Rapport d'activité 2015 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	4
4.	Vidéosurveillance	4
5.	Contrôle préalable de projets informatiques	5
6.	Avis exprimés, pratique	8
7.	Législation	9
8.	Surveillance et décisions de justice	10
9.	Police	11
10.	Cas particulier	12
11.	Points abordés dans le rapport précédent	13
12.	Proposition	13
13.	Annexe	13

1 Introduction

1.1 2015 en bref

Comme le révèlent les projets BE-Print (infrastructure d'impression, de numérisation et de photocopie à disposition dans toute l'administration) et HarmTel (remplacement des appareils de téléphonie par des solutions de communication intégrées au poste de travail informatique), des systèmes intégrés remplacent les solutions individuelles (cf. ch. 5).
Or l'intégration technique de ces systèmes complique les interactions entre les bénéficiaires et les fournisseurs des prestations. La communication doit en particulier être améliorée, surtout lorsque le système change, comme le montrent les exemples suivants: le service d'informatique d'une Direction a suspendu les mesures techniques permettant l'application des directives en matière de mot de passe. Le système ainsi configuré a été confié au fournisseur des services informatiques de base. Il a ensuite fallu des mois avant que les bénéficiaires des prestations (responsables des applications) décèlent cette lacune, pourtant importante (cf. ch. 10). Un contrôle de l'application SUSA de l'Office de la circulation routière et de la navigation (OCRN) a révélé un problème similaire: l'application est exploitée dans le centre de calcul de la Bedag. L'instruction concernant la sûreté de l'information et la protection des données, soigneusement mise à jour par l'OCRN, ne lui a toutefois jamais été remise (cf. ch. 3).
De plus en plus de données sont traitées sur des terminaux mobiles tels que téléphones intelligents et tablettes.
L'examen du système de gestion des terminaux mobiles (MDM) de la Police cantonale a révélé qu'il est indispensable de protéger les données d'une manière appropriée sur ces appareils (p. ex. pour ce qui est de l'effacement des données en cas de perte de l'appareil). Toutefois, il a aussi montré que le système utilisé permet d'effectuer des contrôles des terminaux mobiles au moyen desquels les collaborateurs pourraient être surveillés, ce qui est inadmissible (cf. ch. 9.2).
Le Bureau pour la surveillance de la protection des données (le Bureau) a pour mission d'exiger le respect du droit fondamental à la protection des données, même dans un contexte où les moyens informatiques et techniques sont en pleine évolution. Les risques doivent dès lors être réévalués. Il convient de garantir que les données des citoyens sont traitées conformément au droit sur la protection des données. Il s'agit à cet égard de tirer profit des évolutions technologiques (toujours plus de données numériques et de systèmes intégrés). La collaboration avec les mandants doit être renforcée dans le but de trouver des solutions qui soient à la fois sécurisées et agréables pour les utilisateurs. Le Bureau intervient notamment dans le contrôle préalable des projets informatiques. Dans ce cadre, les exigences en matière de sécurité et de protection des données doivent être définies à temps et rigoureusement prises en compte.

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 2015, dont l'une comprenait une visite à l'Office fédéral de la police (fedpol).
- Le Service spécialisé pour handicapés de la vue du canton de Berne (BRSB) accomplit des tâches (liées) financées par le canton et la Confédération. Un échange de vues a révélé que la surveillance de la protection des données incombe dans ce cas au PFPDT (s'agissant de la compétence pour l'Office AI, cf. ch. 8.2).
- Des collaborateurs du Bureau sont membres des groupes de travail «Santé» et «Technologies de l'information et de la communication» de PRIVATIM. Les membres du groupe de travail «Santé» ont effectué une enquête sur le contrôle des factures de prestations stationnaires dans le domaine de l'assurance obligatoire des soins (cf. ch. 13.3; brochures à l'attention des patients, cf. ch. 6).
- PRIVATIM a organisé un cours d'une journée constituant une introduction à la sécurité informatique à l'intention des juristes. Des collaborateurs du Bureau y ont participé.

1.3 Mise en œuvre de l'évaluation sur la base des accords de Schengen

Les commentaires et remarques formulés par le comité d'experts des Etats parties qui a examiné les services du canton de Berne ont été mis en œuvre de la manière suivante:
- L'indépendance du Bureau, ancrée dans la loi sur la protection des données, a été respectée dans le processus d'élaboration du budget 2016: le Conseil-exécutif a notamment renoncé à commenter la création de poste demandée dans le budget.
- La Commission de gestion du Grand Conseil a souligné, dans le cadre de ses débats, qu'elle comprenait l'indépendance du Bureau en ce sens que les décisions prises par ce dernier ne devaient subir d'influence en aucun cas.

- Les accès de la Police cantonale au SIS ont fait l'objet de contrôles en 2015. Ceux-ci ont été effectués par le Commandement de la police, en collaboration avec le Bureau, et sans recourir à des personnes externes. Pour éviter les autocontrôles, qui sont insuffisants, le Bureau a pris part à toutes les étapes importantes de ces contrôles, et a notamment participé à la sélection de l'échantillon des accès devant être examinés. De telles vérifications seront désormais effectuées chaque année.
- Le groupe de coordination Schengen du PFPDT a été informé du fait que le recours à des personnes externes chargées d'effectuer des contrôles nécessite la création d'une base légale et que l'indépendance de ces personnes par rapport aux services contrôlés doit par ailleurs être garantie (cf. ch. 1.2).
- Le Grand Conseil a approuvé l'augmentation de l'effectif du personnel du Bureau (cf. ch. 2.3).
- 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 ont été publiées sur le site Internet du Bureau.

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 ou de conseil 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'a pas à intervenir 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, notamment en cas de cantonalisation, ou si des instances de contrôle estiment qu'une telle augmentation est nécessaire du fait que les tâches ne sont pas accomplies de manière satisfaisante (cf. ch. 1.3).

2.2 Responsabilité propre des services traitant les données

Le Bureau est de plus en plus souvent sollicité pour des exposés. Il a notamment participé à une présentation à l'intention de travailleurs sociaux en milieu scolaire sur les principes fondamentaux du droit de la protection des données et les dispositions régissant les archives, en collaboration avec l'Office des affaires communales et de l'organisation du territoire (OACOT).
- La personne responsable de la protection des données au sein de l'Hôpital de l'Ile a fait, avec une juriste du service juridique, une brève présentation sur la protection des données dans toutes les cliniques (env. 40). Le but de cette démarche était de communiquer aux participants les coordonnées des personnes responsables en cas de question sur la protection des données, d'amener des propositions d'amélioration concrètes et de distribuer des brochures d'information.

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

En 2015, le budget attribuait, pour l'administration cantonale, CHF 32 millions aux investissements dans le domaine informatique et CHF 160 millions à l'exploitation (dont CHF 117 mio destinés à des tiers prestataires de services). Ces chiffres ne concernent pas les hôpitaux ni l'Hôpital de l'Ile, 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 190 000.

