Rapport d'activité 2017 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

1 Introduction

1.1 2017 en bref

Les 13 services régionaux du service psychologique pour enfants et adolescents traitent une grande quantité de données particulièrement dignes de protection. Le Bureau pour la surveillance de la protection des données (le Bureau) avait effectué un contrôle du système de gestion des affaires utilisé jusqu'ici par ces services il y a déjà quelque temps. En 2017, ce système a été remplacé par une nouvelle solution, qui a été soumise au Bureau en vue du contrôle préalable. Un peu par hasard, le Bureau a constaté dans ce cadre que la Direction de l'instruction publique (INS) avait changé l'environnement des postes de travail du service psychologique pour enfants et adolescents, sans passer par la procédure de contrôle préalable. Le passage au nouvel environnement technologique impliquait un changement de système d'exploitation (désormais Windows 10) mais aussi l'abandon de la connexion au réseau chiffrée et sécurisée utilisée jusqu'alors. Entre les postes de travail des collaborateurs des services régionaux et le serveur central situé à l'INS, les données circulaient dès lors de manière non chiffrée. Or ni le service psychologique pour enfants et adolescents ni la Direction n'en avaient conscience. C'est seulement après l'intervention du Bureau que l'INS a cherché à résoudre le problème.

Cet exemple illustre bien les problèmes auxquels le Bureau est sans arrêt confronté. C'est le principe de la boîte noire: le service psychologique pour enfants et adolescents n'a qu'une connaissance superficielle des postes de travail informatiques et de leur capacité à établir des connexions (connectivité). Il ne comprend pas bien le fonctionnement interne de ces outils, qu'il ne peut pas refuser, et peut difficilement l'influencer. La situation est la même pour certaines solutions informatiques qui sont mises à la disposition des services dans le cadre de l'approvisionnement de base. A titre d'exemple, on peut citer le système de gestion des affaires GEVER, qui permet aussi l'archivage électronique des documents (GAE), la solution d'impression BE-Print mais aussi le poste de travail cantonal 2.x ou les services en ligne – des projets qui ont occupé le Bureau durant l'année écoulée. L'attitude des services par rapport au principe de la boîte noire n'est pas toujours la même: alors que certains se réjouissent d'être déchargés de tâches exigeantes, d'autres réalisent qu'ils perdent la maîtrise de leurs données.

Conformément à la loi sur la protection des données, la responsabilité de la gestion des données incombe aux services administratifs. Chaque service est responsable des données qu'il traite dans le cadre de l'accomplissement de ses tâches. Le nouveau droit de la protection des données, tel qu'il doit être adapté pour respecter les directives européennes, exige des services administratifs qu'ils puissent prouver que leurs pratiques sont conformes à la protection des données. Cela implique que les services disposent, à l'avenir, des connaissances nécessaires, même lorsqu'une solution toute faite (et qui constitue de ce fait une «boîte noire») est mise à leur disposition.

La nouvelle ordonnance sur les TIC est incompatible avec ces directives: elle prévoit que le Bureau doit désormais adresser ses recommandations motivées uniquement à l'Office d'informatique et d'organisation (OIO), qui est compétent pour les services informatiques de base, lorsque celles-ci concernent la conception technique ou organisationnelle d'un service informatique. Pour justifier ce changement, il est avancé que le service concerné n'est pas du tout en mesure de procéder aux adaptations demandées par le Bureau. C'est on ne peut plus emblématique des divergences d'opinions entre les partisans de l'accomplissement des tâches relevant du domaine des TIC de manière centralisée et le Bureau.

Le problème de la boîte noire de se pose pas qu'au sein du canton: le Bureau constate que des problèmes similaires surgissent lorsque des services publiques délèguent leurs tâches informatiques dans une large mesure à des prestataires externes, par exemple Swisscom pour la police.

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). Une séance de travail a été organisée en 2017. Le Bureau a procédé à la vérification des requêtes de 319 collaborateurs de la Police régionale de l'Oberland bernois bénéficiant d'un accès à ce système. Le contrôle effectué par sondage a révélé que le principe de la proportionnalité était respecté.

Des collaborateurs du Bureau sont membres des groupes de travail «Technologies de l'information et de la communication», «Santé» et «Administration numérique» de PRIVATIM. Le groupe de travail «Santé» s'est intéressé de manière approfondie à la protection des données et à la sécurité du dossier électronique du patient (DEP). Les dispositions prévoyant que la personne concernée doit agir volontairement pour empêcher la communication de données

(opt-out actif) sont problématiques. Elles permettent aux professionnels de la santé d'accéder à des données qui ne sont pas nécessaires à l'accomplissement de leurs tâches. La LDEP exige que les professionnels de la santé travaillant en hôpital et dans les EMS disposent, d'ici à 2020 et 2022, respectivement, de l'infrastructure nécessaire pour lire les documents figurant dans le DEP. Pour les professionnels de la santé travaillant dans d'autres domaines ainsi que pour les patients, le recours au DEP est facultatif. Le groupe de travail s'est intéressé à une autre thématique importante, celle de l'assurance et du contrôle qualité dans le domaine de la santé. Différents registres sont tenus à cet égard. Or ils sont alimentés avec les mêmes données administratives des patients. Il y a dès lors un risque que leurs contenus soient mis en relation. Il est aussi possible de recourir à des évaluations par des pairs pour l'assurance et le contrôle qualité. PRIVATIM a exprimé un avis critique à cet égard en raison de l'absence de bases légales suffisantes. Les membres du groupe de travail ont échangé sur l'étude nationale sur la couverture vaccinale des enfants. Le canton de Berne avait réalisé des travaux préalables à cet égard.
Le groupe de travail «Administration numérique» a l'intention d'élaborer un document de travail sur les relations numériques entre les habitants et l'Etat.

1.3 Modifications intervenues dans le droit supérieur, mise en œuvre de la motion «Assouplissement raisonnable de la protection des données»

Le droit cantonal doit être adapté en raison de la réforme européenne de la protection des données ainsi que de la modernisation de la Convention 108 du Conseil de l'Europe. A cet égard, il convient également de tenir compte du projet de révision totale de la loi fédérale sur la protection des données. Un groupe de travail de la Conférence des gouvernements cantonaux a élaboré un guide à l'intention des cantons. Sous la houlette de la Direction de la justice, des affaires communales et des affaires ecclésiastiques (JCE), un groupe de travail interne composé de représentants de la Direction de la police et des affaires militaires, de la Direction de la magistrature et du Bureau a rédigé une ordonnance législative de substitution, qui entrera en vigueur au 1er août 2018. Les exigences de la motion intitulée «Assouplissement raisonnable de la protection des données» (motion Vogt 224-2016), qui a été adoptée par le Grand Conseil, doivent être prises en considération dans le cadre de la prochaine révision de la loi sur la protection des données.

