

Bericht 2008 der Aufsichtsstelle für Datenschutz

1 Einleitung

1.1 Auf einen Blick

Am 1. Dezember 2008 trat das überarbeitete Datenschutzgesetz in Kraft. Seine Regelungen werden durch die neue Datenschutzverordnung ergänzt. Im gleichen Gesetzgebungsverfahren wurden Datenschutzregelungen in zahlreichen Erlassen überarbeitet. Die neuen Regelungen verbessern die Rechtsstellung der Betroffenen. Diese Verbesserung wird aber nur erreicht, wenn sich die Verwaltungsstellen von Kanton und Gemeinden an die neuen Regelungen halten. Davon darf ausgegangen werden. Missachten staatliche Stellen die Vorgaben jedoch, ist es vorab Sache der Justizinstanzen, die Rechtsumsetzung zu sichern. Mehrere Justizentscheide haben 2008 hierzu klare Signale gesetzt (s. 7).

1.2 Zusammenarbeit mit dem Eidgenössischen Datenschutzbeauftragten und der Vereinigung der Schweizerischen Datenschutzbeauftragten (PRIVATIM)

Im Vorjahr bot eine Ansichtsausschuss des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten für den Regierungsrat Anlass, den Tarifvertrag zwischen dem Verband Bernischer Krankenhäuser und Santésuisse nur mit Vorbehalten zu genehmigen. Die vorgesehenen Datenbekanntgaben sollten damit auf das zulässige Mass verkleinert werden. Im Jahre 2008 hat der Regierungsrat zu allen Verträgen mit der gleichen Regelung erneut Vorbehalte angebracht. Santésuisse hat auch diese Vorbehalte vor dem Bundesverwaltungsgericht angefochten. Ein Entscheid steht noch aus.

Zum Betrieb des Pilotprojektes des nationalen Polizeiindexes nahmen Mitarbeiter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, des Bundesamtes für Polizeiwesen und der kantonale Datenschutzbeauftragte bei der Kantonspolizei einen gemeinsamen Augenschein vor.

Die Verordnung über den nationalen Teil des Schengener-Informationssystems verpflichtet den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und die kantonalen Datenschutzbehörden zum Aufbau einer koordinierten Aufsicht in Bezug auf dieses System. Hierzu fanden zwei Sitzungen statt. Vorab war eine Information an die vom System Betroffenen über ihre Datenschutzrechte zu erstellen.

Die Vereinigung der kantonalen Datenschutzbeauftragten (PRIVATIM) führte Informationsveranstaltungen zu Datenschutz und Technik und zu den Aufgaben der kantonalen Datenschutzbehörden im Staatsschutz durch.

(Zur weiteren Zusammenarbeit s. 6.2 und 8).

Rapport d'activité 2008 du Bureau pour la surveillance de la protection des données

1 Introduction

1.1 2008 en bref

La loi révisée sur la protection des données est entrée en vigueur le 1^{er} décembre, de même que la nouvelle ordonnance sur la protection des données qui la complète. La procédure législative a offert l'occasion de remanier les prescriptions relatives à la protection des données contenues dans de nombreux actes législatifs, et d'améliorer ainsi la position des personnes concernées. A condition toutefois que les services administratifs tant cantonaux que communaux respectent les nouvelles dispositions – comme on est en droit de l'attendre. Dans le cas contraire, il appartient avant tout aux autorités administrant la justice de garantir l'application du droit. Différentes décisions de justice rendues en 2008 sont autant de signaux univoques à cet égard (cf. ch. 7).

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

Un avis du préposé fédéral à la protection des données et à la transparence avait amené le Conseil-exécutif, en 2007, à assortir de réserves son approbation de la convention tarifaire conclue entre l'Association des établissements hospitaliers bernois et santésuisse dans le but de réduire la communication de données à un strict minimum. Au cours de l'exercice, le Conseil-exécutif a émis les mêmes réserves à propos de toutes les conventions similaires, et santésuisse les a une nouvelle fois attaquées devant le Tribunal administratif fédéral, qui doit encore se prononcer.

Des collaborateurs du préposé fédéral à la protection des données et à la transparence ainsi que de l'Office fédéral de la police ont procédé auprès de la Police cantonale, avec le délégué cantonal à la protection des données, à une inspection commune portant sur l'exploitation du projet pilote d'index national de police.

L'ordonnance sur la partie nationale du Système d'information Schengen oblige le préposé fédéral à la protection des données et à la transparence et les autorités cantonales de protection des données à instaurer un système coordonné de surveillance de l'exploitation du système. Deux séances ont eu lieu dans ce contexte. Au préalable, il s'était agi d'informer toutes les personnes concernées par le système de leurs droits en matière de protection des données.

PRIVATIM, l'association des commissaires suisses à la protection des données, a organisé des séances d'information sur la protection des données et la technique ainsi que sur les tâches des autorités cantonales de protection des données en matière de protection de l'Etat.

(Cf. ch. 6.2 et 8 s'agissant de la coopération dans d'autres domaines.)

2 Aufgabenumschreibung, Prioritäten, Mittel

2.1 Prioritäten

Für das Bearbeiten der Geschäfte gilt unverändert folgende Prioritätenfolge: 1. Datenschutzkonzepte für Informatikprojekte, 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. Der Mitwirkung an den Gesetzgebungsarbeiten zum Datenschutzgesetz und zur Datenschutzverordnung kam ein hoher Stellenwert zu. Eine hohe Priorität hatten auch die organisatorischen Arbeiten zum Ausbau der Datenschutzaufsichtsstelle.

2.2 Eigenverantwortung der datenbearbeitenden Stellen

Mit grossem Engagement liess die Erziehungsdirektion den Leitfaden „Datenschutz in den Schulen des Kantons Bern“ erstellen. Die Erziehungsberatungsstelle Interlaken führte für ihre Mitarbeitenden einen Weiterbildungskurs zu Datenschutzfragen durch.

Bundesstellen verlangten von der Steuerverwaltung für zwei Forschungsprojekte heikle Steuerdaten. Die Steuerverwaltung klärte vor der Datenbekanntgabe detailliert ab, ob alle Bedingungen für eine Datenbekanntgabe zu Forschungszwecken eingehalten sind.

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

2.3 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Jahr 2008 waren 40 Millionen CHF in Informatikmittel zu investieren. 152 Millionen CHF (davon 69 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. 2.4).

Der IT-Sicherheitsbeauftragte des Kantons unterstützte die Datenschutzaufsichtsstelle bei der Beurteilung von ISDS-Konzepten erheblich.

Die bei der Datenschutzaufsichtsstelle neu geschaffenen Stellen (wissenschaftliche Mitarbeitende Recht und Informatik) konnten ausgeschrieben werden.

Im November wählte der Grosse Rat den Datenschutzbeauftragten für vier Jahre.

2.4 Kontrollen von Informatikdatenbearbeitungen

Auf eigene Kosten liess die Steuerverwaltung das TaxMe-

2 Description des tâches, priorités, moyens à disposition

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 services de contrôle externes mandatés, 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. La participation aux travaux législatifs concernant la loi et l'ordonnance sur la protection des données a constitué un point fort de l'exercice. De même, les tâches d'organisation requises par l'étoffement du Bureau ont revêtu un caractère prioritaire.

2.2 Responsabilité propre des services traitant les données

La Direction de l'instruction publique a fait preuve d'un grand engagement en publiant ses Lignes directrices sur l'utilisation de données personnelles dans les écoles du canton de Berne. Le service psychologique pour enfants et adolescents d'Interlaken a organisé un cours de perfectionnement sur la protection des données à l'intention de son personnel.

Des services fédéraux ont demandé à l'Intendance des impôts de leur fournir des données fiscales sensibles destinées à deux projets de recherche. Cette dernière, avant de répondre à la requête, a examiné dans les détails si toutes les conditions d'une communication de données à des fins de recherche étaient respectées.

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 40 millions aux investissements dans le domaine informatique, et CHF 152 millions à l'exploitation (dont CHF 69 mio destinés à des tiers prestataires de services). Pour le contrôle des applications informatiques par des services externes (cf. ch. 2.4), la somme prévue était de CHF 130 000.

Le délégué cantonal à la sécurité informatique a apporté au Bureau un soutien très appréciable lors de l'évaluation des concepts SIPD.

Les nouveaux postes créés pour étoffer le Bureau (collaborateurs ou collaboratrices scientifiques dans les domaines du droit et de l'informatique) ont pu être mis au concours.

En novembre, le Grand Conseil a élu le délégué à la protection des données pour une période de quatre ans.

