Kanton Bern
Canton de Berne

Rapport d'activité Bureau pour la surveillance de la protection des données 2022

Bureau pour la surveillance de la protection des données Février 2023

Impressum

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

Maquette et réalisation : noord.ch

Table des matières

1 Avant-propos

Au fond, le droit de la protection des données est assez facile à expliquer. Lorsque des autorités traitent des données personnelles, ce qui est régulièrement le cas dans l'accomplissement de leurs tâches, elles doivent respecter quelques règles et s'assurer que les données qu'elles traitent sont protégées du non-respect de ces règles. Le but du droit de la protection des données n'est pas de compliquer la vie des autorités. Ce qui est en jeu, ce sont les attentes fondamentales auxquelles doit répondre l'État de droit : les personnes qui accomplissent des tâches relevant de la puissance publique doivent s'en tenir aux prérogatives que leur confère la loi (licéité) et, s'il leur faut restreindre des droits ou des libertés des citoyennes et des citoyens, elles doivent le faire avec le plus grand ménagement possible (proportionnalité). Enfin, elles sont tenues d'indiquer aux personnes concernées quelles sont leurs données qui sont traitées et dans quels buts (transparence).

Si cela semble clair et évident de prime abord, les choses se compliquent lorsqu'il s'agit d'appliquer ces quelques principes à la variété des problématiques auxquelles les autorités sont confrontées dans leurs activités quotidiennes. L'administration a-t-elle le droit de copier la totalité des données de son système de gestion des affaires dans un système de test pour contrôler l'exécution de nouvelles fonctionnalités et réaliser des formations ? A-t-elle le droit d'envoyer des SMS non sollicités à des personnes au chômage pour leur rappeler leur prochain rendez-vous dans un office régional de placement (ORP) ? Est-il proportionné d'installer des caméras dans un centre de retour pour pouvoir assurer la sécurité la nuit et le weekend, lorsque le personnel est en effectif réduit ? Une personne a-t-elle le droit de consulter le dossier ouvert par l'office compétent pour déterminer la capacité de conduire de son père entre-temps décédé ?

S'il incombe à chaque autorité de se conformer aux principes de l'État de droit lorsqu'elle traite des données personnelles et d'en assurer la sécurité, on peut ne pas attendre d'elle qu'elle soit en mesure de résoudre toutes les problématiques de protection des données qu'elle rencontre, surtout si la question se pose pour la première fois. C'est déjà beaucoup si l'autorité se rend compte qu'une situation pose des problèmes au regard du droit de la protection des données et demande conseil à l'organe de surveillance compétent ou à un autre service désigné à cet effet.

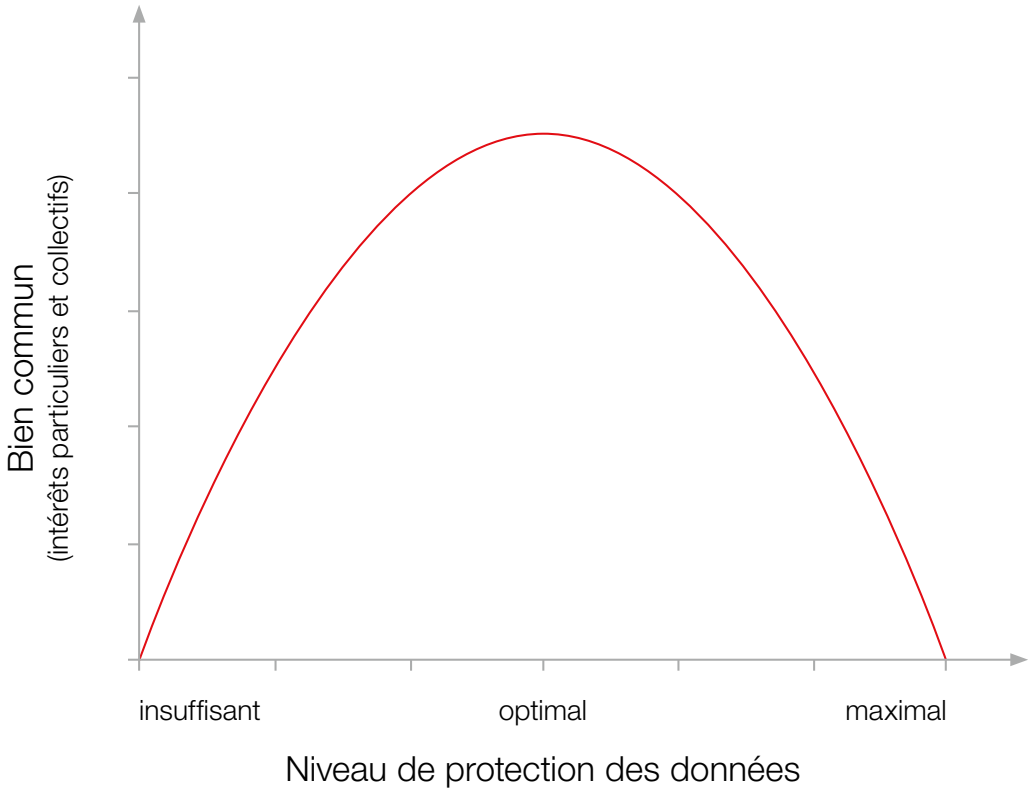
Le présent rapport illustre la grande variété des activités des autorités dans lesquelles se posent des questions de protection des données dont le Bureau pour la surveillance de la protection des données (Bureau) a été saisi dans le cadre de ses activités de conseil et de surveillance durant l'année sous revue.

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 le droit à l'autodétermination informationnelle (c.-à-d. le droit de chaque personne de pouvoir déterminer si des données la concernant sont traitées ou non et dans quels buts), comme un droit fondamental. Un droit fondamental ne peut faire l'objet d'une restriction qu'à certaines conditions : la restriction 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). Évidemment, 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.

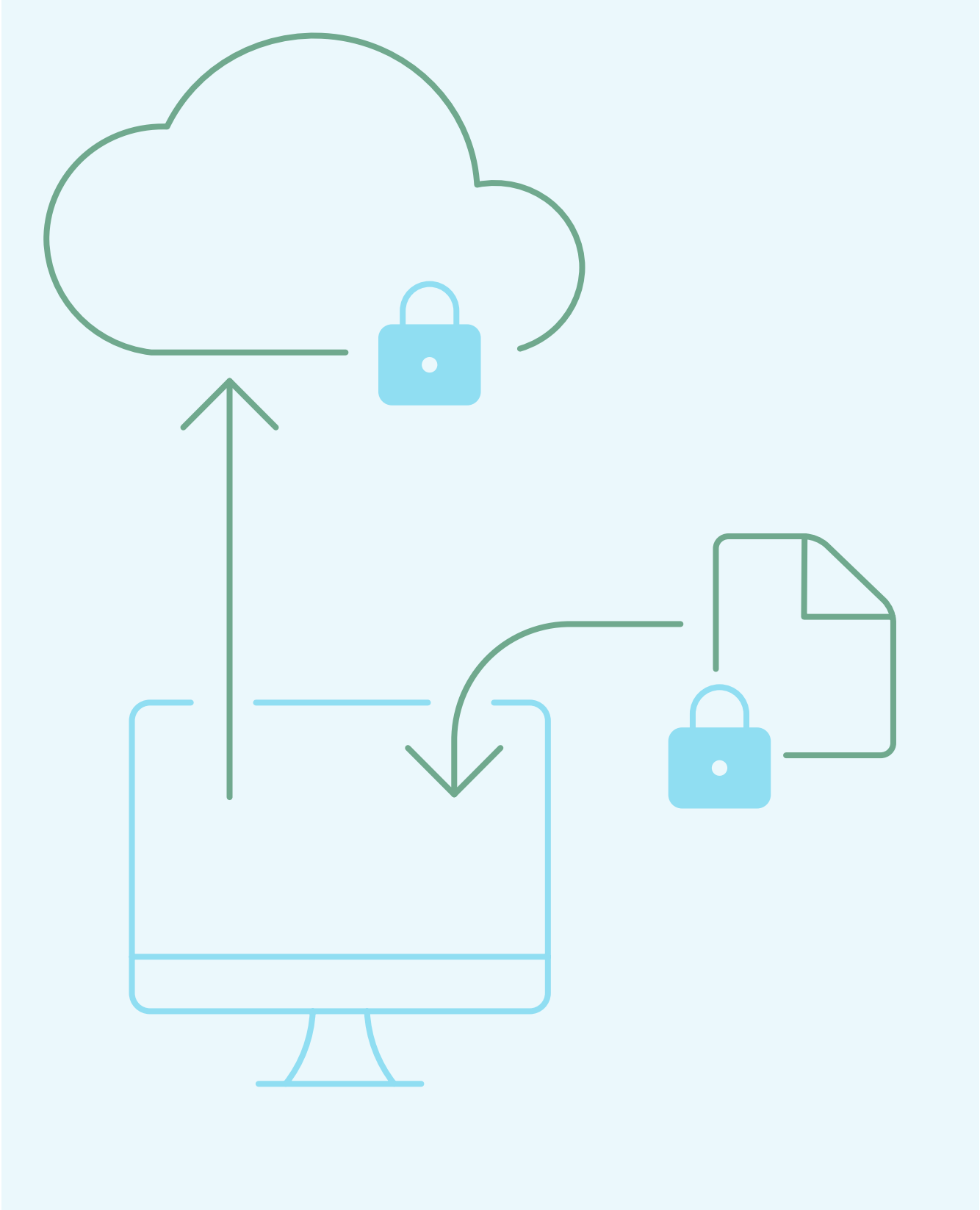
La loi cantonale sur la protection des données (LCPD) précise les devoirs des autorités lors du traitement des données personnelles. Par autorité, il faut comprendre l'administration, mais aussi d'autres entités chargées de tâches publiques comme les écoles et les hôpitaux. Quant au traitement, il se 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.

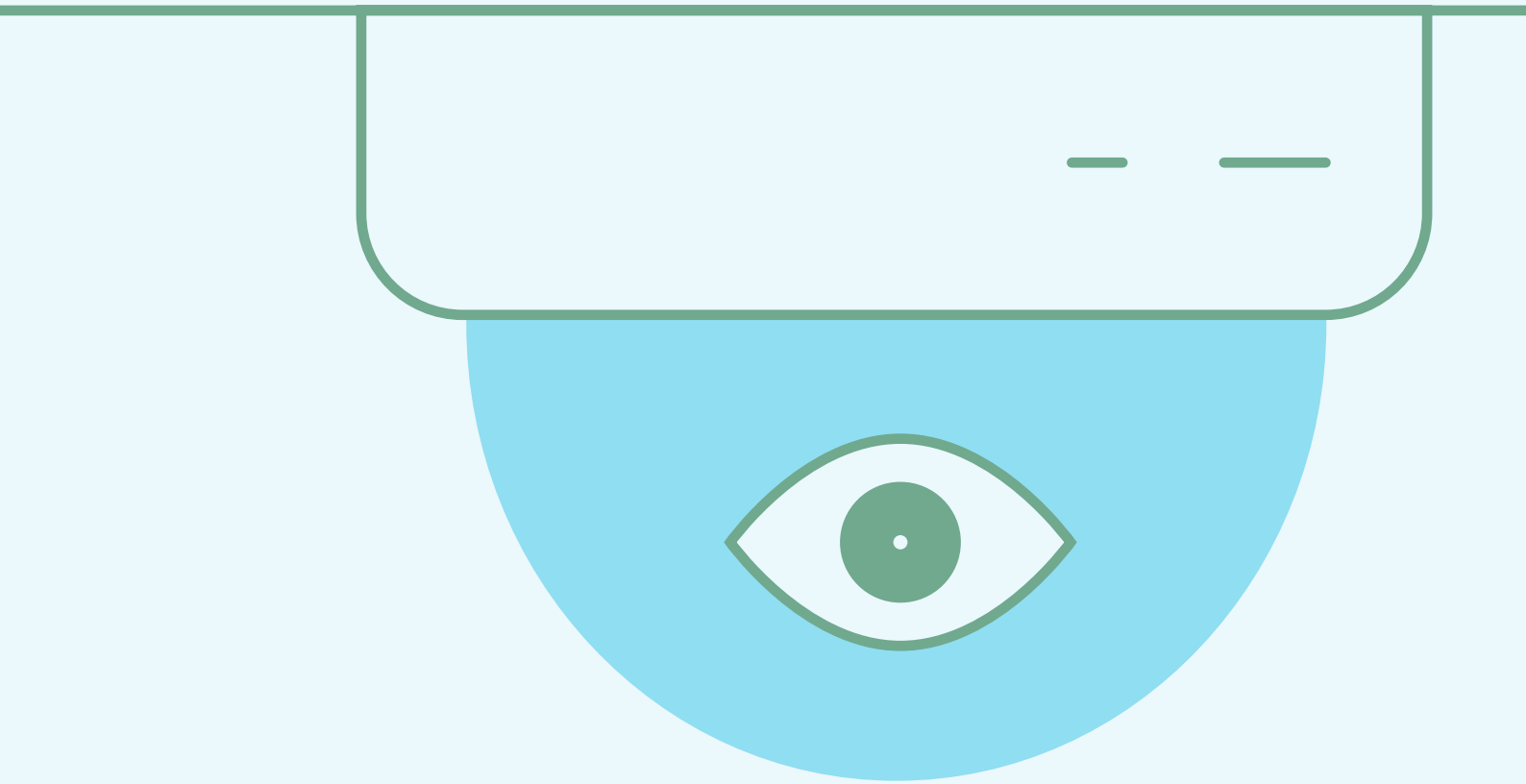
3 Responsabilité et surveillance

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 des 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. À 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, LEp) 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 de 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 s’il ne faut attendre aucun résultat des conseils fournis en vue de la résolution des problèmes et de la coopération avec les autorités.
Ces conseils n’en constituent pas moins une forme de surveillance préventive qui reste essentielle et qui est appelée à gagner en importance alors que les projets informatiques sont de plus en plus conduits selon les principes de l’agilité.
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 2022, le Bureau disposait de 570 pour cent de poste 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 2019. À 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 [DIJ], sécurité [DSE]), de la Chancellerie d'État (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 et des questions relatives aux paroisses.

