2 Bericht der Aufsichtsstelle für Datenschutz

2.1 Einleitung

2.1.1 Auf einen Blick

Informatikanwendungen werden immer komplexer. Etwa das Klinikinformationssystem des Spitalzentrums Biel zeigt dies. Der Zugriff auf die Patientenakte ist von einer Vielzahl sich überschneidender Kriterien abhängig: So dürfen Ärzte und Ärztinnen auch auf die geschlossene Akte einer andern Klinik greifen, falls ein Klinikwechsel stattfand. Dem Pflegepersonal darf aber nur die offene Patientenakte der eigenen Station zugänglich sein. Mit der hohen Komplexität der Systeme wird es auch schwieriger, die Systeme sicher zu betreiben. Die von externen Stellen durchgeführten Kontrollen zeigten bei der Informatiksicherheit ausnahmslos Verbesserungsmöglichkeiten.

2.1.2 Zusammenarbeit mit dem Eidgenössischen Datenschutzbeauftragten und der Vereinigung der Schweizerischen Datenschutzbeauftragten

Verschmutzen Berufsschüler in der Mittagspause die Mikrowellengeräte, sollen sie mit einer biometrischen Zugangskontrolle überführt werden (Fingerprint). Für einen solchen Versuch mögen im Schulumfeld Freiheiten bestehen. Der Versuch zeigt aber, dass biometrische Daten rasch im Alltag anzutreffen sein werden. Die Vereinigung der Schweizerischen Datenschutzbeauftragten führte gemeinsam mit der Stiftung für Datenschutz und Informationssicherheit eine Veranstaltung zum Thema Biometrie durch. Gemeinsam mit weiteren Partnern erfolgte eine Veranstaltung zum Thema Biobanken. (Zur Zusammenarbeit bei Bundeserlassen s. 2.6.1).

2.2 Aufgabenumschreibung, Prioritäten, Mittel

2.2.1 Prioritäten

Für das Bearbeiten der Geschäfte gilt unverändert folgende Prioritätenfolge: 1. Datenschutzkonzepte für Informatikprojekte, 2. Betreuung des Beizugs 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 geringen Wiederholungschancen.
Mehr als 1½ Bundesordner füllten die Unterlagen zum Datenschutzkonzept für das Klinikinformationssystem des Spitalzentrums Biel (s. 2.1.1 und 2.7.1). Sind mehrere

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

2.1 Introduction

2.1.1 2005 en bref

Les applications informatiques deviennent toujours plus complexes, comme en témoigne par exemple le système d'informations cliniques du Centre hospitalier de Bienne. L'accès aux dossiers des patients dépend d'une multitude de critères qui se recoupent: c'est ainsi qu'en cas de transfert d'un patient, les médecins peuvent accéder au dossier clos d'une autre clinique. Par contre, le personnel soignant n'est quant à lui habilité à consulter que le dossier ouvert dans son propre service. Il est d'autant plus difficile de garantir la sécurité de l'exploitation des systèmes que ceux-ci sont extrêmement complexes, et les contrôles effectués par des services externes ont immanquablement révélé des possibilités d'amélioration.

2.1.2 Collaboration avec le préposé fédéral à la protection des données et l'association des Commissaires suisses à la protection des données

Une école professionnelle a cherché à confondre au moyen d'un contrôle biométrique des accès (empreintes digitales) ceux de ses élèves qui, pendant la pause de midi, salissaient les fours à micro-ondes. Il existe certes une marge d'action pour procéder à une telle expérience au sein d'une école. Celle-ci n'en a pas moins révélé à quel point les données biométriques vont rapidement se diffuser dans la vie quotidienne. L'association des Commissaires suisses à la protection des données a organisé en collaboration avec la Stiftung für Datenschutz und Informationssicherheit un symposium consacré à la biométrie. Une manifestation sur les banques de données biologiques a par ailleurs été mise sur pied avec d'autres partenaires. (Cf. ch. 2.6.1 s'agissant de la coopération en relation avec les actes législatifs fédéraux.)

2.2 Description des tâches, priorités, moyens à disposition

2.2.1 Priorités

Les dossiers continuent à être traités en fonction des priorités suivantes: 1) les schémas de protection des données concernant des projets informatiques, 2) le suivi des mandats confiés à des services de contrôle externes, 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.
Les documents relatifs au schéma de protection des données du système d'informations cliniques du Centre hospitalier de

[1] http://www.be.ch/aktuell/default.aspx?action=2&mmid=16821

Datenschutzkonzepte von diesem Umfang zu prüfen, überschreitet dies die Kapazität der Datenschutzaufsichtsstelle. Es ist bezeichnend, dass für vier Datenschutzkonzepte zur Zeit die Behandlung aus Kapazitätsgründen zurückgestellt worden ist (E-VAS JP: Ersatz Veranlagungssystem Juristische Personen der Steuerverwaltung[1], TaxMe–Portal: Internetzugang des Bürgers auf seine Steuerdaten und Infrastruktur für weitere E-Government-Anwendungen[2], QST 2: Ersatz der Applikation Quellensteuer der Steuerverwaltung, FACTScience: Organisatorische und administrative Verwaltung und Planung des Dekanats und der Studienplanung der Medizinischen Fakultät). Die Überprüfung der Ressourcensituation erscheint daher nicht nur mit Blick auf allfällige neue Aufgaben der Datenschutzaufsichtsstelle aus den Abkommen von Schengen und Dublin (s. 2.6.1) sinnvoll.

2.2.2 Eigenverantwortung der datenbearbeitenden Stellen

Viele Amtsstellen klären bei der Datenschutzaufsichtsstelle die Zulässigkeit einer Datenbekanntgabe an eine andere Behörde ab (Amtshilfe). Sie sorgen damit für eine korrekte Datenbearbeitung in diesem besonders heiklen Bereich. (Zur Datenschutzzertifizierung des Amtes für Sozialversicherung und Stiftungsaufsicht s. 2.10.2, zu den Datenschutzanleitungen im Gesundheitswesen s. 2.7).

2.2.3 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Jahr 2005 waren 42 Millionen CHF in Informatikmittel zu investieren. 140 Millionen CHF (davon 59 Mio. CHF für Drittdienstleister) sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). Für die Prüfung von Informatikanwendungen durch externe Prüfstellen stand der Betrag von CHF 130'000 zur Verfügung (s. 2.2.4). Das Amt für Informatik und Organisation finanzierte die Überarbeitung der aktuellen Informatiksicherheits-Sollvorgaben (s. 2.3.1). In den Ausgaben für Informatikprojekte (gerade auch bei Klinikinformationssystemen s. 2.7.1) sind auch Aufwendungen für die Erstellung von Datenschutzkonzepten enthalten. Die Beratung von Gemeinden und Verwaltungsstellen in Datenschutzfragen durch die fachlich zuständigen Rechtsdienste bringt ebenfalls eine Bindung von Ressourcen für den Datenschutz mit sich. Nicht zu übersehen ist aber, dass die Informatikmittel kontinuierlich anwachsen und die von Anfang an knappen Datenschutzmittel mit dieser Entwicklung nicht Schritt halten.

