Rapport d'activité 2013 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 2013 en bref

Au cours de l'année écoulée, le Bureau pour la surveillance de la protection des données (le Bureau) s'est beaucoup occupé des grandes banques de données en réseau. Pour ne citer qu'un exemple: l'Office d'informatique et d'organisation (OIO) rassemble dans la plate-forme GERES toutes les données contenues dans les registres du contrôle des habitants. Une commune a demandé à l'OIO comment elle devait enregistrer les personnes d'appartenance religieuse musulmane. Elle ignorait que, conformément aux bases légales fédérales et cantonales, seule l'inscription de l'appartenance à l'une des quatre communautés religieuses reconnues de droit public par le canton est admissible. L'OIO a informé le Bureau de la demande de la commune. Celui-ci a saisi l'occasion pour demander des informations sur les appartenances religieuses inscrites dans GERES. Il s'est avéré que, pour plus de 200 000 personnes, des désignations qui ne sont pas admissibles avaient été saisies, indiquant que la personne concernée n'appartenait à aucune communauté religieuse (athée) ou qu'elle appartenait à une communauté non reconnue de droit public. Dans la plupart des cas, il n'était pas possible de savoir à quelle communauté religieuse appartenait la personne concernée. Certaines communes avaient toutefois inscrit des renseignements détaillés sur l'appartenance religieuse (24 codes ont été identifiés en tout, p. ex.: quaker). Le Bureau a demandé aux autorités communales de surveillance en matière de protection des données de veiller à ce qu'il soit remédié à cette situation et d'attribuer un seul et même code à toutes les personnes n'appartenant pas à une communauté religieuse reconnue par le canton. Or, cela n'a pas été sans conséquence: le système d'imposition à la source de l'Intendance des impôts, qui se fonde sur les informations de la plate-forme GERES, a interprété certains codes comme signifiant que la situation devait être éclaircie et que la personne concernée devait dans l'intervalle être exemptée d'impôt en général (et non pas seulement d'impôt paroissial). L'Office fédéral de la statistique a déploré la perte d'informations importantes du point de vue statistique. Les autorités de protection de l'enfant et de l'adulte (APEA) avaient demandé à avoir accès aux informations relatives à l'appartenance religieuse dans GERES; il a été décidé que leur demande devait être rejetée, puisque les informations souhaitées ne figureraient de toute façon plus dans GERES à l'avenir.

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 2013. Des collaborateurs du Bureau sont membres des groupes de travail «Santé» et «Technologies de l'information et de la communication» de PRIVATIM. Les membres du groupe de travail «Santé» ont posé en 2013 les jalons pour l'élaboration d'une brochure relative aux dossiers médicaux des patients (anamnèse) ainsi qu'aux mesures qui doivent encore être prises pour que le canton puisse examiner les factures des hôpitaux pour les traitements dispensés dans des institutions (conformément aux nouvelles dispositions sur le financement hospitalier, le canton assume 55 % des frais liés à ces traitements). La brochure pourra être adaptée en fonction des spécificités cantonales. (S'agissant de l'envoi de l'aide-mémoire de PRIVATIM aux autorités communales de surveillance en matière de protection des données, cf. ch. 6 et 9).

2 Description des tâches, priorités, moyens à disposition

2.1 Priorités

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

- 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 pos-

sibilités 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.

- 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.

– 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.

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

– 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.

– 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.

2.2 Responsabilité propre des services traitant les données

L'engagement considérable des participants aux cours organisés par les associations communales, par exemple au cours portant sur la mise en œuvre du manuel «Echanges d'informations entre les autorités», a été relevé.

Les personnes concernées ne peuvent défendre leurs droits que si elles sont en mesure de trouver facilement quelle est l'autorité de surveillance de la protection des données compétente. On peut mentionner à titre d'exemple la présentation du site Internet de la commune de Worb.

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

En 2013, le budget attribuait, pour l'administration cantonale, CHF 49 millions aux investissements dans le domaine informatique et CHF 157 millions à l'exploitation (dont CHF 113 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. 2.4), la somme prévue était de CHF185 000.

Le Bureau a disposé de 4,7 postes à temps complet (dont 0,7 pour le secrétariat). Des informations complémentaires relatives au budget, aux comptes ainsi qu'aux objectifs de NOG (données financières) sont disponibles dans le rapport de gestion de 2013 du canton de Berne (volume I).

3 Contrôle des applications informatiques utilisées

Quatre audits ont été réalisés en 2013:

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

Les services informatiques centraux assurent les services informatiques de base de l'Université de Berne (services de messagerie, services Internet, administration des étudiants, gestion des ressources, etc.). Dans le but d'accroître l'efficacité des prochains contrôles préalables, le Bureau et la direction informatique sont tombés d'accord pour réaliser un examen de la protection de base conformément à la norme ISO 27000. L'établissement d'un catalogue d'examen adapté a constitué un investissement important pour l'Université.
L'examen réalisé sur place a montré que les services informatiques centraux exploitent de manière professionnelle une infrastructure informatique complexe et hétérogène. Du fait de l'importante diversité, les ressources mobilisées pour la mise à jour et la documentation des systèmes sont considérables. Il a été constaté qu'il est nécessaire de prendre des mesures dans ce domaine.

