Kanton Bern
Canton de Berne

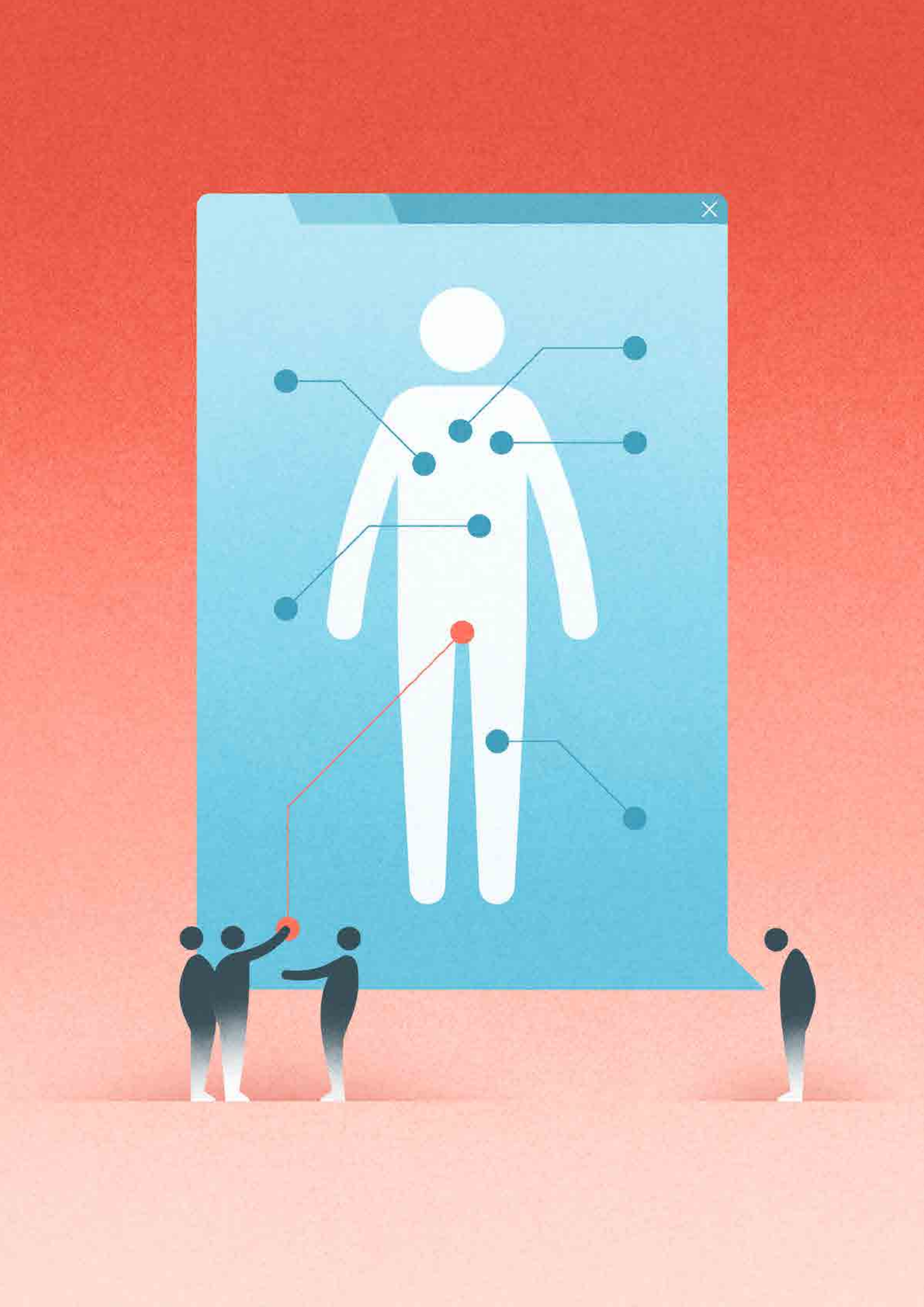
Rapport d'activité Bureau pour la surveillance de la protection des données 2024

Impressum

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

Maquette et réalisation : noord.ch
Illustrations: aurelmaerki.ch

1	**Avant-propos**	5
2	**Droit fondamental à la protection des données**	6
3	**Responsabilité et surveillance**	8
4	**Tâches du Bureau**	10
5	**Organisation, ressources et réseau**	11
6	**Présentation des tâches quotidiennes**	15
6.1	Conseils	15
6.1.1	Conseils à l'intention des autorités	15
6.1.2	Conseils à l'intention des personnes concernées	19
6.1.3	Formation continue	22
6.2	Prises de position formelles	23
6.3	Contrôles préalables	27
6.3.1	Projets informatiques	27
6.3.2	Vidéosurveillance	33
6.4	Audits	35
6.5	Autres instruments relevant du droit de la surveillance	40
6.5.1	Traitement de signalements d'incidents dans le domaine de la protection des données	40
6.5.2	Propositions motivées et recours	40
6.5.3	Haute surveillance des autorités communales et paroissiales de surveillance de la protection des données	41
6.6	Coopération intercantonale	42
7	**Proposition**	45
8	**Liste des abréviations, glossaire**	47



1 Avant-propos

La première loi sur la protection des données du canton de Berne, qui date de 1986 et qui est toujours en vigueur, « a pour but de protéger les personnes contre les abus dans le traitement de données par les autorités ». Cette définition a ceci de positif que, dès l'origine, elle axait la protection sur les personnes visées dans les données, et non pas sur les données en tant que telles. En revanche, on peut s'inquiéter du fait qu'à l'époque on envisageait manifestement la possibilité que les autorités puissent faire une utilisation abusive des données personnelles au point de promulguer une loi spéciale pour y faire obstacle. Aujourd'hui, cette vision est dépassée. La Constitution bernoise de 1993 a instauré un droit fondamental autonome à la protection des données, dont les éléments essentiels sont la légalité et la proportionnalité de tout traitement de données par les autorités, l'exactitude et la sécurité des données ainsi que le droit des personnes concernées à consulter leurs données. C'est donc à juste titre que le projet de nouvelle loi cantonale sur la protection des données adopté en novembre 2024 par le Conseil-exécutif à l'attention du Grand Conseil donne un but plus large à cet acte : « la présente loi vise à protéger le droit fondamental à la protection des données des personnes dont les données personnelles sont traitées par les autorités. »

La protection de la sphère privée n'est pas un droit absolu car, sinon, les autorités ne pourraient pas accomplir les tâches qui leur incombent. Cependant, les règles de l'État de droit contenues dans le droit fondamental à la protection des données prévu par la Constitution cantonale bernoise ne sont pas négociables. Cela s'applique aussi et surtout aux traitements numériques de données, dont les possibilités techniques accroissent les risques pour les droits des personnes concernées : copier, associer et transférer des données numériques est un jeu d'enfant, il est inutile de disposer d'un espace physique pour les conserver et des procédés de traitement avancés sont disponibles à des prix ridicules dans le monde entier. Par conséquent, à chaque fois que des autorités envisagent une mise à niveau technique de leurs traitements de données, la question de savoir si ce sont les spécifications techniques ou la protection des données et la sûreté de l'information qui ont la primauté ne se pose même pas : il faut toujours allier les deux.

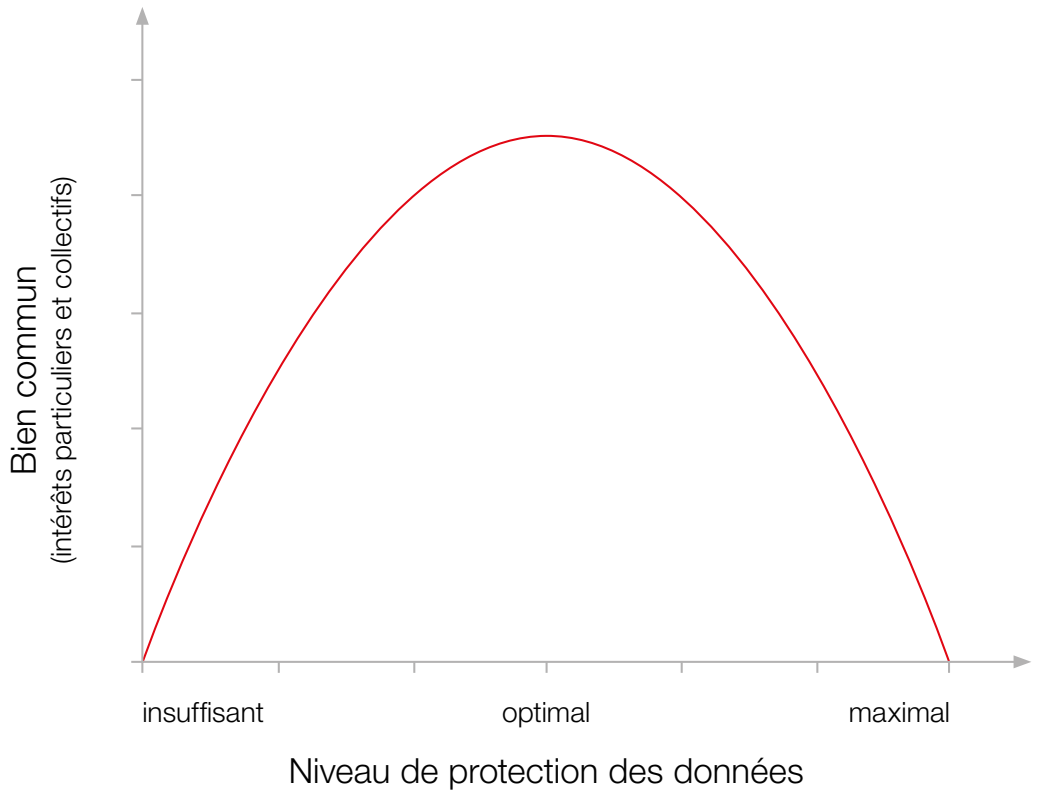
Le Bureau pour la surveillance de la protection des données du canton de Berne (BPD ; ci-après le Bureau) conseille les autorités cantonales dans leurs projets de numérisation et en assure la surveillance. Plus le Bureau est impliqué tôt dans un projet et peut expliquer le cadre établi par la législation sur la protection des données, plus les autorités ont une marge de manœuvre importante pour réaliser leur projet à l'intérieur du cadre législatif et atteindre tous leurs buts dans les limites imparties par la Constitution. En 2024, le Bureau a de nouveau accompagné un grand nombre de projets de numérisation dans tous les secteurs de l'administration cantonale. Le présent rapport en présente une sélection et rend compte des autres activités du Bureau.

Ueli Buri, délégué à la protection des données

2 Droit fondamental à la protection des données

La protection de la sphère privée, qui comprend le droit à l'autodétermination informationnelle (c.-à-d. le droit de chaque personne de pouvoir déterminer si des données la concernant sont traitées ou non et dans quels buts) est un droit fondamental protégé par la Constitution fédérale comme par la Constitution cantonale. Un droit fondamental ne peut faire l'objet d'une restriction qu'à certaines conditions : la restriction doit reposer sur une base légale suffisante, servir un intérêt public prépondérant et être proportionnée au but poursuivi (c.-à-d. être adaptée et nécessaire et avoir des conséquences supportables pour les personnes concernées). Évidemment, ces conditions valent aussi pour le traitement de données personnelles par les 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 la sphère privée de l'individu. Le niveau de protection des données garanti constitutionnellement est donc considéré comme adéquat lorsque le meilleur équilibre possible 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 des intérêts collectifs est maximal.

La loi cantonale sur la protection des données (LCPD) précise les devoirs des autorités lors du traitement de données personnelles. Par autorité, il faut comprendre l'administration, mais aussi les 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 ainsi qu'à la sécurité des données, que l'autorité de surveillance compétente ait été impliquée ou non et que ses recommandations aient été suivies ou non.

Le champ d'application des législations suisse et bernoise sur la protection des données présente une structure fédéraliste. La loi fédérale sur la protection des données (LPD) s'applique aux autorités fédérales et aux personnes privées qui traitent des données (notamment à des fins commerciales), lesquelles sont assujetties à la surveillance du préposé fédéral à la protection des données et à la transparence (PFPDT). Les activités des autorités cantonales et communales du canton de Berne sont régies par la LCPD. Leur surveillance s'inscrit elle aussi dans la logique du système fédéral : le Bureau surveille les traitements de données des autorités cantonales tandis que les communes désignent leur propre organe de surveillance, lequel est à son tour surveillé par le Bureau.

Dans certains cas, un examen approfondi est nécessaire pour déterminer la législation applicable et l'autorité de surveillance compétente. Ainsi, la fondation de droit privé Swisstransplant est assujettie d'une part aux dispositions de la LPD applicables aux responsables du traitement privés et donc à la surveillance du PFPDT, par exemple lorsqu'elle traite les données de son personnel. Mais d'autre part, en sa qualité de service national des attributions au sens de la législation sur la transplantation d'organes, elle est assujettie aux dispositions de la LPD applicables aux organes fédéraux, toujours sous la surveillance du PFPDT. Si la fondation vient par ailleurs à exploiter une plateforme sur laquelle les hôpitaux cantonaux et les centres de transplantation rattachés traitent ou font traiter des données personnelles dans le cadre de l'accomplissement de leurs propres tâches, ces traitements de données devront répondre aux exigences légales cantonales applicables et seront surveillés par l'autorité de la protection des données de chacun des cantons concernés.

