Rapport d'activité 2016 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 2016 en bref

Les services de contrôle externes mandatés par le Bureau pour la surveillance de la protection des données (le Bureau) sont confrontés à divers environnements informatiques: ils ont ainsi dû examiner comment le CHR Frutigen Meiringen Interlaken (FMI AG) gère les droits et les accès à son SIC au moyen d'outils de la dernière génération (notamment utilisation de terminaux mobiles et accès externes). Les résultats ont, dans l'ensemble, été surprenants: les collaborateurs estiment que la solution informatique est facile d'utilisation, et ce aussi dans les situations d'urgence. Les exigences relatives à la prise en charge médicale, qui sont élevées, sont remplies. Les personnes chargées du contrôle ont en outre estimé que la solution informatique était satisfaisante du point de vue de la sûreté de l'information et de la protection des données (cf. ch. 4). La situation n'est pas la même s'agissant des grands projets informatiques de l'administration cantonale: le Bureau a formulé d'importantes réserves au sujet du futur poste de travail cantonal (PTC 2.0), du projet de gestion de la mobilité d'entreprise (EMM, qui concerne les terminaux mobiles utilisés par le canton) ainsi que du système de gestion des affaires et d'archivage BE-GEVER. Au moment de l'élaboration du présent rapport, la question de savoir si les problèmes pourront être résolus était encore ouverte (cf. ch. 5).

L'écart entre ces deux exemples s'explique en partie par le degré d'implication des responsables du domaine: au sein du CHR Frutigen Meiringen Interlaken, c'est un comité constitué de représentants de la direction, du corps médical et du service d'informatique qui a dirigé le projet. Les membres de la direction du projet sont également responsables de la gestion en bonne et due forme des données médicales. La situation est différente dans l'administration cantonale: les activités de l'Office d'informatique et d'organisation (OIO) exercent une influence considérable sur les projets liés à l'approvisionnement de base commun dans le cadre de l'élaboration de la nouvelle stratégie informatique du canton, sous la direction du comité stratégique TIC. Afin de garantir la protection des données, les responsables de domaine doivent être impliqués de manière accrue dans les projets liés à la mise en commun des services de base (cf. ch. 8.7 concernant la gestion des données secondaires de la téléphonie).

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 2016. Des collaborateurs du Bureau sont membres des groupes de travail «Santé» et «Technologies de l'information et de la communication» de PRIVATIM. Ce dernier s'est intéressé de manière approfondie à la thématique de l'informatique mobile et a rédigé un document de travail interne à cet égard. Le groupe de travail «Santé» a quant à lui consacré trois de ses séances à la législation fédérale relative au dossier du patient et rédigé une prise de position.

Le canton de Berne met à la disposition des particuliers intéressés les données du registre foncier sous la forme électronique. L'exploitation de l'infrastructure nécessaire à cet égard, qui est commune à plusieurs cantons, a été confiée à une entreprise privée. Les bureaux du registre foncier concernés ont fondé ensemble l'association TerrAudit en vue d'exercer la surveillance sur cette entreprise. Cette association mandate des tiers pour effectuer les contrôles. Des autorités de surveillance de la protection des données peuvent adhérer à TerrAudit. Le Bureau a renoncé à le faire pour éviter toute confusion entre les contrôles internes à l'administration et les contrôles indépendants.

1.3 Modifications intervenues dans le droit supérieur

Un groupe de travail de la Conférence des gouvernements cantonaux était en train d'élaborer, au début de l'établissement du présent rapport, un guide à l'intention des cantons indiquant les adaptations nécessaires dans les législations cantonales sur la protection des données. Une réforme européenne de la protection des données ainsi que la modernisation de la Convention 108 du Conseil de l'Europe sont à l'origine de cette démarche. Les cantons doivent en outre tenir compte de l'avant-projet de révision totale de la loi fédérale sur la protection des données. La loi sur la protection des données du canton de Berne devra être remaniée, probablement sous la houlette de la Direction de la justice, des affaires communales et des affaires ecclésiastiques (JCE). L'objectif est que l'acte législatif révisé entre en vigueur à l'automne 2018.

2 Descriptions des tâches, priorités, moyens à disposition

2.1 Priorités

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

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

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

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

– Subsidiarité de l'activité de surveillance: la législation sur la protection des données donne aux personnes concernées des moyens efficaces pour se défendre (celles-ci peuvent notamment demander la rectification ou la destruction de données personnelles et faire constater l'illicéité d'une publication). L'autorité de surveillance n'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 et renonce complètement ou partiellement à un examen 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 (objectifs de prestation), 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, bien qu'il soit renoncé à certains contrôles préalables, les responsables de projet veillent par eux-mêmes au respect de la protection des données. S'agissant des conseils dispensés et des interventions réalisées en qualité d'autorité de surveillance, l'accent est mis sur les évolutions techniques qui ont des conséquences particulières sur les droits de la personnalité. La direction du Bureau demandera une augmentation des ressources si des tâches supplémentaires sont confiées à ce dernier, par exemple en cas de cantonalisation, ou si des instances de contrôle estiment qu'une telle augmentation est nécessaire pour garantir l'accomplissement des tâches.

2.2 Responsabilité propre des services traitant les données

Le Bureau a pu sensibiliser les collaborateurs de la fondation Salome Brunner, qui s'occupe d'enfants et d'adolescents présentant des troubles du langage ou de l'audition, aux questions relatives à la protection des données dans le cadre d'un cours de perfectionnement destiné au personnel.
Les autorités de conciliation ont également organisé un cours de perfectionnement à l'intention du personnel du secrétariat.

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 à l'exploitation (dont CHF 128 mio destinés à des tiers prestataires de services). Ces chiffres ne concernent pas l'Hôpital de l'Ile ni les autres hôpitaux, également placés sous la surveillance du Bureau, ni les applications spécialisées qui ne sont pas gérées de manière centralisée.

Pour le contrôle des applications informatiques gérées par des services externes (cf. ch. 3), la somme prévue était de 176 000 francs.

Le Bureau disposait de 5,15 postes à temps complet (dont 0,2 pour le secrétariat) en 2016. Des informations complémentaires relatives au budget, aux comptes ainsi qu'aux objectifs (données financières) sont disponibles dans le rapport de gestion de 2016 du canton de Berne (volume I, ch. 11.3).

3 Contrôle des applications informatiques utilisées

Quatre audits ont été réalisés en 2016:

- Système d'informations cliniques du centre hospitalier régional (CHR) Frutigen Meiringen Interlaken (FMI AG, cf. ch. 1.1)

Au cours des dernières années, les responsables du CHR Frutigen Meiringen Interlaken (FMI AG) ont fourni de gros efforts dans les domaines de la sûreté de l'information et de la protection des données. La gestion des droits et des accès a notamment été professionnalisée et mise en œuvre dans toute l'institution. La tendance à l'utilisation de terminaux mobiles et à l'augmentation des accès externes a été identifiée suffisamment tôt; par conséquent, les questions y relatives ont pu être intégrées à la stratégie en matière de sécurité et les mesures nécessaires ont été prises. L'examen révèle que le CHR prend au sérieux les risques dans les domaines de la sûreté de l'information et de la protection des données et que ses efforts portent leurs fruits. Les lacunes constatées ont immédiatement été comblées et il a été tenu compte des remarques formulées dans les projets en cours. L'intérêt porté aux questions de protection des données et les compétences spécialisées du CHR Frutigen Meiringen Interlaken ont contribué de manière déterminante à l'efficacité et au succès de l'audit.

