Kanton Bern
Canton de Berne

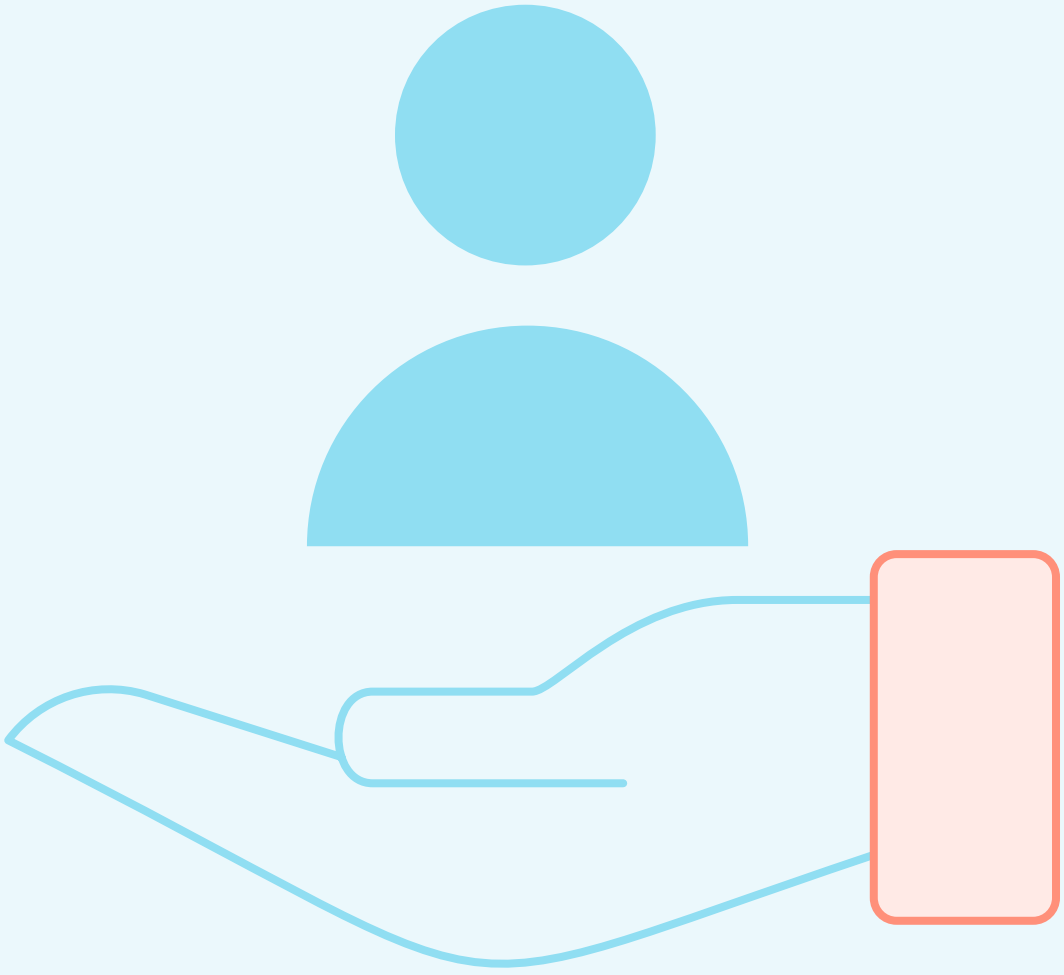
Rapport d'activité Bureau pour la surveillance de la protection des données 2021

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

Il est dans la nature et dans la vocation du droit de la protection des données de trouver comment faire naître, au moyen de règles conformes aux principes de l'État de droit, un juste équilibre entre les droits fondamentaux des individus (protection de la sphère privée) et l'accomplissement des tâches publiques. Peu importe que les intérêts publics dans la balance résultent d'une évolution générale, telle que la transformation numérique de l'administration, ou d'une situation particulière, dans le domaine de la santé par exemple. Même en temps de pandémie, l'accomplissement des tâches publiques et la protection de la sphère privée sont deux pôles qui ne s'excluent pas, mais qu'il importe au contraire de concilier au mieux en fonction de la matière. Le rôle du droit de la protection des données est précisément d'apprécier dans quelle mesure la protection de la santé peut nécessiter d'empiéter sur la sphère privée, pour autant que les droits garantis constitutionnellement soient respectés.

Mais si la pandémie en cours pose des défis particuliers dans le domaine de la protection des données, c'est pour d'autres raisons que la polarité habituelle entre intérêts privés et intérêts publics. En effet, l'exigence fondamentale que tout traitement de données repose sur une base légale suffisante est en soi une source de difficulté lorsque les bases légales changent en permanence, souvent par une procédure législative accélérée, lorsque la Confédération et les cantons ont des compétences normatives en partie parallèles et lorsqu'il faut de surcroît déterminer si les compétences déléguées par le législateur au gouvernement permettent ou non au second d'édicter par voie d'ordonnance des normes à durée limitée qui, en temps « normal », devraient être inscrites dans une loi au sens formel pour être conformes aux principes de l'État de droit. De même, l'appréciation de la proportionnalité est d'autant plus délicate que l'intensité de la menace est controversée au sein de la société, que les informations dont on dispose évoluent en permanence et que les traitements de données concrets sont conçus non pas comme des mesures autonomes, mais comme des éléments d'un dispositif plus vaste (p. ex. la création d'une base de données centralisée des coordonnées).

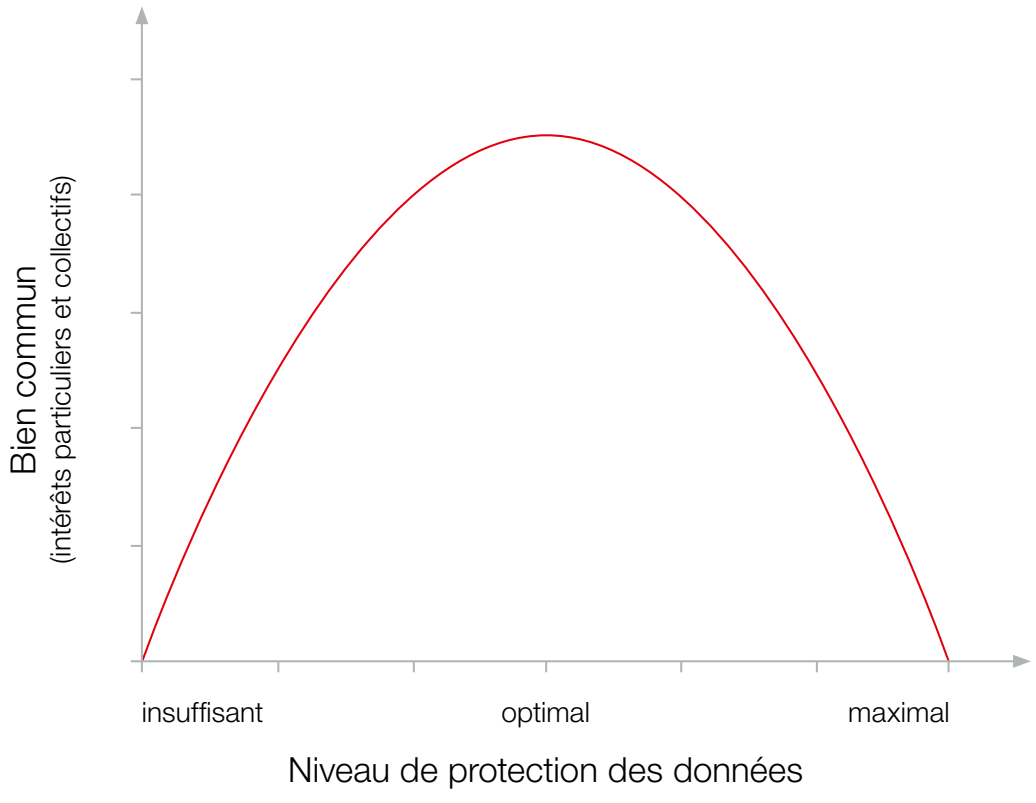
Dans ce contexte, le présent rapport consacre un chapitre à une sélection de dossiers en lien avec la pandémie (ch. 6.1). Cette année encore, les échanges soutenus entre les autorités cantonales responsables de la protection des données et avec le préposé fédéral à la protection des données et à la transparence ont été très utiles pour coordonner la réponse aux défis de taille posés dans le domaine de la protection des données, et pas seulement par la pandémie (ch. 6.7).

Ueli Buri, délégué à la protection des données

2 Droit fondamental à la protection des données

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

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



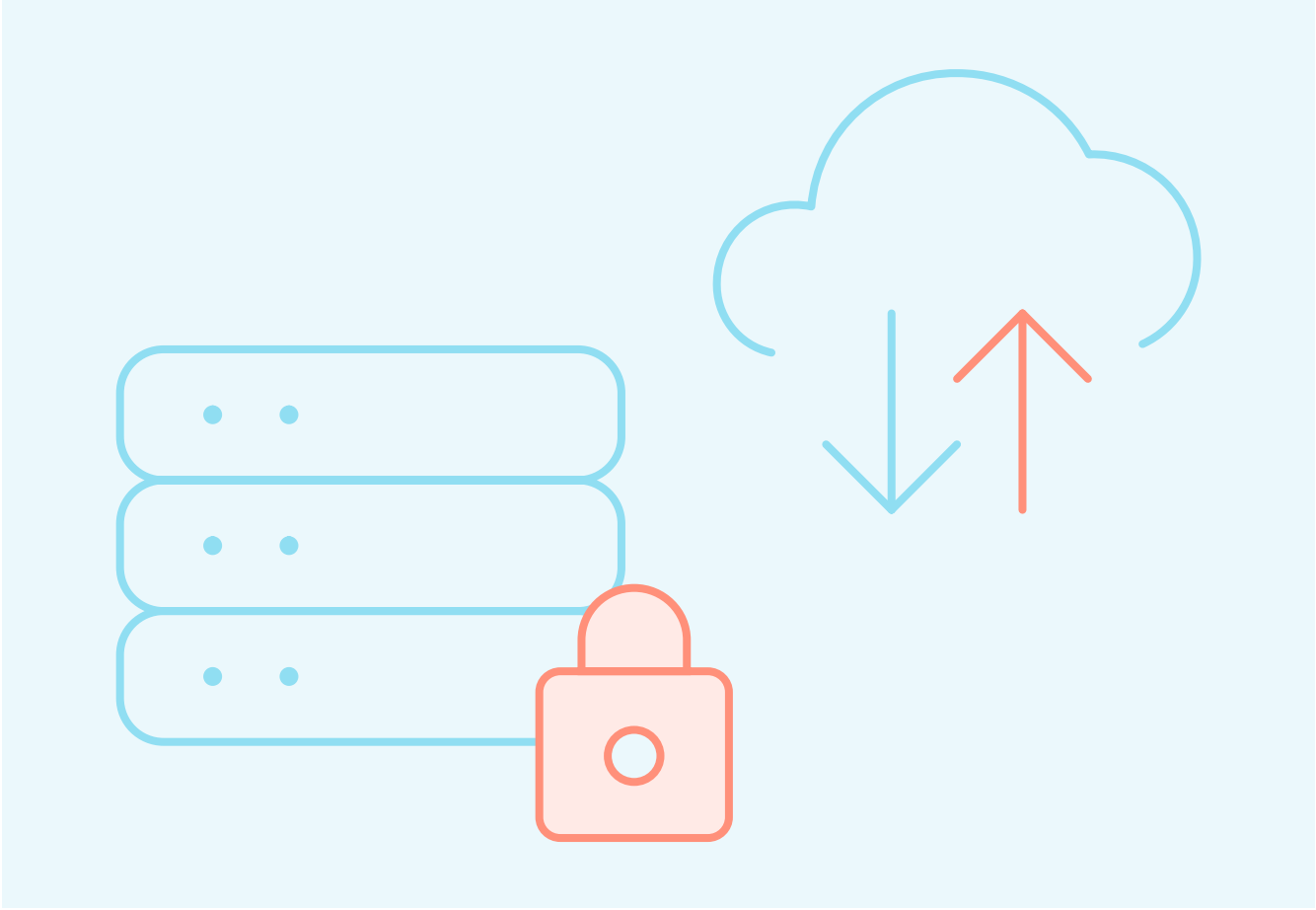
La loi cantonale sur la protection des données (LCPD) précise les devoirs des autorités lors du traitement des données personnelles. Par autorité, il faut comprendre l'administration, mais aussi d'autres entités chargées de tâches publiques comme les écoles et les hôpitaux. Quant au traitement, il se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

