Kanton Bern
Canton de Berne

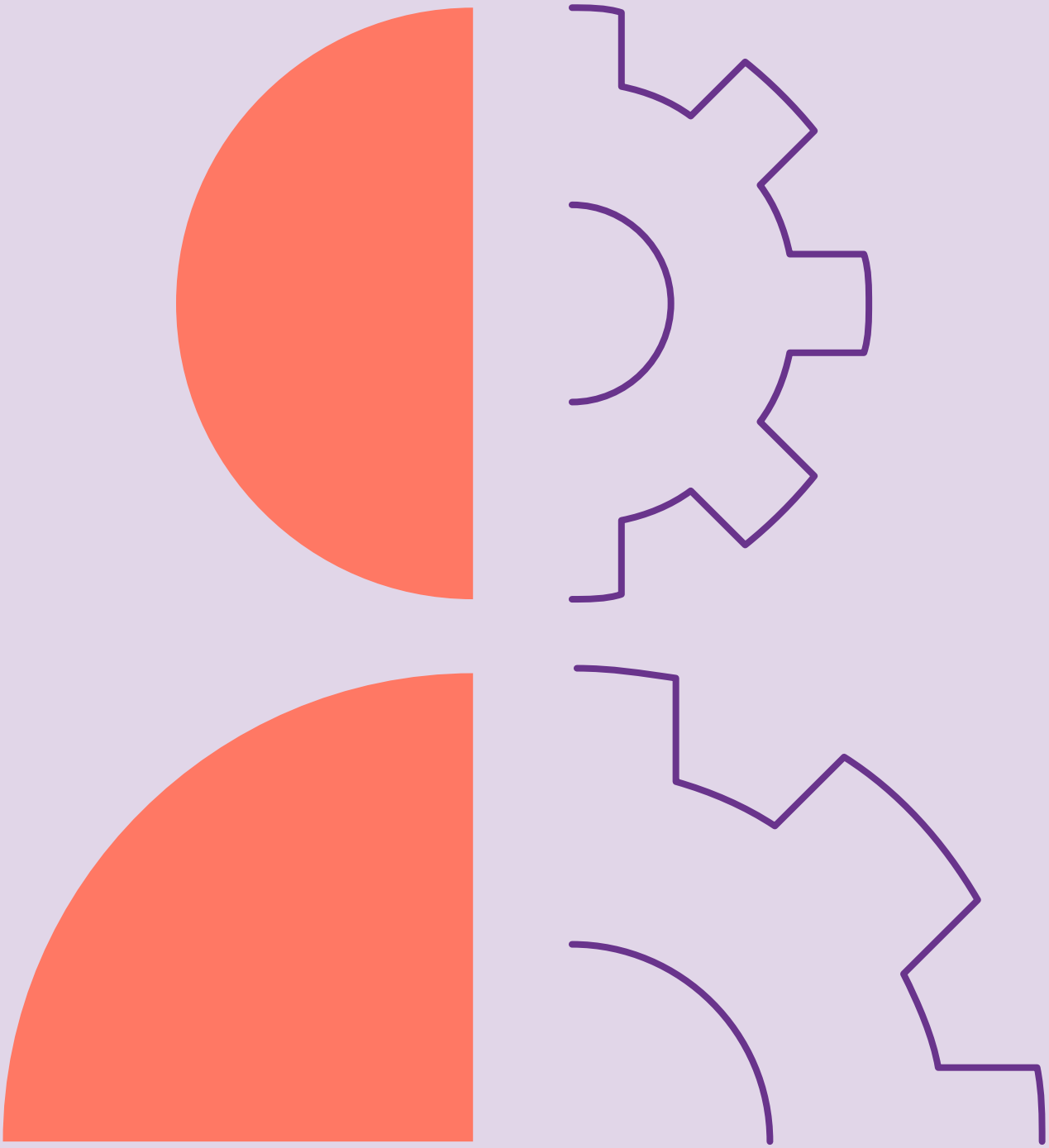
Rapport d'activité Bureau pour la surveillance de la protection des données 2020

Bureau pour la surveillance de la protection des données Février 2021

Impressum

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

Maquette et réalisation : noord.ch



1 Avant-propos

Après les multiples changements intervenus en 2019 parmi le personnel et sur le plan technique, le Bureau pour la surveillance de la protection des données (BPD ; ci-après Bureau) espérait une année 2020 « normale », qui lui permettrait de consolider son organisation interne et ses outils de travail ainsi que ses contacts externes tout en accomplissant ses tâches ordinaires. Mais il y a eu le coronavirus …

Comme le Bureau travaille en très grande partie sur la base de documents électroniques et répond par courrier électronique ou par téléphone à presque toutes les demandes émanant de personnes concernées, il n'a pas eu de difficultés fondamentales à accomplir ses tâches durant les mois où le télétravail a été recommandé ou ordonné. Les seules tâches qui ont été plus compliquées voire impossibles à réaliser ont été les examens relatifs à la sûreté de l'information et la protection des donnés dans les systèmes et applications en service (audits), qui ont normalement lieu dans les services où ils sont utilisés. Ce travail a dû être accompli en partie sous la forme d'entretiens téléphoniques.

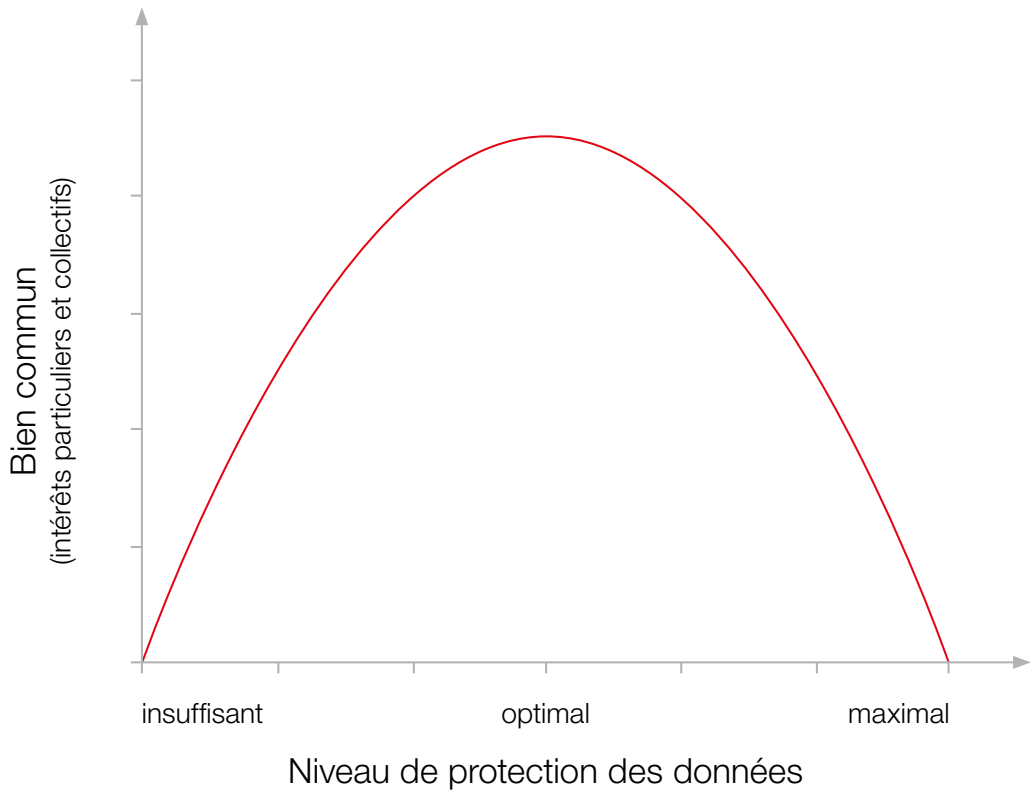
2020 n'en a pas moins réservé un défi particulier : les mesures prises par la Confédération et le canton pour endiguer la pandémie et en atténuer les conséquences sur la vie sociale et économique ont très vite soulevé un grand nombre de nouvelles questions touchant au droit de la protection des données, pour lesquelles les autorités, qui subissaient une pression énorme, mais aussi les personnes concernées (et les médias) voulaient des réponses dans les meilleurs délais. D'aucuns ont même remis intrinsèquement en question le droit de la protection des données, dans lequel ils voyaient un obstacle à une action rapide et efficace des pouvoirs publics. Tout en dispensant ses conseils techniques, le Bureau a donc dû procéder à quelques rappels : notre conception du droit repose sur le principe de l'autodétermination des citoyen·ne·s, y compris dans le domaine de l'information ; de ce fait, leurs droits et leurs libertés ne peuvent être restreints que pour sauvegarder des intérêts publics, comme la protection de la santé ; mais l'action des pouvoirs publics doit toujours respecter les principes fondamentaux de l'Etat de droit, en particulier la légalité et la proportionnalité. C'est pourquoi les autorités ne peuvent pas, selon leur bon vouloir, se mettre soudainement à collecter toutes les données personnelles qui leur sont utiles et à les échanger entre elles. Sinon, nous risquons de nous retrouver subitement dans un Etat policier alors que la législation sur la protection des données est précisément censée nous en protéger. Or, cette législation est tout à fait capable de nous apporter des réponses adaptées même dans des situations extraordinaires grâce à des principes tels que la sauvegarde d'intérêts prépondérants, la proportionnalité du traitement des données et l'adéquation des mesures prises pour préserver la sûreté de l'information.

Ueli Buri, délégué à la protection des données

2 Droit fondamental à la protection des données

La Constitution fédérale et la Constitution du canton de Berne 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 cantonale, 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.