Stephanie Siegrist (collaboratrice scientifique, domaine juridique) est juriste et historienne et travaille depuis 2021 pour le Bureau. Active dans les domaines de la santé et de la formation, elle est principalement responsable des demandes de renseignements et de conseils, des contrôles préalables, de la vidéosurveillance et des prises de position sur des textes de loi.

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.

Constatant que sa charge de travail ne cesse d'augmenter, en particulier dans le domaine des contrôles préalables (cf. ch. 6.3), le Bureau a demandé au Grand Conseil un poste à temps plein supplémentaire dans le cadre du budget 2023, ce que le parlement a accepté. Un séminaire consacré à la satisfaction professionnelle et à la santé des membres du personnel du Bureau a montré que ces personnes ont plaisir à travailler pour notre structure et qu'elles apprécient grandement la culture d'entreprise qui y règne. Elles estiment cependant qu'il y a lieu d'élaborer des mesures additionnelles en vue de maintenir un équilibre sain entre les forces à disposition et le volume de travail à absorber.

En 2022, les charges d'exploitation du Bureau se sont élevées au total à 210 milliers de francs. Environ 75 % de ces charges (157 milliers de fr.) ont été générées par des prestations externes ayant servi aux contrôles informatiques. Par inadvertance, trois factures de l'exercice précédent totalisant 70 milliers de francs n'avaient pas pu être comptabilisées sur 2021. Il en résulte que le Bureau affiche dans le compte d'État 2022 des charges d'exploitation de 279 milliers de francs et qu'il dépasse son budget 2022 de 55 milliers de francs.

Au sein de l'administration cantonale, d'autres organismes se chargent de conseiller les autorités dans le domaine SIPD. Les Directions et la CHA 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 porte un soin tout particulier à son réseau de partenaires au sein de l'administration et s'applique à le développer. En 2022, il a organisé une première rencontre, qui a été suivie d'une réunion de tous les organes de référence pour la protection des données dans le but de renforcer les échanges à la fois entre ces organes et avec le Bureau. Celui-ci 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'information et d'organisation [OIO], Bedag Informatique SA, Police cantonale [POCA] et Groupe de l'Île SA).

Dans l'optique d'aboutir à un programme d'audits SIPD coordonné à l'échelle de l'État, le Contrôle des finances (CF) du canton de Berne et le Bureau ont mis en place une collaboration renforcée sur le plan stratégique.

Membre de privatim, la Conférence des préposé(e)s suisses à la protection des données, le Bureau est régulièrement en contact 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 2022 sous le chiffre 6.6 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 Conseils

6.1.1 Conseils à l'intention des autorités

Utilisation de services en ligne (cloud) par les autorités cantonales

En février de l'année sous revue, privatim a adopté une version révisée de son aide-mémoire sur les risques et les mesures spécifiques à la technologie du cloud. L'autorité qui utilise des services de nuage informatique, notamment proposés par des fournisseurs internationaux ayant des palettes de prestations très largement standardisées sur les plans technique, organisationnel et juridique, perd le contrôle effectif des données qu'il lui incombe de protéger (y compris les données relatives aux utilisatrices et utilisateurs des services de cloud) : il ne maîtrise pas lesquelles de ces données sont traitées, en quels lieux géographiques et à quelles fins, ni qui peut les consulter (y compris dans les entreprises sous-traitantes). Cela présente un risque élevé pour la confidentialité des données, en particulier lorsque le fournisseur, en raison de son ancrage dans un pays étranger, peut être astreint à communiquer des données à des autorités étrangères (*lawful access*). Dans un arrêté de mars 2002 relatif à l'autorisation d'utilisation de Microsoft 365 (M365), le Conseil d'État du canton de Zurich s'est intéressé presque exclusivement à ce dernier risque, qu'il a jugé négligeable dans le cas concret, tandis qu'il a estimé que les risques de dépendance à l'égard du fournisseur et de perte de contrôle étaient inévitables. Il a donc décidé d'autoriser l'administration cantonale zurichoise à utiliser la solution informatique en nuage M365, non sans préciser que chaque unité administrative restait responsable de la protection des données et que les Directions et la Chancellerie d'État devraient si nécessaire édicter des règles complémentaires afin de garantir que l'utilisation de M365 reste conforme au droit.

Le canton de Berne étudie lui aussi l'intégration de M365 dans les services de base TIC de l'administration cantonale. Le Bureau a recommandé au Conseil-exécutif et à l'office responsable du dossier, l'OIO, une démarche différente et conforme à l'aide-mémoire de privatim : il convient de réaliser une analyse de risque globale, incluant l'ensemble des risques pour toutes les personnes concernées et comportant un scénario de sortie, puis, sur cette base, de définir

toutes les mesures techniques et organisationnelles requises pour garantir que chaque service du nuage peut être utilisé de manière sûre et conforme aux prescriptions en matière de protection des données ; les risques résiduels jugés supportables sont à exposer de manière exhaustive et transparente au Conseil-exécutif, qui les accepte et en assume la responsabilité. Au cours de l'année sous revue, le Bureau a continué de conseiller l'OIO en vue de l'élaboration du rapport sur les risques à l'attention du Conseil-exécutif.

En sa qualité de président de privatim, le délégué à la protection des données a été très impliqué dans l'activité de conseil auprès de la Conférence suisse sur l'informatique (CSI), qui devait renouveler son contrat-cadre avec Microsoft concernant l'utilisation de services en ligne par des organes publics suisses pour la période allant du 1er mai 2022 au 30 avril 2025. Pour compléter l'accord négocié à l'automne 2020 relatif à l'application du droit suisse et à la compétence des tribunaux suisses pour les actions visant à faire appliquer les promesses contractuelles de Microsoft concernant la protection des données, des clarifications et des assurances plus poussées ont été obtenues pour ce qui est de la confidentialité des données. Nonobstant cela, il subsiste quelques risques contractuels et la perte de contrôle effective sur les données externalisées. Il est donc absolument indispensable de procéder à une analyse globale des risques.

La société qui gère le centre hospitalier régional de Haute-Argovie, Spital Region Oberaargau AG (SRO AG), a demandé conseil au Bureau sur un dossier dans lequel elle n'était pas responsable de la protection des données sur le cloud : un médecin de famille souhaitait lui donner accès à des comptes rendus d'examens médicaux sur une plateforme en nuage à des fins de concertation, mais SRO AG aurait envoyé ses rapports au médecin de famille par les voies classiques. Bien qu'en l'espèce la responsabilité de la protection des données sur le service de cloud incombe au médecin de famille, le Bureau a recommandé à SRO AG de s'assurer que la consultation de documents sur cette plateforme n'engendrerait pas de risques de sécurité pour ses propres systèmes.

Utilisation systématique des numéros AVS en dehors de l'AVS

Une modification de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS) entrée en vigueur le 1er janvier 2022 permet aux unités des administrations cantonales et communales d'utiliser systématiquement le numéro AVS dans la mesure où l'accomplissement de leurs tâches légales le requiert. L'utilisation du numéro AVS est réputée systématique lorsque ce numéro est lié à des données personnelles collectées de manière structurée. Pour remplir la condition fixée dans la loi, il ne suffit pas que l'utilisation du numéro AVS soit pratique. Il faut établir l'existence d'une nécessité technique – à savoir l'assurance de la qualité et l'amélioration de l'efficacité des traitements de données automatisés – à laquelle il est impossible de faire face correctement sans l'utilisation du numéro

AVS. La permission d'utiliser systématiquement les numéros AVS est assortie de plusieurs obligations pour les autorités habilitées : celles-ci sont tenues de prendre les mesures techniques et organisationnelles prévues par la loi pour protéger les numéros des utilisations abusives (art. 153d LAVS) et d'informer la Caisse centrale de compensation de l'utilisation systématique de ces numéros (art. 153f LAVS). Le canton dans son ensemble doit effectuer régulièrement une analyse des risques portant en particulier sur le risque d'un regroupement illicite de banques de données. Il tient à cet effet un répertoire des banques de données dans lesquelles le numéro AVS est utilisé de manière systématique (art. 153e LAVS). En juillet de l'année sous revue, le Bureau a rendu les Directions et la CHA attentives à ces obligations légales. En décembre, il s'est adressé individuellement aux unités administratives pour leur demander de signaler si elles faisaient une utilisation systématique du numéro AVS et, dans l'affirmative, de rendre compte des mesures prises.

Service de SMS pour les personnes au chômage

L'Office de l'assurance-chômage (OAC) s'est adressé au Bureau car il souhaitait mettre en place un service de SMS utilisant les numéros de mobile fournis par les clientes et les clients dans leurs coordonnées afin de leur rappeler leur prochain rendez-vous pour un entretien en ORP et de les informer des paiements effectués par la caisse de chômage. Le Bureau a jugé que ce projet était en principe admissible parce que l'utilisation prévue des numéros de mobile relevait de l'accomplissement des tâches légales de l'OAC et présentait en outre un intérêt présumé pour les personnes concernées. Il a cependant recommandé de prévoir une possibilité de refus des SMS et de mettre fin aux envois lorsqu'une personne s'y oppose expressément après réception d'un message (*opt out*). En outre, comme il est possible que ces SMS soient lus par des tiers non impliqués, il a conseillé de choisir un texte neutre ne permettant pas d'identifier l'expéditeur ni d'obtenir des indications sur la situation professionnelle de la personne destinataire.

Base légale pour des publications sur Internet

L'OACOT a demandé au Bureau s'il suffisait, pour publier sur Internet des procès-verbaux d'assemblée d'une conférence régionale, que cela soit prévu dans le règlement d'organisation de ladite conférence ou s'il fallait que cette possibilité soit ancrée dans une ordonnance. Les conférences régionales sont des corporations de droit public au sens de la loi sur les communes. Par conséquent, leurs procès-verbaux doivent être publiés, comme ceux des communes. Or, une publication sur Internet ne requiert actuellement pas de prescription particulière pour être autorisée (cf. art. 2 de l'ordonnance sur la protection des données [OPD]). Les conférences régionales régissent l'accomplissement de leurs tâches dans un règlement, dans lequel elles peuvent

faire figurer toutes les dispositions nécessaires à cet effet, dans la mesure où l'ordonnance sur le règlement d'organisation des conférences régionales leur en laisse la latitude. Dans ce contexte, le Bureau a estimé qu'une disposition dans le règlement d'organisation était une base légale suffisante, d'autant que ces règlements sont soumis au référendum facultatif.

La version révisée de la loi sur l'information adoptée par le Grand Conseil en 2022 (nouveau titre : loi sur l'information et l'aide aux médias, LIAM) apporte une nouvelle base légale à toutes les autorités cantonales et communales : elle les autorise à communiquer des données personnelles sur Internet dans le cadre d'informations d'intérêt général, dans la mesure où aucun intérêt public ou privé prépondérant ne s'y oppose (art. 15b en relation avec l'art. 16, al. 1, lit. *a* et *c* LIAM).