2.4 Contrôle du traitement de données informatiques

L'Intendance des impôts a chargé à ses frais un service ex-

Portal – eine den Steuerpflichtigen zur Verfügung stehende Internetanwendung zur Abfrage ihrer Steuerdaten – durch eine externe Stelle überprüfen. Die Prüfung bestätigte, dass es einem Steuerpflichtigen nicht möglich ist, auf die Daten anderer Steuerpflichtiger zuzugreifen. Festgestellt wurden einige wenige, nicht gravierende, technische Schwachpunkte. Das Staatssekretariat für Wirtschaft (SECO) liess durch eine Drittstelle prüfen, ob im Bereich RAV/LAM/KAST im Kanton Bern eine genügende Datenschutzsensibilisierung bestehe und ob die Datenschutzmassnahmen technisch umgesetzt seien. Eine Datenschutzprüfung der Fachanwendungen fand nicht statt. Zum Zeitpunkt der Prüfungshandlungen wurden keine Anhaltspunkte gefunden, die auf ein insgesamt nicht ausreichendes Niveau der Datenschutzsensibilisierung schliessen liessen. Ein Verbesserungspotential wurde im Umgang mit portablen Speichermedien, mit nicht mehr benötigten Datenträgern sowie in der Mitarbeiterschulung und bei der Berechtigungsvergabe festgestellt. Es ist erfreulich, dass Bundesstellen gegenüber kantonalen Stellen, die Bundesrecht vollziehen, Prüfungen durchführen. Der Sache dienlich wäre es allerdings, wenn die kantonale Datenschutzaufsichtsstelle über solche Prüfungen vorgängig informiert und beigezogen würde.

Die externe Kontrollstelle stellte bei der Datenschutzprüfung der Informatikanwendung IDIS (Labor-, Geschäftskontroll- und Abrechnungssystem) des Institutes für Infektionskrankheiten (IFIK) folgendes fest: Sämtliche Labor- und qualitätsbezogenen Prozesse seien ausführlich und vorbildlich dokumentiert. Das gelte gerade auch für die Einführung neuer Mitarbeitender. Diverse Verfahren und Methoden zur Umsetzung von Datenschutz und Informatiksicherheit seien aber nicht oder ungenügend erfüllt. Betroffen seien die Klassifizierung, die Ausbildung und Schulung, die Benutzerüberprüfung, die Dokumentation, die Notfallkonzeption und die Änderungskontrollen. Ein Archivierungskonzept fehle. Zur Informatiksicherheit gab die externe Kontrollstelle dringende Verbesserungsempfehlungen ab. Das IFIK geht die Verbesserungen mit dem Projekt NewIT an.

Die Gefängnisinsassen-Applikation GINA wurde vom externen Kontrolleur insgesamt als eingespielter, gut strukturierter und sicherer Prozess qualifiziert. Die Anwendung genüge den meisten Datenschutz- und Informatiksicherheitsanforderungen. Das Amt für Freiheitsentzug und Betreuung müsse aber die Anstalten und Gefängnisse verstärkt führen. Dem Umgang mit personenbezogenen Daten müsse generell mehr Aufmerksamkeit geschenkt werden. Die Komplexität der Anwendung mache den Benutzenden in den Anstalten und Gefängnissen Mühe. Einige wichtige Funktionalitäten seien noch nicht umgesetzt worden. Die Archivierung und ein Prozess für die Vernichtung und Löschung müssten längerfristig sichergestellt werden. Die Protokollierung müsse ausgeweitet werden. Exportfunktionen und die Möglichkeit zu unkontrollierten Eingaben in bestimmten Datenfeldern seien einzuschränken. Generell müsse der Umgang mit Besucherdaten und mit den medizinischen Daten verbessert werden. Gut fiel die Überprüfung des Serversystems bei der Bedag-Informatik AG aus. Bei einem weiteren externen Datenbearbeiter stellte der externe Kontrolleur dagegen für die physische Sicherheit und den Umfang der Datenhaltung Verbesserungsbedarf fest. Zur Datenweitergabe an Behörden, Krankenkassen und Sozial-

terne d'examiner le portail TaxMe – une application Internet permettant aux contribuables d'interroger leurs données fiscales. L'examen a confirmé l'impossibilité de consulter les données d'un autre contribuable. Il a par ailleurs révélé quelques points faibles de peu de gravité sur le plan technique.

Le Secrétariat d'Etat à l'économie (SECO) a fait examiner par des tiers si, dans le domaine des ORP/LMMT/Act, la sensibilisation aux questions de protection des données était suffisante et si les mesures techniques de protection des données étaient mises en œuvre dans le canton de Berne. Les applications spécialisées n'ont toutefois pas fait l'objet d'une vérification sous l'angle de la protection des données. D'une manière générale, au moment de l'examen, aucun indice d'une sensibilisation insuffisante aux impératifs de protection des données n'a été décelé. Un potentiel d'amélioration a par contre été noté s'agissant de l'utilisation des moyens de stockage mobiles, des supports de données devenus superflus, ainsi que de la formation du personnel et de l'octroi des droits d'accès. Il est réjouissant que les services fédéraux procèdent à des contrôles auprès des services cantonaux qui exécutent le droit fédéral. Il serait toutefois judicieux qu'ils en informent le Bureau au préalable et fassent appel à sa collaboration.

Le service de contrôle externe qui a examiné l'application informatique IDIS (système de laboratoire, de contrôle des affaires et de décompte) de l'Institut des maladies infectieuses (ifiik) sous l'angle de la protection des données a constaté que tous les processus de laboratoire et les processus en relation avec la qualité étaient documentés de manière exhaustive et exemplaire, tout comme la mise au courant des nouveaux collaborateurs et collaboratrices. Par contre, il a relevé que diverses procédures et méthodes destinées à garantir la protection des données et la sécurité informatique n'étaient pas ou pas suffisamment respectées. Ces lacunes concernent la classification, la formation, l'examen des utilisateurs, la documentation, la stratégie à suivre en cas d'urgence et les contrôles des changements. Il n'existe par ailleurs pas de programme d'archivage. Le service de contrôle externe a émis des recommandations urgentes sur la sécurité informatique, et l'ifiik s'emploie à apporter des améliorations dans le cadre du projet NewIT.

L'application GINA (administration des détenus et détenues) a été qualifiée par un contrôleur externe de système sûr, bien structuré et éprouvé, satisfaisant à la plupart des exigences en matière de protection des données et de sécurité informatique. Le contrôleur a toutefois relevé la nécessité de renforcer la conduite des établissements pénitentiaires et des prisons par l'Office de la privation de liberté et des mesures d'encaînement, ainsi que d'accorder une attention accrue, d'une manière générale, au traitement des données personnelles. Il a par ailleurs souligné les points suivants: la complexité de l'application pose des problèmes aux utilisateurs des établissements pénitentiaires et des prisons; certaines fonctions importantes ne sont pas encore disponibles; l'archivage et les processus de destruction et de radiation doivent être garantis à long terme; la journalisation doit être étendue; les fonctions d'exportation et les possibilités de saisie incontrôlée de données dans certains champs doivent être limitées; enfin, le traitement des données des visiteurs et des données médicales doit être amélioré dans l'ensemble. L'examen du système de serveurs géré par la Bedag Informatique SA s'est révélé

ämter seien die beteiligten Benutzer und Stellen zudem zu informieren und zu schulen.

Die Prüfung der Informatikmittel der Opferhilfe (beim Sozialamt der Gesundheits- und Fürsorgedirektion) zeigte, dass die gesetzlichen und kantonalen Vorgaben zu Datenschutz und Informatiksicherheit mehrheitlich gut erfüllt waren. Die Zugriffsrechte auf die Opferhilfe-Software sowie das zentrale Serververzeichnis für ergänzende Daten sind restriktiv und zweckmässig vergeben. Die Prüfung zeigte aber auch einige wenige Optimierungspotenziale mit tiefem oder mittlerem Risiko. Betroffen waren Persönlichkeitsschutz und Informatiksicherheit.

Mit der Anwendung NESKO Frontend stellt die Steuerverwaltung sämtlichen Mitarbeitenden der Steuerverwaltung und den Gemeinden Steuerdaten zur Verfügung (Zugriffportal auf die Anwendungen der Steuerverwaltung). Anhand der Anwendung NESKO AB (amtliche Bewertung) überprüfte der externe Kontrolleur insbesondere die Benutzerauthentifizierung und -autorisierung. Die gesetzlichen und kantonalen Vorgaben zur Informatiksicherheit wurden als mehrheitlich gut erfüllt qualifiziert. Die Anwendung NESKO Frontend sei auf Stufe Applikation und Betriebssystem sicherheitstechnisch gut implementiert. Das ISDS-Konzept stehe zurzeit in Ausarbeitung. Zur Informatiksicherheit wurden einige wenige Empfehlungen in mittlerer oder tiefer Priorität gemacht. So etwa zur Einspielung von Security Patches.