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. Il doit également accomplir des tâches administratives. Or, dans toutes les unités administratives de petite taille, des tâches telles que le remplacement du système de gestion des affaires et d'archivage actuel ou la participation à la commission d'exploitation représentent une charge disproportionnée par rapport aux ressources en personnel. C'est la loi sur la protection des données qui attribue au Bureau 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 le tri des requêtes qu'elles impliquent, sont inscrites 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 dé-

taillée 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 personnelles 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 pour garantir l'accomplissement des tâches.

2.2 Responsabilité propre des services traitant les données

Les collaborateurs des services d'aide sociale en matière d'asile ont bénéficié d'informations sur la protection des données dans le cadre d'un cours de perfectionnement organisé par l'Office de consultation sur l'asile.
Les tribunaux civils ont également organisé un cours de perfectionnement à l'intention du personnel de leur secrétariat.
A la demande de l'association des administrateurs de paroisse bernoise, le Bureau a participé à une séance semestrielle, dans le cadre de laquelle il a répondu à des questions actuelles relatives à la protection des données.

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

En 2016, le budget attribuait, pour l'administration cantonale, 39 millions de francs aux investissements dans le domaine informatique et 164 millions de francs à l'exploitation (dont CHF 128 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 176 000 francs.

Le Bureau a disposé de 5,15 postes à temps complet (dont 0,2 pour le secrétariat). Les circonstances ont été telles qu'un poste à 100 pour cent est resté vacant pendant plus de huit mois. Des informations complémentaires relatives au budget, aux comptes ainsi qu'aux objectifs de NOG (données financières) sont disponibles dans le rapport de gestion de 2017 du canton de Berne (volume I).

3 Contrôle des applications informatiques utilisées

Trois audits ont été réalisés en 2017:

- BE-Print: contrôle de l'infrastructure d'impression et de numérisation

L'infrastructure d'impression constitue l'un des services informatiques de base mis à la disposition des Directions et de la Chancellerie d'Etat. D'un point de vue technique, ce service englobe les appareils multifonctions qui permettent d'imprimer et de numériser des documents ainsi que les dispositifs de liaison et les serveurs permettant d'exploiter les applications utilisées. La fonction d'impression suivie (*follow-me-printing*) permet d'envoyer tous les mandats d'impression au serveur central, exploité par la Bedag, qui les transmet ensuite à l'appareil sur lequel l'utilisateur s'identifie et exécute le mandat en question. S'agissant de la numérisation, après que l'utilisateur s'est identifié sur l'appareil multifonctions, le document numérisé est envoyé au serveur central, qui le conserve dans le dossier de l'utilisateur ou l'envoie à son adresse électronique. L'examen a révélé que les prescriptions relatives à la transmission chiffrée ne sont pas suffisamment mises en œuvre. Le fournisseur de prestations (OIO) ainsi que les Directions concernées et la Chancellerie d'Etat ont été informées du résultat du contrôle.

- Examen de la protection de base de l'infrastructure informatique de la Police cantonale

S'agissant de l'infrastructure informatique de la Police cantonale, qui est complexe, l'examen a porté sur la mise en œuvre des prescriptions de la protection de base. Le contrôle doit montrer dans quelle mesure l'infrastructure, dans le cadre de l'exploitation actuelle, est conforme aux prescriptions SIPD et ainsi diminuer le travail nécessaire lors des prochains contrôles préalables des applications spécifiques. Le rapport d'audit est en cours d'élaboration et doit faire l'objet d'un accord avec la Police cantonale.

- Contrôle des applications informatiques ESCADA/EVENTO des écoles du niveau secondaire II

L'examen a eu lieu en automne 2016. Il a révélé des lacunes importantes dans la gestion des utilisateurs. Les comptes d'anciens collaborateurs étaient notamment toujours actifs. En outre, les droits d'accès n'étaient pas attribués aux utilisateurs selon le principe du besoin de connaître. Cela a pour conséquence que les collaborateurs d'une école ont accès aux dossiers d'élève d'autres écoles. Les prescriptions relatives à l'effacement et à l'archivage des données n'étaient pas mises en œuvre, faute de directives.

- Contrôle de l'offre MS 365 de la Direction de l'instruction publique (paquet Office et service de stockage dans le nuage)

L'élaboration du concept SIPD a pris du retard, ce qui a repoussé l'examen prévu au début de 2018.

Suivi des contrôles effectués en 2016:

- Association Asile Bienne et région (ABR)

Suite au rapport d'audit, la direction a pris les mesures techniques et administratives nécessaires. Toutes les personnes intéressées ont fourni de gros efforts pour que le projet SIPD, qui était ambitieux, puisse être achevé en 2017. L'association ABR est aujourd'hui en mesure de traiter les données particulièrement dignes de protection qui relèvent du domaine de la migration dans le respect de la protection des données.

- Clinique Südhang

La mise en œuvre des questions encore en suspens devrait être réglée avec la migration prévue. Cela concerne en particulier la sécurité de l'accès aux données à distance.

4 Vidéosurveillance

- Plusieurs installations de l'Hôpital de l'Ile ainsi qu'une caméra de l'Office des poursuites et des faillites de Berne Mittelland ont fait l'objet d'un contrôle préalable. Les mesures de surveillance prévues se sont révélées adéquates. Le Bureau a attiré l'attention de l'Hôpital de l'Ile et de l'Office du médecin cantonal sur le fait qu'il convient de demander à ce dernier de lever l'obligation de garder le secret avant l'utilisation d'images sur lesquelles figurent des patients par la Police cantonale. Comme cela avait déjà été le cas, l'examen a également porté sur des caméras qui ne visaient pas à assurer la sécurité mais devaient contribuer à la logistique ou permettre la surveillance médicale de patients. La loi sur la police ne règle pas ce type de cas. La surveillance doit, dans la mesure où elle est nécessaire à l'accomplissement des tâches, se li-

miter à de la surveillance en temps réel. En dehors du champ d'application de la loi sur la police, il manque une base légale formelle pour les enregistrements. Il en va de même pour les caméras qui visent à assurer la sécurité mais qui ne se trouvent pas dans des bâtiments ou des locaux «librement accessibles». C'est la raison pour laquelle l'Hôpital de l'Ile a renoncé à placer une caméra, comme il l'avait prévu, dans une pièce fermée le soir et les week-ends.
Le projet de surveillance de l'Office des poursuites et des faillites a donné l'occasion de préciser les conditions relatives à l'annonce d'une surveillance: seuls les espaces qui font effectivement l'objet d'une vidéosurveillance peuvent être signalés comme tels. Si l'intérieur d'un ascenseur est surveillé par une caméra, il convient de l'indiquer à chaque étage à l'entrée de l'ascenseur. En revanche, il doit être clair que l'entrée principale n'est pas surveillée.

- Caméra permettant de surveiller les émissions de fumée

L'utilisation de caméras de surveillance pour détecter d'éventuelles émissions de fumée non autorisées nécessite une base légale explicite. Etant donné que les personnes concernées doivent donner leur accord, il suffit de compléter l'ordonnance cantonale sur la protection de l'air.