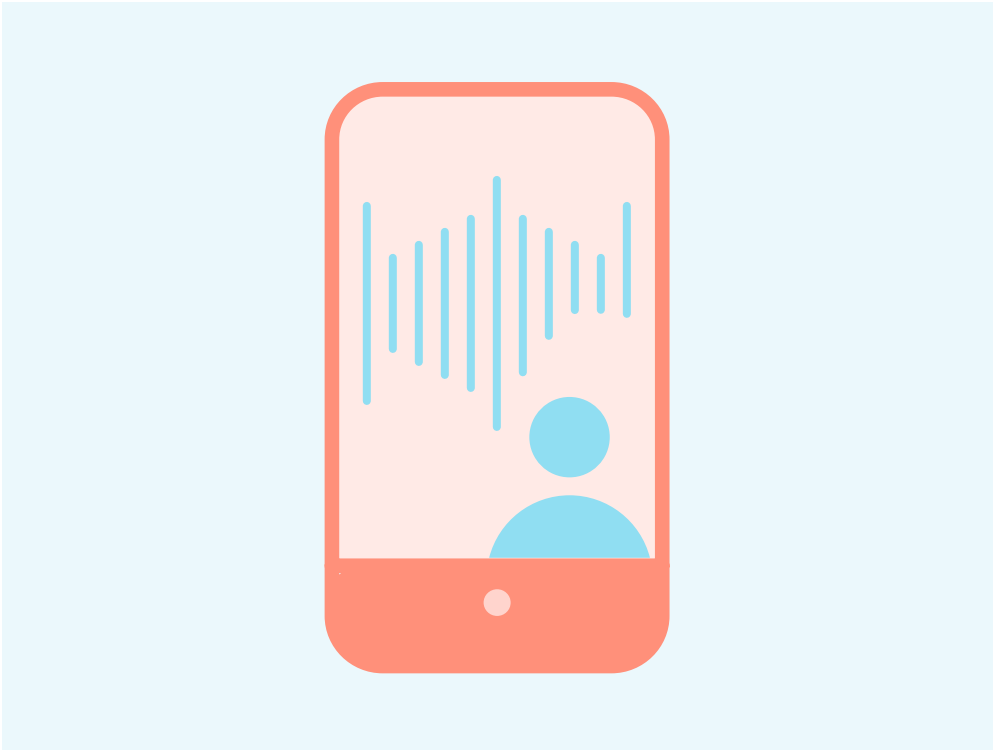
3 Responsabilité et surveillance

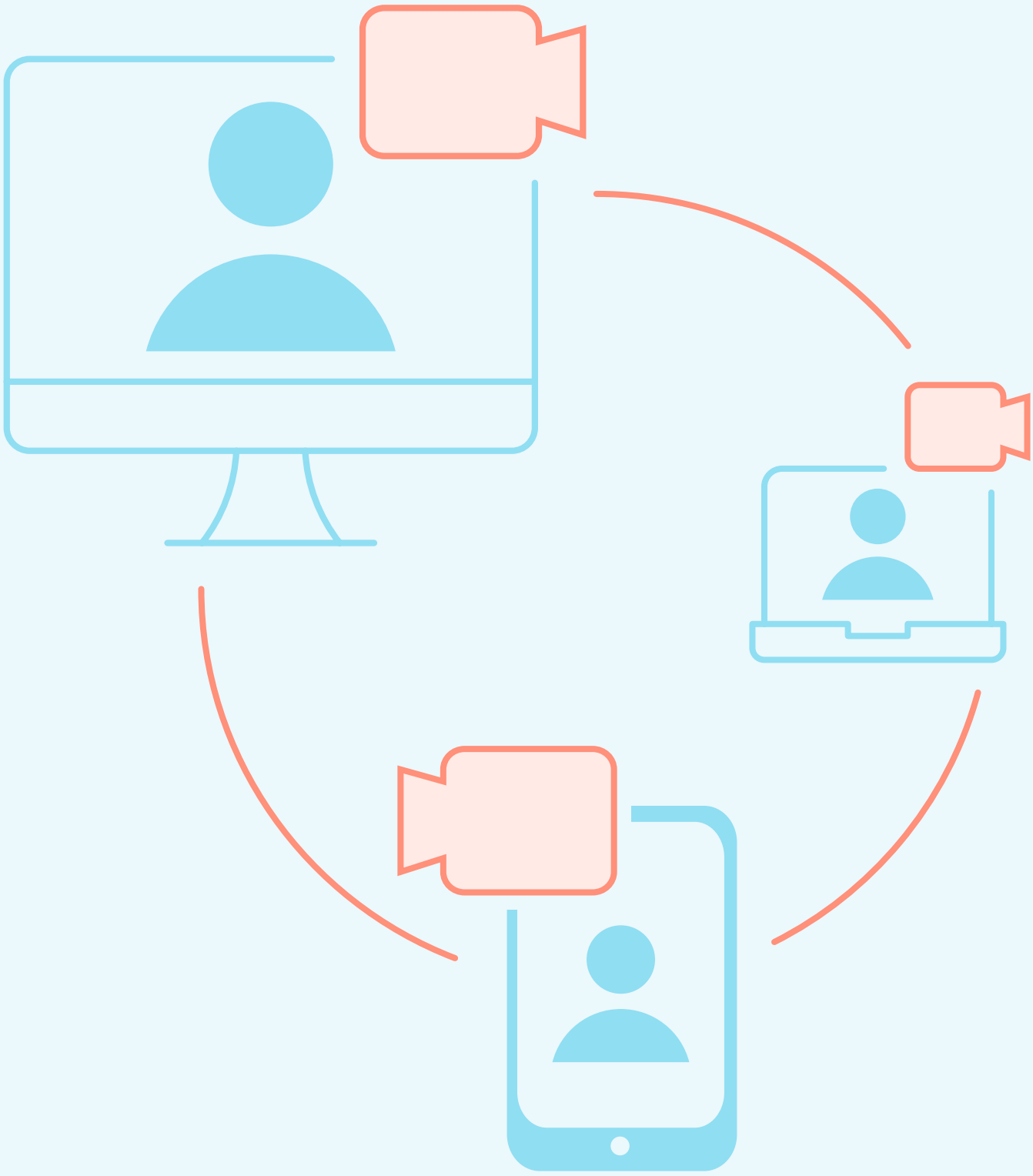
La responsabilité de la protection des données incombe à l'autorité qui, pour accomplir les tâches que lui assigne la loi, traite ou fait traiter des données personnelles. L'autorité doit veiller au respect des prescriptions en matière de protection des données et à la sécurité des données. Cette exigence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

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

Dans certains cas, un examen approfondi est nécessaire pour déterminer la législation applicable et l'autorité de surveillance compétente. 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 des données envisagés qui présentent un risque particulier pour les personnes concernées (contrôle préalable). En outre, il procède à des examens relatifs à la sûreté de l’information dans les systèmes et applications informatiques en service (audits). Le Bureau se veut aussi l’interlocuteur des personnes concernées et se tient à leur disposition pour fournir des conseils, faire office d’intermédiaire ou traiter leurs requêtes. Lorsque la mise en œuvre d’une protection adéquate des données ne saurait être garantie autrement, le Bureau peut rédiger une proposition motivée à l’intention des autorités ou porter les décisions rejetant les propositions motivées jusque devant le Tribunal administratif. Cette option ne doit toutefois servir qu’en dernier recours, c’est-à-dire 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 2021, 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), 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 en général 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 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.

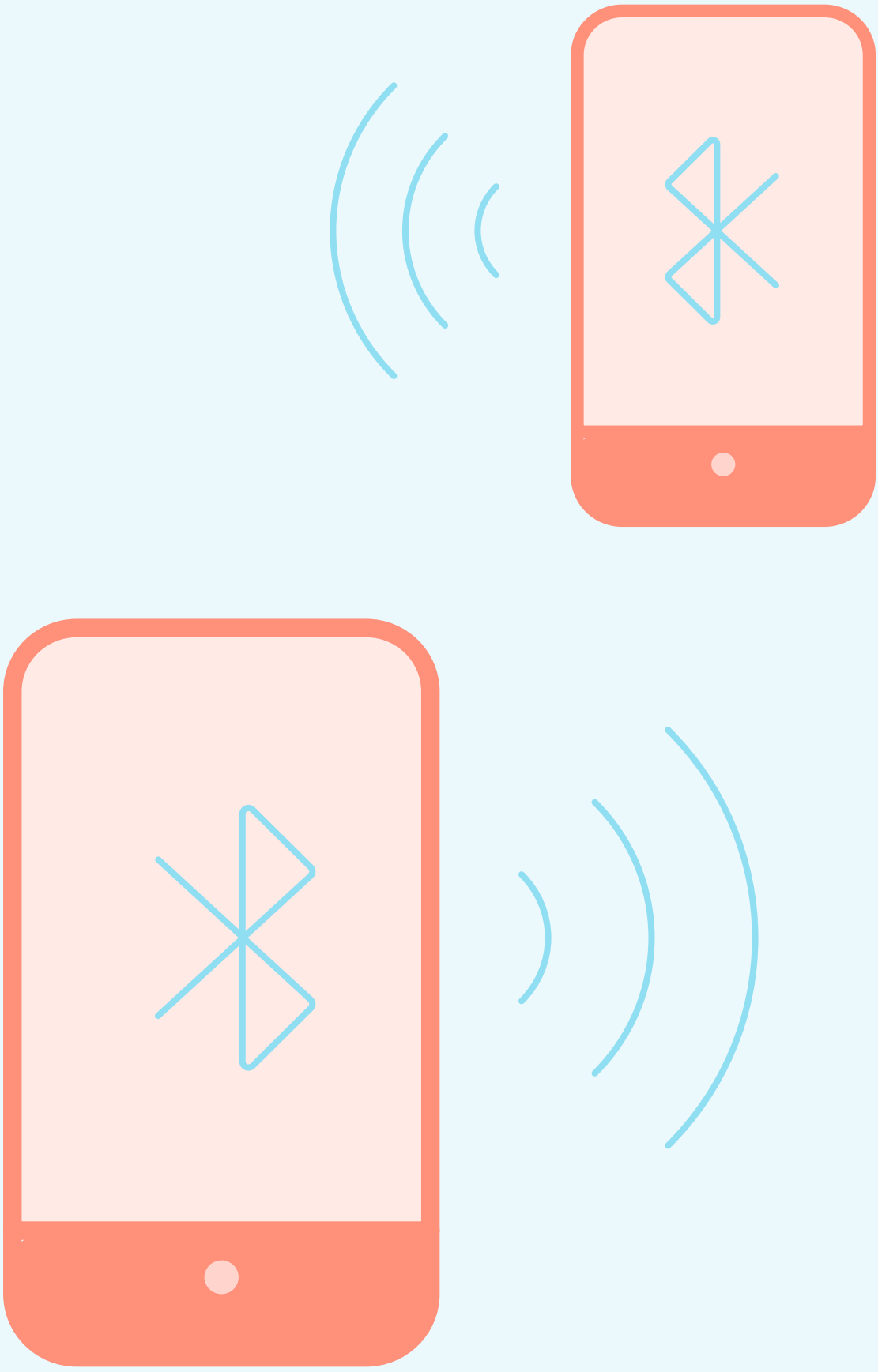
Constatant que sa charge de travail ne cesse d'augmenter, en particulier dans le domaine des contrôles préalables (cf. ch. 6.4.1), le Bureau étudie la possibilité de demander au Grand Conseil un poste à temps plein supplémentaire dans le cadre du budget 2023.

En 2021, les charges d'exploitation du Bureau se sont élevées au total à 243 milliers de francs. Environ 88 % de ces charges (215 milliers de fr.) ont été générées par des prestations externes ayant servi aux contrôles informatiques. Par inadvertance, trois factures totalisant 70 milliers de francs n'ont pas pu être comptabilisées sur 2021. Il en résulte que le Bureau affichera dans le compte d'État 2021 des charges d'exploitation de seulement 174 milliers de francs tandis qu'il dépassera son budget 2022 du montant desdites factures, comptabilisées sur l'année suivante.