En 2015, le Bureau a disposé de 4,7 postes à temps complet (dont 0,7 pour le secrétariat). En raison de l'introduction de la gestion électronique des affaires, il avait déjà en 2014 été renoncé à un poste de secrétariat à 50 pour cent. Entre août et décembre, les ressources disponibles ont permis d'engager une collaboratrice scientifique à 30 pour cent. En raison de la nécessité de former une nouvelle collaboratrice chargée des tâches administratives, le secrétariat a connu une double occupation au mois de décembre (10 % en plus du poste à 20 % qui existait jusque-là). De par l'adoption du budget 2016, le Grand Conseil a autorisé la création d'un nouveau poste à 100 pour cent (collaboratrice scientifique). Les 55 pour cent de poste actuellement disponibles sont compris dans ces 100 pour cent, ce qui signifie que le Bureau dispose, en 2016, de 45 pour cent supplémentaires, soit 5,15 postes à temps complet au total. Le Grand Conseil a décidé une coupe linéaire dans les biens, services et marchandises, dans le budget global. Par conséquent, le montant à disposition pour le contrôle des applications informatiques gérées par des services externes connaît une diminution de CHF 14 000 environ. Des informations complémentaires relatives au budget, aux comptes ainsi qu'aux objectifs de NOG (données financières) sont disponibles dans le rapport de gestion de 2015 du canton de Berne (volume I, cf. ch. 13.3).

3 Contrôle des applications informatiques utilisées

Deux examens (dont l'un portant sur deux services) ont été réalisés en 2015:

- Service d'aide sociale en matière d'asile (SASA) de Bienne et Service cantonal des migrations (SEMI)

L'examen a porté en priorité sur les flux de données entre le SEMI et le SASA.
Le contrôle effectué auprès du SASA par le service de vérification externe a révélé des lacunes importantes pour ce qui est de la protection des données et de la sûreté de l'information. Du point de vue technique, les mesures relatives à la protection de base et à la protection accrue ne sont pas mises en œuvre dans de nombreux domaines. Des données particulièrement dignes de protection sont souvent échangées avec des institutions partenaires sans que les mesures nécessaires ne soient prises (cf. ch. 8.1). Du point de vue organisationnel, le SASA ne dispose pas de prescriptions ni directives claires en matière de classification, d'effacement et d'archivage. Il n'a en outre pas défini un cadre qui permette de passer des contrats suffisamment précis avec les partenaires externes.
Le SEMI traite ses données (décomptes avec les services fédéraux) notamment au moyen de l'application Asydata. Cette application, qui a été mise en service en 2000, ne répond pas aux exigences actuelles en matière de sûreté de l'information et de protection des données. Du fait que des exigences de sécurité élémentaires ne sont pas respectées, des mesures urgentes doivent être prises. L'application contrôle un processus jouant un rôle important pour les affaires. Or, dans son état actuel, elle présente un risque considérable pour le SEMI.

- Application SUSA de l'Office de la circulation routière et de la navigation (exploitée par la Bedag)

Le contrôle a été effectué pour la première fois en collaboration avec le Contrôle des finances du canton de Berne. Le service de vérification externe avait pour mission d'examiner l'exploitation de l'application dans le centre de calcul de la Bedag, et en particulier la manière dont le mandataire et propriétaire des données a transmis les exigences en matière de sûreté de l'information et de protection des données au partenaire externe et comment il veille au respect de ces exigences.
Les responsables de la Bedag ont apporté un soutien constructif aux personnes chargées de l'examen et fourni des informations détaillées sur l'exploitation de l'application. Il a ainsi été constaté que, d'un point de vue technique, la protection de base atteint un très bon niveau. La Bedag exploite ses installations selon ses propres directives, qui se fondent sur la norme ISO 2700x. Les critères permettant d'examiner la maturité et la durabilité des mesures mises en œuvre doivent encore être définis.
Le mandataire doit en principe fixer de manière contraignante dans le contrat des exigences en matière de sûreté de l'information et de protection des données et veiller à ce que ces exigences soient respectées. De ce point de vue, la situation actuelle n'est pas satisfaisante. Il est vrai qu'il existe un concept SIPD pour l'application SUSA, lequel décrit les exigences en matière de sécurité. Ce document n'a toutefois jamais été communiqué à la Bedag, malgré le fait que le contrat le prévoie.

- Suivi des contrôles effectués en 2014
  - Audit de l'infrastructure mobile (téléphones intelligents) de la Police cantonale

Cf. ch. 9.2.

  - Hôpital de Thoune (STS AG)

Suite à l'audit du système d'informations cliniques, la sûreté de l'information et la protection des données ont été intégrées au système de gestion des risques, qui est utilisé pour toute l'institution. La direction a octroyé des ressources dans ce but, et a remanié et optimisé les processus. L'audit est achevé.

  - Centre hospitalier Bienne (CHB)

Les questions qui ne sont pas encore réglées doivent l'être d'ici le milieu de 2016.

4 Vidéosurveillance

Plusieurs installations de vidéosurveillance de bâtiments cantonaux ont été examinées dans le cadre d'une procédure de contrôle préalable, notamment celles des établissements de Thorberg, du complexe des hautes écoles VonRoll de l'Université de Berne et des gymnases de la région Bienne – Seeland.

- Les visites effectuées sur place ont souvent conduit à des adaptations des demandes d'octroi d'une autorisation adressées au Commandement de la police. A plusieurs reprises, des caméras ne pouvant pas faire l'objet d'une autorisation ont été supprimées du projet et des mesures visant à garantir la protection des données y ont été intégrées lorsque cela était nécessaire. S'agissant du complexe des hautes écoles, il a notamment été renoncé aux caméras permettant de filmer des périmètres situés sur l'espace public et, pour les établissements de Thorberg, à celles permettant de surveiller les espaces où se déroulent les visites. Concernant les établissements de l'Office de la privation de liberté et des mesures d'encadrement, une nouvelle directive règle l'utilisation des caméras dans les cellules de sécurité et un mé-

mento relatif à la vidéosurveillance dans les établissements traite du respect du principe de la proportionnalité. S'agissant des gymnases de la région de Bienne, des dispositions relatives à la consignation des contrôles techniques des enregistrements vidéo dans un procès-verbal ont été ajoutées aux documents.

- L'Office des ponts et chaussées (OPC) a soumis au Bureau plusieurs questions relatives à la vidéosurveillance de grands chantiers. Dès lors qu'une caméra permet d'identifier des personnes, une autorisation doit être demandée. Tel est notamment le cas lorsque les images vidéo peuvent être consultées sur Internet ou qu'un arrêt sur image ou un agrandissement sont possibles et qu'un numéro de véhicule ou une personne sont reconnaissables ou peuvent être identifiés d'après les circonstances. L'OPC a tenu compte des réserves et des propositions d'amélioration du Bureau.

