Kanton Bern
Canton de Berne

Rapport d'activité Bureau pour la surveillance de la protection des données 2019

Bureau pour la surveillance de la protection des données Février 2020

Impressum

Edition: Bureau pour la surveillance
de la protection des données du canton
de Berne

Maquette et réalisation: noord.ch


Y
U
J
N
G

1 Avant-propos

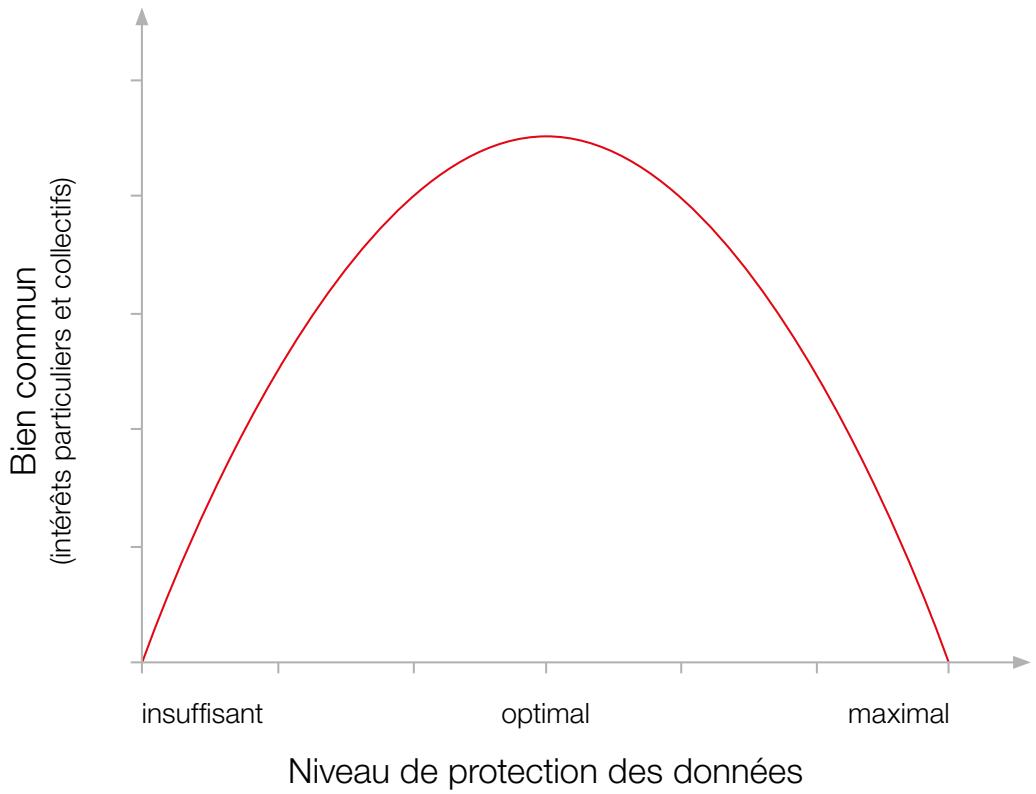
Dans le programme de législature 2019 à 2022 arrêté le 8 janvier 2019, le Conseil-exécutif s'est notamment fixé comme but de faire avancer la transformation numérique de l'administration au moyen d'une stratégie déployée dans toutes les Directions et d'appliquer la primauté du numérique dans la communication entre l'Etat et les particuliers, entre l'Etat et les entreprises ainsi qu'entre les autorités. Dans ce but, il a approuvé la Stratégie pour une administration numérique du canton de Berne le 26 juin 2019. Cette stratégie fixe notamment les conditions auxquelles les prestations de services électroniques fournies par les autorités doivent répondre pour être considérées comme bonnes. La confiance est primordiale (en ce qui concerne notamment la protection de la personnalité et des données ainsi que la sécurité des informations). Pour la population et l'économie, il s'agit en effet de l'élément décisif pour l'utilisation des prestations de services numériques. Ainsi, la protection des données, en plus d'être l'un des socles de l'Etat de droit et de la démocratie, sert aussi de critère de qualité et, finalement, d'argument de vente en faveur des communications électroniques avec les autorités.

Le Bureau pour la surveillance de la protection des données (le Bureau), dont le personnel a été renouvelé pour moitié au printemps 2019 après trois départs dont deux à la retraite, a lui aussi défini une stratégie en 2019. Parmi les objectifs stratégiques figurent la garantie d'un niveau optimal de protection des données (ch. 2 *infra*) prévu par la législation et appliqué par l'administration, qu'elle soit cantonale ou communale; le développement des compétences des autorités dans le domaine de la protection des données et de la sûreté de l'information ainsi que le renforcement de la position du Bureau d'interlocuteur indépendant prêt à conseiller et soutenir les Directions, les offices et les services qui le désirent au moment d'assumer leurs responsabilités en matière de protection des données (ch. 6, lit. *a infra*). Par ailleurs, l'intégration précoce du Bureau dans les projets législatifs concernant la protection des données (lit. *b infra*) ou dans les projets informatiques (lit. *c infra*) lui permet d'exercer une forme de surveillance préventive. La question n'est donc plus tant de savoir *si*, au vu des circonstances, le traitement des données personnelles est admissible, mais *comment* une telle opération peut se faire conformément au cadre légal. Servant à indiquer aux organes concernés les domaines dans lesquels le niveau de protection peut être encore accru, les contrôles de sécurité des systèmes et applications informatiques utilisés (lit. *d infra*) poursuivent le même but. Enfin, la protection des données doit s'imposer comme une évidence aux autorités qui traitent des données personnelles, c'est-à-dire probablement toutes les autorités, puisque c'est ainsi que se gagne la confiance de la population censée utiliser les services numériques qu'elles proposent.

2 Droit fondamental à la protection des données

La Constitution fédérale et la Constitution cantonale définissent la protection de la sphère privée, qui comprend la protection contre un emploi abusif des données personnelles, comme un droit fondamental. Un droit fondamental ne peut faire l'objet d'une restriction qu'à certaines conditions: elle doit reposer sur une base légale suffisante, servir un intérêt public prépondérant et être proportionnée au but poursuivi (c.-à-d. être adaptée et nécessaire, tandis que ses conséquences doivent être supportables pour les personnes concernées). Evidemment, ces conditions valent également pour le traitement des données personnelles par des autorités. Selon la Constitution du canton de Berne, ces dernières doivent par ailleurs s'assurer que les données traitées sont exactes et les protéger contre un emploi abusif (sécurité des données).

Par ailleurs, la Constitution cantonale charge les autorités cantonales et communales de tâches publiques, par exemple dans les domaines de la formation, de la santé, de l'économie ou de la sécurité, qui doivent être accomplies dans l'intérêt commun. Or il arrive que cet intérêt prime sur la sphère privée de l'individu. Le niveau de protection des données garanti par la Constitution est donc considéré comme *adéquat* lorsqu'un équilibre idéal est atteint entre la protection des droits individuels fondamentaux d'une part et l'intérêt de la communauté à l'accomplissement des tâches publiques ainsi qu'à l'efficacité de l'administration d'autre part. Le niveau de protection des données est optimal lorsque le bien commun, découlant de la réalisation des intérêts individuels et collectifs, est maximal.