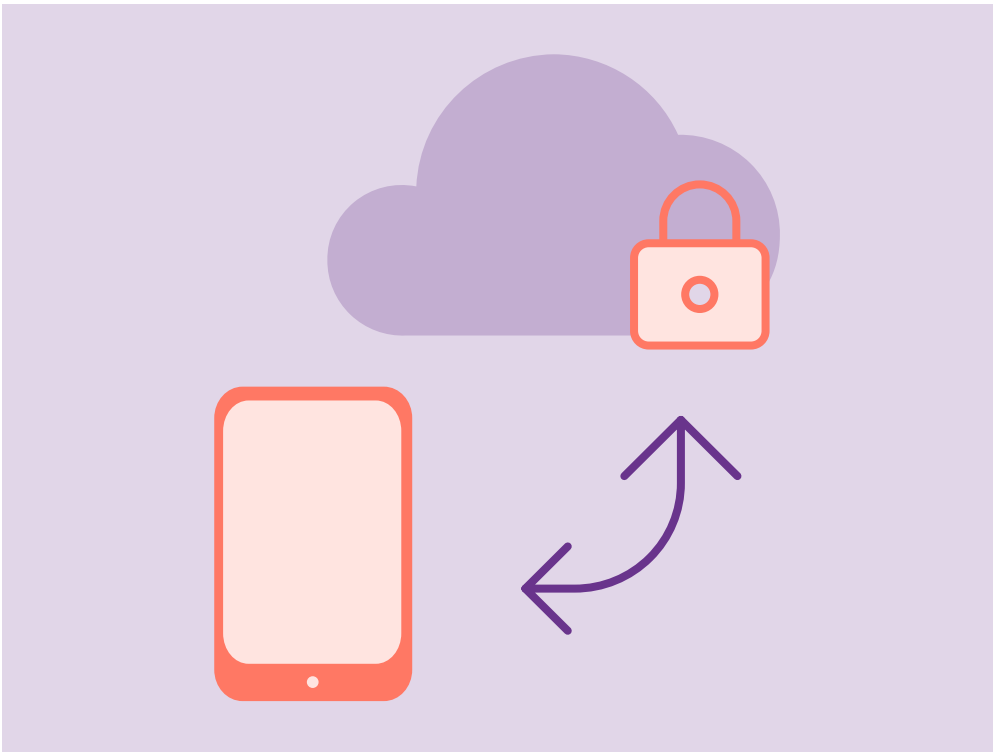
La loi cantonale sur la protection des données (LCPD) précise les devoirs des autorités lors du traitement des données personnelles. Par autorité, il faut comprendre l'administration, mais aussi d'autres entités chargées de tâches publiques comme les écoles et les hôpitaux. Quant au traitement, il se 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. Le recueil de données est autorisé uniquement dans un but déterminé et il est en principe interdit d'utiliser des données à d'autres fins que celles prévues. 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.

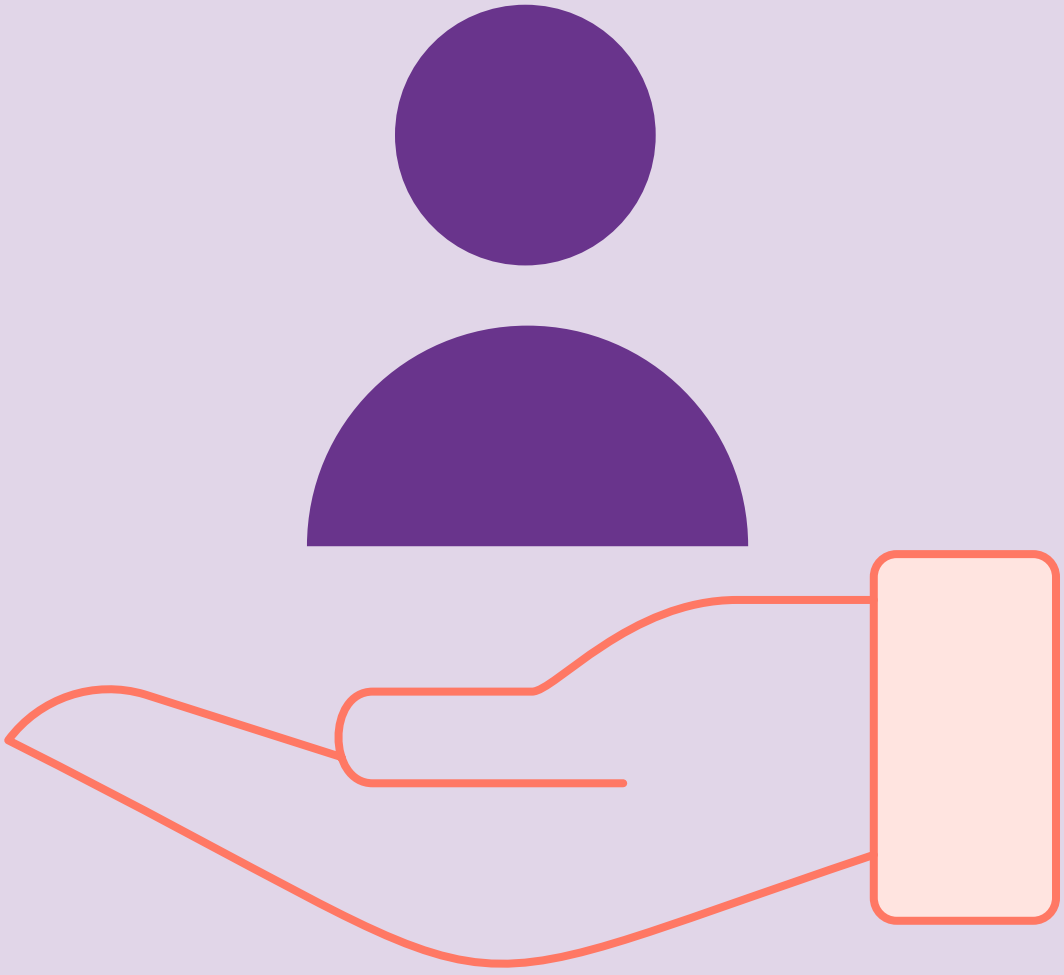
3 Responsabilité et surveillance

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 loi fédérale sur la protection des données (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 préposé fédéral à la protection des données et à la transparence (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. Inversement, l'exécution par les autorités cantonales des lois fédérales (p. ex. la loi sur les épidémies) est assujettie à la législation sur la protection des données du canton concerné.





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 dans 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 2020, le Bureau disposait de 510 pour cent de poste (sur un effectif autorisé de 515 %) et employait sept personnes. Cinq 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 (travaux publics et transports, intérieur et justice, sécurité), de la Chancellerie d'Etat (CHA) et des autorités de justice.

Anders Bennet (délégué à la protection des données suppléant, responsable informatique) est informaticien et assume depuis plus de 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 de la sûreté de l'information et de la protection des données (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 Direction de la santé, des affaires sociales et de l'intégration (DSSI) et de la Direction de l'instruction publique et de la culture (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 Direction des finances (FIN) et de la Direction de l'économie, de l'énergie et de l'environnement (DEEE) ainsi que 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.

Michael Weber (collaborateur scientifique, domaine juridique) est avocat et travaille depuis avril 2020 pour le Bureau. Actif dans les domaines de la santé et de la formation, il traite des demandes de renseignements et de conseils, procède à des contrôles préalables et rédige des prises de position sur des textes de loi touchant à la protection des données.

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 2020, les charges d'exploitation du Bureau se sont élevées au total à 153 milliers de francs (budget : 167 milliers de fr.). Environ 80 % de ces charges (122 milliers de fr.) ont été générées par des prestations externes ayant servi aux contrôles informatiques (le dernier contrôle de l'année sous revue a été facturé en janvier dernier seulement ; il sera donc imputé sur l'exercice 2021).

Au sein de l'administration cantonale, d'autres organismes se chargent de conseiller les autorités dans le domaine SIPD. Les Directions et la 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 (OACOT) pour les questions de protection de données d'ordre général et auprès des Directions et de la CHA 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. Office d'informatique et d'organisation [OIO], Bedag Informatique SA, Police cantonale [POCA] et Groupe de l'Ile SA [Insel Gruppe]).

Dans l'optique d'aboutir à un programme d'audits SIPD coordonné à l'échelle de l'Etat, le Contrôle des finances du canton de Berne et le Bureau envisagent une collaboration renforcée sur le plan stratégique.

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 préside la Conférence depuis novembre 2020 tandis que la responsable des domaines de la santé et de la formation dirige le groupe de travail Santé. Par ailleurs, il y a toujours une personne du Bureau dépêchée pour participer aux autres groupes de travail thématiques (actuellement : cyberadministration, sécurité et TIC). Pour de plus amples informations, voir les sujets traités en 2020 sous le chiffre 6.7 plus bas.

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 Coronavirus

Les mesures prises par la Confédération et le canton pour lutter contre la pandémie de coronavirus et pour atténuer ses répercussions sur la vie sociale et économique ont occupé le Bureau très régulièrement depuis mars 2020 dans divers domaines de son activité. Ce sujet saillant mérite donc un tour d'horizon complet pour commencer ce compte rendu.

6.1.1 Conseils à l'attention des autorités

covidtracker.ch

La DSSI a recommandé publiquement la plateforme covidtracker.ch, qui a été conçue par des particuliers avant d'être reprise par l'Ecole polytechnique fédérale de Zurich (EPFZ) dans le but de fournir, sur la base de données anonymes, des chiffres permettant de suivre l'évolution épidémiologique et d'établir des statistiques. Estimant que la responsabilité de la DSSI était engagée au moins partiellement au regard du droit de la protection des données, le Bureau a recommandé que les quatre derniers chiffres des numéros de téléphone ne soient pas des données requises car, combinées avec le numéro postal d'acheminement du domicile, ils peuvent permettre de retrouver l'identité des usagers de la plateforme. Par la suite, le numéro de téléphone a été entièrement supprimé, d'autant qu'il ne remplissait pas le but qui lui avait été assigné, à savoir reconnaître et regrouper les signalements émanant d'une même personne.

Publication du nombre d'infections par commune

Pendant la période où le nombre de cas était suffisamment faible pour cela, la DSSI a commencé à publier sur Internet le nombre quotidien de nouvelles infections par commune. Le Bureau a jugé que cette publication était problématique s'agissant des très petites communes, dont le faible nombre d'habitants donnait la possibilité de savoir qui avait contracté le virus. Le Bureau a donc recommandé instamment à la DSSI de renoncer à nommer les communes, ce que la DSSI a fait en se contentant dès lors de parler de « très petite commune » dans tel ou tel arrondissement administratif.

Mémento à l'attention du personnel cantonal concernant le télétravail

Pendant le premier semi-confinement en mars 2020, l'OIO a élaboré un mémento donnant au personnel cantonal des conseils techniques pour travailler à la maison. Sur la recommandation du Bureau, il y a rajouté quelques explications consacrées à la protection des données. Ce texte, rédigé par le Bureau, rappelle que l'obligation de garder le secret s'applique aussi vis-à-vis de la famille et qu'il faut donc veiller à la confidentialité des documents et des entretiens lorsque l'on travaille à domicile. Contrairement au bureau, où les documents sont éliminés selon des règles précises, les dossiers professionnels ne doivent pas finir dans le bac de papier à recycler. Le mémento donne en outre une liste, établie par la déléguée à la protection des données du canton de Zurich et privatim, d'applications de visioconférence qui sont jugées globalement conformes à la protection des données et auxquelles il est possible de recourir en période de pandémie dans les situations où Skype for Business ne peut pas être utilisé.