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 de données électroniques 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 et porter les décisions rejetant une proposition motivée 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. Les conseils du Bureau 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 2024, le Bureau disposait de 670 % de poste et employait huit personnes. Cinq d'entre elles ont une formation en droit, tandis que les trois autres sont informaticiens ou réviseurs spécialisés 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 ainsi que 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 en tant qu'employé du canton de Berne. Sa tâche première au sein du Bureau comprend la planification et l'exécution des contrôles des systèmes et applications en service 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 suit les activités de la Direction de la santé, des affaires sociales et de l'intégration (DSSI). Elle vérifie les aspects juridiques des documents SIPD lors des contrôles préalables.

Liz Fischli-Giesser (collaboratrice scientifique, domaine juridique) est avocate et travaille depuis 2012 pour le Bureau. Elle est principalement responsable de la Direction des finances (FIN) et de la Direction de l'économie, de l'énergie et de l'environnement (DEEE) ainsi que de la vidéosurveillance et des questions relatives aux paroisses.

Christina Hug Gnägi (collaboratrice scientifique, domaine juridique) est avocate. Elle a rejoint le Bureau au printemps 2024. Elle suit principalement des dossiers de conseils, de projets législatifs et de contrôles préalables dans le domaine de tâches de la DSSI (administration et institutions de santé).

Samuel Kaufmann (collaborateur scientifique, domaine informatique), qui travaille depuis 2016 dans le domaine du développement informatique, est entré au Bureau en 2023 pour suivre les aspects techniques des contrôles préalables.

Michael Weber (collaborateur scientifique, domaine juridique) est avocat et travaille depuis avril 2020 pour le Bureau. 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 dans le domaine de la Direction de l'instruction publique et de la culture.

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.

La révision totale de la LCPD prévoit de transférer au Bureau la tâche de conseiller et surveiller la plupart des communes dans le domaine de la protection des données (voir les points 6.2 et 6.5.3). Selon les renseignements fournis par l'Office des affaires communales et de l'organisation du territoire (OACOT), le canton de Berne comptait en novembre 2024 335 communes municipales et communes mixtes, 182 communes bourgeoises et 241 paroisses. Pour assumer les nouvelles tâches qui lui incomberont à compter de 2026, le Bureau a besoin de quatre postes à plein temps supplémentaires. Il avait inscrit la moitié des charges correspondantes dans le budget 2025 afin de pouvoir échelonner le recrutement et la formation du personnel requis. Mais comme le projet de révision n'avait pas encore été adopté lorsque la Commission des finances a préavisé le budget, celle-ci et à sa suite le Grand Conseil ont biffé l'augmentation des effectifs demandée, invoquant que le Parlement devait d'abord délibérer au sujet de la révision. Bien que cette approche puisse se comprendre, elle appelle néanmoins une réserve. Si la LCPD totalement révisée est adoptée lors de la session d'hiver 2025 et entre en vigueur en juin 2026 comme cela est prévu actuellement, le Bureau ne pourra même pas commencer à recruter en janvier 2026. Par conséquent, dans la mesure où le Grand Conseil approuve le principe du transfert des tâches au Bureau lors de la première lecture du projet en été 2025, le Bureau doit être autorisé à mettre au concours les premiers nouveaux postes et, s'il reçoit des candidatures appropriées, à pourvoir ces postes dès l'automne et l'hiver 2025. Ou alors les dispositions transitoires doivent prévoir que le transfert des tâches n'est pas effectif avant 2027. À défaut, le Bureau ne sera pas en mesure d'accomplir la totalité de ses tâches légales au début.

En 2024, les charges d'exploitation du Bureau se sont élevées au total à 226 000 francs. Environ 80 % de ces charges (180 000 fr.) ont été occasionnées par des prestations externes ayant servi aux contrôles informatiques.

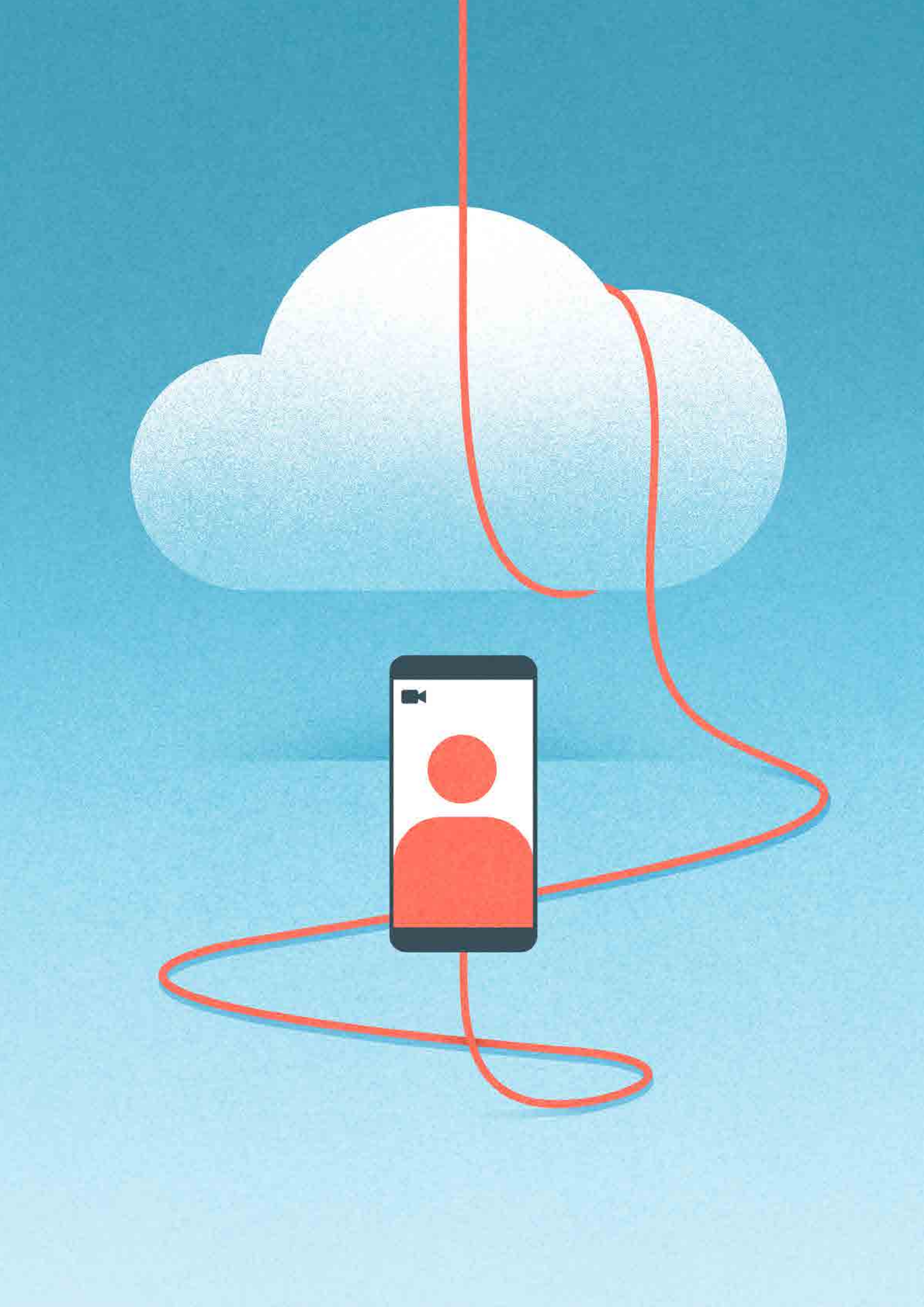
Au sein de l'administration cantonale, d'autres organismes se chargent de conseiller les autorités dans le domaine SIPD. Les Directions et la CHA disposent chacune d'au moins un organe de référence pour la protection des données, qui conseille leurs offices, et d'une ou un responsable de la sécurité de l'information (RSI BE). Les autorités communales peuvent s'adresser à l'OACOT pour les questions de protection des données d'ordre général, aux Directions et à la CHA pour les questions particulières (p. ex. concernant la numérisation à l'école obligatoire). Soucieux de développer la prise de conscience et les connaissances de toutes les autorités dans le domaine de la protection des données, le Bureau a convié cette année encore tous les organes de référence à une présentation technique approfondie, suivie d'une discussion, concernant la communication de données par les autorités. Il a en outre proposé aux membres du personnel de la DIJ, de la FIN et de la CHA, à la demande de leurs RSI BE respectifs, une introduction à la protection des données.

Le Bureau accorde par ailleurs une attention spéciale aux contacts institutionnels avec les autorités qui sont régulièrement confrontées à des questions

compliquées relevant du droit de la protection des données (p. ex. Office d'informatique et d'organisation [OIO], Bedag Informatique SA, Police cantonale [POCA] et Groupe de l'Île).

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 est régulièrement en contact avec ses homologues des autres cantons et avec le PFPDT. Il s'agit, d'une part, de garantir l'échange de savoirs et d'expériences sur 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 déléguée à la protection des données suppléante et responsable juridique 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 2024 sous le point 6.6 plus bas.



6 Présentation des tâches quotidiennes

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

6.1 Conseils

6.1.1. Conseils à l'intention des autorités

Niveau de protection adéquat pour le transfert de données personnelles aux États-Unis

Sur le modèle de l'Union européenne (UE), la Suisse a conclu avec les États-Unis un cadre pour la protection des données (*Swiss-US Data Privacy Framework*) qui donne aux entreprises de ce pays la possibilité d'obtenir une certification si elles respectent un ensemble d'exigences en matière de protection des données. En août 2024, le Conseil fédéral a estimé que ce nouveau cadre offrait un niveau de protection adéquat pour le transfert de données personnelles vers des entreprises certifiées aux États-Unis. Même si la LCPD, qui exige elle aussi un niveau de protection adéquat dans le pays de destination pour que des données personnelles puissent être transférées à l'étranger (en particulier en cas d'utilisation de services en nuage étrangers), ne se réfère pas expressément au droit fédéral, elle a néanmoins la possibilité de s'en inspirer. L'OIO a soumis au Bureau pour avis préalable sa note d'information à ce sujet destinée à l'administration cantonale. Ce dernier lui a indiqué que, comme les entreprises américaines ont la possibilité de révoquer elles-mêmes leur certification à tout moment, il faut prendre deux mesures pour pouvoir utiliser les services en nuage d'une entreprise de ce pays. Premièrement, il faut s'assurer régulièrement que la certification est en cours de validité afin de pouvoir constater au plus vite son éventuelle suppression. Deuxièmement, il faut avoir préparé un scénario de sortie en cas de révocation de la certification afin de pouvoir mettre immédiatement fin à l'utilisation des services en nuage concernés.

Mise en place d'un filtre de Bloom chez une tierce partie de confiance

Un institut de l'Université de Berne (UniBE) a voulu savoir si les médecins ont le droit d'anonymiser les données de leur patientèle en recourant à une tierce partie de confiance. Une ou un auxiliaire aurait généré une valeur de hachage, c'est-à-dire une valeur numérique univoque, pour les données de la patientèle « nom »,

« prénom », « date de naissance » et « genre ». Cette valeur aurait accompagné les données relatives à la maladie communiquées à l'institut. Celui-ci aurait été dans l'incapacité de retrouver l'identité des personnes concernées tout en conservant la possibilité de s'assurer de l'absence de doublons dans les jeux de données.

Les médecins sont tenus par le droit de la protection des données et par le droit pénal de traiter les informations de manière confidentielle et de protéger les secrets. Ils ont le droit de faire appel à des auxiliaires, mais ils doivent mettre un soin particulier à les sélectionner, à les instruire et à les contrôler. Il est important que les devoirs des auxiliaires soient réglés dans des contrats leur imposant de ne pas divulguer les secrets qui leur sont confiés. Ainsi, une question s'est posée lors de l'analyse de la solution comportant une tierce partie de confiance qui a été réalisée avec l'accompagnement du Bureau : comment les médecins pourraient-ils honorer leur obligation de sélectionner, instruire et contrôler les auxiliaires sans prendre le risque de divulguer des secrets et, ainsi, de commettre un acte répréhensible ? Au final, l'autorité concernée a décidé de ne pas recourir à cette solution.

Compétence légale pour surveiller les registres médicaux

Le Bureau et le PFPDT ont étudié avec l'UniBE quel était le droit de la protection des données applicable aux registres médicaux tenus par l'UniBe pour l'ensemble de la Suisse et quelle autorité était compétente en matière de surveillance de la protection des données. Quatre constellations de traitement ont été distinguées : l'UniBE peut mener ses propres travaux de recherche, elle peut accomplir une tâche publique pour le canton ou pour la Confédération et elle peut agir sur mandat de personnes privées. L'étude a déterminé quel était le droit de la protection des données applicable et qui était l'autorité de surveillance compétente dans chacune de ces constellations et de quelle constellation relevait chaque registre. Ce travail a permis de définir clairement les compétences légales et l'attribution des registres.