Die Erziehungsdirektion stellt den Berufsschulen und Gymnasien seit 2005 die Schulverwaltungsanwendung Evento zur Verfügung. Die externe Kontrollstelle führte die Überprüfung dieser Anwendung bei vier Schulen durch (drei Berufsschulen und ein Gymnasium). Aus Sicherheitsgründen sei den Lehrkräften vorläufig ein Zugriff auf die Anwendung von zu Hause aus nicht möglich. Etwa Noteneinträge könnten allein vom Arbeitsplatz der Lehrkraft in der Schule aus erfolgen. Zur Anwendung sei eine umfangreiche Dokumentation vorhanden. Diese sei aber nicht auf die Prozesse und Abläufe der Schulen abgestimmt. Das gelte ebenfalls für die Dokumentation zu Datenschutz und Informatiksicherheit. Die Anwendung weise einige Schwächen auf, die in naher Zukunft angepackt werden müssten. So arbeiteten etwa einige Superuser ständig mit (organisatorisch eingeschränkten) Administrationsrechten. Längerfristig anzugehen sei die Archivierung und ein Prozess für die Datenvernichtung. Der externe Kontrolleur empfahl auch eine umgehend umzusetzende Massnahme: Die Erziehungsdirektion hatte den Systembetreiber angewiesen, gelegentlich die komplette Datenbank nicht anonymisiert und unverschlüsselt über das Internet auf einen Server des Anwendungsherstellers zu kopieren. Dies, damit spezifische Probleme gelöst und Dokumentationen erstellt werden konnten. Ein solches Vorgehen sei fahrlässig und unverzüglich einzustellen.

Die durch die externen Kontrollstellen festgestellten – auch schwerwiegenden – Mängel zeigen die Notwendigkeit von Kontrollen. Unter dem überarbeiteten Datenschutzgesetz (s. 6.2) wird der jährliche Prüfplan künftig nicht mehr durch den Regierungsrat, sondern unmittelbar von der Datenschutzaufsichtsstelle verabschiedet werden. Auch künftig sollen jedoch die Daten bearbeitenden Stellen in die Planung und Ausgestaltung der Kontrollen eingebunden werden. Die hohe Bereitschaft zur Umsetzung von Empfehlungen sollte damit erhalten

positiv. Dans le cas d'un autre service externe traitant des données par contre, le contrôleur externe a constaté que tant la sécurité physique que l'étendue des données stockées requéraient des améliorations. Il a relevé en outre la nécessité de sensibiliser et de former les personnes et services concernés au sujet de la transmission de données aux autorités, aux caisses-maladie et aux services sociaux.

Il est ressorti de l'examen des auxiliaires informatiques du service chargé de l'aide aux victimes d'infractions au sein de l'Office des affaires sociales (Direction de la santé publique et de la prévoyance sociale) que le plus souvent, les dispositions légales et les consignes cantonales relatives à la protection des données et à la sécurité informatique sont bien respectées. Les droits d'accès au logiciel de l'aide aux victimes ainsi qu'au répertoire de serveur central pour les données complémentaires sont accordés de manière restrictive et opportune. Quelques rares éléments liés à la protection de la personnalité et à la sécurité informatique présentent un risque faible à moyen et peuvent donc encore être optimisés.

Avec l'application NESKO Frontend, l'Intendance des impôts (ICI) met des données fiscales à la disposition de l'ensemble de son personnel ainsi que des communes (portail d'accès aux applications de l'ICI). Le contrôleur externe a en particulier examiné l'authentification des utilisateurs et les autorisations accordées à ces derniers dans le cas de l'application NESKO AB (Evaluation officielle). Il est parvenu à la conclusion que les dispositions légales et les consignes cantonales relatives à la sécurité informatique sont dans l'ensemble bien observées, et que l'application NESKO Frontend est correctement implémentée du point de vue de la sécurité, liens avec le système d'exploitation compris. Le concept SIPD est en cours d'élaboration. Quelques recommandations peu ou moyennement prioritaires ont été formulées sur la sécurité informatique, par exemple au sujet de l'installation de rustines de sécurité.

La Direction de l'instruction publique met depuis 2005 l'application de gestion scolaire Evento à la disposition des écoles professionnelles et des gymnases. Le service de contrôle externe l'a examinée dans trois écoles professionnelles et un gymnase, et a constaté ce qui suit: pour des raisons de sécurité, les enseignants et enseignantes ne sont pour l'instant pas autorisés à accéder à l'application depuis la maison et ne peuvent donc inscrire les notes par exemple qu'à l'école; une documentation détaillée est certes disponible, mais elle ne se réfère pas spécifiquement aux procédures suivies par les écoles – remarque qui vaut également dans le cas de la protection des données et de la sécurité informatique; l'application présente quelques points faibles devant être corrigés soit rapidement, comme le fait que des super-utilisateurs travaillent en permanence avec des droits d'administrateurs (limités au plan organisationnel), soit à plus long terme, dans le cas de l'archivage et de la mise en place d'un processus de destruction des données. La Direction de l'instruction publique avait par ailleurs demandé à l'exploitant du système de copier de temps à autre la banque de données complète sur un serveur du fournisseur, via Internet, sans l'avoir préalablement anonymisée ni cryptée. Le contrôleur externe a considéré qu'en ordonnant une telle démarche, destinée à la résolution de certains problèmes spécifiques et à l'établissement de documentation, la Direction faisait preuve de négligence et qu'elle devait donc immédiatement mettre fin à cette pratique.

bleiben.

Die Finanzkontrolle hat im Rahmen der Wirtschaftsprüfung die Risikobeurteilung im Informatikbereich aller Dienststellen weitergeführt.

3 Informatiksicherheits-Sollvorgaben

Die Ende 2007 vom Regierungsrat verabschiedeten Weisungen über die Informatiksicherheit und den Datenschutz (ISDS) waren 2008 erstmals umfassend anzuwenden und sind insgesamt gut umgesetzt worden. Nützlich sind die der Verwaltung zur Verfügung gestellten elektronischen Werkzeuge zur Ausarbeitung einzelner Teildokumente des ISDS-Konzepts. Die Weisungen wie die elektronischen Werkzeuge müssen jedoch ständig weiterentwickelt werden. Rechtsänderungen - etwa durch das neue Datenschutzgesetz (s. 6.2) -, aber auch Feststellungen in der praktischen Anwendung, bedingen dies. Die Datenschutzverordnung sieht vor, dass die ISDS-Weisungen des Regierungsrats durch eine Direktionsverordnung der Finanzdirektion abgelöst werden.

Die Prüfung der ISDS-Konzepte führte bei der Datenschutzaufsichtsstelle zu einem erheblichen Aufwand (s. 4.).

Die Datenschutzgesetzgebung verpflichtet auch die gemeinderechtlichen Körperschaften zu einer Vorabkontrolle. Zum Erlass der hierzu nötigen Informatiksicherheitsollvorgaben sind die Gemeinden autonom. Neu umschreibt die Datenschutzverordnung (s. 6. 3) aber auch für die Gemeinden die grundsätzlichen technischen und organisatorischen Massnahmen. Umschrieben werden die Risiken, vor denen die Systeme zu schützen sind, die besonderen technischen und organisatorischen Massnahmen und die Protokollierungsvorgaben.

In seiner Antwort auf die Interpellation Masshardt unterstrich der Regierungsrat die Bedeutung der Informatiksicherheitsollvorgaben. So wird den Verwaltungsstellen vorgegeben, alle Laptops mit einer Verschlüsselungssoftware auszurüsten und damit die gespeicherten Daten zu schützen. Der Regierungsrat geht davon aus, dass damit ein Datenmissbrauch nach Verlust mobiler Datenträger verhindert werden kann. Er weist aber auch darauf hin, dass die flächendeckende Umsetzung der Weisung nicht feststeht. Die Einführung einer Meldepflicht für Fälle von Datenverlust ab mobilen Informatikmitteln lässt der Regierungsrat prüfen.

4 Betreute Informatikprojekte (Vorabkontrollen)

Die bereits vor einem Jahr aus Ressourcengründen zurückgestellten Datenschutzkonzepte PARIS und TS-BVE blieben erneut unbehandelt (PARIS der Universität Bern: Partnerinformationssystem u. a. zur Koordination der Daten der Angestellten von Universität und Kanton und zur Verwaltung der

Les défauts – parfois graves – constatés par les services de contrôle externes témoignent bien de la nécessité des vérifications. Sous le régime de la loi révisée sur la protection des données (cf. ch. 6.2), c'est le Bureau, et non plus le Conseil-exécutif, qui adopte le plan annuel d'examen. Les services traitant les données doivent toutefois rester impliqués dans la planification et l'organisation des contrôles. De la sorte, on peut s'attendre à ce qu'ils continuent à se montrer très ouverts aux propositions d'amélioration.

A l'occasion des audits internes, le Contrôle des finances a poursuivi son appréciation des risques dans le domaine informatique des différents services.