- Bureau d'encaissement des amendes:

Au cours de la procédure d'encaissement, des informations sont échangées entre plusieurs instances par l'intermédiaire de plusieurs systèmes. Les collaborateurs ont – au vu des tâches qu'ils assument – des droits d'accès disproportionnés aux données figurant dans le système de contrôle des affaires des tribunaux. Depuis l'introduction de ce système, aucune entrée n'a été effacée. Une stratégie de radiation doit être définie ou des prescriptions doivent être établies. L'absence d'annonce active lorsqu'un débiteur retardataire a effectué un paiement constitue une faiblesse de la procédure.
Dès 2014, le bureau d'encaissement des amendes ne dépendra plus, d'un point de vue organisationnel, de la Direction de la justice, des affaires communales et des affaires ecclésiastiques (JCE) mais sera rattaché à la Direction de la magistrature. Celle-ci était présente au moment de la présentation du rapport d'examen.

- Clinique Südhang:

La clinique Südhang soigne les personnes dépendantes à l'alcool. En tant que fondation, elle assume une tâche conformément à la législation sur la santé publique. Les données personnelles particulièrement dignes de protection sont traitées de manière responsable. La direction impose des processus et des structures clairs. Un spécialiste affilié à la clinique s'occupe de l'infrastructure informatique interne. Il se charge également de l'administration des droits d'accès. Les applications et les serveurs sont en revanche exploités par un prestataire externe. Les conventions de prestations passées avec ce dernier sont bien claires.
Des manquements ont toutefois été constatés s'agissant de la conservation des données: il n'est pas fait de distinction entre les dossiers activés et les dossiers désactivés et aucune stratégie de radiation et d'archivage n'est définie. Pour ce qui est des échanges de courriels, un cryptage doit être introduit, par exemple en utilisant le service «HIN Mail», qui est largement répandu dans le secteur de la santé.

- Taxe d'exemption de l'obligation de servir:

L'application ATEO (application pour la taxe d'exemption de l'obligation de servir) est gérée par une entreprise externe et exploitée dans un centre de calcul externe (Abraxas Informatik AG). C'est seulement après une intervention énergique de la direction de l'office que les personnes chargées de l'examen ont obtenu les droits d'accès à l'application et aux systèmes. Les processus sont bien rôdés et les responsables traitent les données avec précaution. Toutefois, la question de l'effacement et de l'archivage des données dans l'application ATEO n'est pas réglée. La dépendance directe par rapport au prestataire externe pour ce qui est des activités principales présente un risque considérable. En outre, les conventions de prestation passées avec ce prestataire ne sont pas suffisamment claires s'agissant de la protection

des données et de la sécurité de l'information. Un concept portant sur la sûreté de l'information et la protection des données (concept SIPD) doit être établi; la mise en œuvre des prescriptions relatives aux mots de passe et à la journalisation est insuffisante.

Suivi des contrôles effectués en 2012:

- Spital STS AG, Thoune

Les constats de l'examen réalisé en 2012 ont été passés en revue avec le Bureau et un plan de mesures ainsi qu'un calendrier ont été définis. Les premiers résultats ont été présentés: un responsable SIPD a été nommé et l'analyse des risques ainsi que d'autres documents SIPD ont été établis; certains de ces documents ont déjà été approuvés et leur mise en œuvre a pu débuter.

- Office AI

Les constats de l'examen réalisé en 2012 ont été discutés avec les autorités de surveillance des cantons qui utilisent aussi l'application OSIV. Celles-ci ont par la suite examiné la situation.

4 Vidéosurveillance

Différents contrôles préalables ont porté sur la vidéosurveillance. Il convient de distinguer entre les caméras placées à l'intérieur et à l'extérieur ainsi qu'entre la vidéosurveillance avec et sans enregistrement. En règle générale, lorsqu'il y a vidéosurveillance avec enregistrement, il a été possible de renoncer à la surveillance en temps réel, et inversement (Caisse de compensation et Office AI de Berne).

Les enregistrements vidéo sont considérés comme des atteintes graves portées au droit fondamental à la protection des données et nécessitent une base légale formelle. Dans un avis émis à l'égard de la Police cantonale, le Bureau a souligné que cette observation vaut aussi pour les enregistrements dans des bâtiments publics qui ne sont pas accessibles à tous.

Si des entrées d'un hôpital public sont surveillées, des patientes et patients apparaissent forcément dans les enregistrements et ceux-ci sont donc soumis au secret professionnel. Il est vrai que, dans les cas concrets (p. ex. en cas de vol), seule la Police cantonale peut exploiter de tels enregistrements. Pour qu'elle puisse le faire, les médecins et le personnel soignant de l'hôpital devraient toutefois être libérés de leur devoir de discrétion. Etant donné que l'Office du médecin cantonal, qui est compétent en la matière, n'octroie pas de dérogations générales, le Commandement de la police a demandé qu'il soit renoncé aux enregistrements (Spital Netz Bern AG).
Dans différents établissements d'exécution des peines et mesures et prisons du canton de Berne, de nombreuses caméras sont utilisées. A l'instigation du Bureau, l'Office de la privation de liberté et des mesures d'encadrement distribue à ses collaborateurs une notice les engageant à respecter la législation sur la protection des données s'agissant des installations de vidéosurveillance.

5 Contrôle préalable de projets informatiques

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

- S'agissant du contrôle préalable de son SIC (kiSro), le centre hospitalier régional de Haute-Argovie (SRO AG) doit expliquer comment la protection des personnes exposées (protection VIP) ainsi que la journalisation des accès (lecture) sont mises en œuvre. Une stratégie d'archivage et de radiation des données doit en outre être établie (cf. ch. 8.4).