Communication de données de l'Assurance immobilière Berne aux autorités fiscales

En vue d'une modification législative, l'Intendance cantonale des impôts (ICI) examine s'il faut à l'avenir calculer la valeur officielle des immeubles en se basant sur la valeur assurée auprès de l'Assurance immobilière Berne (AIB). Pour travailler sur cette nouvelle méthode de calcul, l'ICI a demandé à l'AIB une sélection de données personnelles au titre de l'entraide administrative. Interrogé à ce sujet par la DEEE en sa qualité d'autorité de surveillance de l'AIB, le Bureau a établi que la communication des données demandées était possible en vertu des bases légales existantes et plus spécialement de l'article 15 LCPD, qui permet le traitement de données personnelles dans un but sans relation directe avec les

personnes intéressées. L'AIB a néanmoins décidé, par précaution, de ne pas communiquer à l'ICI les données demandées. La FIN prévoit donc d'édicter une ordonnance exploratoire relative à un nouveau système d'évaluation officielle qui habilite et oblige expressément l'AIB à communiquer ces données.

Une deuxième demande adressée au Bureau, cette fois par l'AIB elle-même, portait sur la divulgation des valeurs d'assurance immobilière aux fins du calcul de l'impôt sur les résidences secondaires, sachant que la loi sur les impôts habilite les communes à régler la perception de cet impôt par voie de règlement. Selon le Bureau, la valeur d'assurance d'un bâtiment regroupant plusieurs logements, qu'il comprenne ou non des résidences secondaires, n'est pas une donnée personnelle car la valeur globale d'un immeuble ne contient pas d'informations sur une personne précise. Sa divulgation ne donne donc pas à la commune d'informations relatives à des personnes dont le logement n'est pas une résidence secondaire, informations dont la commune n'a pas besoin. Il en va autrement de la quotepart de chaque propriétaire d'une résidence secondaire à la valeur globale de l'immeuble. Avant de communiquer ces données, l'AIB doit donc s'assurer auprès de la commune qui les demande qu'elles seront utilisées exclusivement pour calculer l'impôt sur les résidences secondaires. Ce point a d'ailleurs été spécifié dans les explications relatives au règlement que la commune concernée a adopté dans l'intervalle.

Projet de coordination matérielle avec la Commission cantonale d'éthique de la recherche

Les autorités cantonales qui font de la recherche rentrant dans le champ d'application de la loi relative à la recherche sur l'être humain ont besoin d'une autorisation de la Commission cantonale d'éthique de la recherche (CCER). Elles doivent également soumettre au Bureau leur documentation SIPD pour contrôle préalable, pour autant que les conditions légales soient remplies. Les deux autorités vérifient la sécurité du traitement des données personnelles dans le cadre de leurs tâches légales respectives. En raison de ce chevauchement de compétences, le Bureau et la CCER ont envisagé une coordination matérielle, mais ils ont finalement décidé de ne pas s'engager sur cette voie. En effet, seule une fraction des demandes traitées par la CCER aurait effectivement entraîné un chevauchement de compétences si bien que la coordination entre les deux autorités aurait représenté une charge de travail disproportionnée pour la commission. En contrepartie, les deux autorités sont convenues d'intensifier leurs échanges techniques.

Consentement des personnes concernées à un niveau inférieur de protection des données

Un hôpital a demandé au Service du médecin cantonal à être globalement exempté de l'obligation de respecter les exigences en vigueur en matière de

sécurité des données parce qu'il voulait communiquer avec sa patientèle par courriel, SMS ou WhatsApp. En contrepartie, les personnes concernées auraient signé une déclaration de consentement. Le Bureau a estimé qu'il n'était pas admissible d'abaisser de manière générale le niveau de sécurité des données en se fondant sur le consentement de toutes les personnes concernées car une telle démarche ne repose sur aucune base légale. En vertu du droit à l'autodétermination informationnelle, les personnes concernées peuvent certes consentir à un niveau de protection inférieur dans un cadre restrictif, mais cela ne doit pas avoir pour effet qu'une autorité se dispense de manière générale de prendre les mesures de sécurité exigées par la loi car, dans ce cas, le consentement n'a pas le caractère facultatif requis pour être valable. Il est possible de communiquer des données de santé sous une forme non sécurisée uniquement si la personne concernée en a fait la demande expresse de son propre chef.

Communication d'initiales aux pharmacies pour lutter contre la falsification d'ordonnances

Une pharmacie située près de la frontière du canton de Berne a demandé au Bureau pourquoi le Service pharmaceutique cantonal bernois, pour lutter contre la falsification d'ordonnances, lui communiquait seulement les initiales des personnes ayant tenté d'obtenir des médicaments au moyen d'une ordonnance falsifiée. Elle précisait que les services pharmaceutiques de son canton et d'un autre canton limitrophe lui fournissaient des noms entiers. L'enquête du Bureau a montré que les pharmaciennes et pharmaciens bernois étaient tenus par la loi de ne pas honorer les prescriptions médicales falsifiées et de les signaler à l'Office de la santé. Toutefois, aucune base légale ne permet au Service pharmaceutique cantonal de communiquer ces informations à l'ensemble des pharmacies bernoises ou proches de la frontière cantonale pour les alerter. La communication des initiales apparaît au Bureau comme un moyen pragmatique et licite de lancer néanmoins une alerte. Les initiales communiquées sont un pseudonyme et la clé permettant de retrouver l'identité d'une personne déterminée ne sort pas du Service pharmaceutique. Le pseudonyme n'est décrypté par la personne concernée elle-même que si celle-ci tente d'utiliser l'ordonnance falsifiée. Sinon, c'est-à-dire dans la plupart des cas, l'alerte reste sans lien avec une personne déterminée.

Utilisation de Microsoft Bing Copilot pendant les cours à l'Inforama

L'Office de l'agriculture et de la nature a demandé au Bureau si le personnel enseignant et les élèves pouvaient utiliser Microsoft Bing Copilot (anciennement Bing Chat Enterprise, BCE) pendant les cours. Le copilote Bing est une application d'intelligence artificielle générative qui aide à produire des textes. Il ressort des recherches menées par le Bureau que les données des utilisatrices et utilisateurs et des entreprises sont protégées dans la version sous licence entreprise et que

les données des chats ne sont pas sauvegardées. Le Bureau en a conclu que le copilote Bing présenté dans la documentation pouvait être utilisé dans le cadre des licences existantes pour Microsoft 365 (M365) dans la mesure où les conditions d'utilisation établissent qu'il est interdit d'entrer des données personnelles lors de son emploi. L'Inforama a intégré des dispositions dans ce sens dans ses instructions relatives à l'utilisation d'applications interactives à l'intention du personnel, du corps enseignant et des élèves.

Faut-il une base légale expresse pour les procédures d'appel dans eBau?

Afin d'assurer l'exécution de la loi cantonale sur l'énergie et d'accomplir ses tâches dans le domaine de la protection de l'air, l'Office de l'environnement et de l'énergie (OEE) a besoin de données matérielles et de données personnelles enregistrées par les communes dans le système de procédure électronique d'octroi du permis de construire (eBau). L'OEE a demandé au Bureau quelle sorte de base légale était requise pour accéder aux données d'eBau. Pour obtenir des données personnelles dans des cas individuels (entraide administrative), il suffit en principe que l'autorité à qui sont destinées ces données en ait besoin pour accomplir une tâche légale. En l'espèce, l'OEE a besoin des données personnelles demandées pour deux de ces tâches : le contrôle des installations de combustion et l'enregistrement des déclarations de remplacement d'un chauffage. Si l'accès aux données en procédure d'appel est proportionné et ne comporte pas de risque particulier pour les personnes concernées, il n'est pas nécessaire que la procédure d'appel repose sur une réglementation expresse. Le Bureau a cependant souligné que la nécessité des données pour l'accomplissement d'une tâche, qui doit avoir un caractère impératif s'agissant de données particulièrement dignes de protection, devait être exposée de manière qualifiée pour qu'une procédure d'appel puisse être considérée comme admissible. Pour des raisons de sécurité du droit et de transparence des traitements de données, le Bureau prône plus généralement l'élaboration d'une réglementation expresse. S'agissant de données personnelles normales, un acte du rang de l'ordonnance suffit.

6.1.2. Conseils à l'intention des personnes concernées

Communication d'une adresse bloquée à des cohéritiers

Une habitante de la ville de Berne avait demandé au contrôle des habitantes et des habitants que son adresse ne soit pas communiquée à des personnes privées. Suite au décès du père de cette personne, la préfecture de Berne – Mittelland a rendu une décision administrative dont tous les membres de la communauté héréditaire ont reçu une copie indiquant leurs adresses respectives

complètes. La personne concernée a dénoncé ce procédé à l'autorité de surveillance. Après étude du dossier, le Bureau a fait les observations suivantes. Suite au décès d'une personne, la préfecture doit prendre contact avec ses ayants droit afin de faire connaître aux membres de la communauté héréditaire leur premiers droits et devoirs (et p. ex. proposer une personne habilitée à dresser des actes authentiques). Pour que la communauté héréditaire puisse agir en main commune, il faut que l'ensemble de ses membres soient impliqués, raison pour laquelle chacun doit savoir qui sont les autres membres de la communauté et avoir la possibilité de les contacter. Dans ce contexte, la communication de l'adresse bloquée était licite. Dans des situations particulières, il arrive qu'un intérêt prépondérant de la personne concernée (p. ex. sa mise en danger) exclue la communication des données en question. Si des indices dans ce sens s'ajoutent au blocage de l'adresse, la préfecture doit entendre la personne avant de communiquer son adresse afin de pouvoir faire une pesée complète des intérêts en jeu.

Vérification de la nécessité des données demandées dans un questionnaire de santé

Venue aux cliniques dentaires universitaires de l'UniBE (ZMK) pour un traitement d'hygiène dentaire, une personne privée s'est ensuite plainte auprès du Bureau de l'étendue du questionnaire de santé auquel elle avait dû répondre. Après avoir étudié les faits et demandé une prise de position aux ZMK, le Bureau a abouti aux conclusions suivantes. Un traitement d'hygiène dentaire est généralement lié à un diagnostic de médecine dentaire et constitue donc un traitement de médecine dentaire. Bien que les travaux d'hygiène dentaire soient pratiqués majoritairement par du personnel formé agissant sur délégation et non pas directement par la ou le dentiste en personne, les questionnaires d'admission et d'anamnèse restent les mêmes. Le traitement des informations demandées dans le questionnaire de santé dans le cadre de l'hygiène dentaire est donc un impératif pour les ZMK et il est conforme au droit de la protection des données.

Publication des procès-verbaux d'assemblée communale

Bien que les communes du canton de Berne aient encore leur propre organe de surveillance de la protection des données (cf. 6.5.3), le Bureau a fourni des renseignements d'ordre général à des citoyennes et citoyens. Il a ainsi notamment expliqué que les communes étaient autorisées à publier sur leur site Internet les procès-verbaux des assemblées communales. Selon la loi sur l'information et l'aide aux médias (LIAM), les assemblées communales sont publiques. Par ailleurs, la loi sur les communes impose aux communes de consigner les délibérations de l'assemblée communale dans un procès-verbal. Enfin, la LIAM dispose que les autorités informent d'office sur leurs activités d'intérêt général, de préférence sur Internet. L'information est limitée par les intérêts publics ou privés

prépondérants qui pourraient s'y opposer, notamment lorsque des données particulièrement dignes de protection sont concernées.

Anniversaires : indication de l'année de naissance dans le journal de la commune

Le journal d'une commune a félicité l'ensemble des habitantes et habitants de 75 ans ou plus pour leur anniversaire et, à cette occasion, il a publié leur date de naissance. Une personne concernée a dénoncé ce procédé au Bureau, qui, n'étant pas compétent, a transmis la plainte à l'organe communal de surveillance de la protection des données et lui a apporté son soutien en clarifiant les points suivants. La LCPD permet aux communes de prévoir dans leur règlement que la communication systématique de données est autorisée (communication de listes de données). Le règlement de la commune concernée relatif à la protection des données prévoit expressément que des listes de données sont communiquées à la rédaction du journal pour la publication de félicitations à l'occasion des anniversaires. Mais cette possibilité est limitée aux données énumérées dans la LCPD, en l'occurrence l'année de naissance et non pas la date de naissance complète. Il a donc fallu que l'organe communal de surveillance de la protection des données avise le contrôle des habitantes et des habitants qu'il ne devrait plus communiquer à l'avenir que les données autorisées. En outre, le contrôle des habitants, en sa qualité d'autorité responsable, a dû exiger de la rédaction qu'elle supprime intégralement les dates de naissance complètes de ses fichiers et de son site Internet.