Au sein de l'administration cantonale, d'autres organismes se chargent de conseiller les autorités dans le domaine SIPD. Les Directions et la Chancellerie d'État 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 Chancellerie d'État pour les questions particulières (p. ex. concernant la numérisation de l'école). Dans la poursuite de son objectif d'augmenter la prise de conscience et le savoir-faire de toutes les autorités dans le domaine de la protection des données, le Bureau s'applique actuellement à porter un soin tout particulier à son réseau de partenaires au sein de l'administration et à le développer. Il accorde par ailleurs une attention spéciale aux contacts institutionnels avec les autorités qui sont régulièrement confrontées à des questions compliquées relevant du droit de la protection des données (p. ex. Office d'information et d'organisation [OIO], Bedag Informatique SA, Police cantonale [POCA] et Groupe de l'Ile SA [Insel Gruppe]).

Dans l'optique d'aboutir à un programme d'audits SIPD coordonné à l'échelle de l'État, le Contrôle des finances 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 entretient des relations avec ses homologues des autres cantons et avec le PFPDT. Il s'agit, d'une part, de garantir l'échange de savoirs et d'expériences pour les questions qui se posent de la même manière dans tous les cantons et, d'autre part, de coordonner les activités de surveillance dans les projets intercantonaux. Le délégué à la protection des données est membre du comité de privatim et il préside la Conférence depuis novembre 2020 tandis que la responsable des domaines de la santé et de la formation dirige le groupe de travail Santé. Par ailleurs, il y a toujours une personne du Bureau dépêchée pour participer aux autres groupes de travail thématiques (actuellement : cyberadministration, sécurité et TIC). Pour de plus amples informations, voir les sujets traités en 2021 sous le chiffre 6.7 plus bas.



6 Présentation des tâches quotidiennes

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

6.1 Coronavirus

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

6.1.1 Conseils à l'intention des autorités

Dépistage du coronavirus

Une mesure de lutte contre la pandémie de coronavirus consiste à tester les personnes avec ou sans symptômes de maladie afin d'identifier si possible tous les cas d'infection. Le Bureau a apporté son concours à la DSSI et à l'INC en amont des contrôles préalables formels afin que la mise en place des tests étendus dans les écoles et des certificats de test à usage interne dans les hautes écoles soit conforme aux prescriptions de la protection des données (sur ces deux points, lire le ch. 6.1.4) ainsi qu'en ce qui concerne l'activité du camion de dépistage dans les communes. Il a adressé des recommandations aux communes concernées, leur demandant de prêter attention aux procédures d'inscription en ligne et de récupération de résultats effectuées par des membres de leur personnel au nom de personnes sans expérience d'Internet.

Base de données centrale des coordonnées

En vue de la réouverture des espaces intérieurs des restaurants à la fin mai 2021, la DSSI a demandé au Bureau s'il serait admissible de créer une base de données centrale pour recueillir les coordonnées de la clientèle et, si oui, selon quelles modalités. La législation fédérale imposait aux personnes exploitant des établissements de restauration de collecter les coordonnées de leur clientèle, de les conserver durant 14 jours et de les communiquer sans délai à l'Office du médecin cantonal s'il en faisait la demande. Or, la DSSI avait constaté combien il pouvait être difficile, en cas de problème grave, de joindre les établissements concernés ou d'obtenir des listes de coordonnées complètes. Elle souhaitait donc que les coordonnées de la clientèle lui soient transmises en continu afin

qu'elle puisse en disposer immédiatement en cas de besoin. Après analyse, le Bureau a considéré que cette mesure cantonale pouvait se fonder sur la LEp si plusieurs conditions étaient remplies : la base de données doit être expressément prévue dans l'ordonnance COVID-19, où il faut également énoncer les prescriptions requises pour limiter au minimum l'atteinte aux droits des personnes concernées (utilisation des coordonnées uniquement pour le traçage des contacts et uniquement suite à un événement ayant un impact sur la santé, destruction des données au bout de 14 jours, contrôle préalable par le Bureau des mesures techniques et organisationnelles prises pour assurer le respect de ces prescriptions [cf. ch. 6.1.4]). Le Bureau a en outre annoncé d'emblée qu'il soumettrait la base de données à un audit dès son entrée en service (cf. ch. 6.5).

Une personne privée a interjeté recours auprès du Tribunal fédéral contre la modification de l'ordonnance COVID-19 adoptée par le Conseil-exécutif en application des préconisations du Bureau. Cette personne estimait que le canton de Berne n'était pas habilité à adopter des règles allant plus loin que le droit fédéral, que la base légale était insuffisante et que la conservation de données en prévision d'une éventuelle utilisation était disproportionnée. Dans son arrêt 2C_369/2021 du 22 septembre 2021, le Tribunal fédéral a jugé que la réglementation attaquée était licite, concluant au rejet du recours.

En quelques jours, la base de données centrale des coordonnées a suscité plusieurs interpellations parlementaires (093-2021, 097-2021 et 102-2021) portant en partie sur la question de la sûreté des données. Le Bureau a apporté son concours à la DSSI pour y répondre.

Interface entre les applications SORMAS/TRACY et VacMe

Pour le traçage des contacts, le canton de Berne utilise l'application SORMAS, recommandée par l'Office fédéral de la santé publique (OFSP), assortie d'une extension qui lui est propre, TRACY. La planification et la documentation des vaccinations contre le COVID-19 sont effectuées avec l'application VacMe. Chacune de ces applications comporte un fichier de données personnelles. Depuis mars 2021, l'article 3a de la loi fédérale COVID-19 prévoit que les personnes suffisamment protégées par un vaccin ne sont soumises à aucune quarantaine. Les cantons sont en outre tenus de signaler à l'OFSP toute percée vaccinale. La DSSI a donc demandé au Bureau à quelles contions il serait admissible d'utiliser une interface pour transférer des données de VacMe vers SORMAS/ TRACY. Le Bureau a expliqué de manière générale à la DSSI quelles étaient les prescriptions du droit de la protection des données qu'il fallait respecter. Il vérifie comment le projet a été concrétisé dans le cadre du contrôle préalable de SORMAS/TRACY, qui est encore en cours (cf. ch. 6.1.4).

Certificat obligatoire pour le personnel du secteur public

Le Bureau a été interrogé sur les conditions à remplir pour que le certificat puisse être imposé au personnel de l'administration cantonale, d'une Église nationale, d'une commune ou d'une paroisse. Après un échange de vues avec l'Office du personnel et l'OACOT, le Bureau est arrivé à la conclusion que les actes législatifs fédéraux applicables (législation sur le travail et ordonnance COVID-19 situation particulière) autorisent les employeurs du secteur public à rendre le certificat obligatoire pour leur personnel dans la mesure où les conditions énoncées dans ces actes sont remplies. La LCPD admet que le traitement de données particulièrement sensibles puisse s'appuyer sur des bases légales dites indirectes, c'est-à-dire qui instaurent une tâche dont l'accomplissement requiert impérativement ledit traitement (p. ex. le devoir d'assistance de l'employeur envers les membres de son personnel). Le Bureau a toutefois précisé que l'imposition d'un certificat est admissible uniquement si elle est proportionnée et cela est le cas uniquement lorsqu'un certificat est nécessaire dans l'environnement de travail concret pour fixer des mesures de protection appropriées ou pour mettre en œuvre un plan de dépistage selon l'ordonnance COVID-19 situation particulière.

6.1.2 Conseils à l'intention des personnes concernées

Identification des personnes non vaccinées et prise de contact directe?

Au nom des personnes concernées, le téléjournal de la SRF a demandé si, comme cela avait été suggéré lors d'un point de presse de la Confédération, il serait admissible que les cantons identifient les personnes non vaccinées et les contactent par téléphone. La réponse a été très claire : sans autorisation du législateur, il n'est pas admissible d'identifier les personnes n'ayant pas reçu un vaccin non obligatoire. Pour cela, il faudrait comparer les données des registres des habitants avec les données de vaccination (dans VacMe pour le canton de Berne) afin de constater qui n'est pas dans les deux bases de données. Cela reviendrait à utiliser les données dans un but très différent de celui prévu et tout porte à croire que les personnes concernées n'y consentiraient pas. Cette appréciation porte aussi sur les numéros de téléphone, si tant est qu'ils soient connus des autorités cantonales.

Comptabilisation de la vaccination contre le COVID-19 dans le temps de travail

Depuis la fin mars 2021, le canton permet à son personnel de comptabiliser jusqu'à une heure de temps de travail par injection de vaccin. Il a été demandé au Bureau s'il était admissible au regard du droit de la protection des données

d'exiger des agentes et des agents qu'ils notent « vaccination contre le COVID-19 » dans le système de saisie des heures de travail. La réponse du Bureau a été positive : contrairement à une maladie ou à un accident, une vaccination préventive ne donne aucun droit légal à décompter du temps de travail ; cette possibilité est donc une prestation accordée volontairement par l'employeur dans un but déterminé. Par conséquent, il est raisonnable d'exiger des membres du personnel qui font usage de cette possibilité, eux aussi volontairement, qu'ils confirment avoir utilisé cette heure dans le but prévu et non pas à leur guise. Toutefois, l'employeur ou son administration du personnel n'ont le droit de se servir de ce renseignement que pour vérifier le temps de travail, et dans aucun autre but, et ils doivent la traiter confidentiellement.

6.1.3 Prises de position formelles

Modifications de l'ordonnance COVID-19 du canton de Berne

En 2021, l'ordonnance COVID-19 cantonale a été modifiée à 18 reprises. De nombreuses modifications avaient un lien avec la protection des données, notamment la création d'une base légale pour la base de données centrale des coordonnées (cf. ch. 6.1.1.). Après l'introduction du certificat obligatoire par le Conseil fédéral, l'ordonnance cantonale a habilité les hautes écoles à enregistrer le nom, le prénom et la date de naissance des personnes contrôlées ainsi que la date d'expiration de leur certificat afin d'éviter les contrôles répétés. Précision importante, l'ordonnance prévoyait que les données devaient être effacées sans délai après l'expiration du certificat. En décembre, le canton de Berne a instauré l'obligation de présenter un certificat ou de se faire tester régulièrement pour les personnes employées dans les hôpitaux, les EMS et les services d'aide et de soins à domicile. En vue de l'édiction de ces dispositions, le Bureau a dialogué avec les Directions impliquées afin de trouver un dispositif qui soit à la fois aussi simple que possible et conforme au droit de la protection des données.

Loi cantonale sur des mesures dans le domaine de la culture en lien avec le COVID-19

Lors des travaux réalisés par l'administration pour préparer la future loi sur les mesures prises dans le domaine de la culture en lien avec l'épidémie de COVID-19, le Bureau a veillé à ce qu'une ordonnance portant introduction de la législation fédérale relative au COVID-19 dans le domaine de la culture soit transposée dans la nouvelle loi. Cette ordonnance et maintenant la loi permettent l'échange de toutes les données personnelles nécessaires entre les autorités compétentes de la Confédération, du canton et des communes, ce dont les actrices et acteurs culturels requérant des aides financières doivent être informés de manière appropriée, comme le demandait le Bureau.

Consultations diverses concernant la législation fédérale

La LEp impose au Conseil fédéral de consulter les cantons avant d'ordonner de nouvelles mesures. Un grand nombre de consultations ont donc été menées auprès des cantons en 2021, avec parfois un délai de réponse de deux jours ouvrés seulement. Le canton de Berne a demandé au Bureau de prendre position dans ce cadre à chaque fois que des questions de protection des données étaient en jeu.

Lors de la consultation concernant le projet « Intensification de la vaccination », le canton de Berne s'est positionné clairement contre la proposition d'informer individuellement les personnes non vaccinées faute de base légale suffisante pour cela, comme le proposait le Bureau (cf. ch. 6.1.2).

Le Bureau a approuvé l'ajout à l'application SwissCovid d'une fonction permettant d'avertir anonymement les personnes ayant participé à une manifestation qu'elles pouvaient avoir été infectées par le COVID-19 lors de cette manifestation, pour autant que sa mise en œuvre soit correcte sur le plan technique, ce qui relève de la responsabilité de la Confédération. Comme l'utilisation de l'application reste facultative, y compris dans ce but, on peut partir du principe que les personnes qui y recourent approuvent le traitement de leurs données.