- Les longues discussions sur le système d'informations cliniques de l'Hôpital de l'Ile (DEP) se sont poursuivies en 2013. Une solution différenciée a été trouvée; celle-ci respecte les prescriptions en matière de protection des données pour ce qui est des champs de recherche et de la distinction entre dossiers activés et dossiers désactivés. Le Bureau attend la preuve de la mise en œuvre de cette solution pour le printemps 2014 (des retards ont été occasionnés par le manque de convivialité du masque de recherche). Une proposition sommaire relative à la journalisation des accès (lecture) ainsi qu'à l'archivage et l'effacement des données de la journalisation lui a toutefois déjà été soumise.

- S'agissant du contrôle préalable du SIC du Centre psychiatrique de Münsingen (CPM; ORBIS), des propositions de solutions provisoires ont été soumises au Bureau. Une description définitive des fonctionnalités exigées est encore attendue.

- En 2013, une discussion a porté sur les points essentiels du nouveau système de dossiers électroniques des patients que vont introduire les Services psychiatriques universitaires (SPU). En raison de changements de personnel, la documentation SIPD n'a pas pu être finalisée en vue de l'examen pendant l'année écoulée.

- Le Bureau a pris du retard dans l'élaboration de sa quatrième prise de position relative au dossier SIPD révisé ainsi qu'à la stratégie en matière de conservation et de radiation que lui a soumis le CHR Frutigen Meiringen Interlaken (FMI AG) pour son SIC (PROKIS).

- Pour le CHR de Berne (Spital Netz Bern AG), la preuve que les droits d'accès au SIC ont été limités a été apportée et les patients sont informés, au moyen d'une brochure à leur attention, de la possibilité de faire bloquer un dossier désactivé. Après le blocage, le dossier n'est plus visible si le patient revient à l'hôpital. Les procédures pour la conservation et la radiation sont toujours en cours de discussion.

- S'agissant du SIC de la clinique bernoise de Montana, une rencontre a pu avoir lieu sur place et le Bureau a émis une première prise de position.

- La stratégie d'archivage et de radiation relative au système numérique d'archivage du CHR FMI AG (Picture and Communication System, PACS) a été soumise au Bureau, ce qui a permis de clore la procédure de contrôle préalable. Pour la première fois, l'«effacement organisationnel» a été examiné et il a été possible de déterminer dans quelles circonstances il peut être assimilé à l'«effacement physique»: il y a destruction au sens de la loi sur la protection des données lorsqu'aucun moyen technique et organisationnel ordinaire ne permet de rendre à nouveau lisibles des données qui ont été effacées d'un support électronique. Il est également considéré que les données ont été détruites correctement, du point de vue légal, lorsque les services qui seraient en mesure de restaurer ces données sont tenus, de par la loi, de renoncer en principe à restaurer des données qui ont été «détruites». C'est pourquoi le Bureau a exigé qu'il soit garanti que des données effacées ne sont pas rendues à nouveau lisibles (procédures de sauvegarde et de restauration des données).

- L'application de gestion administrative des patients OPALE, utilisée par les trois cliniques psychiatriques bernoises, ne disposait pas de la fonction d'effacement exigée par la législation sur la protection des données. Le fournisseur de l'application en question répond désormais à cette exigence pour les SPU dans la mesure où il supprime toutes les références nominales des données sauvegardées (transformation en données anonymes). Cette fonctionnalité devra encore être examinée.

- S'agissant des Services psychiatriques Jura bernois – Bienne – Seeland (SPJBB), la preuve du remplacement des comptes de groupe par des comptes individuels n'a pas encore été apportée.

- Les documents SIPD concernant le système OPALE tel qu'il a été introduit au CPM ont été remis au Bureau depuis longtemps mais n'ont pas encore pu être examinés faute de ressources suffisantes.

- Pour ce qui est du logiciel de saisie des prestations de soins (tacs) du CPM, un système de pré-archivage avec des droits d'accès limités est en place et les consignes en matière d'effacement ont été mises en œuvre. Le contrôle préalable a ainsi pu être achevé.

- La Ligue bernoise contre le cancer met en œuvre, au moyen de l'application MC-SIS, un programme de dépistage de cancer du sein par mammographie sur mandat du canton de Berne. Dès que les dernières incertitudes auront été levées, le Bureau émettra sa première prise de position.

- S'agissant des documents SIPD relatifs à l'application NICERStat du registre des tumeurs du canton de Berne, une rencontre a eu lieu sur place et le Bureau a émis sa première prise de position.

- Pour ce qui est du système d'annonce des patients en ligne (OPAN) pour les soins à domicile dans le canton de Berne, un examen limité à la protection de base est en cours. Le délégué cantonal à la sécurité informatique du canton (DSI BE) a émis plusieurs prises de position.

- L'examen préalable du logiciel SAP HCM de gestion administrative du personnel de l'Hôpital de l'Ile (projet PERSAP) a pu être achevé après que la stratégie d'archivage et de radiation a été examinée.

- Après une visite sur place, le Bureau a pris position sur le remplacement des terminaux médias des patients et sur le système d'identification des patients du CHR FMI AG.

- Un premier contrôle du système d'informations cliniques KISIM du Centre hospitalier Bienne (CHB SA) a révélé que les documents SIDP n'étaient pas à jour. Le Bureau a par la suite émis de nouvelles prises de position sur ces documents, entre-temps actualisés par le CHB.

Le Bureau a aussi effectué de nombreux contrôles préalables dans d'autres domaines que le secteur de la santé:

- Le contrôle préalable des deux applications de la Direction de l'instruction publique, StipBE-Online et l'application pour les bourses (octroi facilité d'allocations de formation), a pu être achevé, exception faite de la stratégie de radiation.

- S'agissant de l'application BISO-BE (orientation scolaire, professionnelle et personnelle) de la Direction de l'instruction publique, une rencontre a eu lieu sur place. Le Bureau a ensuite émis plusieurs prises de position. Le contrôle préalable a pu être achevé en automne 2013.