Évaluation de fichiers de journalisation en cas de suspicion d'utilisation abusive

L'Intendance des impôts du canton de Berne (Intendance cantonale des impôts, ICI) voulait vérifier s'il est obligatoire d'informer les membres du personnel avant d'évaluer des fichiers de journalisation pour contrôler l'application du devoir de récusation. Le Bureau a répondu par l'affirmative. La loi sur le personnel (LPers) et l'ordonnance sur les données secondaires de communication (ODSC) règlent de façon rigoureuse et détaillée les conditions à respecter et le processus à suivre pour évaluer des fichiers de journalisation. Il est possible de procéder à une évaluation nominale se rapportant à des personnes en lien avec une possible utilisation abusive uniquement en cas de soupçon concret ou d'utilisation abusive avérée (art. 12d, al. 3 LPers). En outre, la personne concernée doit avoir été informée préalablement par écrit de l'existence d'un soupçon concret ou d'un abus avéré (art. 12d, al. 4 LPers). Enfin, l'autorité chargée de l'évaluation doit vérifier que ces conditions ont bien été remplies avant de procéder à l'évaluation (art. 11 ODSC).

Lexique de la protection des données pour l'école obligatoire

L'Office de l'école obligatoire et du conseil (OECO) avait rédigé en 2008 des lignes directrices sur la protection des données. Comme elles ont vieilli, il a décidé de les réviser, travail qui a débuté à l'été 2020. La nouvelle version devrait être adoptée en 2023, sous le nom de « Lexique de la protection des données ».

Le Bureau suit le projet activement dans le cadre de son mandat de conseil. Il a exposé au groupe de projet les dernières évolutions en matière de protection des données, en particulier concernant les risques et les mesures spécifiques à la technologie du cloud. Le futur lexique a pour vocation d'être le premier

ouvrage auquel les établissements de la scolarité obligatoire se réfèrent lorsqu'ils ont des questions relevant du droit de la protection des données, mais aussi de sensibiliser ces établissements à la problématique afin de renforcer leurs compétences dans ce domaine.

Gestion des dossiers médicaux après la cessation d'activité d'un médecin

Un hôpital ayant un mandat de prestation du Conseil-exécutif (c.-à-d. figurant sur la liste des hôpitaux) a demandé au Bureau ce qu'il devait faire des dossiers médicaux de la patientèle d'un médecin de famille après la cessation d'activité de ce dernier.

Le Bureau s'est référé à l'article 26 de la loi sur la santé publique, selon lequel les membres des professions de la santé doivent continuer, après la cessation de leur activité, de s'assurer que les dossiers sont conservés conformément au devoir de discrétion et qu'ils sont accessibles à la patientèle (al. 3). Il n'est pas permis de soumettre les dossiers médicaux à des traitements dépassant ce cadre. Les dossiers peuvent être confiés pour conservation notamment à une personne soumise au même devoir de discrétion, c'est-à-dire une ou un autre médecin. La transmission des dossiers ne requiert pas le consentement des patientes et des patients. Les membres des professions de la santé peuvent cependant se dégager de leur obligation moyennant l'accord écrit de leurs patientes et de leurs patients, en leur remettant leurs dossiers ou en les transmettant au professionnel ou à la professionnelle de la santé assurant la continuation du traitement (al. 4).

6.1.2. Conseils à l'intention des personnes concernées

Compétence pour les demandes de renseignements en matière fiscale

Une personne souhaitant obtenir des renseignements sur les données fiscales la concernant relatives à une année de taxation déterminée a fait appel au Bureau. Il a d'abord fallu déterminer quelle était l'autorité fiscale compétente pour traiter la requête. L'étude du dossier a montré que c'est un service de l'Intendance cantonale des impôts qui est compétent pour ce type de demande, quelle que soit l'autorité fiscale à qui la requête a été adressée (l'une des cinq autorités fiscales régionales ou l'une des trois autorités fiscales communales). Les autorités fiscales régionales et communales ont pour instruction de faire suivre sans délai les demandes de renseignements qu'elles reçoivent. Les citoyennes et les citoyens peuvent ainsi, sans que cela leur porte préjudice, adresser leurs requêtes à n'importe quelle autorité fiscale.

Consultation de données d'une personne décédée

Une personne avait demandé à l'Office de la circulation routière et de la navigation (OCRN) à consulter le dossier établi pour déterminer la capacité de conduire de son père, entre-temps décédé. L'OCRN avait refusé en invoquant la protection des données. Le Bureau a indiqué à la personne une disposition de l'ordonnance sur la protection des données, selon laquelle la consultation des données d'une personne décédée est accordée lorsque la personne requérante justifie un intérêt à la consultation – intérêt qui est établi en cas de proche parenté – et qu'aucun intérêt prépondérant de proches de la personne décédée ou de tiers ne s'y oppose (art. 12 OPD). Grâce à ce renseignement, la personne a été en mesure de répondre à l'OCRN que le droit de la protection des données n'interdisait pas la consultation demandée, mais l'autorisait même expressément.

Envois postaux : la mention de l'expéditeur porte-t-elle atteinte à la protection des données ?

Une personne avait reçu par la poste une amende d'ordre de la POCA dans une enveloppe indiquant « POLICE Bern » comme expéditeur. Elle y a vu une atteinte à la protection des données et s'est adressée au Bureau, qui lui a fourni les explications suivantes. La mention de l'expéditeur sur les envois postaux du canton de Berne indique effectivement que la ou le destinataire a affaire avec l'unité administrative concernée sous une forme ou sous une autre. Toutefois, il y a tellement de raisons pour lesquelles une personne est susceptible d'être en contact avec une autorité et de recevoir des courriers de sa part que la simple mention de cette autorité sur une enveloppe ne permet pas de savoir pour quel motif le courrier a été envoyé. Dans le cas de la POCA, le courrier peut contenir un conseil de protection contre les infractions sollicité par la personne, l'annonce d'une manifestation (p. ex un cortège du 1er août) ou encore une convocation à comparaître si la personne s'est manifestée après un appel à témoins. La simple mention de l'expéditeur, que le personnel de la poste a besoin de connaître au cas où le courrier ne pourrait pas être remis pour pouvoir le retourner sans ouvrir l'enveloppe, ne fournit normalement pas d'autre indication et doit donc être considéré comme licite.

Cela n'exclut cependant pas que, dans des situations particulières, cette mention puisse constituer une atteinte à la protection des données. Si un courrier est expédié par la Commission de recours contre les mesures administratives prononcées en vertu de la loi sur la circulation routière, par exemple, cela donne des indices bien plus concrets sur le contenu de l'envoi et donc sur la personne à laquelle il est destiné. Si, comme c'est déjà le cas au niveau fédéral, les données sur des sanctions administratives sont réputées à l'avenir être des données personnelles particulièrement dignes de protection, dont la communication à des tiers n'est autorisée qu'en cas de nécessité impérative, l'indication de

l'expéditeur in extenso deviendra difficilement admissible dans l'exemple précité tant qu'il est possible de faire figurer à la place une abréviation et une case postale.

Protection des données dans les procédures administratives multipartites (p. ex. procédure d'édiction de plans)

Suite à une plainte en matière de surveillance de la protection des données déposée dans le cadre de la procédure d'édiction d'un plan de route, le Bureau a vérifié dans quelle mesure l'autorité qui instruit le dossier en vue de rendre une décision dans une procédure de première instance impliquant plusieurs parties est autorisée à communiquer des données concernant une partie aux autres parties. Si la loi sur la procédure et la juridiction administratives (LPJA) donne en principe aux parties le droit de consulter toutes les pièces du dossier, la LCPD s'applique également et elle n'autorise la communication de données personnelles à des tierces personnes privées que dans la mesure où cela est nécessaire à l'accomplissement des tâches. Est-il nécessaire qu'une partie connaisse l'identité et les demandes de toutes les autres parties même si cela est sans rapport avec ses propres intérêts ? La réponse ne coule pas de source.

Le Bureau admet qu'il y a des raisons factuelles dans la législation pour autoriser la communication de ces données. Lorsque des oppositions peuvent être formées pour invoquer une violation du droit public, notamment, le fait que chaque personne ayant formé opposition connaisse l'identité et les demandes des autres parties favorise la qualité des oppositions et des éventuels recours et ainsi, in fine, la qualité de la décision de l'autorité. À cela s'ajoutent des aspects d'économie procédurale : s'il fallait que les personnes qui forment opposition ne puissent rien savoir les unes des autres, cela obligerait l'autorité qui instruit le dossier à anonymiser individuellement (par caviardage) les décisions qu'elle rend tout au long de la procédure puis à son terme. Dans les procédures avec un très grand nombre de parties, cela demanderait un travail disproportionné, qui deviendrait difficile à justifier par la protection de la sphère privée. Le Bureau proposera donc, dans le cadre de la révision en cours de la LPJA, que la situation juridique soit clarifiée et que la communication de l'identité et des demandes des parties aux autres parties soit légitimée dans la mesure où aucun intérêt prépondérant ne s'oppose à cette divulgation.

6.1.3. Formation continue

Contribution à la formation du personnel communal et paroissial

Le *Bildungszentrum für Wirtschaft und Dienstleistung* (bwd) propose différentes formations à l'intention des personnes travaillant pour des autorités communales

ou paroissiales. Cela fait de nombreuses années – et 2022 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. Le cours à l'intention du personnel des secrétariats paroissiaux introduit en 2020 a lieu une fois par an et une formation consacrée à la protection des données dans les paroisses est proposée aux autorités paroissiales depuis 2021. Au cours de cette formation, les intervenantes et les intervenants du Bureau expliquent les principes généraux de la protection des données et leur application dans le domaine d'activité de leur auditoire. Ils s'attachent également à établir la discussion et à répondre aux questions concrètes des participantes et des participants en lien avec leur travail quotidien.

Diffusion de connaissances lors d'événements spécifiques

Le délégué à la protection des données a été sollicité pour participer à différents congrès et formations continues. Il s'est exprimé sur les défis auxquels sont actuellement confrontées les autorités de protection des données (dans le cadre de la Journée internationale de la protection des données à l'Université de Lausanne), sur le traitement de données sur mandat par les fournisseurs de cloud (invitation à présenter un exposé dans le cadre du cours sur le droit de la protection des données de l'Université de Lucerne ; 26e *Symposium on Privacy and Security* ; *Workplace Conference* 2022 de la CSI) ainsi que sur la protection des données dans le contexte de la transition numérique dans le système scolaire (colloque de la Haute école pédagogique germanophone).

6.2 Prises de position formelles

Révision totale de la loi sur la protection des données

La LCPD, qui a été introduite en 1986, doit être adaptée aux progrès techniques et aux nouvelles dispositions du droit européen, à savoir la directive (UE) 2016/680 relative à la protection des données dans le domaine du droit pénal et à la révision de la Convention du Conseil de l'Europe pour la protection des données. La directrice de la DIJ ayant chargé l'Office juridique en août 2020 d'élaborer un projet de révision, le Bureau a siégé au sein de deux groupes de travail inter-Directions, l'un consacré au droit européen et l'autre aux questions politiques, afin d'apporter ses idées et ses appréciations. La première procédure de corapport sur le projet destiné à la consultation a eu lieu au cours

de l'année sous revue. Le projet ayant été fortement remanié depuis les séances des groupes de travail, le Bureau a de nouveau fait part de nombreuses idées, qu'elles aient trait à la technique législative ou au fond.

Le Bureau a notamment proposé de renoncer à une nouvelle disposition prévoyant que les autorités sont autorisées à traiter des données personnelles sans base légale si la personne concernée y a consenti ou si elle a rendu ses données accessibles à tout un chacun. En premier lieu, le principe constitutionnel de légalité exige que tout traitement de données personnelles repose sur une base légale. En effet, un traitement de données n'est jamais une fin en soi ; il a toujours pour but d'accomplir une tâche légale et celle-ci doit elle-même reposer sur une base légale, faute de quoi le principe de légalité n'est pas respecté. En deuxième lieu, le principe de la proportionnalité exige que le traitement des données soit nécessaire à l'accomplissement de la tâche considérée. Selon le droit en vigueur, le respect de ce deuxième principe se satisfait d'une norme de délégation suffisamment précise pour légitimer le traitement des données (« base légale indirecte »). Par ailleurs, si la personne concernée a rendu ses données accessibles à tout un chacun, cela peut certes éviter à l'autorité responsable d'avoir à demander lesdites données à la personne concernée, mais cela ne l'habilite pas pour autant à se procurer et à traiter n'importe quelles données, éventuellement dans le seul but de les mettre en réserve car une autorité ne peut utiliser que les données nécessaires à une tâche que lui confère la loi. Ainsi, la permission de traiter des données sans base légale que veut introduire la révision fait miroiter des possibilités plus étendues que ce qu'autorisent dans les faits les principes de légalité et de proportionnalité si bien qu'elle fait naître un risque de traitements illicites par les autorités.