3 Consignes de sécurité informatique

L'instruction concernant la sûreté de l'information et la protection des données (SIPD) arrêtée par le Conseil-exécutif fin 2007, au champ d'application global, a dans l'ensemble été correctement mise en œuvre. Les outils électroniques proposés à l'administration pour élaborer certaines composantes du concept SIPD se révèlent utiles. A l'instar de l'instruction elle-même, ils doivent toutefois être mis à jour en permanence, compte tenu des modifications du droit – comme la révision de la loi sur la protection des données (cf. ch. 6.2) – mais aussi des expériences pratiques. L'ordonnance sur la protection des données prévoit le remplacement de l'instruction SIPD du Conseil-exécutif par une ordonnance de la Direction des finances.

L'examen des concepts SIPD a représenté une charge de travail importante pour le Bureau (cf. ch. 4).

La législation sur la protection des données impose également les contrôles préalables aux collectivités de droit communal. Si les communes sont autonomes s'agissant de l'édiction des consignes de sécurité informatique, elles sont tenues de respecter les nouvelles prescriptions de l'ordonnance sur la protection des données (cf. ch. 6.3) relatives aux mesures techniques et organisationnelles. Ces prescriptions portent sur la protection des systèmes contre les risques, les mesures particulières et la journalisation.

Dans sa réponse à l'interpellation Masshardt, le Conseil-exécutif a souligné l'importance des consignes de sécurité informatique. Il relève que les services administratifs ont l'obligation d'équiper tous les ordinateurs portables d'un logiciel de cryptage afin de protéger les données stockées. Le Conseil-exécutif part du principe que cette mesure permet d'éviter l'utilisation abusive de données en cas de perte d'outils informatiques mobiles, tout en relevant que son application systématique n'est pas garantie. Il indique par ailleurs que la mise en place d'une obligation de signaler la perte de données sur des outils informatiques mobiles est à l'étude.

4. Projets informatiques suivis par le Bureau (contrôles préalables)

Faute de ressources suffisantes, il a fallu reporter pour la deuxième année consécutive le traitement de deux schémas de protection des données: celui du projet PARIS (Partner Informationssystem) de l'Université de Berne, destiné notamment à la coordination des données des employés de l'uni-

Benutzerzugänge zu den Informatiksystemen der Universität Bern, Plattformintegration TS BVE: Einführung der Terminal-server-Architektur in der gesamten Bau-, Verkehrs- und Energiedirektion).

Am letzten Tag des Berichtsjahres gingen der Datenschutzaufsichtsstelle fünf neue ISDS-Konzepte zu Anwendungen der Justiz-, Gemeinde- und Kirchendirektion zu.

Ebenfalls noch offen ist die Behandlung der ISDS-Konzepte GERES und ZPV der Finanzdirektion (Gemeinderegistersystem des kantonalen Amtes für Informatik und Organisation und Zentrale Personenverwaltung der Steuerverwaltung).

Das ISDS-Konzept für das Klinikinformationssystem des Inselspitals (i-pdos) konnte soweit betreut werden, dass einem Ausgabenbeschluss keine datenschutzrechtlichen Hindernisse mehr entgegenstehen. Die sehr aufwändige Überprüfung der Zugriffsrechte wird erst vor der Inbetriebnahme des Systems möglich sein. Sicherergestellt ist aber, dass die einzusetzende Informatiklösung die Umsetzung differenzierter Zugriffsrechte erlaubt.

Nach einer ersten Stellungnahme der Datenschutzaufsichtsstelle verzichtete das Inselspital für das Informatikprojekt M4I (Materialwirtschaftslösung Inselspital) auf einen Patientenbezug. Das Projekt hat damit wesentlich tiefere Datenschutzerfordernisse zu erfüllen.

Zum ISDS-Konzept für die Informatikanwendung FIS 2000 (Finanzinformationssystem) gab die Datenschutzaufsichtsstelle ihren zweiten Prüfbericht ab. Für FIS 2000 wurde das bisherige Datenschutzkonzept den neuen ISDS-Vorgaben angepasst.

Für die Anwendung Office 2007 der Finanzdirektion genügte eine ISDS-Analyse. Mit Office 2007 wird die Büroinfrastruktur zur Verfügung gestellt. Sofern einzelne Anwender diese Infrastruktur für heikle Datenbearbeitungen einsetzen, ist allenfalls anwendungsbezogen ein ISDS-Konzept zu erstellen.

Der Spital Thun-Simmental-Saenenland AG konnte zum ISDS-Konzept für ein Radiologieinformationssystem und digitales Bildarchiv grundsätzlich ein positiver Prüfungsbericht gegeben werden. Umzusetzen sind aber noch die gemachten Auflagen.

Nicht möglich war eine positive Stellungnahme zum Informatikprojekt ELA_DMS der Spitäler fmi ag (elektronische Archivierung und Dokumenten-Management-System).

Die definitive Stellungnahme zum Klinikinformationssystem der Universitären Psychiatrischen Dienste und des Psychiatriezentrums Münsingen war zum Berichtszeitpunkt noch offen.

5 Ansichtsäusserungen, Praxis

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

- Beim Einsatz schwerer Maschinen und Fahrzeuge entstehen erhebliche Gefahren. Das Personalgesetz erlaubt es den kantonalen Stellen, Gesundheitsdaten von Fahrzeugführern und Führern schwerer Maschi-

versität et du canton ainsi qu'à l'administration des accès des utilisateurs aux systèmes informatiques de l'université, et celui du projet d'intégration des plates-formes du ST de la TTE, à savoir l'introduction de la configuration du serveur de terminal dans toute la Direction des travaux publics, des transports et de l'énergie.

Le 31 décembre, le Bureau a reçu cinq nouveaux concepts SIPD concernant des applications de la Direction de la justice, des affaires communales et des affaires ecclésiastiques.

Le Bureau n'a pas encore été en mesure non plus de traiter les concepts SIPD de deux applications de la Direction des finances: GERES (système des registres communaux de l'Office d'informatique et d'organisation) et GCP (gestion centrale des personnes de l'Intendance des impôts).

L'examen du concept SIPD du système d'informations cliniques DEP de l'Hôpital de l'île a pu atteindre un stade suffisant pour qu'aucun obstacle à un arrêté de dépense ne subsiste du point de vue de la protection des données. L'examen des droits d'accès, qui mobilisera d'importantes ressources, ne sera possible que juste avant la mise en service du système. Il est toutefois garanti que la solution informatique retenue permettra une différenciation des droits d'accès.

Suite à une première prise de position du Bureau, l'Hôpital de l'île a renoncé, dans le cas du projet informatique M4I (système de gestion du matériel), à toute référence directe au patient. Les exigences auxquelles le projet doit satisfaire en matière de protection des données s'en trouvent nettement diminuées.

Le Bureau a établi un deuxième rapport d'examen du concept SIPD de l'application FIS 2000 (système d'informations financières). Le schéma de protection des données de FIS 2000 a été adapté aux nouvelles consignes SIPD.

L'application Office 2007 de la Direction des finances – qui consiste en une infrastructure de bureau – n'a requis qu'une analyse SIPD. Si elle devait toutefois servir au traitement de données sensibles, un concept SIPD devrait être établi pour ce type d'utilisation.

Un rapport d'examen positif a pu être adressé au centre hospitalier Simmental-Thoune-Saenenland SA concernant le concept SIPD d'un système d'information radiologique et d'un système numérique d'archivage d'images. Les charges imposées doivent toutefois encore être respectées.

Il n'a par contre pas été possible de rendre un avis positif au sujet du projet informatique ELA_DMS (archivage électronique et système de gestion des documents) du centre hospitalier FMI SA.

Au moment de la rédaction du rapport, aucune prise de position définitive n'avait pu être remise s'agissant du système d'informations cliniques des Services psychiatriques universitaires de Berne et du Centre psychiatrique de Münsingen.

5 Avis exprimés, pratique

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

- L'utilisation de machines et de véhicules lourds recèle des dangers considérables. La loi sur le personnel permet certes aux services cantonaux de collecter des données sur la santé des conducteurs et

nen zu erheben. Ohne eine präzise gesetzliche Grundlage ist es aber nicht zulässig, Daten über die eingenommenen Medikamente zu erheben. Eine solche Datenerhebung wäre auch mit dem Grundsatz der Verhältnismässigkeit nicht vereinbar. Angaben über die Fahrtüchtigkeit (Arztzeugnis) genügen. Dem Tiefbauamt war daher mitzuteilen, eine Weisung, die den Arbeitnehmer zu einer Mitteilung über eingenommene Medikamente verpflichtet, sei widerrechtlich. Da eine dauernde Datenerhebung vorgesehen war, konnte eine Zustimmung der Mitarbeitenden über die fehlende Rechtsgrundlage nicht hinweg helfen.

