Rapport d’activité 2014 du Bureau pour la surveillance de la protection des données du canton de Berne

Bureau pour la surveillance de la protection
des données du canton de Berne
Münstergasse 2
3011 Berne
Téléphone 031 633 74 10
Télécopie 031 633 74 11
info.datenschutz@jgk.be.ch
www.be.ch/bpd

Table des matières

		Page
1.	Introduction	1
2.	Description des tâches, priorités, moyens à disposition	2
3.	Contrôle des applications informatiques utilisées	3
4.	Vidéosurveillance	4
5.	Contrôle préalable de projets informatiques	4
6.	Avis exprimés, pratique	6
7.	Législation	7
8.	Surveillance et décisions de justice	8
9.	Collectivités de droit communal	9
10.	Cas particulier	9
11.	Points abordés dans le rapport précédent	10
12.	Proposition	10
13.	Annexe	11

1 Introduction

1.1 2014 en bref

Il devient de plus en plus rare que les services gèrent leurs applications informatiques de manière autonome et dans leur domaine de compétences exclusivement. De plus en plus souvent, les tâches liées à la gestion de ces applications sont réparties entre différentes entités. Ainsi, c'est désormais l'Office d'informatique et d'organisation du canton de Berne (OIO) qui assure les prestations informatiques de base pour plusieurs services. Or, lui-même a confié l'exploitation de l'infrastructure à la société BEDAG SA (centre de calcul), qui appartient au canton. D'autres services ont conclu des contrats directement avec des prestataires externes. Dans les deux cas, des données particulièrement dignes de protection, issues de diverses applications liées à la gestion des affaires, sont traitées dans des centres de calcul externes.

Avant que ces applications ne soient mises en service, les prescriptions en matière de sécurité informatique ont été présentées dans des concepts SIPD et examinées dans le cadre de procédures de contrôle préalable; leur mise en œuvre, qui relève de la responsabilité des services concernés, a en outre fait l'objet d'une surveillance.

Au cours de l'année écoulée, le Bureau pour la surveillance de la protection des données (le Bureau) a constaté à plusieurs reprises que, après l'introduction de procédures fondées sur le partage des tâches, les prescriptions en matière de sécurité informatique qui avaient été définies

- n'étaient pas communiquées sous une forme contraignante aux partenaires externes (dans le cas des contrats conclus directement par les services) ou
- n'étaient pas traduites en mesures concrètes par les partenaires externes malgré les clauses de délégation figurant dans le contrat (dans le cas où l'OIO joue le rôle d'intermédiaire).

Dans le cas où les tâches sont confiées à la société BEDAG SA, celle-ci, en tant que centre de calcul certifié, garantit une protection de base de son infrastructure informatique en vertu des normes ISO-2700x. Les services ne savent toutefois pas si ces mesures constituent une protection de base suffisante pour leurs applications. Or, pour ces applications, des mesures de sécurité allant plus loin que la simple protection de base sont souvent nécessaires. Les services ne peuvent ainsi plus garantir que toutes les mesures nécessaires en matière de sécurité pour leurs applications sont effectivement prises, ni le prouver. Le Bureau a été confronté à ce problème de «déresponsabilisation» tant dans le cadre de ses interventions en qualité d'autorité de surveillance que lors des contrôles préalables et même lors d'un simple contrôle (cf. ch. 3, 5 et 6).

Un examen du travail du Bureau a été effectué. Conformément aux accords de Schengen/Dublin, un comité d'experts issus des Etats parties a procédé à l'évaluation. Il a recommandé que les mesures introduites lors de la révision de la loi sur la protection des données de 2008 soient renforcées et étendues (cf. ch. 1.3).

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

Le préposé fédéral à la protection des données et à la transparence (PFPDT) coordonne la surveillance du Système d'information Schengen (SIS). Deux séances de travail ont été organisées en 2014. Des collaborateurs du Bureau sont membres des groupes de travail «Santé» et «Technologies de l'information et de la communication» de PRIVATIM. Ce dernier a publié un document relatif aux exigences techniques concernant l'utilisation des systèmes informatiques hospitaliers[1].

PRIVATIM a par ailleurs organisé deux cours d'une journée à l'intention des juristes, l'un constituant une introduction à la sécurité informatique et l'autre proposant un perfectionnement grâce à l'étude de cas pratiques, auxquels les collaborateurs du Bureau ont assisté. (A propos de la nouvelle version du contrat sur l'utilisation de Microsoft Office 365 dans les écoles, cf. ch. 9).

1.3 Evaluation sur la base des accords de Schengen

Le comité d'experts des Etats parties qui a examiné, en plus des services fédéraux, ceux des cantons du Jura, de Neuchâtel et de Berne a formulé les commentaires et remarques suivants:

- L'indépendance du Bureau en matière de budgétisation, ancrée dans la loi sur la protection des données, doit encore être renforcée dans la pratique.
- L'indépendance vis-à-vis de la Commission de gestion du Grand Conseil, elle aussi ancrée dans la loi, doit être comprise en ce sens que

[1] En allemand, ce document s'intitule «Datenschutztechnische Anforderungen an Klinikinformationssysteme». Du fait qu'il est actuellement en cours de traduction, son titre définitif en français n'est pas encore disponible.

celle-ci ne doit avoir aucune influence sur les décisions prises.
- Il convient de contrôler plus souvent, et sur une base périodique, les accès de la Police cantonale au SIS.
- A l'avenir, le Bureau doit procéder lui-même à ces contrôles et non les confier à des prestataires externes.
- Les contrôles effectués par le Commandement de la police en collaboration avec le Bureau constituent un bon outil de travail mais n'en restent pas moins des autocontrôles, qui sont insuffisants.
- Le recours à des personnes externes chargées d'effectuer des contrôles nécessite la création d'une base légale, en collaboration avec le groupe de coordination Schengen (cf. ch. 1.2); l'indépendance de ces personnes par rapport aux services contrôlés doit par ailleurs être garantie.
- Une augmentation de l'effectif du personnel du Bureau doit être proposée aux autorités compétentes.
- Des informations relatives aux bases légales du SIS ainsi qu'un modèle de lettre concernant l'exercice du droit à l'information et à la rectification des données doivent figurer sur le site Internet du Bureau (cf. ch. 1.2; s'agissant des ressources, cf. ch. 2.3).