Le Bureau a également proposé que la responsabilité de la protection des données reste attribuée « à l'autorité qui, pour accomplir les tâches que lui assigne la loi, traite ou fait traiter des données personnelles ». Certes, la nouvelle loi sur l'administration numérique (LAN) contient provisoirement la formule « qui décide du but et du moyen du traitement des données », qui est inspirée du droit européen et de la LPD révisée. Mais il est important de relever que cette formule, que ce soit au niveau européen ou au niveau fédéral, s'applique aussi aux personnes privées qui traitent des données et qu'elle doit donc rester générale. Dans la LCPD, qui s'applique exclusivement aux traitements de données par les autorités, il est possible et nécessaire que la responsabilité continue de se rapporter à l'entité chargée de tâches publiques tenue de garantir la constitutionnalité des traitements de données qu'elle doit effectuer pour accomplir lesdites tâches. La disposition actuelle l'établit sans aucun doute possible, non sans tenir compte du fait que des tâches publiques peuvent être déléguées (auquel cas le destinataire de la délégation devient l'autorité responsable) ou que des traitements peuvent être effectués par des personnes mandatées (auquel cas l'autorité d'origine conserve la responsabilité du traitement).

Loi sur la sécurité de l'information et la cybersécurité

Lorsque l'on traite des données personnelles, il faut en assurer la sécurité – c'est-à-dire la confidentialité, l'intégrité et la disponibilité – par des moyens techniques et organisationnels appropriés. Ce besoin de protection concerne non seulement les données personnelles mais aussi les informations factuelles nécessaires pour assumer des tâches publiques. La loi sur la sécurité de l'information et la cybersécurité (LSIC) définit le cadre légal dans lequel les autorités garantissent la sûreté du traitement des informations et de l'utilisation des outils des technologies de l'information et de la communication. Comme pour la révision de la LCPD, le Bureau a participé activement aux travaux préparatoires de cette nouvelle loi. De ce fait, le projet présenté lors de la première procédure de corapport était suffisamment au point pour que le Bureau n'ait que des observations ayant trait à la technique législative à apporter, observations reprises en quasi-totalité par la Direction chargée du dossier (FIN).

Du point de vue matériel, le Bureau estimait important que la LSIC contienne, à l'instar de la loi fédérale correspondante, une disposition relative à la gestion des risques pour la sécurité informatique qui impose aux autorités d'évaluer continuellement ces risques, de prendre les mesures nécessaires pour les éliminer ou les réduire à un niveau tolérable et de documenter l'acceptation des risques inévitables. Cette idée a été intégrée dans l'avant-projet destiné à la consultation (art. 5, al. 2 AP-LSIC).

Modification de la loi sur la police

Le Tribunal fédéral ayant abrogé certaines dispositions de la loi sur la police (LPol) après sa révision totale en 2020, il a fallu procéder à une nouvelle révision de cet acte. Lors de la première procédure de corapport puis de la consultation publique qui a suivi, le Bureau a soulevé deux points critiques importants. Concernant la recherche automatisée de véhicules, c'est-à-dire l'enregistrement électronique de plaques d'immatriculation et la comparaison avec des banques de données policières, le projet de loi instaure la possibilité de conserver durant 100 jours les données n'ayant débouché sur aucune procédure (no hits) et de les utiliser pour des analyses ultérieures. Si, comme cela est prévu, 22 appareils d'enregistrement fixes sont achetés et installés à des emplacements à forte densité de circulation comme le Grauholz, où plus de 100 000 véhicules passent chaque jour, le canton accumulera un stock permanent de plusieurs centaines de millions de données, tout cela en vue d'établir des correspondances hypothétiques durant les 100 jours de conservation. La conservation massive de données de citoyennes et de citoyens intègres et le contrôle permanent auquel ceux-ci seraient soumis de ce fait pendant les 100 jours suivant l'enregistrement constitueraient, de l'avis du Bureau, un dangereux pas vers un État policier, démarche qu'il convient de qualifier de disproportionnée et donc d'inconstitutionnelle même avec une base légale. Le

fait que le projet de révision repose sur une proposition de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) n'y change rien.

La deuxième critique porte sur la collaboration entre les corps de police cantonaux. Le besoin légitime de renforcer cette collaboration et plus spécialement les échanges de données dans ce cadre est incontesté. La voie qui s'impose pour cela est celle d'un concordat qui définisse avec une précision suffisante les tâches à assumer conjointement ainsi que les entités qui en sont responsables. Le concordat peut également réglementer les données personnelles traitées et les accès à ces données, préciser quel est le droit de la protection des données applicable et indiquer la ou les autorités de surveillance compétentes. La CCDJP a donc lancé un projet d'élaboration de concordat, avec l'accompagnement technique de privatim (cf. ch. 6.6). Mais pour accélérer les échanges de données, la CCDJP invite les cantons à modifier leur loi sur la police de façon à pouvoir donner unilatéralement aux autres cantons un accès à leur système d'information policière. Le Bureau estime qu'une telle habilitation unilatérale serait inconstitutionnelle : lorsque l'article 28 de la Constitution cantonale exige que toute restriction d'un droit fondamental, en l'espèce le droit à l'autodétermination informationnelle, soit justifiée par un intérêt public prépondérant, il est clair qu'il doit s'agir de l'intérêt de la collectivité publique qui restreint le droit fondamental. C'est en effet la seule manière d'atteindre l'équilibre recherché entre les droits fondamentaux garantis par le canton et les tâches publiques du canton. Que l'accès à des données protégées par la Constitution bernoise permette à d'autres cantons de mieux accomplir les tâches légales qui leur ont été confiées par un autre législateur ne saurait constituer un intérêt public prépondérant. Pour pouvoir instaurer l'équilibre requis par la Constitution à l'intérieur d'un « espace juridique » intercantonal, il est indispensable que l'accès accordé aux données policières pour l'accomplissement des tâches communes soit réciproque. En outre, si les cantons peuvent accorder des accès unilatéralement, cela générera un tissu disparate de responsabilités, de solutions techniques et organisationnelles, de lois applicables et d'autorités de surveillance compétentes.

Ordonnances de Direction sur les droits d'accès aux fichiers centralisés de données personnelles délivrés par les Directions

Entrée en vigueur en mars 2021, la loi sur les fichiers centralisés de données personnelles (LFDP) et ses ordonnances d'exécution (O GERES et O GCP) permettent d'organiser simplement les droits d'accès des autorités cantonales aux banques de données visées. Les Directions, la CHA et la Direction de la magistrature peuvent définir elles-mêmes les profils de base et les profils standard dont ont besoin leurs unités d'organisation, mais avant d'édicter ou de modifier leur réglementation des droits d'accès, elles sont tenues de la soumettre au Bureau pour une prise de position formelle. Le Bureau vérifie si les différents

droits d'accès prévus reposent sur une base légale suffisante, si la nécessité d'accéder aux données en procédure d'appel est correctement motivée et si les droits d'accès accordés sont proportionnés. Ces réglementations étaient à édicter dans les douze mois suivant l'entrée en vigueur de la LFPD, soit jusqu'au 28 février 2022 au plus tard. Au cours de l'année sous revue, le Bureau a pris position sur plusieurs de ces réglementations, dans leur première version ou après modification. Il s'agit de celles de l'INC, de la DIJ, de la DSE, de la DEEE et de la Direction de la magistrature. Grâce à la qualité de la collaboration informelle qui a eu lieu durant l'élaboration de ces textes, les éventuelles divergences ont été éliminées en amont et le Bureau a pu rendre des avis formels brefs et approuver les réglementations avec un minimum de réserves.

Modification des trois ordonnances concernant le domaine universitaire

Les trois lois relatives à l'enseignement supérieur (loi sur l'Université, loi sur la Haute école spécialisée bernoise et loi sur la Haute école pédagogique germanophone) sont entrées en vigueur après révision le 1er mars 2022, accompagnées de leurs ordonnances d'exécution respectives également modifiées. Les trois ordonnances prévoient que les enseignantes et les enseignants doivent divulguer les mandats exercés dans des conseils d'administration ou des conseils de fondation et que ces informations doivent être publiées. À l'Université, cette règle s'applique à l'ensemble du corps professoral tandis que, dans les deux autres institutions, elle vaut seulement pour les membres du corps enseignant « ayant un degré d'occupation élevé ». Lors de la procédure de corapport, le Bureau a proposé que les rapports explicatifs précisent pour quelles raisons factuelles cette différence a été instaurée et à partir de quel taux un degré d'occupation est réputé élevé. Les explications demandées ont été intégralement fournies : les chaires professorales constituent généralement l'activité principale des titulaires tandis que les personnes qui enseignent dans les deux autres institutions universitaires exercent le plus souvent une activité professionnelle dans leur domaine, raison pour laquelle la publication des mandats est limitée aux enseignantes et enseignants ayant un taux d'occupation supérieur à 50 %.

Ordonnance sur l'administration numérique

L'ordonnance sur l'administration numérique (OAN) est le texte d'exécution de la nouvelle LAN. Ces deux actes entrent en vigueur le 1er mars 2023. Comme pour la LAN, le Bureau a pu apporter des idées importantes lors des travaux préparatoires effectués par le groupe ad hoc. Pour pouvoir utiliser de nouveaux outils numériques, il faut se conformer à des normes définies et respecter des processus. Lorsque des conditions déterminées sont réunies, les outils TIC doivent être soumis au contrôle préalable du Bureau avant leur utilisation. Le traitement des données de contact nécessaires pour les échanges sous forme numérique avec des particuliers, telles les adresses électroniques, les numéros

de téléphone fixe et mobile et les numéros d'identification, est expressément régi dans l'OAN. Il avait été envisagé d'imposer aux membres du personnel cantonal d'utiliser leur téléphone mobile privé à des fins de service, mais l'idée a été abandonnée faute de base légale dans la LAN. Du point de vue de la protection des données, il aurait été possible d'exiger la communication du numéro de téléphone mobile privé de la part de celles et ceux qui ont obtenu une participation à l'achat de leur appareil ou qui jouissent d'un abonnement gratuit ou à tarif réduit. Les principes et les exigences applicables aux échanges électroniques avec les autorités dans les procédures administratives seront réglés dans la LPJA.

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 par voie électronique de données 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 2022, le Bureau a traité 134 contrôles préalables concernant des projets informatiques (2021 : 138) et en a achevé 94 (2021 : 77), soit 68 % (2021 : 55,8 %). 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 défauts relevés) ; (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.

Nouvel ERP du canton de Berne

Le nouveau progiciel de gestion intégrée (*Enterprise Resource Planning*, ERP) adopté par le canton de Berne a remplacé, au 1er janvier 2023, les anciens systèmes d'information sur les finances (FIS) et sur le personnel (PERSISKA). En vue de cette étape de grande envergure, le Bureau a examiné la totalité de la documentation SIPD du nouvel ERP au cours d'un contrôle préalable réalisé en plusieurs fois. En complément, il a contrôlé la solution PANSYS, qui, durant une

période transitoire, sert à l'Office du personnel de système d'archivage pour certaines parties de PERSISKA. Le Bureau a demandé qu'une adaptation importante soit apportée aux droits d'accès à l'ERP : à l'heure actuelle, des membres du personnel travaillant dans le domaine des finances peuvent consulter des données d'autres offices de la même Direction dont ils n'ont pas besoin pour l'accomplissement de leurs tâches. Cette possibilité fait naître un risque élevé de contravention au droit de la protection des données et, le cas échant, au secret de fonction et à des obligations particulières de garder le secret. Les responsables du projet ont confirmé au Bureau que les droits d'accès concernés seraient limités par des moyens techniques dans les meilleurs délais. D'ici là, les Directions ont adressé aux collaboratrices et collaborateurs concernés une directive leur interdisant d'accéder aux données dont ils n'ont pas besoin pour l'accomplissement de leurs tâches. Les accès à l'ERP sont journalisés et des contrôles aléatoires sont pratiqués pour en vérifier la licéité.