En ce qui concerne le transport international de voyageurs, la Confédération a proposé que les cantons mettent en place un système leur permettant de recevoir les résultats de test des voyageurs entrés en Suisse. Le canton de Berne a rejeté cette proposition pour des raisons de protection des données entre autres : d'une part, les cantons ne connaissent pas les données personnelles ni le statut vaccinal de toutes les personnes entrant en Suisse ; d'autre part, la mise en place d'une solution conforme à la protection des données aurait demandé un énorme travail, y compris dans le domaine du contrôle préalable, travail que les cantons n'étaient pas en mesure de fournir en temps utile.

6.1.4 Contrôles préalables

Tests préventifs à grande échelle dans les écoles et les hautes écoles

Avant de lancer les tests préventifs à grande échelle dans les établissements bernois de l'enseignement obligatoire et du secondaire II, la DSSI a informé le Bureau de la procédure informatisée prévue en cas de tests poolés positifs et elle lui a soumis pour contrôle préalable son application spécialisée PROCESS. Après l'élimination des quelques défauts constatés, le contrôle a pu être conclu avec un résultat positif. Le Bureau a continué d'accompagner la DSSI lorsqu'elle a abandonné les tests à grande échelle en milieu scolaire au profit d'un dispositif

de tests en cas de flambée. Il examinera les nouvelles procédures du point de vue du droit de la protection des données dès qu'il aura reçu les documents nécessaires pour procéder au contrôle préalable.

À l'automne 2021, le Conseil fédéral a rendu le certificat obligatoire pour assister aux cours dans les hautes écoles. En très peu de temps, les hautes écoles ont mis en place à l'interne des possibilités de test pour les étudiantes et les étudiants (ainsi que pour les membres de leur personnel). Lors d'une conférence téléphonique, l'Université de Berne a présenté au Bureau le dispositif qu'elle envisageait de mettre en place : accès réservé aux personnes en possession d'une carte de légitimation ou d'une pièce d'identité, prélèvement de l'échantillon sur place, saisie des données sur une plateforme et analyse de laboratoire à l'Institut des maladies infectieuses de l'université. L'université a ensuite transmis la documentation SIPD requise pour le contrôle préalable, qui a abouti à un résultat positif malgré deux défauts ayant une significativité moyenne et un défaut jugé faiblement significatif.

Base de données centrale des coordonnées

Lorsque les espaces intérieurs des restaurants ont pu rouvrir en mai 2021, le canton de Berne a mis en service sa base de données centrale des restaurants et des événements afin de pouvoir identifier et prévenir les personnes présumées infectées (sur la question de la licéité, voir le ch. 6.1.1). Les établissements tenus de collecter les coordonnées de leur clientèle en vertu de la législation fédérale, c'est-à-dire les restaurants mais aussi les discothèques et les salles de danse, devaient transmettre quotidiennement par voie électronique à la base de données centrale les coordonnées qu'elles avaient collectées. Comme l'exige l'ordonnance cantonale COVID-19, la DSSI a soumis la documentation SIPD fin mai au Bureau en vue du contrôle préalable.

Mais comme il était apparu que la documentation risquait d'être présentée tardivement et que le Bureau était disposé à approuver une mise en service anticipée de la base de données centrale pour autant que certaines conditions impératives soient remplies, les mesures techniques et organisationnelles les plus importantes avaient été définies à un stade antérieur. Ainsi, les données sont cryptées de façon à ce qu'il soit impossible de faire des recherches par personnes (ce qui permettrait d'établir des profils), mais seulement de faire des recherches par lieux et heures. De plus, seuls les membres habilités des équipes de traçage des contacts peuvent effectuer une recherche après y avoir été autorisés par une ou un épidémiologiste et décrypter les fichiers de données personnelles dans l'application TRACY. La conservation des données personnelles enregistrées dans la base de données est limitée à 14 jours.

Dans la documentation SIPD qui lui a été remise par la suite, le Bureau a détecté plusieurs défauts ayant une significativité élevée. Ils concernent principalement

l'absence ou le degré de détail insuffisant de certaines explications relatives à des questions importantes du point de vue du droit de la protection des données. Après plusieurs reports de délai, la DSSI a remis sa prise de position à la fin octobre 2021. L'examen de ce document était encore en cours à la fin de l'année sous revue.

Application spécialisée SORMAS/TRACY (gestion du traçage des contacts COVID-19)

Responsable du traçage des contacts, la DSSI utilise pour ce faire depuis l'automne 2020 l'application spécialisée SORMAS, recommandée et mise à disposition par la Confédération. Début 2021, la DSSI a complété l'application par TRACY, une application développée par le canton de Berne sous Power Apps. Avec SORMAS/TRACY, la DSSI traite des données de santé, c'est-à-dire des données personnelles particulièrement dignes de protection, dans le cadre de la gestion des contacts.

La DSSI a remis une première documentation SIPD au printemps 2021 afin que le Bureau réalise un contrôle préalable (a posteriori). Suite à ce contrôle, le Bureau a notifié à la Direction plusieurs dizaines de défauts concernant la sûreté de l'information et la protection des données. Le contrôle ne peut pas être clôturé car les conditions de la gestion des contacts sont mouvantes et le Bureau n'a pas obtenu toutes les informations dont il a besoin. Par conséquent, la conformité de l'exploitation de SORMAS/TRACY avec les dispositions en matière de protection des données n'est toujours pas garantie. Il s'agit là d'une situation problématique car les données personnelles traitées dans cette application sont particulièrement dignes de protection. Cela n'est satisfaisant ni pour le Bureau, ni pour la DSSI en tant que Direction responsable.

La DSSI a fait savoir qu'elle prévoyait des changements dans le domaine de la gestion des contacts en 2022. Le Bureau pense qu'avec la collaboration de la Direction, le contrôle préalable pourra aboutir à un résultat positif au cours de cette année.

Application spécialisée VacMe (gestion numérique de la vaccination contre le COVID-19)

Pour planifier et documenter les vaccinations contre le COVID-19 dans le canton de Berne, la DSSI utilise l'application VacMe, développée spécialement pour le canton de Berne. Comme la gestion des contacts, la vaccination contre le COVID-19 est soumise à des conditions qui changent souvent. Le Bureau a néanmoins réussi, avec le concours de la direction du projet VacMe, à clore le contrôle préalable avec un résultat positif avant la fin de l'année sous revue. Compte tenu de l'ensemble des circonstances, il semble donc que la conformité

de l'exploitation de VacMe avec les dispositions en matière de protection des données soit garantie.

Parmi les défauts constatés par le Bureau, l'absence de base légale mérite une mention particulière. Les traitements de données personnelles (particulièrement dignes de protection) présentés pour contrôle dans le cas concret n'ont pas de base légale suffisante, que ce soit dans le droit cantonal ou dans le droit fédéral. Avant la vaccination, le canton de Berne demande le consentement au traitement des données. Ce consentement est en principe donné volontairement (par la population désireuse de se faire vacciner) et pour un traitement défini de manière suffisamment concrète et claire. Néanmoins, un consentement délivré dans de telles conditions ne saurait remplacer totalement une base légale. C'est pourquoi le Bureau a recommandé à la DSSI que le canton édicte la base légale formelle requise au cas où surviendraient d'autres pandémies nécessitant que le canton mette en œuvre un programme de vaccination.

Vidéosurveillance d'un centre de vaccination

Il était prévu de compléter la surveillance assurée par Securitas dans les centres de vaccination du Wankdorf et de BernExpo par un dispositif étendu de vidéosurveillance. Selon la loi sur la police (LPol), le placement de bâtiments publics sous vidéosurveillance à des fins de protection de ces bâtiments et de leurs usagers doit être examiné sous l'angle du droit de la protection des données dans le cadre de la procédure de consultation de la POCA (cf. ch. 6.4.2). Étant donné l'urgence du dossier, le Bureau a contribué à accélérer la procédure de contrôle préalable en apportant des explications et en traitant ce dossier en priorité. Le rapport de contrôle a mis en évidence plusieurs points qu'il aurait fallu améliorer pour que la vidéosurveillance soit conforme aux dispositions en matière de protection des données. Mais après avoir réévalué les risques de sécurité dans les centres de vaccination concernés, l'état-major spécial coronavirus a décidé de renoncer à la vidéosurveillance et les équipements concernés ont été démontés.

6.2 Conseils

6.2.1 Autorités

Retransmission audiovisuelle de cours donnés dans les hautes écoles

Les hautes écoles souhaiteraient pouvoir continuer la retransmission audiovisuelle de cours après la pandémie. Elles se sont donc adressées au Bureau pour obtenir son avis à ce sujet. Le Bureau a examiné les bases légales en vigueur dans le domaine de hautes écoles. Sa première appréciation l'a conduit à considérer que ces retransmissions sont en principe licites dans la mesure où les principes généraux du droit de la protection des données sont respectés, en particulier celui de la proportionnalité. Le Bureau estime en effet que les tâches légales des hautes écoles constituent la base légale indirecte requise dans chacun de leurs cas. Mais avant d'émettre un avis final, il souhaite avoir des échanges de vues avec les services de surveillance de la protection des données des autres cantons universitaires.

Carte numérique des religions dans le canton de Berne

Le délégué aux affaires ecclésiastiques et religieuses a demandé au Bureau quelles étaient les prescriptions du droit de la protection des données à respecter pour créer une carte numérique des religions. À ce jour, la LCPD s'applique également aux personnes morales. Il faut donc une base légale suffisante pour traiter les données (particulièrement dignes de protection) des communautés religieuses. La compétence accordée constitutionnellement aux cantons d'organiser les rapports entre l'État, d'une part, et les Églises ainsi que les autres communautés religieuses, d'autre part, inclut de pouvoir faire évoluer ces rapports. Sur la base de cette norme générale de délégation, le Bureau a estimé que le traitement de données de base était admissible à la condition que chacune des communautés religieuses concernées donne son accord et puisse révoquer son consentement à tout moment. S'agissant du traitement de données plus poussées, par exemple à des fins de monitorage, le Bureau a recommandé de créer ou au moins d'envisager de créer une base légale expresse.

Privilège de la recherche pour des recherches généalogiques privées

Une personne privée faisant des recherches généalogiques a demandé à consulter les procès-verbaux d'une commune afin de comprendre les processus politiques de l'époque et de les intégrer dans son travail de généalogie. De manière générale, ces procès-verbaux ne sont pas accessibles avant l'expiration du

délai de protection. Mais la loi sur l'archivage (LArch) autorise une consultation anticipée à des fins scientifiques, en se référant à la LCPD. L'OACOT a demandé au Bureau si la recherche généalogique privée est considérée comme de la recherche scientifique au sens de la loi. Dans un cas semblable, le Tribunal administratif avait fait référence à la définition de la recherche de la Confédération, selon laquelle la recherche scientifique peut aussi être effectuée pour répondre à des intérêts privés (arrêt Tadm 100.2010.335). Le Bureau a donc estimé qu'il était possible de considérer comme scientifique un projet de recherche généalogique ayant une certaine importance socio-historique, non sans préciser qu'il était nécessaire de définir dans une convention les mesures de protection des données à observer pour que la communication des données soit conforme à la LCPD.

Modification de la loi sur l'archivage

Le Bureau a été étroitement impliqué par les Archives de l'État dans les travaux menés au sein de l'administration cantonale pour préparer la révision de la LArch. Il a siégé au sein de deux groupes de travail, qui se sont occupés d'une part de questions générales de terminologie et de systématique, ce qui incluait en particulier la coordination des dispositions régissant les archives avec le droit de la protection des données, et d'autre part de la question de l'archivage des dossiers psychiatriques. Le Bureau a également approfondi des questions particulières lors d'échanges de vues bilatéraux avec les Archives de l'État, notamment concernant le délai de protection des documents contenant des données personnelles particulièrement dignes de protection et les effets des obligations légales de garder le secret. Cette démarche a été très fructueuse : tous les aspects importants de la protection des données ont pu être abordés et pris en compte dès le stade des échanges informels si bien que, lors de la procédure formelle de corapport, le projet n'a plus suscité que des propositions et des remarques mineures de la part du Bureau.