6.1.2 Conseils à l'attention des personnes concernées

Collecte des coordonnées dans les restaurants

L'obligation de collecter les coordonnées imposée aux restaurants a suscité de nombreuses questions parmi les personnes concernées. Elles se sont interrogées en particulier sur l'admissibilité de collecter la date de naissance ou se sont plaintes de l'utilisation de listes sur lesquelles les coordonnées des autres convives étaient visibles. Le Bureau était également le premier point de contact pour les questions concernant l'application de la législation fédérale sur la protection des données dans les établissements privés. Il a donc répondu à ces demandes et informé *a posteriori* l'autorité compétente, à savoir le préposé fédéral, des réponses fournies.

La collecte de la date de naissance est expressément prévue dans une ordonnance que le canton de Berne a édictée en se fondant sur la loi sur les épidémies de la Confédération. Selon la DSSI, elle est nécessaire dans certains cas pour identifier formellement les client·e·s. Le Bureau a fait remarquer à plusieurs reprises à la DSSI qu'il fallait un nombre suffisant de cas concernés pour justifier une obligation généralisée et il a recommandé de vérifier en détail ce point en particulier et de le corriger si nécessaire la prochaine fois que l'adéquation des mesures serait contrôlée, comme le prescrit le droit fédéral.

La collecte de coordonnées directement sur des listes est clairement inadmissible au regard du droit de la protection des données. C'est pourquoi l'ordonnance du Conseil fédéral qui prescrit cette collecte stipule que la confidentialité des données doit être assurée lors de la collecte. La DSSI propose sur son site Internet des listes au format Excel qui peuvent être utilisées pour rassembler les

coordonnées collectées au sein d'un établissement voire pour les transmettre à l'Office du médecin cantonal, mais pas pour la saisie des données par la clientèle elle-même. Sur la recommandation du Bureau, la DSSI a précisé ce point clairement sur son site Internet.

6.1.3 Prises de position formelles

Ordonnance sur les mesures de soutien dans le secteur de la culture

Pour appliquer l'ordonnance COVID de la Confédération dans le secteur de la culture, il fallait une ordonnance cantonale sur le même sujet. Les directives de l'Office fédéral de la culture prévoyaient que les requérant·e·s devaient consentir à ce que leurs données soient communiquées à des tiers dans la mesure où cela serait nécessaire pour traiter leur demande. Consulté au sujet du projet d'ordonnance cantonale, le Bureau a relevé le caractère singulier de cette construction juridique. En effet, pour être valable, le consentement d'une personne doit avoir été donné volontairement. Il est donc apparu au Bureau, suivi en cela par l'INC, qu'il serait plus judicieux et plus transparent de prévoir dans l'ordonnance cantonale une base légale autorisant les communications de données nécessaires et précisant qu'il suffisait d'en informer les requérant·e·s.

Ordonnance sur les mesures dans le domaine de l'accueil extrafamilial

Pendant la situation extraordinaire, le Conseil-exécutif a édicté des dispositions prévoyant des aides financières en faveur de l'accueil des enfants dans les garderies et les organisations d'accueil de jour en se fondant directement sur la Constitution cantonale. Pour appliquer correctement la compensation des charges, il fallait tenir compte des montants perçus au titre de l'aide sociale par les parents qui font garder leurs enfants. Or, les informations sur les prestations de l'aide sociale sont considérées comme des données personnelles particulièrement dignes de protection, dont le traitement et en particulier la communication doivent être expressément prévus dans une loi. À la demande du Bureau, il a donc été précisé dans l'ordonnance que l'Office de l'intégration et de l'action sociale (OIAS) pouvait se procurer auprès des fournisseurs de prestations concernés des données personnelles concernant des mesures d'aide sociale. Un avant-projet, qui permettait aux institutions concernées d'échanger ces données, a été jugé par le Bureau comme allant trop loin car il était clair que la communication était nécessaire dans un seul sens.

Ordonnance sur les mesures destinées à lutter contre l'épidémie de COVID-19

Se fondant sur les dispositions pertinentes de la législation fédérale, le canton de Berne a prescrit la collecte des coordonnées de la clientèle, imposant cette obligation d'abord aux bars et aux discothèques. Les prescriptions cantonales allaient plus loin que les consignes fédérales puisqu'elles demandaient que soient également collectés un numéro de téléphone portable et une adresse électronique afin de pouvoir contacter très rapidement les personnes si nécessaire. Un mois plus tard, l'obligation de collecter les coordonnées a été étendue à tous les établissements de restauration, des contrôles des mesures de protection ayant montré qu'il y avait des incertitudes dans un trop grand nombre de cas et que les mesures prises étaient insuffisantes. Mais dans ce cas, la collecte de numéros de téléphone portable et d'adresses électroniques n'était pas prévue. Le Bureau a estimé que l'extension de la collecte des coordonnées aussi bien que la différence faite entre les catégories d'établissements étaient proportionnées : les restaurants sont fréquentés par de larges pans de la population (y compris par des gens qui n'ont pas de téléphone portable ou d'adresse électronique) et les contacts entre les clients sont plus contrôlés que dans les bars et les discothèques. Le Bureau a toutefois émis des doutes sur la nécessité de collecter la date de naissance en plus de l'adresse complète (lire les explications à ce sujet sous le ch. 6.1.2 plus haut).

6.1.4 Contrôles préalables

Application spécialisée SORMAS pour le traçage des contacts

L'application SORMAS (*Surveillance and Outbreak Response Management System*) est utilisée par divers cantons, dont le canton de Berne, pour assurer le traçage des contacts. En mai 2020, les autorités de la DSSI responsables de cette application ont informé le Bureau, à sa demande, que l'application serait utilisée dans le canton. Peu après, elles ont fait savoir au Bureau qu'elles allaient démarrer avant la fin du mois un essai pilote utilisant des données personnelles réelles et que l'application serait définitivement mise en service en septembre 2020. À la date de clôture de la rédaction du présent rapport d'activité, les autorités responsables n'ont pas transmis au Bureau de documentation SIPD pour qu'il procède au contrôle préalable. La conformité de SORMAS avec les dispositions en matière de protection des données n'est donc pas établie pour le moment, ce qui apparaît comme hautement problématique du fait que l'application utilise des données personnelles particulièrement dignes de protection.

6.2 Conseils

6.2.1 Autorités

Répétition de la votation sur l'appartenance cantonale de la commune de Moutier

La CHA s'est adressée à plusieurs reprises au Bureau pour éclaircir des questions relevant du droit de la protection des données en vue de la répétition de la votation à Moutier. La loi sur l'organisation de votations relatives à l'appartenance cantonale de communes du Jura bernois (LAJB) habilite le Conseil-exécutif à prendre des mesures particulières pour assurer le bon déroulement des votations. C'est ainsi que s'est notamment posée la question de savoir si la CHA pouvait obtenir un accès à la plateforme des systèmes des registres communaux GERES afin de vérifier les entrées dans le registre électoral de la commune de Moutier. Le Bureau a estimé que la LAJB le permettait, mais que la CHA devrait démontrer pour chaque attribut de GERES pourquoi elle avait besoin d'y avoir accès afin d'accomplir la tâche sur laquelle portait la demande. Sur le plan formel, ce nouvel accès à GERES devait être légitimé par l'ajout dans l'ordonnance sur l'harmonisation des registres officiels d'une disposition définissant également tous les autres droits d'accès des autorités cantonales.

Utilisation de Microsoft 365 dans l'administration cantonale

L'utilisation de services en ligne comme Microsoft 365 a pour conséquence que des données personnelles et autres sont traitées dans le domaine d'autorité du fournisseur, c'est-à-dire dans son infrastructure et avec la participation de son personnel. Du point de vue de la protection des données, il s'agit d'un traitement de données sur mandat. Cela suppose que le respect de la protection et de la sûreté des données est garanti aussi chez le fournisseur, et cette garantie doit être définie dans un contrat approprié entre l'autorité et le fournisseur. La Conférence suisse sur l'informatique (CSI) et Microsoft avaient conclu un contrat-cadre stipulant que les contrats relatifs à des services en ligne étaient régis par le droit irlandais et que les litiges, en particulier concernant les violations de la protection des données, devaient être portés devant les tribunaux irlandais. Privatim a estimé que ces dispositions étaient insuffisantes et, par une action de conseil auprès de la CSI, elle a pu obtenir la conclusion d'un avenant au contrat prévoyant que les promesses concernant la protection des données figurant dans le contrat avec Microsoft, en particulier son *Data Protection Addendum* (DPA), pourraient être interprétées selon le droit suisse et qu'en cas de litige il serait possible d'en demander l'application auprès de tribunaux suisses.

On ne pouvait cependant pas en conclure que l'administration cantonale pouvait utiliser sans réserve les produits Microsoft 365. Le 2 juillet 2020, le délégué à la protection des données de l'Union européenne a publié une étude mettant en évidence divers autres problèmes de protection des données concernant aussi les autorités en Suisse. En outre, la Cour de justice européenne, dans un arrêt du 16 juillet 2020 (arrêt Schrems II), a invalidé le bouclier de protection des données UE – Etats-Unis (*EU-US Privacy Shield*) si bien qu'il n'est plus possible de transférer des données personnelles de l'UE vers les Etats-Unis sans autres garanties. Peu après, le PFPDT est arrivé à la même conclusion en ce qui concerne le bouclier de protection des données Suisse – Etats-Unis (*Swiss-US Privacy Shield*).

Pour l'administration cantonale, cela signifie qu'avant d'utiliser un service déterminé, il faut vérifier en détail où sont traitées et stockées quelles données (une telle vérification est en cours concernant *MS Azure Multi-Factor Authentification*), quels sont les sous-traitants de Microsoft qui contribuent au service et qui pourraient avoir accès aux données, comment Microsoft peut minimiser la collecte et l'évaluation de données relatives aux utilisateurs de ce service, etc. Il est très satisfaisant de constater que l'OIO, qui est compétent en la matière, assume cette responsabilité avec le plus grand sérieux et procède aux clarifications recommandées par le Bureau avec la minutie requise.