- Des communes ont demandé à plusieurs reprises ce qu'elles pouvaient entreprendre contre les caméras de personnes privées réalisant des enregistrements vidéo sur l'espace public. La vidéosurveillance non autorisée d'espaces publics par des privés n'est pas admissible. Toutefois, du fait qu'il n'existe pas de bases légales, il convient de rechercher une solution par le dialogue, si nécessaire assorti d'une menace de sanction pénale, en recourant aux moyens prévus par la loi fédérale sur la protection des données (actions civiles, recours au PFPDT).

- La Direction de la police et des affaires militaires (POM) a publié les rapports d'évaluation concernant les installations de vidéosurveillance rédigés par ses offices, dont celui du Commandement de la police (cf. ch. 13.3).

- (S'agissant de la question de la proportionnalité, pour ce qui est de la vidéosurveillance d'institutions dont les collaborateurs sont soumis au secret professionnel: cf. ch. 8.4).

5 Contrôle préalable de projets informatiques

Le Bureau a examiné un grand nombre de projets informatiques, dont beaucoup d'applications utilisées dans le secteur de la santé, en particulier des systèmes d'informations cliniques (SIC). En voici quelques exemples (la liste n'est pas exhaustive):

- S'agissant du système d'informations cliniques de l'Hôpital de l'Ile (DEP), le Bureau a examiné la stratégie d'archivage et de radiation qui lui a été remise. Il a constaté que celle-ci constituait une solution minimale mais qu'elle était suffisante dans la mesure où les dossiers médicaux sont effacés après une durée déterminée. Les délais de conservation légaux minimaux doivent être respectés. Il revient aux professionnels de la santé responsables de décider si le délai de conservation doit être prolongé dans les cas où il existe un lien médical. Le Bureau est quant à lui d'avis que, si un tel lien existe, le délai de conservation de l'ancien dossier médical doit être prolongé, à moins que les informations nécessaires puissent être intégrées d'une autre manière au nouveau dossier. Il ne dispose cependant pas de connaissances médicales et cette décision ne relève pas de sa responsabilité. Les champs de recherche (dossiers actifs et dossiers clos) doivent encore être adaptés pour être conformes aux prescriptions relatives à la protection des données. Le contrôle préalable a ainsi pu être achevé.

- 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), les documents SIPD révisés ont été remis au Bureau. Celui-ci a par conséquent pu émettre une prise de position définitive et mettre fin au contrôle préalable.

- S'agissant du système d'informations cliniques de la Clinique bernoise Montana, plusieurs questions relatives à la sûreté de l'information étaient encore en suspens. La remise des documents SIPD révisés a permis de clarifier ces aspects et le contrôle préalable a ainsi pu être achevé.

- Le Bureau a émis une deuxième prise de position sur le système d'informations cliniques Cariatides des Services psychiatriques du Jura bernois (SPJBB). Du fait que l'organisation des droits d'accès est complexe, une démonstration sur place s'est révélée utile. Celle-ci a montré que quelques modifications étaient nécessaires pour des raisons de proportionnalité. Ces modifications doivent être effectuées et présentées dans les documents SIPD révisés. A la fin de 2015, les SPJBB n'avaient respecté ni le délai initialement prévu ni le délai supplémentaire qui leur avait été octroyé.

- Plusieurs discussions ont eu lieu entre le Bureau et les Services Psychiatriques Universitaires de Berne (SPU) concernant le système d'informations cliniques des SPU. Les questions qui ne sont pas encore réglées ont été abordées, notamment celles de l'attribution des droits d'accès selon les mandats, pour les fonctions transversales, de la matrice des droits d'accès et des rôles ainsi que de la recherche de patients. Concernant l'organisation des droits d'accès, une démonstration a aussi eu lieu sur place. Le Bureau attend des explications com-

plémentaires par écrit au début de 2016, à la suite de quoi il pourra émettre une nouvelle prise de position.

- Dans le cadre du contrôle préalable du système d'information de laboratoire (SIL) du Centre psychiatrique de Münsingen (CPM), certaines questions relatives à la protection de base n'étaient pas encore réglées. Tel est désormais le cas et le contrôle préalable a ainsi pu être achevé.

- L'examen des documents SIPD relatifs à l'application Acuraid (utilisée pour la recherche dans le domaine de l'acuponcture) de l'Institut de médecine complémentaire de l'Université de Berne a révélé que cette application ne peut pas être exploitée de manière conforme aux prescriptions relatives à la protection des données et qu'elle ne doit par conséquent pas être utilisée.

- S'agissant du système d'informations cliniques de l'hôpital régional de l'Emmental (RSE AG), de nombreux échanges ont eu lieu au sujet des droits d'accès. Il a fallu examiner – comme c'est généralement le cas dans le cadre des contrôles préalables – si l'organisation du RSE AG, et plus précisément celle des droits d'accès au SIC, ne faisait qu'exploiter au maximum la marge de manœuvre eu égard à la protection des données ou si elle dépassait les limites admissibles. Dans sa première prise de position, le Bureau a notamment exigé que la fonction de recherche soit limitée et que la recherche de patients VIP soit rendue plus difficile. Une liste de questions relatives à l'examen de la matrice des droits d'accès a en outre été établie et des réponses doivent être apportées.

- Le Bureau a pris du retard dans l'examen des améliorations apportées, à sa demande, au système d'informations cliniques du CHR Frutigen Meiringen Interlaken (FMI AG). Il doit notamment vérifier que, dans la fonction de recherche, les patients en psychiatrie ne sont visibles que pour les psychiatres.

- Après que le Bureau a émis deux prises de position sur le système d'informations cliniques du CPM, deux questions doivent encore être réglées: le fabricant du logiciel a émis une prise de position relative à la procédure de conservation et d'effacement qui doit encore être examinée. Le concept SIPD révisé, auquel doivent être intégrées des informations relatives à la plateforme pour l'échange de données (informations sur les flux de données entre le SIC et cette plateforme, spécification des interfaces), doit quant à lui encore être remis au Bureau.

- Concernant l'hôpital régional de Haute-Argovie (SRO AG), le contrôle préalable a pris du retard en raison d'un changement de personnel et du remplacement du système d'informations cliniques par un autre logiciel. Les documents remaniés soumis au Bureau ne sont pas complets, raison pour laquelle ils ne peuvent pas être examinés pour le moment. Des renseignements sur la sûreté de l'information (qui est insuffisante) font notamment défaut.

- Le Bureau a émis deux prises de position sur le système d'information de laboratoire de l'Institut des maladies infectieuses (IFIK) de l'Université de Berne. Il a suggéré qu'une banque de données de recherche (contenant des données pseudonymisées) soit créée et que les chercheurs n'aient accès qu'à ces informations. Une description détaillée de la gestion des accès doit encore être soumise au Bureau.

- Le contrôle préalable du Case Management Formation professionnelle a pu être achevé. Deux remarques ont toutefois été formulées: l'historique des changements est lié aux données principales et doit par conséquent être conservé aussi longtemps que celles-ci. Les données de la journalisation des accès (lecture) doivent en revanche impérativement être effacées après une année. L'autorité responsable doit en outre veiller à ce que les conditions générales concernant la sûreté de l'information et la protection des données aient été approuvées (signature) et soient respectées.

