Kanton Bern
Canton de Berne

Rapport d'activité Bureau pour la surveillance de la protection des données 2023

Bureau pour la surveillance de la protection des données Février 2024

Impressum

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

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

Table des matières

1 Avant-propos

En 1974, il y a exactement 50 ans, l'auteur-compositeur allemand Reinhard Mey, connu du public francophone sous le nom de Frédérik Mey, chantait : « Au-dessus des nuages, la liberté semble être infinie ». Aujourd'hui, cette image prend un tout autre sens, évoquant plutôt la tentation que le nuage informatique représente pour l'administration cantonale. L'externalisation du traitement des données dans un nuage ouvre des possibilités qui étaient auparavant inabordables sinon inimaginables. Les services internationaux d'informatique en nuage, qui sont potentiellement à la disposition de l'ensemble des internautes (nuage public), permettent des économies d'échelle grâce à l'attribution dynamique des capacités de calcul et de stockage dont chaque client a besoin au moment considéré, ce qui réduit les coûts d'investissement. Toutefois, le transfert de données personnelles dans une infrastructure dont les autorités responsables ignorent presque tout entraîne des dépendances et des pertes de contrôle dans le domaine de la protection des droits fondamentaux.

C'est pourquoi le Bureau pour la surveillance de la protection des données (Bureau) a été saisi de nombreuses questions concernant l'utilisation de l'informatique en nuage durant l'année sous revue, tant de la part de l'administration cantonale que de l'administration décentralisée. La mise en place des services de la suite Microsoft 365 (M365) a été un thème récurrent. Les risques résiduels associés à l'utilisation prévue de M365 dans l'administration cantonale ont été présentés au Conseil-exécutif, qui les a acceptés. À la fin de 2023, la procédure de contrôle préalable des mesures encadrant cette utilisation dans le but de protéger les droits fondamentaux n'était pas encore achevée. L'Université de Berne et le Groupe de l'Île SA ont eux aussi soumis au Bureau leurs plans respectifs d'introduction de M365. La perte de contrôle est bien moindre dans les services en ligne proposés en Suisse. C'est ce qui ressort de l'examen de la plateforme de participation numérique du canton, à laquelle le fournisseur a apporté des modifications techniques et organisationnelles suivant les préconisations du Bureau.

Un nouveau thème s'est invité à l'agenda de la protection des données : l'utilisation de l'intelligence artificielle (IA) dans le traitement des données personnelles. Les fournisseurs de services d'IA privés, souvent basés sur un nuage, et les personnes privées qui utilisent ces services peuvent généralement opérer en se fondant sur leurs intérêts personnels prépondérants, sur le consentement des personnes concernées et sur des exclusions de responsabilité à caractère contractuel. Ce n'est pas le cas des autorités publiques, qui font face à de nombreuses questions concernant en particulier la légalité, la finalité, la justesse des résultats et la responsabilité.

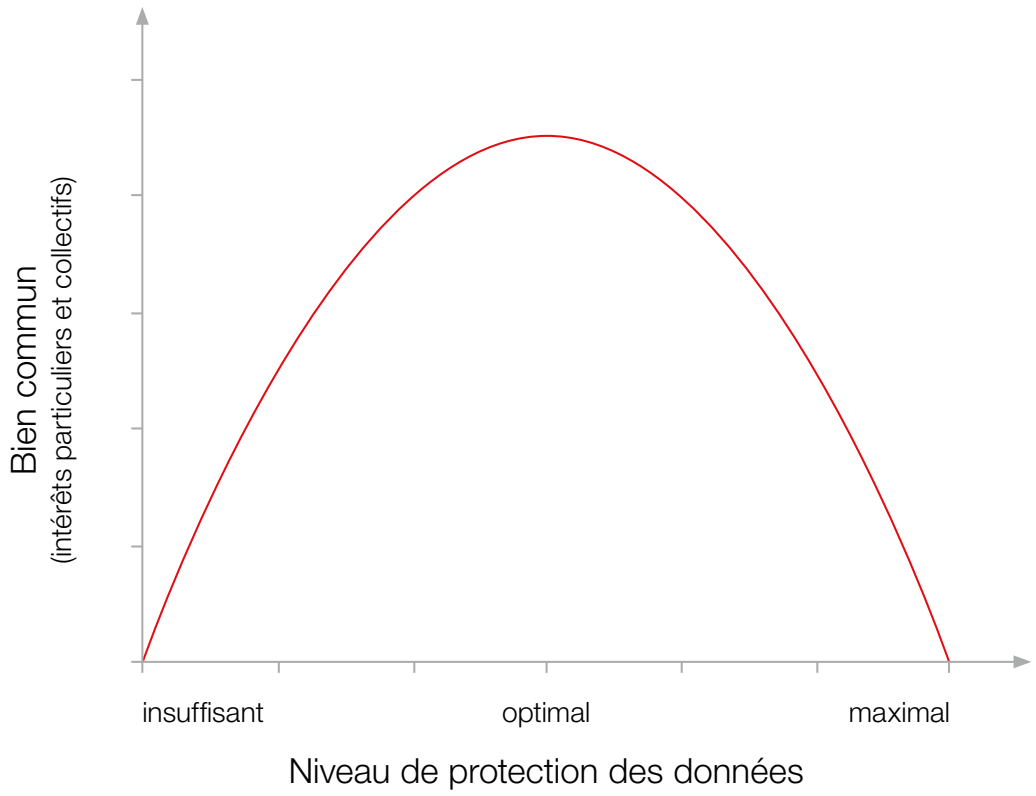
Le présent rapport illustre la grande variété des activités des autorités qui ont soulevé des questions de protection des données dont le Bureau a été saisi dans le cadre de ses activités de conseil et de surveillance durant l'année sous revue.