Modification de la loi cantonale sur la protection des données

La LCPD doit être adaptée aux prescriptions du droit européen, notamment suite à la modernisation de la Convention du Conseil de l'Europe pour la protection des données et à une modification de la directive (UE) 2016/680, contraignante pour la Suisse, dans le domaine du droit pénal. Cette révision permettra également de moderniser la LCPD pour faire face à l'évolution des technologies. Dans le cadre des travaux préparatoires menés au sein de l'administration cantonale, le Bureau a apporté son concours à deux groupes de travail inter-Directions. La réflexion a porté sur des questions matérielles relevant de la protection des données, mais aussi sur des questions politiques (concernant notamment la désignation de la personne déléguée à la protection des données et la surveillance

parlementaire à laquelle elle est soumise) et sur la future organisation de la surveillance de la protection des données dans les communes (cf. ch. 6.6.2).

Utilisation de Microsoft 365 dans l'administration cantonale

L'utilisation de services en ligne (informatique en nuage) n'est pas interdite par principe aux autorités, mais elle fait naître un ensemble de défis et de risques, notamment pour la confidentialité des données, qu'il est important d'étudier préalablement avec soin afin de les ramener à un niveau acceptable par des mesures appropriées. Il faut mentionner en particulier la faible marge de manœuvre laissée par des contrats fortement standardisés, le traitement des données dans des États où la protection des données n'est pas adéquate, le recours à des sous-traitants mal connus (en partie établis dans des États où les données sont mal protégées), le traitement de données relatives aux utilisatrices et aux utilisateurs par l'entreprise qui fournit le nuage à des fins qui lui sont propres et la possibilité que des autorités étrangères accèdent aux données.

Pour mettre en œuvre l'authentification à deux facteurs exigée par le Bureau, qui consiste à compléter l'identifiant et le mot de passe par un autre facteur d'authentification pour accéder à des données personnelles particulièrement dignes de protection, un produit de Microsoft reposant sur les services en ligne *Azure Active Directory* et *Azure Multi-Factor Authentication* a été évalué. Des échanges nourris au sein de l'administration ainsi qu'avec des personnes représentant Microsoft ont été nécessaires pour clarifier un grand nombre de questions juridiques, techniques et organisationnelles en vue d'évaluer les risques mentionnés et de pouvoir y faire face par des mesures appropriées, par exemple en renonçant à une authentification par SMS ou message vocal qui aurait exigé le transfert de données aux États-Unis. Les risques résiduels ont paru supportables au Bureau comme aux autres services cantonaux impliqués et ils ont été acceptés expressément par la direction de l'OIO dans une décision formelle.

Alors que la question de l'authentification à deux facteurs portait au départ uniquement sur les données des utilisatrices et des utilisateurs parmi le personnel de l'administration cantonale, la généralisation de Microsoft 365, c'est-à-dire de services de communication et de collaboration et d'applications Office basées sur le Web, engage potentiellement les données des citoyennes et des citoyens bernois. Ce projet de généralisation requiert donc une analyse des risques de bien plus grande envergure, que le Conseil-exécutif a demandé à l'OIO et à la Bedag de réaliser avec le concours du Bureau. La décision relative à l'ampleur à donner aux mesures visant à réduire les risques au minimum et aux risques résiduels à supporter devra également être prise par le Conseil-exécutif.

6.2.2. Personnes concernées

Vidéosurveillance privée sur le domaine public

Une personne a fait savoir au Bureau qu'une entreprise privée avait installé deux caméras sur le toit d'un bâtiment pour surveiller son site, mais que le champ de ces caméras débordait sur la voie publique, et elle voulait savoir quelles étaient ses possibilités d'intervention. En principe, les dispositifs de vidéosurveillance des personnes privées doivent être évalués selon les dispositions de la loi fédérale sur la protection des données; elles relèvent donc du domaine de compétence du PFPDT. Mais comme, en l'espèce, la voie publique et donc le domaine public de la commune étaient concernés, la personne a pu demander aux autorités communales de clarifier les faits et d'exiger de l'entreprise exploitant les caméras qu'elle cesse de filmer la rue.

Communication de données au programme de dépistage du cancer du sein

Une femme a demandé au Bureau s'il était admissible que le canton de Berne communique ses données au programme donna de dépistage du cancer du sein par mammographie. Selon la loi bernoise sur la santé publique, le dépistage précoce des maladies fait partie des soins de santé publique. Se fondant sur cette base légale, le canton a d'abord chargé la Ligue bernoise contre le cancer de réaliser le programme de dépistage du cancer du sein, puis il a rejoint les cantons de Saint-Gall, des Grisons et de Soleure pour confier cette tâche à la ligue contre le cancer de Suisse orientale (Krebsliga Ostschweiz). La Ligue contre le cancer est ainsi autorisée à accéder aux adresses des femmes âgées de 50 ans ou plus et à les inviter à participer au programme de dépistage. Mais toute femme a la possibilité d'indiquer à donna qu'elle ne souhaite plus recevoir ses courriers et que les données la concernant que le programme pourrait détenir doivent être effacées.

Erreurs d'adressage de documents fiscaux

Une personne privée s'est plainte auprès du Bureau d'une erreur d'adressage de documents fiscaux. Le Bureau lui a prêté assistance dans ses démarches pour établir les faits et il a demandé aux autorités fiscales des explications concernant cet incident. Il est apparu qu'un retour du courrier par la poste à l'Intendance des impôts avait entraîné un changement d'adressage sans vérification de l'adresse par l'autorité fiscale ou la commune. Par la suite, plusieurs documents fiscaux ont été envoyés à de mauvais destinataires. Après les interventions de la personne auteure de la plainte et du Bureau, la commune a corrigé l'adresse indiquée et l'Intendance des impôts, son processus de gestion des changements d'adresse.

Accès à ses propres données auprès du Ministère public

En vertu de la LCPD, toute personne peut exiger de recevoir par écrit des renseignements sur les données la concernant qui sont traitées par une autorité. Sur demande également, la personne intéressée peut consulter ses données si aucune circonstance particulière ne s'y oppose. Le Ministère public était prêt à laisser une personne consulter les documents concernés dans ses locaux, mais il avait refusé de délivrer les renseignements demandés par écrit au motif que la possibilité de consultation étendue répondait aussi au droit d'obtenir des renseignements. Après un bref échange avec le Ministère public, le Bureau a informé la personne qu'elle pouvait demander au Ministère public une décision formelle relative à sa demande de renseignements écrits et recourir contre cette décision devant le Parquet général. Dans les affaires concrètes concernant des personnes individuelles, le Bureau peut conseiller ces personnes sur leurs droits et faire office de médiateur entre elles et les autorités, mais il n'est pas habilité à donner des instructions aux autorités, ni à représenter les personnes concernées comme le ferait une étude d'avocats.

6.2.3. Formation continue

Contribution à la formation du personnel communal

Le *Bildungszentrum für Wirtschaft und Dienstleistung* (bwd) propose différentes formations à l'intention des personnes travaillant pour des autorités communales. Cela fait de nombreuses années – et 2021 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. Les cours à l'intention du personnel des secrétariats paroissiaux introduits en 2020 ont été complétés, en 2021, par une formation destinée aux autorités paroissiales consacrée à la protection des données dans les paroisses. Au cours de cette formation, les intervenantes et 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 a parlé du traitement de données sur mandat par les fournisseurs de cloud (10ème conférence de l'Université de Berne sur les

achats dans le domaine des technologies de l'information, Workplace Conference 2021 de la Conférence suisse sur l'informatique [CSI], Schulthess Forum 2021 sur la protection des données dans les villes et les communes), de la protection des données dans le domaine scolaire (14e Journée suisse du droit de la protection des données) et de questions de protection des données durant la pandémie (congrès organisé conjointement par *Swiss DPO Association* et *Swiss Healthcare Privacy Professionals*).

En outre, le Bureau a été représenté à un événement de formation continue destiné aux préfètes et aux préfets pour présenter les fondements de la protection des données ainsi que les expériences réalisées par le Bureau avec les communes et leurs services de surveillance de la protection des données.

6.3 Prises de position formelles

Modification de l'ordonnance sur l'école obligatoire : carte talent

L'ordonnance sur l'école obligatoire a été modifiée afin d'instaurer une carte talent destinée aux élèves possédant des talents particuliers. Dans les domaines artistiques, la carte est délivrée par une commission spécialisée, qui atteste sous une forme qualifiée que l'élève possède les aptitudes requises pour accéder à un programme d'encouragement ou à une formation spécifique. Le Bureau avait souhaité que l'ordonnance aborde déjà la question des données personnelles qui seraient contenues dans la carte talent. Mais comme cela restait encore à définir lorsque l'ordonnance a été modifiée, l'INC, qui a la responsabilité de ce dossier, consultera de nouveau le Bureau dès que le projet de carte talent aura été élaboré pour s'assurer que les prescriptions légales en matière de protection des données sont bien prises en compte.

Nouvelle loi sur les finances

Le projet de nouvelle loi sur les finances adopté par le Conseil-exécutif à l'intention du Grand Conseil en novembre 2021 contient des dispositions détaillées sur le traitement des données dans les systèmes d'informations financières et, via une modification indirecte de la loi sur le personnel, dans le système d'information sur le personnel du canton de Berne. En étroite collaboration avec le Bureau, les deux textes ont été dotés des bases légales claires requises par la LCPD pour traiter des données personnelles particulièrement dignes de protection et pour consulter des données de cette nature contenues dans des fichiers centralisés de données personnelles du canton selon la loi sur les fichiers centralisés de données personnelles (LFDP).

Réglementation des droits d'accès aux fichiers centralisés de données personnelles

Deux nouveaux textes de loi sont entrés en vigueur en même temps que la LFDP le 1er mars 2021 : l'ordonnance sur la plate-forme des systèmes de registres communaux (O GERES) et l'ordonnance sur le système de gestion centrale des personnes. Ces deux textes prévoient que les Directions, la CHA et la justice doivent réglementer les droits d'accès à ces deux bases de données et les soumettre pour avis au Bureau avant d'édicter ces règlements. Tous les accès doivent reposer sur une base légale suffisante et être nécessaires pour accomplir les tâches légales, ce qui doit être expliqué de manière fondée au Bureau. Au cours de l'année sous revue, le Bureau a rendu un avis formel sur les réglementations des droits d'accès de la FIN, de la DIJ et de la DSSI. La CHA n'en édicte pas car elle n'a plus l'usage des fichiers de données concernés.

Le Bureau a également conseillé des communes et des paroisses ainsi que leurs services de surveillance lors de l'élaboration ou de l'examen de leur réglementation des droits d'accès. Une commune ou une paroisse doit avoir une réglementation propre uniquement dans la mesure où elle a besoin d'accès autres que ceux déjà attribués à toutes les communes et paroisses dans l'annexe de l'O GERES.

Modification de l'ordonnance sur le marché du travail : enregistrements vidéo

L'ordonnance sur le marché du travail contient un nouvel ensemble de dispositions détaillées relatif à l'enregistrement vidéo et audio d'entretiens menés avec la clientèle à des fins d'assurance de la qualité et de formation du personnel. Un enregistrement ne peut être effectué qu'avec le consentement écrit de toutes les personnes participantes et le consentement peut être révoqué à tout moment sans motif. Les enregistrements doivent être supprimés dans les six mois à compter de leur réalisation et immédiatement si les personnes enregistrées le demandent. Le Bureau ayant été impliqué dans la rédaction de ces nouvelles dispositions, il n'a eu qu'une suggestion à apporter concernant le rapport lors de la procédure de corapport formelle.

Modification de la loi sur l'information

Lors des travaux préparatoires menés au sein de l'administration, le Bureau a pu faire valoir l'ensemble de ses points de vue, notamment concernant la concordance matérielle de la loi sur l'information avec la LCPD. Il a donc pu donner son plein accord au projet lors de la première procédure de corapport et de la consultation. Il a toutefois dû intervenir, lors de la deuxième procédure de corapport, contre une modification apportée par la CHA à l'instigation d'une autre Direction. Comme le demandait le Bureau, le nouveau projet habilite les autorités à publier

sur Internet des informations d'intérêt général même si elles contiennent des données personnelles, les données personnelles concernées devant être effacées dès que l'intérêt public ne justifie plus qu'elles soient accessibles au public. Cette dernière exigence est expressément requise par le droit constitutionnel (principe de proportionnalité), raison pour laquelle le Bureau n'a pas admis que la loi sur l'information se contente de faire référence à la LCPD. Il a cependant confirmé que l'obligation d'effacer les données portait uniquement sur les publications des autorités et non pas sur Internet en général, où il est impossible d'empêcher des tiers de faire circuler des contenus déjà publiés.