- Le Bureau a émis une nouvelle prise de position concernant l'application Kernsystem Lehre (KSL) de l'Université de Berne. La stratégie des autorisations a été examinée à la lumière des principes régissant l'octroi des droits et certains rôles (échantillon) ont été analysés. Des précisions doivent encore être apportées à la documentation SIPD relative à l'archivage et à l'effacement des données, qui doit être remise au Bureau.

- Concernant UNICARD, le Bureau attend toujours la preuve de la mise en œuvre des mesures relatives à l'archivage.

- L'examen de la stratégie d'archivage et de radiation du système d'administration des étudiants IS-Academia de la Haute école spécialisée bernoise (HESB), qui a été soigneusement remaniée et contient désormais des délais différenciés, a permis d'achever le contrôle préalable.

- Le Bureau a émis une première prise de position dans le cadre du contrôle préalable du système d'informations financières ESAP de la HESB et de la Haute école pédagogique de Berne (PHBern). Il s'est en particulier intéressé au traitement des données du personnel, qui est délicat du point de vue de la protection des données.

- Après plusieurs demandes de prolongation de délai, l'Office des personnes âgées et handicapées (OPAH) a présenté au Bureau les raisons pour lesquelles les données traitées au moyen du logiciel utilisé pour l'examen et le versement de prestations individuelles (ZERO) doivent toutes être conservées et ne peuvent pas être éliminées progressivement. Il lui a en outre proposé deux variantes d'effacement conformes aux prescriptions de la protection des données. Le contrôle préalable a ainsi pu être achevé.

- S'agissant du nouvel outil d'analyse web Adobe Analytics, le contrat d'externalisation a dû être examiné. Ce contrat concrétise les conditions prévues par la législation sur la protection des données régissant les rapports avec le prestataire étranger (telles que l'application du droit suisse, et plus précisément cantonal, de la protection des données, le for juridique et les possibilités d'audit). La déclaration de protection des données se trouvant sur le site du canton (sous «Mentions légales») a été adaptée. Elle énumère désormais les données qui sont collectées au moment de la consultation du site et qui peuvent être évaluées sous une forme anonyme. Il est en outre possible de désactiver le traçage par Adobe Analytics (option de retrait).

- Le logiciel de ServiceNow sert au traitement des annonces de problème et des demandes des utilisateurs dans le cadre de l'exploitation quotidienne de l'infrastructure informatique du canton. L'application est exploitée dans les centres de calcul du fournisseur. La transmission des données et des caractéristiques d'authentification est codée. L'examen du Bureau a révélé la nécessité de définir les cas dans lesquels ServiceNow ne doit pas être utilisé. Une procédure spécifique permet de veiller à ce qu'aucune donnée particulièrement digne de protection ou pour laquelle il existe une obligation particulière de garder le secret ne soit traitée.

Du fait que le prestataire de services est étranger (entreprise américaine qui a un siège en Europe), le contrat passé avec ServiceNow Pays-Bas a dû faire l'objet d'un examen particulier. Puisque ServiceNow a adhéré à l'accord établissant une sphère de sécurité entre la Suisse et les Etats-Unis (Safe Harbor), le contrat se fonde sur le contrat-type pour l'externalisation du traitement de données à l'étranger élaboré par le PFPDT. L'arrêt rendu en 2015 par la Cour de justice de l'Union européenne a en outre dû être pris en compte dans le cadre de l'examen. Selon cet arrêt, l'accord «Safe Harbor» n'empêche pas les autorités américaines d'accéder aux données d'une manière non conforme au principe de la proportionnalité et ne satisfait par conséquent pas aux exigences de l'Union européenne, selon lesquelles un «niveau de protection adéquat» doit être garanti.

Le PFPDT est parvenu à la conclusion que ces constats s'appliquaient également au «Safe Harbor Framework», passé entre la Suisse et les Etats-Unis, et au niveau de protection des données adéquat en Suisse. D'ici à ce que l'UE ait pu clarifier la situation et obtenir de nouvelles garanties de la part des Etats-Unis, toutes les parties doivent s'engager à ce que les personnes concernées soient informées que les Etats-Unis peuvent avoir accès à leurs données, à ce que des moyens non juridictionnels efficaces soient disponibles et à se soumettre aux jugements le cas échéant.

Conformément au contrat conclu avec ServiceNow Pays-Bas, ServiceNow est notamment tenu au maintien du secret pour toutes les données, qui ne peuvent être traitées que dans des centres de calcul suisses. Le contrat est soumis au droit suisse et un for suisse est constitué. Pour autant que les dispositions contractuelles soient respectées, les données qui ne sont pas sensibles peuvent être traitées de manière conforme à la protection des données.

- Le logiciel FTAPIs de l'entreprise allemande QSC AG offre une plateforme d'échange de données avec un chiffrement bout-à-bout (*end-to-end encryption)* particulièrement sûr. Cette plateforme peut être exploitée par la Bedag. Il est prévu qu'elle soit mise à la disposition des collaborateurs, ainsi que de leurs invités, sur leur place de travail (ordinateurs fixes) ou, en chemin, sur des terminaux mobiles. L'examen du Bureau a révélé que cet outil ne doit, à l'heure actuelle, être utilisé que sur des ordinateurs fixes. En outre, deux conditions doivent être remplies: il convient de prouver que la solution de cryptage est sûre et de trouver des moyens techniques permettant de limiter l'utilisation de la plateforme à des infrastructures fixes. L'utilisation de la plateforme depuis les terminaux mobiles (téléphones intelligents, tablettes, ordinateurs portables, miniportables, etc.) n'est pas admissible pour la raison suivante: il n'est pas encore possible, du point de vue technique, de protéger les données sensibles et notamment de séparer les données privées des données professionnelles.

- S'agissant du service d'impression BE-Print, utilisé dans toute l'administration, le Bureau a déjà émis l'avis que le concept SIPD ne doit pas se contenter de décrire le projet d'infrastructure et porter en priorité sur le remplacement des imprimantes. C'est un nouveau service qui est mis à disposition, dont les possibilités dépassent largement l'impression. Des fonctions telles que l'impression suivie (*follow-me-printing*) et la numérisation (avec envoi vers une adresse

électronique ou un dossier) requièrent une large palette de modules techniques et de mesures organisationnelles qui doivent être harmonisés. Le système devient plus complexe et, par conséquent, les risques augmentent. La disponibilité ne dépend plus seulement d'un terminal, mais d'une chaîne fonctionnelle dont tous les maillons doivent être opérationnels: identification, droits d'accès, transmission, traitement, impression. Le fait que les différentes composantes du système (serveurs, réseaux, système d'identification) sont confiées à différents services et prestataires augmente encore la complexité (cf. ch. 1.1).
A cela s'ajoute le fait que, pour accéder aux fonctions d'impression et de numérisation, des données permettant l'identification doivent être saisies sur l'appareil multifonctions, qui ne dispose pas d'un vrai clavier. Il n'est pas aisé de saisir correctement le mot de passe. Etant donné que, lors de la numérisation, des données particulièrement dignes de protection sont aussi transférées, le cryptage de ces données à partir de l'appareil permettant la numérisation doit être prévu.
L'OIO n'a pas encore soumis au Bureau de concept SIPD relatif à la télécopie.