- Die Registerharmonisierungsverordnung erlaubt es den Verwaltungsstellen, auf einer Rechnung die Kontoangaben des Rechnungsadressaten aufzuführen. Das war gegenüber einer Privatperson festzuhalten, die sich an dieser Information störte. Gegenüber der rechnungsstellenden Verwaltungseinheit war aber klar zu stellen, dass sie die Verantwortung für die bei der Rechnungsstellung bearbeiteten Daten vollumfänglich zu tragen hat. Verlangt eine Person Auskunft über ihre Daten, ist es der rechnungsstellenden Verwaltungseinheit nicht erlaubt, die betroffene Person einfach an das beauftragte Rechenzentrum weiter zu verweisen.
- Voraussichtlich auf den 1. Juli 2009 hin wird die Regelung der Videoüberwachung im Polizeigesetz in Kraft treten. Gegenüber mehreren interessierten Stellen, insbesondere Schulen, war festzuhalten, dass vor diesem Datum eine Videoüberwachung mit Aufzeichnung in öffentlich zugänglichen Räumen nicht zulässig ist. Nach Inkrafttreten der neuen Regelung ist eine Videoüberwachung nur zulässig, wenn die Kantonspolizei ihr zustimmt, wenn ein erhöhtes Schutzbedürfnis besteht und die Videoüberwachung zum Schutz der Gebäude und ihrer Benutzenden erforderlich ist. Die zuständige Stelle hat die Videoüberwachung mit einer Verfügung mit Rechtsmittelbelehrung anzuordnen. Die Verfügung ist zu veröffentlichen. Zur Beschwerdeführung ist auch die (kommunale) Datenschutzaufsichtsstelle befugt. Dieser ist die Videoüberwachung zur Vorabkontrolle zu unterbreiten. Schliesslich darf die Auswertung der Videoaufzeichnungen nur durch die Kantonspolizei erfolgen. Ein Auswerten setzt eine Strafanzeige, einen Strafantrag oder konkrete Verdachtsgründe für eine Straftat voraus. Ohne Auswertung sind die Aufnahmen 100 Tage nach ihrer Erstellung zu vernichten.

6 Gesetzgebung

6.1 Schengen/Dublin

Vertreter der Europäischen Union überprüften im Frühjahr, ob die in der Schweiz getroffenen Datenschutzmassnahmen den Übereinkommen von Schengen/Dublin genügen. Der Kanton Bern hatte hierzu vor allem darzulegen, wie er den Datenschutzanforderungen mit dem revidierten Datenschutzgesetz

conductrices de machines lourdes; sans base légale précise, il n'est toutefois pas admis d'étendre cette collecte de données aux médicaments consommés. Ce ne serait d'ailleurs pas non plus compatible avec le principe de la proportionnalité, puisque des données sur l'aptitude à conduire (certificat médical) sont suffisantes. Il s'est donc agi d'informer l'Office des ponts et chaussées du caractère illicite d'une instruction obligeant les salariés à indiquer quels médicaments ils absorbent. Du fait qu'une collecte permanente de données était prévue, il n'était pas possible de remédier à l'absence de base légale en obtenant l'assentiment des personnes concernées.

- L'ordonnance sur l'harmonisation des registres officiels permet aux services administratifs de faire figurer sur une facture le compte du destinataire de celle-ci. Le Bureau l'a confirmé à un particulier que cette mention dérangeait, tout en attirant l'attention du service administratif qui avait établi la facture sur sa pleine et entière responsabilité quant aux données traitées lors de la facturation. Si une personne demande des renseignements sur ses propres données, le service en question ne saurait se contenter de la renvoyer au centre de calcul mandaté.
- La réglementation de la vidéosurveillance dans la loi sur la police révisée entrera probablement en vigueur le 1^{er} juillet 2009. Le Bureau a dû relever à l'intention de plusieurs milieux intéressés, et en particulier des écoles, que la vidéosurveillance de lieux publics librement accessibles assortie d'un enregistrement des images n'était pas admise avant cette date. Après l'entrée en vigueur des nouvelles dispositions, la vidéosurveillance ne sera autorisée qu'avec l'approbation de la Police cantonale, s'il existe un besoin de protection accru et que cette mesure est requise pour protéger le bâtiment et ses utilisateurs et utilisatrices. Il appartiendra au service compétent d'ordonner la vidéosurveillance par voie de décision qu'elle publiera en l'assortissant d'une indication des voies de droit. L'autorité (communale) de surveillance de la protection des données aura également qualité pour recourir. Le projet de vidéosurveillance devra par ailleurs lui être soumis en vue d'un contrôle préalable. Enfin, seule la Police cantonale sera habilitée à analyser des images enregistrées. Elle ne pourra le faire qu'en cas de dénonciation, de plainte pénale ou d'indices concrets de la commission d'un acte punissable. Les enregistrements qui ne seront pas traités devront être détruits après 100 jours.

6 Législation

6.1 Schengen/Dublin

Des représentants de l'Union européenne ont examiné au printemps si les mesures de protection des données prises en Suisse satisfaisaient aux conditions des accords de Schengen/Dublin. Le canton de Berne a en particulier dû indiquer comment il entendait s'acquitter de ses obligations en la

und dem Ausbau der Datenschutzaufsichtsstelle genügen will. Die vorgesehenen Massnahmen erfüllten die Anforderungen.

6.2 Datenschutzgesetz

Das teilrevidierte Datenschutzgesetz gibt der Datenschutzaufsichtsstelle eine Rechtsmittelmöglichkeit bei abgelehnten Empfehlungen, sieht eine umfassende Kostenlosigkeit für die Einsicht in und für Auskünfte über die eigenen Daten vor und regelt den grenzüberschreitenden Datenverkehr detailliert. Der oder die kantonale Datenschutzbeauftragte wird durch den Grossen Rat auf Antrag des Regierungsrats auf vier Jahre gewählt (s. 4). Die kantonale Datenschutzaufsichtsstelle verfügt über ein eigenes Budget, das der Regierungsrat dem Grossen Rat unverändert unterbreiten muss. Wichtigere kantonale Informatikprojekte werden einer Vorabkontrolle unterstellt. Dies gilt auch für grössere Informatikprojekte von gemeinderechtlichen Körperschaften. (S. auch 1.1).

6.3 Datenschutzverordnung

Neben den technischen und organisatorischen Massnahmen des Datenschutzes (s. 3.) umschreibt die Datenschutzverordnung, welche technischen Mittel besondere Risiken enthalten und damit einer Vorabkontrolle unterstellt sind. Zur Behandlung von Auskunftsgesuchen wird eine 30-tägige Frist vorgegeben. Wie im Bundesrecht wird nahen Angehörigen ein Auskunftsrecht zu Daten über Verstorbene eingeräumt. Treffen gemeinderechtliche Körperschaften keine selbständige Regelung, wird für die Datenschutzaufsichtsstellen dieser Körperschaften eine abgestufte Ausgabenbefugnis vorgegeben.

Die Direktionen und die Staatskanzlei werden verpflichtet, mindestens eine Kontaktstelle für Datenschutz zu schaffen. Damit die Datenschutzaufsicht im Spitalbereich durch die kantonale Datenschutzaufsichtsstelle wahrgenommen werden kann, ist die Spitalversorgungsverordnung geändert worden.

6.4 Bundeserlasse

Die Vereinigung der Schweizerischen Datenschutzbeauftragten (PRIVATIM) nimmt zu Bundeserlassen nur noch vereinzelt Stellung. Hat sich PRIVATIM geäussert, schliesst sich die kantonale Datenschutzaufsichtsstelle dieser Äusserung wenn möglich an. Unter anderem nahm PRIVATIM zur Verordnung über den nationalen Teil des Schengener-Informationssystems (N-SIS) und das SIRENE-Büro sowie zum Rahmenbeschluss betreffend den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Stellung.

6.5 Kantonale Erlasse

Folgende Gesetzgebungsarbeiten sind aus Datenschutzsicht erwähnenswert:

Nach durchgeführtem Vernehmlassungsverfahren unterbreite-

matière avec la loi sur la protection des données révisée et grâce à l'étoffement du Bureau. Les mesures prévues ont été considérées comme répondant aux exigences.

6.2 Loi sur la protection des données

La loi partiellement révisée sur la protection des données prévoit une possibilité de recours du Bureau en cas de rejet de ses recommandations, ainsi que la gratuité de la consultation de ses propres données et de la communication de renseignements en la matière. Elle contient en outre une réglementation détaillée des flux transfrontières de données. La personne déléguée à la protection des données est désormais élue pour quatre ans par le Grand Conseil sur proposition du Conseil-exécutif (cf. ch. 4). Le Bureau dispose de son propre budget que le Conseil-exécutif doit soumettre sans modification au Grand Conseil. Les projets informatiques d'une certaine importance, du canton et des collectivités de droit communal, doivent maintenant faire l'objet d'un contrôle préalable (cf. aussi ch. 1.1).