6.4 Contrôles préalables

6.4.1. Projets informatiques

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

En 2020, le Bureau a traité 138 contrôles préalables concernant des projets informatiques (2020 : 123) et en a achevé 77 (2020 : 58), soit 55,8 % (2020 : 47,2 %). 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.

Registre des tumeurs Berne et Soleure (KRBESO)

La loi fédérale sur l'enregistrement des maladies oncologiques (LEMO) est en vigueur depuis le 1er janvier 2020. Elle constitue la base légale permettant de collecter dans l'ensemble de la Suisse des données nombreuses et très complètes sur les maladies oncologiques, les lésions précancéreuses et certaines

tumeurs bénignes. Chaque canton doit tenir un registre selon la LEMO. La tenue du registre des maladies oncologiques des cantons de Berne et Soleure (KRBESO) a été confiée à l'Institut de pathologie de l'Université de Berne. Le KRBESO utilise le logiciel d'enregistrement gratuit fourni par la Confédération (RSW), qui a remplacé le logiciel précédent, NICERStat. Le KRBESO est actuellement le seul registre travaillant avec RSW en phase de production. D'autres registres ont adapté NICERStat afin de se conformer aux conditions énoncées dans la LEMO.

L'adoption du logiciel national RSW a requis un contrôle préalable. Le Bureau a examiné la documentation SIPD du KRBESO et de la Confédération. Durant cet examen, il a été en contact avec la coordinatrice du KRBESO ainsi qu'avec des représentantes et des représentants de la division Transformation numérique de l'OFSP. En raison de la forte charge de travail que la pandémie représente pour l'OFSP, les adaptations requises dans la documentation SIPD de la Confédération ont pris beaucoup de retard. Comme le contrôle préalable du Bureau présentait un intérêt pour tous les autres cantons qui envisageaient d'adopter eux aussi RSW, privatim (cf. ch. 6.7) est intervenue auprès de l'OFSP pour le prier de ne plus tarder à traiter les questions sur lesquelles le KRBESO devait rendre réponse au Bureau. Celui-ci a finalement pu achever la procédure de contrôle préalable en décembre 2021, avec un rapport positif.

Outils de visioconférence

Plusieurs outils de visioconférence ont été soumis en même temps au contrôle préalable du Bureau. Cette concentration était due aux besoins créés par le télétravail pendant la pandémie, mais pas seulement. L'OIO a par exemple mis en place l'application Zoom pour compléter les canaux de communication existants après que le fournisseur a accepté que la convention-cadre conclue avec la fondation SWITCH pour le domaine des hautes écoles soit également valable pour d'autres organes publics. Il a fallu prendre diverses mesures pour assurer une utilisation du logiciel conforme à la protection des données : le Bureau a exigé que le cryptage de bout en bout des échanges de données, qui restreint peut-être certaines fonctions mais garantit que le fournisseur n'a aucun accès aux contenus, soit configuré comme un réglage par défaut et pas seulement comme une option. Parce que les comptes utilisateurs sont administrés aux États-Unis, qui ne sont pas considérés comme un État offrant un niveau de protection des données adéquat, il fallait en outre que l'ouverture d'un compte soit facultative et que les utilisatrices et utilisateurs soient clairement informés, avant l'ouverture de leur compte, du transfert de leurs données et du risque que des autorités étrangères y accèdent.

En ce qui concerne l'application My Justice de l'Office de l'exécution judiciaire (OEJ), qui avait été évaluée et recommandée par le programme HIS d'harmonisation de l'informatique dans la justice pénale de la Confédération et des

cantons, le Bureau a demandé certaines mesures, comme l'exclusion de l'utilisation de cette application dans le domaine de la télémédecine, où la législation impose des obligations particulières de garder le secret. Dans le cadre de son passage au poste de travail cantonal, l'INC avait besoin de l'application Microsoft Teams Desktop App pour pouvoir maintenir tous les services informatiques d'EDUBERN destinés aux écoles de l'enseignement obligatoire et du degré secondaire II. Ces services avaient été audités par le Bureau en 2018, lequel, en l'état des connaissances à l'époque, les avait jugés conformes à la protection des données. Mais cette appréciation a été remise en cause après l'arrêt Schrems II rendu en 2020 par la Cour de justice européenne, qui estimait que l'exportation de données aux États-Unis était en grande partie illicite, et suite à un examen détaillé de l'ensemble des contrats conclus avec Microsoft. Toutefois, le Bureau a toléré, principalement pour des raisons de confiance légitime, la poursuite de l'utilisation de l'application jusqu'à ce que Microsoft 365 soit mis en place dans l'administration cantonale (cf. ch. 6.2.1).

Gestion des prestations particulières d'encouragement et de protection destinées aux enfants

En vue de l'entrée en vigueur de la nouvelle loi sur les prestations particulières d'encouragement et de protection destinées aux enfants, l'Office des mineurs devait mettre en place pour le 1er janvier 2022 un nouveau système de traitement des commandes et de préfinancement des prestations impliquant une multitude de fournisseurs. Le système comporte plusieurs éléments : un accès externe basé sur le portail BE-Login pour les commanditaires et les fournisseurs de prestations ; une plateforme de processus pour les échanges de données ; et un logiciel de gestion des dossiers pour le stockage et la conservation des dossiers. Étant donné le caractère particulièrement digne de protection des données traitées concernant les enfants, il fallait notamment examiner les mesures prises pour garantir que les données ne soient pas accessibles à des personnes non autorisées et que les données non destinées à être archivées soient effacées de manière sûre à l'expiration de la durée de conservation.

La même plateforme de processus étant déjà utilisée par une autre Direction, le Bureau a suggéré à l'OIO et à la Bedag d'élaborer une documentation SIPD générique pour ce service et de la soumettre au contrôle préalable du Bureau afin qu'elle puisse servir de base aux autres Directions et offices du canton.

Application spécialisée InfoSearch de la Police cantonale

La LPol et le Code de procédure pénale autorisent, pour autant que des conditions restrictives soient remplies, à mener des enquêtes ou des recherches secrètes avant ou après qu'un crime ou un délit a été commis. Les agentes et agents infiltrés qui ont obtenu la garantie de leur anonymat ont droit à ce que

leur véritable identité demeure cachée aux tiers non habilités, y compris s'agissant de membres de la police, et qu'elle ne figure pas dans les pièces du dossier. L'application spécialisée InfoSearch est utilisée pour gérer les sources anonymes que constituent les agentes et les agents infiltrés sous une identité d'emprunt et les documenter en même temps que les informations recueillies pendant l'infiltration. Étant donné le degré de confidentialité très élevé des données, le premier contrôle de la documentation SIPD effectué par le Bureau a abouti à plusieurs constatations significatives concernant notamment le cryptage des données, la garantie de la confidentialité vis-à-vis des prestataires externes ainsi que la sûreté de l'effacement des données et des sauvegardes devenues inutiles. La POCA a accepté tous ces constats et elle y a remédié en adoptant des mesures ou des spécifications supplémentaires.

Dialogueurs (chatbots)

Deux offices ont soumis au Bureau en même temps des documentations SIPD en vue de la mise en place de dialogeurs pour répondre automatiquement aux questions des utilisatrices et des utilisateurs en se basant sur des termes identifiés. Le dialogueur de l'Office des assurances sociales (OAS) a pour vocation de répondre à des questions de fond sur le droit à la réduction des primes d'assurance-maladie. Celui de l'OIO a une fonction d'assistance : il a pour but de fournir aux membres du personnel de l'administration cantonale une première réponse à leurs questions ou de les diriger vers les pages d'information pertinentes. Les deux dialogueurs avaient en commun de ne pas être destinés à traiter des données personnelles, mais il n'y a pas de moyen technique d'empêcher les utilisatrices et les utilisateurs d'entrer des données personnelles dans le champ de texte. Il convenait donc de s'assurer que les citoyennes et les citoyens ou les membres du personnel du canton soient avertis de manière claire et immanquable, avant l'utilisation des dialogueurs, qu'ils n'ont pas le droit d'entrer des données permettant de les identifier ou d'identifier d'autres personnes (p. ex. noms, adresses électroniques, numéros AVS, etc.). Le dialogueur de l'OAS a été dispensé du contrôle préalable formel parce que le fournisseur et ses serveurs sont localisés en Suisse et que les conditions imposées par le canton de Berne dans le domaine SIPD avaient été convenues contractuellement. Dans le cas de l'OIO, qui recourt aux services de prestataires internationaux, il a fallu un contrôle préalable formel pour établir quelles mesures supplémentaires avaient été prises pour réduire les risques en cas d'utilisation du dialogueur d'assistance non conforme aux prescriptions.

6.4.2. 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.

Office de la population

Le Bureau a examiné pour la première fois la vidéosurveillance de l'Office de la population (OPOP). L'OPOP est responsable de l'application des dispositions relatives au séjour des personnes étrangères, de l'octroi de l'aide d'urgence aux requérantes et requérants d'asile déboutés et de l'exécution des expulsions. Pour des raisons de sécurité, l'office combine une surveillance en temps réel et des enregistrements dans les espaces accessibles à la clientèle. L'examen du Bureau a entraîné plusieurs améliorations au regard de la protection des données. Les salles où se déroulent les entretiens, par exemple, restent placées sous surveillance pour la sécurité du personnel et de la clientèle, mais les membres du personnel peuvent à tout moment interrompre l'enregistrement s'ils l'estiment inutile. Une nouvelle directive explique les aspects SIPD aux membres du personnel et garantit que les caméras ne sont pas utilisées pour surveiller le personnel.

Hôpital de l'Île

À l'Hôpital de l'Île, le Bureau a examiné les caméras rajoutées dans plusieurs bâtiments et dans le parking pour compléter le système de surveillance existant. Elles devaient soit être utilisées pour assurer la sécurité publique, en combinant surveillance en temps réel et enregistrements, soit permettre une surveillance en temps réel pour garantir la santé des patientes et des patients dans le cadre de l'accomplissement des tâches de l'hôpital. Le simple fait qu'une personne se rende à l'hôpital en tant que patiente ou patient est une donnée personnelle de santé. Par conséquent, les images de patientes et de patients sont des données particulièrement dignes de protection, sur lesquelles les professionnelles et les professionnels de la santé sont tenus de garder le secret. Les exigences à remplir en matière de sûreté des données sont donc très élevées et le Bureau ne manque pas de le rappeler aux responsables.

Systèmes vidéo mobiles de la Police cantonale

En août 2021, la POCA a démarré un projet pilote de caméras-piéton, c'est-à-dire des caméras portées par les agentes et les agents des forces de l'ordre pour sécuriser les preuves. L'année précédente, le Bureau avait étudié la question des bases légales de cette pratique, sur laquelle il avait donné son avis à l'occasion d'un rapport du Conseil-exécutif (voir le ch. 6.3 du rapport annuel 2020). Au cours de l'année sous revue, la POCA a soumis au Bureau la documentation SIPD relative à l'utilisation de systèmes de vidéo mobiles, ce qui inclut les caméras-piéton. Les bases légales existantes permettent d'utiliser ces caméras uniquement lorsqu'il existe des indices concrets laissant présumer qu'un crime ou un délit est imminent ou a été commis. Par conséquent, les caméras ne peuvent pas tourner en permanence, mais elles doivent être activées par les personnes qui les portent en fonction des circonstances. Le Bureau a donc vérifié non seulement les mesures techniques et organisationnelles prises pour sécuriser l'utilisation des enregistrements, mais aussi la documentation concernant la formation des agentes et agents de police concernés.

6.5 Audits

Dans le cadre de son mandat légal de surveillance de l'application des prescriptions relatives à la protection et à la sûreté des données, le Bureau a mené huit audits dans ce domaine. Il a également réalisé avec le Contrôle des finances un audit de l'application spécialisée GINA-Web. Il est prévu de reconduire et développer la collaboration avec le Contrôle des finances en 2022.