- Webcams

Après le dépôt d'une pétition, une commune a posé des questions au Bureau sur une caméra qu'elle avait installée sur son bâtiment scolaire. Sur le conseil du Bureau, la caméra a été configurée de telle sorte que les images des rues et des places publiques, des entrées d'habitation, des fenêtres et des esplanades soient pixélisées. De cette manière, les images ne peuvent être agrandies (zoom) que de manière restreinte et ne peuvent pas être traitées individuellement. Les responsables au niveau communal ont en outre organisé une séance publique afin de garantir que les éventuels souhaits en vue d'une meilleure protection de la sphère privée puissent être pris en considération.

5 Contrôle préalable de projets informatiques

Le Bureau a de nouveau examiné un grand nombre de projets informatiques. La liste suivante n'est pas exhaustive, elle ne fait que donner des exemples d'examens en cours ou achevés en 2017.

5.1 Contrôles préalables en cours

- TREE2, application informatique de l'Université de Berne pour un projet de recherche en sciences sociales, qui s'intéresse au passage des jeunes de l'école obligatoire à une formation supérieure et à la vie d'adulte. Le Bureau a émis une première prise de position, dans laquelle il demandait aux responsables du projet d'effectuer les adaptations nécessaires dans le concept SIPD et de les mettre en œuvre.

-Axioma, service psychologique pour enfants et adolescents: une démonstration sur place (qui est possible à un stade avancé de la procédure de contrôle préalable) permet souvent au Bureau de se faire une meilleure idée du projet qu'un contrôle se limitant à des documents. Tel a été le cas pour Axioma. La question de savoir si les coordonnées de toutes les personnes impliquées dans des processus de conseil doivent être accessibles à tous les services psychologiques pour enfants et adolescents du canton est encore en discussion, de même que celle de la vérifiabilité de l'activité de l'administration dans le cas où les dossiers sont tenus uniquement sous forme électronique (cf. ch. 1.1).

-BEJUNE, application permettant de traiter les données dans le domaine du dépistage du cancer du sein dans le Jura bernois ainsi que dans les cantons du Jura et de Neuchâtel: après que le Bureau a émis une première prise de position en 2016, les documents SIPD remaniés doivent être examinés en vue des derniers éclaircissements.

- IBAS, système de décompte de la SAP pour les personnes handicapées: la mise en service est prévue pour le début de 2019. Le Bureau avait émis une première prise de position. Par la suite, il lui a été communiqué que les documents SIPD ont été remaniés après que le mandat de réalisation avait été confié à une entreprise et que, dans ce cadre, il avait été tenu compte de ses remarques.

- La Haute école spécialisée bernoise (BFH) a mis à jour son système d'exploitation (désormais Windows 10) et installé Microsoft Office 365 en local. Le fonctionnement d'Office 365, offre qui propose le paquet Microsoft Office et une certaine capacité de stockage dans ce que l'on nomme un nuage, et par conséquent l'examen visant à déterminer si les prescriptions SIPD sont respectées demandent des connaissances très spécialisées et des ressources importantes. Le Bureau a effectué un premier examen des documents qui lui ont été remis, en se concentrant sur les aspects liés à la sûreté de l'information. La BFH doit intégrer à ses documents SIPD de nombreuses informations, notamment au sujet du chiffrement, de l'authentification ainsi que de l'intégrité et de l'effacement des données.

- Les réponses aux questions posées sur le fonctionnement du SIC des SPU ont été soumises au Bureau pour examen. Les documents

complètement remaniés relatifs au schéma des rôles et des droits lui ont également été remis. Des mesures doivent encore être prises s'agissant de la consultation de la journalisation des accès (lecture), qui doit être limitée aux personnes exerçant des tâches de contrôle.

- L'organisation des droits d'accès des médecins assistants, au sein du RSE AG, a donné lieu à des échanges entre le Bureau et cette institution. Dans les deux hôpitaux du RSE, ces médecins fournissent des prestations (de nuit) et disposent par conséquent de droits d'accès très étendus. La restriction de ces accès demandée par le droit de la protection des données doit à l'heure actuelle être examinée, compte tenu des exigences relatives au traitement de données de personnes exposées (VIP).

- S'agissant du SIC des FMI AG, la gestion des personnes exposées (VIP) doit également être examinée du point de vue du droit de la protection des données. Dans le cadre d'un entretien à l'hôpital d'Interlaken (FMI AG), la question de l'attribution des droits d'accès selon les mandats, pour les fonctions transversales (p. ex. physiothérapie ou conseil en matière de diététique), a fait l'objet d'intenses discussions. Les FMI AG ont par la suite proposé qu'un système d'alerte soit utilisé. Ainsi, le dossier médical d'un patient ne devrait pouvoir être consulté par sa diététicienne que si le médecin traitant a activé la fonction d'alerte, et ainsi débloqué le dossier du patient concerné, qui peut dès lors être consulté par les personnes autorisées. L'accès illimité, pour la diététicienne, à toutes les données des patients de l'hôpital serait contraire au principe de la proportionnalité, puisqu'elle n'intervient qu'auprès d'une petite partie des personnes hospitalisées.

- Après un changement de personnel, les responsables du centre hospitalier régional de Haute-Argovie (SRO AG) ont remanié en profondeur les documents SIPD relatifs au SIC. C'est pourquoi une discussion des questions encore en suspens ainsi qu'une présentation du SIC ont eu lieu en 2017 et que les documents remaniés à la suite de celles-ci ont à nouveau été soumis au Bureau pour examen. Ce dernier a exigé clairement que les aspects relatifs à la sécurité informatique, qui n'avaient pas encore été traités jusqu'ici, soient réglés.

- Décisions stratégiques de principe, projet ERP

S'agissant des décisions relatives aux questions stratégiques de principe et à la validation de la phase conceptuelle du projet ERP (Enterprise Resource Planning, progiciel de gestion intégré [PGI]), le Bureau a pris connaissance du fait que le concept SIPD est en cours d'élaboration.

- Arrêts domiciliaires sous surveillance électronique

En vertu du droit fédéral, l'application Electronic Monitoring (EM) permet d'exercer une surveillance électronique sur les peines privatives de liberté prononcées contre des adultes et des adolescents ainsi que sur des mesures ambulatoires (p. ex. arrêts domiciliaires). Toutes les données collectées sont particulièrement dignes de protection. Le canton de Berne a aujourd'hui adopté la solution du canton de Zurich. Les résultats du premier contrôle préalable, effectué en 2016, ont été pris en considération lors du remaniement des documents. Les questions du respect du principe de la proportionnalité s'agissant du recours au suivi GPS, des critères autorisant une surveillance en temps réel, de la conservation et de l'élimination des données collectées ainsi que de la limitation de l'accès des fournisseurs du logiciel externes aux données sont encore en suspens.