6.3 Ordonnance sur la protection des données

Outre les mesures techniques et organisationnelles de la protection des données (cf. ch. 3), l'ordonnance sur la protection des données précise les moyens techniques présentant des risques particuliers et devant par conséquent faire l'objet d'un contrôle préalable. Elle impose un délai de 30 jours pour le traitement des demandes de renseignements. A l'instar du droit fédéral, l'ordonnance accorde aux proches des personnes décédées le droit de consulter les données de celles-ci. A moins que les collectivités de droit communal n'adoptent une réglementation propre, leurs autorités de surveillance disposent annuellement d'une compétence en matière d'autorisation de dépenses fixée dans l'ordonnance selon un barème se référant à leur taille. Les Directions et la Chancellerie d'Etat sont tenues de désigner au minimum un organe de contact pour la protection des données.

Enfin, l'ordonnance sur les soins hospitaliers a été modifiée afin que le Bureau puisse se charger de la surveillance de la protection des données dans le domaine hospitalier également.

6.4 Législation fédérale

L'association des commissaires suisses à la protection des données (PRIVATIM) ne prend plus que sporadiquement position sur des actes législatifs fédéraux. Le cas échéant, le Bureau se rallie si possible à son avis. PRIVATIM s'est en particulier prononcée au sujet de l'ordonnance sur la partie nationale du Système d'information Schengen (N-SIS) et sur le bureau SIRENE, ainsi qu'à propos de la décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

6.5 Législation cantonale

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

Au terme de la procédure de consultation, le Conseil-exécutif

te der Regierungsrat den Entwurf für ein Archivgesetz dem Grossen Rat. Dass vorab den Justizinstanzen ihre Daten auch nach der Archivierung noch für die Praxisbildung zur Verfügung stehen sollen, wurde präzisiert.

Zum Einführungsgesetz zur Zivilprozessordnung, zur Strafprozessordnung und zur Jugendstrafprozessordnung war darauf hinzuweisen, dass die aktuellen Regelungen zur Datenaufbewahrung bei der Polizei auch in den neuen Einführungserlass aufzunehmen sind. Zu regeln ist sodann die Zuständigkeit für datenschutzrechtliche Verfügungen, und es sind Rückmeldungen an die Polizei über Urteile vorzusehen. Es soll dies der Polizei ermöglichen, die ihr vorgegebene Datenvernichtung korrekt umzusetzen. Schliesslich waren zur Anzeigepflicht - etwa von Gesundheitspersonen - Präzisierungen anzubringen.

Schon in der Vorbereitungsphase konnte die Datenschutzaufsichtsstelle zum Einführungsgesetz zum Bundesgesetz über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung aufzeigen, welche rechtlichen Grenzen bei der Regelung von Überwachungsmassnahmen gegenüber Versicherten zu beachten sind.

Zur kantonalen Tierschutzverordnung war festzuhalten, dass Meldungen von Tierärzten über tierschutzwidriges Verhalten von Tierhaltern nur in einem Gesetz, nicht aber in einer Verordnung vorgesehen werden dürfen. Es handelt sich um einen schweren Eingriff in das Grundrecht auf Datenschutz.

(Zur Regelung der Videoüberwachung im Polizeigesetz s. 5., zu Datenschutzgesetz und -Verordnung s. 6.2 und 6.3).

7 Aufsichts- und Justizentscheide

7.1 Löschung von Vorermittlungsdaten bei der Polizei

Nach einer sicherheitspolizeilich motivierten Identitätsfeststellung im Zusammenhang mit einer Anti-WEF Demonstration speicherte die Polizei Personendaten des Betroffenen für zwei Jahre in ihre Vorermittlungsdatenbank. Diese dient zur Verbrechensverhütung oder –aufklärung. Auf einen Rekurs hin verpflichtete die Anklagekammer des Obergerichts in ihrem Entscheid die Polizei, dem Löschungsgesuch des Betroffenen umgehend stattzugeben. Es sei im konkreten Fall nicht ersichtlich, inwiefern die zweijährige Aufbewahrung zur Verbrechensverhütung oder –aufklärung dienen könne.

7.2 Sozialhilfegesuch: Dritte, die Unterstützung leisten, müssen bekannt gegeben werden

Wegen fehlender Mitwirkung bei der Bedürftigkeitsprüfung hatte eine Einwohnergemeinde ein Gesuch um Sozialhilfe abgelehnt. Das Verwaltungsgericht schützte diesen Entscheid.

Die Gesuchsteller hatten die Namen von Drittpersonen nicht genannt, welche sie angeblich freiwillig finanziell unterstützt hatten. Damit sei die Herkunft der Gelder nicht überprüfbar.

a soumis au Grand Conseil un projet de loi sur l'archivage. Une précision a été apportée, selon laquelle les données archivées doivent, pour la jurisprudence, rester à la disposition des autorités de justice notamment.

Le Bureau a relevé la nécessité d'inscrire la réglementation actuelle relative à la conservation des données par la police dans la loi portant introduction du code de procédure civile, du code de procédure pénale et de la loi sur la procédure pénale applicable aux mineurs. Il s'agissait en outre de régler, dans cette même loi, la compétence de rendre des décisions en matière de protection des données, et de prévoir la communication des jugements à la police afin qu'elle puisse respecter ses obligations en matière de destruction des données. Enfin, des précisions ont dû être apportées au sujet de l'obligation de dénoncer imposée, par exemple, aux professionnels de la santé.

S'agissant de la loi portant introduction de la loi fédérale sur les prestations complémentaires à l'AVS et à l'AI, le Bureau a pu attirer l'attention, dès la phase préparatoire, sur le cadre légal à respecter dans la réglementation des mesures de surveillance à l'égard des assurés.

A propos de l'ordonnance cantonale sur la protection des animaux, le Bureau a dû préciser que seule une loi, et non une ordonnance, pouvait obliger les vétérinaires à annoncer les comportements de détenteurs et de détenteuses d'animaux contraires à la législation sur la protection des animaux. Il s'agit en effet d'une atteinte grave au droit fondamental à la protection des données.

(Cf. ch. 5 s'agissant de la réglementation de la vidéosurveillance dans la loi sur la police, et ch. 6.2 et 6.3 à propos de la loi et de l'ordonnance sur la protection des données.)

7 Surveillance et décisions de justice

7.1 Radiation des données des enquêtes préliminaires de la police

Après un contrôle d'identité auquel elle avait procédé pour des motifs de sécurité dans le cadre d'une manifestation anti-WEF, la police a conservé les données personnelles de l'intéressé pendant deux ans dans sa banque de données relative aux enquêtes préliminaires – banque destinée à la prévention et à l'élucidation des crimes. Saisie d'un recours en la matière, la Chambre d'accusation de la Cour suprême a, dans sa décision, obligé la police à donner immédiatement suite à la demande de radiation de l'intéressé, au motif qu'elle ne voyait pas en quoi la conservation des données pendant deux ans pouvait, en l'espèce, servir à la prévention ou à l'élucidation de crimes.

7.2 Demande d'octroi de l'aide sociale: les noms de tiers accordant des prestations doivent être indiqués

Une commune municipale a rejeté une demande d'octroi de l'aide sociale faute de participation des requérants à la détermination du besoin d'aide sociale. Le Tribunal administratif a protégé cette décision.

Les requérants avaient refusé d'indiquer le nom de tiers qui, selon leurs dires, les avaient volontairement soutenus sur le plan financier. Dès lors que l'origine des montants était invéri-

Es bleibe offen, ob es sich um freiwillige Unterstützungsleistungen oder allenfalls um Zahlungen aus privatrechtlicher oder öffentlichrechtlicher Verpflichtung handle. Dies verunmögliche eine Anspruchsprüfung.

7.3 Soll eine Sozialhilfebehörde einen Massnahmenvollzug mitfinanzieren, ist die Bekanntgabe der Straftaten nicht zulässig

Die Polizei- und Militärdirektion entschied auf Laienbeschwerde hin, es sei widerrechtlich der unterstützungspflichtigen Sozialhilfebehörde mit der Einweisungsverfügung die dem Eingewiesenen zur Last gelegten Straftaten bekannt zu geben. Eine gesetzliche Grundlage für eine solche Bekanntgabe fehle und deren Kenntnis sei für die Aufgabenerfüllung der Sozialhilfebehörde (Teilbeteiligung an den Vollzugskosten) nicht erforderlich.

7.4 Auch der Inhalt eines Protokolls muss verhältnismässig sein

Zu den Aufgaben eines Regierungsstatthalters gehört die Vermittlung zwischen Bevölkerung und Behörden. Zur Überprüfung der Aufgabenerfüllung genügt es, wenn über ein Vermittlungsgespräch ein Beschlussesprotokoll erstellt wird. In einem Beschwerdeentscheid wies das Verwaltungsgericht den Regierungsstatthalter an, das zu detaillierte Diskussionsprotokoll zu kürzen.