2 Description des tâches, priorités, moyens à disposition

2.1 Priorités

Le Bureau doit notamment contrôler le traitement des données, veiller à la mise en œuvre des prescriptions relatives à la sécurité des données, conseiller les membres de l'administration et les personnes concernées, se charger de l'examen préalable de projets informatiques et veiller de manière générale au respect des droits inscrits dans la législation sur la protection des données. C'est la loi sur la protection des données qui lui attribue ces tâches de large envergure. Toutefois, les ressources disponibles ne permettent au mieux que des interventions ponctuelles. Il convient donc de déterminer, pour chaque activité, quel est le degré de priorité et quels moyens doivent être engagés. Les critères suivants permettent de répondre à ces questions:

– Préséance de l'autorité compétente: ce sont les autorités communales de surveillance en matière de protection des données ou les services juridiques de l'administration cantonale compétents qui conseillent les services administratifs communaux et cantonaux. S'agissant des questions communales, les autorités communales de surveillance en matière de protection des données conseillent les personnes concernées. Il convient de renvoyer toute personne ou tout service qui adresse une demande directe au Bureau à l'autorité compétente. Ces compétences et les modes de fonctionnement qui en résultent sont ancrés dans l'ordonnance sur la protection des données.

– FAQ: Si une question, qu'elle soit formulée par une personne ou par un service administratif, est posée à plusieurs reprises ou si l'on peut s'attendre à ce qu'elle le soit, il convient de publier rapidement la réponse, rédigée dans une forme générale, sur le site Internet. Lorsque la question est à nouveau posée, il suffit alors de renvoyer à cette publication.

– Standards de qualité différenciés: lorsqu'il s'agit de répondre à une personne ou à une autorité non professionnelle, le Bureau peut se contenter d'envoyer des instructions (sans arguments juridiques). En revanche, lorsqu'il doit prendre position au sujet de documents émanant d'une autorité de justice, une réponse détaillée et approfondie d'un point de vue juridique est nécessaire. Le standard de qualité doit être défini au préalable.

– Subsidiarité de l'activité de surveillance: la législation sur la protection des données donne aux personnes concernées des moyens efficaces pour se défendre (celles-ci peuvent notamment demander la rectification ou la destruction de données personnelles et faire constater l'illicéité d'une publication). L'autorité de surveillance n'intervient pas lorsque de telles possibilités sont offertes. Les personnes concernées doivent toutefois être informées de leurs droits. S'il y a lieu de croire que des problèmes de fonctionnement existent, l'autorité de surveillance doit engager les moyens nécessaires (p. ex. contrôles) au suivi de ces problèmes.

– Contrôles préalables: les consignes applicables aux contrôles préalables visent à inciter les responsables de projet à mettre en œuvre les prescriptions en matière de protection des données. Cet objectif peut être atteint même si le Bureau se contente d'une vérification formelle du dépôt des documents assortie ou non d'un examen partiel du contenu. Celui-ci peut notamment renoncer totalement à un tel examen si un responsable de projet lui a déjà soumis à plusieurs reprises des documents qui étaient en ordre, si un projet a une importance secondaire ou si sa charge de travail globale ne lui permet pas d'entamer de nouveaux examens (adaptation aux variations de la charge de travail). Il y a notamment lieu de procéder à des contrôles partiels lorsque, dans certains domaines, des constats peuvent être tirés de précédents examens (p. ex. sur la sécurité de l'infrastructure informatique utilisée) ou lorsque certains domaines sont connus pour présenter des risques

importants (p. ex. droits d'accès à des données particulièrement dignes de protection).

– Renonciation à prendre position au sujet d'actes législatifs fédéraux: dans la procédure législative, les mêmes questions se posent régulièrement en termes semblables pour tous les cantons. Pour ces questions, le Bureau se contente de diffuser la prise de position de PRIVATIM et, le cas échéant, de participer à l'élaboration de celle-ci.

Les tâches sont attribuées aux collaborateurs en fonction de la région (communes), de l'unité administrative cantonale (Direction) et du domaine (p. ex. droit cantonal sur les Eglises). Ceux-ci fixent eux-mêmes les priorités en fonction des critères susmentionnés. La priorisation des affaires relatives aux contrôles préalables s'effectue en collaboration avec la direction du Bureau. Si les collaborateurs ne parviennent plus à respecter les délais de réponse fixés (conformément aux objectifs de prestation de NOG), certaines priorités peuvent être déplacées, le dossier peut être confié à un autre collaborateur, le traitement d'un dossier peut être (partiellement) abandonné ou le standard de qualité revu à la baisse, avec l'accord de la direction du Bureau. Celle-ci garantit toutefois que les applications informatiques font dans tous les cas l'objet d'un contrôle, que le suivi des contrôles est assuré et que, malgré le fait qu'il est renoncé à certains contrôles préalables, les responsables de projet veillent par eux-mêmes au respect de la protection des données. S'agissant des conseils dispensés et des interventions réalisées en qualité d'autorité de surveillance, l'accent est mis sur les évolutions techniques qui ont des conséquences particulières sur les droits de la personnalité. La direction du Bureau demandera une augmentation des ressources si des tâches supplémentaires sont confiées à ce dernier, par exemple en cas de cantonalisation, ou si des instances de contrôle estiment qu'une telle augmentation est nécessaire pour garantir l'accomplissement des tâches (cf. ch. 1.3).

2.2 Responsabilité propre des services traitant les données

L'OIO a mis sur pied, avec la Haute école de Lucerne, une formation CAS sur la sécurité informatique, à laquelle ont participé principalement les (futurs) responsables de la sécurité informatique du canton de Berne et les experts de la Confédération en matière de sécurité. La Chancellerie d'Etat a organisé une présentation sur la protection des données dans le cadre d'une formation continue à l'intention des collaborateurs des services de traduction.

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

En 2014, le budget attribuait, pour l'administration cantonale, CHF 34 millions aux investissements dans le domaine informatique et CHF 161 millions à l'exploitation (dont CHF 117 mio destinés à des tiers prestataires de services). Ces chiffres ne concernent pas l'Hôpital de l'Ile ni les autres hôpitaux, également placés sous la surveillance du Bureau, ni les applications spécialisées qui ne sont pas gérées de manière centralisée.