- Les travaux relatifs au contrôle des projets suivants ont été suspendus jusqu'à la fin de l'examen de la protection de base à l'Université de Berne (cf. ch. 2.4): UNICARD, Kernsystem Lehre (KSL) et Studitracker (administration des étudiants). S'agissant du système UNICARD et de l'application KSL, le Bureau a prié l'Université de lui fournir les renseignements et les documents manquants.

- Concernant les applications spécialisées Escada (gestion des contrats d'apprentissage, y compris l'attribution des notes d'examen) et Evento (logiciel pour la gestion d'école utilisé pour l'administration des écoles et des cours ainsi que la planification des manifestations et des ressources), un concept SIPD commun a été soumis au Bureau. Celui-ci a exigé qu'une planification actualisée de la mise en œuvre des mesures de protection de base qui ne sont pas encore réalisées lui soit remise. Il examinera si la stratégie différenciée en matière de droits d'accès ainsi que la stratégie d'archivage et de radiation des données qui lui ont été soumises sont satisfaisantes et si une procédure pour la gestion des comptes des utilisateurs a été introduite.

- A l'instigation du Bureau, la Haute école spécialisée bernoise (HESB) a renoncé à demander un extrait de casier judiciaire des candidats (absence de base légale). Les extraits qui avaient déjà été sauvegardés sous forme électronique ont été effacés. Le système d'information universitaire et d'administration des étudiants IS-Academia de la HESB a continué d'être développé (interfaces et intégration de nouveaux départements); la documentation SIPD a été révisée et soumise au Bureau, qui doit émettre sa troisième prise de position.

- Après une discussion préalable, les documents SIPD relatifs au Case management Formation professionnelle (CM FP) ont été soumis au Bureau pour examen (CM-online). Le suivi des cas doit permettre de veiller à ce que les adolescents et jeunes adultes à problèmes multiples parviennent à s'insérer dans la vie professionnelle et réussissent leur carrière.

- S'agissant du logiciel pour l'examen et le versement de prestations individuelles par l'Office des personnes âgées et handicapées (ZERO), une stratégie d'archivage et de radiation doit encore être établie.

- Le flux de travaux requis par les déclarations de maladie est soumis, pour les services administratifs cantonaux (Office du personnel), à la loi cantonale sur la protection des données; pour l'assureur, les dispositions de la loi sur l'assurance-maladie relatives à la protection des données et de la loi fédérale sur la protection des données s'appliquent. Le flux de travaux (formulaire électronique) soumis au Bureau par l'Office du personnel pour contrôle préalable respecte ces prescriptions légales.

- Tant que durent les rapports de travail, il convient de distinguer entre deux catégories de données particulièrement dignes de protection: d'une part les données qui doivent être détruites après cinq ans (p. ex. simples certificats médicaux) et d'autre part celles qui ne devront être détruites que cinq ans après la fin des rapports de travail (p. ex. certificats faisant partie du dossier de candidature). C'est ce qu'a révélé l'examen du projet Webarchiv de l'Office du personnel.

- Concernant le concept SIPD revu du système cantonal d'informations financières (FIS), certaines questions sont encore en suspens (droits d'accès, stratégie d'archivage, informations sur les systèmes intégrés).

- Il en va de même pour le concept SIPD revu du système d'information sur le personnel du canton de Berne (PERSISKA).

- Le projet de communication des programmes électronique (CdPe) respecte les prescriptions de la législation sur la protection des données. Il reste à déterminer si l'accès prévu par le portail BE-Login, nouvellement mis en service, les respecte aussi. Les documents relatifs au contrôle préalable de BE-Login n'ont été soumis au Bureau que peu avant que le système soit mis à la disposition de la population.

- Les documents SIPD relatifs au système de traitement des cas des onze autorités de protection de l'enfant et de l'adulte (APEA) ont également été remis en retard au Bureau. La direction du projet n'a pas soumis un concept SIPD à ce dernier, mais un règlement relatif au traitement tel que l'exige l'administration fédérale. Les indications relatives à la sécurité informatique n'expliquaient pas de manière suffisamment claire quelles mesures doivent encore être prises. Les collaborateurs n'ont pas seulement accès aux données de l'autorité pour laquelle ils travaillent, mais à celles de tout le canton, ce qui est contraire au principe de la proportionnalité.

- Plusieurs séances ont eu lieu concernant la protection de base de l'infrastructure informatique de la Direction de l'instruction publique.

- Le Bureau a achevé, avec considérablement de retard, le contrôle préalable relatif au système d'analyse des crimes violents devant servir à l'identification des criminels en série (ViCLAS) géré par la Police cantonale pour tous les cantons (concordat). Dans la procédure d'octroi d'une autorisation actuellement en cours, il conviendra de prendre en considération que le système n'est plus renouvelé par le fournisseur, ce qui entraîne des problèmes de sécurité.

- Etant donné que la Police cantonale envisage une réorganisation stratégique, la procédure de contrôle préalable relative au système de rapports OboraNew, qui était aussi en retard, s'est réglée d'elle-même.

- Si la police doit avoir la possibilité d'accéder aux données de l'administration pénitentiaire pour pouvoir vérifier si une personne appréhendée se trouve en détention, une base légale est nécessaire. C'est ce qu'avait indiqué le Bureau à l'Office de la privation de liberté et des mesures d'encadrement il y a déjà longtemps. Puisque la base légale nécessaire manque encore, l'application partielle Police-Tool n'a pas pu être mise en service. L'office concerné a renoncé à une décision allant contre la prise de position du Bureau à ce sujet.