- Système de gestion des affaires et d'archivage BE-GEVER GAE

Le projet BE-GEVER GAE fait partie de l'approvisionnement de base commun. Dans le cadre du contrôle préalable de la stratégie d'entreprise y relative (rapport 2016), deux aspects se sont révélés problématiques:

- A la différence de ce qui se fait à la Confédération, pour les documents classés sous forme électronique (bureau sans papier), ni signature électronique ni double authentification ne sont requises pour accéder au système. A cet égard, le Bureau a formulé une recommandation motivée à l'intention de la Chancellerie d'Etat (qui a déjà introduit le système au titre de projet pilote). Celle-ci a rendu une décision de rejet, que le Bureau a attaquée au moyen d'un recours de droit administratif (cf. ch. 8.1). Les mêmes problèmes se posent pour l'exploitation du système BE-GEVER GAE, qui a débuté sans contrôle préalable, par le Secrétariat général de la Direction des finances, l'Administration des finances, l'Intendance des impôts ainsi que l'Office du personnel.

- Les mandants (les Directions ou leurs unités administratives) peuvent attribuer les droits d'accès, y compris au-delà des frontières d'une Direction. Afin que des lacunes en matière de sécurité puissent être évitées, une même échelle de classification doit être utilisée pour tout le canton. Or tel n'est pas le cas pour le moment; l'examen des concepts SIPD des mandants qui ont été soumis au Bureau permettra de voir quelles sont les conséquences de l'absence d'une telle classification. L'organisation des droits d'accès à l'interne et la durée de conservation des documents et des fichiers log constitueront deux autres aspects importants du contrôle.

- Postes de travail PTC 2.x

Le personnel de l'administration doit être équipé de nouveaux postes de travail (nouveaux clients), munis du système d'exploitation Windows 10. Il s'agira d'acheter des postes fixes et des appareils mobiles. Après un premier examen du concept SIPD, le Bureau a notamment constaté

- que les appareils doivent remplir des exigences accrues pour que des données personnelles particulièrement dignes de protection puissent y être traitées et
- que la connectivité des appareils doit être prise en considération.

Les appareils doivent être configurés de manière standardisée conformément à un code de bonne conduite, qui doit être établi, et une surveillance doit pouvoir être exercée quant au respect de ces exigences. Les processus relatifs à l'installation de mises à jour de sécurité et relatives à l'assistance doivent en outre être documentés et mis en œuvre. Le Bureau a transmis ses recommandations à l'OIO. Le contrôle préalable n'a pas pu être achevé, car cet office a étendu le projet.

-BEKOS

Le projet informatique en vue de la coordination des institutions pédagogiques et sociopédagogiques cantonales de la SAP vise à harmoniser l'infrastructure informatique (y c. communication) et les logiciels de base utilisés par les membres du corps enseignant et de l'administration. Le contrôle préalable a révélé des lacunes considérables aux niveaux de la conception et de la technique. Bien que le Bureau ait soutenu activement l'élaboration d'un concept SIPD qu'il puisse examiner, aucun document ne lui a été remis à ce jour.

- Autonomisation des institutions psychiatriques: les trois cliniques psychiatriques ont été autonomisées au 1er janvier 2017. Malgré leur nouvelle forme juridique, elles restent soumises à la loi cantonale sur la protection des données. Du point de vue technique, l'autonomisation signifie que les prestations informatiques cantonales, par exemple le service de messagerie et Internet, mais aussi les services liés aux centres de calculs indispensables à l'exploitation, ne sont plus disponibles pour ces institutions, qui doivent se créer une infrastructure informatique propre ou développer l'infrastructure existante. Contrairement à ce que proposait le Bureau, les cliniques ont décidé d'élaborer un concept SIPD pour chaque site. Chaque concept SIPD doit tenir compte des risques inhérents au domaine de la psychiatrie et décrire une protection de base adaptée. Cette manière de procéder permet de réduire considérablement les charges liées au contrôle préalable des applications spécifiques. Au moment de l'établissement du présent rapport, les SPJBB avaient soumis au Bureau un concept SIPD pour examen.

5.2 Contrôles préalables achevés

Les procédures de contrôle préalable suivantes ont pu être achevées:

- GELAN 2015, nouveau système d'information agricole des cantons de Berne, Fribourg et Soleure;
- Mise à jour de PERSISKA, système central d'informations sur le personnel du canton de Berne;
- Snagit, application de groupe de l'OIO pour l'élaboration et l'amélioration de vues d'écran (captures d'écran et vidéos);
- Optinomic, application du Centre de compétences pour l'être humain et ses dépendances Südhang;
- Flux de travail (workflow) des créanciers de l'Université de Berne;
- CASEnet, application pour le suivi des dossiers (case management) des membres du corps enseignant de la Haute école pédagogique de Berne (PHBern);
- Système d'informations sur le personnel et les traitements du Centre psychiatrique de Münsingen (PIS CPM);
- Kernsystem Lehre (KSL) de l'Université de Berne, application utilisée pour le suivi électronique des examens, le répertoire électronique des cours et la gestion des auditoires;
- BIHAM, application web de l'Université de Berne pour la gestion des stages de médecine de premier recours (examen rapide des aspects relatifs à la protection des données, sans les aspects relatifs à la sûreté de l'information);
- Outil utilisé par le Centre de puériculture (CP BE) pour le conseil et l'établissement de rapports, numérisation des processus de travail (gestion du personnel et des adresses, données de base, conseil des clients);
- Plateforme BCEE, Bourse cantonale des emplois de l'enseignement (examen rapide des aspects relatifs à la protection des données).
- Le contrôle préalable du SIC du CPM a pu être achevé après que le fournisseur du logiciel a confirmé que les procès-verbaux d'effacement ne contiennent pas de données médicales relatives aux patients (si tel n'était pas le cas, le droit à l'oubli des personnes concernées ne serait pas respecté). En raison des réflexions relatives au droit de la personnalité, le procès-verbal d'effacement ne doit pas contenir d'informations détaillées, d'un point de vue technique, mais plutôt constituer une preuve de l'effacement des données (plausibilité). En d'autres termes, le procès-verbal (ou les tableaux sur lesquels il se fonde) ne doit pas contenir de données relatives aux patients, sans

quoi l'effacement n'est pas considéré comme suffisant.
- Gestion de la mobilité d'entreprise (EMM, gestion des terminaux mobiles) des services informatiques de base et de la Police cantonale
Le contrôle préalable du projet de gestion de la mobilité d'entreprise a été achevé. L'exploitation du logiciel de gestion a été confiée à Swisscom. La Police cantonale a soumis au Bureau un projet similaire en vue du contrôle préalable.
- OSIV de l'Office AI
Un Office AI a entrepris des démarches en vue de soumettre au contrôle préalable son système de gestion des affaires OSIV, qui devait être renouvelé. Si un service administratif se déclare incompétent, il transmet l'affaire en question au service responsable. Etant donné que le droit fédéral de la protection des données ne connaît pas de procédure correspondant à celle du contrôle préalable, le Bureau n'a pas pu transférer l'affaire au PFPDT. La jurisprudence du Tribunal fédéral sur la question de la compétence est inconstante; elle ne permet pas au Bureau d'engager des ressources – en particulier lorsqu'il s'agit de formuler une recommandation motivée – alors qu'il pourrait être établi en fin de compte qu'il n'était pas compétent.