8 Sozialhilfe

Zur Bekämpfung des Missbrauchs in der Sozialhilfe überwies der Grosse Rat im Frühjahr zwei Motionen. Datenbekanntgaben zwischen Behörden sollen erleichtert werden. Die Gesundheits- und Fürsorgedirektion gab ein Rechtsgutachten in Auftrag. Dieses soll zeigen, ob und wo ein Handlungsbedarf besteht und wie neue Regelungen aussehen sollen. Wichtige Informationen hierzu sind auch dem von der Stadt Bern ausgearbeiteten Umsetzungsbericht Sozialhilfe zu entnehmen. Nationalrat Lustenberger reichte auf Bundesebene ein Postulat zur Evaluation des Austausches personenbezogener Informationen zwischen Behörden des Bundes und der Kantone in ausgewählten Bereichen ein. In der vom Bund zur Bearbeitung eingesetzten Arbeitsgruppe nimmt ein Vertreter von PRIVATIM teil (s. 1.2). Auch auf Gemeindeebene wurden parlamentarische Vorstösse eingereicht. Mehrere Gemeinden führen koordiniert mit der Gesundheits- und Fürsorgedirektion Pilotprojekte zum Einsatz von Sozialinspektoren durch. Die Datenschutzaufsichtsstelle begrüsst die eingeleiteten Überprüfungen. Es ist allerdings fraglich, ob beim Einsatz von Sozialinspektoren eine Gemeinderatsverordnung für die verdeckte Beobachtung mit Videokameras im öffentlichen Raum als Rechtsgrundlage genügt.

9 Gemeinderechtliche Körperschaften

Das überarbeitete Datenschutzgesetz nimmt die kommunalen Datenschutzaufsichtsstellen verstärkt in die Pflicht. Die parlamentarische Aufsichtskommission (und Datenschutzaufsichtsstelle) von Worb lieferte ein Beispiel dafür, dass kommunales Aufsichtshandeln durchaus wirkungsvoll sein kann.

fiabile, il était impossible de déterminer s'il s'agissait de prestations volontaires ou alors de paiements découlant d'engagements de droit privé ou de droit public et, partant, d'examiner le droit à l'octroi de l'aide sociale.

7.3 Illégalité de la communication des infractions commises à l'autorité sociale qui cofinance l'exécution de mesures

Suite à un recours formé par un particulier non assisté d'un avocat, la Direction de la police et des affaires militaires a posé le principe de l'illégalité de la communication de la décision de placement mentionnant les infractions commises à l'autorité sociale tenue de verser des prestations. Il n'existe en effet pas de base légale autorisant une telle communication, et l'autorité sociale n'a pas besoin des données en question pour accomplir sa tâche (participation aux frais d'exécution).

7.4 Validité du principe de la proportionnalité dans le cas d'un procès-verbal également

Un préfet a notamment pour tâche de jouer un rôle d'intermédiaire entre la population et les autorités. Pour l'examen de l'accomplissement de la tâche, il suffit qu'un entretien mené à ce titre fasse l'objet d'un procès-verbal des décisions. En conséquence, le Tribunal administratif a enjoint à un préfet, dans une décision sur recours, d'abrégé un procès-verbal trop détaillé.

8 Aide sociale

Au printemps, le Grand Conseil a adopté deux motions relatives à la lutte contre les abus dans l'aide sociale, tendant à ce que les échanges de données entre autorités soient facilités. La Direction de la santé publique et de la prévoyance sociale a demandé une expertise juridique visant à déterminer si une intervention s'imposait et laquelle, et quel devait être le contenu d'éventuelles nouvelles réglementations. Un rapport sur la mise en œuvre de l'aide sociale établi par la ville de Berne fournit également des informations importantes à cet égard. Ruedi Lustenberger, conseiller national, a pour sa part déposé au niveau fédéral un postulat sur l'évaluation des échanges de données entre autorités fédérales et cantonales dans certains domaines. Un représentant de PRIVATIM (cf. ch. 1.2) fait partie du groupe de travail institué pour traiter ce postulat. Des interventions parlementaires ont également été déposées au niveau communal, et plusieurs communes mènent avec la Direction de la santé publique et de la prévoyance sociale des projets-pilotes sur l'engagement d'inspecteurs sociaux. Le Bureau se félicite des recherches entreprises, mais doute qu'une ordonnance du conseil communal sur la surveillance cachée de l'espace public au moyen de caméras vidéo soit une base légale suffisante pour le recours à des inspecteurs sociaux.

9 Collectivités de droit communal

La loi révisée sur la protection des données met davantage à contribution les autorités communales de surveillance de la protection des données. L'une d'entre elles, la commission parlementaire de surveillance de Belp, a fourni un bon exemple d'efficacité: elle a mandaté un service de contrôle externe

Für 13'000 CHF prüfte eine externe Kontrollstelle das Extranet der Gemeinde und stellte schwere Sicherheitsmängel fest. Die Pensionskasse einer Gemeinde hat mit ihrem Fragebogen zum Neueintritt von Versicherten den Verhältnismässigkeitsgrundsatz zu respektieren. Auf Nachfrage eines kommunalen Personaldienstes wurde aufgezeigt, welche Fragen zum Gesundheitszustand vor allem auch in zeitlicher Hinsicht zu weitgehend waren.

Das Amt für Gemeinden und Raumordnung passte das Musterdatenschutzreglement der überarbeiteten Datenschutzgesetzgebung an. Über diese wurden die Gemeinden zudem mit einem Informationsschreiben informiert (s. 6.2 und 6.3).

(Zur Vorabkontrolle in Gemeinden s. 6.3, zum Videoeinsatz 5, zum Einsatz von Sozialinspektoren 8).

10 Berichtspunkte der Vorjahre

(S. 1.2: Vorbehalte des Regierungsrats zu den Verträgen mit Santéuisse; 3: Informatiksicherheits-Sollvorgaben; 5: Videoüberwachung; 6: Assoziierung an Schengen/Dublin; 6.5: Archivgesetz).

10.1 Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei

Für die Fernüberwachung von Lichtsignalen (mit Digitalkameras für die Geschwindigkeitsüberwachung und für das Erfassen von Rotlichtmissachtungen) ist die Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei zu ergänzen. Für die Informatikanwendung Methamorphose UVEK (Online-Zugriff der Kantonspolizei auf die Datenbank des Dienstes für besondere Aufträge des UVEK für die Überwachung des Post- und Fernmeldeverkehrs) genügt eine zusätzliche interne Weisung. Beides steht zurzeit beim Polizeikommando in Ausarbeitung.

10.2 Rechtsgrundlage für das System VICLAS der Kantonspolizei

Die Kantonspolizei Bern speichert für alle schweizerischen Polizeikörper Informationen zu geklärten und ungeklärten Sexual- und Tötungsdelikten in der Datenbank des Systems VICLAS. Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren bereinigt zurzeit den Konkordatsentwurf, der diese Datenbank rechtlich abstützen soll. Er soll den Kantonen im Verlauf des Jahres 2009 zur Beschlussfassung unterbreitet werden.

10.3 Abfrage von Fahrzeughaltern per SMS

Das kantonale Strassenverkehrsgesetz erlaubt es dem Strassenverkehrs- und Schifffahrtsamt, Fahrzeughalterdaten auf SMS-Abfrage hin bekannt zu geben. Ein Fahrzeughalter wollte vom Strassenverkehrs- und Schifffahrtsamt in Erfahrung bringen, ob, von welcher Nummer aus und zu welchem Zeitpunkt über ihn SMS-Abfragen gemacht worden seien. Die Datenschutzaufsichtsstelle wies das Strassenverkehrs- und Schifffahrtsamt darauf hin, dass solche Auskünfte vom daten-

qui, pour une somme de CHF 13 000, a examiné l'extranet de la commune et a constaté de graves lacunes en matière de sécurité.

La caisse de pension d'une commune doit respecter le principe de la proportionnalité en rédigeant le formulaire destiné aux nouveaux assurés. A la demande d'un service communal du personnel, le Bureau a indiqué quelles questions relatives à l'état de santé dépassaient le cadre admissible, notamment parce qu'elles portaient sur des faits trop anciens.

L'Office des affaires communales et de l'organisation du territoire a adapté le règlement type sur la protection des données à la législation révisée, et a informé les communes au sujet des nouvelles dispositions légales (cf. ch. 6.2 et 6.3).

(Cf. ch. 6.3 en ce qui concerne le contrôle préalable, ch. 5 s'agissant de la vidéosurveillance et ch. 8 à propos de l'engagement d'inspecteurs sociaux.)

10 Points abordés dans le rapport précédent

(Cf. ch. 1.2: réserves du Conseil-exécutif à propos des conventions conclues avec santéuisse; ch. 3: consignes de sécurité informatique; ch. 5: vidéosurveillance; ch. 6: association aux accords de Schengen/Dublin; ch. 6.5: loi sur l'archivage.)

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

L'autorisation délivrée à la Police cantonale d'exploiter le système informatique de surveillance à distance, par caméras numériques, des signaux lumineux (respect des feux rouges) et des limitations de vitesse doit être complétée. Dans le cas de l'application 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) par contre, il suffit d'édicter encore une instruction interne. Le Commandement de la police s'emploie actuellement à combler ces deux lacunes.