- APEA: contrôle de l'application spécialisée utilisée pour la gestion des dossiers des clients

Les autorités de protection de l'enfant et de l'adulte (APEA) traitent une grande quantité de données personnelles particulièrement dignes de protection. Dans le canton de Berne, elles sont au nombre de onze, et sont chargées chacune d'un arrondissement. A l'heure actuelle, tous les collaborateurs ont accès à tous les dossiers de tous les arrondissements (49 000 dossiers au total). Il est vrai que ces accès se fondent sur une base légale, mais le législateur fixe aussi des conditions afin de garantir la proportionnalité (le cercle des personnes bénéficiant d'un accès doit ainsi être restreint p. ex. aux personnes faisant partie du service de permanence et les accès doivent être journalisés). Ces conditions ne sont toutefois pas respectées dans la pratique. La disponibilité exigée de par la loi n'est pas non plus garantie: en cas d'urgence, il devrait être possible d'accéder en tout temps à un dossier. Pour des raisons économiques notamment, les conventions passées avec le fournisseur ne satisfont toutefois pas à ces exigences.
Les responsables des arrondissements des APEA sont les propriétaires des données des

clients et les bénéficiaires des prestations informatiques. A cet égard, ils sont dépendants du Service d'informatique de la JCE. Celui-ci reçoit des prestations de l'OIO pour ce qui touche à l'exploitation et des fournisseurs de logiciel en ce qui concerne les applications. L'OIO a lui-même délégué à la Bedag les tâches relatives à l'exploitation. Les APEA n'ont presque aucun contrôle ni aucune influence sur cette chaîne de prestations, étant donné qu'il n'y a pas de reporting leur permettant d'obtenir des informations claires. La question se pose dès lors de savoir dans quelle mesure les présidents des APEA peuvent assumer leurs responsabilités.
Le concept SIPD doit faire partie intégrante du contrat de prestations, afin que le fournisseur puisse prendre les mesures nécessaires à la mise en œuvre des exigences en matière de sûreté de l'information et de protection des données. Or, le concept SIPD relatif à l'application spécialisée utilisée pour la gestion des dossiers des clients n'a pas été intégré au contrat. Les APEA communiquent avec d'autres services par courrier postal, courrier électronique et télécopie. Dans certains cas, des données particulièrement dignes de protection sont envoyées par courriel sans avoir été cryptées. Les télécopieurs sont principalement utilisés comme appareils de réception.

- Contrôle des applications informatiques de l'Intendance des impôts (ICI)

L'examen a été réalisé en collaboration avec le Contrôle des finances. L'accent a été mis sur le traitement des données au moyen de l'application NESKO (taxation des personnes physiques); les conditions techniques et organisationnelles chez le destinataire des prestations (ICI), le mandant (OIO) et le prestataire (Bedag) ont été examinées. Le Bureau a évalué les aspects juridiques et contractuels alors que le Contrôle des finances s'est concentré sur les questions relatives à l'application et à l'organisation. Tous deux se sont fondés sur le concept SIPD élaboré et validé en 2016. Le rapport d'audit était encore en cours d'élaboration au moment de la rédaction du présent rapport.

- Contrôle des applications informatiques des écoles secondaires (ESCA-DA/EVENTO)

Le contrôle a été effectué en automne. Au moment de l'établissement du présent rapport, les résultats étaient en cours de vérification et d'évaluation. Le rapport sera terminé au cours du premier trimestre de 2017.

Suivi des contrôles effectués en 2015:

- Contrôle du point de vue de la protection des données de l'association Asile Bienne et région (ABR)

La direction a immédiatement pris les mesures exigées dans le rapport d'audit. Se fondant sur la norme ISO 2700x, elle a fait élaborer un concept SIPD et évaluer les risques. Il a été constaté que le mode d'exploitation actuel et l'infrastructure informatique existante ne pouvaient pas satisfaire aux exigences et devaient être conçus différemment. Un projet a été lancé et devrait bientôt être achevé.

- Examen de la protection de base de l'Université de Berne

Toutes les mesures qui devaient être prises suite au contrôle SIPD ont pu être mises en œuvre en 2016. L'audit est ainsi achevé.

4 Vidéosurveillance

- Plusieurs installations permettant de surveiller des bâtiments cantonaux ont à nouveau fait l'objet d'un contrôle préalable en 2016, notamment une caméra du centre pour le sport et les sciences du sport de l'Université de Berne (Zentrum für Sport und Sportwissenschaften) et plusieurs caméras de l'Hôpital de l'Ile. Les mesures de surveillance prévues se sont révélées adéquates. Etant donné que le personnel est soumis au secret professionnel médical, il a été exigé de l'Hôpital de l'Ile qu'il informe ses collaborateurs au moyen d'un mémento, d'une convention ou d'une directive les engageant à respecter la législation sur la protection des données s'agissant des installations de vidéosurveillance et du secret professionnel. Les caméras qui ne se trouvent pas dans les bâtiments de l'Hôpital de l'Ile librement accessibles et ne garantissent pas la sécurité mais assurent une fonction logistique dans l'intérêt des patients n'ont pas pu être autorisées sur la base de la loi sur la police. Les installations de surveillance en temps réel sont toutefois admissibles dans la mesure où elles permettent de garantir l'accomplissement des tâches prévues par la loi. Les enregistrements qui étaient planifiés dans des bâtiments de l'hôpital fermés la nuit ont en revanche été jugés inadmissibles. En effet, la vidéosurveillance assortie d'un enregistrement constitue une atteinte grave aux droits fondamentaux. Or il n'existe pas de base légale formelle pour autoriser ce type de surveillance dans les hôpitaux.

- L'organisation Jura bernois Tourisme a posé au Bureau diverses questions relatives à son projet d'installation de webcams panoramiques. Il était prévu de publier sur Internet les images filmées sur des places publiques, des entrées d'habitation, des esplanades privées, etc. Ces

images peuvent être agrandies, enregistrées, traitées et réutilisées individuellement. Les personnes et véhicules filmés peuvent ainsi être reconnus. Lorsque les images permettent de reconnaître des personnes, ces dernières doivent consentir à être filmées et autoriser la publication des images sur Internet. En outre, seules les autorités communales compétentes en vertu de la loi sur la police peuvent surveiller au moyen de caméras les lieux publics et librement accessibles de telle manière que des personnes soient reconnaissables, et ce pour des raisons de sécurité uniquement. Des webcams ne peuvent dès lors être installées que si elles sont configurées et placées de telle sorte que ni des personnes ni des plaques d'immatriculation ne soient identifiables et qu'elles ne puissent pas l'être après traitement des images.