(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:

- Un service social a exigé que le service responsable des successions et des mises sous scellés d'une commune lui révèle des informations issues d'un testament afin de procéder à l'examen des droits du concubin d'une personne défunte. Dans l'avis qu'il a émis à l'intention de l'autorité communale de surveillance, le Bureau parvenait à la conclusion que la loi sur l'aide sociale constituait une base légale suffisante pour la communication de ces informations.

- Les collaborateurs des organismes auxquels sont confiées des tâches publiques au moyen d'un mandat ou d'une convention de prestations sont soumis au secret de fonction. Tel est aussi le cas lorsque l'institution concernée a été nouvellement constituée comme entité de droit privé. C'est l'exercice de certaines fonctions de service public qui est déterminant pour la qualification de fonctionnaire au sens du code pénal, et non le droit du personnel applicable aux rapports de service.

- La plate-forme cantonale GERES est alimentée par les communes et exploitée par l'OIO, conformément à la loi sur l'harmonisation des registres officiels. Mise en place à l'origine par la Bedag pour le canton de Berne, elle a depuis 2015 été développée par l'association «GERES community», qui regroupe 16 cantons. Aussi bien le service compétent de l'OIO que les autorités de protection des données d'autres cantons ont, à plusieurs reprises, posé des questions juridiques au Bureau sur l'exploitation actuelle de la plate-forme et l'introduction des nouvelles normes nationales relatives aux interfaces (standards eCH). Le Bureau a relevé que, dans la banque de données GERES, seules les données pour lesquelles il existe une base légale peuvent être traitées. Selon lui, en outre, l'organisation des droits d'accès, en particulier aux historiques, doit respecter la protection des données et les données qui ne sont plus considérées par les communes comme devant figurer dans un registre doivent être effacées dans un délai de cinq ans.

- Un coach a demandé au Bureau d'examiner la question de la confidentialité dans le cadre des mesures du marché du travail (MMT). Il travaillait pour une entreprise privée qui, sur mandat du beco, propose des mesures du marché du travail pour la réinsertion de personnes sans emploi. Ses remarques ont poussé le Bureau à soumettre au beco des questions et propositions d'amélioration en vue de garantir la confidentialité. Ces démarches ont permis les éclaircissements et améliorations suivants: la présence d'une tierce personne, en vue de garantir la qualité, n'est requise que pour les coachings de candidature (et non plus pour les coachings de stabilisation), et seulement avec l'accord préalable des personnes concernées. Le formulaire utilisé pour établir le rapport final mentionne désormais que les informations doivent se limiter à ce qui est nécessaire et proportionné en vue de la réinsertion. Les personnes concernées sont informées dès le début de la remise de rapports à leur conseiller de l'orientation professionnelle. Elles peuvent prendre position sur le rapport final, dont elles obtiennent ensuite une copie. Les courriels qui contiennent des données particulièrement dignes de protection doivent désormais être chiffrés; si tel n'est pas le cas, les données doivent être envoyées par courrier postal. Les prestataires de MMT doivent en outre disposer de leur propre règlement sur la protection des données et pouvoir compter sur un responsable en la matière. Ces exigences font partie intégrante des contrats passés entre le beco et les prestataires de services.

- Un particulier a formulé une remarque qui a poussé le Bureau à se demander si les enve-

loppes utilisées par l'Administration des finances du canton de Berne pour l'encaissement des amendes étaient conformes aux exigences de la protection des données. Des tiers pouvaient en effet déduire, au vu de l'enveloppe, qu'il s'agissait d'une amende. Sur recommandation du Bureau, la pratique en matière d'envoi a été adaptée et les enveloppes portent désormais seulement une abréviation interne au canton.

- A plusieurs reprises, des particuliers ont posé des questions relatives à l'effacement des inscriptions dans les systèmes d'information de la police. Les délais varient de manière considérable en fonction du contenu et de l'avancée de la procédure et sont régis par des dispositions légales fédérales et cantonales. L'effacement de données est également possible sur demande, lorsque la conservation des informations pourrait avoir des conséquences négatives pour les personnes concernées, par exemple lorsque celles-ci ont été acquittées. Dans tous les cas, le Bureau renseigne sur la procédure et les droits. Une demande de destruction de données nécessite en général le dépôt préalable d'une demande de renseignements et de consultation.

- Dans une commune, plusieurs centaines de personnes ont signé une pétition contre la construction d'une halle d'engraissement. La commune a transmis les signatures aux principaux intéressés. Par la suite, les pétitionnaires ont subi des pressions, à titre personnel. C'est pourquoi l'une des personnes concernées a demandé conseil au Bureau. La liberté de pétition, qui est garantie par la Constitution, accorde à toute personne le droit d'adresser une pétition aux autorités *sans encourir de préjudice*. Le Tribunal fédéral a confirmé que la liberté de pétition permet d'adresser des demandes, des propositions, des critiques ou des plaintes à des autorités sans que leurs auteurs doivent craindre d'être harcelés ou de subir des préjudices juridiques d'une quelconque nature. La commune est par conséquent tenue de traiter les données relatives aux pétitions de manière confidentielle. Elle ne peut les utiliser pour des prises de contact ultérieures. En tant qu'expression d'un engagement politique, ces informations constituent en outre des données particulièrement dignes de protection, qui ne peuvent être transmises qu'en présence d'une base légale formelle. La transmission des données par la commune constituait par conséquent une violation de la protection des données.

- Un établissement d'hôtellerie et de restauration a demandé au Bureau s'il était possible de numériser les documents d'identité des clients de l'hôtel au lieu de les photocopier. Le contrôle des clients est régi par la loi sur l'hôtellerie et la restauration et les instructions de la Direction de l'économie publique qui s'y rapportent. Les indications qui doivent être demandées aux hôtes hébergés y sont énumérées de façon exhaustive. Il s'agit des nom et prénom, adresse, date de naissance et nationalité. Dans le cadre du contrôle des clients, les établissements d'hôtellerie et de restauration ne peuvent par conséquent ni copier ni numériser les documents d'identité des clients. Il revient au PFPDT de déterminer si une telle pratique est admise dans le cadre des contrats d'hébergement de droit privé.

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.

7.2 Législation cantonale

- Dans le cadre de la procédure de corapport relative à la modification de la loi sur les constructions visant à introduire des procédures électroniques d'octroi du permis de construire et d'édiction des plans (eBUP), le Bureau a constaté que le canton de Berne, contrairement à d'autres cantons qui recourent déjà à de telles procédures, prévoit que le dépôt public aura désormais lieu sur Internet, ce qui implique la publication de toutes les demandes de permis de construire concernées en ligne. A cet égard, des questions relatives à la protection des données peuvent se poser, notamment lorsque les données personnelles devant être publiées sont particulièrement dignes de protection. Etant donné qu'à l'avenir les requérants n'auront plus le choix entre la forme électronique et la forme papier, il convient de leur offrir la possibilité d'exclure certains documents de la publication sur Internet ou d'anonymiser certains passages, si la publication ne peut être restreinte.