La LCPD précise les devoirs des autorités lors du traitement des données personnelles. Par autorité, il faut comprendre l'administration, mais aussi d'autres entités chargées de tâches publiques comme les écoles et les hôpitaux. Quant au traitement, il se définit comme toute activité ayant directement trait aux données personnelles, et notamment le fait de les recueillir, de les conserver, de les modifier, de les combiner, de les communiquer ou de les détruire. La législation fixe de surcroît les droits des personnes concernées, à savoir le droit aux renseignements et à la consultation de leurs données, à leur rectification si elles sont fausses et à leur suppression lorsqu'elles sont inutiles. Finalement, elle règle le statut et les devoirs des autorités cantonales et communales chargées de la surveillance de la protection des données par rapport aux autres autorités et aux personnes intéressées.

3 Responsabilité et surveillance

La responsabilité de la protection des données incombe à l'autorité qui, pour accomplir les tâches que lui assigne la loi, traite ou fait traiter des données personnelles. L'autorité doit veiller au respect des prescriptions en matière de protection des données et à la sécurité des données. Cette exigence s'applique de toute manière, peu importe que l'autorité de surveillance compétente s'implique ou que ses recommandations soient suivies.

Le champ d'application des législations suisse et bernoise sur la protection des données répond à une structure fédéraliste: La LPD s'applique aux autorités fédérales et aux privés qui traitent les données (notamment à des fins commerciales), alors que les activités des autorités cantonales et communales du canton de Berne sont régies par la LCPD. La question de l'autorité de surveillance compétente s'inscrit elle aussi dans la logique du système fédéral: pour les autorités fédérales et les privés, la compétence revient au PFPDT, pour les autorités cantonales, la surveillance est exercée par le Bureau et, pour les autorités communales, par l'autorité de surveillance désignée par la commune pour son domaine de juridiction. Cette dernière autorité est à son tour surveillée par le Bureau.

Dans certains cas, un examen approfondi est nécessaire pour déterminer la législation applicable et l'autorité de surveillance compétente. A ce titre, l'entreprise BLS SA fait figure d'exemple: bien qu'elle appartienne aujourd'hui majoritairement au canton de Berne, elle reçoit la concession du transport de personnes de la part de la Confédération dans le cadre de son monopole. Ainsi lorsqu'elle traite des données, notamment par l'intermédiaire d'une application d'achat de billets, c'est la LPD qui régit ses activités et le PFPDT qui est chargé de la surveillance.

4 Tâches du Bureau

L'article 34 LCPD énumère les tâches qui incombent au Bureau. Le Bureau soutient les autorités cantonales dans l'exercice de leur responsabilité en matière de protection et de sécurité des données. Sur le plan informel, il dispense ses conseils aux autorités et, sur le plan formel, il prend position sur les projets d'acte législatif et les autres mesures relevant de la protection des données ainsi que sur les différents traitements électroniques des données envisagés qui présentent un risque particulier pour les personnes concernées (contrôle préalable). En outre, il procède à des examens relatifs à la sûreté de l'information pour les systèmes et applications informatiques en service (audits). Le Bureau se veut aussi l'interlocuteur des personnes concernées et se tient à leur disposition pour fournir des conseils, faire office d'intermédiaire ou traiter leurs requêtes. Lorsque la mise en œuvre d'une protection adéquate des données ne saurait être garantie autrement, le Bureau peut rédiger une proposition motivée à l'intention des autorités ou porter les décisions rejetant les propositions motivées jusque devant le Tribunal administratif; cette option ne doit toutefois servir qu'en dernier recours, c'est-à-dire si les conseils fournis en vue de la résolution des problèmes et la coopération avec les autorités ne promettent aucun résultat. Le Bureau garantit aussi la transparence en tenant le registre des fichiers des autorités cantonales, ce qui donne aux personnes concernées la possibilité d'exercer leurs droits (renseignement, consultation, rectification et suppression).

5 Organisation, ressources et réseau

Le 31 décembre 2019, le Bureau disposait de 500 pour cent de poste (sur un effectif autorisé de 515 %) et employait six personnes. Quatre d'entre elles ont une formation en droit, tandis que les deux collaborateurs restants sont respectivement informaticien et réviseur spécialisé en informatique.

Ueli Buri (délégué à la protection des données) dirige le Bureau depuis le 1er mars 2019. A ce titre, il chapeaute la direction stratégique du Bureau ainsi que la définition des objectifs de prestation annuels et gère la conduite du personnel et les tâches opérationnelles. Par ailleurs, il suit principalement les activités de trois Directions (DTT, DIJ, DSE), de la Chancellerie d'Etat et des autorités de justice.

Anders Bennet (délégué à la protection des données suppléant, responsable informatique) est informaticien et assume depuis environ dix ans une fonction de réviseur informatique comme employé du canton de Berne. Sa tâche première au sein du Bureau comprend la planification des contrôles des systèmes et applications en service et leur exécution, ainsi que le suivi de la mise en œuvre des mesures organisationnelles et techniques dans le domaine SIPD.

Rahel Lutz (déléguée à la protection des données suppléante, responsable juridique) est avocate et travaille depuis 2009 pour le Bureau. Elle a pris la tête des domaines de la santé et de la formation en 2012 et est l'interlocutrice de la DSSI et de l'INC pour toutes les questions relevant de la protection des données. Elle vérifie les aspects juridiques des documents SIPD lors des contrôles préalables.

Liz Fischli-Giesser (collaboratrice scientifique, domaine juridique) est avocate et travaille depuis 2012 pour le Bureau. Elle est principalement responsable de la FIN et de la DEEE, de la vidéosurveillance en général et des questions relatives aux paroisses.

Daniel Stucki (collaborateur scientifique, domaine juridique) est avocat et actif depuis 2008 dans la branche informatique. Il travaille depuis début 2019 pour le Bureau et se charge principalement de fournir des conseils et des renseignements et de procéder aux contrôles préalables dans les domaines de la santé et de la formation.

Urs Wegmüller (collaborateur scientifique, domaine informatique) travaille depuis 2000 dans le domaine de la sûreté de l'information. Il a pris ses fonctions auprès du Bureau en 2017 et veille aux aspects techniques des contrôles préalables.

En 2019, les charges d'exploitation du Bureau s'élevaient au total à 202 milliers de francs (budget: 227 milliers de fr.). Dans leur vaste majorité (160 milliers de fr.), ces charges ont été générées par des prestations externes ayant servi aux contrôles informatiques.

Au sein de l'administration cantonale, d'autres organismes se chargent de conseiller les autorités dans le domaine SIPD. Les Directions et la Chancellerie d'Etat disposent chacune d'au moins un organe de référence pour la protection des données, formé pour conseiller les offices et services, et d'un responsable de la sécurité informatique. Les autorités communales peuvent prendre leurs informations auprès de l'Office des affaires communales et de l'organisation du territoire pour les questions de protection de données d'ordre général et auprès des Directions et de la Chancellerie d'Etat pour les questions particulières (p. ex. concernant la numérisation de l'école). Dans la poursuite de son objectif d'augmenter la prise de conscience et le savoir-faire de toutes les autorités dans le domaine de la protection des données, le Bureau s'applique actuellement à porter un soin tout particulier à son réseau de partenaires au sein de l'administration et à le développer. Il accorde par ailleurs une attention spéciale aux contacts institutionnels avec les autorités qui sont régulièrement confrontées à des questions compliquées relevant du droit de la protection des données (p. ex. OIO, Bedag SA et groupe de l'Ile [Insel Gruppe SA]).