Communication par courriel crypté en cas d'obligation particulière de garder le secret

Une personne privée n'ayant pas apprécié qu'un notaire lui ait communiqué des projets de contrat par courriel non crypté, elle s'est renseignée auprès du Bureau sur la licéité de cette démarche. Dans le cadre de l'exercice de leur activité professionnelle principale, les notaires sont considérés comme des autorités et sont donc assujettis à la LCPD. Selon la LCPD, les mesures de protection à prendre dépendent du risque encouru par la personne concernée. Par principe, les données particulièrement dignes de protection ne peuvent être transmises que sous une forme cryptée. Du point de vue de la protection des données, c'est donc le contenu concret des contrats qui détermine si le courriel doit être crypté ou non. Toutefois, les notaires sont soumis au secret professionnel en vertu du Code pénal suisse. Ce seul fait leur impose, de l'avis général de la doctrine et de la jurisprudence, de communiquer sous forme cryptée. Si la personne privée avait exprimé le souhait de communiquer sous une forme non cryptée, cela aurait été licite (cf. 6.1.1). Dans le cas contraire, les données couvertes par une obligation particulière de garder le secret doivent être communiquées sous une forme cryptée, quelle que soit leur qualification au regard du droit de la protection des données.

Visibilité du statut sur MS Teams dans l'administration cantonale

Un membre du personnel cantonal a demandé au Bureau s'il était licite que son statut dans la nouvelle application MS Teams (disponible, occupé, absent, etc.) soit visible pour ses supérieures et supérieurs – de même d'ailleurs que pour l'ensemble du personnel cantonal – et permette ainsi une surveillance totale. En ce qui concerne la visibilité des entrées du calendrier dans MS Outlook, le Bureau avait exigé que celle-ci soit désactivée par défaut afin que chaque utilisatrice ou utilisateur doive paramétrer lui-même qui a accès à quelles entrées (rien, seulement créneaux horaires libres et occupés, objet/lieu, contenu). Le calendrier présente deux différences importantes avec Teams. Premièrement, il est avant tout un outil d'organisation personnelle du travail et pas un moyen de communication. Deuxièmement, les entrées du calendrier peuvent être consultées sans limite de temps, c'est-à-dire aussi bien pour le passé que pour l'avenir, si bien que le calendrier est susceptible de divulguer beaucoup plus d'informations que le statut momentané sur Teams. A contrario, Teams est un moyen de communication. Savoir si un membre du personnel cantonal est joignable à un instant donné est une information utile. Comme Teams affiche uniquement le statut au moment considéré, il faudrait que des tiers observent une personne déterminée en permanence pour pouvoir établir son « profil de travail ». Mais surtout, chaque utilisatrice et utilisateur peut à tout moment modifier son statut manuellement et donc décider quel statut est affiché dans Teams.

Pas d'obligation de communiquer une adresse électronique à la commune de domicile

Depuis février 2024, les communes peuvent enregistrer et utiliser l'adresse électronique de leurs habitantes et habitants en vertu de l'ordonnance sur l'établissement et le séjour des Suissesses et des Suisses (OES). Dans sa lettre d'information, une commune a donc demandé à ses habitantes et habitants de lui communiquer leur adresse électronique afin qu'elle puisse leur envoyer ses factures et le courrier courant par voie électronique uniquement. Cela a conduit un citoyen à demander au Bureau s'il était licite que la commune ne veuille communiquer que par voie électronique et s'il était tenu de lui indiquer son adresse électronique. Il n'est pas obligatoire de fournir une adresse électronique à sa commune. L'OES crée une possibilité supplémentaire pour les communes, mais en aucun cas une nouvelle obligation pour les habitantes et les habitants. Le rapport explicatif concernant l'OES est clair à ce sujet : « Cela ne signifie bien sûr pas qu'il soit obligatoire de posséder une adresse électronique ou un téléphone portable, ni de communiquer cette adresse ou le numéro de téléphone. Pour la commune, disposer de telles données permet toutefois une prise de contact simple et rapide avec la personne concernée en cas de besoin. »

6.1.3. Formation continue

Contribution à la formation du personnel communal et paroissial

Le Bildungszentrum für Wirtschaft und Dienstleistung (bwd) propose différentes formations à l'intention des personnes travaillant pour des autorités communales ou paroissiales. Cela fait de nombreuses années – et 2024 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 », de la formation du personnel administratif des écoles de langue allemande et du personnel des secrétariats de paroisse. De plus, une formation consacrée à la protection des données dans les paroisses est proposée aux autorités paroissiales depuis 2021. Au cours de cette formation, les intervenantes et 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.

Au printemps 2024, le délégué à la protection des données a participé pour la première fois à la nouvelle formation continue pour le personnel communal francophone organisée par le Centre de formation professionnelle Berne francophone (ceff) à Tramelan, dans laquelle la protection des données et la sûreté de l'information sont une discipline d'examen.

Le Bureau s'est également adressé au personnel communal à l'occasion d'un séminaire du GAC Berne, dans le cadre de la conférence sur les médias et l'informatique organisée par le Département des écoles de la ville de Bienne et lors d'une rencontre de réseautage proposée par la préfecture de Berne – Mittelland.

Diffusion de connaissances lors d'événements spécifiques

Des représentantes et des représentants du Bureau ont été sollicités pour participer à différents congrès et formations continues. Ils se sont exprimés sur les principes de la protection des données (perfectionnement proposé par l'Office des écoles moyennes et de la formation professionnelle ; Conférence des écoles professionnelles du canton de Berne; gymnase de Neufeld), mais aussi sur des sujets plus spécifiques (la protection des données dans le contexte des achats publics lors d'un congrès d'Educa ; la communication de données en Suisse et à l'étranger dans le cadre de la 17e Journée suisse du droit de la protection des données de l'Université de Fribourg ; les échanges de données avec des fournisseurs de prestations, notamment privés, par delà les frontières cantonales lors du forum Schulthess de 2024 sur la protection des données dans les villes et les communes).

Guide pour les échanges d'informations entre les autorités

Le guide pour les échanges d'informations entre les autorités, qui datait de 2012, a été remanié et publié dans sa nouvelle version sur le site du Bureau en novembre 2024. Il explique de manière aussi claire que possible quand et comment les autorités cantonales et communales peuvent ou doivent échanger des informations entre elles.

6.2 Prises de position formelles

Révision totale de la loi cantonale sur la protection des données

Après la consultation relative à l'avant-projet de révision totale de la LCPD en 2023, le Bureau a eu une nouvelle occasion de donner son avis durant l'année sous revue, lors de la deuxième procédure de corapport. Malgré ses nombreuses propositions concernant la loi et le rapport (majoritairement des points de technique juridique), le Bureau a estimé que, globalement, le projet avait été élaboré avec grand soin et qu'il était abouti sur les points essentiels. En ce qui concerne le projet adopté par le Conseil-exécutif à l'intention du Grand Conseil le 13 novembre 2024, le Bureau a essentiellement les remarques ci-après à apporter.

Le registre des fichiers des autorités cantonales tenu par le Bureau sera allégé : seuls les fichiers contenant des données sensibles (anciennement « données particulièrement dignes de protection ») y seront inscrits. L'administration espère que sa charge de travail en sera réduite. Le registre consultable en ligne constitue, pour les personnes concernées, un point de départ important pour exercer leur droit constitutionnel à la consultation de leurs données, à leur rectification et à leur suppression si elles n'ont pas ou plus d'utilité. Ce droit est acquis pour toutes les données personnelles, quel que soit le niveau de protection dont elles sont dignes. Si le registre est limité aux fichiers contenant des données sensibles, les citoyennes et les citoyens seront privés de la possibilité de se renseigner de manière autonome sur les fichiers existants, leur base légale, le but de leur traitement et la communication de leurs données à des tiers. De plus, la nouvelle loi obligera les autorités à fournir des informations plus étendues sur les données personnelles qu'elles se procurent. Or, l'autorité peut renoncer à l'information lorsque la personne concernée dispose déjà des renseignements nécessaires, par exemple parce qu'ils apparaissent dans le registre des fichiers. Si les fichiers ne contenant pas de données personnelles particulièrement dignes de protection ne sont plus inscrits dans le registre, les autorités auront moins de fichiers à déclarer, mais davantage de travail d'information à faire individuellement auprès des personnes concernées.

Selon le projet de LCPD, le registre devra faire état des systèmes algorithmiques de prise de décision utilisés par les autorités qui présentent un risque élevé pour les personnes concernées. Le projet s'abstient cependant de régler le devoir d'informer lorsque des décisions individuelles pouvant avoir des conséquences significatives pour la personne concernée sont prises de manière automatisée. Le Conseil-exécutif part du principe que les décisions de cette nature donnent toujours lieu à une décision formelle, raison pour laquelle il juge que le devoir d'information doit être réglementé dans la loi sur la jurisprudence et la juridiction administratives. La Confédération, pour sa part, a inscrit le devoir d'information prescrit par la Convention du Conseil de l'Europe révisée dans sa nouvelle loi sur la protection des données. Dans son message, le Conseil fédéral écrit certes lui aussi que les décisions visées revêtent « généralement » la forme de décisions formelles, mais la doctrine relative à la LPD estime unanimement que le devoir d'information s'applique aussi aux autres décisions individuelles automatisées. Le but est que la personne concernée ait la possibilité de faire examiner la décision par une personne physique. De fait, il existe de nombreux domaines dans lesquels les autorités prennent des décisions qui ne constituent pas des décisions formelles et qui pourront être prises à l'avenir en recourant à l'intelligence artificielle (IA), d'autant qu'il existe déjà des applications pour ce faire. On peut citer en particulier la sélection de dossiers de candidature, la correction et la notation automatiques de tests (p. ex. à l'école) ou encore l'appréciation du danger découlant d'une infraction concrète *(predictive policing*) ou du risque de récidive d'une personne ayant commis une infraction. Par conséquent, le Bureau estime qu'il est insuffisant de limiter le champ d'application du devoir d'information aux décisions formelles.

Révision totale de la loi sur l'aide sociale

Le Bureau a rendu un avis circonstancié lors de la consultation concernant la révision totale de la loi sur l'aide sociale, avis qu'il a ensuite publié sur son site Internet après avoir été interrogé à plusieurs reprises à ce sujet et en concertation avec la DSSI, en charge du dossier. Outre des remarques relevant de la technique juridique et de la systématique des lois visant à améliorer la lisibilité du projet, le Bureau a relevé notamment que les membres du personnel des services sociaux étaient tenus au secret en matière d'aide sociale, mais pas au secret médical lorsqu'ils reçoivent des informations de la part de professionnelles et de professionnels de la santé. Ils n'en sont pas moins tenus, avant de faire éventuellement suivre ces informations à des tiers, de procéder à une pesée des intérêts en accordant une importance particulière à l'obligation de garder le secret des professionnelles et professionnels de la santé. Le Bureau a également rappelé qu'il n'est plus possible de parler de « pseudonymisation » lorsque l'on évalue des données personnelles en utilisant le numéro AVS à la place du nom (voir ci-dessous). Il s'agit en fait d'un traitement de données non nominal se rapportant à des personnes, à l'instar de l'évaluation de données secondaires selon la législation sur le personnel. Le Bureau a en outre jugé non admissible que la DSSI ait accès

à des dossiers d'aide sociale individuels pour répondre à des interventions parlementaires ou à des impératifs de communication.

Modification de l'ordonnance fédérale sur la transplantation

Le Bureau a été invité à donner son avis au sujet de la modification de l'ordonnance fédérale sur la transplantation en vue de l'établissement de la réponse du canton de Berne à la consultation. Sur proposition du Bureau, le Conseil-exécutif a indiqué dans sa réponse que la consultation par les membres du personnel de l'Office fédéral de la santé publique de données comportant le numéro AVS comme identifiant personnel ne pouvait pas être qualifiée d'accès limité à des données protégées par des pseudonymes. De nos jours, en effet, les numéros AVS sont utilisés systématiquement comme identifiants personnels dans tellement de domaines administratifs (p. ex. le registre foncier et le casier judiciaire) qu'ils ne répondent plus aux exigences d'une pseudonymisation efficace parce qu'un trop grand nombre d'acteurs ont la possibilité de les relier à des personnes déterminées.

Accès des notaires au système de gestion centrale des personnes

Pour accomplir leurs tâches officielles, les notaires bernois ont accès depuis plusieurs années à certaines données enregistrées sur la plateforme des systèmes des registres communaux (GERES). Mais GERES couvre uniquement les personnes physiques domiciliées dans le canton de Berne, et pas les personnes morales ni les propriétaires fonciers domiciliés hors du canton. C'est pourquoi il est prévu de donner aux notaires un accès au système de gestion centrale des personnes (GCP) de l'Intendance cantonale des impôts. Même si cet accès est légitime sur le plan matériel, le Bureau s'est attaché à vérifier que la méthode employée respectait les prescriptions légales. Alors que l'ordonnance GERES déléguait entièrement la réglementation des droits d'accès aux Directions, à la Chancellerie d'État et à la justice, l'ordonnance GCP définit dans une annexe les autorités qui ont accès au système et les profils dont elles peuvent disposer. Les Directions doivent respecter ce cadre lorsqu'elles réglementent leurs droits d'accès en interne. Autrement dit, pour que la DIJ puisse donner aux notaires un accès à la GCP, il faut d'abord que le Conseil-exécutif complète l'ordonnance afférente. Pour le Bureau, l'accès à la GCP rend inutile l'accès à GERES, raison pour laquelle la DIJ pourra supprimer les droits d'accès des notaires à GERES.