Enregistrements des conversations téléphoniques

Un hôpital souhaitant enregistrer des conversations téléphoniques lorsque des menaces sont prononcées s'est adressé au Bureau pour demander si cela était autorisé et, si oui, sous quelle forme. Selon le Bureau, une telle démarche serait illicite voire punissable au regard du droit de la protection des données. En principe, les conversations téléphoniques non publiques ne peuvent être enregistrées qu'avec le consentement des personnes qui y participent. Les exceptions sont définies dans la loi : en particulier, « n'est pas punissable […] celui qui, en tant qu'interlocuteur ou en tant qu'abonné de la ligne utilisée, aura enregistré des conversations téléphoniques avec des services d'assistance, de secours ou de sécurité » afin qu'une intervention rapide et efficace puisse avoir lieu. En l'espèce, cette condition n'était pas remplie : l'enregistrement des conversations n'aurait pas porté que sur les numéros d'urgence et le but n'était pas de pouvoir mener à bien une intervention médicale. De plus, le traitement des données envisagé n'avait pas de base légale suffisante au regard du droit de la protection des données.

6.2.2 Personnes concernées

Traitement électronique de données pour l'établissement des cartes d'élève

L'élève d'un gymnase a demandé au Bureau si l'application développée par son établissement pour le téléversement de photos en vue de l'établissement des cartes d'élève était compatible avec le droit de la protection des données. Le Bureau a demandé des renseignements complémentaires au gymnase concerné. Après avoir clarifié les faits, le Bureau a pu constater que l'application était utilisée pour traiter un nombre très important de photos de personnes. Or ces portraits sont considérés comme des données personnelles. Parce qu'il est possible d'en tirer éventuellement des informations particulièrement dignes de protection (notamment sur la santé ou sur la religion des personnes représentées), le Bureau a estimé et estime que l'application remplit les conditions d'un assujettissement à l'obligation de contrôle préalable. Or, elle a manifestement été mise en service sans contrôle préalable. La poursuite de son utilisation est donc subordonnée à l'élaboration dans les meilleurs délais de la documentation SIPD requise et à la remise de cette documentation au Bureau pour qu'il puisse la contrôler. Le Bureau a avisé le gymnase que l'application était assujettie à l'obligation de contrôle préalable. Les documents devraient lui être soumis au début de 2021.

Demandes concernant la publication sur Internet d'informations relatives à la propriété

Depuis août 2020, tout le monde peut consulter le nom des propriétaires inscrits dans le registre foncier et, via la plateforme BE-Login, accéder à leur date de naissance. Cela a suscité de nombreuses demandes de la part de personnes concernées, demandes auxquelles les réponses suivantes ont été apportées. Le Code civil prévoit que toute personne peut, sans devoir justifier d'un intérêt, obtenir du bureau du registre foncier le nom et l'identification du propriétaire. Selon l'ordonnance fédérale sur le registre foncier (ORF), l'identification du propriétaire se fait en indiquant la date de naissance, le sexe et le lieu d'origine ou la nationalité. L'ORF habilite en outre les cantons à rendre publiques en ligne les données du registre foncier consultables sans devoir rendre un intérêt vraisemblable. Ils doivent cependant garantir que l'accès aux données ne pourra avoir lieu qu'en relation avec un immeuble déterminé (ce qui exclut en particulier la possibilité de faire une recherche par nom) et que le système d'information sera protégé contre les appels en série. Ces deux consignes ont été appliquées dans le canton de Berne. La publicité du registre foncier et des données sur la propriété est légitime sur le plan juridique car la propriété confère un droit exclusif sur un bien qui était public à l'origine. Les propriétaires fonciers ont le droit d'exploiter et de valoriser leurs immeubles et d'exclure que des tiers en aient la jouissance. Le registre foncier crée la transparence requise dès lors

qu'il est public. Si l'accès d'un bien est interdit à des tiers, le cas échéant sous peine de sanctions juridiques, ceux-ci ont le droit de savoir qui leur impose cette restriction. De plus, le contenu du registre foncier est réputé connu dans son ensemble (fiction juridique : « Nul ne peut se prévaloir de ce qu'il n'a pas connu une inscription portée au registre foncier »).

Conseil et médiation dans le cadre de la consultation restreinte d'un dossier auprès de la Police cantonale

Une personne concernée s'est adressée au Bureau parce qu'en consultant des entrées à son sujet dans le journal de la Police cantonale (POCA), elle a constaté que les documents contenaient de nombreux passages caviardés. Le droit d'une personne de consulter les données la concernant prévu dans la LCPD ne peut être restreint que si un intérêt public important et prépondérant ou des intérêts de tiers particulièrement dignes de protection s'y opposent. Pour expliquer le caviardage, la POCA a invoqué des motifs en lien avec les tactiques d'intervention. Le Bureau, intervenant en qualité de conseiller et de médiateur entre la personne concernée et l'autorité, a demandé quel type d'informations recouvrait chaque caviardage. Il est apparu qu'il s'agissait toujours d'informations sans rapport avec la personne concernée, comme le nom d'agent·e·s de police, des numéros de plaque d'immatriculation et des fréquences radio ou encore des données concernant d'autres personnes. Selon le responsable de la protection des données de la POCA, il est très rare que des informations au sujet de la personne concernée soient caviardées. Le Bureau ayant le mandat légal de défendre les intérêts des personnes à qui il n'est pas possible de fournir des informations, ou seulement de manière limitée, il a convenu avec la POCA qu'elle le consulterait systématiquement si des cas semblables devaient se représenter.

Plaintes diverses concernant l'envoi de données fiscales

Plusieurs personnes ont dénoncé au Bureau des erreurs d'adressage de données fiscales. Comme la violation de la protection des données avait déjà été commise au moment où ces dénonciations sont intervenues après, le Bureau n'a pas pu prévenir ou annuler les erreurs concernées. Il a néanmoins demandé aux autorités fiscales en cause comment elles comptaient éviter ce genre d'inadvertance à l'avenir. Il en est ressorti qu'à chaque recours ou plainte l'Intendance des impôts a établi les causes de l'incident de manière correcte et mis à profit ces cas pour vérifier et améliorer ses procédures internes. Le Bureau a en outre recommandé aux autorités fiscales de sensibiliser régulièrement leur personnel à la garantie du secret fiscal dans le cadre de la gestion des données fiscales.

6.2.3 Formation continue

Contribution à la formation du personnel communal

Le *Bildungszentrum für Wirtschaft und Dienstleistung* (bwd) propose différentes formations à l'intention des personnes travaillant pour des autorités communales. Cela fait de nombreuses années – et 2020 ne fait pas exception – que le Bureau enseigne la matière « Protection des données et sûreté de l'information » dans le cadre de la filière aboutissant au brevet de « Bernische Gemeindefachfrau/ Bernischer Gemeindefachmann » et de la formation du personnel administratif des écoles de langue allemande. L'enseignement porte sur les principes généraux du droit de la protection des données et sur leur application dans le domaine d'activité des participant·e·s. Il comprend en outre le traitement de questions concrètes qui se posent dans la vie professionnelle quotidienne, ce qui est un aspect important. Un nouvel ensemble de cours a été organisé pour la première fois en 2020 à l'intention du personnel des secrétariats paroissiaux. L'intervenante du Bureau y a abordé des questions supplémentaires, comme la portée en droit de la protection des données des dispositions particulières contenues dans la nouvelle loi sur les Eglises nationales (LEgN) et dans les nouveaux règlements de ces institutions relatifs à la protection des données.

Diffusion de connaissances lors d'événements spécifiques

La pandémie a entraîné l'annulation ou le report à une date ultérieure de plusieurs formations continues organisées par des autorités où des membres du Bureau avaient été invités à intervenir. Un représentant du Bureau a néanmoins pu participer à une rencontre des secrétaires communaux de l'arrondissement administratif de Thoune ainsi qu'à une formation continue organisée par le gymnase du campus de Muristalden, lors desquelles il a présenté les fondements de la protection des données ainsi que des questions d'actualité. Un représentant du Bureau a en outre donné une conférence lors du colloque digma sur la protection des données dans la pratique quotidienne des villes et des communes ainsi qu'à un événement en ligne d'Educa, l'agence spécialisée dans les technologies de l'information et de la communication pour le domaine de l'éducation.

6.3 Prises de position formelles

Modification de la loi sur la santé publique

Les projets d'actes législatifs et autres mesures intéressant la protection des données doivent être soumis préalablement au Bureau afin qu'il prenne position. Lorsqu'il a examiné une modification de la loi sur la santé publique (LSP), le Bureau a porté une attention particulière à la question de l'inspection des établissements de santé ambulatoires. Selon le projet de modification, il sera possible de consulter des données personnelles particulièrement dignes de protection (p. ex. des dossiers de traitement) dans le cadre de ces inspections. De plus, les nouvelles dispositions imposent aux personnes chargées de la gestion des établissements de santé ambulatoires et à celles qui y travaillent le devoir de collaborer pleinement aux inspections. Grâce à un échange constructif entre le Bureau et la DSSI, qui était responsable du dossier, il a été possible de trouver une solution optimale du point de vue de la protection des données afin que les dispositions en question respectent les exigences imposées par la protection des données au niveau cantonal (traitement de données par des autorités cantonales), par la loi fédérale sur la protection des données (traitement de données par des personnes privées) et par le Code pénal (secret professionnel).

La bonne collaboration entre le Bureau et la DSSI a également permis de trouver des solutions viables du point de vue de la protection des données pour d'autres projets de loi, notamment la nouvelle loi sur les prestations de soutien aux personnes en situation de handicap (LPHand).

Procédure de permis de construire par voie électronique

Une révision de la loi sur les constructions et du décret concernant la procédure d'octroi du permis de construire a été lancée en vue de créer les bases légales permettant de conduire la procédure du permis de construire par voie électronique. Cette révision prévoit que les dossiers de demande de permis de construire seront consultables par voie électronique pendant la période de dépôt public. Or, ces dossiers peuvent contenir des informations particulièrement dignes de protection sur les auteur·e·s des demandes, par exemple si la demande porte sur l'installation d'un fauteuil monte-escaliers. Tant que le dépôt public est effectué dans les locaux de l'administration communale, la consultation du dossier est de fait limitée aux tiers qui sont prêts à consacrer du temps à cette démarche. *A contrario*, un accès via Internet rend la consultation théoriquement possible dans le monde entier et avec des outils automatisés. Le Bureau a donc demandé une prescription imposant aux communes de prendre les mesures appropriées pour garantir la sûreté de l'information et la protection des données. Il est envisageable, par exemple, de protéger l'accès au dossier par un mot de passe valable uniquement pour la

procédure considérée, qui est communiqué aux personnes souhaitant consulter le dossier durant la période de dépôt public. Au sujet de l'examen relatif à l'application spécialisée eBau, lire les explications sous le chiffre 6.5.