Pour le contrôle des applications informatiques gérées par des services externes (cf. ch. 3), la somme prévue était de CHF 182 000.

Le Bureau disposait de 4,7 postes à temps complet (dont 0,7 pour le secrétariat). Après l'introduction d'un système de gestion des affaires électronique, il a été renoncé à un poste de secrétariat à 50 pour cent. Des informations complémentaires relatives au budget, aux comptes ainsi qu'aux objectifs de NOG (données financières) sont disponibles dans le rapport de gestion de 2014 du canton de Berne (volume I).

3 Contrôle des applications informatiques utilisées

Trois audits ont été réalisés en 2014:

- Examen de la protection de base de l'infrastructure informatique de la Direction de l'instruction publique du canton de Berne

Les services informatiques (SI) centraux assurent les services informatiques de base (services de messagerie, services Internet, administration des écoles, gestion des ressources, etc.) de la Direction de l'instruction publique (INS). Dans le but d'accroître l'efficacité des prochains contrôles préalables, le Bureau et la direction informatique sont tombés d'accord pour réaliser un examen de la protection de base conformément à la norme ISO 27000. L'examen réalisé sur place a montré que les services informatiques centraux exploitent de manière professionnelle une infrastructure informatique complexe et hétérogène. Il a cependant révélé que des mesures devaient en particulier être prises concernant la collaboration avec les prestataires externes. En effet, la direction informatique de l'INS n'a qu'une idée assez vague de la configuration et de la qualité du service de l'infrastructure pare-feu, qui est gérée à l'extérieur et qui joue pourtant un rôle important

dans la sécurité du réseau, et n'en a aucun contrôle (cf. ch. 1.1).

- Centre hospitalier Bienne SA (CHB)

Le système d'informations cliniques du CHB a été examiné, avec le soutien professionnel du service d'informatique et du responsable de l'exploitation. L'examen a révélé la frontière délicate entre utilisation optimale de toutes les données médicales disponibles et respect de la protection des données personnelles des patients. Ses résultats montrent que le système informatique opérationnel fonctionne de manière fiable et que l'application est gérée avec soin. De plus, les principales personnes impliquées sont sensibles aux questions relatives à la protection des données. Du point de vue technique, les responsabilités en matière d'encadrement des prestataires externes doivent être précisées et des directives relatives à l'exécution des processus de maintenance doivent être élaborées. Les mesures relatives à la mise en œuvre de la stratégie en matière d'accès doivent être appliquées rapidement.

- Audit de l'infrastructure mobile (téléphones intelligents) de la Police cantonale

Le contrôle de l'infrastructure mobile de la Police cantonale porte sur la gestion des terminaux mobiles (Mobile Device Management, MDM) et les téléphones intelligents. Au moment de l'établissement du présent rapport, l'évaluation du contrôle n'était pas encore terminée.

- Suivi des contrôles effectués en 2013
  - Examen de la protection de base à l'Université de Berne

Les constats de l'examen réalisé en 2013 ont été passés en revue avec le Bureau et un plan de mesures ainsi qu'un calendrier ont été définis. Grâce au soutien décisif des responsables SIPD de l'Université de Berne, une grande partie des mesures ont déjà été mises en œuvre. La fin des travaux est prévue pour le milieu de 2015.

  - Clinique Südhang

Des mesures urgentes ont déjà été prises. L'élaboration d'une stratégie de radiation est en cours.

  - Bureau d'encaissement des amendes

La Direction de la magistrature a pris position sur la question du délai de conservation applicable ainsi que sur l'existence d'une procédure d'appel.

4 Vidéosurveillance

Plusieurs installations de vidéosurveillance de bâtiments cantonaux ont été examinées dans le cadre d'une procédure de contrôle préalable, notamment celles de la caserne de Berne et des postes de police. Il a régulièrement été procédé à des adaptations du champ de caméra, lorsque, de manière disproportionnée, un large périmètre extérieur était filmé, par exemple un trottoir situé sur le domaine public ou une route publique adjacente.

La loi sur l'exécution des peines et mesures (LEPM) prévoit que les visites, dans les établissements pénitentiaires, ne peuvent être surveillées au moyen de caméras qu'«ouvertement» (à savoir que les caméras doivent être visibles, pour les personnes concernées) et «dans des cas motivés». C'est ce qu'a révélé une analyse effectuée suite à une question. Ces conditions n'étant pas remplies, les caméras installées dans les espaces destinés aux visites de l'établissement de Thorberg ont dû être retirées.

S'agissant des bâtiments administratifs de l'OIO, le Bureau a demandé à voir l'autorisation requise suite à une déclaration parue dans les médias. L'exploitant a par la suite reconsidéré le but de l'installation et renoncé à utiliser des caméras à l'avenir.

Un accord a été trouvé avec la Police cantonale concernant la procédure de mise en œuvre de l'obligation d'évaluer les installations de vidéosurveillance dès 2015. Les autorités compétentes ou les exploitants doivent procéder à l'évaluation des installations conformément aux prescriptions de l'ordonnance sur la vidéosurveillance dans les cinq ans qui suivent la mise en service de celles-ci et publier un rapport à ce sujet. La Police cantonale donnera des instructions aux autorités communales et cantonales à cet égard.

5 Contrôle préalable de projets informatiques

Le Bureau a de nouveau examiné un grand nombre d'applications utilisées dans le secteur de la santé, en particulier des systèmes d'informations cliniques (SIC):

- Dans le cadre du contrôle préalable de l'application MC-SIS, utilisée pour le programme de dépistage de cancer du sein par mammographie, qui est mis en œuvre par la Ligue bernoise contre le cancer sur mandat du canton, une deuxième rencontre sur place a eu lieu au cours de 2014. Deux prises de position ont été émises par la suite. Les documents SIPD révisés n'ont pas encore pu être remis au Bureau en raison du manque de personnel.

- Au début de l'année, le Bureau a à nouveau émis deux prises de position sur l'application NICERStat du registre des tumeurs du canton de Berne. Grâce à la bonne collaboration avec

les personnes responsables, le contrôle préalable a ensuite pu être achevé.