Scannage centralisé des factures de créanciers de l'administration cantonale et du courrier adressé aux offices des poursuites et des faillites

L'OIO a soumis au Bureau pour contrôle préalable l'application de gestion des factures de créanciers (« Service Inputmanagement Kreditoren-Rechnungen ») de Swiss Post Solutions (SPS) SA. À l'avenir, l'ensemble des factures de créanciers, avoirs et rappels adressés au canton de Berne seront centralisés pour numérisation et traitement. Le service fourni par SPS inclut le raccordement de la plateforme de scannage de SPS au système de gestion des créanciers de l'ERP du canton de Berne (SAP VIM). SPS, qui appartenait à la Poste suisse, a été intégralement vendu et transféré à AS Equity Partners GmbH courant 2022. Les recommandations du Bureau concernaient notamment deux aspects : les fichiers stockés temporairement entre deux étapes de traitement doivent être cryptés ; les envois personnels, confidentiels ou secrets doivent être transmis à leurs destinataires respectifs par le fournisseur du service sans avoir été ouverts, c'est-à-dire sans traitement. Toute contravention à ces prescriptions est passible d'une peine conventionnelle.

Il est prévu d'utiliser les mêmes prestations techniques et organisationnelles de base pour centraliser progressivement les courriers envoyés aux offices des poursuites et des faillites et transmettre les documents numérisés aux applications spécialisées de ces offices (projet Digipost@DIJ-BAKA). La documentation SIPD afférente reposant en grande partie sur celle réunie pour la gestion des factures de créanciers, le Bureau a pu reprendre, lors de ce contrôle préalable, une partie des constatations qu'il avait déjà faites dans le premier dossier.

Il ressort de ces deux contrôles préalables que les processus peuvent se dérouler dans des conditions conformes au droit de la protection des données, mais qu'il faut établir, avant le transfert de l'exploitation du centre de calcul de La Poste à

celui de Swisscom (suite à la reprise de SPS SA), comment la protection des données et la sûreté de l'information sont assurées chez le nouveau fournisseur.

Copie des mandants de BE-GEVER

L'OIO a soumis au Bureau une extension du concept SIPD portant sur la gestion électronique des affaires de l'administration cantonale (BE-GEVER) prévoyant que toutes les données de tous les mandats des Directions et des offices seraient régulièrement copiées du système de production vers le système de test, où elles seraient disponibles à des fins d'essai et de formation. Pour le Bureau, cette démarche n'était ni licite, ni proportionnée. En effet, le traitement des données personnelles visées à des fins de test ou de formation ne correspond pas au but pour lequel ces données ont été recueillies à l'origine. Le principe de l'affectation à un but déterminé (art. 5, al. 4 LCPD) demande donc que ce nouveau but repose sur une base légale suffisante, qui régisse soit ledit traitement, soit une tâche dont l'accomplissement requiert ledit traitement. En admettant que l'on considère que la maintenance et le bon fonctionnement de BE-GEVER sont une tâche légale de l'administration cantonale, encore faut-il démontrer en quoi il est nécessaire d'utiliser des données réelles pour les tests et impossible de travailler sur des données fictives. Le simple fait que la préparation de cas appropriés pour effectuer des tests demande beaucoup de travail ne saurait en aucun cas justifier l'atteinte à un droit fondamental que constituerait le traitement de données personnelles à des fins non prévues. Dans des cas exceptionnels, il peut arriver que des essais doivent impérativement être réalisés avec des données réelles, notamment pour tester une interface avec un autre système dépourvu d'environnement de test. Mais même en pareil cas, le nombre de données utilisées doit rester proportionné, c'est-à-dire limité à ce qui est nécessaire, ce qui n'aurait pas été le cas dans le projet de copie intégrale présenté.

Le Bureau a modifié son appréciation lorsque le projet, à la demande des Archives de l'État, a été limité à une copie unique des données d'une sélection de quatre mandants. Cette démarche permettrait, dans le cadre d'un projet, de tester les fonctionnalités, les performances, la durée des transactions et l'applicabilité pratique du versement électronique aux Archives de l'État des données ayant une valeur archivistique puis de détruire ces données dans le système de test. Dans cette nouvelle configuration, le Bureau a jugé qu'il était effectivement impératif d'employer des données réelles car le processus de versement aux archives est irréversible et il doit donc être testé dans des conditions proches de la réalité afin d'éviter que des erreurs graves apparaissent seulement au stade de la mise en production, alors qu'elles ne peuvent plus être corrigées, ce qui causerait une perte de données irréversible. Des données fabriquées spécifiquement pour des tests ne peuvent pas refléter suffisamment l'hétérogénéité et la grille quantitative des données à traiter en production. La limitation à quatre mandants et la durée du projet ont paru proportionnées au Bureau.

Application spécialisée AssistMe

Le plan stratégique du canton de Berne en faveur de l'intégration des personnes handicapées entend renforcer la responsabilité individuelle des personnes adultes en situation de handicap et encourager leur participation sociale. C'est pourquoi il garantit le libre choix entre le recours à des prestations en institution (foyers, centres de jour, ateliers) et le recours à des prestations en ambulatoire (assistance, coaching sur le lieu de travail). Toute personne a droit aux prestations requises pour couvrir ses besoins individuels d'encadrement et de soins liés au handicap. Dans la pratique, cela signifie que les personnes concernées doivent s'adresser directement au canton pour obtenir sa participation aux coûts. Pour cela, il leur faut saisir dans un système de décompte les dépenses qu'elles ont encourues en lien avec leur handicap, d'une part, et les contributions financières qu'elles ont reçues de tous les financeurs de prestations (assurances sociales, caisses-maladie), d'autre part. Les décomptes sont vérifiés par le canton, qui paie le montant net correct. Une solution basée sur le Web est en cours de développement en vue de la réalisation du changement de système. Elle est appelée à remplacer le système de décompte actuel basé sur Excel.

Dans ce contexte, l'Office de l'intégration et de l'action sociale (OIAS) a remis au Bureau pour vérification la documentation SIPD de l'application AssistMe, qui avait subi un contrôle préalable en 2019 alors qu'elle portait le nom d'IBAS. L'application, qui est actuellement en phase de production pilote, doit être étendue et adaptée en vue de l'entrée en vigueur de la loi sur les prestations de soutien aux personnes en situation de handicap le 1er avril 2024. Le concept SIPD ayant été complété à la demande du Bureau sur des points importants (notamment le concept de test, la migration des données, la sûreté de l'authentification des utilisatrices et des utilisateurs et le raccordement au nouvel ERP), ce deuxième contrôle préalable a pu être clôturé.

Mise hors service de l'application spécialisée SORMAS

Dans le cadre de la gestion des contacts durant la pandémie de COVID-19, la DSSI a utilisé les applications spécialisées SORMAS (*Surveillance* and *Out-break Response Management System*) et TRACY pour traiter des données de santé rapportées à des personnes, c'est-à-dire des données personnelles particulièrement dignes de protection. Ces applications étaient donc assujetties au contrôle préalable du Bureau. La cessation de la gestion des contacts ayant été agendée au 1er avril 2022, le Bureau a clôturé le contrôle préalable bien qu'il n'ait jamais eu en sa possession de documentation SIPD complète jusqu'à cette date. À la place, il a analysé dans une procédure séparée la mise hors service de SORMAS, et plus spécialement l'effacement ou l'anonymisation de toutes les données de santé traitées avec cette application. Le Bureau a pu clôturer cet examen après trois échanges de courriers formels.

Application spécialisée Minddistrict

La clinique privée Wyss AG souhaite intégrer des interventions en ligne dans la psychothérapie ordinaire (« traitement mixte ») pour compléter la gamme de traitements usuels qu'elle propose. À cet effet, elle prévoit de mettre en place une solution standard basée sur le Web du nom de « Minddistrict E-Mental-Health-Plattform » (Minddistrict), une plateforme permettant de dispenser des soins psychiques. Elle s'est adressée bien en avance au Bureau pour planifier avec lui la réalisation du contrôle préalable en vue de vérifier la conformité de l'application avec les normes en matière de données personnelles particulièrement sensibles et de protection des données.

Concrètement, l'application Minddistrict est utilisée en appui du parcours de guérison individuel, depuis la prévention jusqu'au suivi post-traitement, grâce à différentes offres et fonctions. Elle permet en outre d'effectuer des interventions en ligne basées sur des données probantes ainsi que des consultations vidéo certifiées. La clinique Wyss n'utilise pas cette dernière possibilité. Les patientes et les patients peuvent par ailleurs tenir un journal sur l'application. Les dossiers médicaux ne sont toutefois pas gérés sur Minddistrict, mais exclusivement dans le système informatique de la clinique. Le Bureau a soulevé un point important : la durée de conservation de 15 ans lui est apparue excessive. Dans sa prise de position, la clinique a expliqué qu'il se produisait souvent des rechutes nécessitant une réadmission dans l'établissement, auquel cas il était très intéressant de pouvoir reprendre la précédente thérapie au stade où elle avait été arrêtée. Elle a précisé que, dès qu'un compte est désactivé, plus personne n'a accès aux données. Dans ces conditions, le Bureau a considéré que le délai de conservation était objectivement motivé.

Système d'information clinique EPIC KISS

L'application KISS du fournisseur américain de systèmes EPIC que le Groupe de l'Île prévoit de mettre en place est un nouveau système d'information clinique associé pour la première fois à une fonction de pilotage. Elle permettra de gérer une prise en charge interdisciplinaire de la patientèle en mettant à disposition, partout et en tout temps, l'ensemble des informations de santé d'une personne rassemblées dans un unique dossier. La saisie structurée et continue des données dans EPIC KISS permettra d'évaluer ces données et de garantir la qualité des thérapies ainsi que le respect des normes de sécurité dans le processus thérapeutique.

Lorsque le Bureau a été informé du projet d'introduction d'EPIC KISS, il a insisté auprès du Groupe de l'Île pour être impliqué dans la démarche. Le Groupe de l'Île s'est félicité que le Bureau accompagne le projet avant même le stade de l'élaboration de la documentation SIPD. Les institutions du groupe sont appelées à passer d'une gestion des dossiers médicaux par cas à une gestion

par patient. Il y a donc lieu de penser que la séparation des droits de consultation pour chaque traitement dispensé est appelée à s'assouplir. Le Bureau a donc fait savoir dès le départ au Groupe de l'Île que le système plus ouvert qu'il projette devrait comporter des dispositifs suffisants pour garantir que le principe de proportionnalité est toujours respecté. Avant que le groupe ne remette au Bureau la documentation SIPD pour contrôle préalable (ce qui devrait avoir lieu en 2023), le système fera l'objet d'une démonstration qui permettra de porter une première appréciation sur la réglementation des droits d'accès prévue pour l'application. En raison de l'interdépendance des systèmes, la conception de ces règles aura un impact sur l'application spécialisée Medical Content Plattform, le système de gestion des contenus du domaine de la santé. Cette solution sera utilisée pour mettre à la disposition du personnel médical une grande partie des contenus médicaux, c'est-à-dire concrètement des clichés, documents, signaux biologiques, fichiers audio et vidéo produits par des systèmes expert externes ou mis à disposition par des médecins traitants externes ou des institutions partenaires.

Application spécialisée eArchiv ARTS

Jusqu'ici, les Services psychiatriques universitaires (SPU) conservaient les dossiers médicaux sur papier ou sous forme numérique, voire les deux. Projetant de mettre en place l'application eArchiv ARTS, les SPU ont contacté le Bureau en amont pour lui demander un contrôle préalable garantissant la conformité avec les prescriptions en matière de protection des données. eArchiv ARTS est un système d'archivage documentaire numérique universel qui permet de conserver de manière ordonnée et conforme à la loi des données et des documents de la patientèle. Les constatations et les recommandations du Bureau étaient essentiellement de nature technique et visaient à assurer la sûreté des informations et des données. Grâce aux explications des SPU et aux rajouts dans la documentation SIPD, le Bureau a pu clore le contrôle préalable sans avoir constaté de défauts importants.

6.3.2. Vidéosurveillance

La LPol entièrement révisée est en vigueur depuis 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.

La loi du 23 janvier 2018 sur l'exécution judiciaire (LEJ) contient elle aussi des dispositions relatives à la vidéosurveillance, qui concernent les établissements d'exécution judiciaire et les véhicules de transport : la vidéosurveillance peut être utilisée pour l'accomplissement des tâches, notamment pour assurer la sécurité et l'ordre public, ainsi que pour protéger le personnel, les personnes détenues et les tiers dans les lieux surveillés. Ainsi, le recours à la vidéosurveillance sous une forme appropriée est considéré comme admissible même en l'absence de base légale explicite s'il est nécessaire pour remplir des tâches légales (p. ex. surveillance en temps réel en cas de placement dans la salle de réveil d'un hôpital après une intervention).