Ordonnances d'exécution de la LFDP

La nouvelle loi sur les fichiers centralisés de données personnelles (LFDP) et ses ordonnances d'exécution concrétisent le principe de la collecte unique des données (« once only »), qui veut que les données personnelles nécessaires à plusieurs autorités pour accomplir leurs tâches respectives (qui ont donc l'autorisation légale de les traiter) soient regroupées dans un même système de consultation afin d'améliorer leur exactitude et leur exhaustivité. Une collaboratrice du Bureau a participé activement au groupe de travail qui a préparé l'ordonnance sur la plateforme des systèmes des registres communaux (O GERES) et l'ordonnance sur le système de gestion centrale des personnes géré par l'Intendance des impôts (O GCP). Ces nouvelles ordonnances entrent en vigueur le 1er mars 2021, abrogeant la loi et l'ordonnance sur l'harmonisation des registres officiels. Elles définissent pour l'accès aux données un profil de base et des profils standard adaptés à des besoins particuliers. Pour le Bureau, il était important que le profil de base, qui est en principe accessible à toutes les autorités habilitées, ne contienne pas de données particulièrement dignes de protection ou sensibles pour d'autres raisons. En ce qui concerne les profils standard, il a fallu s'assurer qu'ils donnent accès à des données personnelles uniquement dans la mesure où cela est nécessaire et proportionné pour accomplir une tâche. Il a donc été décidé qu'un attribut comme la confession ou le numéro AVS constituerait un profil en soi. Les Directions devront édicter des ordonnances pour régler les droits d'accès de leurs autorités et des autorités qui leur sont rattachées et les soumettre au Bureau pour avis préalable ; en ce qui concerne les autorités communales, les profils d'accès à GERES sont définis directement dans l'annexe de l'ordonnance.

Loi sur l'administration numérique

Une loi sur l'administration numérique (LAN) a été préparée pour régler les principes de la numérisation de l'administration cantonale bernoise. Le Bureau a pu travailler dès le début à l'élaboration du projet au sein d'un groupe d'accompagnement, en s'intéressant prioritairement à la protection des données. Il est ainsi apparu que les multiples traitements de données numériques nécessitaient de combler des lacunes dans la législation sur la protection des données et appelaient des améliorations importantes, comme la clarification des règles applicables au traitement de données par des tiers (traitement de données sur mandat), à la responsabilité de la protection des données lorsque plusieurs autorités décident du but et des moyens d'un traitement de données et à la coordination de l'activité de surveillance lorsqu'un même projet de traitement numérique de données intéresse plusieurs autorités cantonales si bien que la

protection des données dans ce cadre est soumise à la surveillance de plusieurs services.

Les dispositions de la LAN sur ces points complètent provisoirement la LCPD. Elles seront prises en compte dans la révision de la LCPD déclenchée par les nouvelles dispositions européennes en matière de protection des données.

Rapport sur le port de caméras-piéton à la POCA

Le 2 décembre 2020, le Conseil-exécutif a approuvé le rapport sur le port de caméras-piéton à la POCA en réponse à une intervention parlementaire. Dans ce rapport, il explique que la POCA recourra davantage à des caméras-piéton en 2021 dans la mesure où les bases légales en vigueur le permettent. La loi cantonale sur la police et le Code de procédure pénale suisse autorisent les prises de vue (y compris secrètes) lorsqu'il existe des indices concrets laissant présumer qu'une infraction est imminente ou a été commise et que d'autres formes d'investigation n'auraient aucune chance d'aboutir ou seraient excessivement difficiles. La loi sur la police contient en outre une base légale autorisant la surveillance vidéo lors de manifestations de masse, sans préciser sous quelle forme (installation fixe ou mobile). Le Bureau a pris position sur le rapport avant son adoption.

La vidéosurveillance doit en principe avoir une légitimité démocratique élevée car elle concerne toujours des personnes sans rapport avec l'infraction suspectée ou le trouble observé. Cela est encore plus vrai s'agissant de caméras mobiles, dont il est difficile par définition de sortir du champ. C'est pourquoi leur utilisation doit être expressément prévue dans une loi au sens formel. Si ce n'est pas le cas, il faudrait alors au minimum que le gouvernement autorise formellement leur utilisation et qu'il instaure la transparence requise par voie d'ordonnance. C'est ce qui a été fait concernant les drones avec l'entrée en vigueur de la nouvelle ordonnance sur la police au 1er janvier 2020. Mais il n'y a toujours pas de base légale pour les caméras-piéton.

6.4 Contrôles préalables

6.4.1 Projets informatiques

Les projets devant être soumis au Bureau pour le contrôle préalable sont ceux qui prévoient le traitement des données par voie électronique d'un grand nombre de personnes (critère quantitatif) et qui satisfont à au moins un des critères qualitatifs suivants : il ne peut être établi avec certitude qu'une base légale suffisante existe ; il s'agit de données personnelles particulièrement dignes

de protection ou pour lesquelles il existe une obligation particulière de garder le secret ; ou des moyens techniques présentant des risques particuliers pour les droits de la personnalité des personnes concernées sont employés.

En 2020, le Bureau a traité 123 contrôles préalables concernant des projets informatiques (2019 : 113) et en a achevé 58 (2019 : 69), soit 47,2 pour cent (2019 : 61,1 %). Une procédure standardisée s'applique : (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.

Application Hospitalisation

L'application Hospitalisation (HOSP) est un instrument permettant d'établir électroniquement les factures hospitalières et les garanties de prise en charge des frais pour les hospitalisations hors du canton. Elle illustre l'avancement de la transition numérique dans le domaine de la santé, qui pose à tous les acteurs des questions juridiques et techniques complexes. En l'espèce, le contrôle préalable a porté une attention particulière à la mise en œuvre technique de la consultation des données sur la plateforme des systèmes des registres communaux GERES car il est prévu qu'elle soit réalisée non pas par des membres du personnel déterminés, mais par un système informatique (communication de machine à machine). Les solutions de ce type accroissent généralement la complexité de l'administration des droits d'accès à l'intérieur de l'application.

Nouvelle application spécialisée pour la migration

Fondée sur de nouvelles bases légales, la restructuration du domaine de l'asile et des réfugiés dans le canton de Berne est entrée en vigueur le 1er juillet 2020. Il a donc fallu consolider les systèmes informatiques employés dans ce domaine. La nouvelle application spécialisée pour la migration (NFAM) a remplacé une multitude d'applications antérieurement utilisées par les services externes chargés de l'exécution. Le Bureau a été convié à suivre ce projet informatique très complexe à un stade précoce et il a eu des échanges réguliers et intensifs avec la direction du projet. Grâce à la prise en compte de cette procédure itérative dans l'étude du projet, le Bureau a pu sensibiliser les autorités compétentes de la DSSI et de la Direction de la sécurité (DSE) aux enjeux de protection des données et de sûreté de l'information. Malgré l'envergure du projet, les autorités ont ainsi bénéficié d'une grande sécurité de planification, qui leur a permis de franchir les étapes dans les délais prévus.

Nouveau système de gestion des dossiers de la POCA (Rialto)

Une procédure importante de contrôle préalable réalisé durant l'année sous revue a porté sur le nouveau système de gestion des dossiers NeVo / Rialto de la POCA. Ce système basé sur la solution standard SAP ICM (*Investigative Case Management*), qui est en cours de développement, est appelé à remplacer les multiples systèmes actuellement utilisés pour gérer les dossiers relevant de la police. Le Ministère public du canton de Berne y participe, à la fois en ce qui concerne les adultes et en ce qui concerne les mineurs, mais avec un mandant strictement séparé pour la gestion de ses données. Etant donné l'envergure et la complexité du projet, le premier contrôle effectué par le Bureau a débouché sur 86 constats, dont la plupart étaient moyennement significatifs. Ils portaient sur des aspects divers, allant du contrat d'exploitation avec Swisscom aux mesures techniques pour garantir la sûreté des données en passant par les délais admissibles pour la conservation des données. Après une prise de position détaillée de la POCA et une révision du concept SIPD, il restait dix observations à traiter, dont une nouvelle concernant les échanges de données entre la POCA et le Ministère public. Le contrôle préalable a pu être clôturé après leur résolution, c'est-à-dire après que la POCA a défini les mesures à prendre et indiqué qu'elle les appliquerait.

NeVo / Rialto apportera une amélioration essentielle sur un point crucial pour la protection des données : pour qu'ils puissent assurer leurs missions, les membres de la POCA ont des droits de consultation parfois très étendus dans les systèmes d'information, mais les accès en lecture seule ne donnent pas lieu à procès-verbal. Comme l'accès à des données en partie ultrasensibles est autorisé uniquement si cela est absolument nécessaire à l'accomplissement d'une tâche, il faut prévoir des mécanismes de contrôle appropriés. Dans NeVo / Rialto, des procès-verbaux d'accès en lecture seule seront établis et des contrôles aléatoires seront effectués.

Raccordement de Dr. Tax au système général NESKO

Dans le cadre de sa transition numérique, l'Intendance des impôts a décidé de permettre le dépôt en ligne des déclarations d'impôt établies avec des logiciels tiers. À l'heure actuelle, quelque 100 000 contribuables utilisent déjà le logiciel Dr. Tax pour remplir leur déclaration. Ce sera donc le premier logiciel à être raccordé au système NESKO de l'Intendance des impôts. Le Bureau a contrôlé le nouveau service d'importation en ligne nécessaire à ce raccordement et demandé la clarification de questions concernant divers aspects de la sécurité de la transmission des données.

Nuage informatique GELAN

Le canton de Berne gère le système complet d'information agricole GELAN pour lui-même et, en vertu de conventions de prestations, pour les cantons de Fribourg et Soleure. Il est prévu de développer le système pour en faire une plateforme de services infonuagique qui sera gérée par le centre de calcul de la Bedag Informatique SA. Ces nouveautés constituant une modification substantielle d'un traitement de données existant, elles devaient être soumises au Bureau pour qu'il effectue un contrôle préalable. Le Bureau a contrôlé la migration prévue des serveurs physiques de GELAN 4 vers la nouvelle plateforme de services infonuagique. Il fallait examiner notamment l'accès à distance par VPN (*Virtual Private Network*) et le respect des dispositions de l'ordonnance sur les données secondaires de communication (ODSC), en vigueur depuis janvier 2020.