Convention intercantonale sur l'échange de données à des fins d'exploitation de plateformes de recherche et de systèmes de bases de données communs (concordat POLAP)

Une motion de 2018 (18.3592) chargeait le Conseil fédéral de créer une base de données de police nationale et centralisée ou une plateforme reliant les bases de données de police cantonales existantes. La Confédération n'ayant pas la compétence législative pour mettre en œuvre cette motion, les travaux en vue de l'élaboration des bases légales requises pour créer une plateforme nationale de recherche de données policières se déroulent sur mandat de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP). Dans son rapport d'activité 2022, le Bureau avait expliqué au sujet de la révision de la loi bernoise sur la police pourquoi il jugeait hautement problématique que la législation bernoise donne unilatéralement aux autres cantons un accès au système d'information policière du canton de Berne (p. 25). Depuis, le Tribunal fédéral s'est lui aussi exprimé sur cette question au sujet de la loi sur la police du canton de Lucerne : en raison des nombreuses différences voire divergences entre les réglementations cantonales, il ne voit pas comment un système d'information policière commun à la Confédération et aux cantons pourrait être mis en place de façon à atteindre le but visé (jugement 1C_63/2023 du 17.10.2024, consid. 6.5). Le Bureau juge que la formule du concordat est nettement mieux adaptée. D'ailleurs, privatim accompagne depuis plusieurs années les travaux dans ce sens (cf. rapport d'activité 2023 du Bureau, p. 43). Au cours de l'année sous revue, la CCDJP a envoyé en consultation un projet de concordat, sur lequel le canton de Berne a pris position. Après avoir entendu le Bureau dans le cadre de la procédure de corapport, le Conseil-exécutif a proposé que la constitutionnalité du projet de convention soit étudiée dans un avis de droit. Selon lui, il y a lieu en particulier de déterminer dans quelle mesure la convention est compatible avec la répartition constitutionnelle des compétences et si les bases légales qu'elle instaure, en partie par substitution à la loi, sont suffisamment précises pour justifier des atteintes graves à des droits fondamentaux. Le Conseil-exécutif ajoutait que, selon lui, l'absence d'avis de droit à ce sujet compromettrait le processus de ratification dans les 26 parlements cantonaux. Pour le Bureau, il y aurait en outre le risque qu'un concordat ne satisfaisant pas aux exigences constitutionnelles soit invalidé par le Tribunal fédéral.

L'inconvénient de la convention intercantonale réside dans son manque de flexibilité. Une fois qu'elle a été adoptée et ratifiée par les cantons parties, il est extrêmement difficile de l'adapter en fonction de l'évolution des circonstances et des besoins. Il existe une troisième voie, la plus propre mais aussi la plus laborieuse : inscrire dans la Constitution fédérale que la Confédération est compétente pour réglementer la consultation de données policières entre les cantons ainsi qu'entre la Confédération et les cantons. C'est ce que demande une motion (23.4311) que les Chambres fédérales ont adoptée et transmise au Conseil fédéral en juin 2024.

6.3 Contrôles préalables

6.3.1. Projets informatiques

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

En 2024, le Bureau a traité 160 contrôles préalables et premières lectures concernant des projets informatiques (2023 : 133) et en a achevé 90 (2023 : 63).

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.

Système d'information clinique EPIC du Groupe de l'Île

Le contrôle préalable du nouveau système d'information clinique du Groupe de l'Île s'est achevé durant l'année sous revue avec sa troisième itération. EPIC est un système de documentation des traitements qui repose sur une gestion par patient et non plus sur une gestion par cas. Cette nouvelle approche a pour but de faciliter la prise en charge interdisciplinaire. Afin que l'ensemble des sites, cliniques, domaines médicaux et catégories professionnelles puissent collaborer au besoin, la documentation de l'ensemble des traitements sera regroupée dans un dossier central pour chaque patiente ou patient. Il est prévu d'accorder au personnel médical des droits d'accès étendus. Les dix recommandations en suspens à la clôture du contrôle préalable ont été largement appliquées avant la fin de l'année sous revue. Ainsi, le consentement des patientes et des patients à ce que leurs données soient transmises au besoin à des hôpitaux suisses et étrangers utilisant également EPIC a été fortement remanié. De même, la recommandation demandant que les mesures de contrôle prévues à titre de compensation pour les droits d'accès étendus aux dossiers en cours et aux dossiers clos soient activées et leur efficacité contrôlée a été globalement mise en œuvre. L'audit réalisé par le Groupe de l'Île sur la réalisation des mesures de contrôle a

mis en évidence quatre domaines dans lesquels il y avait des progrès à faire. EPIC intègre une plateforme sur laquelle des contenus médicaux sont mis à la disposition des professionnelles et professionnels de la santé sous forme de documents, images, signaux biologiques, fichiers audio et fichiers vidéo (medical content plattform). Le contrôle préalable de cette application spécialisée s'est achevé lui aussi avec des éléments en suspens, dont la résolution a été soumise au Bureau avant la fin de l'année sous revue.

Comme tout contrôle préalable, celui d'EPIC avait un caractère exclusivement documentaire, reposant sur une autodéclaration de l'autorité responsable (situation visée). La mise en œuvre des mesures définies pour protéger les données des patientes et des patients (situation réelle) n'est jamais examinée dans le cadre du contrôle préalable. C'est l'affaire d'éventuels audits ultérieurs.

Interface pour le versement de données dans le dossier électronique du patient

L'interface développée pour l'application spécialisée VacMe afin d'offrir aux habitantes et habitants du canton de Berne la possibilité de verser automatiquement dans leur dossier électronique du patient leur dossier de vaccination contre le COVID enregistré dans VacMe requérait un nouveau contrôle préalable car il s'agit d'une modification substantielle de l'application. Le Bureau a exigé une assurance claire que le transfert porterait exclusivement sur les données des vaccinations contre le COVID pour lesquelles le canton avait coordonné la campagne nationale durant la pandémie, ce qui lui donnait une base légale suffisante (à compléter par le consentement des patientes et des patients), alors que ce n'était pas le cas des autres vaccinations auxquelles VacMe avait été étendu par la suite. Le Bureau a en outre émis de nombreuses recommandations concernant la mise en œuvre technique, que la DSSI, en charge du dossier, a appliquées.

Nouveau système de gestion des cas dans l'aide sociale (démarrage du contrôle préalable)

Le programme NFFS (de l'allemand Neues Fallführungssystem) vise à mettre en place un système de gestion des cas au sein des services sociaux communaux, des autorités cantonales de protection de l'enfant et de l'adulte ainsi que des services spécialisés dans l'intégration. Il s'agit d'un projet de transformation numérique de grande envergure pour le canton de Berne. Il est complexe et coûteux, avec un calendrier ambitieux. Plus de 85 autorités cantonales et communales utiliseront le nouveau système pour traiter un très grand nombre de données personnelles considérées comme particulièrement dignes de protection, ce qui impose des bases légales claires et des exigences accrues à respecter pour les mesures techniques et organisationnelles de protection des données.

C’est pourquoi la DSSI a impliqué le Bureau dans ses travaux à un stade très précoce. Dans un premier temps, le système de gestion des cas sera déployé dans une sélection de services sociaux (phase pilote). Selon le calendrier actuel, il sera étendu aux autres organisations utilisatrices d’ici 2028. Le contrôle préalable du système a pu démarrer vers la fin de l’année sous revue, après des entretiens nourris entre les services de la DSSI impliqués dans le programme NFFS et le Bureau, suite auxquels les documents fournis ont été remaniés et précisés.

Mise en place de M365 par différentes autorités

Comme expliqué dans le rapport d’activité 2023 (p. 27 s.), l’externalisation de traitements de données dans des services de nuage expose les droits fondamentaux des personnes concernées à un ensemble de dangers supplémentaires du fait de la perte de contrôle que cette externalisation fait encourir à l’autorité responsable. Si l’accord Data Protection Addendum de Microsoft, valable internationalement, les contrats cadre également standardisés et d’autres accords complémentaires ont permis d’apporter des réponses générales aux questions que l’utilisation de M365 par les autorités pose du point de vue du droit des contrats, de nombreux autres aspects dépendent de l’utilisation concrète que chaque autorité responsable fait de cette plateforme. D’une part, chaque autorité est un cas à part, avec un mandat légal qui lui est propre, des données à traiter qui ont des caractéristiques particulières (notamment sur le plan de la sensibilité) ainsi que des procédures et donc des besoins de fonctionnement spécifiques. D’autre part, l’introduction de M365 n’implique pas que tous les traitements de données devront être accomplis sur le nuage. M365 regroupe de multiples applications, qui peuvent être utilisées localement (comme les logiciels bien connus de la suite Office que sont Word, Excel, PowerPoint et Outlook) ou qui peuvent être complétées ou remplacées par des services locaux (en particulier pour la sauvegarde des données).

Le fait que des entreprises américaines certifiées en application du cadre pour la protection des données conclu entre la Suisse et les États-Unis offrent depuis la mi-septembre 2024 une protection des données considérée comme adéquate signifie uniquement qu’il est désormais admissible de leur transférer des données personnelles. Cela ne change rien aux autres conditions qui doivent présider à l’utilisation de services en nuage. Les autorités responsables de la protection des données qui envisagent d’utiliser des services en nuage américains doivent vérifier, comme pour tout autre traitement de données sur mandat, si les conditions légales d’une externalisation sont remplies, évaluer les risques associés, ramener ces risques à un niveau supportable par des mesures appropriées et accepter expressément les risques résiduels.

Au cours de l’année sous revue, la POCA et la Caisse de compensation du canton de Berne (CCB) ont soumis au contrôle préalable du Bureau leurs projets respectifs d’introduction de M365 comme solution de bureautique automatisée. À

l'instar de l'administration cantonale, la POCA et la CCB interdisent à leur personnel d'utiliser les services en nuage pour traiter des données personnelles particulièrement dignes de protection. Dans le cas de la CCB, une directive de l'Office fédéral des assurances sociales interdit que les données personnelles de personnes assurées soient traitées à l'étranger si ce n'est en application d'une loi prévoyant un échange international de données. Après application des recommandations du Bureau, les deux projets ont été jugés globalement conformes pour ce qui est de la protection des données.

L'Autorité bernoise de surveillance des institutions de prévoyance et des fondations (ABSPF), qui prévoyait également une migration vers M365, a soumis sa documentation au Bureau pour contrôle préalable. Une question s'est posée : est-il possible d'utiliser la solution de courrier électronique Exchange Online sous la forme d'un service en nuage ? L'ABSPF a expliqué qu'elle ne traitait pas de données personnelles particulièrement dignes de protection pour accomplir ses tâches légales. Mais comme elle ne peut pas empêcher que des tiers lui adressent des courriels concernant des données sensibles dans des affaires pour lesquelles elle n'est pas compétente, ses boîtes mail sont vidées deux fois par jour. Dans ces circonstances, le Bureau a estimé que l'utilisation d'Echange Online était admissible.

Système de gestion du temps de l'Université de Berne sans MS Azure

L'UniBe prévoyait d'adopter un nouveau système de gestion du temps proposé par un fournisseur utilisant la solution en nuage MS Azure. Ce fournisseur étant privé, il avait acheté les services qu'il utilisait sans bénéficier des conditions générales de protection des données ni des accords complémentaires en faveur des pouvoirs publics. Or, ces accords complémentaires (notamment la convention-cadre concernant Administration numérique suisse) contiennent des dispositions particulières régissant le droit applicable et le for juridique en cas de litige (la Suisse au lieu de l'Irlande). Pour que l'externalisation des données ne soit pas préjudiciable aux personnes concernées, le fournisseur devait soit obtenir les mêmes concessions de la part de Microsoft, soit proposer sa solution avec d'autres ressources. Suite à cet avis, le fournisseur a effectué un changement technologique en cours de contrôle préalable afin d'utiliser d'autres ressources que celles de Microsoft.

Étude de cohorte « Bern, get ready » (BEready) de l'Université de Berne

Le Bureau a vérifié si le traitement électronique de données personnelles prévu par l'UniBE aux fins de l'étude de cohorte BEready était conforme au droit de la protection des données. L'étude a pour but de recueillir d'importantes données à long terme sur un échantillon de personnes couvrant la population du canton de

Berne afin d'améliorer les connaissances sur les maladies infectieuses et la capacité à réagir face à de nouvelles menaces sanitaires. BEready porte sur environ 1500 ménages composés d'adultes, d'enfants et d'animaux domestiques dans l'ensemble du territoire du canton. Comme la solution prévue reposait en partie sur des services en nuage de Microsoft, le Bureau a demandé notamment qu'il soit expressément fait état des risques résiduels associés, en particulier le risque de perte de maîtrise vis-à-vis de Microsoft, et que ceux-ci soient acceptés par les instances dirigeantes de l'institut compétentes à cet effet.