- En 2014, le Bureau a émis plusieurs prises de position dans le cadre du contrôle préalable du SIC de la clinique bernoise de Montana. Les aspects relevant du droit sur la protection des données ont pu être réglés. Plusieurs questions relatives à la sécurité de l'information sont toutefois encore ouvertes.

- Au cours de l'année écoulée, le Bureau a émis plusieurs prises de position sur le SIC des Services psychiatriques universitaires de Berne (SPU). Des séances ont en outre été organisées avec les personnes responsables. Les questions relatives à l'attribution des droits d'accès selon les mandats, pour les fonctions transversales, à la mise au net de la matrice des droits d'accès et des rôles ainsi qu'à la recherche de patients ne sont pas encore réglées.

- Le contrôle préalable du système d'information de laboratoire (SIL) du Centre psychiatrique de Münsingen (CPM) a pu être achevé, quelques questions relevant de la protection de base restant toutefois encore en suspens.

- S'agissant du système d'informations cliniques des Services psychiatriques Jura bernois – Bienne – Seeland (SPJBB), les documents SIPD ont été déposés. Le Bureau a ensuite émis une première prise de position. Une deuxième prise de position suivra dans peu de temps.

- Concernant l'application de gestion administrative des patients OPALE des SPJBB, le Bureau a reçu à la fin de 2014 la confirmation que les comptes de groupe ont été remplacés par des comptes individuels, ce qui a permis d'achever le contrôle préalable.

- L'application de gestion administrative des patients OPALE des SPU ne disposait pas d'une fonction d'effacement. Une telle fonctionnalité ayant été créée, le Bureau a pu achever le contrôle préalable.

- S'agissant du système d'informations cliniques DEP de l'Hôpital de l'Ile, la solution trouvée, qui respecte les prescriptions en matière de protection des données pour ce qui est des champs de recherche et de la distinction entre dossiers activés et dossiers désactivés, n'a pas encore pu être introduite du fait de l'apparition de nouveaux problèmes d'application. Une stratégie d'archivage et de radiation a été soumise au Bureau en 2014. Elle n'est toutefois pas suffisamment détaillée; elle ne donne en particulier aucune information sur la manière dont sera géré l'important volume de données accumulées en raison du grand nombre de cas traités chaque année (prolongation de la durée de conservation des documents relatifs à des traitements antérieurs en cas de réadmission du patient).

- Le Bureau a émis une prise de position relative au dossier SIPD révisé ainsi qu'à la stratégie en matière de conservation et de radiation que lui a soumis le CHR Frutigen Meiringen Interlaken (FMI AG) pour son SIC (PROKIS). Les FMI AG ont pris du retard dans les améliorations devant être apportées.

- De nombreux échanges ont eu lieu au cours de l'année écoulée avec le Centre psychiatrique de Münsingen (CPM) concernant son système d'informations cliniques (ORBIS). Le concept SIPD remanié a été déposé au printemps 2014, à la suite de quoi le Bureau a émis une prise de position. Le concept révisé a ensuite été soumis au Bureau, qui doit à nouveau l'examiner. Il s'agira notamment de vérifier si une fonction d'effacement conforme au droit sur la protection des données a été créée comme cela avait été demandé et peut être mise en œuvre.

- Terminaux multimédia pour patients des FMI AG: ce projet met différentes fonctionnalités à la disposition des patients, qui peuvent notamment accéder à Internet et à la télévision ainsi qu'allumer ou éteindre la lumière à distance. Aucune donnée du patient n'apparaît dans le terminal. Un contrôle préalable a été effectué et a pu être achevé.

- Gestion des données des utilisateurs (Identity Management) des FMI AG: la technologie introduite permet de soutenir les processus relatifs à la gestion des comptes utilisateurs et des droits. Ce projet pourrait être appliqué à d'autres cas similaires, puisqu'il permet d'éviter des risques critiques au moment de l'attribution et du retrait des droits d'accès ainsi que de gérer les droits d'accès aux applications de manière standardisée et d'exercer une surveillance de manière centralisée.

- Il a été procédé à un examen sommaire de l'application ZAPSAP de la Direction des travaux publics, des transports et de l'énergie, qui est utilisée pour la gestion des coûts de construction, la gestion du temps et des mandats ainsi que la gestion commerciale de biens immobiliers. Une séance avec les personnes responsables a en outre eu lieu. L'examen des aspects relevant du droit sur la protection des données a pu être achevé en 2014. Certaines questions relatives à la protection de base ne sont toutefois pas encore réglées (cf. ch. 1.1).

- Le système d'administration des étudiants Studitracker de l'Université de Berne a fait l'objet d'un contrôle préalable abrégé. Le Bureau avait déjà vérifié la protection de base

dans le cadre de l'examen des services informatiques de base fournis par les services centraux.

- S'agissant du logiciel pour l'examen et le versement de prestations individuelles par l'Office des personnes âgées et handicapées (ZERO), les personnes responsables ont soumis une première proposition relative à l'effacement des données. Les questions posées par le Bureau à la suite de cette proposition restaient sans réponse à la fin de 2014.

- Projet BE-Print: le projet d'infrastructure BE-Print prévoit de remplacer l'infrastructure actuelle des imprimantes par des appareils multifonctions reliés à des réseaux de communication. Le concept SIPD qui a été présenté ne tenait pas compte du traitement de données personnelles au moyen de cette infrastructure. Il a été refusé par le Bureau (cf. ch. 1.1).

- HarmTel: le concept SIPD relatif à l'harmonisation de la téléphonie et à l'introduction de Microsoft Lync qui a été soumis au Bureau présente, du point de vue de celui-ci, d'importantes lacunes. L'utilisation de terminaux mobiles n'a par exemple pas été prise en considération, malgré la tendance actuelle et irréversible de «consumérisation» des technologies de l'information. Les questions de savoir si le statut de présence peut, dans certaines configurations, entraîner une surveillance des collaborateurs qui n'est pas admissible et comment traiter les données secondaires ainsi produites n'ont pas été suffisamment étudiées.

- DMS OSIV: le contrôle préalable du système de gestion des documents de l'assurance-invalidité de Berne a été achevé.

- PTC 2010: pour garantir la sécurité de la configuration des clients, un concept SIPD est indispensable. Or, la majorité des Directions ne disposent pas d'un tel concept. La Direction des finances met le sien à la disposition des Directions intéressées (cf. ch. 1.1).

