosurveillance autorisées

- 9: [http://www.geoportal.sites.be.ch/site/fr/bve\\_geo\\_karte\\_](http://www.geoportal.sites.be.ch/site/fr/bve_geo_karte_video)  
video