En raison du manque de ressources, le Bureau n'a pas pu rattraper le retard considérable qu'il a pris dans les procédures de contrôle préalable en cours. Il est en revanche parvenu à traiter dans une large mesure les nouveaux projets qui lui ont été soumis dans un délai approprié. L'attitude de certains chefs de projet à l'égard des prescriptions relatives au contrôle préalable a donné au Bureau l'impression que ces derniers cherchent à appliquer le principe du moindre effort. En effet, certains documents soumis avaient visiblement fait l'objet de peu de soins et présentaient des contradictions internes. Dans de tels cas, le Bureau renvoie les documents à l'expéditeur pour amélioration et attire l'attention des chefs de projet sur le fait que les documents relatifs au contrôle préalable sont un instrument à leur service avant tout, pour garantir que les données sont traitées conformément à la législation sur la protection des données.

(S'agissant des installations de vidéosurveillance également soumises à un contrôle préalable, cf. ch. 4; s'agissant de la procédure de recours dans la procédure de contrôle préalable d'un système d'informations cliniques, cf. ch. 8.4).

6 Avis exprimés, pratique

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

- Les journaux DHCP, combinés à d'autres éléments, permettent notamment de savoir quels collaborateurs ont consulté une page Internet donnée. Ils peuvent être conservés 4 à 6 semaines pour détecter des erreurs techniques. Si un service veut conserver ces données plus longtemps, par exemple pour constater que des collaborateurs font un usage abusif d'Internet, une base légale est nécessaire. C'est ce qu'a défendu le Bureau contre l'avis de la Direction des finances et de l'OIO.

- Si un service veut publier des photographies de personnes sur Internet, une base légale est nécessaire. Si la personne concernée a donné son accord, une disposition dans une ordonnance suffit. Le Bureau a rédigé un aide-mémoire au sujet de la publication de photographies sur Internet, dans lequel il mentionne notamment les droits des tiers et des collaborateurs. Ceux-ci ont en effet le droit de se défendre et notamment d'exiger la suppression des photographies publiées de manière illicite.

- Microsoft 365 (MS365) est une offre qui propose le paquet Microsoft Office et une certaine capacité de stockage dans ce que l'on nomme un nuage (cloud computing; les données et les programmes sont sauvegardés sur des serveurs qui ne sont généralement pas situés en Suisse) à des conditions avantageuses. Cette offre séduit en particulier les écoles, car elle rend superflues la maintenance et l'assistance dans une large mesure. Du point de vue de la protection des données, le traitement de données à l'étranger est problématique. Le fait que, avec une telle offre, le for juridique se trouve à l'étranger interdit aux écoles d'introduire cette solution (car elles auraient de la peine à faire valoir leurs droits). C'est ce qui a été expliqué à des responsables des écoles intéressés par l'offre de Microsoft. Le Bureau a transmis aux autorités communales de surveillance un aide-mémoire de PRIVATIM contenant des explications à ce sujet. Il semble toutefois difficile de lutter contre l'engouement croissant pour de tels services. Il n'est pas rare que des plateformes de communication modernes recourent automatiquement à de telles prestations (p. ex. synchronisation avec iCloud [Apple] ou la plateforme média Google+).

- Plusieurs demandes concernaient l'obligation de renseigner les autorités fiscales. Le Bureau a confirmé que des factures liées à des frais de santé ainsi que des données relatives aux clients des entreprises pouvaient être consultées en vertu de l'obligation de renseigner et de collaborer ancrée dans la loi sur les impôts.

- Les questionnaires détaillés visant à déterminer le domicile fiscal des résidents à la semaine ont été critiqués à plusieurs reprises. Ces ques-

tionnaires ont été revus et adaptés pour mieux respecter les prescriptions en matière de protection des données. Les questions concernant des données personnelles particulièrement dignes de protection, comme les activités politiques, religieuses ou philosophiques, sont désormais facultatives.

- Les offices régionaux de placement (ORP) peuvent fournir à des employeurs le curriculum vitae de demandeurs d'emploi. Un CV ne peut toutefois être transmis que s'il existe une base légale ou, au cas par cas, si la personne concernée a donné son accord par écrit. Les personnes concernées n'avaient pas toujours conscience que, en cochant «oui» à côté de «curriculum vitae sur demande», dans la rubrique «Echange de données» de la convention de réinsertion, elles donnaient leur accord pour la transmission de leur CV à des employeurs. A l'avenir, il conviendra d'attirer leur attention sur ce point.

- La question de savoir s'il est possible de détruire, et dans quels délais, les données et les documents des procédures pénales, des enquêtes policières et du casier judiciaire est régulièrement posée. Les délais varient en fonction du contenu et de l'état de la procédure. Ils peuvent être déduits des dispositions légales fédérales et cantonales (droit pénal, droit procédural dans le domaine pénal, législation introductive cantonale). Avant de demander la destruction de tels documents, il convient de déposer une demande de renseignement et de consultation.

- Un carnet (par exemple) dans lequel un collaborateur consigne certaines données qu'il ne transmet à personne peut être considéré comme un instrument de travail personnel. La loi sur la protection des données ne s'applique pas à de tels instruments. Si les données consignées concernent des tiers, ceux-ci n'ont par conséquent pas le droit de les consulter. Ils n'ont pas non plus le droit de demander que ces données soient corrigées ou détruites. Cela vaut aussi pour des notes qui auraient été prises à l'aide de moyens techniques (ordinateur, téléphone portable). Pour cette raison, quelques collaborateurs de la police ont estimé que des photographies ou des vidéos prises au moyen de leur téléphone portable (p. ex. prises de vue à l'intérieur d'un appartement ou photographies de prostituées) devaient aussi être considérées comme des instruments de travail personnels. Or, cela n'est pas admissible puisque le droit de la police, en application de la loi sur la protection des données, n'autorise en aucun cas la collecte de telles données.