- Suite à la modification de la loi sur le personnel, les litiges en matière de responsabilité, s'agissant des organisations privées qui fournissent des prestations sur mandat du canton, sont désormais exclusivement soumis à la juridiction civile. Le Bureau a proposé de prévoir une exception contraire et d'abandonner le versement de dépens à la partie adverse dans les litiges en matière de responsabilité qui concernent des hôpitaux, des maisons de naissance et des services de sauvetage répertoriés. En effet, sans une telle exception, les risques financiers

pour les personnes qui font valoir la responsabilité de l'Etat en raison d'une infraction au droit de la protection des données sont très importants, et les personnes concernées risquent bien souvent de renoncer à porter plainte.

- Le Bureau a également pris position sur une autre révision prévue de la loi sur le personnel. Celle-ci crée des bases pour le traitement de données personnelles liées à l'utilisation de l'infrastructure électronique de l'administration, par exemple la téléphonie et l'utilisation d'un poste de travail informatique. A cet égard, le Bureau avait déjà exigé à plusieurs reprises qu'une base légale claire soit prévue, notamment dans le cadre du contrôle préalable relatif au projet d'harmonisation de la téléphonie. Il s'inquiétait en particulier du fait que l'enregistrement et l'évaluation de telles données implique toujours le traitement de données particulièrement dignes de protection, que des profils personnels sont créés et qu'il est ainsi possible de tirer des conclusions sur le comportement au travail des utilisateurs. Et ces tendances prennent de l'ampleur. Le Bureau a examiné si le projet règle de manière suffisante du point de vue du contenu, du but et de l'étendue les atteintes graves portées au droit fondamental à la protection des données qu'il implique et si le principe de la proportionnalité est respecté.

- Le Bureau a participé au groupe de travail chargé de l'élaboration d'une nouvelle loi sur les fichiers électroniques de données personnelles. Cette loi doit d'une part remplacer la loi actuelle sur l'harmonisation des registres officiels et d'autre part constituer une base légale pour la création de nouveaux fichiers de données personnelles. Le Bureau a prêté une attention particulière aux exigences devant être remplies pour le traitement de données particulièrement dignes de protection dans le cadre d'une procédure d'appel. Les travaux législatifs seront poursuivis en 2018.

- Dans le cadre de la procédure de corapport relative à la révision de la loi sur l'aide sociale, le Bureau a relevé qu'il convenait de préciser le terme d'anonymisation, s'agissant de la livraison de données de l'aide sociale aux organismes et aux fournisseurs de prestations de la SAP.

- Suite à la révision de l'ordonnance cantonale contre les épizooties, ce sont désormais les communes qui doivent tenir les registres des chiens et de leurs propriétaires. L'ordonnance règle l'accès des autorités et des particuliers aux données. Elle prévoit qu'une liste des organisations de protection des animaux, refuges pour animaux et cabinets vétérinaires indiquant l'étendue de leurs droits de consultation soit publiée sur Internet.

- Le Bureau a pris position sur le projet d'ordonnance sur les technologies de l'information et de la communication de l'administration (OTIC), qui concerne le pilotage et la responsabilité des services informatiques de base (cf. ch. 1.1).

8 Surveillance et décisions de justice

8.1 Recommandations motivées concernant le projet BE-GEVER GAE (application Axioma)

Le projet informatique BE-GEVER GAE, qui concerne toute l'administration cantonale, est en procédure de contrôle préalable depuis le printemps 2016 (cf. ch. 5.1). En plus du concept d'entreprise, divers modèles destinés aux futurs mandants (offices ou Directions) ont été soumis au Bureau. La Chancellerie d'Etat a introduit BE-GEVER GAE en tant que projet pilote (sous-projet) et est ainsi passée au bureau sans papier. En l'absence d'une double authentification et d'une signature électronique, les documents traités n'ont pas la force probante nécessaire pour garantir le suivi de l'activité de l'Etat. La Chancellerie d'Etat a rejeté une recommandation motivée du Bureau, qui demandait de combler ces lacunes. Le Bureau a par conséquent formé un recours de droit administratif.
En 2017, le Bureau a déduit des bulletins d'information de l'OIO que la Direction des Finances était la première à avoir introduit GEVER GAE dans tous ses offices. Se fondant pour l'essentiel sur les mêmes arguments que ceux qu'il avait présentés à la Chancellerie d'Etat, le Bureau a formulé des recommandations à l'intention de ces offices (sauf l'OIO), en tant qu'autorités responsables. Il a demandé que les documents SIPD nécessaires lui soient remis dans les délais et qu'une procédure d'identification avec double authentification (qui soit suffisante, au vu de l'état de la technique) soit mise en place aussi rapidement que possible. Dans l'immédiat, il a exigé que tous les documents enregistrés dans BE-GEVER requièrent une signature électronique, jusqu'à l'introduction de la double authentification. Enfin, il a précisé que, dans l'intervalle, les collaborateurs qui, faute de moyens techniques suffisants, ne peuvent recourir à la signature électronique doivent continuer de documenter l'activité de l'Etat sur papier.
La Direction des finances s'est saisie de la procédure. Elle a donné suite aux recommandations, pour ce qui est du dépôt des documents SIPD, et décidé de suspendre le reste jusqu'au jugement entré en force du Tribunal administra-

tif relatif à l'introduction du projet GEVER GAE (sous-projet) par la Chancellerie d'Etat. Le Bureau a formé un recours de droit administratif contre sa décision.

8.2 Consultation de la «watchlist»

Un détenu a demandé à consulter la «watchlist» dans son intégralité. Cette liste, tenue par le chef de l'Office de l'exécution judiciaire (OEJ) depuis 2013, recense toutes les personnes internées ou considérées à risque car l'infraction commise a suscité un intérêt médiatique particulier. L'inscription d'une personne sur cette liste implique qu'un allégement de sa peine ne peut lui être octroyé qu'avec l'accord du chef de l'OEJ. Le requérant a pu consulter les données le concernant mais il n'a pas eu accès aux données anonymisées des autres personnes se trouvant sur la liste. Il a fait appel au Tribunal fédéral, faisant valoir que le rejet de sa demande de consultation était arbitraire.
Le Tribunal fédéral a rejeté le recours. Selon lui, l'instance précédente n'a pas violé le droit fédéral en considérant que les intérêts publics de la protection des données avaient plus de poids que le droit à l'information du recourant. Il a précisé qu'il ne suffit pas de masquer les noms des personnes concernées pour dissimuler leur identité, d'autant plus que le recourant exécute une peine avec plusieurs de ces personnes. Il a en outre estimé qu'il n'était pas nécessaire d'examiner la légalité de la «watchlist», étant donné qu'elle ne faisait pas l'objet du litige.
Dans deux autres cas, des détenus ont exigé que leur nom soit retiré de la liste, au motif que le retentissement médiatique n'est pas proportionnel à la dangerosité de l'auteur d'une infraction. La Cour Suprême a estimé que la «watchlist» n'était pas opportune ni nécessaire et qu'elle ne respectait pas le principe de la proportionnalité. Ses arguments reprenaient pour l'essentiel ceux du Bureau (cf. rapport de 2016, p. 10 s.). Les raisons pour lesquelles certaines personnes éveillent un intérêt de la part des médias et d'autres non ne sont pas transparentes, selon la Cour Suprême. La POM a par conséquent abandonné la tenue de sa liste.