Membre de privatim, la Conférence des préposé(e)s suisses à la protection des données, le Bureau entretient des relations avec ses homologues des autres cantons et avec le PFPDT. Il s'agit, d'une part, de garantir l'échange de savoirs et d'expériences pour les questions qui se posent de la même manière dans tous les cantons et, d'autre part, de coordonner les activités de surveillance dans les projets intercantonaux. Le délégué à la protection des données est membre du comité de privatim et il y a toujours une personne du Bureau dépêchée pour participer aux groupes de travail thématiques (actuellement: cyberadministration, sécurité et TIC). Par ailleurs, la poursuite des activités du groupe de travail «Santé» fait suite à l'initiative du Bureau.

6 Présentation des tâches quotidiennes

La présentation suivante propose un choix parmi tous les domaines et toutes les affaires qui ont occupé le Bureau. Ont été retenues les affaires qui revêtent une importance particulière sous l'angle technique et les tâches qui illustrent bien le travail du Bureau.

6.1 Conseils

6.1.1 Autorités

Publication des adresses des propriétaires sur Internet

Public, le registre foncier doit garantir la publicité des informations sur les rapports de propriété et permettre une identification des propriétaires. Le droit du registre foncier fédéral prévoit certes que les noms, dates de naissance et lieux d'origine soient communiqués, mais ne mentionne pas l'adresse. L'explication réside certainement dans le fait qu'il n'existe pas d'obligation d'actualiser le registre foncier. Dans le canton de Berne, l'adresse est tirée de la GCP et mise à jour, ce qui accroît la pertinence du registre public. Cependant, l'information permet des conclusions qui n'ont rien à voir avec le registre foncier. Il est par exemple possible de savoir quand l'un des deux copropriétaires ne vit plus dans le logement qui lui appartient. En cas de publication des adresses des propriétaires sur Internet, un moyen technique doit exister pour que les personnes qui invoquent un intérêt digne de protection puissent demander le blocage de leur adresse.

Accès aux dossiers du domaine de la protection de l'enfant et de l'adulte

Précédemment, un audit effectué auprès des APEA avait révélé que chacun des membres de l'autorité et des collaborateurs pouvait accéder à l'ensemble des dossiers des onze autorités régionales par l'intermédiaire du programme GEVER. Or un tel accès dépasse largement le cadre nécessaire à l'accomplissement de la mission qui leur est confiée. Une nouvelle version du système GEVER permet à présent l'octroi différencié des droits d'accès, de sorte qu'ils se limitent aux dossiers de l'APEA pour laquelle travaille la personne. Pour les membres de l'autorité qui assurent une permanence pour plusieurs régions, pour certains collaborateurs des chancelleries et pour le secrétariat du directoire, qui doivent au besoin avoir encore la possibilité d'accéder à tous les dossiers, un historique de journalisation et des contrôles par sondage doivent garantir que les accès ne sont utilisés que si une tâche concrète le requiert impérativement, conformément aux instructions.

Perte d'une clé USB

L'article 8 OiDPD, ordonnance entrée en vigueur en septembre 2018, prévoit qu'en cas de violation de la protection des données l'autorité responsable la notifie sans délai au Bureau (*data breach notification*). Il faut noter que même les autorités qui ne sont pas soumises à cette ordonnance prennent la problématique de la violation de la protection des données au sérieux. Preuve en est qu'une autorité cantonale du domaine de la santé a communiqué au Bureau une violation de ce type, sans pourtant y être tenue. Dans le cadre d'une procédure de révision, elle avait envoyé au CF une clé USB sous pli postal; cette dernière contenait entre autres des données personnelles faisant l'objet d'une obligation particulière de garder le secret qui n'étaient pas chiffrées. La clé a supposément été retirée de son enveloppe à l'aide d'un couteau avant que le personnel du CF n'ait pu récupérer le courrier de la case postale. L'annonce faite volontairement par l'autorité est un signe jugé très positif par le Bureau et la gestion des erreurs mise en place par cette autorité peut servir d'exemple. La révision prévue de la LCPD créera une obligation générale d'annoncer les violations de la protection des données. Le Bureau continue d'accepter les annonces volontaires des autorités qui ne sont pas assujetties à l'OiDPD.

Remise des données secondaires d'un membre du corps enseignant à l'autorité d'engagement

Une autorité d'engagement voulait obtenir les données secondaires de Microsoft Office 365 d'un de ses employés, qui travaillait à domicile, afin de pouvoir vérifier l'exactitude des périodes de travail saisies. Les données secondaires sont des informations sur l'utilisation (p. ex. qui a utilisé quelle application et pour quelle durée). Vu l'ordonnance sur le personnel, le Bureau a précisé les conditions du traitement de ces données comme suit: La surveillance ne peut avoir lieu qu'en présence d'un soupçon d'abus suffisamment étayé et qu'après avoir été annoncée. Depuis le 1er janvier 2020, l'ordonnance sur les données secondaires de communication règle l'enregistrement et l'évaluation de ces données de manière contraignante au niveau cantonal (ch. 6, lit. *b*).

Remise de données personnelles à une Eglise nationale

Au 1er janvier 2020, les Eglises nationales sont devenues responsables de leur propre personnel conformément à la LEgN. Jusqu'à cette date, c'est le DAE qui assumait cette responsabilité. La nouvelle loi règle aussi le transfert des rapports de travail, mais, étant donné qu'elle n'entrait pas en vigueur avant 2020, la question s'est posée de savoir à partir de quand les données personnelles pouvaient être transmises à l'Eglise réformée évangélique. Le Bureau est parvenu à la conclusion que l'Eglise nationale avait le droit d'obtenir les données

des ecclésiastiques dont elle devenait responsable quelques mois avant l'entrée en vigueur de la loi afin qu'elle dispose du temps nécessaire pour gérer les salaires et préparer les autres aspects relevant du droit du personnel.

Projet de recherche sur la violence domestique

Le Service de lutte contre la violence domestique de la POM a demandé au Bureau de suivre le début du projet de recherche sur la violence domestique, auquel participent les autorités de deux cantons ainsi que des associations privées. Les données traitées dans le cadre du projet sont sensibles, particulièrement dignes de protection et placées sous le sceau du secret. La protection des données devait donc dès le début être prise en compte de manière appropriée. Un tableau a été remis aux participants pour qu'ils connaissent leurs obligations précises en matière de protection des données.

6.1.2 Personnes concernées

Médiation dans le cadre de la consultation d'un dossier auprès de la Police cantonale (POCA)

Lors de la consultation de son dossier, un citoyen n'a pas trouvé toutes les informations qu'il attendait. Il a donc pris contact avec le Bureau, qui a joué son rôle d'intermédiaire en vérifiant que le système mobile qui permet d'interroger les bases de données de la POCA ne contenait pas d'autres renseignements que ceux soumis au citoyen. L'information que ce dernier voulait trouver portait sur le fait qu'il fallait contacter un interlocuteur spécifique de la POCA pour toutes les circonstances liées à une personne précise. Or il s'agissait d'un ordre de service interne destiné au corps de police et ne relevait donc aucunement de la catégorie des données personnelles pour lesquelles un droit de consultation doit être accordé.

Remise de listes d'adresses aux sociétés de tir

Des jeunes gens ont régulièrement reçu des invitations non sollicitées de la part de sociétés de tir. Le Bureau a reçu une demande à propos du droit des communes de transmettre des adresses aux associations en question. Il s'est avéré que les cours de jeunes tireurs sont considérés comme une formation avant l'entrée en service au sens de l'ordonnance fédérale concernée. Aussi les communes sont-elles autorisées à donner les adresses des jeunes de 15 à 20 ans aux sociétés de tir.