- AMA-Nesko de l'Intendance des impôts: il n'a pas été possible d'établir clairement de quelle manière les exigences SIPD sont mises en œuvre par les partenaires externes; le même problème avait déjà été rencontré dans le cadre d'autres contrôles préalables en relation avec Nesko. L'Intendance des impôts commande des prestations à l'OIO et non pas directement au prestataire de services. Le Bureau demande que la transparence soit assurée (cf. ch. 1.1).

- Le remaniement des concepts SIPD du système cantonal d'informations financières (FIS) et du système d'informations sur le personnel (PERSISKA) n'est pas encore terminé.

- L'examen du portail BE-Login a entraîné quelques adaptations: les exigences en matière de mot de passe ont notamment été relevées (longueur, fréquence du changement, etc.). En outre, il convient de vérifier, avant l'intégration d'applications spécialisées, que les services tiers garantissent la sécurité des données au moyen de leur propre service d'identification ou d'enregistrement (cf. ch. 1.1).

- Un nouvel outil d'analyse web, «Adobe Analytics», est introduit pour permettre de procéder à l'évaluation statistique des sites Internet du canton. Les données des utilisateurs saisies au moment de l'accès à un site seront immédiatement anonymisées grâce à des mesures techniques. Les utilisateurs sont informés au sujet de l'évaluation statistique et peuvent mettre un terme à la saisie de leurs données. Puisque c'est à Londres que des tiers procèdent à l'évaluation des données collectées, les aspects relevant du droit sur la protection des données doivent être réglés dans un contrat d'externalisation, lequel doit inclure les CG SIPD du canton de Berne. Le contrat doit encore être soumis au Bureau.

- Le contrôle préalable relatif au système d'analyse des crimes violents devant servir à l'identification des criminels en série de la police a pu être achevé en 2013. L'autorisation d'exploiter, qui doit être délivrée par le Conseil-exécutif, n'est toutefois pas encore disponible.

En raison du manque de ressources, le Bureau n'a à nouveau pas pu rattraper le retard considérable qu'il a pris dans les procédures de contrôle préalable en cours. Il est en revanche parvenu à traiter la majorité des nouveaux projets qui lui ont été soumis dans un délai approprié.

(S'agissant des installations de vidéosurveillance également soumises à un contrôle préalable, cf. ch. 4; s'agissant de la proposition motivée formulée dans le cadre de la procédure préalable relative à la procédure de conservation et d'effacement pour un système d'informations cliniques, cf. ch. 8.1).

6 Avis exprimés, pratique

Les éléments suivants donnent une idée des nombreuses demandes adressées au Bureau:

- L'utilisation de moyens de communication privés, combinée au recours à des applications informatiques librement disponibles pour la sauvegarde, la synchronisation et le traitement de données, conduit, par exemple dans les écoles, à un mélange des données privées et professionnelles. En outre, il existe un risque que, au moment de la synchronisation d'appareils privés au moyen de services publics (Public Cloud) comme iCloud ou Skydrive, des données pro-

fessionnelles soient transférées par accident. Le Conseil fédéral estime, dans ses directives concernant la sécurité des TIC dans l'administration fédérale, qu'aucune donnée particulièrement digne de protection ne doit être enregistrée sur un terminal mobile privé. Cela n'est admissible que sur des terminaux conçus ou configurés pour la communication mobile cryptée.

- Le feedback au supérieur ou à la supérieure hiérarchique, dans le formulaire d'entretien d'évaluation périodique (EEP), ne fait pas partie de l'évaluation des performances et du comportement. Il relève du domaine personnel confidentiel et sert au développement de la qualité. C'est pourquoi il a sa place dans le dossier conservé par le supérieur ou la supérieure hiérarchique. L'Office du personnel adaptera le formulaire d'EEP à moyen terme de telle sorte que ce feedback ne soit plus automatiquement repris dans le dossier administratif personnel.

- Les entretiens de conseil du Service de consultation de l'Office du personnel (SCPers) sont soumis au secret de fonction. Les informations relatives à des addictions, par exemple, doivent être tenues confidentielles. Elles font parties des données personnelles particulièrement dignes de protection et ne peuvent être transmises que si une base légale l'autorise explicitement. Du fait qu'aucune base légale ne le prévoit, les collaborateurs du SCPers ne peuvent transmettre de telles informations aux supérieurs hiérarchiques sans le consentement libre et explicite de la personne concernée.

- Les communes ne peuvent publier des statistiques fiscales que pour autant qu'il ne soit pas possible d'établir des liens avec des personnes déterminées. Pour les petites communes, il convient d'examiner si cette condition peut être remplie par exemple en regroupant les données de plusieurs communes ou les catégories de revenus.

- Différentes demandes portaient sur l'admissibilité de contrats d'externalisation. En principe, les autorités du canton de Berne peuvent confier le traitement de données à des tiers si cette possibilité n'est pas exclue et si la sécurité des données peut être garantie dans le contrat par l'énoncé des conditions générales SIPD du canton (CG SIPD). Le mandataire est soumis à la loi sur la protection des données et doit prendre toutes les mesures techniques et organisationnelles nécessaires pour garantir la sécurité des données. En cas d'externalisation du traitement des données à l'étranger, il convient de satisfaire à des exigences supplémentaires ainsi que de respecter les limites définies par la loi sur la protection des données.

- Il n'est pas question, pour un groupe de travail cantonal, d'utiliser le chat XING. En effet, avec XING, des données sont traitées à l'étranger par des tiers. Les prescriptions de la loi sur la protection des données, notamment pour ce qui concerne la confidentialité et la disponibilité des données ainsi que la communication à l'étranger, doivent être respectées. Les exigences en matière de sécurité devant être remplies varient en fonction du type de données et du besoin de protection. Il convient de garantir que les droits de la protection des données, notamment l'accès à ses propres données ainsi que la possibilité de demander leur rectification et leur effacement, soient respectés (for suisse). XING fait valoir que les données des membres sont uniquement sauvegardées en Allemagne et que les flux de données sont sécurisés au moyen d'un cryptage SSL. Il précise qu'un contrat a été signé avec le prestataire Akamai (Etats-Unis) concernant le traitement des données, lequel respecte notamment les prescriptions de l'UE. Ces déclarations ne peuvent toutefois pas être vérifiées. La conformité au droit cantonal sur la protection des données et les endroits où les données sont traitées ne peuvent pas être établis avec certitude.