Bienne (cf. ch. 2.1.1 et 2.7.1) remplissent plus d'un classeur fédéral et demi. L'examen de plusieurs schémas de cette envergure excède les capacités du Bureau. Il est révélateur, à cet égard, que le traitement de quatre schémas soit actuellement reporté faute de ressources (E-VAS JP: remplacement du système de taxation des personnes morales de l'Intendance des impôts[3], portail TaxMe: accès Internet du citoyen à ses données fiscales et infrastructure pour d'autres applications de cyber-administration[4], QST 2: remplacement de l'application de l'Intendance des impôts concernant l'impôt à la source, FACTScience: gestion et planification du Décanat sous les angles organisationnel et administratif ainsi que planification des études à la Faculté de médecine). Au vu de ce qui précède, un réexamen de la question des ressources paraît judicieux, d'autant plus que les accords de Schengen et de Dublin pourraient imposer de nouvelles tâches au Bureau (cf. ch. 2.6.1).

2.2.2 Responsabilité propre des services traitant des données

Nombreux sont les services qui, soucieux de ne pas commettre d'erreurs dans un domaine particulièrement sensible, consultent le Bureau sur l'admissibilité de la transmission de données à une autre autorité (entraide administrative). (Cf. ch. 2.10.2 s'agissant de la certification obtenue par l'Office des assurances sociales et de la surveillance des fondations en matière de protection des données, et ch. 2.7 au sujet des instructions en matière de protection des données dans le domaine de la santé.)

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

Les investissements prévus dans le domaine informatique se montaient à 42 millions de francs, alors que 140 millions de francs (dont CHF 59 mio destinés à des tiers prestataires de services) devaient être consacrés à l'exploitation (montants budgétés). Une somme de 130 000 francs était en outre disponible pour le contrôle des applications informatiques par des services externes (cf. ch. 2.2.4). Par ailleurs, l'Office d'informatique et d'organisation a financé la mise à jour des consignes en matière de sécurité informatique (cf. ch. 2.3.1). A cela s'ajoute que les dépenses destinées aux projets informatiques (et en particulier aux systèmes d'informations cliniques, cf. ch. 2.7.1) incluent désormais les charges liées à l'établissement des schémas de protection des données. Enfin, les conseils qui sont dispensés aux communes et aux unités administratives par les services juridiques spécialisés compétents entraînent également l'affectation de moyens à la protection des données. Il n'en reste pas moins que les ressources consacrées à l'informatique ne cessent de croître tandis que celles qui sont destinées à la protection des don-

---

2 http://www.fin.be.ch/site/sv-taxme

3 http://www.be.ch/aktuell/default-f.aspx?action=2&mmid=16822

4 http://www.fin.be.ch/site/fr/sv-taxme

2.2.4 Kontrollen von Informatikdatenbearbeitungen

Die Überprüfung der Ordnungsbussenzentrale durch eine externe Kontrollstelle ergab im Wesentlichen ein positives Bild. Mehrere Empfehlungen der Kontrollstelle wurden unmittelbar umgesetzt. Differenzen zur Betriebsbewilligung (Adresserhebung, Archivierung) stehen noch zur Klärung an. Ein ähnliches Bild zeigte die Prüfung der Informatikanwendung ELAR (elektronisches Archiv) des Amtes für Migration und Personenstand. Die vorgeschlagenen, zum Teil gewichtigen Verbesserungen will das Amt für Migration und Personenstand umsetzen. Die gleiche Haltung nimmt das Amt für Informatik und Organisation zu den bei der Prüfung des kantonsweit im Einsatz stehenden Zeiterfassungssystems inova.time ein. Zum Zeitpunkt der Berichterstattung lag der Prüfungsbericht zu der beim Polizeikommando durchzuführenden Überprüfung der Anwendung OBORA (Protokollierung der Zugriffe auf Rapporte etc.) noch nicht vor. Gleiches gilt für den Prüfbericht zur Anwendung SCHÜBE der Erziehungsdirektion (elektronische Schülerbeurteilung[5]).
Die Erfahrungen mit dem Beizug externer Kontrollstellen sind nach wie vor positiv. Die Bereitschaft der datenbearbeitenden Stellen zu Verbesserungen ist hoch.
Die fehlende Aktualität der Informatiksicherheits-Sollvorgaben (s. zu deren Überarbeitung 2.3.1) verlangt von den externen Kontrolleuren nicht selten eine gewisse Improvisation. Findet diese in Absprache mit der datenbearbeitenden Stelle statt, erleidet die Akzeptanz gegenüber den Prüfungsberichten keinen Einbruch.
Die Finanzkontrolle hat im Rahmen der Wirtschaftsprüfung die Risikobeurteilung im Informatikbereich der Dienststellen weitergeführt. Den im BEDAG-Gesetz umschriebenen Auftrag zu einer jährlichen schwerpunktmässigen Prüfung der Informatiksicherheit durch eine externe Fachstelle setzte die BEDAG-Informatik AG mit einem Aufrechterhaltungsaudit um (Aufrechterhaltung des Zertifikats für die Informatiksicherheit nach dem British Standard BS 7799–2:2002[6]). Die Datenschutzaufsichtsstelle begrüsst die für den Erwerb und Erhalt von Zertifikaten erforderlichen Kontrollhandlungen. Was die Prüfungen abdecken, ist jedoch genauer zu prüfen. Der Auftraggeber kann unter Umständen den Gegenstand der Zertifizierung einschränken und damit von der Kontrolle ausnehmen. So hat die BEDAG-Informatik AG die in BS 7799 vorgesehenen Teile „Disziplinierung, Heimarbeit und Sicherheitsüberprüfung von Mitarbeitenden“ von der Zertifizierung ausgenommen.

nées, d'emblée limitées, ne suivent pas la même évolution.

2.2.4 Contrôle du traitement de données informatiques

L'examen de la centrale des amendes d'ordre par un service de contrôle externe a dégagé une image d'ensemble positive, et plusieurs des recommandations formulées à cette occasion ont été immédiatement prises en compte; quelques divergences par rapport à l'autorisation d'exploiter (collecte des adresses, archivage) font encore l'objet d'une mise au point. La même constatation favorable vaut pour l'examen de l'application informatique ELAR (archives électroniques) de l'Office de la population et des migrations, qui entend mettre en œuvre les améliorations proposées, dont certaines revêtent une importance capitale. L'Office d'informatique et d'organisation a adopté une attitude semblable lors de l'examen du système de saisie du temps de travail inova.time, en usage à l'échelle cantonale. Le compte rendu de l'examen dont l'application OBORA du Commandement de la police doit faire l'objet (journalisation des accès aux rapports, etc.) n'était toujours pas disponible au moment de la rédaction du présent rapport, pas plus que celui de l'application "Schübe" (évaluation des élèves sur support électronique) de la Direction de l'instruction publique[7].
Les expériences faites lors du recours à des services de contrôle externes restent positives, et les services traitant des données se montrent très ouverts aux propositions d'amélioration.
Il n'est pas rare que le caractère quelque peu dépassé des consignes en matière de sécurité informatique (cf. ch. 2.3.1 s'agissant de leur actualisation) amène les contrôleurs externes à improviser. Leurs solutions de remplacement restent toutefois bien acceptées par les services traitant des données pour autant que ceux-ci aient pu participer à leur élaboration.
A l'occasion des audits internes, le Contrôle des finances a poursuivi son appréciation des risques dans le domaine informatique des différents services. La Bedag Informatique SA qui est tenue, de par la loi sur la Bedag, de faire contrôler chaque année les points essentiels de la sécurité de l'information par un organe spécialisé externe et indépendant, s'est acquittée de ce mandat en demandant un audit de suivi (maintien de la certification de la sécurité informatique selon le British Standard BS 7799-2:2002[8]). Le Bureau se félicite des contrôles effectués en vue de l'obtention et du maintien des certificats. Il n'en reste pas moins nécessaire d'examiner de plus près la portée de telles démarches, car le mandant peut dans certains cas limiter l'objet de la certification et soustraire ainsi divers domaines au contrôle. La Bedag Informatique SA a procédé de la sorte en excluant de la certification les volets "discipline, travail à domicile et contrôle de sécurité concernant les collaborateurs" prévus dans le BS 7799.