Système de gestion SAP : externalisation de traitements de données dans le nuage

La première étape de l'introduction du système SAP en remplacement des systèmes d'information sur les finances (FIS) et sur le personnel (PERSISKA) qui avait été présentée au Bureau reposait exclusivement sur des composants exploités en interne. Dans une deuxième étape, il était prévu de se procurer certains services non plus auprès de la Bedag, mais dans le nuage de SAP. C'est pourquoi l'Administration des finances (AF) et l'Office du personnel (OP) ont soumis au contrôle préalable du Bureau une stratégie générale de sécurisation de l'information en ce qui concerne l'AF et un concept de protection des données pour les premiers processus de gestion du personnel appelés à migrer sur le nuage en ce qui concerne l'OP. Dans les deux cas, il s'agissait uniquement de traitements de données personnelles n'étant pas particulièrement dignes de protection, ainsi que le Conseil-exécutif l'avait prescrit pour l'introduction de M365 dans l'administration cantonale. Les données personnelles présentant un besoin accru de protection ne peuvent pas être traitées dans le nuage de SAP tant que la mise en œuvre de nouvelles solutions techniques probantes (p. ex. des solutions de cryptage) n'est pas attestée. Comme en outre les services en nuage de SAP utilisent une plateforme MS Azure, il a fallu également examiner les risques en découlant. La documentation sur le système d'administration des cours de formation et de perfectionnement internes destinés au personnel cantonal (Learning Management System) présentée par l'OP montrait que les exigences au regard du droit de la protection des données étaient remplies.

Utilisation de WhatsApp dans les processus de recrutement

L'OP s'est adressé au Bureau au sujet d'un projet qui permettrait de déposer des candidatures par WhatsApp. Selon le Bureau, il n'est pas licite de recourir à WhatsApp pour des traitements de données placés sous la responsabilité d'autorités. En effet, lors de l'installation de cette application, toutes les données de contact de l'utilisatrice ou de l'utilisateur sont communiquées à Meta, y compris celles de personnes qui n'utilisent pas WhatsApp et qui n'ont jamais consenti à la communication de leurs données. D'autre part, les données secondaires également transmises sont utilisées par Meta à ses propres fins (p.

ex. pour proposer des « amis » sur d'autres réseaux sociaux), ce qui contrevient au principe du respect de la finalité de la collecte des données. Dès lors que des autorités proposent un canal de communication déterminé, en l'occurrence pour déposer des candidatures, il leur appartient de s'assurer que ce canal peut être utilisé en conformité avec le droit de la protection des données. Les autorités ne doivent pas inciter les personnes à la recherche d'un emploi à violer les droits de la personnalité de tiers, pas plus qu'elles ne doivent tirer profit de violations antérieures de la protection des données. Le Bureau a donc jugé illicite l'utilisation de WhatsApp dans les processus de recrutement. Il a recommandé à l'OP d'envisager plutôt d'améliorer ce qu'il propose déjà pour les candidatures par voie numérique.

Recherche automatisée de véhicules avec enregistrement des passages

Depuis une modification de la LPol entrée en vigueur en août 2024, la Police cantonale peut conserver jusqu'à 60 jours les données de la saisie automatisée de plaques de contrôle de véhicules « à des fins de recherche de personnes ou d'objets et pour déceler, prévenir et poursuivre des crimes ou des délits » et, à certaines conditions, les évaluer ultérieurement (le Bureau a exposé ses réserves de principe à ce sujet dans son rapport d'activité 2022, p. 24 s.). Auparavant, la POCA pouvait seulement comparer ces données avec des bases de données policières et, en l'absence de concordance, elle était tenue de les détruire sans délai. La possibilité de sauvegarder les passages voulue par la révision constituant une modification substantielle du traitement de données, elle a dû être soumise au Bureau pour un contrôle préalable. Celui-ci a notamment recommandé que la suppression des données sur les serveurs de la corporation de droit public Technique et informatique policières Suisse (TIP) soit définie plus en détail. La POCA ayant appliqué les recommandations du Bureau, la mise en œuvre du nouvel instrument a été jugée globalement conforme à la protection des données. Mais dans un arrêt d'octobre 2024 concernant la loi sur la police du canton de Lucerne, le Tribunal fédéral a rappelé que seule la Confédération était compétente pour légiférer dans le domaine de la poursuite pénale et que, par conséquent, les dispositions cantonales régissant la recherche automatisée de véhicules ne sont pas admissibles lorsque leur but premier est la poursuite pénale (cf. arrêt 1C_63/2023, c. 3.5). Or, selon la loi bernoise sur la police, la recherche automatisée de véhicules doit également servir au travail de prévention de la police. Les dispositions en question de la LPol ont elles aussi donné lieu à un recours devant le Tribunal fédéral, qui établira dans quelle mesure la recherche automatisée de véhicules et plus spécialement la mise en réserve de quantités importantes de données sont proportionnées lorsque la prévention est leur seule finalité.

Gestion électronique des dossiers du service de protection des données de la ville de Berne

Le service de la ville de Berne en charge de la protection des données est le FADS (Fach- und Aufsichtsstelle Datenschutz). Le FADS et l'Organe de médiation ont étudié l'introduction d'un nouveau système de gestion électronique des dossiers qui inclut des données personnelles particulièrement dignes de protection et qui, de ce fait, doit être soumis à un contrôle préalable. Mais le FADS, qui est l'organe communal chargé des contrôles préalables, ne pouvait pas examiner son propre projet de traitement de données. Il a donc demandé au Bureau de bien vouloir réaliser ce contrôle. En vertu de la LCPD, le Bureau exerce la haute surveillance sur les autorités communales de surveillance de la protection des données. Il doit en outre collaborer avec les autres organes de surveillance de la protection des données du canton et, moyennant un accord à cet effet, il peut assumer des tâches dans ce domaine dans d'autres collectivités publiques. Sur cette base, le Bureau était disposé à réaliser le contrôle préalable demandé. Ses recommandations concernant la documentation reçue, qui était en ordre comme l'on pouvait s'y attendre, portaient avant tout sur des questions de documentation technique, notamment concernant la séparation des données de plusieurs clients sur le même hôte. Le FADS a appliqué l'ensemble des recommandations du Bureau.

6.3.2. Vidéosurveillance

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

Ainsi, le recours à la vidéosurveillance sous une forme appropriée est considéré comme admissible même en l'absence de base légale explicite s'il est nécessaire pour accomplir des tâches légales (p. ex. surveillance en temps réel en cas de placement dans la salle de réveil d'un hôpital après une intervention).

Protection de base de l'infrastructure de vidéosurveillance de l'Hôpital de l'Île

Les années précédentes, l'Hôpital de l'Île avait soumis au Bureau pour contrôle préalable plusieurs dispositifs de vidéosurveillance implantés sur différents sites, notamment la maison Anna Seiler. C'est la première fois qu'il interrogeait le Bureau sur la protection de base de l'ensemble de son infrastructure de vidéosurveillance. L'examen réalisé n'était donc pas un véritable contrôle préalable car il portait sur une infrastructure déjà en service. Il s'agissait plutôt de créer un socle en vue de procédures ultérieures de contrôle préalable dans le domaine de la vidéosurveillance afin qu'à l'avenir il soit possible de se fonder sur l'infrastructure contrôlée et de limiter les contrôles ultérieurs aux modifications apportées à l'infrastructure ou aux caméras. L'infrastructure de vidéosurveillance d'un hôpital doit être conforme aux exigences de protection accrue des données de la patientèle, qui sont des données personnelles particulièrement dignes de protection et font l'objet d'obligations particulières de garder le secret. L'examen de la documentation n'a pas permis de contrôler définitivement la totalité des aspects parce que les responsables de l'Hôpital de l'Île y ont inclus des références à des documents déposés en 2021/22 pour l'audit de la protection de base des TIC en général. Or, cet audit n'avait pas porté sur l'infrastructure de vidéosurveillance et ses composants, comme le réseau, les serveurs, les clients mobiles et le cryptage, raison pour laquelle il n'a pas été possible de contrôler la situation visée. Il faudra donc passer ces composants en revue à l'occasion d'un prochain audit.

Vidéosurveillance de la commune de Gessenay

L'organe communal de surveillance de la protection des données de Gessenay a demandé au Bureau des conseils en vue du contrôle préalable d'un projet de la commune. Celle-ci avait l'intention de surveiller les entrées et les sorties principales de la vallée avec des caméras de veille panoramique et des caméras de reconnaissance des plaques d'immatriculation pour renforcer le sentiment général de sécurité de la population et aider les autorités de police lorsqu'elles recherchent des personnes ayant commis une infraction. À l'instar de l'organe communal de surveillance de la protection des données, le Bureau a estimé que la vidéosurveillance envisagée n'était pas licite. Le projet était non seulement disproportionné, mais dépourvu de base légale. La LPol permet de mettre en place des dispositifs de vidéosurveillance uniquement dans des lieux délimités où des infractions ont été commises ou peuvent légitimement être attendues (zones prioritaires de criminalité ou de danger). Or, les axes de circulation et les carrefours ne sont pas en soi des lieux particulièrement dangereux, pas plus que l'ensemble du territoire communal. Une vidéosurveillance aussi étendue s'apparenterait à une violation de la substance même du droit fondamental à la protection des données.

Vidéosurveillance d'un point communal de collecte de déchets

Une commune s'est renseignée auprès du Bureau concernant la possibilité de placer sous vidéosurveillance un point de collecte de déchets où des déchets non autorisés sont régulièrement abandonnés. Une telle surveillance suppose que le comportement visé constitue une infraction à prévenir ou à sanctionner. Le Code pénal suisse permet aux cantons d'édicter des dispositions pénales supplémentaires visant à réprimer certains comportements par une amende. Quant à la loi bernoise sur les communes, elle habilite ces dernières à prévoir dans leurs actes législatifs que certaines contraventions sont passibles de l'amende. La commune concernée avait effectivement fait usage de cette possibilité dans son règlement sur les déchets. Elle avait donc en principe la possibilité de mettre en place une vidéosurveillance en vertu de la LPol. Le Bureau a précisé que le contrôle préalable du dispositif incombait à l'organe communal de surveillance de la protection des données.

6.4 Audits

Dans le cadre de son mandat légal de surveillance continue de l'application des prescriptions relatives à la sûreté de l'information et à la protection des données (SIPD), le Bureau a mené huit audits SIPD au cours de l'année sous revue, en se concentrant sur les applications spécialisées essentielles de l'administration et sur le domaine de la santé, conformément à sa stratégie axée sur les risques. Les audits réalisés ont porté principalement sur la protection de base des TIC et des équipements médicaux, c'est-à-dire des appareils utilisés pour les traitements et les diagnostics. Le Bureau a en outre assuré le suivi de la réalisation des mesures SIPD préconisées à l'issue de ses audits des années précédentes. Cet accompagnement continu lui permet de conserver une vue d'ensemble dans la durée.

Dans un environnement très changeant (notamment en raison des projets de numérisation), il est essentiel pour le Bureau de comprendre les défis que les services audités ont à relever. En le contactant à un stade précoce pour bénéficier de son accompagnement dès le départ, les services concernés s'assurent de bénéficier des meilleures conditions pour obtenir une évaluation SIPD qualifiée et utile. Les exigences en la matière sont encore souvent considérées comme des obstacles. Mais il s'agit là d'une vision réductrice car, en réalité, les exigences SIPD jouent un rôle essentiel dans l'identification et la réduction des risques associés au traitement électronique des données. Sans mesures SIPD efficaces, les offres numériques du canton ne pourraient pas résister aux attaques malveillantes. Les pertes de données que le canton subirait de ce fait éroderaient fortement la confiance. Ainsi, la démarche proactive et axée sur les risques mise en pratique par le Bureau contribue à conforter la confiance des citoyennes et des

citoyens dans les offres numériques que le canton leur propose en nombre croissant.

Enseignements généraux

Si des progrès ont pu être observés, force est de constater que les autorités auxquelles des tâches ou des mesures sont préconisées dans le domaine SIPD s'emploient à les accomplir ou à les réaliser avec une diligence variable. Il y a de multiples raisons à cela. Il arrive que les affaires courantes et les projets ne laissent pas suffisamment de ressources disponibles pour mettre en œuvre les mesures SIPD. Parfois, il n'y a pas de pilotage efficace (gouvernance) des exigences dans ce domaine. Un pilotage efficace a besoin d'objectifs mesurables et vérifiables. Avec une gouvernance institutionnalisée, la totalité des exigences et des mesures SIPD bénéficient d'un pilotage systématique. Les audits n'ont pas toujours permis de constater qu'une telle démarche était pratiquée.

En ce qui concerne les hôpitaux, le Bureau a noté, comme les années précédentes, que l'exploitation des équipements médicaux était fortement dépendante des fournisseurs. Les hôpitaux ont relativement peu de contrôle sur l'infrastructure médicale et sur la sécurité de son exploitation. La vue d'ensemble des équipements médicaux critiques n'est pas assurée partout. Il est important de comprendre que l'hôpital responsable doit veiller au respect des exigences SIPD à chaque fois qu'un appareil est évalué, acquis, exploité ou mis hors service.

On constate depuis plusieurs années que les autorités responsables délèguent de plus en plus de tâches SIPD à des prestataires et fournisseurs externes (chaîne logistique). Cette évolution est liée notamment à la transformation numérique et à l'essor des solutions et des services en nuage. Or, les chaînes logistiques externes sont par définition hors du champ d'influence et de contrôle des autorités responsables. Ainsi, on observe que le pilotage et la surveillance des chaînes logistiques dans le domaine SIPD ne sont pas assurés partout de manière vérifiable.