- Une institution privée qui accomplit des tâches conformément à la législation sur l'aide sociale ne peut pas stocker ses données dans le nuage Wuala. Il est vrai que ce service remplit en partie les prescriptions en matière de protection des données pour les services d'informatique en nuage (cloud computing). Toutefois, pour que son utilisation soit admissible, des droits de contrôle du mandant, notamment, devraient être ancrés dans les conditions générales ainsi que dans la directive en matière de protection des données. En outre, Wuala refuse, dans une large mesure, d'assumer les responsabilités. L'utilisation de l'anglais comme langue de procédure vient encore compliquer la mise en œuvre du droit. Enfin, il faut mentionner que Wuala crypte les données, mais que le prestataire dispose, dans certaines circonstances, des clés de cryptage, en tout cas temporairement.

7 Législation

7.1 Législation fédérale

PRIVATIM ne prend plus que sporadiquement position sur des actes législatifs fédéraux. Si l'association l'a fait ou a répercuté des prises de position de ses membres, le Bureau se rallie à l'avis exprimé, à moins qu'il y ait lieu de tenir compte de spécificités bernoises (cf. ch. 2.1). PRIVATIM a publié une prise de position sur la loi fédérale sur la sécurité de l'information. S'agissant de la modification de la loi fédérale sur les étrangers ainsi que d'autres actes légi-

slatifs relatifs au droit des étrangers, PRIVATIM a renoncé à prendre position.

7.2 Législation cantonale

La révision de la loi sur le marché du travail crée les bases légales nécessaires pour le traitement et l'échange de données personnelles particulièrement dignes de protection dans le cadre de la collaboration interinstitutionnelle (CII). Des précisions relatives aux autorités autorisées et au traitement des données ont été introduites dans la loi révisée.

L'accès, pour une APEA, aux données des autres autorités de protection de l'enfant et de l'adulte nécessite une base légale. La révision de la loi sur la protection d'enfant et de l'adulte tient compte de la constatation formulée par le Bureau à ce sujet dans le cadre du contrôle préalable du système de gestion des affaires. Elle crée aussi une base légale pour l'organisation de séances de réseau. Une modification indirecte de la loi sur la protection des données précise qu'il n'est désormais plus possible de prévoir, dans les règlements communaux, que le contrôle des habitants fournisse des renseignements sur la capacité civile.

Plusieurs prises de position ont porté sur les compléments apportés à l'ordonnance sur l'harmonisation des registres officiels. Pour des raisons organisationnelles, les droits d'accès à la gestion centrale des personnes (GCP) doivent notamment être remplacés par des droits d'accès à GERES. La plateforme GERES rassemble toutes les données contenues dans les registres du contrôle des habitants des communes. Le Bureau a ainsi eu une occasion de vérifier la nécessité des droits d'accès existants.

Dans le cadre de la révision partielle de l'ordonnance sur le personnel, l'ordonnance sur la communication de données personnelles a aussi été modifiée. Le Bureau a exprimé son avis à deux reprises. Il a suggéré de continuer à limiter le champ d'application à la communication de données personnelles à l'aide de moyens électroniques, à savoir à la procédure d'appel (en particulier par l'intermédiaire d'Internet ou d'intranet). La publication d'images dans la presse écrite est déjà réglée par la base légale relative à l'accomplissement des tâches de l'autorité. S'agissant de l'accord tacite, le Bureau a toutefois précisé qu'il peut être suffisant dans certains cas. En règle générale, la personne concernée doit toutefois donner son accord exprès. C'est la seule manière de garantir qu'elle a conscience de l'étendue de la communication et qu'elle sait qu'elle a la possibilité de la refuser.

L'ordonnance de Direction sur la gestion et l'archivage des documents des collectivités de droit public et de leurs établissements remplace la directive de l'Office des affaires communales et de l'organisation du territoire jusque-là en vigueur. Le Bureau a demandé que des délais de conservation proportionnés soient fixés. Il n'a pas toujours eu gain de cause. Il faut s'attendre à ce que des adaptations soient régulièrement rendues nécessaires en raison notamment de modifications intervenues dans le droit supérieur.

8 Surveillance et décisions de justice

8.1 Stratégie d'un hôpital en matière de conservation et de radiation

Dans le cadre du contrôle préalable de son système d'informations cliniques, un hôpital a soumis au Bureau une stratégie de conservation et de radiation. Celle-ci prévoyait que le délai de conservation des documents relatifs aux traitements passés soit prolongé à chaque nouveau traitement. L'hôpital justifiait cette façon de procéder notamment par le fait que le dossier d'un patient constitue un tout et que chaque décision médicale se fonde sur les traitements plus anciens. Selon lui, le traitement d'un patient n'est achevé que lorsque celui-ci ne se rend plus à l'hôpital et donc lorsque le dernier traitement est terminé. Par conséquent, le délai de conservation ne commence à courir qu'à la fin du dernier traitement.
Le Bureau a formulé une recommandation motivée, dans laquelle il constatait que la procédure prévue n'était pas conforme aux prescriptions de la législation sur la protection des données. Un délai de conservation doit être fixé pour chaque cas médical (traitement); celui-ci court, par conséquent, de manière différenciée pour chaque cas. S'il existe un lien médical, le délai de conservation d'un document lié à un traitement plus ancien qui n'a pas encore été supprimé peut être prolongé. Pour certains services spécialisés, l'on peut supposer l'existence d'un lien médical entre des cas anciens et nouveaux traités au sein du même service. Dans les autres cas, il incombe au professionnel de la santé qui s'occupe du cas actuel d'évaluer s'il existe un lien médical ou non.