Centres de retour d'Aarwangen et de Champion

L'Office de la population (OPOP) est responsable de l'octroi de l'aide d'urgence aux requérantes et requérants d'asile déboutés. Il gère des centres de retour notamment à Aarwangen et à Champion, dont il a confié la direction à la société ORS Service AG (ORS).

Lorsque le contrôle préalable a été réalisé, le centre d'Aarwangen hébergeait surtout des familles avec des enfants en âge scolaire. Afin de protéger les résidentes et les résidents des personnes qui s'introduisent clandestinement dans les centres pour y passer la nuit et de pouvoir intervenir rapidement en cas de débordements parmi les résidentes et les résidents, l'OPOP avait l'intention d'assurer une surveillance en temps réel des entrées arrière et des corridors desservant les chambres et les appartements durant la nuit, le weekend et les jours fériés, c'est-à-dire lorsque le personnel d'ORS sur place est en effectif réduit. Lors du contrôle préalable, le Bureau a estimé que cette surveillance limitée dans le temps et sans enregistrement était proportionnée.

Le centre de retour de Champion est situé sur un vaste terrain comportant des bâtiments annexes et des entrées offrant peu de visibilité. Il est de ce fait difficile de limiter l'accès au site par des mesures de construction et de contrôler totalement les accès. Lors du contrôle préalable, les résidents étaient presque exclusivement des adultes, en grande majorité de jeunes hommes, dont certains présentaient des troubles psychiques graves. Selon l'OPOP, l'absence de perspectives combinée à la consommation et au deal d'alcool et de drogue créent un risque très élevé de violence physique à l'encontre du personnel et des résidents, y compris du fait de personnes extérieures sans autorisation d'accès, ainsi que d'autres infractions. L'office a donc souhaité procéder à une surveillance en temps réel, dans ce cas 24h sur 24, afin de réduire les délais d'intervention ; il prévoyait également d'enregistrer les images afin de pouvoir les fournir comme moyens de preuve à la POCA en cas d'infraction. L'OPOP ayant expliqué

qu'en l'absence de vidéosurveillance il faudrait engager plus de personnel de sécurité coûtant cher, le Bureau lui a répondu qu'une optimisation des coûts était un motif insuffisant pour porter atteinte à des droits fondamentaux. Il a donc demandé des informations sur l'effectif du personnel présent sur place ainsi qu'une liste des incidents des deux dernières années dans lesquels il aurait été important d'avoir une surveillance en temps réel ou des enregistrements vidéo. Sur la base de ces éléments et compte tenu des circonstances exposées ci-dessus ainsi que de la grande distance qui sépare le centre de retour du poste de police le plus proche, le Bureau a estimé que la vidéosurveillance projetée serait proportionnée. Il s'est cependant réservé le droit de suivre l'évolution des incidents et, si nécessaire, de modifier son appréciation de l'efficacité et de la proportionnalité des mesures prises.

Lors de la procédure de corapport ayant trait à la réponse du Conseil-exécutif à l'interpellation 103-2022 Junker Bernhard (« Vidéosurveillance dans les centres de retour »), le Bureau a obtenu que ses exigences concernant la documentation et le suivi du nombre d'incidents pour lesquels la vidéosurveillance aura été utile figurent dans la réponse du Conseil-exécutif au Grand Conseil.

Prisons et établissements d'exécution judiciaire

En 2010, le Bureau avait procédé à un contrôle très général de la vidéosurveillance dans l'ensemble des prisons régionales et des établissements d'exécution judiciaire du canton de Berne. Depuis lors, la LEJ est entrée en vigueur et les dispositifs de surveillance des établissements ont été partiellement renouvelés et développés pour suivre les progrès techniques.

Dans ce contexte, l'Office de l'exécution judiciaire (OEJ) a entrepris, en concertation avec le Bureau, de mettre à jour la documentation SIPD de chaque institution. Ces travaux ont démarré en 2020. Le Bureau s'est rendu dans la prison régionale de Thoune, dans l'établissement pénitentiaire de Hindelbank et dans le centre d'exécution de mesures de Saint-Jean pour se faire une idée de la situation et des besoins de ces institutions, d'une part, et pour expliquer les exigences à remplir pour qu'une vidéosurveillance soit conforme au droit, d'autre part. Suite à ces visites, le Bureau a évalué au cours de l'année sous revue les documentations SIPD des prisons régionales de Berne, Bienne, Berthoud et Thoune, des établissements d'exécution judiciaire de Hindelbank et de Saint-Jean, du Tribunal régional de Berne-Mittelland (dans les locaux provisoires de la Préfecture de Berne), de la Division cellulaire de l'hôpital de l'Île et du Domaine des transports de l'OEJ. L'office a accepté et appliqué les recommandations du Bureau concernant chacune des institutions, notamment la pixélisation des sanitaires dans les cellules de sécurité et de l'espace public hors des établissements. Le Bureau a donc pu confirmer que les dispositifs actuels de vidéosurveillance, ou plus précisément les plans établis pour ces dispositifs, étaient conformes au droit.

Vidéosurveillance à l'Hôpital de l'Île

À l'Hôpital de l'Île, le Bureau a eu deux installations de vidéosurveillance à évaluer, l'une pour la salle d'attente du service d'hématologie et l'autre pour les unités D et E de la clinique pédiatrique. Il s'agissait dans les deux cas de surveillance en temps réel de la patientèle pour des raisons de sécurité médicale, et non à des fins policières régies par les dispositions de la LPol. La question se posait de savoir dans quelle mesure les images vidéo retransmises sur des segments du réseau intérieur jugés sûrs par le Groupe de l'Île devaient ou non être soumis à un cryptage supplémentaire (le cryptage est impératif en cas de transport sur des réseaux publics). Le Bureau a recommandé de prévoir un cryptage supplémentaire à moyen terme, aspect sur lequel il reviendra lors de l'examen de l'ensemble de l'infrastructure vidéo de base.

6.4 Audits

Dans le cadre de son mandat légal de surveillance de l'application des prescriptions relatives à la protection des données et à la sûreté de l'information, le Bureau a mené 12 audits dans ce domaine, dont quatre en collaboration avec le CF. L'audit SIPD du système informatique central de la POCA (Rialto) a été reporté en raison du contrôle spécial auquel le CF prévoyait de soumettre ce système l'année d'après. La collaboration avec le CF se poursuit en 2023.

Conformément à la stratégie dont il s'est doté pour la période de 2019 à 2023, le Bureau a concentré ses contrôles sur des applications spécialisées centrales, des services TIC de base et le domaine de la santé en cherchant plus spécialement à évaluer les risques. Il a en outre assuré un suivi continu de la réalisation des actions correctives préconisées à l'issue de ses audits des années précédentes. C'est ainsi, notamment, que l'introduction de mesures permettant de contrôler les accès au système de gestion des dossiers des autorités de la protection de l'enfant et de l'adulte a pu être menée à bien.

Accompagner la mise en œuvre de mesures est une tâche normale du Bureau, gage d'efficacité et d'obtention des résultats souhaités. Elle implique notamment de procéder des contrôles a posteriori rigoureux afin de s'assurer que les services concernés ont effectivement remédié de manière vérifiable aux lacunes relevées. Or, le Bureau a bien été obligé de constater à maintes reprises au cours des années écoulées que les tâches dans le domaine SIPD n'obtenaient pas toute l'attention requise de la part des services responsables. 2022 ne fait pas exception : ces tâches ont souvent été exécutées « incidemment ». Le manque d'attention et les retards qui en découlent dans la mise en œuvre des améliorations préconisées augmentent le risque de ne pas

pouvoir faire face suffisamment vite aux dangers généraux posés par la cybercriminalité, dont le niveau d'activité est resté élevé au cours de l'année sous revue. Le temps qui s'écoule entre l'identification d'une déficience et son élimination effective est souvent trop long. Les services responsables doivent également contrôler périodiquement la résistance de leurs systèmes face aux risques de cybersécurité et, si nécessaire, procéder aux adaptations appropriées. Or, le respect vérifiable des prescriptions légales laisse toujours beaucoup à désirer. Par contre, le Bureau se félicite de constater qu'en 2022 les responsables ont plus souvent pris contact avec lui pour exposer leur situation et dialoguer en vue de définir des mesures d'amélioration.

Autodéclaration de la clinique Bethesda

La clinique Bethesda, qui est spécialisée dans le traitement des maladies neurologiques, se décrit comme une institution de pointe dans le domaine de la réadaptation neurologique. La prise en charge comporte principalement des traitements médicaux, des soins et des thérapies. La clinique Bethesda emploie plus de 300 personnes.

L'audit du Bureau avait pour but principal d'évaluer l'autodéclaration de la clinique concernant la sûreté de l'information et la protection des données. À cet effet, le Bureau a remis à l'institution trois listes de vérification reprenant les points de contrôle essentiels de la norme ISO/IEC 27001/2 (tâches SIPD déterminantes par domaine thématique), la première pour l'organisation TIC de la clinique, la deuxième pour les fournisseurs externes de services TIC (en visant un fournisseur clé) et la troisième pour l'application spécialisée centrale. Aux fins de son évaluation, le Bureau s'est intéressé en premier lieu aux risques SIPD et en second lieu à l'exhaustivité, à la traçabilité et à la vérifiabilité de la situation décrite dans la déclaration spontanée.

En résumé, le Bureau a eu l'impression que la clinique Bethesda avait déjà atteint un niveau acceptable dans le domaine de la protection des données et de la sûreté de l'information. Globalement, l'institution accorde aux tâches dans ce domaine une attention appropriée à la taille de son organisation et aux traitements de données qu'elle effectue. Il existe néanmoins un clair besoin d'amélioration et d'optimisation, dont la significativité a été jugée moyenne, mais aussi parfois élevée. La clinique Bethesda a reconnu les déficits existants et elle prévoit de concevoir et de mettre en œuvre des actions correctives. Le Bureau contrôlera ultérieurement les progrès accomplis et les résultats obtenus. La collaboration s'est déroulée dans une ambiance toujours cordiale et professionnelle.

Protection de base de la clinique privée Wyss AG

La clinique privée Wyss propose depuis 1845 des services ambulatoires, des séjours hospitaliers et un hôpital de jour pour les personnes atteintes de maladies psychiques. Elle emploie quelque 340 personnes au total, sur son site principal de Münchenbuchsee et sur ses sites de Berne et Bienne.

L'activité d'audit a porté essentiellement sur les exigences dans le domaine SIPD ainsi que sur la manière dont la protection de base des TIC répond à ces exigences. La protection de base englobe l'ensemble des procédures, mesures, organisations, processus, outils, infrastructures et systèmes techniques, données, dispositifs, etc., mis en place pour assurer la sécurité des processus opérationnels (traitement des données) et leur conformité avec les prescriptions en matière de protection des données.

L'audit a mis en évidence des lacunes dans tous les domaines contrôlés, avec un risque associé jugé élevé dans la majeure partie des cas. Cependant, le Bureau a également constaté que la clinique privée Wyss avait déjà pris des mesures radicales et bien ciblées pour améliorer la sûreté des informations et la protection des données. Le Bureau suivra activement la mise en œuvre de ses préconisations. L'audit s'est déroulé dans une ambiance conviviale et coopérative.

Protection de base de l'hôpital de Langenthal (SRO AG)

SRO AG est le centre hospitalier régional de Haute-Argovie. La société exploite, en plus de l'hôpital de Langenthal, des centres de santé et des logements protégés. Elle emploie environ 1100 personnes.

En 2019, le Bureau avait examiné la protection de base de l'infrastructure informatique de SRO AG. L'examen avait mis en évidence un important potentiel d'amélioration et d'optimisation dans tous les domaines, avec en particulier 28 remarques assorties de recommandations. L'audit de suivi réalisé par le Bureau en 2022 a consisté à apprécier la mise en œuvre des recommandations et le fonctionnement vérifiable des mesures dans le domaine SIPD.

L'audit de suivi a montré que dix recommandations pouvaient être considérées comme mises en œuvre alors que 13 recommandations ne l'étaient pas encore totalement. Dans le cas de cinq recommandations, la mise en œuvre n'a pas encore commencé. Le Bureau continuera de suivre avec attention les travaux d'amélioration restant à accomplir. L'audit de suivi s'est déroulé dans une atmosphère professionnelle et constructive.