- Il en va du projet d'harmonisation de la téléphonie (HarmTel) comme du projet BE-Print: il ne s'agit pas simplement de remplacer les téléphones, mais d'investir dans des moyens de communication modernes et complexes. Avec le passage de systèmes analogiques à des systèmes numériques (Voice over IP), l'infrastructure téléphonique intègre le monde numérique. Cela signifie que plusieurs systèmes et plusieurs sources de données constituent ensemble une nouvelle plateforme de communication (outil de collaboration). On passe du téléphone traditionnel à un terminal qui permet d'accéder à toutes les données qui sont disponibles pour l'utilisateur – pas seulement les siennes, mais aussi celles que d'autres collaborateurs ont débloquées.

Plusieurs cycles de travail et des concessions seront nécessaires avant que le Bureau estime que le projet est conforme aux prescriptions de la protection des données. Des conditions claires sont toutefois posées: s'agissant des terminaux mobiles, seul le remplacement des appareils DECT est admis, à l'exclusion de tous les autres systèmes. Il est interdit d'utiliser des terminaux mobiles pour accéder au système de téléphonie tant que ceux-ci ne sont pas protégés au moyen d'un système de gestion (solution EMM) et ne répondent pas aux exigences de la protection des données (projet en cours relatif à la gestion des terminaux mobiles). Pour recevoir un appel par l'intermédiaire de Microsoft Lync / de la plateforme Skype (base de HarmTel), le terminal doit être débloqué, ce qui contrevient aux directives de la protection de base. Si un mot de passe respectant les directives en matière de mot de passe (8 caractères au minimum, dont un caractère spécial, comprenant des majuscules et minuscules) est introduit, débloquer l'appareil devient trop compliqué. Une solution à ce problème est encore recherchée.

Il a en outre fallu garantir que l'indication du statut (présence) ne serait pas utilisée pour surveiller les collaborateurs: ceux-ci peuvent gérer eux-mêmes leur statut et des directives à l'intention des supérieurs relatives à cet instrument sont ancrées dans l'ordonnance sur le personnel.

Avec l'introduction de HarmTel, les données secondaires (qui a communiqué, combien de temps et avec qui) sont soumises au contrôle de l'OIO, mais celui-ci n'en a pas la maîtrise. Si quelqu'un exige qu'on lui livre ces données, par exemple le Ministère public, il ne revient pas à l'OIO de décider mais au propriétaire des données. L'OIO se doit de respecter cette règle vis-à-vis des autres Directions mais surtout vis-à-vis du Grand Conseil et des tribunaux. Les données secondaires ne doivent pas être conservées plus de dix jours (cf. ch. 1.1).

- Le logiciel BVM-Tool est utilisé par l'Office AI pour lutter contre les abus dans le domaine de l'assurance. Conformément au but, des données très sensibles sont traitées au moyen de cet outil. Grâce à l'expérience acquise au cours des précédents contrôles ainsi qu'à la bonne collaboration entre l'Office AI et le Bureau, le contrôle préalable a pu être effectué de manière très efficace.

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.)

6 Avis exprimés, pratique

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

- Les patients ont de nombreux droits en matière de protection des données. Parmi ceux-ci, le droit de consulter et de copier leur dossier est le plus important. De plus, ils peuvent en principe décider qui peut avoir accès à quel contenu de leur dossier. Le Bureau a publié une brochure à ce sujet en 2015. Celle-ci se fonde sur des bases de PRIVATIM (cf. ch. 1.2).

- Le Bureau a constaté que les interactions complexes entre les plateformes pour l'échange de données (qui sont de plus en plus utilisées) ne sont pas suffisamment prises en considération. Il a souligné que les processus (flux de données) de tous les systèmes liés à la plateforme concernée doivent être pris en compte dans la documentation du contrôle préalable afin que l'intégrité des données puisse être garantie.

- Il est délicat de fournir des renseignements par téléphone ou à la réception d'un hôpital à des autorités, car le fait de donner une réponse confirme que la personne concernée est à ce moment en traitement. Or cette information est soumise à l'obligation de garder le secret et la divulguer est passible d'une sanction pénale. Les professionnels de la santé et leurs auxiliaires (p. ex. réceptionnistes) ne peuvent fournir de tels renseignements que si une base légale explicite le prévoit ou si elles ont obtenu le consentement de la personne concernée ou été déliées du secret professionnel par l'Office du médecin cantonal. Le Bureau consent toutefois une exception, dans le cas où l'autorité veut tout simplement prendre contact avec le patient, mais seulement si les trois conditions suivantes sont remplies: 1. L'autorité sait que le patient séjourne à l'hôpital. 2. Le patient n'a pas donné d'autre ordre. 3. L'autorité demande uniquement des renseignements lui permettant de prendre contact avec le patient durant son séjour à l'hôpital.

- Puisque les paroisses n'ont pas de contrôle des habitants, le règlement type sur la protection des données de l'OACOT ne leur est pas applicable pour ce qui touche aux renseignements communiqués sous forme de liste. Les paroisses traitent des données relatives à leurs membres qui sont particulièrement dignes de protection puisqu'elles concernent l'appartenance religieuse. Il n'est pas admissible de fournir à des privés des renseignements sous forme de liste concernant des données particulièrement dignes de protection, ni du point de vue de la protection des données ni de celui de la législation sur l'information.

- A quel moment les courriers annonçant la sortie d'une Eglise doivent-ils être détruits? La sortie d'une Eglise nationale est réglementée dans la législation sur les Eglises. La déclaration écrite que requiert la loi n'est pas considérée, dans la législation sur les archives, comme ayant une valeur archivistique. Elle ne doit par conséquent être conservée que pour la période durant laquelle elle peut servir de moyen de preuve (en cas de créance fiscale de la paroisse). Le délai de conservation maximal doit être déterminé au cas par cas, en fonction de l'entrée en force de la taxation (impôt paroissial), mais il ne peut excéder trois ans. Au plus tard au moment où la taxation entre en force, la déclaration n'est plus nécessaire et elle doit être détruite.

- L'outil d'évaluation de l'entreprise américaine SurveyMonkey peut-il être introduit? En acceptant la directive en matière de protection des données de l'entreprise, les utilisateurs de cet outil consentent à ce que les données collectées soient transmises à des sous-traitants établis dans des pays qui ne satisfont pas au niveau de protection des données suisse ou européen. En outre, SurveyMonkey précise qu'elle peut à tout moment modifier sa directive en matière de protection des données. Ces deux dispositions contreviennent à la loi sur la protection des données. Le traitement des données n'est en effet possible dans de tels pays que si un niveau de protection adéquat peut être garanti par contrat. Un tel contrat ne peut manifestement pas être conclu avec SurveyMonkey. L'utilisation de cet outil n'est par conséquent pas admissible.