- S'agissant de l'installation de caméras par des personnes privées sur l'espace public, cf. ch. 11.3.

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):

- En 2016, le Bureau a émis quatre prises de position sur le système d'informations cliniques de l'hôpital de l'Emmental. Il s'est, à cet égard, contenté d'évaluer la proportionnalité de l'organisation des droits d'accès. A l'heure actuelle, des explications doivent encore être fournies s'agissant des éventuels accès exceptionnels, notamment en cas d'urgence, ainsi que de la protection des personnes exposées telles que les collaborateurs.

- S'agissant du système d'informations cliniques du centre hospitalier régional de Haute-Argovie, une rencontre a eu lieu sur place. Une présentation du système a été organisée et les questions en suspens ont pu être discutées. Le Bureau a ensuite pu émettre sa première prise de position. Il a constaté que les droits d'accès sont trop développés.

- Après une longue période d'attente, les documents SIPD complets relatifs à l'application MC-SIS, utilisée pour le programme de dépistage de cancer du sein par mammographie dans le Jura bernois, lequel est dirigé par le Centre de dépistage du cancer du sein BEJUNE, ont été remis au Bureau. L'examen de ces documents a révélé que certaines améliorations doivent encore être apportées. Il manque notamment une description complète des flux de données, un schéma détaillé des rôles et des droits ainsi qu'une stratégie en matière de conservation et de radiation.

- S'agissant du contrôle préalable de l'application Optinomic du Centre de compétences pour l'être humain et ses dépendances Südhang, une rencontre a eu lieu sur place. Une présentation de l'application a été organisée et les incertitudes ainsi que la suite de la procédure ont pu être discutées. Le centre a ensuite soumis ses documents SIPD remaniés au Bureau. Celui-ci avait notamment demandé que les indications relatives à l'application Optinomic soient mises à jour (nouvelle version), que la matrice des droits d'accès soit précisée et clarifiée et qu'une stratégie en matière de conservation et de radiation soit établie.

- Les trois institutions psychiatriques ont été autonomisées au 1er janvier 2017. Malgré leur nouvelle forme juridique (société anonyme), elles restent soumises à la loi cantonale sur la protection des données. Du point de vue technique, cela 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. Du point de vue juridique, les nombreuses infrastructures et applications seront toutes soumises au contrôle préalable, puisque les données traitées dans ce domaine sont en règle générale particulièrement dignes de protection. Le Bureau a proposé qu'un concept SIPD commun soit élaboré pour tous les sites; celui-ci doit tenir compte des risques inhérents au domaine de la psychiatrie et décrire une protection de base adaptée. Cette solution aurait permis de réduire considérablement les charges liées au contrôle préalable des applications. Les institutions ont toutefois décidé d'élaborer un concept SIPD pour chaque site. Au moment de l'établissement du présent rapport, les Services psychiatriques Jura bernois – Bienne-Seeland (SPJBB) avaient déjà soumis leur concept SIPD. Le Bureau était en contact avec les deux autres institutions.
Depuis leur autonomisation, les institutions psychiatriques disposent aussi de leur propre système de gestion des données du personnel. A la demande de l'Office du personnel, le Bureau a examiné une convention réglant les conditions (notamment l'étendue et la durée, qui est de deux ans) auxquelles les institutions continuent d'avoir accès aux données du système d'informations personnelles du canton. Cette convention prévoit notamment que les institutions doivent soumettre leur système d'informations personnelles à un contrôle préa-

lable et qu'elles doivent annoncer leurs fichiers de données personnelles au registre des fichiers (cf. ch. 6 et 8.3).
Pour ce qui est du contrôle préalable du système d'informations sur le personnel (PIS) du Centre psychiatrique de Münsingen (CPM), le Bureau a déjà émis une première prise de position.

- Le CPM a reçu un retour au sujet de l'effacement définitif des données dans son SIC. D'ici à ce que les mesures décrites puissent être mises en œuvre, le CPM utilise une solution provisoire. Il convient de déterminer quels contenus constituent une preuve sûre de l'effacement des données. Si le procès-verbal est établi avec l'indication du nom du patient, le droit à l'oubli des personnes concernées n'est pas respecté.

- S'agissant du système d'informations cliniques Cariatides des SPJBB, le Bureau a émis une troisième prise de position. Celle-ci ne concerne pas les droits d'accès, étant donné que ces derniers ne pourront être organisés et décrits de manière à respecter les prescriptions relatives à la protection des données qu'une fois introduite la nouvelle version du système.

- Au cours de l'année sous rapport, le Bureau et les Services psychiatriques universitaires de Berne (SPU) ont à nouveau eu de nombreux échanges au sujet des questions encore en suspens relatives au système d'informations cliniques, et notamment de la fonction d'effacement. Les SPU ont revu l'organisation des droits d'accès et soumis au Bureau un concept SIPD remanié ainsi qu'une nouvelle matrice des droits d'accès. Le Bureau a ensuite émis une nouvelle prise de position et formulé un certain nombre de questions.

- S'agissant du contrôle préalable du système de décompte IBAS pour les personnes handicapées (solution web, crédit de réalisation de CHF 3,2 millions) de l'Office des personnes âgées et handicapées (OPAH), les documents SIPD ont été soumis au Bureau.

- Après un certain nombre d'échanges par écrit et une rencontre sur place, qui a permis de discuter les aspects peu clairs, l'Université de Berne a soumis au Bureau un concept SIPD simplifié relatif aux applications servant à la gestion des flux de créanciers.

- L'Université de Berne a déposé les concepts SIPD de deux projets informatiques (eForms et ZundL) en vue du contrôle préalable. Ceux-ci concernent d'une part l'introduction de formulaires électroniques à l'intention de l'administration et d'autre part la saisie du temps de travail et des prestations. Les deux applications sont exploitées dans l'infrastructure des services informatiques. Cela a considérablement facilité le contrôle préalable, puisque l'infrastructure des services informatiques avait subi un examen de la protection de base au cours de l'année précédente et qu'elle avait été jugée satisfaisante (cf. ch. 3). Les deux contrôles sont achevés.

- L'Université de Berne a fourni les précisions demandées au sujet de l'archivage et de l'effacement des données dans l'application Kernsystem Lehre (KSL), qui est utilisée pour le suivi électronique des examens, le répertoire électronique des cours et la gestion des auditoires.

- S'agissant d'UNICARD (carte de légitimation à puce pour les étudiants et les collaborateurs), la confirmation que les prescriptions en matière d'archivage sont mises en œuvre doit encore être apportée.