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.
Au moyen d'une motion relative à la loi sur le renseignement, le Grand Conseil a exigé du Conseil-exécutif, allant contre une proposition de ce dernier, qu'il s'engage, dans le cadre de la procédure de consultation, pour que le parlement continue d'exercer la haute surveillance. Il a ainsi donné un signal fort: le droit du canton à exercer une surveillance dans le domaine de la protection de l'Etat, particulièrement sensible du point de vue de la protection des données, doit être sauvegardé.
S'agissant de la loi fédérale sur l'enregistrement des maladies oncologiques, le Bureau a souligné que, pour les données sommaires, une base légale formelle suffit mais que, pour les données complémentaires, l'accord de la personne concernée est nécessaire. En outre, il a suggéré que les données originales transmises soient détruites, après que l'organe national d'enregistrement du cancer les a enregistrées et a effectué le contrôle de qualité, puisqu'elles ne sont plus utilisées. Il a par ailleurs renvoyé à la prise de position de PRIVATIM.
La protection et l'information des patients font partie des buts du registre des professionnels de la santé qui est consultable en ligne. Le principe de proportionnalité, ancré dans la législation sur la protection des données, exige que les données nécessaires soient réduites au minimum: du point de vue de la protection des patients, si une personne figure sur la liste des professionnels de la santé avec ses titres de fin d'études reconnus (ainsi que, lorsque cela est nécessaire, l'information «au bénéfice d'une autorisation d'exercer»), cela est suffisant. Il n'y a pas lieu d'indiquer si une entrée existait auparavant. Le Bureau l'a souligné dans le cadre du projet de révision de l'accord intercantonal sur la reconnaissance des diplômes de fin d'études.

7.2 Législation cantonale

S'agissant de la loi sur le Contrôle des finances, la proposition du Bureau, à savoir la création d'une base légale formelle, comme pour une procédure d'appel, régissant l'accès aux données du système d'informations financières FIS, a été adoptée en première lecture par le Grand Conseil.

Des données à référence spatiale («géodonnées») peuvent facilement, si elles sont mises en relation ou combinées, devenir des données

à référence nominale. Si l'on recoupe par exemple une information sur une personne non déterminée avec une adresse, l'on peut obtenir une référence nominale. Les possibilités de combiner des données sont illimitées. Cela constitue des bases importantes pour la planification et la recherche, mais cela comporte aussi des risques. Le Bureau a déjà pu exprimer son avis au cours des travaux préparatoires relatifs à la nouvelle loi cantonale sur la géoinformation. Il a formulé d'autres remarques dans un corapport, soulignant notamment que, s'agissant des géodonnées à référence nominale incorrectes, la responsabilité du canton ne peut pas être exclue.

Concernant l'ordonnance portant introduction du Concordat instituant des mesures contre la violence lors de manifestations sportives, le Bureau a attiré l'attention sur la réserve mentionnée dans la disposition de la loi sur la police relative à la vidéosurveillance. S'agissant de l'obligation, pour les autorités pénales qui rendent le jugement, d'annoncer les condamnations prononcées à la police, il a exigé une base légale formelle.

Différentes prises de position ont porté sur les compléments apportés à l'ordonnance sur l'harmonisation des registres officiels. Des questions relatives à la proportionnalité des accès accordés se posent régulièrement. Si un service obtient un droit d'accès à GERES (qui rassemble toutes les données contenues dans les registres du contrôle des habitants), son droit d'accès à la gestion centrale des personnes (GCP) doit lui être retiré dans la mesure où son besoin d'être informé peut être ainsi satisfait. Dans ce contexte, il a été constaté que les personnes ayant accès au système d'information sur les données relatives aux immeubles GRUDIS avaient aussi accès à la GCP. Leur accès n'était pas limité aux données des personnes ayant un lien avec des immeubles, mais leur permettait de consulter toutes les données de la GCP. Il a été remédié à cette situation.

Le Bureau a formulé deux remarques sur la révision totale de l'ordonnance sur les soins hospitaliers. La Direction de la santé publique et de la prévoyance sociale a confirmé que l'Office des hôpitaux ne gérerait qu'un recueil de données à des fins statistiques (sans référence aux collaborateurs concernés) pour calculer le potentiel de formation.

L'ordonnance de Direction sur la gestion et l'archivage des documents des collectivités de droit public et de leurs établissements doit remplacer la directive de l'Office des affaires communales et de l'organisation du territoire actuellement en vigueur. Le Bureau a été impliqué à un stade précoce. Il s'est exprimé sur des questions générales relatives à l'archivage d'une part et sur des points de détail relatifs aux délais de conservation d'autre part.

8 Surveillance et décisions de justice

8.1 Droit de consulter un rapport de supervision refusé

Des problèmes sont survenus entre des collaborateurs d'un organe cantonal, raison pour laquelle une supervision a été ordonnée. L'un des collaborateurs concernés a demandé à consulter le rapport produit dans ce cadre. Selon la Direction de la police et des affaires militaires, l'on a refusé, à juste titre, de mettre à sa disposition une copie du rapport intégral. D'après elle, dans la mesure où le rapport contenait des données personnelles d'autres collaborateurs associées à des données personnelles du requérant, des intérêts publics prépondérants ainsi que des intérêts privés particulièrement dignes d'être protégés s'opposaient au droit à la consultation. Si le contenu du rapport n'avait pas été tenu secret, le but de la supervision, à savoir restaurer la collaboration et ainsi favoriser le bon déroulement de l'activité administrative, n'aurait pas pu être atteint. En outre, la Direction affirme qu'il était dans l'intérêt des collaborateurs de pouvoir exprimer leur état d'esprit dans le cadre d'une supervision en équipe sans avoir à craindre des répercussions négatives.