Sites Internet des autorités

1. Collecte des adresses IP lors de l'envoi d'un formulaire en ligne
Une personne ayant soumis un formulaire de contact sur le site de la POCA a demandé au Bureau si la collecte de son adresse IP était légale. La responsabilité du contenu et d'une configuration conforme aux règles appartient à l'autorité qui publie un formulaire en ligne. Elle doit disposer d'une base légale suffisante pour recueillir chacune des données, ce qui n'allait en l'occurrence pas de soi. Le Bureau a estimé que la collecte séparée de l'adresse IP était inutile et a recommandé à la POCA d'y renoncer à l'avenir. En effet, les adresses IP communiquées par l'intermédiaire du formulaire en ligne sont déjà enregistrées de manière centralisée pour des raisons techniques et conservées durant une période relativement courte avant d'être automatiquement supprimées. Etant donné qu'il est possible de s'adresser à la POCA par d'autres moyens, le Bureau a renoncé à la rédaction formelle d'une proposition motivée.

2. Installation de cookies
Un établissement de droit public a publié sur son site Internet une déclaration de protection des données mentionnant l'installation de cookies que les visiteurs n'avaient pas la possibilité de refuser. Un entretien avec les personnes responsables a servi à distinguer les cookies qui pouvaient être installés par des autorités (à savoir ceux qui sont indispensables au bon fonctionnement) des autres (ceux qui visent uniquement de meilleures conditions d'utilisation ou ceux qui sont prévus à des fins commerciales). Le site Internet en question a été modifié dans un délai raisonnable.

Cas de sosie

Troublée, une citoyenne a indiqué au Bureau qu'une photo de son père décédé, probablement prise dans un hôpital bernois, se trouvait sur Internet et servait à illustrer des articles. Le Bureau lui a donné des conseils qui lui ont permis de découvrir, après quelques recherches, que la personne photographiée n'était pas son père mais celui du photographe lui-même. Les deux hommes étaient si semblables que leurs enfants ne pouvaient pas les différencier au premier coup d'œil.

Numérisation de l'école obligatoire

L'école obligatoire relève des communes et les établissements sont par conséquent soumis à leur organe de surveillance de la protection des données (ou alors à celui des syndicats de communes concernés). Néanmoins, le Bureau reçoit régulièrement des demandes pour ce domaine. L'utilisation du produit édité par Google «G Suite for Education» et de Google Chrome Books pose des questions complexes qui sont une source permanente de préoccupation pour les autorités communales comme pour les parents. Les divers courriers envoyés

directement ou en copie au Bureau montrent que les parents portent un regard critique sur les conditions d'utilisation de Google. Au niveau cantonal, on s'efforce de soutenir les écoles par différents moyens pour les questions liées au droit de la protection des données. Par exemple, la Haute école pédagogique de Berne propose non seulement différentes ressources auxiliaires ainsi que des prestations de conseil, mais aussi un outil en ligne qui permet aux écoles de générer un prospectus de sensibilisation sur la base d'un système de feux tricolores. En outre, le Bureau essaie, dans le cadre des activités de privatim, de faire en sorte que les contrats-cadre conclus par l'agence spécialisée «educa.ch» avec les gros fournisseurs de logiciels offrent aux institutions helvétiques de formation des conditions conformes au droit suisse et respectant les exigences en matière de protection des données.

Transmission du numéro AVS des participants dans le cadre d'un cours de la protection civile

Une personne servant dans la protection civile a demandé au Bureau si l'envoi d'une liste avec son numéro AVS à tous les participants d'un cours de service était admissible. Faisant suite à cette demande, le Bureau a pris contact avec l'office de la protection civile concerné dans le cadre de ses activités de surveillance et l'a interrogé sur le but de la démarche ainsi que sur les bases légales qui lui permettaient de transmettre le numéro AVS, les informations sur l'activité professionnelle des participants et leur date de naissance. L'autorité a répondu qu'il s'agissait d'un essai et que la liste avait été envoyée à la demande des participants, tout en ajoutant que les trois catégories de données avaient été définies dans le cadre de procédures internes. Le Bureau a constaté que la transmission de ces informations n'avait pas de fondement juridique au-delà de cette première expérience et n'était donc pas admissible. Par contre, le traitement interne des trois catégories de données par l'autorité dans le cadre de l'accomplissement du mandat qui lui était confié repose sur des bases légales suffisantes. Le Bureau a donc demandé à l'office de modifier la convocation relative à la protection civile.

La LCPD protège-t-elle les dénonciateurs anonymes?

Une personne voulait savoir si la LCPD la protégeait dans son anonymat en cas de dénonciation, en l'occurrence auprès de la police. Il faut d'abord établir si cette loi est applicable ou non. C'est seulement le cas lorsque la dénonciation ne donne lieu ni à une procédure pénale ni à une procédure de justice administrative; sinon, les dispositions procédurales s'appliquent. Si les circonstances sont régies par la LCPD, la protection lors de la consultation des documents par la personne dénoncée se limite au seul cas où la personne qui a dénoncé peut faire valoir un intérêt particulièrement digne de protection. La jurisprudence fixe des critères très élevés pour définir l'existence d'un intérêt de la sorte: il faut par exemple la preuve d'un risque concret pour l'intégrité ou d'une menace

sérieuse sur la personnalité. Il s'agit d'une situation exceptionnelle; ainsi, la personne qui a émis la dénonciation doit en général assumer son acte.

6.2 Prises de position formelles

Loi sur les fichiers centralisés de données personnelles (LFDP)

La nouvelle loi doit créer la base légale permettant aux données personnelles que plusieurs autorités ont besoin de traiter pour accomplir leurs tâches d'être rassemblées dans des fichiers centralisés. Seules les autorités qui disposent d'une base légale suffisante dans leur domaine pour le traitement des données pourront accéder à ces fichiers. En guise de solution transitoire, l'annexe de la LFDP présume que les catégories de données expressément mentionnées pour chaque loi spéciale sont nécessaires à l'accomplissement des tâches. A moyen terme, ces lois spéciales devront être complétées (dans le cadre des projets actuels de révision; les compléments nécessaires ont par exemple déjà été apportés à la loi sur le notariat). Tandis qu'à présent les accès à GERES doivent être octroyés par le Conseil-exécutif à l'issue d'un processus politique, les Directions pourront à l'avenir décider elles-mêmes de l'octroi des autorisations nécessaires dans leurs domaines. La mesure vise à casser la rigidité des procédures. En parallèle, chaque nouvelle réglementation concernant les droits d'accès devra être soumise à l'examen du Bureau, qui pourra porter les divergences notoires jusque devant le Tribunal administratif, assurant ainsi un contrôle de leur admissibilité sur le plan juridique. L'office responsable du projet législatif (OIO) a impliqué activement le Bureau dès les travaux préparatoires, de sorte que le projet de loi adopté par le Conseil-exécutif prend au mieux en compte la protection des données.