Services immobiliers

La Promotion économique du canton de Berne propose aux entreprises un service d'intermédiaire pour la recherche de sites d'implantation. Une nouvelle application basée sur Internet, appelée « PEBE services immobiliers », lui permettra de standardiser les offres immobilières et le traitement des demandes de renseignements. Comme des secrets d'affaires des clients, qui requièrent un niveau de protection supérieur, pourront être concernés, le Bureau a vérifié notamment la sûreté de l'information dans l'application. Quelques questions se sont posées concernant les droits d'accès et la suppression des comptes inactifs.

6.4.2 Vidéosurveillance

La loi sur la police (LPol) entièrement révisée est entrée en vigueur le 1er janvier 2020. Elle contient des dispositions partiellement nouvelles concernant la vidéosurveillance. Si les exigences matérielles en la matière sont largement reprises du droit antérieur, l'approbation de la POCA n'est plus nécessaire pour placer les bâtiments publics sous vidéosurveillance à des fins de protection. La POCA doit néanmoins être consultée et tenir compte dans son avis du résultat du contrôle préalable effectué par l'organe chargé de la surveillance de la protection des données, c'est-à-dire pour les autorités cantonales le Bureau. Celui-ci a donc élaboré une liste de contrôle des exigences à prendre en compte concernant la sûreté de l'information et la protection des données (checkliste SIPD), outil que la POCA a mis en ligne sur son site Internet.

Prison régionale de Thoune et établissement d'exécution judiciaire de Saint-Jean

Le dernier contrôle préalable de la vidéosurveillance dans les prisons régionales et les établissements d'exécution judiciaire du canton de Berne remontait à 2010. Depuis lors, les technologies, les équipements et les bases légales ont évolué. Outre la vidéosurveillance autorisée par la LPol pour prévenir et poursuivre des infractions, la loi sur l'exécution judiciaire de 2018 permet de recourir à la vidéosurveillance pour soutenir l'accomplissement des tâches d'exécution judiciaire (p. ex. pour surveiller l'état de santé de détenus). C'est pourquoi le Bureau et l'Office de l'exécution judiciaire (OEJ) ont prévu que les documents SIPD de toutes les institutions concernées seraient mis à jour et soumis à un nouveau contrôle du Bureau. Suite au dépôt d'un recours par un citoyen, le premier contrôle a porté sur la prison régionale de Thoune, où une inspection sur place a été effectuée. Il est apparu que le dispositif de vidéosurveillance de l'établissement était globalement conforme à la loi, même si des adaptations ponctuelles étaient nécessaires. Elles concernent notamment la correction du cadrage de certaines caméras extérieures et l'utilisation de caméras dont la direction et le niveau de zoom pouvaient être modifiés par le personnel en service. Une deuxième inspection sur site a été conduite dans l'établissement d'exécution judiciaire de Saint-Jean, une institution d'exécution judiciaire en milieu ouvert, où les nécessités sont différentes de ceux d'une prison.

Institut des maladies infectieuses

L'Institut des maladies infectieuses (IFIK) de l'Université de Berne dispose d'un laboratoire de sécurité biologique de niveau 3. La protection de ce laboratoire doit être conforme aux prescriptions de l'ordonnance fédérale sur l'utilisation confinée. La vidéosurveillance est considérée comme l'une des mesures les mieux adaptées. Après un entretien préalable, l'institut a donc remis la documentation requise pour le contrôle préalable. Le Bureau a examiné le projet de surveillance utilisant six caméras, en s'arrêtant en particulier sur la proportionnalité et sur la sûreté des données.

Le contrôle préalable a conduit à clarifier une question concernant la destruction des enregistrements vidéo. Le Bureau estimait que les personnes responsables qui avaient transmis des enregistrements à la POCA en raison d'un incident devaient détruire ces enregistrements sur leurs supports juste après la transmission. La POCA a corroboré l'avis du Bureau dans le cadre de ce contrôle préalable.

6.5 Audits

En 2020, le Bureau a mené sept audits dans le domaine SIPD, dont cinq en collaboration avec un partenaire qualifié. Un audit est encore en cours.
Le Bureau a suivi activement la mise en place des mesures d'amélioration résultant de dix audits ayant abouti de 2016 à 2019, dont un a pu être clôturé.

Dans le cadre de ce travail de suivi, le Bureau a constaté que la mise en œuvre durable de mesures formelles, techniques ou organisationnelles dans le domaine SIPD requerrait une attention soutenue de la part des services responsables, mais que celle-ci n'a pas toujours été à la hauteur attendue. Des retards parfois considérables ont été pris. Cela s'explique notamment par la mobilisation que requièrent les affaires courantes et par la situation extraordinaire qui a régné en 2020 en raison des mesures prises par les autorités pour endiguer la pandémie. Or, plus il faut du temps pour mettre en œuvre les améliorations dans le domaine SIPD, moins on est à même de faire face correctement aux menaces dans le domaine de la cybersécurité, qui évoluent en permanence. Le Bureau attend donc des services responsables et des organes décisionnaires qu'ils tiennent compte de ce risque lorsqu'ils priorisent leurs tâches.

Active Directory (AD) Services / Management

Objet de l'audit : l'audit a porté sur les services d'annuaire centralisé Microsoft Active Directory (services AD) à l'OIO. L'OIO met ces services à la disposition de l'administration cantonale via un contrôleur et un serveur de domaine gérés et administrés par la Bedag Informatique SA. Avec ces services, la structure du réseau technique est calquée sur l'organisation de l'administration cantonale. Ces services administrent différents objets sur le réseau cantonal, comme les utilisateurs, les groupes, les ordinateurs, d'autres services, les serveurs, les fichiers partagés ou encore des périphériques tels que les imprimantes et les scanners, avec leurs propriétés distinctives. Un administrateur système peut organiser, mettre à disposition et surveiller les informations relatives aux objets enregistrés sur le réseau.

But de l'audit : l'audit avait pour but d'évaluer la sûreté des services AD, y compris les systèmes périphériques, les interfaces, la gestion des changements et du lancement des nouvelles versions (*Change and Release Management, CRM*), la gestion de la configuration des services, les mesures de contrôle et d'assurance de la qualité, la gestion des accès, la conservation des données et l'assistance.

Résultat de l'audit : globalement, l'audit a révélé des risques moyens à élevés dans tous les domaines examinés, et donc un potentiel substantiel d'amélioration et d'optimisation. Sur un plan général, le Bureau a déploré que la documentation sur les services AD ne corresponde pas à la version utilisée, ce qui empêche de

cadrer efficacement l'exploitation de ces services. Il faut en particulier mieux expliquer comment est conçue la gestion des droits d'accès privilégiés (c.-à-d. de niveau élevé) et limiter davantage ces droits. Il y a lieu également d'améliorer l'application et le contrôle de l'efficacité des directives régissant les mots de passe ainsi que la gestion des points faibles.

La collaboration s'est déroulée de façon professionnelle et dans un bon esprit de coopération entre toutes les parties prenantes. Le Bureau suivra activement la mise en œuvre des mesures d'amélioration préconisées.

BE-Login

Objet de l'audit : BE-Login est le portail d'accès aux services de cyberadministration sur lequel les citoyen·ne·s et le personnel des services cantonaux accèdent aux applications spécialisées de l'administration cantonale qui leur sont destinées. Placé sous la responsabilité de l'OIO, le portail BE-Login est développé et exploité par l'entreprise Bedag Informatique SA.

But de l'audit : l'audit avait pour but d'évaluer la sûreté de l'information de BE-Login en inspectant son code conformément au projet *Open Web Application Security Project* (OWASP), y compris les systèmes périphériques, les interfaces, la gestion des changements et du lancement des nouvelles versions (*Change and Release Management, CRM*), la gestion de la configuration, les mesures de contrôle et d'assurance de la qualité, la gestion des accès, la conservation des données et l'assistance.

Résultat de l'audit : les contrôles portant sur la sûreté du code du logiciel, sur le processus de connexion et sur les processus d'exploitation ont mis en évidence des risques parfois élevés. Le Bureau attend des mesures d'amélioration immédiate sur ces points. Il a en outre constaté d'autres risques moyens ou faibles. Globalement, au moment où l'audit a été réalisé, BE-Login présentait des défauts de sécurité importants. Comme il est prévu d'y raccorder d'autres applications au fil de la numérisation de l'administration cantonale, BE-Login sera encore plus exposé. Le Bureau a donc demandé que les actions correctives requises soient entreprises sans attendre, par ordre de priorité basé sur la criticité des défauts constatés, afin d'accroître rapidement le niveau de sécurité de toutes les applications raccordées. Il a en outre recommandé de ne pas raccorder de nouvelles applications à BE-Login tant que la preuve de l'élimination des défauts critiques n'est pas apportée. L'OIO a suivi globalement cette recommandation.

La collaboration s'est déroulée de façon professionnelle et dans un bon esprit de coopération entre toutes les parties prenantes. Le Bureau suivra activement la mise en œuvre des mesures d'amélioration préconisées. Il se réserve la possibilité de soumettre ces mesures à un examen approfondi.

Protection de base de l'infrastructure informatique de la BFH

Objet de l'audit : la Haute école spécialisée bernoise (BFH) compte un effectif estudiantin d'environ 7000 personnes ainsi que 2500 collaboratrices et collaborateurs sur 26 sites à Berne, Bienne, Berthoud, Macolin, Nidau, Vauffelin et Zollikofen. Son service informatique (Services IT) fournit des prestations centralisées dans le domaine des TIC. Les départements gèrent en outre leur propre environnement, par exemple pour leur informatique de gestion ou pour leurs laboratoires ; ces domaines ne relèvent pas de la responsabilité des Services IT. Même si la BFH a une infrastructure informatique indépendante de celle de l'administration cantonale, elle utilise cependant certaines de ses applications, en particulier dans le domaine du personnel.

But de l'audit : il s'agissait de vérifier dans quelle mesure la protection de base de l'infrastructure informatique et les mesures mises en œuvre dans le domaine SIPD remplissaient les exigences en matière de sûreté de l'information et de protection des données. L'audit a reposé sur la revue de documents, sur des entretiens avec les responsables des Services IT ainsi que sur la soumission de systèmes techniques à des inspections et à des tests ponctuels.

Résultat de l'audit : l'audit a mis en évidence l'existence dans tous les domaines contrôlés de risques moyens, mais aussi élevés. La protection de base de l'infrastructure informatique de la BFH au moment de l'audit ne peut pas être qualifiée d'adéquate. Cependant, la BFH a lancé un projet de système de gestion de la sécurité informatique (BFH ISMS) afin de poser les fondements d'une protection de base adéquate qui soit pilotée activement.