Protection de base de l'hôpital régional de l'Emmental (RSE AG)

L'hôpital régional de l'Emmental fournit des prestations médicales sur deux sites, à Berthoud et à Langnau. Sa palette comprend les soins de base dans ses disciplines principales (chirurgie, médecine, gynécologie et obstétrique), complétés par une offre de spécialisations. L'institution est dotée d'environ 950 postes à temps plein, sans compter les personnes en formation. En 2021, elle a pris en charge quelque 10 500 cas. RSE AG possède une organisation TIC interne qui fournit les services importants dans ce domaine.
Lors de l'audit, le Bureau a vérifié la conformité de la protection de base TIC avec les normes applicables et les cadres de référence, comme les normes ISO/IEC 27001, 27701 ou les spécifications de l'office fédéral allemand pour la sécurité en matière de technologies de l'information (BSI), ainsi que les mesures mises en œuvre de manière vérifiable (processus, tâches, contrôles, infrastructure, organisation) afin de remplir les exigences dans le domaine SIPD. L'évaluation a porté sur les domaines suivants : gouvernance TIC, concepts SIPD, gestion des changements et du lancement des nouvelles versions, gestion des accès, sécurité des réseaux, sécurité des clients et des serveurs, externalisation et sécurité physique (des centres de calcul).

Au moment de la rédaction du présent rapport, le résultat consolidé de l'audit n'était pas encore établi. L'audit s'est déroulé en bonne intelligence, dans une ambiance conviviale.

Terminaux de la Police cantonale bernoise

La POCA prend les mesures appropriées, y compris en dispensant des informations et des conseils, pour assurer la sécurité et l'ordre public. Le corps de la POCA compte quelque 2700 personnes. L'institution dispose d'une organisation informatique interne, qui met des services TIC à disposition avec le concours de prestataires externes.

L'audit réalisé, qui comportait plusieurs volets, avait trait à la sécurité technique des terminaux de la POCA, également appelés « clients ». Une attention particulière a été vouée au client standard de la POCA fonctionnant avec le système d'exploitation Windows 10, dont la configuration a été examinée pour déterminer si les règles de bonnes pratiques en matière de sécurité étaient appliquées. Le concept SIPD pour les clients et pour l'infrastructure Windows a également été intégré dans l'évaluation. Le but était de comparer les risques et les mesures définis dans le concept (situation à atteindre) avec l'état des clients standard mis à disposition (situation effective) et de faire une analyse critique des points pertinents pour la sécurité. En outre, le trafic réseau du client a été analysé. Un test d'intrusion a été réalisé sur un client physique et sur un poste de travail virtuel dans le but premier de déterminer s'il était possible d'identifier et d'exploiter des points faibles pour étendre les droits d'accès.

L'environnement soumis au test d'intrusion a obtenu une note moyenne. Les résultats montrent qu'il n'était pas configuré conformément aux règles de bonnes pratiques actuelles, avec beaucoup de configurations peu sûres et de lacunes de sécurité. Un grand nombre de risques de sécurité ont en outre été identifiés sur le client Windows physique, dont certains présentaient une significativité élevée. La POCA a immédiatement étudié et engagé des actions correctives. Le Bureau suivra avec attention la mise en œuvre de ces mesures. L'audit s'est déroulé dans un esprit de professionnalisme et de convivialité.

Application spécialisée NFAM

La nouvelle application spécialisée NFAM met à disposition des fonctions pour gérer les cas et les dossiers de bout en bout de manière uniforme, toutes Directions confondues, dans le domaine de l'intégration et pour tous les autres processus du canton relevant du droit des étrangers. Les questions ayant trait à l'aide sociale dans le domaine de l'asile et des réfugiés sont du ressort de la DSSI, la mise en œuvre opérationnelle étant assurée par des partenaires régionaux de la Direction. Au sein de la DSSI, c'est l'OIAS qui est en charge de l'aide sociale, de l'insertion des personnes réfugiées, requérantes d'asile ou en situation de handicap ainsi que de l'animation de jeunesse et de l'accueil extrafamilial des enfants. Cet office a la responsabilité globale du processus d'asile. La DSE et le service des migrations de l'OPOP assument toutes les tâches en lien avec l'entrée, le séjour et le travail des étrangères et des étrangers qui relèvent de leur compétence.

L'audit a porté principalement sur la mise en œuvre des mesures dans le domaine SIPD, le fonctionnement sous l'angle de la gouvernance SIPD, les concepts SIPD, la gestion des droits d'accès, la conservation des données, les interfaces ainsi que les services externes et l'externalisation.

Des problèmes ont été détectés dans l'ensemble des domaines audités. Ainsi, des mesures préconisées par le Bureau lors du contrôle préalable (art. 17a LCPD) n'ont pas été réalisées de façon vérifiable. L'orientation stratégique et le pilotage opérationnel dans le domaine SIPD n'étaient pas assez clairement perceptibles. Les activités de contrôle imposées par la réglementation n'étaient pas accomplies comme elles auraient dû l'être. La documentation SIPD (concept) et l'analyse des risques n'étaient pas à jour. La programmation du logiciel n'intégrait pas suffisamment les principes de la prise en compte de la sécurité dès le stade de la conception (*Security by Design*) et d'un paramétrage par défaut favorable au respect de la vie privée (*Privacy by Default*). Un besoin d'optimisation est apparu dans la gestion des droits d'accès. Les données traitées dans les systèmes de test étaient des données de production. Le Bureau a estimé que les manquements constatés et les risques qui en découlaient revêtaient une importance majeure. L'audit, qui a été effectué en étroite collaboration avec le CF, s'est révélé difficile en raison de la complexité du contexte.

Application spécialisée NESKO

Le canton de Berne comptabilise chaque année 6 milliards de francs de recettes fiscales. Les données fiscales sont traitées avec le système informatique NESKO de l'ICI. L'application spécialisée utilisée pour la taxation des personnes physiques, NESKO VA-NP, est l'un des systèmes informatiques clés de l'ICI. En exploitation depuis de nombreuses années, elle est considérée comme robuste. Il est crucial qu'elle soit conforme aux prescriptions en matière de sûreté de l'information et de protection des données, d'où l'importance de l'analyse SIPD ainsi que de la conception et de la réalisation de mesures efficaces dans ce domaine afin de pouvoir faire face de manière appropriée à des risques comme les accès non autorisés ou les pertes de données.

L'audit a porté principalement sur la réalisation, le fonctionnement et la conception des mesures dans le domaine SIPD, la gestion des droits d'accès, la conservation des données, les interfaces ainsi que les services externes et l'externalisation, en prenant en considération la gouvernance en matière de SIPD.

L'audit a constaté notamment des lacunes dans la gouvernance SIPD. Il n'y a pas de stratégie rigoureuse dans ce domaine et la définition des compétences (propriété des données) n'est pas rationnelle. Le rôle clé de responsable de la sécurité ne dispose pas des ressources suffisantes pour assumer les tâches qui lui sont attribuées. Il faudrait en outre élaborer un concept SIPD pour l'application spécialisée VA-NP et pour chacune des autres applications spécialisées importantes de NESKO et résoudre le problème de l'insuffisance de la gestion des droits d'accès. Le développement des logiciels a clairement besoin d'être optimisé en vue de prendre en compte de manière vérifiable les principes de la sécurité dès le stade de la conception et d'un paramétrage par défaut favorable au respect de la vie privée. Réalisé en étroite collaboration avec le CF, l'audit s'est déroulé dans une ambiance de professionnalisme et d'écoute mutuelle.

Application spécialisée GELAN

Le système complet d'information agricole GELAN est en service dans les cantons de Berne, Fribourg et Soleure. Il a été développé en permanence et comporte désormais 15 extensions totalement intégrées. Les données relatives aux surfaces sont saisies dans un système d'information géographique. GELAN sert à gérer les paiements directs ainsi que l'exécution dans les domaines suivants notamment : améliorations structurelles, projets d'utilisation durable des ressources, protection de la nature, protection animale, législation sur les épizooties, protection des eaux et contrôles. L'application spécialisée GELAN est utilisée au total par plus de 30 000 exploitantes et exploitants agricoles et par quelque 500 agentes et agents des trois administrations cantonales pour assurer l'exécution de la législation sur l'agriculture. Chaque

année, des subventions avoisinant le milliard de francs sont gérées sur GELAN. Une refonte du système, en service depuis 1999, est prévue ces prochaines années.

L'audit a porté principalement sur la gouvernance SIPD, la réalisation et le fonctionnement des mesures demandées par le concept SIPD, le contrôle de l'application vérifiable de la conception définie (situation à atteindre) par rapport à la situation effective en matière de SIPD, la gestion des droits d'accès à GELAN, la conservation des données, les interfaces ainsi que les prestations externes et l'externalisation.

Des possibilités d'amélioration ont été constatées dans l'ensemble des domaines audités, notamment dans le pilotage de la sûreté de l'information et de la protection des données (documentation manquante ou lacunaire, p. ex. stratégie SIPD, gestion des risques, etc.). Par ailleurs, l'architecture du système n'était documentée qu'incomplètement. Sur le plan opérationnel, les droits d'accès des administrateurs étaient très étendus et les exigences en matière de SIPD étaient lacunaires et peu précises en ce qui concerne le développement et le test des logiciels de GELAN. L'audit s'est déroulé en étroite collaboration avec le CF, dans une ambiance conviviale et réceptive.

Service de base BE-Web

L'OIO est le centre de compétences du canton de Berne pour les TIC et la transformation numérique. Le service BE-Web, qui met à la disposition de l'administration cantonale un système de gestion des contenus de ses sites Internet dont l'accès est public, a été mis en place fin 2021 dans le cadre d'un projet. La gestion de la plateforme technique est assurée par la Bedag. Les services d'intégration et de mise en œuvre ainsi que l'exploitation technique de la plateforme sont externalisés. En outre, l'OIO utilise des services externes sur le cloud pour l'analyse et l'amélioration des pages Internet, pour l'exécution de fonctions de recherche et pour la représentation d'images intégrées.
Dans le cadre de BE-Web, l'office fournit aux Directions l'infrastructure technique de base et un mandant technique leur permettant de gérer leurs sites Internet dédiés sous leur propre responsabilité.

L'audit a porté principalement sur le respect des prescriptions relatives à la protection de base TIC et des exigences applicables lorsqu'un niveau de protection supérieur est requis selon les normes et les cadres de référence, comme les normes ISO/IEC 27001, 27701 ou les spécifications du BSI. Le Bureau a en outre évalué les mesures mises en œuvre pour assurer le pilotage SIPD requis, les tâches et les processus dans le domaine SIPD, l'infrastructure technique de base et l'organisation de ce domaine.

Des défauts présentant un risque élevé à moyen pour la sûreté de l'information et la protection des données ont été observés dans de nombreux domaines. Ainsi, la responsabilité et le pilotage du domaine SIPD manquaient de clarté et la mise en production ordinaire de l'application n'avait pas été accomplie selon des modalités vérifiables. De plus, des tâches SIPD définies dans le projet n'avaient pas été effectuées (p. ex. un test de sécurité de grande ampleur avant la mise en service). Des documents fondamentaux, comme l'analyse du niveau de protection requis et des risques, le concept SIPD, le concept des droits d'accès définissant les principes à respecter ainsi que les mesures SIPD, étaient incomplets et n'étaient pas à jour. L'intégration de la plateforme d'exploitation productive BE-Web dans le réseau présentait en outre des défauts techniques. L'audit s'est déroulé en bonne intelligence.

Service de base BE-Plateformes d'applications

Le service BE-Plateformes d'applications (APF) de l'OIO consiste à offrir aux Directions une plateforme centrale standardisée servant de base technique aux applications spécialisées et aux applications de groupe. Cette forme de service TIC est généralement appelée « Platform as a Service » (PaaS). Il s'agit d'une forme d'informatique en nuage dans laquelle la plateforme technique supportant les applications est mise à disposition par un prestataire externe. Dans le cadre d'un projet, le canton de Berne a migré plus de 200 applications spécialisées des systèmes informatiques décentralisés des Directions vers la plateforme centralisée APF.

L'audit a porté sur le respect des prescriptions relatives à la protection de base TIC et des exigences applicables lorsqu'un niveau de protection supérieur est requis selon les normes et les cadres de référence, comme les normes ISO/IEC 27001, 27701 ou les spécifications du BSI, les mesures SIPD implémentées dans les tâches et les processus essentiels, l'exploitation de la plateforme APF, l'infrastructure TIC, les contrats de prestations et les organisations responsables en interne et à l'extérieur.