8.2 Destruction et archivage de données personnelles

Le Tribunal administratif a communiqué à l'INS, à titre informatif, un jugement relatif à un échec de l'examen d'avocat qui n'avait pas été anonymisé (connaissance de la jurisprudence dans le domaine de la formation / des examens). La personne concernée a par la suite exigé de l'INS qu'elle supprime toutes les données personnelles traitées suite à la communication de

ce jugement. Elle a en outre demandé que tout le dossier relatif à sa demande de destruction des données soit éliminé après la fin de la procédure.
Le Tribunal administratif, qui a été saisi, estime que la communication d'un jugement non anonymisé aurait nécessité une base légale et qu'elle était donc contraire au droit. Selon lui, le traitement des données effectué par l'INS dans le cadre de la procédure qui a suivi était conforme au droit, mais il résultait directement du traitement illicite des données effectué par le Tribunal administratif. Du fait que la loi sur la protection des données prévoit aussi un droit à l'élimination des effets d'un traitement illicite, la conservation et l'archivage de dossiers relatifs à une demande de suppression sont limités. Les prescriptions en matière d'archivage ne s'appliquent pas et le dossier doit être éliminé.

8.3 Notes incorrectes dans un système informatique

L'École professionnelle industrielle et artisanale de Berne (GIBB) a modifié les notes de plusieurs années d'une personne, alors qu'elles étaient entrées en force, sans avoir introduit une procédure formelle de révision. Ces modifications signifiaient, pour la personne concernée, qu'elle avait échoué à l'examen de fin d'apprentissage. La GIBB a expliqué que des problèmes techniques avec le logiciel d'application Evento sont à l'origine de ces notes incorrectes. Le Tribunal administratif, qui a été saisi par la personne concernée, a observé que les notes, une fois entrées en force, ont un caractère contraignant et qu'elles ne peuvent être modifiées qu'au moyen d'une procédure de révision. Il a souligné en outre que l'ouverture d'une telle procédure nécessite l'existence de justes motifs – dans le cas présent, la découverte a posteriori de faits ou de preuves importants. Il a souligné que les problèmes liés à Evento, avec pour résultat des notes incorrectes, étaient déjà connus au moment de la première remise des notes. Selon lui, l'école n'aurait par conséquent pas dû s'attendre à ce que les notes s'affichent de manière correcte dans les bulletins. Elle aurait dû demander aux enseignants de vérifier que les notes (au moins celles se trouvant en dessous de la moyenne) correspondaient à ce qui figurait dans Evento – un effort jugé acceptable par le Tribunal administratif. Celui-ci a ainsi rejeté l'existence de motifs valables ainsi que la possibilité de revenir sur les notes déjà notifiées et entrées en force.

9 Collectivités de droit communal

- L'année dernière, le Bureau avait informé toutes les autorités communales de surveillance que le contrat relatif à l'utilisation de Microsoft Office 365 dans les écoles ne respectait pas les prescriptions en matière de protection des données et ne devait pas être signé. Des négociations avec Microsoft ont permis à PRIVATIM d'obtenir une nouvelle version du contrat, qui est désormais conforme à la législation sur la protection des données (il remplit un classeur fédéral et est en partie en anglais). Les autorités communales de surveillance en ont été informées.
- La Direction de la justice, des affaires communales et des affaires ecclésiastiques indique aux communes, dans une nouvelle directive ISCB, quelles appartenances religieuses elles doivent inscrire dans le registre du contrôle des habitants et avec quel code. Il est ainsi possible de prendre des mesures contre les inscriptions fautives qui ont été constatées l'année dernière.
- Le Bureau a participé aux cours organisés à l'intention des collaborateurs des communes. L'un des cours a été donné en français. (Concernant le remplacement de la directive sur l'archivage, cf. ch. 7.2).

10 Cas particulier

10.1 Google Street View

Un arrêt du Tribunal fédéral oblige Google, pour son produit Street View, à procéder à l'anonymisation complète des prises de vues à proximité des établissements sensibles, et notamment à flouter tous les visages des personnes et toutes les plaques d'immatriculation. Selon ce jugement, les moyens nécessaires à l'anonymisation manuelle ne sont pas disproportionnés, compte tenu des intérêts de la protection de la personnalité qui sont en jeu. Pour le canton de Berne, Google a soumis à la Chancellerie d'Etat une liste de 39 pages, en précisant à cette dernière qu'elle pouvait demander les compléments nécessaires, le cas échéant, dans un délai d'un mois. La liste n'a pas été établie soigneusement. Manifestement, Google s'est contenté d'effectuer une recherche, selon certains critères, dans un registre d'adresses ou de numéros de téléphone. L'entreprise n'a pas pris en compte les services sociaux et les autorités tutélaires (aujourd'hui autorités de protection de l'enfant et de l'adulte), contrairement à ce que prescrivait le Tribunal fédéral. En outre, il semble même peu probable que Google ait, une fois la liste établie, procédé à un contrôle. Cela explique par exemple que Google ait proposé de considérer les crèches et garderies contenues dans le répertoire comme des établissements sensibles, mais ait aussi inclus dans la liste les adresses de toutes les personnes dont le nom se rapprochait du nom de ces établissements. En procédant de la sorte, l'entreprise a cherché à minimiser les moyens engagés pour garantir les droits de la personna-

lité des personnes concernées et à faire en sorte que ce soit le canton qui doive en assumer les coûts. Cela va à l'encontre du jugement du Tribunal fédéral et le canton a refusé de collaborer.

11 Points abordés dans le rapport précédent

(3: suivi des contrôles préalables effectués en 2013, 5: contrôles préalables effectués, 7.2: base légale créée pour la publication de photographies sur Internet sur la base du mémento du Bureau, 8.1: proposition motivée dans la procédure de contrôle préalable relative à la conservation de données dans un système d'informations cliniques; 9: directive ISCB relative à l'inscription de l'appartenance religieuse).

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.