---

5 http://www.erz.be.ch/site/fb-volksschule-beurteilung04

6 http://www.sqs.ch/index/leistungsangebot/h779.htm

7 http://www.erz.be.ch/site/fr/fb-volksschule-beurteilung04

8 http://www.sqs.ch/fr/index/leistungsangebot/h779.htm

2.3 Datensicherheit

Die Überschwemmungen führten bei Verwaltungsstellen im Berner Oberland zu längeren Unterbrüchen des kantonalen Weitbereichsnetzes BEWAN. Netzwerke umfassend vor Ausfällen zu sichern, ist nicht möglich. Für die durch die Überschwemmungen stark geforderten Regierungsstatthalterämter führte der Netzunterbruch zum Ausfall der als Terminalserver-Lösung aufgebauten Systeme, etwa der Textsysteme. Die Regierungsstatthalterämter halfen sich unter anderem mit Notebooks weiter. Vor solchen Erfahrungen leuchtet es ein, wenn etwa das Spitalzentrum Biel für sein Klinikinformationssystem vorsieht, dass die zur Patientenpflege dringend notwendigen Daten auf den Stationen auf Notebooks abkopiert und ständig aktualisiert werden müssen (s. 2.7.1).

2.3.1 Informatiksicherheits-Sollvorgaben

Die vom Regierungsrat gesetzte Frist zur Überarbeitung der Informatiksicherheits-Sollvorgaben (Ende 2005) wurde nicht eingehalten. Das Amt für Informatik und Organisation zog bei der Ausarbeitung eine externe Stelle bei. Umfangreiche Papiere liegen als Entwurf vor. Neben der Gesamterneuerung der Informatiksicherheits-Sollvorgaben arbeitet das Amt für Informatik und Organisation ständig an Weisungen zu Teilbereichen. So wurde etwa eine Weisung zum sicheren Einsatz von Drahtlosnetzwerken erlassen.

2.3.2 Sicherheit von E-Mail

Zum Datenschutzkonzept für das Informatikprojekt BEMAIL III (Erneuerung der kantonalen Mailinfrastruktur) war festzuhalten, dass dieses Projekt nicht zur Einführung eines sicheren Mailsystems führt. Dieses Ziel soll allenfalls mit einem separaten Projekt erreicht werden. Für ein sicheres Mailsystem von Bedeutung ist das Informatikprojekt „Einsatz der Admin-PKI[9]“. Es soll den Zugang zu Bundesanwendungen mittels elektronischer Zertifikate ermöglichen (Anmeldeinfrastruktur). Der Einsatz dieser elektronischen Zertifikate für einen sicheren Mailbetrieb ist in einem künftigen Ausbau denkbar. Das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur[10] umschreibt die Voraussetzungen für den Einsatz elektronisch unterschriebener Mails. Die Firma Swisscom Solutions hat inzwischen die Zertifizierung als Dienstanbieter für qualifizierte elektronische Signaturen erhalten[11]. Der Einsatz von solchen Zertifikaten ist für den Kanton Bern aber bis auf weiteres nicht vorgesehen.

2.3 Sécurité des données

Dans certains services administratifs de l'Oberland bernois, les inondations ont entraîné d'assez longues interruptions du réseau cantonal de communications longues distances BEWAN. En tout état de cause, il n'est pas possible de protéger complètement les réseaux contre les pannes. Dans les préfectures, fortement sollicitées lors des intempéries, l'interruption du réseau a rendu inutilisables les systèmes – traitement de texte notamment – dont le fonctionnement est assuré par des serveurs de terminaux. En conséquence, il a notamment fallu recourir à des ordinateurs portables. A la lumière de telles expériences, il est compréhensible que le système d'informations cliniques du Centre hospitalier de Bienne par exemple prévoie l'obligation de copier et d'actualiser en permanence sur des portables, dans les services, les données indispensables aux soins des patients (cf. ch. 2.7.1).

2.3.1 Consignes en matière de sécurité informatique

Le délai imparti par le Conseil-exécutif pour remanier les consignes de sécurité informatique (fin 2005) n'a pas été respecté. L'Office d'informatique et d'organisation a fait appel à un service externe, et de nombreux documents existent déjà à l'état de projets. Outre le renouvellement intégral des consignes précitées, l'office élabore en permanence des instructions concernant des domaines partiels. L'une d'entre elles, édictée pendant l'exercice, concerne la sécurité de l'utilisation des réseaux sans fil.

2.3.2 Sécurité du courrier électronique

Le Bureau a relevé à propos du schéma de protection des données du projet informatique BEMAIL III (renouvellement du système cantonal de messagerie électronique) que la sécurité du système n'était pas garantie. Le cas échéant, un projet distinct pourrait permettre de combler cette lacune. En matière de sécurité du courrier électronique, le projet informatique portant sur l'utilisation de l'infrastructure Admin-PKI[12] – qui doit permettre l'accès aux applications de la Confédération au moyen de certificats électroniques (infrastructure de certification) – n'est pas dénué d'importance. Lors d'une extension future, il est envisageable de recourir à de tels certificats afin de garantir la sécurité de la messagerie électronique. La loi fédérale sur les services de certification dans le domaine de la signature électronique[13] fixe les conditions applicables à l'utilisation de courriels munis d'une signature électronique. Depuis son entrée en vigueur, la société Swisscom Solutions a obtenu la certification en tant que prestataire de signatures électroniques qualifiées[14]. Le can-

9 http://www.sik.admin.ch/D/ite/docs/2004/StudiePKI-V51.pdf

10 http://www.admin.ch/ch/d/sr/c943_03.html

11 http://www.swisscom.com/GHQ/content/Media/Medienmitteilungen/2005/20051207_01_elektronische_Signaturen.htm?lang=de

12 http://www.sik.admin.ch/D/App/PKI/doc/EtudePKI-V51.pdf

13 http://www.admin.ch/ch/f/rs/c943_03.html

14 http://www.swisscom.com/GHQ/content/Media/Medienmitteilungen/2005/20051207_01_elektronische_Signaturen.htm?lang=fr

2.4 Informatikprojekte

Zu drei Informatikprojekten der Steuerverwaltung (s. 2.2.1) wurden Datenschutzkonzepte wohl erstellt, diese der Datenschutzaufsichtsstelle aber erst auf Rückfrage hin nach dem Ausgabenbeschluss unterbreitet. Die Vorgabe des Regierungsrates, Informatikprojekte ab CHF 100'000 nur mit einem Datenschutzkonzept zum Ausgabenbeschluss zu unterbreiten, muss sich daher nach wie vor noch festigen.