- Les dossiers de candidature contiennent des données particulièrement dignes de protection. Or de telles données ne peuvent être transmises qu'une fois cryptées, ce qui n'est pas possible avec la solution standard myCareer. Le canton doit mettre à disposition un système de transmission ou un réseau télématique sécurisé. C'est pourquoi il ne peut pas utiliser myCareer et doit chercher une autre solution.

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). S'agissant de la procédure de consultation relative à la révision totale de la loi fédérale sur l'analyse génétique humaine (LAGH), le Bureau a transmis la prise de position de PRIVATIM.

7.2 Législation cantonale

La révision de la loi sur le marché du travail a permis de créer une base légale cantonale pour l'échange de données dans le cadre de la collaboration interinstitutionnelle (CII) prévue par le droit fédéral sur l'assurance-chômage ainsi que pour la mise en place d'une plateforme électronique.

Du fait que plusieurs institutions indépendantes les unes des autres ont accès à ces données dans le cadre de la CII, il s'agit d'une procédure

d'appel pour laquelle une base légale formelle est nécessaire. Toutes les remarques formulées par le Bureau ont été prises en compte. Le Conseil-exécutif est tenu d'inscrire les exigences concrètes en matière de protection des données relatives au traitement et à l'échange des données dans une ordonnance. La plateforme, en tant que projet informatique, doit faire l'objet d'un contrôle préalable.

- Dans la pratique, il s'est avéré que la notion d'anonymisation n'était dans bien des cas pas très claire. C'est pourquoi le Bureau a suggéré d'introduire une définition de cette notion dans le rapport relatif à la modification de la loi sur l'aide sociale.

- Depuis la 6ème révision de l'ordonnance sur l'harmonisation des registres officiels (OReg), en plus des autorités fiscales du canton et des communes, dix offices assumant des tâches relevant du droit fiscal (ou leurs systèmes, de manière automatique) ont accès à la gestion centrale des personnes (GCP). Toutes les autres autorités, qui ont perdu leur accès à la GCP, ont désormais accès à la nouvelle plateforme GERES. Le Bureau a vérifié que tous les nouveaux accès respectent les prescriptions en matière de protection des données.

L'OReg prévoyait jusqu'à présent que les communes n'avaient accès qu'aux données de leurs habitants. Dans la pratique, cette disposition n'était pas respectée, puisque l'accès à la GCP était octroyé pour tout le canton. C'est pourquoi les communes ont demandé à avoir accès à toutes les données de GERES à l'échelle du canton. Le Bureau et les autorités de surveillance des quatre communes les plus grandes ont indiqué qu'un tel accès était contraire au principe de la proportionnalité et présentait un risque pour la sphère privée – en particulier pour les personnes exposées. Le Conseil-exécutif, dans la révision de l'ordonnance, a octroyé aux communes, dans un profil séparé, l'accès à un nombre réduit d'informations pour tout le canton, ce qui devrait faciliter le suivi des arrivées et des départs. Les accès (lecture) doivent être consignés mais ne peuvent être examinés qu'en cas de soupçon. Les mesures nécessaires pour protéger les personnes exposées doivent encore être prises. Le fait que les services sociaux régionaux aient désormais accès à toutes les données contenues dans les registres du contrôle des habitants des communes qui leur sont rattachées n'a pas été controversé. Le Bureau a vérifié, en collaboration avec l'OIO, qu'une base légitimait l'accès à toutes les informations contenues dans GERES.

Certains accès ont été mis au net. Ainsi il ne sera désormais plus possible de consulter les informations relatives à la profession, étant donné qu'il n'y a aucune obligation d'annoncer et de saisir ces données, raison pour laquelle il ne peut être garanti qu'elles sont exactes et complètes. Les historiques des données personnelles, qui comprenaient toutes les données relatives aux événements passés, ont également été nettoyés: conformément aux prescriptions de la loi sur l'harmonisation des registres officiels, la plateforme GERES doit, pour ce qui est des données personnelles, refléter la situation actuelle et non tout l'historique. Les données des personnes qui ont quitté le canton de Berne ou sont décédées doivent être effacées au plus tard après cinq ans. La mise au net n'est pas encore achevée.

- S'agissant de la modification de l'ordonnance sur les soins hospitaliers, le Bureau a donné son avis sur le contenu et l'étendue des données personnelles nécessaires dans le cadre de l'aumônerie dans les hôpitaux. Il a indiqué que les collaborateurs de l'aumônerie ne doivent avoir accès qu'aux données relatives à l'état de santé des patients dont ils ont besoin pour leurs activités. Il a souligné que la mise en œuvre de cette exigence, d'un point de vue technique, est difficile lorsque l'accès aux données a lieu par l'intermédiaire d'un système d'informations cliniques.

8 Surveillance et décisions de justice

8.1 Invitation à utiliser sans délai le système sécurisé de messagerie électronique formulée par le Bureau en sa qualité d'autorité de surveillance

BE-Mail Secure est installé sur le poste de travail de tous les collaborateurs du SEMI. Cette solution pour la transmission sécurisée des courriels permet d'envoyer des messages cryptés également aux services qui ne disposent pas de ce système et d'en recevoir de leur part. Dans le cadre de l'audit des services d'aide sociale en matière d'asile et du SEMI (cf. ch. 3), le Bureau a été informé de deux envois de courriel. Dans les deux cas, des données particulièrement dignes de protection (en plus de la photo et du nom, informations sur l'ethnie, la religion, des condamnations pénales et la détention) étaient transmises par courriel sans avoir été cryptées. En réaction à la mise en danger manifeste des intérêts dignes de protection des personnes concernées, le Bureau a exigé de l'Office de la population et des migrations (OPM) qu'il veille sans délai à ce que le système sécurisé de messagerie électronique soit utilisé. La direction de l'OPM a édicté une directive en ce sens dans un délai de quelques jours.