La collaboration s'est déroulée de façon professionnelle et dans un bon esprit de coopération entre toutes les parties prenantes. Le Bureau procédera en temps opportun à une nouvelle évaluation du projet BFH ISMS et de ses résultats.

Application spécialisée eBau

Objet de l'audit : le Grand Conseil bernois a adopté en 2014 une motion demandant une simplification de la procédure d'octroi du permis de construire. La mise en œuvre de la motion, toujours en cours au moment de la réalisation de l'audit puisque le projet eBau dure de 2015 à 2022, vise à permettre le déroulement de la procédure de permis de construire sous forme électronique dans l'ensemble du canton de Berne. Basé sur une technologie web, la solution eBau sera obligatoire après la clôture du projet. Elle couvre la totalité de la procédure d'octroi du permis de construire, des requêtes à l'examen par l'autorité responsable en passant par les contributions des services officiels et des services spécialisés compétents.

But de l'audit : les contrôles effectués ont porté sur la gouvernance en matière de SIPD, les concepts SIPD et les mesures de protection, les processus de gestion

des utilisateurs, l'externalisation, la conservation des données et les interfaces. L'audit a reposé sur la revue de documents et sur des entretiens avec les responsables.

Système de base BE-GEVER

Objet de l'audit : le système électronique de gestion des affaires (service BE-GEVER) utilise la solution CMI AXIOMA de la société CM Informatik AG pour proposer les fonctionnalités d'une solution globale de gestion des affaires et des documents qui comprend la gestion des dossiers, le contrôle des flux et le contrôle des affaires dans l'ensemble de l'administration cantonale. Selon la directive GEVER, les documents de l'administration cantonale pertinents pour les affaires doivent être traités avec le service BE-GEVER, c'est-à-dire dans le système de gestion électronique des affaires. Le service BE-GEVER et le système de base sont sous la responsabilité de l'OIO et exploités par la Bedag Informatique SA. BE-GEVER permet aux Directions et à la CHA ainsi qu'à leurs offices de travailler dans leur propre environnement logique grâce à des mandants dédiés. L'archivage des documents n'est pas couvert par BE-GEVER.

But de l'audit : les contrôles ont porté sur les exigences SIPD prévues pour le système de base BE-GEVER. L'audit a reposé sur la revue de documents et du système de base ainsi que sur des entretiens avec les responsables du système à l'OIO et à l'entreprise Bedag Informatique SA.

Résultat de l'audit : des risques ont été constatés dans tous les domaines contrôlés ; ils peuvent être qualifiés de moyens pour une grande partie, mais sont élevés dans certains cas. En particulier, il n'y avait pas de concept SIPD à jour et complet pour l'exploitation en place. Le Bureau a en outre constaté que les documents gérés dans BE-GEVER étaient enregistré non pas dans une banque de données dédiée, mais sur des serveurs de fichiers. Or, ce type de serveurs ne permet pas d'exclure que des accès en lecture non autorisés et non détectés aient eu lieu (p. ex. avec les droits d'accès d'un administrateur système). Le Bureau a donc estimé qu'au moment où les contrôles ont été réalisés la confidentialité des données personnelles et des autres informations dignes de protection n'était pas garantie de manière totale et transparente pour tous les mandants de BE-GEVER. Il a demandé que les mesures nécessaires soient prises rapidement pour offrir une garantie vérifiable de la confidentialité des données traitées dans BE-GEVER. Il a en outre recommandé que les documents et les données classés « secret » ne soient pas traités dans ce système.

La collaboration s'est déroulée de façon professionnelle et dans un bon esprit de coopération entre toutes les parties prenantes. Le Bureau suivra activement la mise en œuvre des mesures d'amélioration préconisées. Il se réserve la possibilité de soumettre leur réalisation à un examen.

Protection de base de l'infrastructure informatique de STS AG à Thoune

Objet de l'audit : l'hôpital Simmental-Thun-Saanenland AG (STS AG) compte plus de 1900 employé·e·s à temps partiel ou à temps plein. L'hôpital de Thoune est responsable des soins hospitaliers médicaux (soins de base et prestations spécialisées) et d'un centre d'urgences interdisciplinaire. Tous les services techniques nécessaires au fonctionnement de l'hôpital (gestion des locaux, informatique, administration, technique, etc.) sont situés sur le site de Thoune. Le centre hospitalier STS AG comprend également l'hôpital de Zweisimmen, des services psychiatriques et un service de sauvetage. Gérée par le *Chief Information Officer*, l'organisation TIC se compose des domaines Infrastructure informatique, Applications et Informatique médicale, chacun étant placé sous la responsabilité d'une direction. Les systèmes informatiques centraux sont hébergés dans le centre de calcul de l'hôpital de Thoune ; les autres sites n'ont en principe pas de serveurs locaux et utilisent les systèmes centraux hébergés à Thoune.

But de l'audit : il s'agissait d'évaluer si la protection de base de l'infrastructure informatique et les mesures mises en œuvre dans le domaine SIPD répondaient de manière vérifiable aux exigences en matière de sûreté de l'information et de protection des données. L'évaluation devait porter en particulier sur la gouvernance et le concept SIPD, la gestion des changements et du lancement des nouvelles versions (*Change and Release Management, CRM*), la gestion des accès, la sécurité des réseaux, du stockage ainsi que des clients et des serveurs, l'externalisation, les points restés en suspens depuis l'audit de 2012 ainsi que la sécurité physique sur le site de Thoune. L'audit a reposé sur la revue de documents, sur des entretiens avec les responsables ainsi que sur la réalisation d'inspections et de tests techniques ponctuels.

Résultat de l'audit : l'audit a mis en évidence l'existence dans tous les domaines contrôlés de risques faibles pour une partie et moyennement élevés pour une autre partie. Globalement, de bonnes conditions sont réunies pour une protection de base adéquate de l'infrastructure informatique. Il faut cependant que les mesures et les tâches identifiées antérieurement comme étant nécessaires dans le domaine SIPD soient priorisées plus clairement sur la base des risques, que le calendrier de leur réalisation soit adapté en conséquence et que leur efficacité soit contrôlée. L'audit n'a pas non plus permis de conclure entièrement à un renforcement et à une vérification systématiques des systèmes techniques. Des possibilités d'amélioration ont été observées concernant la sécurisation des flux de données à l'intérieur du réseau ainsi que dans les échanges avec l'extérieur.

La collaboration s'est déroulée de façon professionnelle et dans un bon esprit de coopération entre toutes les parties prenantes. Le Bureau suivra activement la mise en œuvre des mesures d'amélioration préconisées.

Système d'information Schengen (SIS) au Service des migrations

Objet de l'audit : 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 2020 les accès du Service des migrations du canton de Berne (SEMI).

But de l'audit : dans le cas du SIS, il s'agit de vérifier si ce système est utilisé de manière conforme aux prescriptions légales. Les contrôles effectués ont porté sur les accès au SIS, sur la compréhension par le personnel du SEMI des enjeux de la protection des données, sur la gestion des droits d'accès et sur le résultat des contrôles annuels des autorisations d'accès au SIS. Des renseignements complémentaires ont en outre été demandés concernant les rôles du SEMI correspondant aux autorisations d'accès au SIS.

Résultat de l'audit : dans les accès au SIS qu'il a contrôlés, le Bureau a constaté que le système avait été utilisé pour les tâches du SEMI comme il se doit. Il n'a pas constaté d'irrégularités (p. ex. aucun utilisateur n'a fait de requête sur lui-même ou sur des personnalités publiques). Toutefois, le Bureau a remarqué un déficit concernant la formation et l'information régulières au sujet du système. Par ailleurs, le SEMI n'a pas pu produire les résultats d'un contrôle régulier des droits d'accès au SIS, ni la documentation conceptuelle requise concernant la gestion de ces droits. Le Bureau a recommandé au SEMI de combler les lacunes constatées.

6.6 Autres instruments relevant du droit de la surveillance

6.6.1 Propositions motivées et recours

La loi prévoit que le Bureau, lorsqu'il constate des irrégularités ou des lacunes, recommande d'y remédier en présentant une proposition motivée. Si l'autorité responsable ne veut pas donner suite à la proposition ou n'est prête à le faire que partiellement, elle rend une décision, que le Bureau peut attaquer devant la Direction compétente ou le Tribunal administratif (art. 35, al. 3 à 5 LCPD). Dans la pratique, le Bureau n'utilise pas la forme de la proposition motivée pour présenter ses recommandations, notamment lorsqu'elles font suite à des questions qui lui ont été adressées, à des contrôles préalables ou à des audits, parce que les autorités responsables sont généralement disposées à appliquer spontanément des recommandations fondées sur des bases techniques. Il faudrait qu'une

autorité ne suive pas une préconisation importante du Bureau (visant p. ex l'élimination d'une irrégularité évidente ou d'un risque élevé) pour que celui-ci recoure à la voie formelle de la proposition motivée.

En 2020, le Bureau n'a pas présenté de proposition formelle et n'a pas formé de recours contre une décision négative d'une autorité responsable.

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

Développement de la surveillance de la protection des données au niveau communal

Comme l'avait constaté le Bureau en 2019, il n'est pas rare que les questions de droit délicates et les problématiques techniques confrontent les autorités communales et leur organe de surveillance à la limite de leurs capacités et que les communes ne bénéficient pas de conseils suffisants (cf. rapport d'activité 2019, p. 32). La révision de la LCPD qui a débuté offre l'opportunité de revoir et, le cas échéant, d'adapter la disposition de la loi imposant à chaque commune de désigner pour son domaine sa propre autorité de surveillance. C'est pourquoi le Bureau a d'abord invité l'Association des communes bernoises (ACB) et l'OACOT à participer à un groupe de travail informel pour confirmer la nécessité d'agir sur ce plan et esquisser des pistes de solution. Le résultat de ces travaux a été présenté à un cercle plus large réunissant des représentant·e·s des préfectures et de six communes de tailles variées pour en discuter et poursuivre la réflexion.

L'orientation qui se dessine est que la très grande majorité des communes doivent être délivrées de l'obligation d'avoir leur propre organe de surveillance et, à la place, bénéficier des conseils et de la surveillance du Bureau, qui interviendrait en qualité de centre de compétences à l'échelle du canton. Seules les communes les plus grandes qui sont équipées de systèmes informatiques complexes doivent conserver leur propre organe de surveillance car il connaît les spécificités locales et est en dialogue permanent avec les autorités responsables. Cette hypothèse de travail appelle une analyse approfondie du cahier des charges de l'organe de surveillance et la clarification des rapports entre la surveillance de la protection des données et la surveillance exercée par les préfectures en vertu du droit communal.