- L'Institut de médecine de premier recours de l'Université de Berne utilise une application web pour la gestion (en particulier attribution et décompte) des stages de médecine de premier recours, qui sont obligatoires pour les étudiants en médecine. Le Bureau a procédé à un examen rapide des documents qui lui ont été soumis. Il a demandé que les contrats passés avec les partenaires lui soient remis; ceux-ci devront encore être examinés de ponctuellement. Le Bureau a renoncé à examiner les aspects relatifs à la sûreté de l'information.

- Dans le cadre du contrôle préalable de l'application CASEnet, qui sert au suivi des dossiers (case management) des membres du corps enseignant de la Haute école pédagogique de Berne (PHBern), le Bureau a émis sa première prise de position. La PHBern a apporté les améliorations demandées aux documents SIPD dans les délais. Certaines questions relatives au schéma des rôles et des droits n'ayant pas été suffisamment éclaircies, le Bureau a demandé des explications complémentaires, qui lui ont été fournies oralement.

- Le projet informatique BEKOS (coordination des institutions cantonales pédagogiques et sociopédagogiques) de la Direction de la santé publique et de la prévoyance sociale (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. Le projet a entretemps été transféré aux services informatiques de la Direction de l'instruction publique (INS).

- Le Bureau a émis une deuxième prise de position dans le cadre du contrôle préalable du système d'informations financières ESAP de la

Haute école spécialisée bernoise (HESB) et de la PHBern. Une stratégie en matière d'archivage, qui indique, pour chaque phase, la durée de conservation des différents types de données dans le système et les personnes ayant accès à ces données, doit encore être établie.

- L'application Electronic Monitoring (EM) permet, en vertu du droit fédéral, 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). Dans le canton de Berne, un nombre limité d'appareils de surveillance sont actuellement en service. A l'avenir, la surveillance doit toutefois être étendue à l'ensemble de la Suisse. D'ici à 2017, le canton de Berne doit se raccorder au système de surveillance électronique du canton de Zurich. Les données collectées sont particulièrement dignes de protection. Le contrôle préalable a révélé que le service compétent a pris de nombreuses mesures, qui étaient nécessaires, dans les domaines de la sûreté de l'information et de la protection des données mais que d'autres questions et aspects devront encore être réglés en cas de raccordement au système zurichois. Le canton de Berne reste en effet responsable en cas de traitement des données par des tiers. En tant que partenaires externes, les tiers doivent respecter les prescriptions de la législation bernoise sur la protection des données. La question se pose par exemple de savoir si le recours à un suivi GPS est uniquement utilisé lorsque cela est nécessaire. Les critères autorisant une surveillance active (en temps réel) doivent être précisés, des informations relatives à la conservation et à l'élimination des données de la localisation doivent être apportées et l'accès des fournisseurs du logiciel externes aux données collectées doit être restreint.

- Le système d'information agricole GELAN 2015 remplace GELAN 2011. Il s'agit d'une application web dans laquelle les cantons de Berne, Fribourg et Soleure saisissent leurs données agricoles conformément au droit fédéral, en particulier toutes les données de calcul et les sanctions administratives. Les utilisateurs de cette application sont informés au moyen d'un mémento du fait qu'ils sont responsables du respect de la protection et de la sécurité des données. GELAN 2015 remplit les exigences en matière de sûreté de l'information et de protection des données. Le contrôle préalable a pu être achevé, sauf pour ce qui concerne la stratégie d'archivage et de radiation.

- Le «cyberrecrutement du canton de Berne» (système électronique de gestion des candidatures) a été soumis au Bureau en vue d'un contrôle préalable. Le produit choisi est utilisé par différents clients de droit public, notamment la Confédération et d'autres cantons. Si le canton offre un système de communication et de traitement des données, il est responsable de manière générale de la sécurité des données. Les questions relatives au fournisseur de la plateforme informatique externe et à la sécurité des données ont pu être éclaircies. Le fournisseur est contractuellement tenu de respecter les conditions générales du canton de Berne concernant la sûreté de l'information et la protection des données (CG SIPD). Les personnes déposant leur candidature sont informées de l'étendue et de la sécurité des traitements de données au moyen d'une déclaration.

- Le système de gestion des certificats offre aux services du personnel et aux supérieurs hiérarchiques des fonctionnalités permettant de générer des certificats de travail. Il est développé et exploité par la Bedag. Les certificats ne sont pas conservés dans le système. Une copie est déposée dans le dossier personnel.

- L'OIO a soumis au Bureau sa nouvelle solution pour les formulaires en ligne. Celle-ci met à la disposition de l'administration une solution uniforme pour élaborer des formulaires en ligne. Elle offre en particulier la possibilité de transférer des données cryptées et un accès sécurisé réservé aux personnes autorisées. Dans ce cas aussi, le respect des CG SIPD a été garanti par la signature d'un contrat.

- L'examen de l'outil statistique Scoppo a fourni les résultats provisoires suivants: partant du principe que le traitement des données en question se fonde sur une base légale, l'outil ne peut être utilisé que si les données ne sont pas particulièrement dignes de protection, que la protection de base est garantie par un contrat conformément aux CG SIPD et que l'élimination des données, une fois l'enquête achevée, est assurée. S'agissant des données particulièrement dignes de protection, les mesures SIPD pour une protection accrue doivent avoir fait l'objet d'un contrat et la preuve que ces mesures sont mises en œuvre doit être apportée dans un concept SIPD. A l'heure actuelle, il n'est pas possible de transférer de telles données sous une forme cryptée. Pour les enquêtes réalisées de manière anonyme, l'outil ne pourrait être utilisé que si l'anonymat est garanti.

- Le logiciel Octosam, qui a été soumis au Bureau, est un système de gestion des licences pour l'administration cantonale. Le contrôle préalable a révélé que les données collectées risquaient de comporter des informations précises sur les collaborateurs. Au niveau du canton, il serait ainsi possible de savoir qui (adresse IP) a

travaillé quand et combien de temps avec tel logiciel sous licence. La collecte de telles données en vue de connaître le comportement au travail constituerait une atteinte grave aux droits fondamentaux des collaborateurs. Une telle atteinte ne serait admissible que si une base légale formelle l'autorisait expressément.

- Le contrôle préalable du projet de gestion de la mobilité d'entreprise (EMM, gestion des terminaux mobiles) s'est révélé délicat. Le projet a, pour le Bureau, un caractère exemplaire puisque l'utilisation de terminaux mobiles est déjà largement répandue et qu'il convient de trouver des solutions réalistes et tournées vers l'avenir. L'infrastructure mobile doit pouvoir être exploitée de manière à la fois conforme à la loi et pratique pour les utilisateurs. C'est justement là que réside la difficulté: les mesures en matière de sûreté de l'information ne sont mises en œuvre que si elles sont pratiques pour les utilisateurs. Les questions de la séparation des données et applications privées et professionnelles, de l'utilisation de terminaux privés (Bring your own device, BYOD), du traitement de données particulièrement dignes de protection, de l'authentification sécurisée des utilisateurs, de la configuration et de la surveillance des terminaux (protection contre les virus, blocage, etc.) ainsi que de la diversité des équipements et des systèmes ont été abordées. Le contrôle préalable n'a pas encore pu être achevé (cf. ch. 1.1).