Une autre constatation porte sur la gestion de projets. Lors de ses audits, le Bureau a relevé de manière répétée que les responsables de projet n'assumaient pas la totalité de leurs tâches SIPD lors de l'introduction de nouvelles applications spécialisées. Dans une partie des cas, il n'y avait pas de trace de la transmission des résultats SIPD visés (situation à atteindre) lors du passage de la phase de projet à la phase d'exploitation (clôture du projet pour mise en service). De ce fait, les exigences SIPD et les documents essentiels à ce sujet n'avaient pas été vérifiés ni acceptés en intégralité et n'avaient ensuite été transmis que partiellement aux responsables de l'exploitation. Il y a là un potentiel d'amélioration.

Protection de base de l’infrastructure informatique de la clinique privée Linde AG

Le Bureau a réalisé un audit de la clinique privée Linde AG, qui appartient au groupe Hirslanden, pour vérifier que la protection de base de son infrastructure informatique remplissait les exigences SIPD (normes, cadres de référence, organisation, processus et contrôles). L’évaluation a porté sur les domaines suivants : gouvernance TIC, concepts SIPD et mesures de protection, processus de gestion des utilisatrices et utilisateurs, conservation des données, sécurité des réseaux, sécurité des clients et des serveurs, gestion des changements et des mises à jour, externalisation, sécurité physique des centres de calcul. Ces dernières années, les TIC de la clinique privée Linde AG ont été presque totalement intégrées dans l’infrastructure informatique centrale du groupe Hirslanden.

Des défauts ont été relevés dans presque tous les domaines audités, avec un risque associé jugé moyen ou élevé dans la majorité des cas. L’examen a mis en évidence un manque de clarté dans l’attribution de certaines compétences, l’absence d’instructions à jour et approuvées par le management dans le domaine SIPD, une documentation pas toujours complète et des déficits techniques. Des améliorations sont nécessaires également en ce qui concerne les contrôles et la vision d’ensemble de la chaîne logistique. D’autres constatations portaient sur la gestion de la continuité. Malgré la grande complexité technique et la forte charge de travail des membres du personnel impliqués dans les affaires courantes et dans les projets, le Bureau a pu accomplir sa mission dans un cadre agréable et transparent.

Application spécialisée SUSA de l’Office de la circulation routière et de la navigation

Le Bureau a évalué le respect des exigences SIPD, les processus informatiques et les contrôles SIPD en lien avec l’application SUSA de l’Office de la circulation routière et de la navigation (OCRN). L’audit a porté sur les domaines suivants : externalisation, gouvernance SIPD, concepts SIPD et mesures de protection, gestion des changements et des mises à jour, processus de gestion des utilisatrices et utilisateurs.

Globalement, les défauts relevés sont associés à des risques jugés faibles ou moyens. Il y a une marge de progression en particulier en ce qui concerne les contrôles SIPD auprès des fournisseurs, le pilotage de la gestion des risques et la sensibilisation des membres du personnel. L’audit a pu être réalisé efficacement grâce au concours actif et à la serviabilité du personnel de l’OCRN.

Équipements médicaux des hôpitaux FMI

Le Bureau a audité la protection de base des équipements médicaux des hôpitaux FMI pour évaluer le respect des prescriptions et directives internes (organisation, technique, processus) ainsi que des normes et des cadres de référence dans le domaine SIPD, mais aussi les mesures SIPD déjà mises en place (processus, contrôles, organisation). L'audit a porté sur les domaines suivants : gouvernance SIPD, concepts SIPD et mesures de protection, processus de gestion des utilisatrices et utilisateurs, gestion des changements et des mises à jour, externalisation.

Dans tous les domaines examinés, les défauts constatés étaient majoritairement associés à des risques moyens ou élevés. Il manquait en particulier des directives SIPD agréées. Au moment de l'évaluation, elles n'étaient pas encore validées ni mises en œuvre. Il n'y avait pas non plus de panorama complet et consolidé décrivant l'ensemble des équipements médicaux et permettant d'en assurer la surveillance. L'évaluation a mis en évidence des lacunes dans la traçabilité de la gestion des risques dans les chaînes logistiques et dans l'exploitation des équipements médicaux. Les prescriptions requises dans le domaine de la gestion de la continuité ainsi qu'un test sont en cours d'élaboration. Le Bureau a pu réaliser son audit dans une ambiance constructive et conviviale.

Application de groupe Umantis de l'Office du personnel

Le Bureau a vérifié si l'application de groupe Umantis de l'Office du personnel respectait les exigences SIPD. Cette application gère numériquement toute la chaîne des tâches de recrutement du personnel cantonal. L'audit a porté sur les domaines suivants : gouvernance SIPD, concepts SIPD et mesures de protection, processus d'exploitation, gestion des identités et des accès, externalisation, contrats de prestations, conservation des données et interfaces, gestion de la continuité de l'exploitation et des situations d'urgence.

Des constatations ont été faites dans tous les domaines, avec des risques associés jugés moyens voire élevés. Des améliorations s'imposent en particulier concernant les contrôles auprès des fournisseurs, la mise à jour de la documentation et la gestion de la continuité. L'audit a pu être mené à bien dans une bonne ambiance, grâce au concours d'un personnel chevronné et prévenant.

Systèmes SAP du canton de Berne gérés par l'Administration des finances

L'AF gère le *Customer Center of Expertise* (CCoE) pour les systèmes SAP de l'administration cantonale. Le Bureau a vérifié si ces systèmes respectaient les exigences SIPD concernant l'organisation, les processus et les contrôles en

s'intéressant plus spécialement aux processus de gestion des utilisatrices et utilisateurs. En raison de la criticité des droits d'accès dans l'environnement de base de SAP, le paramètre « SE06 », qui gère la possibilité de modifier le système, a fait l'objet d'une vérification approfondie.

L'examen a mis en évidence des risques moyens et élevés. Il a été possible de déterminer qu'une partie des constatations correspondaient à des points restés en suspens les années précédentes dans le projet d'introduction de SAP. Il y a donc des corrections à apporter dans la mesure où, lorsque les systèmes SAP sont validés pour l'exploitation ordinaire dans l'environnement de production, ils ne devraient plus contenir de rôles ni de droits spécifiques à la phase de projet. L'audit s'est déroulé sur la base d'une coopération excellente et constructive entre le Bureau et les membres du personnel de l'AF responsables du CCoE.

Protection de base de l'infrastructure informatique de l'Université de Berne

Les services informatiques centraux de l'UniBe ont été audités pour évaluer le respect des exigences SIPD dans la protection de base de l'infrastructure (normes et cadres de référence, organisation, processus et contrôles). L'audit a porté sur les aspects suivants des processus centraux : gouvernance SIPD, concepts SIPD et mesures de protection, processus de gestion des utilisatrices et utilisateurs, conservation des données, sécurité des réseaux, sécurité des clients et des serveurs, externalisation, sécurité physique des centres de calcul.

Des risques moyens ou élevés ont été identifiés dans tous les domaines évalués. Les instituts de l'UniBE conçoivent la majeure partie de leur infrastructure informatique de manière autonome, sans intervention directe des services informatiques de l'université, raison pour laquelle les prescriptions SIPD, les processus, les systèmes, les réseaux et les applications sont coordonnés de manière variable et incomplète à l'échelle de l'infrastructure informatique globale de l'université. Cela accroît les risques auxquels l'UniBE s'expose de manière générale dans le domaine informatique. Par conséquent, des changements organisationnels et structurels s'imposent. L'évaluation s'est déroulée dans une ambiance constructive et conviviale, avec des interlocutrices et des interlocuteurs clairement prêts à aider le Bureau à accomplir sa tâche.

Application spécialisée Evidence des préfectures

Les préfectures utilisent l'application spécialisée Evidence pour la gestion électronique de leurs dossiers. Le Bureau a choisi la préfecture de Berne – Mittelland pour y pratiquer un audit représentatif. L'audit a porté sur les domaines suivants : gouvernance SIPD, concepts SIPD et mesures de protection, processus d'exploitation, gestion des identités et des accès, externalisation, contrats de

prestations, conservation des données et interfaces, gestion de la continuité et des situations d'urgence.

Le Bureau a fait des constatations assorties de risques moyens ou élevés dans tous les domaines audités. Des déficits sont apparus dans la gouvernance TIC, la documentation (exhaustivité et actualisation), les contrôles SIPD et la gestion de la continuité. Ces déficits devront être comblés par des actions correctives appropriées. D'un abord agréable et chevronnés, les membres du personnel de la préfecture et les spécialistes de la gestion numérique de la DIJ ont apporté une contribution déterminante à la bonne réalisation de cette évaluation.

Protection de base de l'infrastructure informatique de Spitex Bern

Le Bureau a audité la protection de base de l'infrastructure informatique de Spitex Bern pour évaluer le respect des prescriptions et directives internes dans le domaine SIPD (organisation, technique, processus) ainsi que des normes et des cadres de référence, mais aussi les mesures déjà mises en place (processus, contrôles, organisation). À cet effet, les domaines suivants ont été soumis à une analyse particulièrement approfondie : gouvernance SIPD, concepts SIPD et mesures de protection, processus de gestion des utilisatrices et utilisateurs, conservation des données, sécurité des réseaux, sécurité des clients et des serveurs, gestion des changements et des mises à jour, externalisation, sécurité physique des centres de calcul.

L'audit a mis en évidence des risques en majorité moyens ou élevés. Pour son informatique, Spitex Bern recourt principalement à des fournisseurs et à des prestataires externes. C'est une démarche courante car la fourniture de services informatiques ne fait pas partie du cœur de métier de Spitex Bern. Les risques caractéristiques généralement associés à ce modèle d'externalisation sont notamment l'insuffisance des contrôles et la perte de transparence, concernant par exemple la sécurité et l'actualisation de l'infrastructure informatique mise à disposition. Ce modèle demande en outre une bonne dose de confiance car la majeure partie des connaissances techniques sont externalisées. L'audit s'est déroulé dans une ambiance de convivialité, d'ouverture et de serviabilité exemplaires.

6.5 Autres instruments relevant du droit de la surveillance

6.5.1. Traitement de signalements d'incidents dans le domaine de la protection des données

En vertu de l'ordonnance portant introduction de la directive de l'UE relative à la protection des données à caractère personnel (OiDPD), les autorités du canton de Berne – dans un premier temps celles de la police et de la justice pénale – sont tenues de signaler au service chargé de la surveillance de la protection des données les cas de destruction, de modification ou de divulgation de données à des personnes non autorisées ne résultant pas d'un acte volontaire. Dans le cadre de la révision de la LCPD, il est prévu d'étendre cette obligation à l'ensemble des tâches publiques. Le Bureau recommande d'ores et déjà à toutes les autorités de lui signaler les incidents dans le domaine de la protection des données pour permettre une concertation sur les mesures à prendre, lesquelles peuvent inclure, dans des cas déterminés, l'information des personnes concernées.

Durant l'année sous revue, le Bureau a reçu le signalement de dix incidents, dont un rentrant dans le champ d'application de l'OiDPD (erreur de présentation d'une convocation judiciaire par la poste). Les autres incidents concernaient le détournement du Notebook d'une conseillère par des clients d'une institution d'éducation spécialisée, la publication du dossier d'un patient sur un groupe WhatsApp, l'accès non protégé par Internet à un grand nombre d'informations personnelles sur les élèves d'une institution de formation, l'utilisation d'un outil en ligne pour convertir un fichier contenant les noms de toutes les clientes et tous les clients d'une autorité active dans un domaine sensible ou encore l'accès au compte utilisateur d'une personne auprès d'une autorité par les usagers qui lui succédaient sur le même appareil.

6.5.2. 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 2024, le Bureau n'a pas présenté de proposition formelle et n'a pas formé de recours contre une décision négative d'une autorité responsable.

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

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

Les communes ont choisi des solutions variées pour garantir l'indépendance requise par la loi. Beaucoup de petites et moyennes communes ont désigné leur organe de révision des comptes comme autorité de surveillance. Dans les communes dotées d'un parlement, c'est souvent la commission de gestion qui assume cette fonction. Certaines communes ont mandaté une étude d'avocats spécialisée. La ville de Berne est la seule qui ait son propre bureau de surveillance de la protection des données.

Il en découle que les connaissances des organes de surveillance communaux en matière de sûreté de l'information et de protection des données ainsi que le champ et la qualité des conseils qu'ils peuvent dispenser à leurs autorités communales sont hétérogènes. C'est pourquoi il est prévu, dans le cadre de la révision totale de la LCPD, de confier au Bureau la tâche de conseiller et surveiller la plupart des communes dans le domaine de la protection des données. En attendant, le Bureau ne fait qu'adresser des renseignements aux autorités communales, en rappelant qu'il n'est pas leur autorité de surveillance (et en indiquant l'éventuelle autorité de surveillance communale compétente). Encore ne le fait-il que dans une mesure très limitée faute de ressources en personnel (cf. 6.3.2 concernant la vidéosurveillance dans les communes).