Ordonnance sur les données secondaires de communication (ODSC)

La révision de la loi sur le personnel, entrée en vigueur au 1er janvier 2020, a donné lieu à de nouvelles prescriptions concernant le traitement des données secondaires résultant de l'utilisation de l'infrastructure électronique par les employés de l'administration cantonale. Celles-ci se verront concrétisées par l'ODSC. Le Bureau a pu participer tôt aux travaux et par conséquent approuver le projet final de l'ordonnance. Bien que cette dernière s'appuie sur le droit fédéral, elle apporte aussi quelques précisions et prévoit des règles plus strictes pour la protection des données du personnel de l'administration cantonale. Par exemple, l'exploitant du système ou les services désignés par les prescriptions SIPD ne peuvent procéder à des évaluations non nominales se rapportant aux personnes que sur mandat de l'autorité responsable ou avec son

accord. En outre, ces évaluations doivent se limiter à des pointages. Le rapport contient des explications et des remarques claires pour une application de l'ODSC conforme à la protection des données.

eDéménagement (fin de la 1re phase)

Il s'agit d'un projet exploratoire du canton de Berne devant permettre aux citoyens et citoyennes d'annoncer leur changement de domicile non pas en se rendant au guichet, mais en ligne. L'Office des affaires communales et de l'organisation du territoire a mis un terme à la première phase du projet et lancé la deuxième phase le 23 septembre 2019. L'avis du Bureau a été entièrement pris en compte concernant la première phase avant que la suite du projet soit autorisée. La prochaine étape consistera en un examen de la sûreté de l'information mené par un prestataire externe. Dans le cadre de l'affaire, le Bureau reste en contact avec les responsables de la protection des données des autres cantons, puisque le projet eDéménagement est déployé sur l'ensemble de la Suisse (de manière probatoire ou productive) et doit donc donner lieu à une coordination entre les autorités de surveillance.

Révision de 2020 de la loi sur l'école obligatoire

Le Bureau a été invité à donner son opinion lors de la préparation du projet législatif avant son envoi en procédure de consultation. Dans son corapport, le Bureau a indiqué que la base légale prévue pour la communication de données servant à l'établissement des besoins des enfants et des jeunes en matière de pédagogie spécialisée n'était pas suffisante parce que les données personnelles concernées étaient considérées comme particulièrement dignes de protection. Les remarques sont restées sans effet, malgré le manque d'argument convaincant. Le Bureau a fermement exprimé une nouvelle fois son avis dans le cadre de la procédure de consultation.

Ordonnance portant introduction de la législation fédérale sur l'enregistrement des maladies oncologiques (OiLEMO)

La loi fédérale sur l'enregistrement des maladies oncologiques et l'ordonnance qui s'y rapporte sont entrées en vigueur au 1er janvier 2020. Lors de la procédure de corapport sur l'ordonnance cantonale d'application, le Bureau a suggéré l'ajout au catalogue du contrat de prestation établi par l'Office du médecin cantonal et l'organe d'enregistrement du cancer de quelques éléments minimaux relevant du droit de la protection des données et de ses aspects techniques. La SAP a repris la proposition d'ajouter les dispositions en matière de sûreté de l'information et de protection des données et l'obligation de remettre les données à la nouvelle institution cantonale en cas d'expiration du contrat. Par contre, l'obligation de supprimer les données après leur transmission à une nouvelle

institution a été jugée superflue. Etant donné que le transfert des données électroniques ne signifie pas automatiquement que le service qui y procède n'en dispose plus lui-même, il aurait été souhaitable que l'acte législatif le mentionne explicitement. Toujours est-il que la règle générale de la LCPD reste applicable et que les données devenues inutiles sont à supprimer. Le droit de traitement étant transmis à la nouvelle institution, l'ancienne perd le sien et doit donc supprimer les données.

Révision de la loi sur les soins hospitaliers (LSH)

Dans son corapport concernant la révision de la LSH, le Bureau a été particulièrement attentif à la disposition relative à la fourniture des données. Les hôpitaux répertoriés doivent fournir les données administratives et désormais aussi médicales concernant les prestations cofinancées par le canton sans anonymisation préalable, dans la mesure où elles sont indispensables à un contrôle efficace de la facturation. Etant donné que ce contrôle était auparavant effectué par les caisses-maladie sur la base d'une convention collective et non par le canton, la conformité de la nouvelle procédure au droit de la protection des données était pour le Bureau sujette à caution. Il a demandé à la SAP de bien vouloir tirer au clair avec lui les questions encore ouvertes. De là est né un échange constructif qui a permis une consolidation du projet soumis à la procédure de consultation.

Procédure de consultation fédérale concernant la modification de la loi sur les profils d'ADN

La Confédération veut désormais permettre le phénotypage, à savoir l'établissement des caractéristiques morphologiques (comme la couleur des yeux, des cheveux et de la peau), à partir du matériel ADN trouvé là où un acte punissable a été commis. Dans l'ébauche de la prise de position du canton de Berne, la POM voulait étendre les analyses permises à d'autres caractéristiques (comme le daltonisme congénital). Le Bureau s'est opposé à la demande au motif que l'atteinte aux droits des personnes qui seraient prises en compte à cause de leur conformité avec les résultats d'analyse serait notablement plus marquée.
En effet, ces personnes devraient notamment donner un aperçu de leur état physique, qui constitue une information particulièrement digne de protection.
Malheureusement, le Conseil-exécutif n'a pas tenu compte des objections du Bureau et a approuvé la prise de position rédigée par la POM.

6.3 Contrôles préalables

6.3.1 Projets informatiques

Les projets devant être soumis au Bureau pour le contrôle préalable sont ceux qui prévoient le traitement des données (régulièrement par voie électronique) d'un grand nombre de personnes (critère quantitatif) et qui satisfont à au moins un des critères qualitatifs suivants: lorsqu'il ne peut être établi avec certitude qu'une base légale suffisante existe, lorsqu'il s'agit de données personnelles particulièrement dignes de protection ou pour lesquelles il existe une obligation particulière de garder le secret ou lorsque les moyens techniques présentant des risques particuliers pour les droits de la personnalité des personnes concernées sont employés.

En 2019, le Bureau a traité 113 contrôles préalables concernant des projets informatiques (2018: 71) et en a achevé 69 (2018: 28), soit 61,06 pour cent (2018: 39,44 %). Une procédure standardisée a été introduite au printemps 2019: (1) réception des documents SIPD; (2) première lecture (admissibilité); (3) amélioration éventuelle de la part de l'autorité; (4) contrôle préalable (examen des aspects juridiques et techniques, rédaction d'une ébauche de rapport avec indication de la significativité élevée, moyenne ou faible des points examinés); (5) prise de position de l'autorité lorsque le degré de significativité est élevé ou moyen; (6) contrôle, rédaction du rapport de contrôle préalable selon les standards prévus et clôture de la procédure.

Gestion électronique des affaires (GEVER), mandants des Directions et des offices

Le contrôle préalable du concept SIPD «BE-GEVER – application de groupe», valable pour tous les mandants, était tout à fait atypique. En effet, le projet se décrivait au début comme une seule application prévoyant plusieurs possibilités de configuration spécifique et son utilisation pour le traitement concret des données personnelles n'était pas défini. Il faut donc établir pour chaque mandant d'une Direction ou d'un office un concept SIPD complémentaire à soumettre au Bureau pour le contrôle préalable. Lors de ce contrôle, le Bureau vérifie quelles données personnelles sont traitées – pour les unités qui travaillent avec des applications spécialisées, il peut s'agir uniquement des données des collaborateurs selon les circonstances – et si l'accès aux données particulièrement dignes de protection est adéquatement restreint (les informations à cet égard sont déduites à partir du plan de classement et des directives de l'unité organisationnelle). Par ailleurs, les règles s'appliquant à la conservation et à l'archivage font l'objet d'un contrôle de plausibilité et la manière dont les droits des personnes concernées sont garantis est examinée (notamment pour ce qui est de l'accès aux renseignements, de la consultation et du blocage des données).