2.4.1 Betreute Projekte

Ein Datenschutzkonzept unterbreiteten die Projektleitungen für die Projekte ePub (elektronische Prüfungsadministration der Universität Bern, s. 2.5 und 2.6.2), EITIS (Ersatz technische IT-Infrastruktur der Justiz-, Gemeinde- und Kirchendirektion), Integration MOFIS (Anschluss an das Motorfahrzeuginformationssystem des Bundes), Einsatz Admin-PKI (s. 2.3.2) und BEMAIL III (s. 2.3.2). Das Amt für Migration und Personenstand unterbreitete zwei Projekte. Bei DIFA (Digitalisierung und Indexierung der Familienregister und Burgerrodel) ging es um eine freiwillige Prüfung, da das Datenschutzgesetz auf öffentliche Register des Privatrechtsverkehrs keine Anwendung findet. Hinzuweisen war unter anderem auf die Schutzbedürfnisse erkennbarer Angehöriger verstorbener Personen. Für GAGED (Geschäftskontrolle Garantienehmer/Garantiegeber für Reisekosten ausländischer Besucher) muss vorerst noch eine Rechtsgrundlage geschaffen werden. Neben dem Klinikinformationssystem des Spitalzentrums Biel (s. 2.2.1 und 2.7.1) waren für Spitäler folgende Projekte zu prüfen: M4I (Materialwirtschaftslösung Inselspital), Ablösung FINANZ400 und HANDEL400 Spitalgruppe Bern und Laborinformationssystem des Spitalzentrums Biel. Neue Personensuchsysteme für Spitäler erlauben die Gesprächsaufzeichnung für interne Notfallanrufe. Das Psychiatriezentrum Münsingen war darauf hinzuweisen, dass solche Gesprächsaufzeichnungen unverhältnismässig sind und die erforderliche Rechtsgrundlage fehlt.

(Zu den bei der Behandlung von Datenschutzkonzepten entstandenen Ressourcenproblemen und den zurückgestellten Datenschutzkonzepten s. 2.2.1).

2.4.2 Aufsichtsrechtliche Rückfragen zu Informatikprojekten

Bei Online-Voranmeldungen an Hochschulen werden regelmässig besonders schützenswerte Daten übertragen.

2.4 Projets informatiques

Des schémas de protection des données ont certes été établis pour trois projets informatiques de l'Intendance des impôts (cf. ch. 2.2.1), mais n'ont été soumis au Bureau que suite à l'intervention de ce dernier, une fois la dépense autorisée. Cet exemple montre bien que le respect de la consigne du Conseil-exécutif selon laquelle les demandes d'autorisation de dépense pour tous les projets informatiques portant sur un montant supérieur à 100 000 francs doivent impérativement être accompagnées d'un schéma de protection des données ne va toujours pas de soi.

2.4.1 Projets suivis par le Bureau

Des schémas de protection des données ont été présentés par les directions de divers projets informatiques: ePub (administration électronique des examens à l'Université de Berne, cf. ch. 2.5 et 2.6.2), EITIS (remplacement de l'infrastructure informatique de la Direction de la justice, des affaires communales et des affaires ecclésiastiques), projet MOFIS (accès aux registres nationaux des conducteurs et des véhicules), utilisation de l'infrastructure Admin-PKI (cf. ch. 2.3.2) et BEMAIL III (cf. ch. 2.3.2). L'Office de la population et des migrations a présenté deux projets: A propos de DIFA (numérisation et indexation du registre des familles et du rôle des bourgeois), l'examen était de nature facultative car la loi sur la protection des données ne s'applique pas aux registres publics dans lesquels sont consignés des faits de droit privé. Dans ce contexte, le Bureau a notamment dû relever que les proches reconnaissables de personnes décédées doivent bénéficier d'une protection. S'agissant de GAGEC (contrôle de gestion pour les garanties concernant les visiteurs étrangers), il convient dans un premier temps de créer une base légale. Outre le système d'informations cliniques du Centre hospitalier de Bienne (cf. ch. 2.2.1 et 2.7.1), les projets suivants ont été examinés dans le domaine hospitalier: M4I (système de gestion du matériel de l'Hôpital de l'Ile), remplacement de FINANZ400 et de HANDEL400 du groupe Spital Bern et système de gestion de l'information de laboratoire du Centre hospitalier de Bienne. De nouveaux systèmes de recherche de personnes destinés aux hôpitaux permettent l'enregistrement des appels d'urgence internes. Le Bureau a dû attirer l'attention du Centre psychiatrique de Münsingen sur le caractère disproportionné de tels enregistrements de conversations et sur l'absence de base légale en la matière.

(S'agissant de l'insuffisance des ressources pour traiter les schémas de protection des données et des reports qui en résultent, il est renvoyé au ch. 2.2.1.)

2.4.2 Interventions de l'autorité de surveillance à propos de projets informatiques

La transmission de données particulièrement dignes de protection est fréquente lors de préinscriptions en ligne aux

Das setzt eine verschlüsselte Datenübertragung voraus. Sowohl die pädagogische Hochschule als auch die Universität sicherten die Einführung einer Verschlüsselung auf aufsichtsrechtliche Nachfrage hin zu. Das Polizeikommando regelte auf aufsichtsrechtliche Nachfrage hin die Zugriffsrechte auf die Fotos der Mitarbeitenden in der Datenbank AVANTI.

2.5 Internet und E-Government

(S. zum Informatikprojekt ePub 2.4.1 und 2.6.2; zur Online-Anmeldung an Hochschulen 2.4.2; zum TaxMe-Portal der Steuerverwaltung 2.2.1).

2.6 Gesetzgebung

2.6.1 Bundeserlasse, Schengen/Dublin

Zum Bundesgesetz über polizeiliche Informationssysteme des Bundes (BPI)[15] sowie zum Vorentwurf zur Änderung des Gesetzes und der Verordnung über die Ausweise für Schweizer Staatsangehörige (Einführung des biometrischen Passes[16]) verwies die Datenschutzaufsichtsstelle kantonsintern jeweils auf die Stellungnahme der Vereinigung der Schweizerischen Datenschutzbeauftragten.
Die Konferenz der Kantonsregierungen befasst sich zur Zeit mit den Auswirkungen der Abkommen zwischen der Schweiz und der EG über die Assoziierung der Schweiz an Dublin und Schengen[17]. Diese Abkommen umschreiben auch Anforderungen an die kantonalen Datenschutzaufsichtsstellen. Für den Kanton Bern wird – soweit zur Zeit ersichtlich – für die folgenden Bereiche verstärkt zu prüfen sein, ob die aktuelle Ausgestaltung der Datenschutzaufsicht genügt: Wirksame Einwirkungsbefugnisse der Datenschutzaufsichtsstelle (wie Recht zur Stellungnahme, Anordnungsrecht, Verwarnungs- oder Ermahnungsbefugnis), Klagerecht bzw. Anzeigebefugnis, Wahl/Abwahlvorgaben, Unzulässigkeit einer vollumfänglichen administrativen Zuordnung zu einer Organisationseinheit der Exekutive, genügende personelle und finanzielle Ressourcen.