8.2 Autorité de surveillance de la protection des données compétente pour l'Office AI

Un assuré ayant fait l'objet d'une dénonciation a demandé à l'Office AI de Vevey le nom de l'auteur de la dénonciation. L'office a rejeté sa demande. L'assuré a fait recours auprès du Tribunal des assurances sociales du canton de Vaud. Celui-ci a déclaré qu'il n'était pas compétent et a transmis l'affaire au Tribunal administratif fédéral. Ce dernier a reconnu qu'il était compétent mais a rejeté le recours. Le Tribunal fédéral, qui a ensuite été saisi, a fondé sa décision sur une prise de position du PFPDT, selon laquelle les offices AI exécutent le droit fédéral bien qu'il s'agisse d'organes cantonaux. Le Tribunal fédéral a estimé que les offices AI ne faisaient pas partie de l'administration fédérale et indiqué qu'ils n'étaient d'ailleurs pas mentionnés dans les dispositions régissant l'organisation de la Confédération. Selon lui, les autorités cantonales ne sont pas soumises à la législation fédérale sur la protection des données. Les offices AI ont été créés en tant qu'organes cantonaux explicitement désignés comme tels par des conventions entre la Confédération et les cantons. Le Tribunal fédéral a admis le recours et a renvoyé l'affaire au Tribunal administratif cantonal compétent. Il a ainsi reconnu que les autorités cantonales de surveillance de la protection des données sont compétentes pour les offices AI cantonaux. Après l'arrêt du Tribunal administratif fédéral, le Bureau avait transmis une question de point de vue ouverte au PFPDT (définition des droits d'accès dans l'application informatique OSIV de l'Office AI de Berne). L'arrêt du Tribunal fédéral concernant le canton de Vaud a permis d'élucider de manière définitive la question de la compétence, aussi pour le canton de Berne.

8.3 Rectification et élimination de dossiers de la police cantonale

Une personne a demandé qu'une information la concernant parue dans le journal de la police cantonale soit rectifiée. La police cantonale a rejeté sa demande. Dans le cadre d'un recours, la Direction de la police et des affaires militaires a estimé que les jugements de valeur et les présentations de faits controversés ne pouvaient pas être rectifiés ou éliminés. Selon elle, la personne concernée peut uniquement exiger, dans de tels cas, que soit enregistrée une version contradictoire appropriée. Elle ajoute qu'il en va de même en cas de rapports juridiques conflictuels, en particulier entre citoyen et Etat, lorsque les points de vue divergent. La justesse des indications controversées peut le cas échéant être examinée dans le cadre d'une procédure formelle (procédure de justice).

8.4 Vidéosurveillance en direct ou avec enregistrement: proportionnalité et importance du secret professionnel

Le Commandement de la police a autorisé une collectivité de droit communal à exercer une surveillance en temps réel. Il n'a en revanche pas admis la vidéosurveillance avec enregistrement. Parmi les locataires des bâtiments dont l'accès faisait l'objet d'une surveillance au moyen de caméras se trouvaient notamment des établissements médicaux. C'est pourquoi les enregistrements n'auraient pu être exploités qu'après la levée du secret médical. Dans le cadre d'une procédure d'autorisation pour un hôpital, le Commandement de la police avait appris que l'Office du médecin cantonal refusait une levée générale du secret médical. Dans sa décision, la Direction de la police et des affaires militaires a souligné que les enregistrements appartenaient à la collectivité de droit public, et non à un membre du corps médical. Selon elle, la levée du secret professionnel n'était par conséquent pas nécessaire pour exploiter les enregistrements. Elle parvenait à la conclusion qu'une vidéosurveillance dissuasive avec enregistrement respectait le principe de la proportionnalité et que le recours de la collectivité de droit public devait par conséquent être admis.

9 Police

9.1 Autorisation d'exploiter le système ViCLAS

Le Conseil-exécutif a octroyé l'autorisation requise tant par la loi sur la police que par le concordat ViCLAS pour l'exploitation de la banque de données ViCLAS, qui contient des informations sur les grands criminels et est utilisée dans toute la Suisse. Les remarques formulées par le Bureau dans le cadre de la procédure de contrôle préalable ont été prises en compte. L'autorisation est limitée à cinq ans. Cette durée limitée s'explique par le fait que la police canadienne, qui concède la licence, n'adapte actuellement plus le programme aux évolutions informatiques.

9.2 Audit de la téléphonie mobile (MDM)

En plus de nombreux problèmes relatifs à la sécurité informatique, l'audit a révélé que le risque de surveillance des collaborateurs était considérable. L'organe de contrôle externe a en effet constaté que les collaborateurs n'étaient pas suffisamment informés de l'étendue de la collecte des données. Ils n'avaient notamment pas connaissance du fait que des informations sur l'itinérance (roaming) étaient entreposées auprès du Commandement de la police. Celui-ci peut également savoir, au moyen de la gestion de terminaux mobiles (MDM), quelles sont les

applications qu'un collaborateur a installées sur un appareil (même si une utilisation à des fins privées est admise). Il lui est en outre possible de voir en temps réel dans quelle zone de réception se trouve un téléphone portable. Puisque les collaborateurs sont tenus de garder les téléphones qui leur sont donnés allumés y compris durant leurs loisirs, afin de pouvoir réagir en cas d'alarme, il est possible de les localiser même en dehors des heures de service. Or il n'existe pas de base légale formelle pour justifier une telle atteinte au droit fondamental à la protection des données.
Pour les téléphones intelligents disposant d'anciens systèmes d'exploitation, le problème ne se pose pas: si les collaborateurs ne désactivent pas la fonction de localisation, cela signifie qu'ils acceptent la possibilité d'être surveillés. Le problème est que désactiver cette fonction revient à enlever la possibilité au Commandement de police d'effacer, au moyen de la MDM, les données enregistrées sur l'appareil à des fins professionnelles en cas de vol – possibilité qui avait été demandée. Par ailleurs, si un collaborateur fait des photos à des fins professionnelles avec son téléphone, il n'est pas exclu que ces données soient synchronisées sur son ordinateur privé – et qu'elles soient sauvegardées dans le nuage par l'intermédiaire d'iTunes. Une solution permettant de séparer les données privées et professionnelles doit être recherchée.
Le Commandement de la police a au préalable pris des mesures organisationnelles en vue de résoudre le problème. L'acquisition de nouveaux téléphones intelligents permet de garantir que les systèmes d'exploitation iOS actualisés peuvent être installés. Les documents relatifs à ces appareils n'ont pas encore été soumis dans leur intégralité au Bureau en vue du contrôle préalable. L'audit a révélé que l'exploitation d'un système MDM est délicate et comporte des risques de violation des droits de la protection des données. Il a toutefois aussi montré à quel point il est nécessaire que les terminaux mobiles sur lesquels sont traitées des données pour l'accomplissement de tâches publiques soient gérés et protégés au moyen d'un système MDM. Le Commandement de la police a été le seul à reconnaître le problème et à chercher une solution. Des terminaux mobiles sont pourtant utilisés dans toute l'administration cantonale. Le projet relatif à un système MDM pour toute l'administration (cf. ch. 5, remarques concernant HarmTel), qui vient d'être lancé, arrive tard.

9.3 Capteur IMSI

Le Bureau a souligné, à l'intention de la Direction de la police et des affaires militaires, que l'acquisition d'un capteur IMSI est soumise à la procédure de contrôle préalable des projets informatiques.