8.3 Annonce d'une incapacité à conduire à l'autorité compétente en matière de circulation

En cas de doute sur les capacités physiques ou psychiques de l'assuré à conduire un véhicule motorisé en toute sécurité, l'office AI peut signaler l'assuré à l'autorité cantonale compétente en matière de circulation. Dans la procédure de recours administratif, c'est le tribunal saisi qui peut le faire (effet dévolutif), et ce en particulier dans les cas où des doutes sérieux surviennent pour la première fois durant la procédure judiciaire. Dans le cas concret, le tribunal a notifié son jugement à l'Office de la circulation routière et de la navigation du canton de Berne, après que la recourante avait exprimé, selon un rapport établi par l'hôpital, qu'elle voulait se blesser ou blesser quelqu'un d'autre pour pouvoir trouver la paix. Selon ce rapport, des voix intérieures lui auraient suggéré d'éteindre les phares de sa voiture alors qu'elle conduisait dans l'obscurité.

8.4 Consultation du registre d'impôt

Une personne qui demandait à consulter les données fiscales de personnes riches, imposées d'après la dépense dans l'Oberland bernois, a obtenu gain de cause devant le Tribunal fédéral, comme tel avait déjà été le cas devant le Tribunal administratif. Les deux instances sont parvenues à la conclusion que la disposition de la loi sur les impôts en vigueur jusqu'à la fin de 2015 était applicable et qu'elle devait être interprétée en ce sens que le registre d'impôt est pleinement public. L'une des personnes concernées a exigé que ses données soient bloquées mais cela n'a eu aucun effet, étant donné que l'autorité fiscale est tenue par la loi de communiquer les données. Selon le tribunal, les renseignements demandés ne constituaient en outre pas des données personnelles particulièrement dignes de protection, raison pour laquelle l'atteinte que constitue leur communication devait être qualifiée de peu sévère. C'est seulement avec la révision de la loi sur les impôts que le canton de Berne a décidé que la personne demandant la consultation devrait établir qu'elle a un intérêt économique pour obtenir des données fiscales.

8.5 Recommandation motivée contre l'accès des SPU SA à des données personnelles

Depuis leur autonomisation, du point de vue juridique, au 1er janvier 2017, les SPU SA peuvent accéder en ligne aux données de PERSISKA (système d'information sur le personnel du canton de Berne) préexistantes, en vertu d'une convention passée avec le canton. L'accès est limité aux données sur les salaires qui ont moins de cinq ans. Après son autonomisation, l'institution a estimé, se fondant sur une expertise, qu'elle n'était pas tenue d'inscrire ses données dans le registre cantonal des fichiers et de soumettre son système d'information sur le personnel à un contrôle préalable, étant donné que c'était la loi fédérale sur la protection des données qui s'appliquait.
L'accès électronique automatisé d'une entreprise privée au système PERSISKA doit être considéré comme une procédure d'appel. Etant donné que le système contient des données particulièrement dignes de protection, une telle procédure n'est admise que si elle se fonde sur

une base légale formelle. Or une telle base n'existe pas dans le cas présent. A cela s'ajoute le fait que les collaborateurs peuvent difficilement exercer les droits que leur garantit la loi fédérale sur la protection des données (p. ex. droit à la rectification et à la suppression des données), puisqu'en cas de litige ce sont des tribunaux civils qui sont compétents – avec les risques financiers que cela implique. Par conséquent, des intérêts publics et privés prépondérants s'opposent au maintien de cet accès en ligne. Conformément à la loi cantonale sur la protection des données, l'autorité qui est en mesure de communiquer les données est tenue, en l'occurrence, de le faire au cas par cas. C'est pourquoi le Bureau a formulé une recommandation motivée à l'intention de l'Office du personnel et lui a demandé de prendre les mesures qui s'imposent.

8.6 Notification de décisions de l'Intendance des impôts par voie électronique, décision de la Direction des finances

Depuis 2016, les contribuables ne peuvent plus recevoir leurs factures sous la forme électronique (e-factures) sur leur portail d'e-banking et les décisions et les décisions sur recours relatives à la taxation par courrier postal. Le Bureau a attiré l'attention de l'Intendance des impôts sur le fait que cette nouvelle pratique ne respecte pas les exigences en matière de protection des données. Les contribuables doivent donner leur consentement de manière séparée pour la notification par la voie électronique des factures d'une part et des décisions et décisions sur recours d'autre part. Le Bureau a demandé à l'Intendance des impôts, au moyen d'une recommandation motivée, de donner le choix aux contribuables de manière à ce que les prescriptions en matière de protection des données soient respectées. L'Intendance des impôts a rendu une décision de rejet par rapport à la demande du Bureau. Celui-ci a par conséquent déposé un recours administratif auprès de la Direction des finances, qui l'a rejeté. Le recours formé par le Bureau devant le Tribunal administratif est pendant.

8.7 Intervention de l'autorité de surveillance au sujet de la récupération d'un compte utilisateur

Une question adressée à la Bedag a révélé que le compte d'un collaborateur d'un office parti depuis longtemps à la retraite était encore actif. Les droits d'accès liés à ce compte permettaient de procéder à des évaluations spécialisées sur l'hôte. L'organisation des droits pour ce faire avait été difficile à mettre en place, raison pour laquelle les droits n'avaient pas été transmis à la personne ayant succédé au collaborateur retraité. Celle-ci travaillait simplement sur le compte de son prédécesseur et renouvelait sous son identité les mots de passe lorsque le système l'exigeait. Suite à l'intervention du Bureau, la direction de l'office a mis fin à cette pratique.

9 Collectivités de droit communal

(Cf. ch. 2.2, 4, 6, 7 et 8.4).

10 Points abordés dans le rapport précédent

(3: suivi des contrôles préalables effectués en 2016, 5: contrôles préalables effectués, 8.2: décisions judiciaires relatives à l'admissibilité de la «watchlist», 8.6: décision de la Direction des finances relative à un recours administratif sur la communication par voie électronique des décisions relatives à la taxation fiscale).

11 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.