2.6.2 Kantonale Erlasse

Das Informatikprojekt GERES (zentrale Plattform für Einwohnerkontrollen[21]) bedarf einer Abstützung in einem Gesetz. Diese soll im Gesetz über die Harmonisierung amtlicher Register erfolgen. Die im Gesetzesentwurf vor-

hautes écoles, ce qui présuppose un cryptage. Tant la Haute Ecole Pédagogique que l'Université de Berne ont promis l'introduction d'une telle mesure à la demande de l'autorité de surveillance. C'est également suite à l'intervention de cette autorité que le Commandement de la police a réglementé les droits d'accès aux photos des collaborateurs et collaboratrices dans la banque de données AVANTI.

2.5 Internet et cyber-administration

(Cf. ch. 2.4.1 et 2.6.2 à propos du projet informatique ePub, ch. 2.4.2 s'agissant des inscriptions en ligne aux hautes écoles, et 2.2.1 au sujet du portail TaxMe de l'Intendance des impôts.)

2.6 Législation

2.6.1 Législation fédérale, Schengen/Dublin

Le Bureau a renvoyé les instances cantonales à la prise de position de l'association des Commissaires suisses à la protection des données au sujet de la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP)[18] et de l'avant-projet de modification de la loi et de l'ordonnance sur les documents d'identité des ressortissants suisses (introduction du passeport biométrique[19]).
La Conférence des gouvernements cantonaux traite en ce moment des répercussions qu'auront les accords passés avec l'Union européenne au sujet de l'association de la Suisse à Schengen/Dublin[20]. Ces accords définissent entre autres des exigences vis-à-vis des services cantonaux responsables de la protection des données. Pour le canton de Berne, il s'agira d'examiner avec une attention accrue – au vu des connaissances actuelles – si l'organisation de la surveillance de la protection des données est suffisante dans les domaines suivants: pouvoirs effectifs d'intervention (p. ex. droit de rendre des avis, d'ordonner certaines mesures, de formuler un avertissement ou une admonestation), droit d'ester en justice ou de dénoncer les violations, consignes en matière d'élection ou de non-réélection, inadmissibilité d'une subordination administrative intégrale à une unité d'organisation de l'exécutif, mise à disposition des ressources humaines et financières nécessaires.

2.6.2 Législation cantonale

Le projet informatique GERES (plate-forme centrale pour la tenue des registres du contrôle des habitants[27]) requiert une base légale, qui trouvera sa place dans la loi sur l'harmonisation des registres officiels. De l'avis du Bureau toutefois,

15 http://www.fedpol.ch/d/archiv/medien/2005/050304_BPI_Vorentwurf_d.pdf
16 http://www.fedpol.ch/d/brennpunkt/index.htm
17 http://www.fedpol.ch/d/archiv/medien/2005/06051.htm
18 http://www.fedpol.ch/f/archiv/medien/2005/050304_BPI_Vorentwurf_f.pdf
19 http://www.fedpol.ch/f/brennpunkt/index.htm
20 http://www.fedpol.ch/f/archiv/medien/2005/06051.htm
21 http://www.fin.be.ch/site/kaio-projekt-geres-aktuell

gesehene Einführung einer persönlichen Identifikationsnummer (PIN, ZPV-Nummer) erfolgt nach Auffassung der Datenschutzaufsichtsstelle jedoch ohne genügende Schutzmassmassnahmen. Für unzulässig hält die Datenschutzaufsichtsstelle es zudem, gegenseitige Abrufverfahren in besonders schützenswerte Daten einzig auf Verordnungsstufe zu regeln.

Im Entwurf zu einem kantonalen Strassenverkehrsgesetz[22] wird davon abgesehen, für die Bekanntgabe von Fahrzeughalterinnen und Fahrzeughaltern eine Abrufmöglichkeit via Internet zu schaffen. Möglich soll einzig eine kostenpflichtige Telefonauskunft im Einzelfall sein. Für die Fahrzeughalterinnen und -Halter besteht eine Sperrmöglichkeit.

In der Spitalversorgungsverordnung[23] werden die Erbringer von Spital- und Rettungsleistungen verpflichtet, eine gemeinsame, fachlich unabhängige Aufsichtsstelle für Datenschutz zu führen. Damit werden die bisher in den Spitalgemeindeverbänden geführten Datenschutzaufsichtsstellen ersetzt.

Das Informatikprojekt ePub (2.4.1) führte zu einer Anpassung des Universitätsstatuts. Das in der bisherigen Fassung bestehende Verbot, auf elektronischem Weg heikle Personendaten zu übermitteln, soll aufgehoben werden. Dies kann nur dann zulässig sein, wenn für eine verschlüsselte Datenübertragung gesorgt wird. Ungenügend ist die Aufhebung des Verbotes zudem um die elektronische Gesuchstellung oder Eröffnung von Prüfungsentscheiden abzustützen. Hierzu ist eine differenzierte Regelung der elektronischen Verfahrensvorgaben zu treffen.

Mit der Personaldatenbekanntgabeverordnung[24] hat der Regierungsrat eine Rechtsgrundlage zur Bekanntgabe von nicht besonders schützenswerten Daten über Mitarbeitende auf dem Intranet oder auf dem Internet geschaffen. Gedacht ist an Telefon- und E-Mailverzeichnisse und an Publikationen, wie sie durch Zertifizierungsdienste (s. 2.3.2) verlangt werden. Die Finanzdatenabgleichsverordnung[25] schafft die Rechtsgrundlage um in den Finanzinformationssystemen Daten durch Abgleich mit andern Informatiksystemen aktualisieren zu können. Es geht um nicht besonders schützenswerte Daten.

Zur Verordnung über die Anstellung der Lehrkräfte und zur Verordnung über die Anstellung und Entschädigung der

l'introduction d'un numéro d'identification personnel (PIN, numéro GCP) prévue par le projet de loi n'est pas assortie de mesures de protection suffisantes; de plus, il n'est pas admissible de régler dans une simple ordonnance les procédures d'appel de données particulièrement dignes de protection.

Le projet de loi cantonale sur la circulation routière[28] ne prévoit que des interrogations téléphoniques soumises à émolument, au cas par cas, mais pas de procédure d'appel par Internet des données relatives aux personnes qui détiennent un véhicule. Ces dernières disposent par ailleurs d'un droit de blocage de leurs données.

L'ordonnance sur les soins hospitaliers[29] impose aux prestataires de soins hospitaliers et préhospitaliers l'obligation de désigner une autorité de surveillance commune indépendante pour la protection des données, qui remplacera les actuelles autorités de surveillance des services hospitaliers.

Le projet ePub (cf. ch. 2.4.1) entraîne une adaptation des statuts de l'Université, et il est prévu de supprimer l'interdiction de l'échange électronique de correspondance contenant des données personnelles particulièrement dignes de protection. Or, un tel changement n'est admissible que si le cryptage des données à transférer est garanti. La suppression de l'interdiction ne permet pas à elle seule l'envoi électronique de demandes ou la notification des décisions sanctionnant les examens, et une réglementation différenciée des procédures électroniques est indispensable.