- Le projet BE-GEVER fait partie de l'approvisionnement de base commun (cf. ch. 1.1). Tout comme pour le projet de gestion de la mobilité d'entreprise, les unités administratives doivent désormais travailler avec ce système de gestion des affaires et d'archivage, dont l'exploitation est centralisée. Dans le cadre du contrôle préalable, deux aspects se sont révélés problématiques. D'une part, à 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. Cela signifie que le système journalise les modifications apportées aux documents et créé différentes versions en conséquence mais qu'il ne peut pas prouver avec une sécurité suffisante qui a fait les changements. Or l'action publique doit pouvoir être prouvée. Cela garantit en fin de compte que cette action n'est pas arbitraire. Sans une authentification satisfaisante, il n'est plus possible, une fois les dossiers papier abandonnés, de présenter des documents suffisamment solides. S'il n'est pas remédié à ce problème, BE-GEVER ne remplit pas les exigences en matière de protection des données pour ce qui est de l'exactitude des données. D'autre part, les mandants (unités administratives des Directions) doivent pouvoir classifier leurs données de manière autonome et attribuer les droits d'accès. Pour favoriser la collaboration, le système permet les échanges de documents entre mandants ou le classement commun de dossiers. Afin que des lacunes en matière de sécurité puissent être évitées, toutes les personnes concernées – y compris celles qui ne font pas partie de l'unité administrative – doivent utiliser la même échelle de classification. La question de savoir comment cette exigence peut être mise en pratique, étant donné que le canton ne dispose pas, contrairement à la Confédération, de prescriptions générales en matière de classification, n'a pas pu être éclaircie dans le cadre de la procédure de contrôle préalable.

- Les équipements informatiques des membres de l'administration doivent être remplacés (nouveaux clients, projet PTC 2.0, cf. ch. 1.1). Le système d'exploitation Windows 10 a été choisi. Des terminaux fixes et mobiles seront utilisés. Après un premier examen du concept SIPD, le Bureau a notamment constaté que les appareils doivent remplir des exigences plus élevées en matière de SIPD afin que des données personnelles particulièrement dignes de protection puissent être traitées de manière standard et que la question de la connectivité des appareils (notamment de leur intégration aux réseaux de communication) doit être prise en compte. Il a précisé que les appareils doivent être configurés de manière standardisée conformément aux codes de bonne conduite et qu'une surveillance doit pouvoir être exercée quant au respect de ces exigences. Les processus relatifs à l'installation de mises à jour pour la sécurité et l'assistance doivent en outre être définis à l'avance et respectés. Le contrôle préalable n'était pas encore achevé au moment de l'établissement du présent rapport.

En raison du manque de ressources, le Bureau n'a pas pu rattraper suffisamment le retard considérable qu'il a pris dans les procédures de contrôle préalable en cours. Le contrôle préalable du système de gestion des affaires AXIOMA des APEA, qui était encore en cours, a pu être achevé grâce à l'audit réalisé (cf. ch. 3). La plupart des nouveaux projets qui ont été soumis au Bureau ont pu être traités. Les temps de réponse ont toutefois été supérieurs aux objectifs fixés dans la majorité des cas.

(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:

- Il est en principe admissible, du point de vue de la protection des données, qu'un assureur veuille procéder au controlling des prestations au sein d'un hôpital et qu'il demande à cet égard que des documents médicaux détaillés lui soient fournis pour examiner un échantillon rétrospectivement. Cette manière de procéder se fonde sur une base légale suffisante et elle est confirmée par la jurisprudence du Tribunal fédéral. L'assureur peut demander toutes les informations qui sont, d'un point de vue objectif, nécessaires au controlling des prestations (caractère économique). A contrario, cela signifie toutefois que l'hôpital ne doit lui fournir que les documents nécessaires. L'assureur ne doit pas justifier en détail sa demande et il peut procéder à l'examen sur la base d'échantillons. L'hôpital peut cependant transmettre les informations demandées au service des médecins-conseils plutôt que directement à l'assureur. Les assurés disposent eux aussi de cette possibilité, dont l'assureur doit les informer.

- Si des institutions accomplissant des tâches publiques sont dissoutes, la question de la conservation ultérieure des données personnelles se pose. Bien souvent, les obligations en matière de conservation sont transférées aux ayants cause. Si aucune institution ne prend le relais, il convient de trouver un organisme responsable pour assurer la conservation. C'est souvent la «collectivité publique mère», c'est-à-dire la personne morale dont faisait partie l'institution dissoute, qui remplit ce rôle. Dans le cas où il n'y a pas non plus de «collectivité publique mère», une autre institution accomplissant des tâches de même nature peut être désignée organisme responsable. En l'absence d'une telle institution, les données devant être conservées peuvent être transmises aux Archives de l'Etat, même par les communes.

- Le Bureau a demandé à la SAP si, dans le cadre de la fusion du Spital Netz Bern AG et de l'Hôpital de l'Ile (groupe de l'Ile), la question du secret professionnel avait été traitée. Il a suggéré d'informer le public sur la gestion de la documentation des soins. Il y a un consensus pour dire que la documentation des soins ne peut être transmise par l'institution qui l'a établie à une autre institution (p. ex. issue d'une fusion) qu'avec le consentement de la personne concernée et que cette exigence doit se répercuter sur l'organisation des droits d'accès au SIC de l'institution en question.

- Lorsqu'une ancienne collaboratrice dénonce à l'Office des mineurs, en sa qualité d'autorité de surveillance, des dysfonctionnements au sein d'une crèche, la question se pose de savoir dans quelle mesure la directrice de cette crèche doit pouvoir consulter le dossier auprès de l'OM. En vertu du droit sur la protection des données, il doit être garanti que la directrice de la crèche peut consulter les informations qui la concernent ainsi que la crèche (personne morale). Il convient toutefois de vérifier qu'aucun intérêt public prépondérant ni aucun intérêt de tiers qui soit particulièrement digne de protection ne s'oppose à la consultation. Dans le cas précité, il s'agissait de déterminer s'il fallait indiquer qui était l'auteur de la dénonciation ou si des intérêts particulièrement dignes de protection s'opposaient à ce que son identité soit dévoilée. Selon la jurisprudence, l'identité ne doit pas être révélée lorsque la dénonciation présente un intérêt public, que le contenu de la dénonciation est fondé et que cela pourrait porter un préjudice à l'auteur de la dénonciation. Par préjudice on entend par exemple le recours à la violence ou des déprédations. Si l'on parvient à la conclusion que l'identité de l'auteur de la dénonciation ne doit pas être révélée, il convient de déterminer s'il suffit de masquer son nom ou si certains passages entiers doivent être cachés.