(Concernant la vidéosurveillance par la police cantonale, cf. ch. 4; concernant la rectification et l'élimination, cf. ch. 8.3)

10 Cas particulier

10.1 Non-respect des directives en matière de mot de passe durant plusieurs mois

Pour se connecter à un poste de travail électronique, il est nécessaire d'introduire un mot de passe. Or, entre juillet 2014 et mars 2015, les directives en matière de mot de passe, applicables à tout le canton, n'ont pas été correctement mises en œuvre s'agissant des collaborateurs de la Direction de la justice, des affaires communales et des affaires ecclésiastiques (JCE), du fait que les mécanismes de protection avaient été désactivés. La configuration du système en cause avait déjà été remarquée en mai 2013. Le système ainsi configuré permet, contrairement à ce que prévoient les directives en matière de mot de passe, de choisir un mot de passe simple (par exemple 20162016). De plus, il ne limite pas le nombre de tentatives, en cas de saisie erronée du mot de passe (il autorise 999 tentatives, alors que la directive cantonale n'en prévoit que 3). Il exige en revanche que le mot de passe soit changé tous les 30 jours, ce qui est correct. En mars 2015, le problème a dû être résolu, sur le plan technique, non pas par la JCE mais par l'OIO, qui est le prestataire de services. C'est lui en effet qui fournit les services informatiques de base, cadre dans lequel la JCE a transféré ses applications depuis 2014. L'application des directives en matière de mot de passe avait entraîné des problèmes de connexion pour les utilisateurs. C'est pourquoi le Service d'informatique de la JCE avait décidé d'ignorer ces directives. La disponibilité des applications exploitées par les différents services de la JCE pouvait ainsi continuer d'être garantie.
Cet exemple montre à quel point il est important, dans le cas de systèmes fortement intégrés, que le propriétaire des données assume la responsabilité de toute la chaîne de services: la confidentialité des données traitées par les services était menacée. Or la direction du service concerné doit veiller à protéger ses données. Cela signifie qu'elle doit s'assurer aussi bien auprès du service d'informatique de la Direction qu'auprès des prestataires centraux de services informatiques (prestations de base) qu'ils sont en mesure d'accomplir leurs tâches conformément aux prescriptions (sélection).

Elle doit en outre fournir aux prestataires de services toutes les instructions nécessaires afin qu'ils agissent de manière correcte. Ceux-ci sont dans tous les cas tenus d'informer les responsables des applications (bénéficiaires des prestations) de tous les changements de système qui pourraient avoir des répercussions sur la sécurité. Cela ne dispense pas les bénéficiaires des prestations de s'assurer – par exemple dans le cadre de rapports sur la gestion, qui peuvent être institutionnalisés – que le cadre légal est respecté et de veiller à ce que l'exploitation de toutes les solutions informatiques soit sûre et conforme aux prescriptions de la législation sur la protection des données (contrôle).

11 Points abordés dans le rapport précédent

(3 et 9.2: suivi des contrôles préalables effectués en 2014, 5: contrôles préalables effectués).

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.

29 janvier 2016

Le délégué à la protection des données: *Siegenthaler*

13 Annexe

13.1 Abréviations et désignations

ABR: Asile Bienne et région (association)
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
AI: assurance-invalidité
Bedag (Bedag Informatique SA): entreprise fondée en 1990 et détenue par le canton de Berne
BRSB: Service spécialisé pour handicapés de la vue du canton de Berne
Cf.: confer (voir)
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
CHB: Centre hospitalier Bienne
CII: collaboration interinstitutionnelle
CPM: Centre psychiatrique de Münsingen
DEP: dossier électronique du patient (système d'informations cliniques de l'Hôpital de l'Ile)
EMM: gestion de la mobilité d'entreprise (voir aussi MDM)
ESAP: projet de remplacement du système de finances et de gestion du personnel de la Haute école spécialisée bernoise et de la Haute école pédagogique de Berne
FAQ: foire aux questions
Fedpol: Office fédéral de la police
FMI AG: hôpitaux de Frutigen, Meiringen et Interlaken
FTAPI: FTAPI (File Transfer Application Platform for Integration) Software GmbH est une entreprise munichoise qui développe et distribue des solutions hautement sécurisées pour le transfert de données commerciales (d'après Wikipédia)
GCP (gestion centrale des personnes): banque de données de l'Intendance des impôts contenant des informations sur les personnes physiques et morales
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
IFIK: Institut des maladies infectieuses de l'Université de Berne
ISO: Organisation internationale de normalisation
ISO 2700x: suite ou famille de standards comprenant les normes de sécurité de l'information (d'après Wikipédia)
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 / plateforme Skype: 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)
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)
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)
OIO: Office d'informatique et d'organisation
OPM: Office de la population et des migrations

OSIV: système d'information Open System IV, application informatique utilisée par plusieurs offices AI
PFPDT: préposé fédéral à la protection des données et à la transparence
PRIVATIM: association des Commissaires suisses à la protection des données
QSC AG: prestataire de services informatiques, gestionnaire de réseau et fournisseur de produits Internet et télécommunication allemand dont le siège se trouve à Ossendorf (Cologne) (d'après Wikipédia)
RSE AG: hôpital régional de l'Emmental
SAP: Direction de la santé publique et de la prévoyance sociale
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)
SIC: système(s) d'informations cliniques
SIL: système d'information de laboratoire
SIPD: sûreté de l'information et protection des données
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
SPJBB: Services psychiatriques Jura bernois – Bienne – Seeland à Bellelay
SPU: Services psychiatriques universitaires
SRO: centre hospitalier régional de Haute-Argovie
SUSA: application de l'Office de la circulation routière et de la navigation
TI: technologies de l'information
ViCLAS (Violent Crime Linkage Analysis System): système d'analyse des crimes violents devant servir à l'identification des criminels en série
ZERO: programme introduit pour l'examen et le versement de prestations individuelles par l'Office des personnes âgées et handicapées de la SAP

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

8.1: Invitation du Bureau du 2 décembre 2015 adressée à l'OPM concernant la prescription tardive des mesures nécessaires (42.52-6250)
8.2: ATF 1C_125/2015 du 17 juillet 2015
8.3: Décision de la Direction de la police et des affaires militaires BD 123/13 Sn du 20 février 2015
8.4: Décision de la Direction de la police et des affaires militaires BD 238/14 Ho du 28 juillet 2015

13.3 Sitographie

1.2: PRIVATIM: à propos du contrôle cantonal des factures de prestations stationnaires dans le domaine de l'assurance obligatoire des soins
http://www.privatim.ch/files/layout/downloads_de/15_0071_07-FR_privatim-Umfrage_Rechnungspruefung_Ergebnisse_20150213.pdf
2.3: Rapport de gestion:
http://www.fin.be.ch/fin/fr/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html
4: Rapports d'évaluation relatifs aux installations de vidéosurveillance de la Direction de la police et des affaires militaires:
http://www.pom.be.ch/pom/fr/index/direktion/ueber-die-direktion/publikationen
6: Plateformes pour l'échange de données:
http://www.jgk.be.ch/jgk/fr/index/aufsicht/datenschutz/informatiksicherheit.assetref/dam/documents/JGK/DS/fr/DS_Datendrehscheiben_Dokumentation%20in%20der%20Vorabkontrolle%20nach%20Art.%2017a%20KDSG_fr.pdf