Le Conseil-exécutif a créé dans l'ordonnance sur la communication de données personnelles[30] la base légale nécessaire à la diffusion, sur Internet ou Intranet, de données concernant le personnel qui ne sont pas particulièrement dignes de protection. Il s'agit notamment des répertoires téléphoniques et des listes d'adresses électroniques, ou encore des publications exigées par les services de certification (cf. ch. 2.3.2). L'ordonnance sur l'harmonisation des données financières[31] énonce quant à elle la base légale permettant l'actualisation des données – pas particulièrement dignes de protection – qui figurent dans les systèmes d'informations financières grâce à une harmonisation avec celles d'autres systèmes informatiques.

A propos de l'ordonnance sur le statut du personnel enseignant et de l'ordonnance sur la nomination et les indemnités des agents et des agentes de poursuites à fonction accessoire, le Bureau a dû préciser que l'employeur n'a aucun droit

---

22 http://www.be.ch/aktuell/default.aspx?action=2&mmid=16246

23 http://www.sta.be.ch/belex/d/BAG-pdf/BAG_06-10.pdf

24 http://www.sta.be.ch/belex/d/BAG-pdf/BAG_06-12.pdf

25 http://www.sta.be.ch/belex/d/BAG-pdf/BAG_06-13.pdf

26 http://www.sta.be.ch/belex/d/3/321_130.html

27 http://www.fin.be.ch/site/fr/kaio-projekt-geres-aktuell

28 http://www.be.ch/aktuell/default-f.aspx?action=2&mmid=16245

29 http://www.sta.be.ch/belex/f/ROB-pdf/ROB_06-10.pdf

30 http://www.sta.be.ch/belex/f/ROB-pdf/ROB_06-12.pdf

31 http://www.sta.be.ch/belex/f/ROB-pdf/ROB_06-13.pdf

32 http://www.sta.be.ch/belex/f/3/321_130.html

nebenamtlichen Betreibungsweibelinnen und -weibel war darauf hinzuweisen, dass der Arbeitgeber bei Arbeitszeugnissen keinen Anspruch auf Kenntnis der Art der Krankheit hat.
In der kantonalen DNA-Profilverordnung[26] werden vorab die Verantwortlichkeiten für die Umsetzung der im Bundesrecht vorgegebenen Löschungen von Amtes wegen in der DNA-Profildatenbank geregelt.

2.7 Gesundheitswesen

Für sein Personal erliess das Inselspital ein nach Aufgabengebieten aufgegliedertes Datenschutzmerkblatt. Die Gesundheits- und Fürsorgedirektion entwarf einen Leitfaden zur Schweigepflicht von Gesundheitsfachpersonen. (S. zur spitaleigenen Datenschutzaufsichtsstelle 2.6.2).

2.7.1 Klinikinformationssysteme

Mit dem vom Spitalzentrum Biel vorgelegten Datenschutzkonzept zum Klinikinformationssystem (s. 2.1.1, 2.2.1, 2.3) wurden erstmals die vom Spitalamt für alle Spitäler ausgearbeiteten Grundlagenpapiere (Rahmendatenschutzkonzept) für ein Informatikprojekt angewendet. Die erarbeiteten Papiere erwiesen sich als taugliche Grundlage. Mit dem Datenschutzkonzept konnte gezeigt werden, dass das Projekt datenschutzkonform umgesetzt werden kann. Bis zur Inbetriebnahme des Systems ist das Datenschutzkonzept aber fortzuschreiben. Das Zugriffskonzept wurde einzig im Sinne eines Beispiels für ein Drittspital vorgelegt. Es muss nun für das Spitalzentrum Biel konkretisiert werden. Bereits in einem Entscheid aus dem Jahre 1999 hielt die Gesundheits- und Fürsorgedirektion zu einem Spitalinformationssystem fest, der Patientennavigator dürfe die bisher von einem wieder eintretenden Patienten besuchten Abteilungen des Spitals nicht einschränkungslos offen legen. Dieser Vorgabe muss noch Rechnung getragen werden.

2.7.2 APDRG

Das Inselspital und die Spitäler Thun und Aarberg rechnen neu für stationäre Akutpatienten der allgemeinen Abteilung auch mit den Krankenversicherungen nach APDRG ab (Abrechnung nach 641 Fallpauschalen, All Patient Diagnoses Relatet Groups[33]). Bereits zur Abrechnung nach APDRG gegenüber den Unfallversicherungen hielt der Eidgenössische Datenschutzbeauftragte fest, für eine Abrechnung mit APDRG fehle die erforderliche gesetzliche Grundlage. Dies trifft für die Abrechnung gegenüber Krankenversicherungen ebenfalls zu. Dessen ungeachtet genehmigte der Regierungsrat die entsprechenden Verträge

33 http://www.isesuisse.ch/fr/index.htm

34 http://www.isesuisse.ch/fr/index.htm

à ce que les certificats médicaux des salariés renseignent sur la nature de la maladie.
Enfin, l'ordonnance cantonale sur les profils d'ADN[32] règle en particulier les compétences en vue de la mise en œuvre des dispositions de droit fédéral relatives à l'effacement de profils d'ADN effectué d'office.

2.7 Santé

L'Hôpital de l'Ile a édicté à l'attention de son personnel un mémento sur la protection des données structuré en fonction des domaines d'activité. La Direction de la santé publique et de la prévoyance sociale a élaboré pour sa part un guide sur l'obligation de garder le secret imposée aux professionnels de la santé. (Cf. ch. 2.6.2 à propos de l'autorité de surveillance pour la protection des données des prestataires de soins.)

2.7.1 Systèmes d'informations cliniques

La première utilisation, dans le cadre d'un projet informatique, du schéma de protection des données général élaboré par l'Office des hôpitaux est le fait du Centre hospitalier de Bienne, qui s'est fondé sur ces documents de base destinés à l'ensemble des hôpitaux pour établir son propre schéma de protection des données du système d'informations cliniques (cf. ch. 2.1.1, 2.2.1 et 2.3). Les documents en question se sont révélés utiles, et le schéma a permis de montrer que le projet pouvait être réalisé dans le respect des prescriptions relatives à la protection des données. Ce schéma doit toutefois être actualisé jusqu'à la mise en service du système. Le concept d'accès n'avait été conçu qu'à titre d'exemple pour un hôpital quelconque et il s'agit encore de l'adapter aux besoins du Centre hospitalier de Bienne. Dans une décision de 1999 déjà, la Direction de la santé publique et de la prévoyance sociale avait relevé à propos d'un système d'information hospitalier que le navigateur ne pouvait pas renseigner sans restriction sur le fait qu'un patient avait déjà été admis par le passé dans d'autres services. Il convient encore de tenir compte de cette consigne.

2.7.2 APDRG

L'Hôpital de l'Ile ainsi que les hôpitaux de Thoune et d'Aarberg utilisent désormais la méthode APDRG (All Patient Diagnoses Related Groups, décomptes selon 641 forfaits correspondant chacun à une pathologie[34]) également pour les décomptes avec l'assurance-maladie dans le cas des patients en soins aigus hospitalisés en division commune. Or, le préposé fédéral à la protection des données avait déjà relevé l'absence de base légale s'agissant des décomptes selon la méthode APDRG destinés à l'assurance-accidents, et cette constatation vaut également dans le cas de l'assurance-maladie. Le Conseil-exécutif n'en a pas moins approu-

zwischen den Spitälern und santésuisse (Pilotversuch).