- Un particulier a demandé au Bureau d'examiner si la Caisse cantonale de chômage devrait utiliser, pour les courriers postaux destinés à ses assurés, des enveloppes sans mention explicite de l'expéditeur. Le Bureau est parvenu à la conclusion que, dans certaines situations, des tiers non habilités pourraient apprendre qu'une personne est au chômage en voyant l'enveloppe. Tout ce qui concerne les assurances sociales est soumis au secret lié aux assurances sociales, y compris le fait qu'une personne soit au chômage. Sur recommandation du Bureau, la Caisse cantonale de chômage a décidé d'utiliser des enveloppes neutres.

- Des particuliers ont adressé à diverses reprises des demandes de consultation de leurs données au Bureau. Dans de tels cas, il incombe à ce dernier d'indiquer aux personnes requérantes qu'elles doivent s'adresser directement aux autorités cantonales, communales ou fédérales qui ont traité les données en question. Les formulaires types disponibles sur les sites Internet du Bureau et du PFPDT constituent des aides précieuses à cet égard.

- A la demande de l'Intendance des impôts, le Bureau s'est demandé si les demandes de renseignements qui nécessitent de nombreuses copies doivent donner lieu à un émolument. Les travaux préparatoires relatifs à la législation sur la protection des données ont révélé que le législateur n'avait pas voulu, en 2008, consentir d'exception à l'exemption d'émolument. En cas de demande de renseignements abusive, il convient de la rejeter – et non de facturer un émolument.

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 aux textes d'application de la loi sur le dossier électronique du patient (LDEP), le Bureau a répercuté la prise de position de PRIVATIM.

7.2 Législation cantonale

- Suite à la révision de la loi sur le personnel ainsi que de la loi sur les soins hospitaliers, les prétentions en responsabilité contre les hôpitaux et les maisons de naissance répertoriés ainsi que les services de sauvetage doivent toutes être invoquées en application de la procédure civile. Cela accroît de manière très importante 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. Le Bureau part du principe que les patients renonceront à porter plainte dans cette situation. C'est pourquoi il a demandé que le versement de dépens à la partie adverse soit abandonné dans ces cas.

- Dans le cadre de l'élaboration du projet de nouvelle loi sur les Eglises nationales bernoises, le Bureau a fait partie du groupe d'experts et a soutenu, dans la procédure de corapport, la création d'autorités de surveillance de la protection des données indépendantes pour les Eglises nationales. S'agissant de la communication de données relatives aux patients des hôpitaux à des ecclésiastiques de leur Eglise, il a demandé que le principe selon lequel la personne concernée doit donner son consentement avant la communication soit respecté («opt in»). Les paroisses reçoivent des données étendues tirées des registres des habitants au sujet de leurs membres (ainsi que de leur concubin ou concubine et des enfants vivant dans le ménage commun), qui suffisent à l'accomplissement de leurs tâches administratives. La communication des listes de classe par les écoles, sur lesquelles figurent également des enfants sans confession, est par conséquent contraire au principe de proportionnalité.

- Dans le cadre du projet de loi sur l'exécution judiciaire, le Bureau a pu éclaircir de nombreuses questions relatives à la communication de données, à la vidéosurveillance, à l'utilisation de données GPS et à la procédure d'appel. Il a également pu apporter des précisions concernant notamment la base légale formelle nécessaire à la procédure d'appel, le respect des obligations particulières de garder le secret et les exigences posées à la vidéosurveillance. La surveillance généralisée des locaux de visite initialement prévue est contraire au principe de proportionnalité et inconciliable avec certains droits fondamentaux. Une surveillance n'est possible que dans des cas justifiés, et les personnes concernées doivent en être informées au préalable.

- Le projet de loi sur la police prévoit la transmission étendue de données entre autorités ainsi qu'entre autorités et privés dans les situations apparentées à des urgences. Le Bureau a relevé que cette mesure était contraire au principe de proportionnalité et qu'elle mettait en péril le respect des obligations particulières de garder le secret. Lorsque des mesures de police (notamment des surveillances) restreignent le droit fondamental à la protection des données, la protection juridique au sens des dispositions du Code de procédure pénale doit être suffisante. S'agissant des contrôles de sécurité relatifs à des collaborateurs, les bases légales nécessaires doivent être créées. La décision de renoncer à demander l'accord du Commandement de la police pour installer une vidéosurveillance d'un bâtiment cantonal ou communal constitue un retour en arrière.

Les communes ne disposent toujours pas de moyens efficaces pour se prémunir des enregistrements vidéo privés non autorisés dans l'espace public. La comparaison systématique de données électroniques relatives au nombre de nuitées est contraire au principe de proportionnalité.

- L'indication du statut, dans la solution de communication Skype for Business, désormais utilisée dans toute l'administration cantonale, permet de tirer des conclusions sur le comportement des collaborateurs, selon les paramètres définis. La Direction des finances a laissé entendre, au cours de la procédure de contrôle préalable, qu'elle établirait des lignes directrices et des conditions cadres à cet égard à l'occasion de la prochaine révision de l'ordonnance sur le personnel. Cela n'a pas été fait dans le cadre de la révision de 2016.

8 Surveillance et décisions de justice

8.1 Consultation de la «watchlist»

Le chef de l'Office de l'exécution judiciaire (OEJ) a élaboré une «watchlist» dans le cadre de la gestion des risques à l'interne. Toutes les personnes internées ou considérées à risque car l'infraction commise a – au moment-même de sa perpétration, au cours de la procédure ju-

diciaire ou du fait d'incidents dans le cadre de l'exécution – suscité un intérêt public ou médiatique particulier y figurent. Des allégements ne peuvent être octroyés aux personnes se trouvant sur la liste qu'avec l'accord du chef de l'office.
L'une des personnes concernées a demandé à consulter non pas uniquement les données à son sujet mais toute la liste, sous une forme anonymisée. Selon la décision sur recours rendue par la Direction de la police et des affaires militaires (POM), la consultation de données personnelles particulièrement dignes de protection appartenant à des tiers n'est admise que si elle a été prévue par la loi, que les personnes concernées ont donné leur consentement explicite ou que la consultation sert leurs intérêts.
La communication de données personnelles doit en outre être refusée, limitée ou liée à certaines conditions en présence d'intérêts publics majeurs ou d'intérêts privés nécessitant une protection particulière. Il ne suffit pas de masquer les noms des personnes concernées pour dissimuler leur identité. Les données qui restent visibles (p. ex. description des faits, délits ou sanctions prononcées) peuvent en effet permettre de trouver l'identité des personnes concernées – en particulier lorsque celles-ci ont apparu dans les médias. La «watchlist» permet de déterminer quelles sont les personnes qui doivent être impliquées dans les décisions d'allégement et ne constitue en aucun cas un outil de travail qui peut être utilisé à titre personnel exclusivement.