Dans le cadre du suivi des audits ayant abouti de 2016 à 2020, le Bureau a accompagné en continu la mise en œuvre des mesures d'amélioration. Ce suivi actif est une tâche normale du Bureau, gage d'efficacité et d'obtention des résultats souhaités. Le Bureau a ainsi pu constater à maintes reprises que les tâches dans le domaine SIPD requerraient une attention soutenue de la part des services responsables, mais que celle-ci n'a pas toujours été à la hauteur attendue. Des retards ont été pris dans l'accomplissement des tâches, ce qui s'explique notamment par la mobilisation requise par les affaires courantes et par la situation extraordinaire qui a régné en 2021 en raison des mesures prises par les autorités pour endiguer la pandémie. Les retards dans la mise en œuvre des améliorations dans le domaine SIPD augmentent le risque de ne pas pouvoir faire face de manière appropriée et suffisamment rapide aux menaces dans le domaine de la cybersécurité, qui évoluent en permanence. Le Bureau attend donc des services responsables qu'ils tiennent compte de l'accroissement de ce risque lorsqu'ils priorisent leurs tâches, d'autant plus que les activités cybercriminelles ont encore pris de l'ampleur et gagné en qualité au cours de

l'année sous revue. La responsabilité dans le domaine SIPD incombe à tous les services qui traitent des données personnelles.

BE-Net / IPv6

BE-Net regroupe des services techniques de réseau que l'OIO met à la disposition de l'administration cantonale et d'autres clients. Il comprend un réseau étendu (Wide Area Network, WAN), les réseaux locaux câblés (Local Area Networks, LAN) et les réseaux locaux sans fil (Wireless Local Area Networks, WLAN). BE-Net est en service sur 288 sites. Il est à disposition dans l'administration cantonale ainsi que dans 48 écoles et 215 communes et touche ainsi quelque 37 500 utilisatrices et utilisateurs. L'exploitation de BE-Net est externalisée. Il est prévu de remplacer à moyen terme la technologie réseau employée à l'heure actuelle pour la transmission de données entre systèmes informatiques, le protocole Internet en version 4 (IPv4), par sa nouvelle version (IPv6). Or, l'introduction progressive du protocole IPv6 présente des risques élevés dans le domaine SIPD.

L'audit réalisé a porté en premier lieu sur les architectures réseau et sécurité des réseaux WAN et LAN, du protocole IPv6, de la configuration à double pile (dual stack) et des tunnels prévus pour les transferts de données (tunneling) ainsi que sur les stratégies et les méthodes appliquées pour sécuriser le réseau basé sur le protocole IPv6 et pour protéger les données. Le Bureau a également évalué la robustesse des réseaux (résilience) et réalisé un test d'intrusion technique (test de vulnérabilité).

Globalement, l'audit n'a pas mis en évidence de risques SIPD importants. Mais il a constaté quelques risques de niveau moyen ou faible qui requièrent des actions correctives. Le test d'intrusion dans les réseaux a relevé quelques vulnérabilités techniques exploitables. Certains processus opérationnels essentiels doivent également être améliorés. En outre, il faudrait prévoir de réaliser régulièrement des tests de vulnérabilité offrant une traçabilité. L'audit s'est déroulé dans un contexte professionnel et constructif.

BE-Voice / Téléphonie

L'OIO met à la disposition de l'administration cantonale une plateforme de téléphonie et de télécommunication uniforme et standardisée appelée BE-Voice. BE-Voice contient le logiciel Skype for Business, utilisé par quelque 10 000 personnes dans l'administration. À cela s'ajoutent environ 500 téléphones physiques fonctionnant avec un système vocal sur Internet (voice over IP). L'application spécialisée Competella est utilisée pour gérer et diriger les appels sur les numéros principaux des offices ainsi que pour mettre à disposition les

numéros d'assistance et les hotlines. Elle a environ 4500 utilisatrices et utilisateurs. Son exploitation technique est entièrement externalisée.

L'audit réalisé avait notamment pour but d'évaluer la sécurité du service de téléphonie, en se concentrant sur les architectures réseau et infrastructure de BE-Voice et de Competella. Il a également porté sur le respect des prescriptions et l'efficacité de la mise en œuvre de configurations sûres. De plus, des processus opérationnels importants et les conditions contractuelles ont été évalués. Enfin, un test d'intrusion technique a été mené (test de vulnérabilité) en visant une sélection de composants ou de secteurs de BE-Voice particulièrement importants sur le plan technique.

Les constatations faites lors de l'audit présentent un risque SIPD moyen, en ce qui concerne le concept SIPD, la configuration, le renforcement et la sécurité du réseau de téléphonie ainsi que l'exploitation et les processus opérationnels mais aussi en ce qui concerne les contrats de prestations. Le test d'intrusion n'a pas mis en évidence de vulnérabilité critique. Le résultat global peut être qualifié de bon. L'audit s'est déroulé dans un contexte professionnel.

Service de courrier électronique

Le service de courrier électronique que l'OIO met à la disposition de l'administration cantonale est une solution uniforme et standardisée. Il comprend tous les composants techniques nécessaires pour gérer et traiter les courriels, c'est-à-dire les envoyer et les recevoir, sur la base du produit Microsoft Exchange. Une solution Secure Mail, qui permet de crypter les courriels de bout en bout de manière sûre, est également fournie. La mise en œuvre technique et l'exploitation sont externalisées en intégralité.

L'audit avait avant tout pour but d'évaluer si les prestataires responsables répondaient de manière vérifiable aux exigences techniques et organisationnelles dans le domaine SIPD. Il devait être complété par un test d'intrusion technique pour identifier des points faibles.

L'audit a mis en évidence des risques de sécurité moyens dans le domaine SIPD en ce qui concerne le concept SIPD, l'architecture de l'infrastructure, la gestion des accès, les interfaces, les contrats de prestations et le test d'intrusion. Ce dernier a montré que le service utilise en partie des versions d'algorithmes de cryptage dont les points faibles sont connus. Il a également mis en évidence une vulnérabilité pouvant constituer un risque indirect pour le service de courrier électronique. L'audit s'est déroulé dans une ambiance cordiale et professionnelle.

Centre de services

Le Centre de services de l'OIO est le premier point de contact du personnel de l'administration cantonale en cas de questions ou de problèmes de fonctionnement dans les domaines de l'informatique et des télécommunications (service BE-Support). Il lui incombe avant tout de résoudre les problèmes de fonctionnement. Le Centre de services mène des investigations détaillées ou, si nécessaire, transfère les annonces de problème à un service compétent afin qu'il les traite. Les questions et les annonces de problème sont enregistrées et traitées au moyen d'un système de tickets. Le Centre de services dispose de différents outils d'assistance technique et d'une infrastructure pour le traitement, l'analyse et la résolution des problèmes de fonctionnement.

L'audit a porté sur le domaine SIPD. Il s'agissait d'évaluer comment le service BE-Support répond aux exigences SIPD avec les outils d'assistance technique et l'infrastructure technique qu'il utilise.

L'audit a montré la nécessité d'améliorer la formation des membres du personnel du Centre de services dans le domaine SIPD notamment. Il est apparu en outre que, dans ce domaine, les prescriptions du Centre de services n'étaient pas complètes ni obligatoires. De plus, il n'y pas été possible de mettre totalement en évidence comment le Centre de services applique et contrôle ces prescriptions. Enfin, l'infrastructure et les outils d'assistance utilisés présentent des risques SIPD importants. L'OIO entreprendra les améliorations recommandées dans les meilleurs délais. L'audit s'est déroulé dans un esprit de convivialité et d'ouverture.

GINA-Web

GINA-Web est une application spécialisée modulaire basée sur un moteur de gestion des flux (*workflow engine*) et sur une technologie Internet. Elle s'adresse principalement aux spécialistes de l'OEJ, qui l'utilisent pour accomplir leurs processus clés et leurs processus d'assistance relatifs à l'exécution des peines et mesures par les personnes en détention. L'application est également utilisée par des spécialistes du Service de psychiatrie forensique de l'Université de Berne, par des médecins externes devant dispenser des traitements médicaux somatiques sur mandat de l'OEJ et par le personnel chargé de recouvrer les amendes. On enregistre chaque année dans GINA-Web quelque 20 000 à 25 000 jugements bernois, y compris les condamnations à des peines privatives de liberté de substitution. L'application sert en outre à administrer quelque 15 000 dossiers d'exécution de peines ou de mesures par des adultes et des jeunes et à gérer la planification et la mise en œuvre de ces peines et mesures dans les institutions concernées, ce qui représente environ 400 000 jours d'occupation par an. Comme des données personnelles particulièrement dignes de protection sont traitées dans GINA-Web, le niveau de protection requis est élevé.

L'audit avait principalement pour but de contrôler si les prescriptions dans le domaine SIPD étaient respectées de manière vérifiable et transparente, en particulier en ce qui concerne la gouvernance, les concepts, les mesures de protection, les processus de gestion des utilisatrices et utilisateurs, les contrats de prestations avec les fournisseurs importants et d'autres tiers (externalisation), les interfaces de l'application ainsi que la conservation et le cycle de vie des données.

Globalement, l'audit a montré que des exigences importantes en matière de SIPD n'avaient pas encore été mises en œuvre intégralement. Les risques détectés étaient essentiellement de niveau moyen mais, cumulés, ils constituent un risque élevé pour la sûreté de l'information et la protection des données. Le Bureau a donc dû préconiser des actions urgentes pour que l'application puisse être rapidement mise en conformité. L'OEJ a adopté ces préconisations et accordé une priorité haute aux tâches qui en découlent. L'audit s'est déroulé dans une ambiance de cordialité et à d'écoute.

Base de données centrale des restaurants et des événements

Parmi les mesures ordonnées par le Conseil fédéral pour lutter contre l'épidémie de COVID-19 figurait la collecte des coordonnées de la clientèle des installations, établissements et manifestations accessibles au public. Pour les raisons évoquées plus haut (voir le ch. 6.1.1), l'Office de la santé (ODS) a lancé un projet visant à instaurer les conditions requises pour que la collecte des coordonnées puisse être centralisée de manière systématique dans une base de données. Le nombre de personnes potentiellement concernées avait été chiffré à 1 million environ. La base de données centrale des restaurants et des événements développée dans le cadre de ce projet est utilisée par l'ODS pour traiter les coordonnées de personnes physiques et les données relatives aux endroits qu'elles ont fréquentés dans le canton de Berne.

L'audit a contrôlé si les prescriptions dans le domaine SIPD étaient respectées de manière vérifiable dans la gestion centrale des coordonnées. Il a porté sur la gouvernance SIPD, les concepts SIPD et les mesures de protection mises en œuvre, les processus d'exploitation de la base de données et la gestion des accès, les prestations de tiers, y compris les contrats conclus avec ces prestataires, ainsi que la conservation effective et le cycle de vie des données. L'application spécialisée TRACY utilisée pour le traitement opérationnel des données personnelles a été prise en compte de manière limitée (contrôle d'un exemple pratique de traitement de données).

Des déficits présentant un risque moyen pour les personnes concernées ont été détectés dans tous les domaines examinés. Des améliorations ont donc été recommandées. En particulier, l'ODS n'est pas parvenu à démontrer de manière totalement transparente que les données personnelles devenues inutiles sont

effectivement effacées, comme l'exige clairement sa réglementation. Il y a également eu des questions concernant la qualité des données. L'ODS et le Secrétariat général de la DSSI ont adopté les recommandations formulées. L'audit s'est déroulé dans une atmosphère cordiale.

Therefore

La Haute école pédagogique germanophone de Berne (PHBern) forme les futurs enseignants et enseignantes du canton de Berne. La formation de base, le perfectionnement, la recherche, le développement et l'évaluation se déroulent sur des sites en ville de Berne tandis que les centres d'orientation de la PHBern sont répartis dans tout le canton. L'établissement recourt à deux applications spécialisées pour gérer les données du corps étudiant (données personnelles de base, bulletins de notes et dossier électronique) : Omnitracker pour la gestion et la documentation des données et, depuis 2014, Therefore pour l'archivage électronique des dossiers des étudiantes et étudiants. La PHBern utilise Therefore sous sa propre responsabilité sur l'un de ses sites à Berne.

L'audit a porté principalement sur le respect des prescriptions SIPD dans le traitement des données personnelles avec Therefore. À cet effet, le Bureau a contrôlé la gouvernance, les concepts et les mesures de sécurité, les processus d'exploitation, la gestion des identités et des accès ainsi que les contrats de prestations conclus avec des tiers.