8.2 Le droit de consulter un registre de police doit être respecté

Une recourante a demandé à pouvoir consulter les données la concernant contenues dans un registre de police. La Police cantonale lui a refusé ce droit, se contentant de lui fournir une synthèse des informations saisies à son sujet. La Direction de la police et des affaires militaires a estimé que la remise d'une synthèse n'entrait en ligne de compte que si la part de données devant être protégées en raison d'intérêts publics ou de tiers prépondérants était telle que le texte en devenait incompréhensible. Selon elle, cela n'était pas le cas. Les données saisies dans le registre de police auraient donc dû être communiquées à la recourante. La Direction de la police et des affaires militaires estime toutefois que le droit autorise le caviardage de certains passages, par exemple s'ils renseignent sur la stratégie de la police (notamment sur le moment précis de l'intervention), car il s'agit de données d'intérêt public prépondérant qui ne doivent pas être révélées.

8.3 Registre des fichiers

Un centre hospitalier doit inscrire et mettre à jour ses données dans le registre des fichiers.

En fournissant les prestations pour lesquelles il a un mandat conformément à la liste des hôpitaux, il assume une tâche publique. En ce sens, le centre hospitalier est soumis à la loi cantonale sur la protection des données et doit communiquer ses données. Par ailleurs, le Tribunal administratif exclut que le centre hospitalier joue la carte de la concurrence économique dans la mesure où il accomplit des tâches qui lui ont été confiées par le canton. Le Tribunal administratif confirme ainsi la décision de l'instance précédente (Direction de la santé publique et de la prévoyance sociale).

8.4 Procédure de contrôle préalable d'un système d'informations cliniques

Dans le cadre de l'introduction d'un système d'informations cliniques dans un centre hospitalier, le Bureau a déposé un recours auprès du Tribunal administratif contre les points rejetés par la Direction de la santé publique et de la prévoyance sociale en tant qu'instance précédente. Dans son jugement, le Tribunal administratif a soutenu la décision de la Direction, selon laquelle il n'est pas nécessaire, d'une part, d'informer les nouveaux patients que le système d'informations cliniques donne aussi accès aux anamnèses des hôpitaux qui étaient indépendants avant d'être rattachés au centre hospitalier, ni d'autre part, de journaliser les accès (lecture) aux données d'un autre service (selon la taille du service). Le Tribunal administratif a toutefois contredit l'instance précédente sur un point: les données de patients exposés (p. ex. les collaborateurs du centre hospitalier) doivent bénéficier d'une protection particulière.

8.5 Obligation de soumettre au Bureau un projet de plate-forme pour l'échange de données en vue d'un contrôle préalable

Une clinique psychiatrique qui prévoit de remplacer les interfaces existantes (multitude de systèmes de traitement de données) par une plateforme pour l'échange de données (JCAPS) doit soumettre son projet au Bureau en vue d'un contrôle préalable.
Il convient de montrer que, pour chaque champ, les prescriptions en matière de protection des données seront respectées après l'introduction de la plate-forme dans tous les systèmes de traitement des données liés, comme l'a souligné le Bureau dans une proposition motivée (droit de la surveillance).

9 Collectivités de droit communal

Communications du Bureau
Pour la première fois, en 2013, le Bureau a pris position sur des questions actuelles ou récurrentes dans des communications adressées aux autorités communales de surveillance de la protection des données. Ces communications doivent permettre à ces dernières la mise en œuvre efficace et uniforme du droit de la protection des données. Elles ont porté sur la publication de données relatives aux membres non permanents des bureaux électoraux (avril), sur la mise en place du système de gestion électronique des affaires GEVER (juillet), sur l'admissibilité des données relatives à l'appartenance religieuse dans le registre du contrôle des habitants (août, cf. ch. 1) ainsi que sur l'utilisation de Microsoft Office 365 dans les écoles (novembre 2013, cf. ch. 6). Ces communications sont publiées sur le site Internet du Bureau.

Un cours destiné aux autorités communales de surveillance n'a pas pu être donné en raison du nombre insuffisant d'inscriptions. (Concernant le site Internet exemplaire de la commune de Worb ainsi que l'intérêt dont ont fait preuve les participants aux cours, cf. ch. 2.2; concernant le remplacement de la directive sur l'archivage, cf. ch. 7.2).

10 Points abordés dans le rapport précédent

(3: suivi des contrôles préalables effectués en 2012, 5: contrôles préalables effectués, 8.3: registre des fichiers, recours, 8.4: procédures de recours dans la procédure de contrôle préalable d'un système d'informations cliniques, 8.5: recommandation motivée dans la procédure de contrôle préalable de la plate-forme JCAPS.)

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.