8.2 Droit d'accès et de consultation: modalités et étendue

Un étudiant de l'Université de Berne a demandé à consulter tous les dossiers de l'Université le concernant, sans préciser à quels fichiers de données il faisait référence ni où ceux-ci se trouvaient. L'Université lui a refusé l'accès à certaines données, notamment parce que la direction ne savait pas et ne pouvait pas savoir, moyennant un effort raisonnable, avec quelles unités organisationnelles de l'Université il avait eu des échanges.
Selon le Tribunal administratif, qui a été saisi, le droit d'accès et de consultation concerne des données qui ont été traitées dans un fichier. Un fichier contient les données de plusieurs personnes et est organisé de telle manière que les informations peuvent être retrouvées moyennant un effort raisonnable. Le support de données choisi, son affectation, sa structure, la durée et les modalités de la sauvegarde ne jouent aucun rôle.
Par ailleurs, les données qui n'ont pas été organisées sous la forme d'un fichier et n'ont pas d'affectation déterminée mais qui peuvent être retrouvées simplement au moyen du nom d'une personne sont aussi considérées comme des fichiers de données. En ce sens, la correspondance entre une autorité et une personne entre aussi dans cette catégorie.
En outre, l'autorité compétente doit s'organiser de telle manière qu'elle puisse répondre aux demandes de renseignements qui comportent peu de détails. Les exigences posées aux demandes de renseignements et de consultation ne doivent en principe pas être élevées. Aucune motivation n'est requise et les personnes concernées peuvent demander à obtenir des renseignements de manière générale ou à consulter tous les fichiers d'une autorité contenant des données les concernant.
Il suffit que l'identité de la personne requérante soit connue et que celle-ci souhaite obtenir des renseignements ou consulter des données qui ont été traitées dans un fichier. La personne requérante est tenue, en vertu du principe de la bonne foi, de fournir des indications aussi précises que possible en vue de faciliter la recherche.
L'étudiant, qui n'avait que partiellement obtenu gain de cause devant le Tribunal administratif, a saisi le Tribunal fédéral. Celui-ci a rejeté le recours, pour les points sur lesquels il est entré en matière.

8.3 Applicabilité du droit de la protection des données aux recueils de données personnelles

Pour des raisons de nature formelle, le Bureau n'a pas pu entrer en matière sur la demande d'un hôpital, qui souhaitait que son recueil de données personnelles soit retiré du registre des fichiers de données. En effet, la demande ne comportait pas de signature valable.
Se fondant sur une expertise (cf. ch. 11.3), l'hôpital estimait que la loi fédérale sur la protection des données s'appliquait au traitement des données de ses collaborateurs. C'est la raison pour laquelle il a déposé une demande auprès du Bureau. Celui-ci a constaté que, dans ce cas de figure, les litiges relatifs à la protection des données devaient être réglés par des tribunaux civils. Il a ajouté qu'en cas de demande d'effacement ou de rectification de données les collaborateurs couraient désormais le risque de devoir verser des dépens à la partie adverse. Selon lui, la protection juridique des demandes relevant de la protection des données et du droit du travail est, dans l'ensemble, moins bonne qu'auparavant. Ce ne sont pas seulement les collaborateurs de l'hôpital en question qui sont concernés, mais tous les employés des organismes de droit privé chargés d'accomplir des tâches publiques.

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

La Cour de droit social du Tribunal fédéral a estimé, dans une affaire touchant au principe de la publicité dans le canton de Zurich, que la surveillance des offices AI était exercée par le PFPDT – contrairement à ce qu'elle avait établi l'année précédente. Le Bureau continue quant à lui de partir du principe qu'il est compétent pour l'Office AI du canton de Berne. L'inconstance de la jurisprudence complique toutefois ses activités de surveillance.

8.5 Examen des accès aux données fiscales enregistrés du point de vue de la protection des données

La section taxe d'exemption du service d'administration de la taxe d'exemption du canton a accès aux données de l'Intendance des impôts. Les accès ne sont pas limités aux données nécessaires à l'accomplissement des tâches de cette section. Chaque collaborateur autorisé peut ainsi voir les données de toutes les personnes assujetties à la taxe. Ces données ne doivent toutefois être consultées que si l'accomplissement des tâches l'exige. Du fait que les droits ne peuvent pas être limités à titre préventif, l'Intendance des impôts doit journaliser les accès et consultations de données. Les accès peuvent ainsi être vérifiés a posteriori et des mesures peuvent être prises si nécessaire. Dans certaines circonstances, les collaborateurs peuvent ainsi être privés de leurs droits d'accès.

L'examen des données d'accès journalisées a révélé qu'un collaborateur du service d'administration de la taxe d'exemption du canton a consulté les données fiscales d'un ancien collaborateur, sans raisons de service. L'Office de la sécurité civile, du sport et des affaires militaires, qui est compétent en la matière, l'a entendu à ce propos et lui a donné un avertissement. Les collaborateurs seront à nouveau rendus attentifs, dans le cadre du système de contrôle interne, au fait que l'utilisation de l'application spécialisée de l'Intendance des impôts sans lien avec les affaires est problématique.

8.6 Notification des décisions de l'Intendance des impôts par la voie électronique: recommandation motivée

Depuis le 1er janvier 2016, les contribuables qui demandent à ce que leurs factures leur soient envoyées sous la forme électronique reçoivent également les décisions et les décisions sur recours relatives à la taxation sous cette forme. Désormais, ils reçoivent obligatoirement aussi ces décisions sur le portail d'e-banking de leur institut financier. Il n'est plus possible de recevoir les factures sous la forme électronique (e-factures) et les décisions (avec le décompte final des coûts) ainsi que 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. La notification combinée des factures et des décisions, sans le consentement explicite des personnes concernées, n'est admissible qu'en présence d'une base légale claire. L'Intendance des impôts a rendu une décision de rejet par rapport à la demande du Bureau. Celui-ci a par conséquent déposé, au début du mois de mai 2016, un recours administratif auprès de la Direction des finances. Au moment de l'établissement du présent rapport, ce recours était encore pendant.

8.7 Admissibilité de la conservation des données secondaires de la téléphonie

Le Tribunal fédéral a estimé que la loi fédérale sur la surveillance de la correspondance par poste et télécommunication constituait une base légale suffisante pour justifier l'atteinte considérable aux droits fondamentaux que constitue la conservation des données secondaires de la téléphonie (qui a téléphoné à qui, à quelles date et heure et pendant combien de temps). L'arrêt concerne la conservation des données secondaires par les prestataires de services de télécommunication. Fait nouveau, le canton de Berne a enregistré, au cours de l'année sous rapport, une quantité importante de données secondaires de la téléphonie. Cela est dû à la configuration par défaut du système de communication Skype for Business. En effet, si les paramètres ne sont pas modifiés, les données secondaires sont automatiquement sauvegardées dans un fichier se trouvant dans les archives de la boîte de réception électronique des utilisateurs. D'une part la durée de conservation maximale prévue pour les prestataires de services de télécommunication, qui est de six mois, n'a pas été respectée. D'autre part il n'existe pas de base légale. Il est logique que ce soient les autorités d'investigation et de poursuite pénale, qui sont responsables des prescriptions relatives à la collecte de donnée secondaires, qui aient souligné que cette manière de procé-

der n'était pas admissible. En sa qualité de propriétaire des données secondaires de la téléphonie des autorités judiciaires, la Direction de la magistrature est intervenue auprès de l'OIO. Celui-ci devrait, à l'avenir, mieux tenir compte de l'avis des services responsables du traitement des données en cas de modification de la configuration d'applications déjà utilisées dans le cadre de l'approvisionnement de base commun.