Poste de travail cantonal (PTC) 4.0

Le contrôle préalable du projet PTC 4.0 peut aussi être décrit comme atypique dans la mesure où ce projet donne lieu à une pluralité de traitements des données à l'aide des applications les plus variées. C'est pourquoi le système doit permettre un traitement des données personnelles particulièrement dignes de protection et proposer pour ce faire une sécurité suffisante. Finalement un audit a été mené après la mise en service pour savoir si le système remplissait ces conditions (ch. 6, lit. *d*).

Suisse ePolice deux

L'application «Suisse ePolice deux» est un portail qui permet à tout un chacun d'annoncer au corps de police cantonal compétent les petites infractions et les événements de son ressort. L'application est exploitée par l'association chargée de l'harmonisation de l'informatique policière suisse (HIP), à laquelle appartiennent tous les corps de police cantonaux. En tant qu'autorité compétente pour son domaine, la POCA a déposé le projet pour le contrôle préalable. Elle souhaitait que l'examen du Bureau vaille pour tous les cantons, ce qui est formellement impossible au vu de la situation juridique actuelle. Les documents transmis étaient de bonne facture, de sorte que le contrôle préalable a pu être achevé avec succès, même s'il n'a été effectué qu'après la mise en ligne du service. Avec l'accord de l'association HIP, le Bureau a transmis son rapport aux autorités de surveillance des autres cantons. La portée nationale de l'application a une fois de plus montré la nécessité d'une coordination entre les autorités cantonales de surveillance de la protection des données.

Applications spécialisées de la POCA

Sous un angle purement cantonal, la POCA a soumis d'autres nombreux systèmes et applications au contrôle préalable du Bureau, comme un système de consultation des différents registres policiers d'information, un système d'aide à l'engagement ainsi que le projet du mandant GEVER. Etant donné qu'un concept de la protection de base avait déjà été examiné par le Bureau et que les exigences principales documentées en matière de sécurité (concernant notamment le lieu et la protection du centre de calcul) étaient respectées, il n'est pas nécessaire de vérifier de nouveau chacun des aspects lors des contrôles préalables.

Competella

Le système de gestion «Competella» permet aux autorités administratives ou judiciaires une analyse complète des données de téléphonie secondaires (qui parle avec qui et pour combien de temps; quel appel avec quelle personne

aboutit à quelle vitesse ou n'aboutit pas; quel appel est interrompu, etc.). Une telle analyse relève dans une grande mesure de la protection des données du personnel cantonal mais aussi des clients. Lors de la rédaction du présent rapport, le contrôle préalable ne s'était pas encore achevé. Une chose est sûre: des analyses de ce type doivent se limiter au cadre prévu par les nouvelles dispositions de la loi sur le personnel concernant le traitement des données secondaires et l'ordonnance y relative (ch. 6, lit. *b*).

Programme de dépistage du cancer du sein «donna»

En 2018, le Bureau a procédé au contrôle préalable du programme de dépistage du cancer du sein du Jura bernois (programme BEJUNE). En 2019, c'était le tour du programme «donna», qui couvre le reste du territoire cantonal. L'attention du Bureau s'est surtout fixée sur les procédures de travail et les flux de données: de la convocation envoyée aux femmes de la classe d'âge définie à l'envoi des résultats à ces dernières ainsi qu'à leur médecin. Un autre objet du contrôle portait sur le flux de données vers le registre cantonal des tumeurs. Le contrôle s'est déroulé correctement et s'est achevé sans qu'aucun problème majeur ne soit constaté.

A certaines occasions, le Bureau a été consulté à un stade précoce des travaux pour des questions concernant l'obligation du contrôle préalable ou la façon logique de procéder. Il a aussi mené un contrôle à des fins pédagogiques, alors qu'il n'était pas formellement requis.

SOCOM

Le Bureau a reçu l'analyse SIPD de l'application «SOCOM»; l'expéditeur voulait savoir si elle devait faire l'objet d'un contrôle préalable. SOCOM est un logiciel servant à simplifier les procédures d'inscription, de déroulement et de décompte concernant les marchés publics de bétail de boucherie. Une lecture sommaire du projet a montré que les données traitées avec le logiciel n'étaient ni particulièrement dignes de protection, ni soumises à une obligation de garder le secret. Par conséquent, un contrôle préalable au sens de l'article 17a LCPD n'était pas requis. Cette conclusion a été transmise au responsable de la sécurité informatique avec quelques remarques au sujet des mesures de protection SIPD.

Concept portant sur la protection des données de la clinique de réadaptation Schönberg à Gunten

La protection des données intéresse aussi les chefs. Le directeur de la clinique Schönberg à Gunten a remis au Bureau un concept de protection des données en le priant de lui donner son avis et de le conseiller. La démarche a débouché

sur une discussion interdisciplinaire (liant technique et droit) durant laquelle la procédure pour la rédaction d'un concept SIPD complet a été définie. Dans un premier temps, une documentation des infrastructures et des mesures de protection générales y afférentes a été effectuée et soumise au Bureau pour le contrôle préalable (procédure atypique). Ensuite, des documents propres aux applications doivent être élaborés sur la base de la documentation, notamment pour le système de dossier des soins (système d'informations cliniques).

MELBA

L'application «MELBA» de l'Office de l'exécution judiciaire répertorie les compétences individuelles et sociales des personnes qui se trouvent en exécution de peine et gère les exigences professionnelles pour que les qualifications puissent correspondre aux contingences du lieu de travail. Les données personnelles utilisées sont particulièrement dignes de protection, mais le nombre de personnes concernées est si restreint qu'un contrôle préalable n'aurait pas été nécessaire. Etant donné que la nouvelle cheffe de projet responsable de l'application «MELBA» s'occupera prochainement d'autres projets devant faire l'objet d'un contrôle préalable, l'occasion a néanmoins été saisie pour lui permettre de s'exercer, ce qui a porté ses fruits. En effet, la documentation revue sur la base des indications du Bureau était bien meilleure, de sorte que la procédure a pu prendre fin sans autre remarque.

6.3.2 Vidéosurveillance

Ecole d'arts visuels

La POCA, compétente pour l'octroi de l'autorisation, a soumis au Bureau les documents liés à la vidéosurveillance de l'Ecole d'arts visuels du canton de Berne pour qu'il procède à un contrôle préalable. D'une part, la surveillance visait à protéger l'établissement des actes de vandalisme, des dégradations, des vols, etc. D'autre part, il s'agissait d'assurer une protection ciblée des pièces exposées que l'école abrite dans ses locaux en tant qu'annexe des musées de Berne. L'installation de vidéosurveillance, composée de 14 caméras, fonctionne sept jours sur sept, vingt-quatre heures sur vingt-quatre. Le Bureau a envoyé une de ses collaboratrices sur place afin qu'elle observe l'installation. Elle est parvenue à la conclusion qu'à certains endroits (restaurant de l'école, terrasse extérieure et portes d'entrée comprises) le contrôle social exercé par les personnes présentes était suffisant lors des heures d'ouverture du restaurant et qu'un enregistrement porterait inutilement atteinte à la sphère privée des étudiants, du personnel et des visiteurs. Aucune limitation n'a été proposée pour les caméras qui ciblaient les pièces exposées. Dans l'ensemble, le Bureau a trouvé que la vidéosurveillance devait être plus voyante, c'est-à-dire être signalée de manière bien visible.