30 janvier 2015

Le délégué à la protection des données: *Siegenthaler*

13 Annexe

13.1 Abréviations et désignations

A: annexe
Adobe Analytics: outil destiné aux prestataires gérant des sites Internet qui établit des statistiques sur le nombre de visites, la région dans laquelle sont domiciliés les visiteurs ainsi que les contenus consultés.
CG SIPS: conditions générales relatives à la sécurité informatique et à la protection des données définies par l'OIO à l'intention des prestataires externes
Akamai: société dont le siège se trouve à Cambridge (Massachusetts, USA) et qui compte parmi les plus grands fournisseurs d'applications et de contenus en ligne (mise à disposition et accélération) (d'après Wikipédia)
AMA-Nesko: remplacement prévu de l'ordinateur central (système du gros calculateur)
Apple: entreprise américaine dont le siège principal se trouve à Cupertino (Californie, USA) et qui fabrique des ordinateurs et des produits électroniques de divertissement ainsi que des systèmes d'exploitation et des logiciels (d'après Wikipédia)
SCPers: Service de consultation de l'Office du personnel (service de conseil et de renseignement destiné aux agents et aux dirigeants de l'administration cantonale)
BE-Login: portail cantonal d'entrée pour accéder aux services électroniques
ISCB: Information systématique des communes bernoises
CAS (Certificate of Advanced Studies): filière de formation continue
Nuage: méthode ou ensemble de processus qui consiste à mettre à disposition des infrastructures informatiques dématérialisées (p. ex. puissance de calcul, stockage de données, capacités de réseau ou logiciels prêts à l'emploi) adaptées aux besoins de manière dynamique et à travers un réseau (d'après Wikipédia)
DMS: système de gestion des documents
PFPDT: préposé fédéral à la protection des données et à la transparence
INS: Direction de l'instruction publique
FAQ: foire aux questions
FIS: système d'informations financières
FMI AG: hôpitaux de Frutigen, Meiringen et Interlaken
SAP: Direction de la santé publique et de la prévoyance sociale
GERES: solution informatique pour la gestion et l'harmonisation de données personnelles, utilisée, dans le canton de Berne, pour la synthèse de toutes les données des registres du contrôle des habitants
GIBB: école professionnelle industrielle et artisanale de Berne
Google StreetView: complément au service de cartes Google Maps et au logiciel de modélisation géographique Google Earth, qui fournit sur Internet des vues des rues à 360 degrés (d'après Wikipédia)
iCloud: service d'informatique en nuage (cloud computing) offert par Apple
TIC: technologies de l'information et de la communication
SI: services d'informatique
CII: collaboration interinstitutionnelle
DEP: dossier électronique du patient (système d'informations cliniques de l'Hôpital de l'Ile)
ISO: Organisation internationale de normalisation
ISO 2700x: suite ou famille de standards comprenant les normes de sécurité de l'information (d'après Wikipédia)
TI: technologies de l'information
SIPD: sûreté de l'information et protection des données
AI: assurance-invalidité
OIO: Office d'informatique et d'organisation
SIC: système(s) d'informations cliniques
Consumérisation: tendance selon laquelle les collaborateurs amènent leurs terminaux mobiles privés sur leur lieu de travail et veulent en faire un usage professionnel (d'après Wikipédia)
SIL: système d'information de laboratoire
EEP: entretien d'évaluation périodique
MC-SIS (Multi Cancer Screening Information System): logiciel actuellement utilisé pour les programmes de dépistage du cancer du sein
MDM (Mobile Device Management): gestion de terminaux mobiles (GTM)
Microsoft Lync: application de Microsoft qui réunit en un seul environnement différents moyens de communication (notamment téléphonie IP, vidéoconférence et messagerie vocale). Tous les utilisateurs disposent d'informations sur la disponibilité des autres participants (présence, inactivité, durant un certain temps, du clavier et de la souris)
Microsoft Office 365: offre incluant les logiciels Office habituels ainsi que d'autres services Internet (notamment le stockage en ligne et l'offre minutes Skype) sous la forme d'un abonnement mensuel ou annuel (ce qui permet de les utiliser depuis différents appareils)
Objectifs NOG: dans le cadre de la Nouvelle gestion publique, des objectifs de prestation et d'effet doivent être fixés pour chaque unité administrative (ces objectifs sont mentionnés dans le budget ainsi que dans le rapport de gestion du canton de Berne)
NESKO: système informatique de l'Intendance des impôts, servant à la taxation et à la perception
NICER (National Institute for Cancer Epidemiology and Registration): Institut national pour l'épidémiologie et l'enregistrement du cancer

OPALE: application de gestion administrative des patients
OSIV: système d'information Open System IV, application informatique utilisée par plusieurs offices AI
PERSISKA: système d'information sur le personnel du canton de Berne
PRIVATIM: association des Commissaires suisses à la protection des données
CPM: Centre psychiatrique de Münsingen
ORP: office régional de placement
Cf.: confer (voir)
SIS (Système d'information Schengen): système des Etats Schengen grâce auquel les données d'objets ou de personnes recherchés peuvent être notifiées et interrogées très rapidement dans tout l'espace Schengen
SkyDrive: service de stockage de données en ligne de Microsoft (aujourd'hui OneDrive)
SPJBB: Services psychiatriques Jura bernois – Bienne – Seeland à Bellelay
SSL (Secure Sockets Layer): ancienne dénomination pour Transport Layer Security, un protocole de sécurisation des transferts de données sur Internet (d'après Wikipédia)
CHB: Centre hospitalier Bienne
SPU: Services psychiatriques universitaires
VICLAS (Violent Crime Linkage Analysis System): système d'analyse des crimes violents devant servir à l'identification des criminels en série
Wuala: prestataire suisse de services informatiques en nuage permettant de stocker, de manière centralisée, des données sur les serveurs européens de la société LaCie AG (qui est majoritairement états-unienne)
XING: réseau social dont les membres peuvent en priorité gérer leurs relations professionnelles et/ou privées avec d'autres personnes et entrer en contact avec de nouvelles personnes
ZAPSAP: application de la TTE utilisée pour la gestion des coûts de construction, la gestion des mandats et du temps ainsi que la gestion commerciale des biens immobiliers
ZERO: programme introduit pour l'examen et le versement de prestations individuelles par l'Office des personnes âgées et handicapées de la SAP
GCP (gestion centrale des personnes): banque de données de l'Intendance des impôts contenant des informations sur les personnes physiques et morales

13.2 Numéros de référence des décisions de justice mentionnées au chiffre 8

8.1: Proposition motivée du Bureau 42.72-13.5952 du 19 juin 2014
8.2: Jugement du Tribunal administratif JTA 100.2013.156 du 15 avril 2014
8.3: Jugement du Tribunal administratif JTA 100.2014.99U du 13 octobre 2014

13.3 Sitographie

2.3: Rapport de gestion: http://www.fin.be.ch/fin/fr/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html
9: Communications aux autorités communales de surveillance: http://www.jgk.be.ch/jgk/fr/index/aufsicht/datenschutz/kommunaler_datenschutz/mitteilungenetc.html