Le Bureau fera valoir le résultat de ces travaux préparatoires au nom du groupe de travail dans le processus de révision de la LCPD. Les propositions seront soumises à une discussion publique dans le cadre de la procédure législative normale, qui est dirigée par la Direction de l'intérieur de la justice (DIJ).

Conseils en matière de vidéosurveillance communale

Plusieurs organes communaux de surveillance de la protection des données ont demandé au Bureau son soutien pour évaluer des dispositifs de vidéosurveillance dans l'espace public ou à des fins de protection de bâtiments communaux. Une commune et un syndicat de communes souhaitaient surveiller des locaux scolaires, le premier y incluant une place de grillade dans l'enceinte de l'école. Le Bureau a communiqué aux organes de surveillance les documents à remplir pour un contrôle préalable et un rapport ainsi qu'une liste de contrôle pour vérifier la sûreté de l'information et la protection des données. Les questions adressées au Bureau concernaient la sécurité technique des données (p. ex. enregistrements vidéo), la proportionnalité (p. ex. champ des caméras) et la licéité (p. ex. accès aux images réservé exclusivement à la POCA).

Conseils aux organes de surveillance des Eglises nationales

La LEgN a conféré aux trois Eglises concernées la compétence de désigner leur propre organe de surveillance. L'organe de surveillance de l'Eglise réformée évangélique a posé au Bureau une question concernant les échanges d'informations prévus par le Concordat relatif à la formation conjointe des pasteures et pasteurs réformés et leur admission au service de l'Eglise. Celui-ci permet des échanges d'informations afin que les ecclésiastiques qui n'ont pas l'aptitude ou qui ont une aptitude insuffisante pour exercer un ministère pastoral ne puissent pas simplement changer de paroisse ou d'Eglise nationale. Comme l'Eglise réformée évangélique n'est pas membre du concordat, elle voulait clarifier les conditions à remplir pour pouvoir participer à ces échanges d'informations. Selon l'analyse effectuée par le Bureau, la LEgN régit les conditions d'engagement des ecclésiastiques, mais elle précise que le droit des Eglises nationales peut prévoir des conditions d'engagement complémentaires. Cela n'inclut cependant pas de fournir des informations sur l'aptitude au sens du concordat. Ces informations ont très vraisemblablement le caractère de données personnelles particulièrement dignes de protection, dont le traitement doit reposer clairement sur une base légale selon la LCPD (art. 6, lit. *a*). Comme ni la LEgN ni le droit ecclésial ne contiennent de dispositions claires à ce sujet, notamment en ce qui concerne les échanges de données avec d'autres Eglises nationales, le Bureau en a conclu qu'il fallait créer une base légale appropriée ou bien que l'Eglise réformée évangélique devait adhérer au concordat.

6.7 Coopération intercantonale

Groupes de travail de privatim

Le *groupe de travail Cyberadministration* a travaillé longuement sur la nouvelle obligation faite aux autorités de notifier aux autorités de surveillance de la protection des données les incidents dans ce domaine. Dans le canton de Berne, cette obligation s'applique depuis le 1er septembre 2018 à certaines autorités de justice et police (art. 1, al. 1 de l'ordonnance portant introduction de la directive de l'UE relative à la protection des données à caractère personnel). Le groupe de travail a élaboré un formulaire-type de signalement pour les autorités et un document décrivant la procédure à suivre par les autorités de protection des données pour traiter les notifications, et ces documents ont été mis à disposition par privatim. Le Bureau les a adaptés au droit cantonal. Le formulaire de notification peut être téléchargé par les autorités sur le site Internet du Bureau.

Le *groupe de travail Sécurité* a effectué une revue technique de documents de l'Association Electronic Monitoring sous l'angle de la protection des données. L'association projette de mettre en place, avec le concours de fournisseurs externes, une infrastructure qui pourra être utilisée par les cantons pour assurer l'exécution d'arrêts domiciliaires ou d'interdictions de contact ou de périmètre au moyen de bracelets électroniques. Le groupe de travail a mis en lumière les rôles et les responsabilités des différentes parties au regard du droit de la protection des données et présenté une série d'exigences à remplir pour que l'infrastructure soit conforme aux prescriptions cantonales en la matière.

Le *groupe de travail Santé* a repris ses travaux en 2020 sous la direction de la déléguée à la protection des données suppléante du Bureau. Il a travaillé principalement sur le dossier électronique du patient, mais il a dû aussi traiter dans des délais courts des questions d'actualité posées par la lutte contre la pandémie de coronavirus, concernant notamment la publication sur Internet de données anonymisées sur les cas positifs ainsi que la collecte et la sauvegarde des données dans le cadre du traçage des contacts.

Au sein du *groupe de travail TIC*, des représentant·e·s des organes cantonaux de surveillance ayant leurs propres informaticiens ont échangé au sujet de questions d'actualité ayant trait à la sûreté de l'information.

Swiss Library Service Platform (SLSP)

La nouvelle plateforme nationale de bibliothèques SLSP, qui a remplacé les catalogues des bibliothèques universitaires début 2021, a été soumise pour la première fois à un contrôle préalable supracantonal. Les bureaux de surveillance de la protection des données des cantons de Bâle-Ville, Zurich

et Berne ont examiné conjointement les documents SIPD fournis en tenant compte des spécificités des législations cantonales. Ils ont ainsi produit une évaluation commune sur laquelle les autres cantons peuvent s'appuyer.

Registre des tumeurs Berne et Soleure (KRBESO)

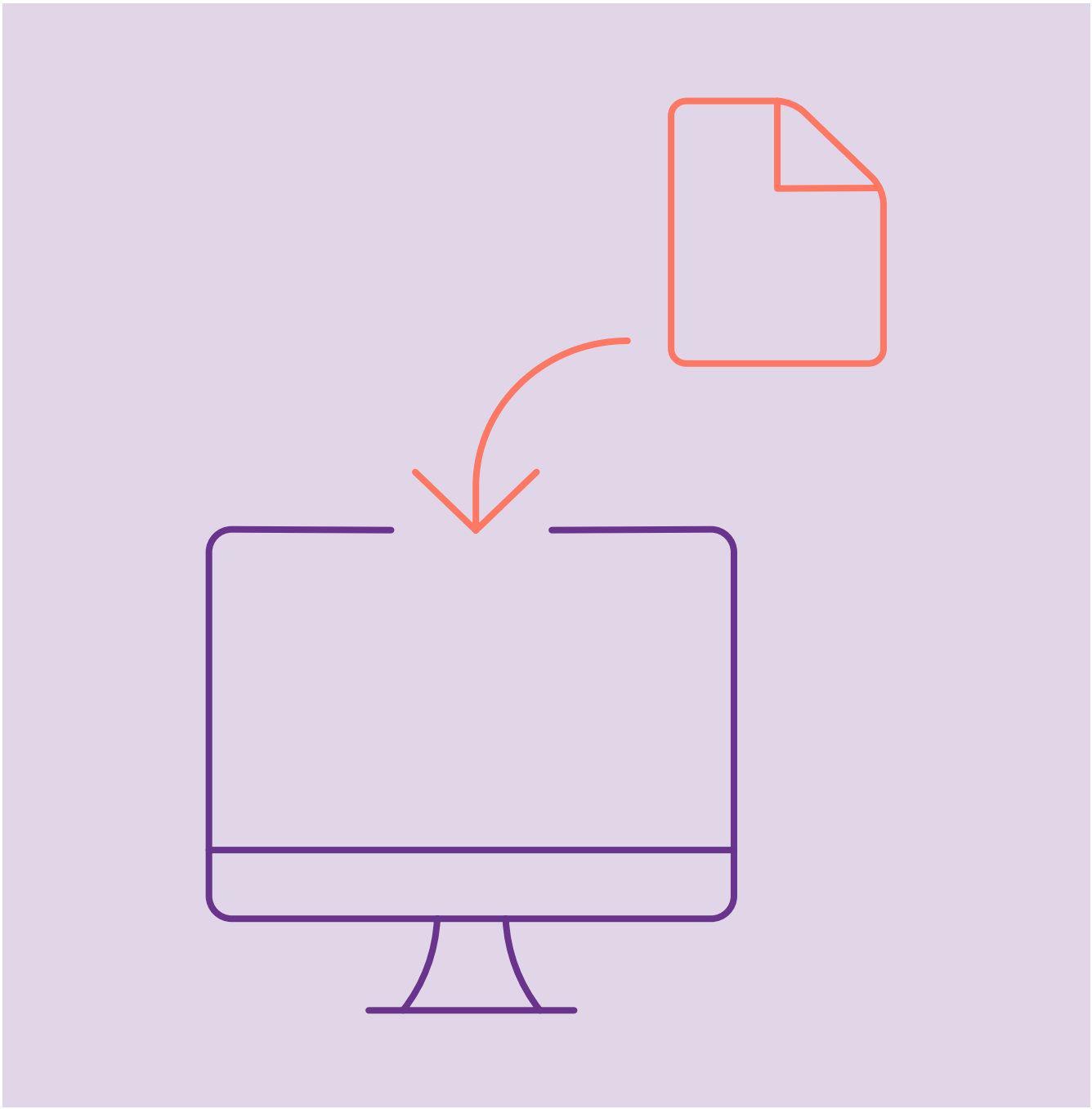
Le registre des tumeurs des cantons de Berne et Soleure rassemble les données des personnes atteintes de maladies oncologiques dans le canton de Berne depuis 2013 et dans le canton de Soleure depuis 2019. Il est tenu à l'aide d'un nouveau logiciel conforme aux charges prévues par la loi fédérale sur l'enregistrement des maladies oncologiques entrée en vigueur le 1er janvier 2020. Le Bureau a rédigé un premier rapport d'audit, qu'il a communiqué à son homologue soleurois afin qu'il puisse en utiliser les résultats et les constats.

7 Proposition

Prise de connaissance.

8 Glossaire

CHA	Chancellerie d'Etat
DSSI	Direction de la santé, des affaires sociales et de l'intégration
INC	Direction de l'instruction publique et de la culture
LCPD	Loi sur la protection des données
LEgN	Loi sur les Eglises nationales
OACOT	Office des affaires communales et de l'organisation du territoire
OIO	Office d'informatique et d'organisation
PFPDT	Préposé fédéral à la protection des données et à la transparence
POCA	Police cantonale
privatim	Conférence des préposé(e)s suisses à la protection des données
SIPD	Sûreté de l'information et protection des données



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