Hôpital d'Aarberg

L'Hôpital d'Aarberg, qui fait partie du groupe de l'Ile, a envoyé au Bureau les documents relatifs à une installation de vidéosurveillance en temps réel, comprenant six caméras, qui doit garantir le fonctionnement du service médical d'urgence de l'hôpital. La vidéosurveillance ne servait aucun objectif de sécurité policière, mais visait à soutenir l'hôpital dans l'exercice de ses tâches vis-à-vis des patients. Par conséquent, l'autorisation de la POCA n'était pas nécessaire et seul un contrôle préalable s'imposait selon les dispositions de la protection des données. Le Bureau a conclu que l'installation était conforme aux prescriptions relatives à la protection des données dès lors que les mesures techniques et organisationnelles requises étaient prises pour la protection des images et du reste du réseau hospitalier – à savoir la connexion des caméras à un réseau qui leur est dédié, le transfert chiffré des images et le recours à un mot de passe pour y accéder.

6.4 Audits

En 2019, le Bureau a mené six examens dans le domaine SIPD et suivi la mise en place des mesures résultant de sept examens ayant abouti entre 2016 et 2018. Un progrès a généralement été constaté dans le cadre du travail de suivi, même s'il a clairement été établi que la mise en œuvre de mesures parfois très étoffées est chronophage et gourmande en ressources.

Hôpital régional de Haute-Argovie (SRO)

Le SRO exploite, en plus de l'Hôpital de Langenthal, des centres de santé et des logements protégés. Il compte environ 190 lits et une patientèle annuelle de 8600 personnes séjournant à l'hôpital et de 49 000 personnes en traitement ambulatoire. Il emploie environ 1100 collaborateurs. L'exploitation de l'infrastructure informatique est en grande partie assurée par le personnel. Des spécialistes externes interviennent dans le cadre de projets ou pour fournir des prestations. Quelque 1300 postes de travail informatiques équipés des systèmes techniques de base sont gérés et administrés de manière centralisée. Au moment de l'examen, de très gros projets concernant l'infrastructure informatique étaient en cours ou prévus.

L'examen de la protection de base de l'infrastructure informatique a porté sur la conduite et l'orientation en matière de sûreté de l'information et de protection des données, les concepts SIPD et les mesures de protection qui en découlent, la gestion des accès, l'administration des données, la sécurité des réseaux, serveurs et clients, la gestion du changement, les conventions conclues avec des tiers (externalisation) et la sécurité du site (salle des serveurs).

Globalement, l'examen a révélé un potentiel d'amélioration et d'optimisation notable dans tous les domaines. Dans un milieu hospitalier où l'organisation est complexe et les infrastructures techniques et technologiques sont hétérogènes, il est nécessaire d'affermir sans relâche la position du domaine SIPD, en raison particulièrement des ressources disponibles que limite la pression générale exercée sur les coûts. Cependant, l'examen a aussi montré qu'on n'avait pas lésiné sur les efforts fournis afin de combler les déficits et de diminuer les risques existants à l'aide de mesures appropriées. L'examen s'est déroulé dans une ambiance très constructive et professionnelle.

Le Bureau accompagnera l'hôpital dans la mise en œuvre des mesures d'amélioration. En outre, il prévoit de mener un examen pour suivre l'évolution du domaine de la technique médicale.

Clients Windows 10 dans les écoles

L'INS propose notamment des clients Windows 10 (eduClient) aux écoles cantonales dans le cadre de l'offre «EDUBERN».

L'examen a porté sur la conduite et l'orientation en matière SIPD ainsi que les contrôles appropriés, les mesures de protection appliquées aux clients, l'administration des clients tournant sous Windows 10, le comportement des utilisateurs, les profils d'utilisateur existants et les droit d'accès, la protection prévue contre les logiciels malveillants et la gestion du changement.

Globalement, l'examen a révélé un potentiel d'amélioration et d'optimisation dans tous les domaines. D'une manière générale, il a cependant été constaté que la gestion des clients Windows 10 répondait déjà dans une large mesure aux exigences en matière de sécurité de l'information et de protection des données et les attentes prévues par les standards reconnus de la protection de base et les directives concernant les mesures techniques de protection étaient presque toujours satisfaites. Des imperfections ont été repérées dans la répartition des compétences, qui manquait de clarté, et dans le traitement des données sur les clients mis à disposition. Les obligations des écoles, en leur qualité de bénéficiaires des prestations et d'organe procédant au traitement des données, restaient en particulier à définir de façon univoque. De plus, de vastes questions se posaient en matière de protection des données quant à l'empressement à recourir aux nouvelles technologies – comme l'utilisation du nuage, des applications, etc. – par les écoles qui, vu la pratique qui se dessine actuellement dans un environ-

nement en perpétuelle mutation, devaient trouver autant que faire se peut une réponse. La collaboration, professionnelle, a atteint son but.

Le Bureau accompagnera les écoles dans la mise en œuvre des mesures d'amélioration.

Réseau sans fil de l'administration cantonale

L'OIO propose un réseau sans fil (BE-Net WLAN) dans le cadre de la fourniture des services de base TIC. Ce service permet aux clients d'établir une connexion sans fil avec le réseau cantonal. Lors de l'examen, on comptait quelque 1000 points d'accès actifs administrés sur plus de 100 sites. Le réseau sans fil est exploité par un prestataire externe.

L'examen a porté sur une sélection de sites et de réseaux. Les sites ont été retenus car ils étaient très fréquentés. Le risque d'une infiltration prévue ou non du réseau cantonal tend probablement à être plus élevé à ces endroits. L'évaluation de la sécurité du réseau sans fil et sa robustesse sont les principaux points examinés. D'autres aspects ont également été étudiés: les processus opérationnels tels que le contrôle des modifications (gestion des changements et des mises à jour), la gestion de configuration, le monitorage, la sécurité des lieux, la sécurité du réseau et les zones de réseau.

Globalement, l'examen a révélé un potentiel d'amélioration et d'optimisation ponctuel dans tous les domaines. En bref, le réseau sans fil opérationnel répond à la plupart des attentes en matière de sécurité et l'infrastructure technique utilisée dispose de mécanismes de protection techniques presque toujours adéquats. Des manques ont surtout été remarqués dans le monitorage systématique et continu ainsi que dans la rapidité de la réaction en cas de dysfonctionnements et d'anomalies. L'examen s'est déroulé de façon professionnelle.

Les mesures d'amélioration recommandées ont déjà partiellement été mises en œuvre ou sont en cours de préparation. Le Bureau reste informé de l'avancée de leur mise en œuvre.

Poste de travail cantonal (PTC)

S'agissant des services de base TIC, les PTC forment les fondements techniques servant à l'utilisation des applications spécialisées et des applications de groupe. Lors du contrôle préalable, le Bureau avait constaté que la description du client PTC 4.0 proposé par l'OIO, qui se fournit auprès d'un prestataire externe, ne satisfaisait pas encore pleinement les exigences du domaine SIPD (ch. 6, lit. *c*).

L'examen qui a porté sur les PTC en service s'est fondé sur des entretiens avec les personnes responsables, l'étude de documents pertinents et les tests techniques de sécurité menés afin que les éventuelles lacunes conceptuelles et techniques en matière de sécurité puissent être découvertes et mises en évidence.

Globalement, l'examen a révélé que les parties impliquées compétentes ont déjà mis en place de bonnes bases conceptuelles. Les mesures organisationnelles qui garantissent une exploitation sûre des PTC 4.0 sont nombreuses à avoir été déjà appliquées ou à être planifiées. Sur le plan technique, les PTC 4.0 sont configurés de manière compétente et montrent l'étendue du savoir-faire technique des responsables. Malgré tout, des points faibles ont été constatés dans tous les domaines examinés. La collaboration s'est déroulée de façon professionnelle et exemplaire entre l'ensemble des parties prenantes.