2.7.3 RAI-Home-Care

Zur Kostenabrechnung werden Heimbewohner mit Beurteilungssystemen eingestuft. In überarbeiteter Form sollen diese Systeme nun auch für den Spitexbereich Einsatz finden[35]. Prof. Thomas Geiser kam in einem für den Spitex Verband Schweiz erstellten Gutachten zum Schluss, für Spitexdienste gelte generell das Eidgenössische Datenschutzgesetz. Der Eidgenössische Datenschutzbeauftragte unterbreitete diese Schlussfolgerung dem Bundesamt für Justiz zur Überprüfung. Dieses kam zum Schluss, für Spitexdienste seien im Regelfall die kantonalen Datenschutzgesetze anwendbar. Die Rahmenbedingungen zum Einsatz von Beurteilungssystemen werden nun auf kantonaler Ebene festzulegen sein.

2.8 Aufsichts- und Justizentscheide

2.8.1 Blankovollmacht zum Einholen von Auskünften durch die IV-Stelle Bern

Wer sich zum Bezug von IV-Leistungen anmeldet, hat nach der Praxis der IV-Stelle Bern eine Vollmacht zu unterzeichnen, worin alle in Betracht fallenden Personen und Stellen, namentlich Ärzte und Ärztinnen, medizinisches Hilfspersonal, Spitäler, Heilanstalten, Krankenkassen, Arbeitgeber, Anwälte und Anwältinnen, Treuhandfirmen, private und öffentliche Versicherungen, Amtsstellen der privaten Fürsorgeeinrichtungen und die zuständigen Stellen der Alters- Hinterlassenen- und Invalidenversicherung ermächtigt werden, der IV-Stelle diejenigen Auskünfte zu erteilen, welche diese für die Abklärung des Anspruches und die Prüfung des Leistungsanspruches des Versicherten sowie die Durchführung des Rückgriffes auf Dritte benötigt. Eine versicherte Person wandte sich gegen diese Praxis mit einer Beschwerde an das Verwaltungsgericht. Die sozialversicherungsrechtliche Abteilung hiess diese Beschwerde nun aus andern Gründen gut, hielt aber ausdrücklich fest, die von der IV-Stelle Bern eingesetzten Blankovollmachten seien rechtmässig.

2.8.2 Krankenversicherungsobligatorium für Sans-Papiers, Amtshilfe

In einem Einzelrichterentscheid hielt die sozialversicherungsrechtliche Abteilung des Verwaltungsgerichts fest, das Sozialversicherungsrecht erlaube es dem Amt für Sozialversicherung und Stiftungsaufsicht zur Durchsetzung des Krankenversicherungsobligatoriums beim Migrationsdienst Rückfrage zu allfälligen asylrechtlichen Entscheidungen über einen Sans-Papiers zu machen.

vé les contrats passés en la matière entre les hôpitaux et santésuisse (phase de test).

2.7.3 RAI-Home-Care

Dans le domaine des services d'aide et de soins à domicile, il est prévu d'utiliser, sous une forme remaniée, les systèmes servant à évaluer les besoins des personnes âgées résidant en institution en vue du décompte des dépenses[36]. Mandaté par l'Association suisse des services d'aide et de soins à domicile, le professeur Thomas Geiser a réalisé une étude dont il ressort que la loi fédérale sur la protection des données est, d'une manière générale, applicable en l'espèce. Le préposé fédéral à la protection des données a soumis ce résultat pour examen à l'Office fédéral de la justice, qui est pour sa part parvenu à la conclusion qu'en principe, le domaine en question est régi par les lois cantonales sur la protection des données. Ainsi, les conditions de l'utilisation des systèmes d'évaluation devront être fixées au niveau cantonal.

2.8 Surveillance et décisions de justice

2.8.1 Procuration en blanc permettant à l'Office AI de Berne d'obtenir des renseignements

Toute personne sollicitant des prestations de l'assurance-invalidité doit, selon la pratique de l'Office AI de Berne, signer une procuration par laquelle elle autorise l'ensemble des personnes et services concernés - à savoir les médecins, le personnel paramédical, les hôpitaux et autres établissements de soins, les caisses-maladie, les employeurs, les avocats et avocates, les sociétés fiduciaires, les compagnies d'assurance tant publiques que privées, les services publics chargés des institutions privées d'aide sociale ainsi que les services compétents de l'assurance-vieillesse, survivants et invalidité - à fournir à l'Office AI les renseignements dont il a besoin pour l'examen et la vérification du droit aux prestations ainsi que pour l'exercice du droit de recours contre un tiers responsable. Une personne assurée a attaqué cette pratique au moyen d'un recours devant le Tribunal administratif. La Cour des assurances sociales a admis le recours pour d'autres motifs, mais a expressément relevé le caractère légal des procurations en blanc utilisées par l'Office AI de Berne.

2.8.2 Régime de l'assurance-maladie obligatoire pour les sans-papiers, entraide administrative

La Cour des assurances sociales du Tribunal administratif a indiqué dans un jugement prononcé par le juge unique que le droit des assurances sociales autorisait l'Office des assurances sociales et de la surveillance des fondations à adresser au Service des migrations des demandes au sujet d'éventuelles décisions rendues selon le droit applicable en matière d'asile au sujet de personnes sans-papiers afin de veiller au respect du régime de l'assurance-maladie obligatoire.

---

35 http://www.spitexch.ch/index.cfm?lang=d

36 http://www.spitexch.ch/f/sub04/aktuelles.cfm?c_d=c_t&cat_id=132

2.8.3 Einsichtsrecht in Krankengeschichten

Die verwaltungsrechtliche Abteilung des Verwaltungsgerichtes hielt in einem erst im Jahr 2005 publizierten Entscheid zum Einsichtsrecht des Patienten in seine Psychiatrieakten fest, eine Einsichtsverweigerung zum Schutz des Patienten oder Dritter dürfe nur erfolgen, wenn die Gründe hierzu detailliert dargelegt würden. Die Gesundheitsgesetzgebung gebe zudem einen Anspruch auf Zusendung der Unterlagen.

2.8.3 Droit de consulter les anamnèses

La Cour de droit administratif du Tribunal administratif a indiqué, dans un jugement publié en 2005 seulement au sujet du droit d'un patient de consulter son dossier psychiatrique, que le refus d'accorder un tel droit dans le but de protéger le patient ou des tiers n'était admissible que s'il était motivé de manière détaillée. La cour a ajouté que la législation sur la santé accordait par ailleurs un droit à l'envoi des documents.

2.9 Gemeinderechtliche Körperschaften

In einem Gutachten für die Stadt Bern kam Prof. Markus Müller zum Schluss, das Polizeigesetz verbiete es Gemeinden, Reglemente zur Videoüberwachung zu erlassen. Die Kompetenz hierzu liege abschliessend beim Kanton. Zum weiteren Vorgehen wurden im Grossen Rat mehrere parlamentarische Vorstösse eingereicht. Eine Klärung der Rechtslage durch eine Änderung des Polizeigesetzes erscheint nötig.