Des possibilités d'amélioration et d'optimisation ont été observées dans tous les domaines contrôlés, avec un niveau de risque moyen en général mais élevé dans le domaine de la gouvernance SIPD. En particulier, le Bureau n'a pas pu établir que la direction de la PHBern soutient de manière probante les exigences dans le domaine SIPD en définissant une politique en la matière qui comporte des objectifs et des mesures et qui fixe un cadre opérationnel. Cette charge est reportée en grande partie sur les responsables informatiques. L'absence de gouvernance dans le domaine SIPD constitue un risque important pour les personnes concernées, en particulier dans le contexte de la stratégie de numérisation adoptée par la PHBern. L'audit s'est déroulé dans une atmosphère conviviale, avec une qualité d'écoute notable.

Hôpitaux Frutigen Meiringen Interlaken AG

Les hôpitaux Frutigen Meiringen Interlaken AG (fmi AG) assurent la couverture en soins médicaux dans une région allant de Frutigen aux grands cols alpins de l'Oberhasli. Les hôpitaux de soins aigus d'Interlaken et de Frutigen pratiquent la chirurgie, l'orthopédie et la traumatologie, la médecine interne ainsi que la gynécologie et l'obstétrique. De plus, fmi AG a établi un service d'urgence ouvert 24 heures sur 24 dans le centre de santé de Meiringen. Le groupe comprend également la résidence pour personnes âgées Frutigland, qui comporte un site à

Frutigen et un site à Aeschi, ainsi que le centre pour personnes âgées Weissenau à Unterseen. Fmi AG emploie quelque 1500 personnes.

Dans un rapport de 2016, le Bureau avait recommandé 27 actions correctives suite à un contrôle dans le domaine SIPD. Depuis, il a suivi l'avancement de la réalisation de ces mesures lors de concertations périodiques formelles avec fmi AG. L'audit réalisé en 2021 avait pour but de vérifier sur pièces que les mesures SIPD avaient été mises en œuvre de manière efficace.

Globalement, l'audit de suivi a montré que, sur les 27 préconisations dans le domaine SIPD formulées en 2016, 16 avaient été réalisées efficacement, dix avaient été mises en œuvre partiellement et une restait à accomplir. Cela montre à nouveau combien la réalisation d'améliorations dans le domaine SIPD est complexe pour les services concernés, en particulier lorsqu'elles portent sur des aspects fondamentaux qui sont communs à plusieurs fonctions et qui impliquent des tiers ainsi que le niveau de direction responsable. Lors de l'entretien de clôture de l'audit de suivi, certaines mesures SIPD ont été controversées. Force a été de constater, une fois de plus, que les responsables ne sont pas toujours pleinement conscients du fait que les exigences dans ce domaine ont le caractère de prescriptions légales et qu'il est obligatoire de s'y conformer pour protéger les personnes concernées. De manière générale, l'audit s'est déroulé dans une atmosphère cordiale et professionnelle.

Groupe de l'Île SA

En 2016, l'Hôpital de l'Île a fusionné avec Spital Netz Bern AG pour former le Groupe de l'Île SA, qui est la plus grande structure de soins médicaux en Suisse. Le groupe prend en charge plus de 800 000 patientes et patients par an et emploie plus de 10 000 personnes. La direction de la technologie et de l'innovation (DTI), qui emploie environ 200 personnes, est responsable de la gestion technique des technologies de l'information et de la communication (TIC) et des technologies médicales. Suite à une restructuration, la DTI a été dotée d'une division « Governance, Risk & Compliance » (GRC), dans l'idée qu'un service extérieur aux équipes opérationnelles serait mieux à même en particulier de contrôler et de traiter les risques SIPD dans le domaine des TIC et des technologies médicales.

Un audit mené en 2018 par le Bureau n'avait pas été idéal, que ce soit durant sa réalisation ou au vu des déficits mis en évidence. Le Bureau avait alors convenu avec les responsables qu'il assurerait un suivi étroit et continu de la réalisation des améliorations dans le domaine SIPD. Suite à des changements importants dans l'organisation et le personnel du Groupe de l'Île, cette réalisation avait d'abord laissé à désirer. Le Bureau a ainsi jugé utile d'effectuer un audit plus étendu dans le domaine SIPD en 2021. Cette procédure a porté au premier chef sur la protection de base des TIC, c'est-à-dire 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 consiste avant tout à vérifier si la confidentialité, l'intégrité, la disponibilité et l'authenticité des données à traiter sont assurées de manière systématique, transparente et vérifiable.

Globalement, le Bureau a constaté qu'au cours de l'année écoulée le Groupe de l'Île avait mis en place des mesures correctes pour améliorer fondamentalement la sûreté de l'information et la protection des données. C'est le cas notamment de l'établissement au sein de la DTI de la division GRC jouissant d'une indépendance par rapport au fonctionnement opérationnel, de la mise en place, encore en cours, d'un système de gestion de la sûreté de l'information ainsi que de la mise en œuvre de processus centraux. Néanmoins, le Bureau estime que la situation globale présente toujours un risque élevé dans le domaine SIPD, qui est difficilement acceptable, et qu'il y a encore des améliorations essentielles à apporter pour que les actions correctives dont la conception est partiellement achevée parviennent à réduire les risques. En particulier, le domaine SIPD ne fait pas encore l'objet de prescriptions et de mesures obligatoires applicables dans l'ensemble du Groupe de l'Île, toutes directions confondues. L'audit s'est déroulé dans une ambiance professionnelle, cordiale et constructive.

6.6 Autres instruments relevant du droit de la surveillance

6.6.1. Propositions motivées et recours

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

En 2021, le Bureau n'a pas présenté de proposition formelle et n'a pas formé de recours contre une décision négative d'une autorité responsable.

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

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

Au cours de l'année sous revue, le Bureau a remis aux responsables de la DIJ chargés du projet de révision de la LCPD les résultats des travaux du groupe de travail informel composé de représentantes et de représentants de l'Association des communes bernoises, de l'OACOT, des préfectures et du Bureau. Ce rapport, dont le contenu a été discuté en 2020 dans le cadre d'un atelier avec des responsables représentant des communes de tailles variées, propose des variantes possibles pour l'organisation future de la surveillance de la protection des données au niveau communal conformément à la loi sur les communes. Ces propositions pourront faire l'objet de discussions élargies au cours de la procédure législative ordinaire.

Conseils en matière de vidéosurveillance communale

Dans le cadre de son mandat de haute surveillance, le Bureau a conseillé plusieurs organes communaux de surveillance de la protection des données sur des questions de vidéosurveillance. Une commune souhaitait connaître la procédure à suivre pour placer des locaux scolaires sous vidéosurveillance et savoir ce qu'elle devait indiquer et sous quelle forme dans sa demande à l'attention de la POCA. Le Bureau a également eu à répondre aux questions d'une personne privée inquiète et à se prononcer au sujet d'un système de vidéosurveillance privé qui débordait sur un passage ouvert au public. Dans ce deuxième cas, c'est une personne travaillant pour la commune qui demandait quels moyens la commune pouvait utiliser pour empêcher une surveillance privée du domaine public.

6.7 Coopération intercantonale

Présidence et bureau 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 plénières durant l'année sous revue, l'une par voie de circulaire et l'autre en présentiel. Avec le retour de Schwyz, Obwald et Nidwald, toutes les autorités cantonales de surveillance de la protection des données sont de nouveau membres de privatim. Le bureau et son comité ont préparé treize réponses de la conférence à des consultations de la Confédération ainsi que des modèles de document à l'intention des membres. Les échanges avec le PFPDT ont porté sur des sujets comme les conséquences de l'arrêt Schrems II de la Cour de justice européenne, l'utilisation systématique des numéros AVS ou encore des questions de fond et de compétences en lien avec la pandémie. Privatim a en outre entretenu ses relations avec la CSI, avec la nouvelle organisation Administration numérique suisse, avec les institutions Educa et SWITCH dans le domaine de l'enseignement et de la recherche ainsi qu'avec la société eOperations AG, au sein de laquelle privatim a œuvré pour que les contrats de prestations des cantons soient conformes aux dispositions en matière de protection des données.

Groupes de travail de privatim

Le *groupe de travail Cyberadministration* et un sous-groupe de travail institué à cet effet ont étudié l'avis de droit que la professeure Astrid Epiney et son assistante Sophia Rovelli ont rendu concernant le principe du « once only » et l'État de droit. Le sous-groupe de travail a élaboré un document d'accompagnement à l'attention des membres de privatim qui sera diffusé avec la publication. Il est apparu lors de ces travaux que la LCPD bernoise offrait un bon exemple de solution conforme au droit de la protection des données.

Le *groupe de travail Sécurité* a tenu deux séances, l'une virtuelle et l'autre physique, pour travailler sur des questions communes concernant la surveillance policière avec des moyens techniques, les échanges de données intercantonaux dans le domaine policier et d'autres aspects de l'activité policière et judiciaire en lien avec la protection des données. Plusieurs membres du groupe de travail ont en outre participé à une séance d'information organisée par la direction du projet de création d'une situation de sécurité nationale (Integriertes Lagebild 4.0) pour impliquer précocement dans le projet les autorités de protection des données des cantons participants afin de pouvoir prendre en compte leurs exigences.

Le *groupe de travail Santé* s'est réuni virtuellement à sept reprises durant l'année sous revue, sous la direction de la déléguée à la protection des données suppléante du Bureau. Cette année encore, les échanges entre les spécialistes de la protection des données dans le système de santé qui composent le groupe de travail ont porté essentiellement sur des questions importantes de protection des données durant la pandémie. Les analyses et les expériences effectuées par le canton de Berne concernant la base de données centrale des coordonnées et la plateforme VacMe ont apporté des éléments intéressants aux autorités de protection des données des autres cantons. Réciproquement, le canton de Berne a appris des choses importantes concernant la documentation et le registre des vaccinations (classification juridique et responsabilité, y compris en ce qui concerne la conservation). Par ailleurs, le groupe de travail a repris la question de l'introduction du dossier électronique du patient. Il a prévu de travailler davantage sur ce sujet en 2022.

Au sein du *groupe de travail TIC*, des représentantes et des représentants des cantons dont les organes de surveillance ont leurs propres informaticiens ont échangé au sujet de questions techniques d'actualité.

7 Proposition

Prise de connaissance.

8 Liste des abréviations

CHA	Chancellerie d'État
CSI	Conférence suisse sur l'informatique
DEEE	Direction de l'économie, de l'énergie et de l'environnement
DIJ	Direction de l'intérieur et de la justice
DSSI	Direction de la santé, des affaires sociales et de l'intégration
DTI	Direction Technologie et innovation de l'Hôpital de l'Île
FIN	Direction des finances
fmi AG	Hôpitaux Frutigen Meringen Interlaken AG
GRC	Division « Governance, Risk & Compliance » de l'Hôpital de l'Île
INC	Direction de l'instruction publique et de la culture
IPv6	Protocole Internet version 6
KRBESO	Registre des maladies oncologiques Berne Soleure
LAN	Local Area Network
LArch	Loi sur l'archivage
LCPD	Loi cantonale sur la protection des données
LEp	Loi fédérale sur la lutte contre les maladies transmissibles de l'homme (loi sur les épidémies)
LEMO	Loi fédérale sur l'enregistrement des maladies oncologiques
LFDP	Loi sur les fichiers centralisés de données personnelles
LPD	Loi fédérale sur la protection des données
LPol	Loi sur la police
OACOT	Office des affaires communales et de l'organisation du territoire
OAS	Office des assurances sociales
ODS	Office de la santé

OEJ	Office de l'exécution judiciaire
OFSP	Office fédéral de la santé publique
O GERES	Ordonnance sur la plate-forme des systèmes des registres communaux
OIO	Office cantonal d'informatique et d'organisation
OPOP	Office de la population
PFPDT	Préposé fédéral à la protection des données et à la transparence
PHBern	Haute école pédagogique de Berne
POCA	Police cantonale
privatim	Conférence des préposé(e)s suisses à la protection des données
SIPD	Sûreté de l'information et protection des données
Tadm	Arrêt du Tribunal administratif
TIC	Technologies de l'information et de la communication
UE	Union européenne
WAN	Wide Area Network

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