24 janvier 2014

Le délégué à la protection des données: *Siegenthaler*

12 Annexe

12.1 Abréviations et désignations

A: annexe
AI: assurance-invalidité
Apple: entreprise américaine dont le siège principal se trouve à Cupertino (Californie, USA) et qui conçoit et commercialise des ordinateurs et des produits électroniques de divertissement ainsi que des systèmes d'exploitation et des logiciels (d'après Wikipédia)
ATEO: application pour la taxe d'exemption de l'obligation de servir
Case Management Formation professionnelle: solution informatique visant à coordonner les mesures et à soutenir tout au long de leur parcours les adolescents et les jeunes adultes dont l'insertion dans la vie professionnelle est menacée
CdPe: communication des programmes électroniques des directions d'école à l'Office du personnel
Cf.: confer (voir)
CHB: Centre hospitalier Bienne
Clinical Trial Unit: unité du Département de recherche clinique de l'Université de Berne qui procède à des études cliniques
CPM: Centre psychiatrique de Münsingen
DEP: dossier électronique du patient (système d'informations cliniques de l'Hôpital de l'Ile)
DHCP (Dynamic Host Configuration Protocol): protocole de configuration dynamique d'hôte
FAQ: foire aux questions
FMI AG: hôpitaux de Frutigen, Meiringen et Interlaken
GCP (gestion centrale des personnes): banque de données de l'Intendance des impôts contenant des informations sur les personnes physiques et morales
GERES: solution informatique pour la gestion et l'harmonisation de données personnelles, utilisée, dans le canton de Berne, pour la synthèse de toutes les données des registres du contrôle des habitants
Google+: réseau social de Google Inc., deuxième plus grand réseau social au monde (d'après Wikipédia)
HESB: Haute école spécialisée bernoise
HESB-Card: carte à puce multifonctionnelle de la HESB (légitimation, comptabilisation des frais)
Historique des événements (anglais: logging): enregistrement automatique de toutes les actions (ou de certaines actions seulement) liées à des processus sur un système informatique (d'après Wikipédia)
iCloud: service d'informatique en nuage (cloud computing) offert par Apple
IS-Academia: système d'information universitaire et d'administration des étudiants
ISO: Organisation internationale de normalisation
JCAPS (Java Composite Application Platform Suite): logiciel favorisant l'intégration de services distribués à l'ensemble des applications d'une entreprise
Journal DHCP (anglais: log ou log file): fichier dans lequel sont enregistrés les événements (cf. historique des événements) et qui permet notamment de suivre le comportement de l'utilisateur d'un ordinateur
KSL: programme informatique de l'Université de Berne
NICER (National Institute for Cancer Epidemiology and Registration): Institut national pour l'épidémiologie et l'enregistrement du cancer
Nuage (informatique en nuage ou cloud computing): accès, via un réseau, à des ressources informatiques immatérielles (par ex. capacité de calcul, stockage des données, capacités de réseau ou logiciels) qui s'adaptent aux besoins de manière dynamique (d'après Wikipédia)
Objectifs NOG: dans le cadre de la Nouvelle gestion publique, des objectifs de prestation et d'effet doivent être fixés pour chaque unité administrative (ces objectifs sont mentionnés dans le budget ainsi que dans le rapport de gestion du canton de Berne)
OboraNew: remplacement du système électronique de rapports de la Police cantonale
OIO: Office d'informatique et d'organisation
OPALE: application de gestion administrative des patients
ORP: office régional de placement
OSIV: système d'information Open System IV, application informatique utilisée par plusieurs offices AI
PACS (Picture Archiving and Communication System): système permettant de gérer les images médicales grâce à des fonctions d'archivage
PERSAP: projet de remplacement du système de gestion administrative du personnel de l'Hôpital de l'Ile
PERSISKA: système d'information sur le personnel du canton de Berne
PFPDT: préposé fédéral à la protection des données et à la transparence
PRIVATIM: association des Commissaires suisses à la protection des données
SAP: Direction de la santé publique et de la prévoyance sociale
SIC: système(s) d'informations cliniques
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

SNB: Spitalnetz Bern AG (réseau constitué des hôpitaux d'Aarberg, de Münsingen et de Riggisberg, des hôpitaux Tiefenau et Ziegler, de l'hôpital et foyer pour personnes âgées de Belp et du centre de soins d'Elfenau)
SPJBB: Services psychiatriques Jura bernois – Bienne – Seeland à Bellelay
SPU: Services psychiatriques universitaires
SRO: centre hospitalier régional de Haute-Argovie
STS AG: groupe hospitalier Thoune-Simmental SA
tacs: système de saisie des prestations pour les hôpitaux
TI: technologies de l'information
TIC: technologies de l'information et de la communication
UNICARD: système informatique de l'Université de Berne servant à l'établissement et à la gestion des cartes de légitimation à puce
VICLAS (Violent Crime Linkage Analysis System): système d'analyse des crimes violents devant servir à l'identification des criminels en série
ZERO: programme introduit pour l'examen et le versement de prestations individuelles par l'Office des personnes âgées et handicapées de la SAP

12.2 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 121/12 du 2 avril 2013
8.2: Décision de la Direction de la police et des affaires militaires BD 158/11 du 8 avril 2013
8.3: Jugement du Tribunal administratif JTA 100.2012.118 du 4 février 2013
8.4: Jugement du Tribunal administratif JTA 100.2012.330 du 15 août 2013
8.5: Proposition motivée du Bureau 42.50-12.5652 du 17 septembre 2013

12.3 Sitographie

2.3: Rapport de gestion: http://www.fin.be.ch/fin/fr/index/finanzen/finanzen/publikationen/geschaeftsberichtstaatsrechnung.html
3: HIN-Mail: http://www.hin.ch/
8.3: Registre des fichiers: http://www.jgk.be.ch/jgk/fr/index/aufsicht/datenschutz/register_der_datensammlungen.html
9: Communications aux autorités communales de surveillance: http://www.jgk.be.ch/jgk/fr/index/aufsicht/datenschutz/kommunaler_datenschutz/mitteilungenetc.html