Le Bureau reste informé de l'avancée de la mise en œuvre des mesures d'amélioration.

Clinique Südhang

La clinique Südhang est un centre de compétences pour l'être humain et ses dépendances qui propose un soutien spécialisé aux personnes dépendantes. La clinique de jour de Berne, les services ambulatoires de Berne, de Berthoud et de Bienne font partie des services ambulatoires régionaux proposés par la clinique Südhang. En 2018, l'infrastructure informatique a connu un changement important. La clinique Südhang fait appel à une assistance externe pour administrer et exploiter son infrastructure technique client et serveur ainsi que ses applications spécifiques.

L'examen a avant tout porté sur la conduite et l'orientation en matière de sûreté de l'information et de protection des données, la mise en œuvre des concepts SIPD et les mesures de protection qui en découlent, ainsi que sur les conventions conclues avec des prestataires externes.

Globalement, l'examen a révélé un potentiel d'amélioration et d'optimisation dans tous les domaines. En bref, les nombreuses tâches du domaine SIPD, tant opérationnelles (processus de sécurité et d'exploitation, contrôles, etc.) que stratégiques, présentaient un défi de taille pour l'organisation existante. La clinique va donc prévoir davantage de ressources et diminuer progressivement les risques et les manques constatés dans le domaine SIPD en prenant les mesures nécessaires. La collaboration s'est déroulée de façon professionnelle et dans un bon esprit de coopération entre toutes les parties prenantes.

Le Bureau accompagnera la clinique dans la mise en œuvre des mesures d'amélioration.

Système d'information Schengen (SIS)

Avec l'acquis de Schengen, la Suisse est tenue de garantir une utilisation du SIS qui soit conforme à la protection des données et doit le vérifier périodiquement. Pour le canton de Berne, l'exercice incombe au Bureau. Ce dernier a vérifié en automne 2019 les accès de la police régionale du Seeland – Jura bernois. Sur la base de l'utilisation qui en a été faite, le Bureau a estimé que le système servait à l'accomplissement des tâches de police conformément à son but. Aucune irrégularité manifeste n'a été constatée (p. ex. aucun utilisateur n'a fait de requête sur lui-même ou sur des personnes de la vie publique). Toutefois, le Bureau a remarqué un manque concernant la formation et l'information régulière au sujet du système. Il a donc recommandé aux responsables de combler cette lacune. La POCA a tenu compte de cette recommandation et défini de nouvelles mesures pour l'information et la formation des collaborateurs.

6.5 Autres instruments relevant du droit de la surveillance

Liquidation d'un recours de droit administratif concernant BE-GEVER

En 2018, le Bureau avait formé recours auprès de la FIN contre l'OIO au sujet de l'introduction de BE-GEVER dans une Direction. La procédure a pris fin avec une transaction. L'OIO s'est engagé à faire tout son possible pour mettre en place une authentification à deux facteurs sur les PTC dès 2020. L'ajout de données d'authentification supplémentaires (en plus du mot de passe, comme élément de reconnaissance) lors de la connexion au poste de travail offre une meilleure garantie du fait que la personne connectée est bien celle autorisée et répertoriée par le système. C'est cette norme qui sert aujourd'hui pour le traitement des données personnelles particulièrement dignes de protection. Une authentification forte lors de la connexion au PTC permet de renoncer à une 2FA pour les applications de groupe ou les applications spécialisées. De son côté, le Bureau a reconnu que le droit de la protection des données n'obligeait pas à recourir à une signature électronique dans un système GEVER. Quant à la question qui se posait au sujet de la responsabilité en matière de protection des données dans une administration fragmentée (l'OIO est compétent pour les services de base et certaines applications, tandis que les Directions, offices et services se chargent de l'implantation des applications spécialisées), une solution a été proposée en vue d'une nouvelle loi sur l'administration numérique.

En 2019, aucune proposition motivée au sens de l'article 35, alinéa 3 LCPD n'a été faite et aucun recours administratif ni de droit administratif n'a été formé.

Haute surveillance des autorités communales de surveillance de la protection des données

Compte tenu de l'autonomie communale, la LCPD prévoit que les communes désignent à leur niveau leur propre autorité de surveillance. Le Bureau, qui exerce la haute surveillance sur ces autorités, ne le fait à présent que de manière passive, c'est-à-dire qu'il attend que l'autorité de surveillance de la commune ou qu'une personne concernée se manifeste. Ces autorités présentent entre elles des différences parfois considérables dans leur disponibilité et la qualité de la surveillance. Les questions de droit délicates et les problématiques techniques confrontent souvent les autorités communales et leur organe de surveillance à la limite de leurs capacités. Ils se demandent pourquoi des sujets qui concernent dans la même mesure plus de 300 communes bernoises (p. ex. numérisation de l'école; ch. 6, lit. *a*) doivent être traités au niveau communal. En vue de la révision de la LCPD, le Bureau élabore des propositions afin d'améliorer le soutien accordé aux autorités communales pour les questions relevant de la sûreté de l'information et de la protection des données.

7 Proposition

Prise de connaissance.

8 Glossaire

APEA	Autorités de protection de l'enfant et de l'adulte
BPD	Bureau pour la surveillance de la protection des données du canton de Berne
CF	Contrôle des finances
DAE	Délégué aux affaires ecclésiastiques (délégué aux affaires ecclésiastiques et religieuses à compter du 1er janvier 2020)
DEEE	Direction de l'économie, de l'énergie et de l'environnement
DIJ	Direction de l'intérieur et de la justice
DSE	Direction de la sécurité
DSSI	Direction de la santé, des affaires sociales et de l'intégration
DTT	Direction des travaux publics et des transports
FIN	Direction des finances
GCP	Gestion centrale des personnes
GERES	*Gemeinderegistersysteme* (systèmes des registres communaux)
GEVER	*Elektronische Geschäftsverwaltung* (gestion électronique des affaires)
HIP	Harmonisation de l'informatique policière suisse
INC	Direction de l'instruction publique et de la culture
INS	Direction de l'instruction publique (INC à compter du 1er janvier 2020)
IP	Protocole Internet
LCPD	Loi [cantonale] sur la protection des données
LEgN	Loi sur les Eglises nationales
LFDP	Loi sur les fichiers centralisés de données personnelles
LPD	Loi fédérale sur la protection des données
LSH	Loi sur les soins hospitaliers
ODSC	Ordonnance sur les données secondaires de communication
OiDPD	Ordonnance portant introduction de la directive (UE) 2016/680 relative à la protection des données à caractère personnel
OiLEMO	Ordonnance portant introduction de la législation fédérale sur l'enregistrement des maladies oncologiques
OIO	Office d'informatique et d'organisation

PFPDT	Préposé fédéral à la protection des données et à la transparence
POCA	Police cantonale bernoise
POM	Direction de la police et des affaires militaires (DSE à compter du 1er janvier 2020)
privatim	Conférence des préposé(e)s suisses à la protection des données
PTC	Poste de travail informatique cantonal
SAP	Direction de la santé publique et de la prévoyance sociale (DSSI à compter du 1er janvier 2020)
SIPD	Sûreté de l'information et protection des données
SIS	Système d'information Schengen
SRO	Spital Region Oberaargau (Hôpital régional de Haute-Argovie)
TIC	Technologies de l'information et de la communication
WLAN	Réseau sans fil
2FA	Authentification à deux facteurs

Bureau pour la surveillance de la protection
des données du canton de Berne

Poststrasse 25
3072 Ostermundigen
+41 31 633 74 10
protectiondesdonnees@be.ch

www.be.ch/bpd