12 janvier 2018

Le délégué à la protection des données: *Siegenthaler*

12 Annexe

12.1 Abréviations et désignations

ABR: Asile Bienne et région (association)
AI: assurance-invalidité
AXIOMA: logiciel de gestion des affaires de CMI Informatik AG
BCEE: Bourse cantonale des emplois de l'enseignement
Bedag (Bedag Informatique SA): entreprise fondée en 1990 et détenue par le canton de Berne
BE-GEVER: projet relatif à l'introduction d'un système de gestion des affaires en vue d'une gestion des affaires sous la forme électronique uniquement
BEJUNE: formes de collaboration contractuelles entre les cantons de Berne, du Jura et de Neuchâtel
BEKOS: projet informatique relatif à la coordination des institutions pédagogiques et sociopédagogiques cantonales de la SAP
BE-Print: infrastructure d'impression et de numérisation faisant partie des services informatiques de base proposés par l'OIO
BFH: Haute école spécialisée bernoise
Cf.: confer (voir)
Connectivité: en informatique, nature d'une connexion ou capacité d'un système à se connecter. Peut aussi se référer à la qualité d'une connexion à un réseau
Convention 108 du Conseil de l'Europe: convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, révisée en 2016
CP BE: Centre de puériculture du canton de Berne
CPM: Centre psychiatrique de Münsingen (devenu autonome au 1er janvier 2017 sous la forme d'une société anonyme)
Cyberrecrutement: procédure de candidature électronique
DEP: dossier électronique du patient: recueil d'informations pertinentes pour le traitement d'un patient ou d'une patiente
E-facture: facture électronique
EM (Electronic Monitoring): application permettant d'exercer une surveillance électronique en cas d'arrêt domiciliaire ou d'interdiction géographique
EMM: gestion de la mobilité d'entreprise
ESCADA/EVENTO: projet d'introduction d'un logiciel de gestion des écoles (niveau secondaire II)
FAQ: foire aux questions
FMI AG: hôpitaux de Frutigen, Meiringen et Interlaken
GAE: gestion des affaires et archivage électroniques
GELAN (acronyme de l'allemand Gesamtlösung EDV Landwirtschaft und Natur): système d'information agricole exploité conjointement par les cantons de Berne, Fribourg et Soleure.
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
GPS (Global Positioning System): système mondial de navigation par satellite indiquant la position et calculant la vitesse.
IBAS: système de calcul des besoins individuels
Impression suivie (*follow-me-printing*): mode d'impression des documents dans lequel tous les mandats d'impression sont envoyés à un serveur qui les transmet ensuite à l'appareil sur lequel un utilisateur s'identifie et exécute le mandat en question
ICI: Intendance des impôts
Informatique mobile: technologie permettant, au moyen d'un ordinateur ou d'autres appareils sans fil, de transmettre des données (notamment textuelles, audio ou visuelles) sans qu'un raccordement physique soit nécessaire. Par informatique mobile on entend principalement la communication mobile et les terminaux mobiles.
KSL: programme informatique de l'Université de Berne
LDEP: loi fédérale sur le dossier électronique du patient
Microsoft Office 365 (MS365): offre incluant les logiciels Office en ligne ainsi que d'autres services Internet sous la forme d'un abonnement mensuel ou annuel (ce qui permet de les utiliser depuis différents appareils) (d'après Wikipédia)
Migration: passage de l'état existant à un nouvel environnement technologique (d'après Wikipédia)
MMT: Mesures du marché du travail, par exemple développement et mise en œuvre de stratégies individuelles de candidature
Norme eCH: document accepté par l'association eCH qui fixe des règles, directives ou particularités relatives à des activités ou leurs résultats pour l'application générale ou réitérée. Il s'agit notamment de normes relatives à l'interopérabilité, de standards de procédure, de modèles de données conceptuels, de définitions de formats et de données, de précisions relatives aux normes internationales existantes et de descriptions de codes de bonne conduite qui peuvent être utiles dans le cadre de nouveaux projets de cyberadministration
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)
OEJ: Office de l'exécution judiciaire
OIO: Office d'informatique et d'organisation

Opt-in (de l'anglais «to opt», choisir): terme issu du domaine du «permission marketing» désignant une procédure dans laquelle une personne physique donne son consentement explicite et préalable à recevoir des prospections directes (le plus souvent par courriel, téléphone ou SMS). A l'inverse, le terme «Opt-out» est utilisé pour désigner une procédure dans laquelle, sans réaction de la part des personnes concernées, il est considéré qu'elles sont consentantes.
Optinomic: logiciel de l'entreprise Optinomic GmbH pour la saisie, la visualisation et l'analyse de données collectées en cours de processus (thérapeutique)
ORP: Office régional de placement
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
PGI: progiciel de gestion intégrée: désigne un logiciel destiné à la planification des ressources d'une entreprise ou d'une organisation
PHBern: Haute école pédagogique de Berne
PRIVATIM: association des Commissaires suisses à la protection des données
PTC 2.x: projet relatif au remplacement des postes de travail informatiques de l'administration cantonale (d'abord HCP puis PTC 2017)
Réforme européenne de la protection des données: le 14 avril 2016, le Parlement européen a approuvé une réforme de la protection des données. Le 4 mai 2016, le règlement général (règlement [UE] 2016/679) et la directive destinée à la police et aux autorités de justice pénale (directive [UE] 2016/680) sur la protection des données ont été publiés dans le journal officiel de l'Union européenne. Les Etats membres de l'UE disposent d'un délai de deux ans pour mettre en œuvre les dispositions de la directive dans le droit national (d'après Wikipédia).
RSE AG: hôpital régional de l'Emmental
SAP: Direction de la santé publique et de la prévoyance sociale
SIC: système(s) d'informations cliniques
SIP: système d'informations sur le personnel
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 (devenus autonomes au 1er janvier 2017 sous la dénomination «Réseau santé mentale SA»)
SPU SA: Services psychiatriques universitaires de Berne (devenus autonomes au 1er janvier 2017 sous la forme d'une société anonyme)
TI: technologies de l'information
TIC: technologies de l'information et de la communication
Traceur GPS: instrument qui permet le suivi GPS et l'enregistrement des trajets parcourus
TREE2: application informatique de l'Université de Berne pour un projet de recherche en sciences sociales
VIP (Very Important Person, personne très importante): en relation avec les systèmes d'informations cliniques, il s'agit des personnes particulièrement exposées, notamment les collaborateurs de la clinique qui s'y feraient traiter

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

8.1: Recommandation motivée 42 2016 6365 du 9 janvier 2017
8.2: Arrêt du Tribunal fédéral ATF 1C_111.2017 du 1er mai 2017
Arrêt SK 17 228 du 10 novembre 2017 de la 2ème Chambre pénale de la Cour Suprême
8.3: Jugement du Tribunal administratif JTA 200.2016.468 du 20 janvier 2017
8.4: Arrêt du Tribunal fédéral ATF 1C-447-449/2016 du 31 août 2017
8.5: Recommandation motivée 42.50-16.6462 du 1er décembre 2017
8.6: Décision 1301.07.00/16.000063/16.001643/Ca du 4 avril 2017 du directeur suppléant des finances

12.3 Sitographie et bibliographie

1.3: Motion Vogt 224-2016: http://www.gr.be.ch/gr/fr/index/geschaefte/geschaefte/suche/geschaeft.gid-94567e2995974f9c82bfde6720219d41.html
2.3: Rapport de gestion: http://www.fin.be.ch/fin/fr/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html
8.5: Astrid Epiney, Zur Abgrenzung des Anwendungsbereichs des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetze, en allemand, Jusletter du 2 mars 2015: http://doc.rero.ch/record/256921/files/Aufsatz146.pdf