8.8 Acquisition d'un capteur IMSI: recommandation motivée

Les documents d'appel d'offres ont révélé que la Police cantonale avait l'intention d'acquérir un capteur IMSI pour un montant de 750 000 francs. Le Bureau a demandé, au moyen d'une recommandation motivée, que le traitement des données prévu lui soit soumis pour examen préalable. Pour des raisons de politique financière, la POM a par la suite renoncé à cette acquisition. Elle n'a pas rendu de décision de rejet en réponse à la recommandation motivée du Bureau.

9 Points abordés dans le rapport précédent

(3: suivi des contrôles préalables effectués en 2015, 5: contrôles préalables effectués. En 2016, une question posée par l'autorité de surveillance à une Direction a révélé que le système ne se bloquait toujours pas après cinq tentatives d'introduire un mot de passe erroné, contrairement à ce que prévoient les directives en matière de mot de passe.)

10 Proposition

Il est proposé au Conseil-exécutif et au Grand Conseil de prendre connaissance du présent rapport conformément à l'article 37 de la loi sur la protection des données.

30 janvier 2017

Le délégué à la protection des données: *Siegenthaler*

11 Annexe

11.1 Abréviations et désignations

ABR: Asile Bienne et région (association)
AI: assurance-invalidité
APEA: autorité de protection de l'enfant et de l'adulte
AXIOMA: logiciel de gestion des affaires de CMI Informatik AG
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
BFH: Haute école spécialisée bernoise
BYOD (Bring Your Own Device: «apportez vos appareils personnels»; en français, parfois PAP, abréviation de «prenez vos appareils personnels» ou encore AVEC, «apportez votre équipement personnel de communication»): pratique qui consiste à utiliser ses terminaux mobiles personnels (ordinateur portable, tablette, téléphone intelligent) dans un contexte professionnel (d'après Wikipédia)
Capteur IMSI: appareil permettant de lire le numéro IMSI (International Mobile Subscriber Identity, numéro unique qui permet d'identifier un usager) d'un téléphone mobile, sauvegardé dans la carte SIM, et de déterminer un périmètre dans lequel se trouve le terminal en question. Il permet aussi d'écouter les communications téléphoniques (d'après Wikipédia).
Case Management: suivi des cas
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
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
CPM: Centre psychiatrique de Münsingen
Cyberrecrutement: procédure de candidature électronique
E-facture: facture électronique
eForms: solution informatique de l'Université (formulaires interactifs)
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 (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
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
Fondation Salome Brunner: écoles logopédiques de Wabern, Bienne et Langenthal ainsi qu'école de pédagogie curative de Wabern (environ 150 collaborateurs au total)
GELAN (acronyme de l'allemand Gesamtlösung EDV Landwirtschaft und Natur): système d'information agricole exploité conjointement par les cantons de Berne, Fribourg et Soleure.
GPS (Global Positioning System): système mondial de navigation par satellite indiquant la position et calculant la vitesse.
IBAS: système de calcul des besoins individuels
ICI: Intendance des impôts
ISO: Organisation internationale de normalisation
ISO 2700x: suite ou famille de standards comprenant les normes de sécurité de l'information (d'après Wikipédia)
LDEP: loi fédérale sur le dossier électronique du patient
MC-SIS (Multi Cancer Screening Information System): logiciel actuellement utilisé pour les programmes de dépistage du cancer du sein
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.
MDM (Mobile Device Management): gestion de terminaux mobiles (GTM)
NESKO: système informatique de l'Intendance des impôts, servant à la taxation et à la perception
Octosam (OctoSAM Inventory): logiciel de l'entreprise Octosoft qui permet de dresser l'inventaire des ordinateurs sur le réseau et donne des informations sur l'utilisation des logiciels installés
OIO: Office d'informatique et d'organisation
OPAH: Office des personnes âgées et handicapées
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)

Optinomic: logiciel de l'entreprise Optinomic GmbH pour la saisie, la visualisation et l'analyse de données collectées en cours de processus (thérapeutique)
PFPDT: préposé fédéral à la protection des données et à la transparence
PHBern: Haute école pédagogique de Berne
PRIVATIM: association des Commissaires suisses à la protection des données
PTC 2.0: 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
Skype for Business (nouveau nom de la plateforme Microsoft Lync): application de Microsoft qui réunit en un seul environnement différents moyens de communication (notamment téléphonie IP, vidéoconférence et messagerie vocale). Tous les utilisateurs disposent d'informations sur la disponibilité des autres participants (présence, inactivité, durant un certain temps, du clavier et de la souris). L'introduction de cette application dans l'administration cantonale a eu lieu dans le cadre du projet HarmTel.
SPJBB: Services psychiatriques Jura bernois – Bienne – Seeland
SPU: Services psychiatriques universitaires
TerrAudit: association fondée par les bureaux du registre foncier des cantons de Berne, de Soleure, des Grisons et du Tessin en vue de la coordination intercantonale des contrôles de plateformes de données et de la collaboration entre autorités dans le domaine du registre foncier
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
UNICARD: carte de légitimation à puce des étudiants et collaborateurs de l'Université de Berne (format carte de crédit) utilisée notamment à la bibliothèque, comme moyen de paiement et comme badge d'accès
ZundL: projet relatif à la saisie du temps de travail et des prestations

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

8.1: Décision de la Direction de la police et des affaires militaires BD 260/15 Ho du 7 septembre 2016
8.2: Jugement du Tribunal administratif JTA 100.2015.204U du 18 avril 2016; arrêt du Tribunal fédéral ATF 1C_200/20161 du 12 août 2016
8.3: Décision du Bureau pour la surveillance de la protection des données du canton de Berne du 27 janvier 2016
8.4: Arrêt du Tribunal fédéral ATF 9C_36/2016 du 16 février 2016
8.5: Intervention de l'autorité de surveillance 42.72-13.6362 du 10 mars 2016
8.6: Recours administratif 42.72-15.6279 du 4 mai 2016
8.7: Arrêt du Tribunal administratif fédéral A-4941/2014 du 9 novembre 2016

11.3 Sitographie et bibliographie

1.3: Communiqué du Conseil fédéral relatif à la révision de la loi fédérale sur la protection des données et aux réformes européennes: https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-56764.html
2.3: Rapport de gestion: http://www.fin.be.ch/fin/fr/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html
4: Liz Fischli-Giesser: Private Videoüberwachungen im kommunalen öffentlichen Raum, KPG-Bulletin (bulletin du groupe d'aménagement cantonal, en allemand) de mars 2016
8.3: 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