2.9 Collectivités de droit communal

Dans une expertise établie à l'attention de la ville de Berne, le professeur Markus Müller est parvenu à la conclusion que la loi sur la police interdit aux communes d'édicter des règlements relatifs à la vidéosurveillance, ce domaine étant de la compétence exclusive du canton. Diverses interventions ont été déposées au Grand Conseil à propos des démarches à entreprendre, et il apparaît nécessaire de clarifier la situation juridique par une modification de la loi sur la police.

2.10 Berichtspunkte des Vorjahres

(S. 2.2.4, 2.3.1, 2.6.2: DNA-Profilverordnung, 2.7.2, 2.8.1).

2.10 Points abordés dans le rapport précédent

(Cf. ch. 2.2.4, 2.3.1, 2.6.2: ordonnance sur les profils d'ADN, 2.7.2 et 2.8.1.)

2.10.1 Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei

Der Regierungsrat hat die Betriebsbewilligung für die Vorermittlungsdatenbank des Dezernats Personenfahndung (Übernahme in das System ABI) erteilt. Für die Bewilligung des Systems VICLAS liegt ein Bewilligungsentwurf vor. Weder ein Entwurf noch eine Betriebsbewilligung besteht nach wie vor zur Fernüberwachung von Lichtsignalen (mit Digitalkameras zur Geschwindigkeitsüberwachung und zur Erfassung von Rotlichtmissachtungen) und zum Informatikprojekt Metamorphose UVEK (Online-Zugriff auf die Datenbank des Dienstes für besondere Aufträge des UVEK zur Überwachung des Post- und Fernmeldeverkehrs)[37].

2.10.1 Autorisation d'exploiter les systèmes de traitement des données de la Police cantonale

Le Conseil-exécutif a délivré une autorisation d'exploiter la banque de données relative aux enquêtes préliminaires de la Brigade "recherche de personnes" (intégration dans le système ABI). S'agissant du système ViCLAS, un projet d'autorisation a été élaboré. Par contre, aucune autorisation d'exploiter, même à l'état de projet, n'existe pour le système informatique de surveillance à distance, par caméras numériques, des signaux lumineux (respect des feux rouges) et des limitations de vitesse, ni pour le projet Metamorphose du DETEC (accès en ligne à la banque de données du Service des tâches spéciales du DETEC, auquel incombe la surveillance de la correspondance par poste et télécommunication)[38].

Kontrollen der Informatikdatenbearbeitungen im Amt für Sozialversicherung und Stiftungsaufsicht

Das Amt für Sozialversicherung und Stiftungsaufsicht wurde nach GoodPriv@cy zertifiziert[39]. Damit setzt es den Auftrag aus der Krankenversicherungsverordnung zum Aufbau eines internen Kontrollsystems und zum regelmässigen Beizug einer externen Datenschutzkontrollstelle um.

2.10.2 Contrôles du traitement informatisé des données à l'Office des assurances sociales et de la surveillance des fondations

L'office a obtenu le label GoodPriv@cy au terme d'une procédure de certification[40]. Il respecte ainsi le mandat énoncé dans l'ordonnance sur l'assurance-maladie, qui l'oblige à mettre en place un système de contrôle interne et d'en confier périodiquement le réexamen à un organe indépendant.

---

37 http://www.be.ch/aktuell/default.aspx?action=2&mmid=15743

38 http://www.be.ch/aktuell/default-f.aspx?action=2&mmid=15744

39 http://www.sgs.ch/index/leistungsangebot/lgpr.htm

40 http://www.sgs.ch/fr/index/leistungsangebot/lgpr.htm

2.10.3 Fehlende Datenlöschung im Geschäftskontrollsystem TRIBUNA der Gerichte

Eine externe Kontrollstelle stellte die fehlende Löschung vor einem Jahr fest. Das Obergericht hat zur Behebung des Mangels eine Arbeitsgruppe eingesetzt. Verbesserungen sind noch nicht umgesetzt.

2.10.4 Vorübergehend zu weit gehende Zugriffsrechte für Gemeinden in der Informatikanwendung IS-NESKO der Steuerverwaltung

Seit September sind die vorübergehend zu weit gehenden Zugriffsrechte der Gemeinden in der Informatikanwendung IS-NESKO behoben. Zugriffe der Gemeinden auf besonders schützenswerte Daten werden neu bei den nach wie vor kantonsweit offenstehenden Registerdaten (wie Adresse, Zivilstand, Beruf, Familienstruktur, steuerrelevante Konfession) protokolliert.

2.11 Besonderes

2.11.1 Heikle Herkunftsangaben im Finanzinformationssystem FIS 2000

Das Finanzinformationssystem FIS 2000 steht praktisch allen Dienststellen zur Verfügung. Das System enthält eine Adressdatei. Mit dieser sollen neben anderem mehrfache Adresserfassungen verhindert werden. In der Adressdatei war ersichtlich, welche Dienststelle die Adresse erstmals aufgenommen hatte. Damit konnte beispielsweise festgestellt werden, dass eine Person mit einem Untersuchungsrichteramt oder mit einer psychiatrischen Klinik Kontakt hatte. Dieser in der gesamten Kantonsverwaltung mögliche Rückschluss kann die Betroffenen erheblich beeinträchtigen. Die Finanzverwaltung hat das System nun geändert. Die genauen Adressherkunftsangaben sind nur noch für die eingebende Organisationseinheit ersichtlich.

3. Januar 2006 SIM/sib

2.10.3 Absence de radiation des données dans le système de contrôle des affaires des tribunaux TRIBUNA

Il y a une année, un service de contrôle externe avait relevé l'absence de radiation des données dans le système. La Cour suprême a institué un groupe de travail dans le but de combler cette lacune. Aucune amélioration n'a encore été apportée à ce jour.

2.10.4 Droit d'accès provisoirement trop étendu des communes à l'application informatique IS-NESKO de l'Intendance cantonale des impôts

Le problème du droit d'accès trop étendu des communes à l'application informatique IS-NESKO a été résolu en septembre. Il existe désormais une journalisation des accès des communes aux données du registre particulièrement dignes de protection (comme l'adresse, l'état civil, la profession, la structure familiale, la confession lorsque celle-ci joue un rôle en matière fiscale), qui restent accessibles à l'échelle cantonale.

2.11 Cas particuliers

2.11.1 Problème posé par les indications de provenance dans le système d'informations financières FIS 2000

Le système d'informations financières FIS 2000 est à la disposition de pratiquement tous les services. Il contient un fichier d'adresses devant notamment empêcher qu'une même adresse soit saisie à plusieurs reprises. Jusqu'à récemment, le ficher indiquait quel service avait enregistré l'adresse et, partant, était entré le premier en contact avec une personne, révélant par exemple si cette dernière avait eu affaire à un service de juges d'instruction ou à une clinique psychiatrique. Le fait qu'une telle indication soit accessible à l'ensemble de l'administration cantonale pouvait donc porter une atteinte considérable aux intérêts de la personne concernée. L'Administration des finances a modifié le système, de sorte que la provenance exacte de l'adresse n'est plus visible que pour l'unité administrative qui l'a saisie.

3 janvier 2006