6.6 Coopération intercantonale

Présidence et comité de privatim

Le délégué à la protection des données préside privatim, la Conférence des préposé(e)s suisses à la protection des données, depuis novembre 2020. La conférence a tenu deux assemblées générales durant l'année sous revue. Lors de son assemblée de printemps, elle a apporté différents éclairages concernant les conséquences juridiques d'infractions à la protection des données sous l'angle du droit de la protection des données, de la loi fédérale sur la sécurité de l'information, de la responsabilité de l'État et du droit pénal. Privatim a rédigé un total de onze prises de position en réponse à des consultations de la Confédération et de la CCDJP. Elle en a mis certaines à la disposition de ses membres comme modèle de réponse. La conférence a eu de nombreux échanges avec des organisations ayant une activité intercantonale, notamment Administration numérique suisse, l'agence Educa, la Conférence suisse des offices de la formation professionnelle, le groupe de travail Droit dans l'exécution des peines de la CCDJP et TIP, auxquelles elle a dispensé des conseils sur l'application du droit de la protection des données dans leurs projets respectifs. Cette année encore, privatim a échangé régulièrement avec le PFPDT, notamment pour se concerter au sujet de la consultation concernant le concordat POLAP (cf. 6.2), ainsi qu'avec l'Office fédéral de la justice au sujet d'une simplification du droit de la protection des données et des compétences de surveillance applicables durant la phase pilote d'introduction dans un premier ensemble de cantons de la plateforme justitia.swiss de communication électronique au sein des juridictions.

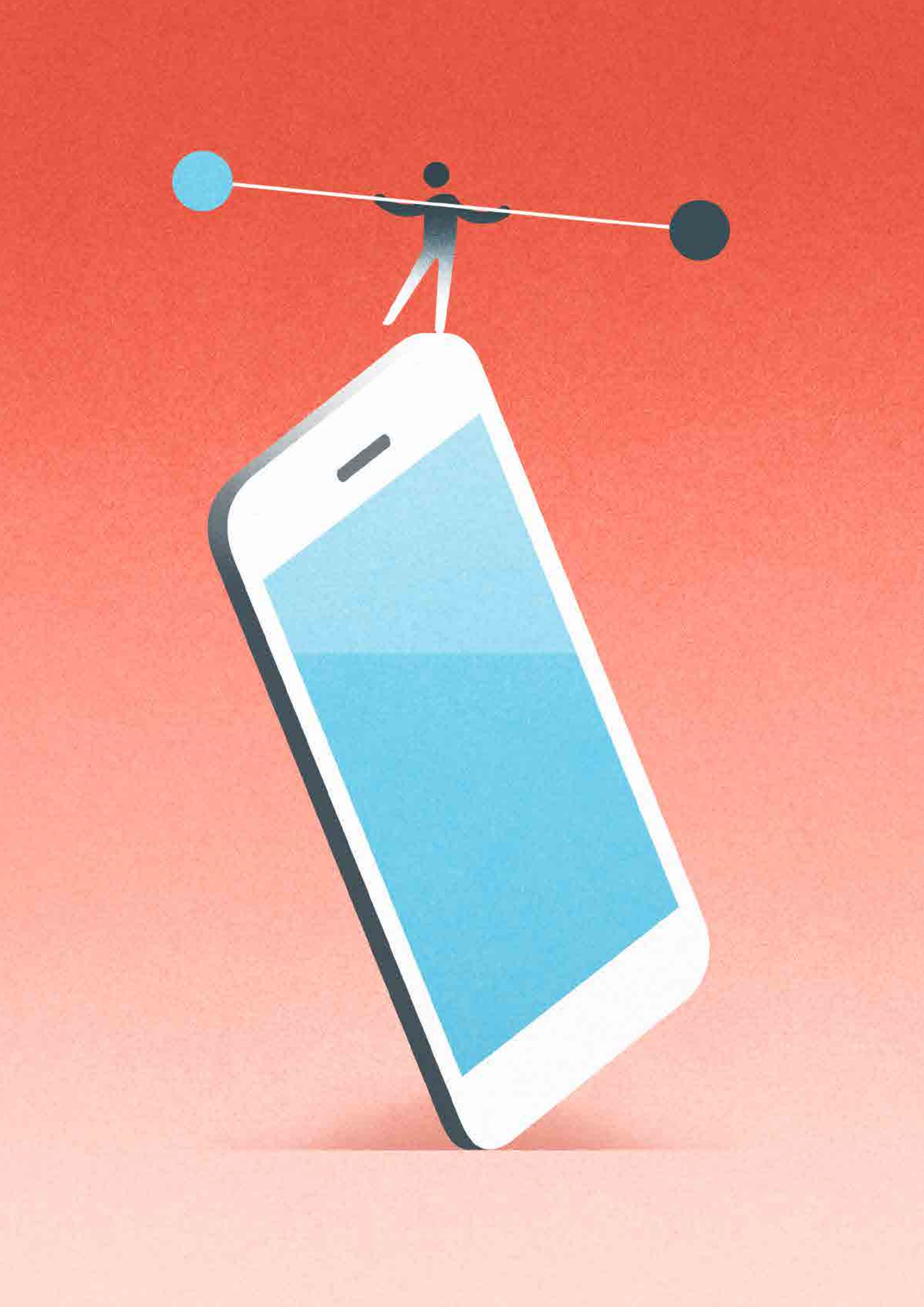
Groupes de travail de privatim

Le *groupe de travail Cyberadministration* s'est réuni à trois reprises, notamment pour étudier le projet Justitia 4.0 d'introduction de la communication électronique au sein des juridictions ainsi que l'accord cadre entre la Suisse et les États-Unis sur la protection des données et la décision d'adéquation afférente du Conseil fédéral.

Le *groupe de travail Sécurité* a accompagné l'association Electronic Monitoring dans ses travaux en vue du renouvellement du système national suisse de surveillance électronique dans l'exécution judiciaire notamment, projet dont il a soumis la documentation SIPD à plusieurs évaluations. Il a également contrôlé le projet de convention de traitement sur mandat entre TIP et un fournisseur de prestations informatiques dans le cadre du projet intercantonal « Integriertes Lagebild 4.0 » et préparé pour le comité de privatim une prise de position en réponse à la consultation sur le concordat POLAP.

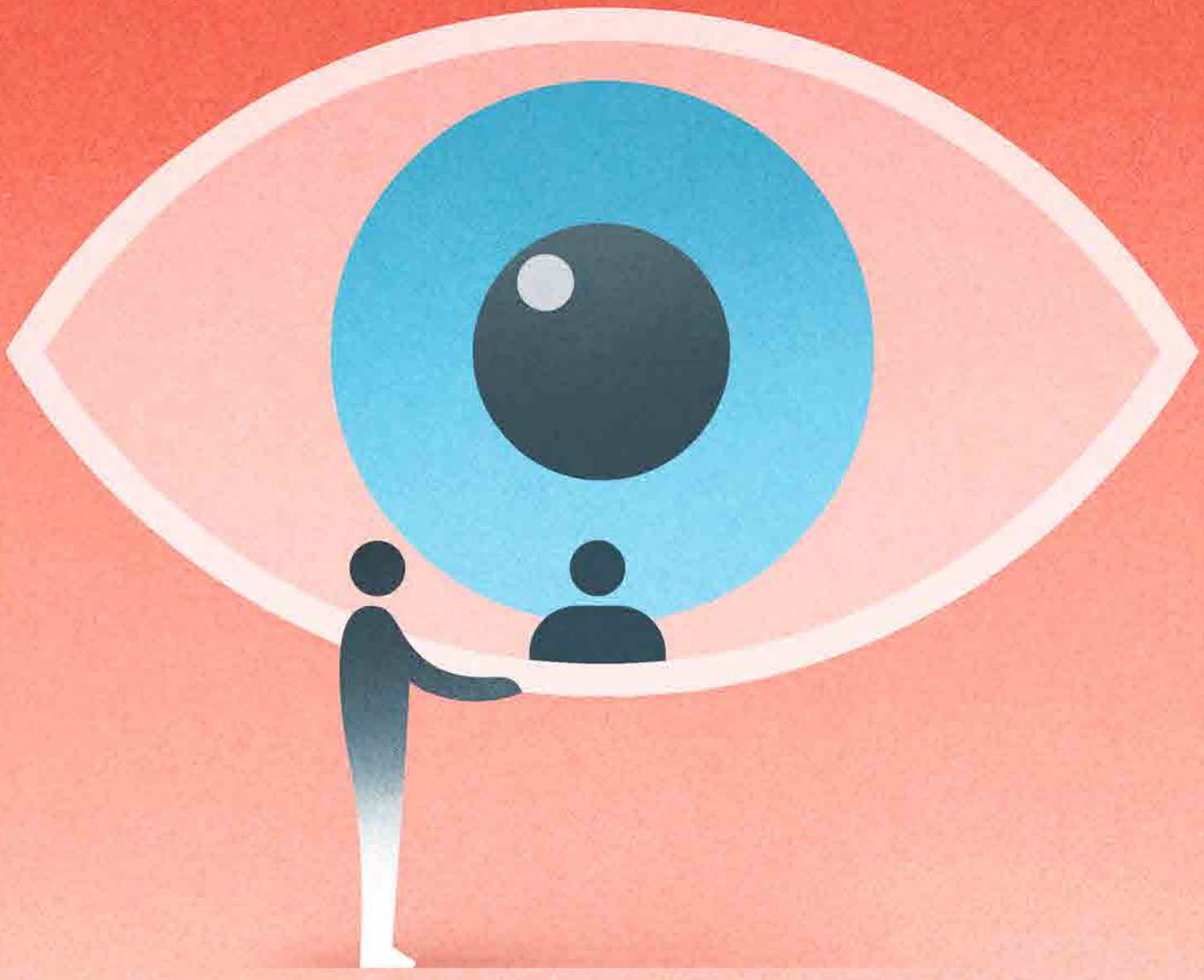
En 2024, le *groupe de travail Santé* s'est réuni sous la direction de la déléguée à la protection des données suppléante et responsable juridique, deux fois à distance et une fois en présentiel. Ses membres ont eu des échanges d'expérience nourris à propos de sujets d'actualité concernant ou susceptibles de concerner plusieurs cantons ou tous les cantons et la Confédération. Suite aux investigations du Bureau concernant les flux de données entre le Service pharmaceutique cantonal et les pharmacies en vue de lutter contre la falsification d'ordonnances (cf. 6.1.1), les membres du groupe de travail ont été invités à vérifier les bases légales et les pratiques pertinentes dans leur domaine de surveillance. Par ailleurs, le groupe a décidé de se doter de connaissances de base spécifiques pour se préparer à faire face à de futures problématiques. Il a ainsi fait venir deux spécialistes pour des exposés sur l'intelligence artificielle dans le domaine de la santé.

Les organes de surveillance qui ont leurs propres spécialistes de la sûreté de l'information les ont délégués pour discuter, au sein du *groupe de travail TIC*, de questions d'actualité et d'évolutions à caractère technique.



7 Proposition

Prise de connaissance.



8 Liste des abréviations, glossaire

ABSPF	Autorité bernoise de surveillance des institutions de prévoyance et des fondations
AF	Administration des finances
AIB	Assurance immobilière Berne
Al.	Alinéa
Art.	Article
AVS	Assurance-vieillesse et survivants
BPD	Bureau pour la surveillance de la protection des données du canton de Berne
C.	Considérant
CCB	Caisse de compensation du canton de Berne
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCER	Commission cantonale d'éthique de la recherche
CCoE	Customer Center of Expertise SAP du canton de Berne
CHA	Chancellerie d'État
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
eBau	Application spécialisée pour l'octroi électronique du permis de construire
FADS	Service de la protection des données de la ville de Berne (Fachstelle Datenschutz)
FIN	Direction des finances
GCP	Gestion centrale des personnes
GERES	Système des registres communaux
LIAM	Loi sur l'information et l'aide aux médias

IA	Intelligence artificielle
IT	Informatique
LCPD	Loi cantonale sur la protection des données
LPD	Loi fédérale sur la protection des données
LPol	Loi sur la police
M365	Microsoft 365
MS	Microsoft
NFFS	Nouveau système de gestion des cas (Neues Fallführungssystem)
OACOT	Office des affaires communales et de l'organisation du territoire
OCRN	Office de la circulation routière et de la navigation
OEE	Office de l'environnement et de l'énergie
OES	Ordonnance sur l'établissement et le séjour des Suissesses et des Suisses
OiDPD	Ordonnance portant introduction de la directive de l'UE relative à la protection des données à caractère personnel
OIO	Office d'informatique et d'organisation
OP	Office du personnel
PFPDT	Préposé fédéral à la protection des données et à la transparence
P.	page
P. ex.	Par exemple
POCA	Police cantonale
POLAP	Plateforme nationale de consultation de données policières
privatim	Conférence des préposé(e)s suisses à la protection des données
RSI BE	Responsable de la sécurité de l'information
S.	et suivante (page)

SIPD	Sûreté de l'information et protection des données
TIC	Technologies de l'information et de la communication
TIP	Corporation Technique et informatique policières Suisse
UE	Union européenne
UniBE	Université de Berne
USA	États-Unis d'Amérique
ZMK	Cliniques dentaires de l'Université de Berne

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