10.2 Base légale pour le système VICLAS de la Police cantonale

La Police cantonale bernoise enregistre à l'intention de tous les corps de police suisses les informations relatives aux infractions contre l'intégrité sexuelle et aux homicides, élucidés ou non, dans la banque de données du système VICLAS. La Conférence des directrices et directeurs des départements cantonaux de justice et police met actuellement au point un projet de concordat devant servir de base légale à ce système qu'il est prévu de soumettre aux cantons en 2009.

10.3 Obtention par SMS de renseignements sur les détenteurs de véhicules

La loi cantonale sur la circulation routière autorise l'Office de la circulation routière et de la navigation à communiquer des renseignements sur les détenteurs de véhicules par SMS. Un détenteur de véhicule a voulu savoir si un tiers avait obtenu des informations à son sujet et le cas échéant à partir de quel numéro et à quel moment. Une telle demande relève du droit d'accès et du droit de consulter ses données garantis par la législation sur la protection des données, comme le Bureau l'a

schutzrechtlichen Auskunfts- und Einsichtsrecht umfasst sind.

10.4 Fehlende Datenlöschung im Geschäftskontrollsystem TRIBUNA der Gerichte

Eine externe Kontrollstelle stellte die fehlende Löschung vor vier Jahren fest. Das Obergericht hat nun ein Archivierungs- und Lösungskonzept erarbeitet. Bis zum Zeitpunkt der Berichterstattung war die beauftragte Informatikfirma nicht in der Lage, das Konzept informatiktechnisch umzusetzen.

11 Besonderes

11.1 Einsatz von Überwachungsdrohnen an der EURO 08

Bereits im Herbst 2006 erlaubte der Bundesrat den Einsatz des Aufklärungsdrohnensystems ADS-95 für den nationalen Einsatzstab während der EURO 08. Eine Datenaufzeichnung untersagte er. Die Kantonspolizei sah einen Drohneneinsatz für die EURO 08 vor allem im Rahmen der Verkehrsüberwachung von Hauptverkehrsachsen und zur Lagebeurteilung bei Menschenansammlungen und Fussgängerströmen vor. Es sollten weder Detailaufnahmen von Personen und Fahrzeugen noch eine Datenaufzeichnung erfolgen. Der Drohneneinsatz sollte damit gleich ausgestaltet werden, wie in einer Einsatzübung der Stadtpolizei Zürich. Der Datenschutzbeauftragte der Stadt Zürich hatte diesen Einsatz für zulässig erklärt. Die kantonale Datenschutzaufsichtsstelle beurteilte die Situation für den Kanton Bern gleich.

12 Antrag

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

23. Januar 2009

Der Datenschutzbeauftragte: *Siegenthaler*

relevé à l'attention de l'Office de la circulation routière et de la navigation.

10.4 Non-effacement des données dans le système de contrôle des affaires TRIBUNA utilisé par les tribunaux

Il y a quatre ans, un service de contrôle externe avait relevé que les données n'étaient pas effacées du système. La Cour suprême a élaboré un projet de stratégie d'archivage et de radiation, mais au moment de la rédaction du présent rapport, la société informatique mandatée n'était pas en mesure de la mettre en œuvre sur le plan technique.

11 Cas particuliers

11.1 Recours à des drones de surveillance lors de l'EURO 08

En automne 2006 déjà, le Conseil fédéral avait autorisé l'utilisation, pendant l'EURO 08, du système de drones d'exploration ADS-95 au profit de l'état-major d'engagement national, tout en interdisant l'enregistrement des données. Dans ce contexte, la Police cantonale prévoyait un recours aux drones avant tout pour surveiller le trafic sur les axes principaux ainsi que pour apprécier la situation en cas de rassemblement ou de flux de piétons. Elle n'envisageait aucune prise de vue détaillée de personnes ou de véhicules, pas plus qu'un enregistrement des données. Ainsi, elle comptait faire la même utilisation des drones que la police municipale de Zurich lors d'un exercice d'engagement, exercice que le délégué à la protection des données de cette ville avait déclaré admissible. Le Bureau a apprécié la situation pour le canton de Berne de manière identique.

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.

23 janvier 2009

Le délégué à la protection des données: *Siegenthaler*

Anhang:**1. Abkürzungen, Bezeichnungen**

ADS 95: Aufklärungs Drohnen System 95
 ELA_DMS: elektronische Archivierung und Dokumenten-Management-System (der Spitäler fmi ag: Spitäler Frutigen, Meiringen, Interlaken)
 EURO 08: Fussballeuropameisterschaft 2008
 Evento: Hochschul- und Schulverwaltungs-, Kursadministrations-, Event- und Ressourcen-Managementsystem
 FIS 2000: Finanz-Informationssystem
 GERES: Gemeinderegister-System
 GINA: Gefängnis Insassen Administration
 IDIS: Infectious Diseases Information System (Infektionskrankheiten-Informationssystem)
 IFIK: Institut für Infektionskrankheiten
 ISDS: Informationssicherheit und Datenschutz
 i-pdos: Integriertes Patientendossier Inselspital
 IT-(Sicherheitsbeauftragter): Informationstechnologie (auch NewIT)
 KAST: Kantonale Amtsstelle
 LAM: Logistik Arbeitsmarktliche Massnahmen
 M4I: Materialwirtschaftslösung Inselspital
 NESKO: Neues Steuerkonzept; Gesamtheit der Steuerveranlagungs- und Steuerbezugsapplikationen (AB: Amtliche Bewertung)
 s: siehe
 Santéuisse: Verband der Schweizer Krankenversicherer (Verein)
 RAV: Regionales Arbeitsvermittlungszentrum
 SECO: Staatssekretariat für Wirtschaft
 SMS: Short message system: Über ein Handy verschickte Kurznachrichte
 TRIBUNA: auf die Bedürfnisse der Organe der Rechtspflege ausgerichtete Geschäftskontrolle
 TS-BVE: Terminalserver, Bau-, Verkehrs- und Energiedirektion
 UVEK: Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
 VICLAS: Violent Crime Linkage Analysis System: Analyse-System zum Verknüpfen von Gewaltdelikten
 WEF: World Economic Forum Davos (Weltwirtschaftsforum)
 ZPV: Zentrale Personenverwaltung

2. Referenznummern der in Ziffer 7 aufgeführten Justizentscheide

7.1: Beschluss der Anklagekammer vom 14. 8. 2008: AK Nr. 2008/193 EMI
 7.2: VGE vom 16.12. 2008: 100.2008.23391U
 7.3: Beschwerdeentscheid der Polizei- und Militärdirektion vom 16. 10. 2008: BD 071/08 Ba
 7.4: VGE vom 22. 09. 2008: 100.2007.23150U

Annexe:**1. Abréviations et désignations**

ACT: autorité cantonale
 ADS 95: système de drones d'exploration 1995
 Cf.: confer (voir)
 DEP: dossier électronique du patient (Hôpital de l'Ile)
 DETEC: Département fédéral de l'environnement, des transports, de l'énergie et de la communication
 ELA_DMS: archivage électronique et système de gestion des documents (du centre hospitalier régional FMI SA: hôpitaux de Frutigen, Meiringen et Interlaken)
 EURO 08: championnat d'Europe de football 2008
 Evento: logiciel standard pour la gestion des écoles de tous les niveaux, l'administration de cours ainsi que la gestion des événements et des ressources
 FIS 2000: système d'informations financières
 GCP: gestion centrale des personnes
 GERES: système des registres communaux
 GINA: programme pour l'administration des détenus et détenues
 IDIS: Infectious Diseases Information System (système d'information sur les maladies infectieuses)
 ifik: Institut des maladies infectieuses
 LMMT: service de logistique des mesures de marché du travail
 M4I: système de gestion du matériel de l'Hôpital de l'Ile
 NESKO: Système informatique de l'Intendance des impôts, servant à la taxation et à la perception
 ORP: office régional de placement
 santéuisse: association regroupant les assureurs-maladie suisses
 SECO: Secrétariat d'Etat à l'économie
 SIPD: sûreté de l'information et protection des données
 SMS: Short message system – message court envoyé par téléphone portable
 TRIBUNA: système de contrôle des affaires adapté aux besoins des organes des différentes juridictions
 TS-BVE: serveur de terminal, Direction des travaux publics, des transports et de l'énergie
 VICLAS: Violent Crime Linkage Analysis System – système d'analyse des crimes violents devant servir à l'identification des criminels en série
 WEF: World Economic Forum Davos (Forum économique mondial de Davos)

2. Numéros de référence des décisions de justice mentionnées au chiffre 7

7.1: arrêt de la Chambre d'accusation du 14.08.2008: AK n° 2008/193 EMI
 7.2: JTA du 16.12.2008: 100.2008.23391U
 7.3: décision sur recours rendue par la Direction de la police et des affaires militaires le 16.10.2008: BD 071/08 Ba
 7.4: JTA du 22.09.2008: 100.2007.23150U