Il est ressorti de l'audit avant tout que l'exécution de tâches convenues contractuellement était insuffisamment contrôlée. Ainsi, le Bureau a constaté que les prescriptions SIPD n'avaient pas été respectées lors de la migration des applications spécialisées et que la mise en œuvre n'avait pas été contrôlée. Des documents SIPD nécessaires manquaient ou n'étaient pas consultables de manière transparente. En outre, la société qui exploite la plateforme APF n'avait pas été avisée d'exigences spécifiques dans le domaine SIPD pour les applications spécialisées. Or, l'absence de vue d'ensemble des exigences SIPD peut avoir un impact négatif sur la plateforme APF. L'audit s'est déroulé dans une atmosphère de professionnalisme et de coopération.

Application de groupe SAP/ERP

Le canton de Berne a mis en place le progiciel de gestion SAP/ERP au 1er janvier 2023, en remplacement des applications de groupe FIS (finances et comptabilité) et PERSISKA (gestion du personnel et comptabilité des traitements). La phase de réalisation a démarré en 2020, suivie de la phase d'introduction à l'automne 2021. La décision de déploiement a été prise en décembre 2022. SAP est un ERP proposant des solutions logicielles pour gérer les processus spécifiques des entreprises de taille moyenne. Il s'agit d'un progiciel complexe couvrant l'ensemble des processus de gestion. SAP est l'abréviation de « systèmes, applications et produits pour le traitement des données ».

Lorsque l'audit a été réalisé, le système SAP/ERP n'avait pas encore été mis en production. Des contrôles limités ont cependant pu être pratiqués sur la gouvernance et la conception en matière de SIPD, la gestion des droits d'accès, la conservation des données, les interfaces ainsi que les prestations externes et l'externalisation.

L'audit a montré que des aspects fondamentaux de la sûreté de l'information et de la protection des données, comme une gouvernance SIPD obligatoire et coordonnée comprenant une gestion des risques et de la sécurité avec des concepts afférents, n'étaient pas encore totalement aboutis ou étaient restés largement en suspens. De plus, la définition de la gestion des droits d'accès était encore embryonnaire. L'audit s'est déroulé dans un climat de coopération et de convivialité.

Système d'information Schengen de la Police cantonale bernoise

En reprenant l'acquis de Schengen, la Suisse s'est engagée à garantir qu'une autorité indépendante surveille la licéité du traitement des données personnelles du Système d'information Schengen (SIS) sur son territoire et de la transmission de ces données à l'extérieur de son territoire. Les autorités cantonales en charge de la protection des données sont ainsi tenues de vérifier périodiquement la licéité du traitement des données personnelles du SIS.

Au cours de l'année sous revue, le Bureau a contrôlé les accès au SIS des agentes et des agents de la police régionale Mittelland – Emmental – Haute-Argovie. L'audit avait pour but d'évaluer l'utilisation du SIS sur la base de la journalisation des accès par le système ainsi que la sensibilisation des agentes et des agents concernés à la protection des données.

Le Bureau a recommandé des optimisations en ce qui concerne l'utilisation du SIS et les résultats de recherche : le personnel a besoin d'être formé ou informé régulièrement pour se familiariser avec les prescriptions du droit de la protection des données à respecter lors du traitement de données person-

nelles issues de recherches sur le SIS, pour approfondir ses connaissances et pour renforcer sa sensibilité au respect de la protection des données dans l'utilisation du SIS. Il est important que les nouveaux membres du personnel soient formés à l'utilisation du SIS rapidement et de manière appropriée. L'audit s'est déroulé dans une ambiance de convivialité et de serviabilité.

6.5 Autres instruments relevant du droit de la surveillance

6.5.1. 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 2022, le Bureau n'a pas présenté de proposition formelle et n'a pas formé de recours contre une décision négative d'une autorité responsable.

6.5.2. Haute surveillance des autorités communales et paroissiales de surveillance de la protection des données

La loi sur la protection des données en vigueur prévoit que les communes et les autres collectivités de droit communal ainsi que les Églises nationales et leurs entités régionales désignent pour leur domaine leur propre autorité de surveillance (art. 33 LCPD). Le Bureau exerce la haute surveillance et il est l'interlocuteur des services de surveillance de la protection des données des collectivités de droit communal (art. 15, al. 3 OPD).

Les communes ont choisi des solutions variées pour garantir l'indépendance requise par la loi. Beaucoup de petites et moyennes communes ont désigné leur

organe de révision des comptes comme autorité de surveillance. Dans les communes dotées d'un parlement, c'est souvent la commission de gestion qui assume cette fonction. Certaines communes ont mandaté une étude d'avocats spécialisée. La ville de Berne est la seule qui ait son propre bureau de surveillance de la protection des données.

Il en découle que les connaissances des organes de surveillance communaux en matière de sûreté de l'information et de protection des données ainsi que le champ et la qualité des conseils qu'ils peuvent dispenser à leurs autorités communales sont hétérogènes. C'est pourquoi le Bureau a de nouveau reçu durant l'année sous revue un grand nombre de questions ayant trait à des affaires communales, que ce soit directement de la part d'autorités communales (dont certaines ne savaient pas qu'elles avaient leur propre organe de surveillance) ou bien de la part d'organes de surveillance communaux (ou de personnes auxquelles ces organes avaient conseillé de s'adresser au Bureau). Certains sujets étaient récurrents, comme les exigences SIPD en cas d'introduction de M365, l'édiction de règlements communaux régissant la protection des données ou les droits d'accès à la plateforme GERES du canton ou encore la vidéosurveillance dans l'espace public et dans les institutions publiques.

Dans le cadre de la révision en cours de la LCPD, un projet de nouvelle réglementation sera soumis à la discussion. Ce projet a été élaboré par un groupe de travail informel auquel participent l'OACOT, l'Association des communes bernoises, des représentantes et des représentants de communes de tailles variées et les préfectures. Selon ce projet, le conseil en matière de protection des données et la surveillance dans ce domaine seraient délégués au Bureau, y compris dans les affaires communales, et seules les quatre plus grandes communes bernoises auraient leur propre autorité de surveillance de la protection des données.

6.6 Coopération intercantonale

Présidence et comité de privatim

Le délégué à la protection des données préside privatim, la Conférence des préposé(e)s suisses à la protection des données, depuis novembre 2020.
La conférence a tenu deux assemblées générales durant l'année sous revue. Elle a pu organiser au printemps la cérémonie pour le vingtième anniversaire de sa création qui avait dû être annulée en 2020 en raison de la pandémie.
Le bureau de privatim et son comité ont rédigé les réponses de la conférence à neuf consultations de la Confédération ainsi que, pour certaines de ces consultations, des modèles de réponse à l'intention des membres. Privatim a

échangé avec le PFPDT sur des questions de compétence en matière de surveillance de la protection des données lorsque des autorités cantonales et communales ainsi que des organisations publiques et privées agissant à la fois dans des domaines relevant de la puissance publique et dans des domaines relevant du droit privé confient des traitements de données à des prestataires privés. La conférence a soutenu l'organisation Administration numérique suisse pour négocier de meilleures règles de protection des données à l'occasion du renouvellement du contrat-cadre de la CSI avec Microsoft pour l'utilisation de services de cloud par des organes publics. Elle a réalisé la revue technique d'un premier projet de concordat intercantonal de coopération et d'échange de données préparé par la Conférence des commandantes et des commandants des polices cantonales de Suisse (CCPCS). Elle est intervenue pour que eOperations Suisse SA remplisse correctement son obligation d'informer les personnes souhaitant déménager au sujet du service eDéménagement. Privatim a des échanges institutionnalisés avec l'agence Educa, qui est mandatée par la Conférence des directrices et directeurs cantonaux de l'instruction publique pour mener plusieurs projets dans le domaine de l'éducation concernant notamment la protection des données.

Pour faciliter le travail des membres intéressés de privatim, le Bureau les a informés sur les constatations pertinentes pour eux réalisées lors du contrôle préalable du logiciel mis à disposition par la Confédération pour tenir les registres cantonaux des tumeurs. Dans d'autres cas, c'est le Bureau qui a pu profiter des travaux préliminaires accomplis par d'autres organes de surveillance.

Groupes de travail de privatim

*Le groupe de travail Cyberadministratio*n et un sous-groupe ad hoc ont proposé un premier séminaire sur le thème « Notification des failles dans la protection des données », qui a joui d'une bonne participation. Il a porté sur la criticité et les risques, les mesures, l'information des services concernés et la procédure de notification. Les enseignements instructifs pour la pratique dans les cantons apportés par ce séminaire servent de base à un remaniement et à une mise à jour des documents d'aide destinés aux cantons.

Le *groupe de travail Sécurité* s'est réuni à deux reprises pour travailler sur des questions communes relatives à la surveillance policière au moyen de dispositifs techniques, aux échanges intercantonaux de données dans le domaine de la police et à d'autres aspects de la protection des données dans le domaine de justice et police. À la demande de la CCPCS, il a évalué le projet de concordat sur l'échange de données à deux reprises, dans un cas pour préparer la prise de position formelle de privatim et dans l'autre pour donner un retour informel sur le projet.

Le *groupe de travail Santé* s'est réuni à quatre reprises au cours de l'année sous revue, alternativement à distance et en présentiel. Composé de spécialistes de la

protection des données dans le secteur de la santé, il s'est de nouveau concentré sur des problématiques post-pandémie importantes, comme la conservation et l'effacement des coordonnées ou les enseignements à tirer en vue d'une révision de la LEp. La discussion au sujet du dossier électronique du patient (DEP) a pris de l'ampleur : les membres du groupe de travail se sont interrogés par exemple sur ce qu'il doit advenir du DEP d'un enfant lorsque celui-ci devient majeur, c'est-à-dire légalement capable de discernement. Le DEP restera un sujet de discussion en 2023.

Au sein *du groupe de travail TIC*, des représentantes et des représentants 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.

7 Proposition

Prise de connaissance.

8 Glossar / Abkürzungen

Al.	Alinéa
AP	Avant-projet
APF	Plateforme d'applications
Art.	Article
AVS	Assurance-vieillesse et survivants
BE-GEVER	Gestion électronique des affaires (de l'administration cantonale)
BSI	Office fédéral allemand pour la sécurité en matière de technologies de l'information
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des commandantes et des commandants des polices cantonales de Suisse
CF	Contrôle des finances
Ch.	Chiffre
CHA	Chancellerie d'État
CSI	Conférence suisse sur l'informatique
DEEE	Direction de l'économie, de l'énergie et de l'environnement
DEP	Dossier électronique du patient
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
ERP	*Enterprise Resource Planning*
FIN	Direction des finances
GELAN	Système complet d'information agricole
GERES	Plateforme des systèmes des registres communaux

ICI	Intendance cantonale des impôts
INC	Direction de l'instruction publique et de la culture
ISO/IEC	Organisation internationale de normalisation /Commission électrotechnique internationale
LAN	Loi sur l'administration numérique
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LCPD	Loi cantonale sur la protection des données
LEJ	Loi sur l'exécution judiciaire
LEp	Loi fédérale sur la lutte contre les maladies transmissibles de l'homme (loi sur les épidémies)
LFDP	Loi sur les fichiers centralisés de données personnelles
LIAM	Loi sur l'information et l'aide aux médias
lit.	Lettre
LPD	Loi fédérale sur la protection des données
LPers	Loi sur le personnel
LPJA	Loi sur la procédure et la juridiction administratives
LPol	Loi sur la police
LSIC	Loi sur la sécurité de l'information et la cybersécurité
M365	Microsoft 365
OAC	Office de l'assurance-chômage
OACOT	Office des affaires communales et de l'organisation du territoire
OAN	Ordonnance sur l'administration numérique
ODSC	Ordonnance sur les données secondaires de communication
OECO	Office de l'école obligatoire et du conseil
OEJ	Office de l'exécution judiciaire

O GCP	Ordonnance sur le système de gestion centrale des personnes
OCRN	Office de la circulation routière et de la navigation
O GERES	Ordonnance sur la plateforme des systèmes des registres communaux
OIAS	Office de l'intégration et de l'action sociale
OIO	Office d'informatique et d'organisation
OPD	Ordonnance sur la protection des données
OPOP	Office de la population
ORP	Office régional de placement
ORS	ORS Service AG
PaaS	*Platform as a Service*
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
SIS	Système d'information Schengen
SORMAS	*Surveillance and Out-break Response Management System*
SPS	Swiss Post Solutions
SPU	Services psychiatriques universitaires de Berne
SRO	Spital Region Oberaargau (hôpital régional de Haute-Argovie)
TIC	Technologies de l'information et de la communication
UE	Union européenne

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