Ueli Buri, délégué à la protection des données

2 Droit fondamental à la protection des données

La 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.

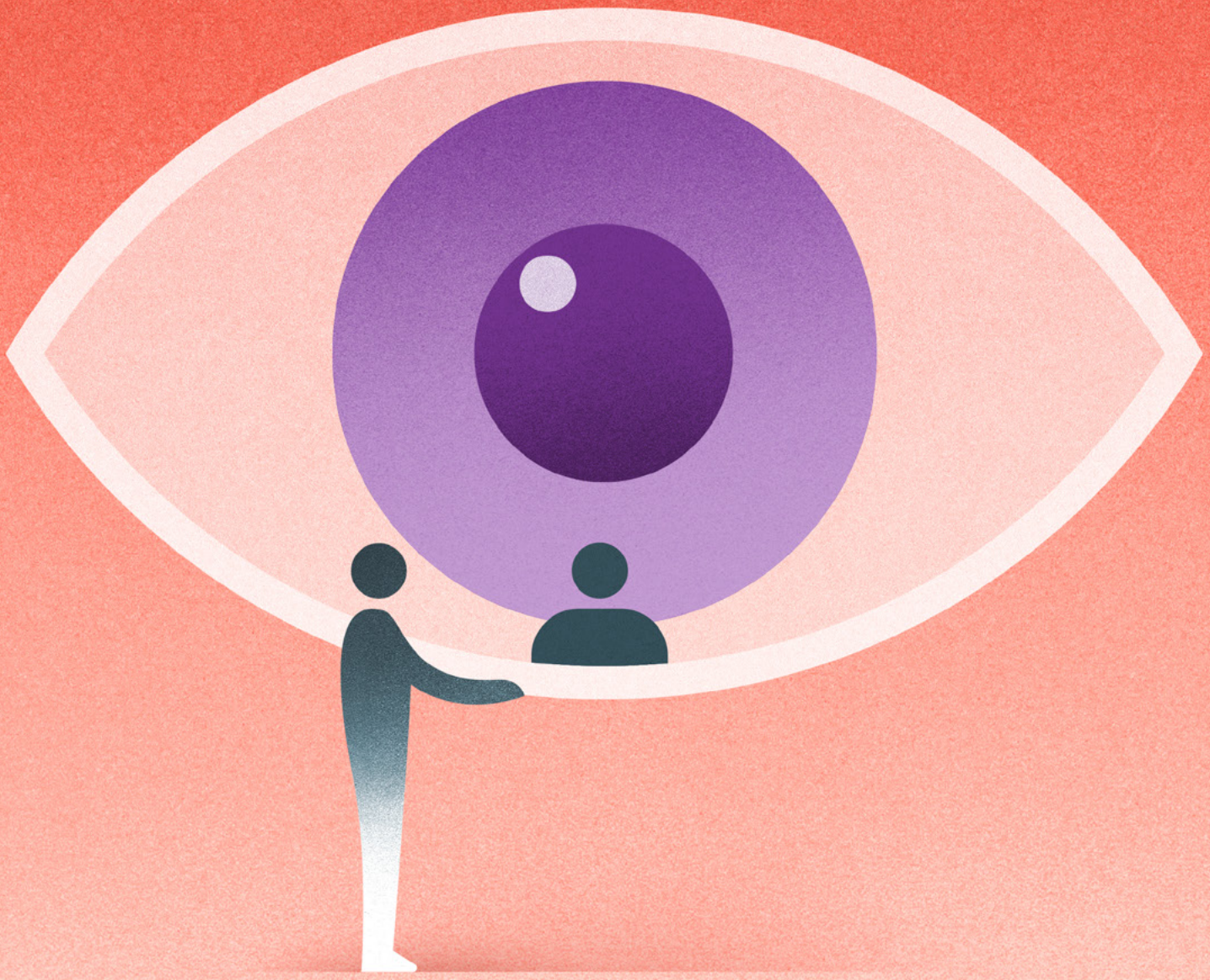
La loi cantonale sur la protection des données (LCPD) précise les devoirs des autorités lors du traitement de données personnelles. Par autorité, il faut comprendre l'administration, mais aussi les autres entités chargées de tâches publiques comme les écoles et les hôpitaux. Quant au traitement, il se 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 2023, le Bureau disposait de 650 pour cent 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, sécurité [DSE]), de la Chancellerie d'État (CHA) et des autorités de justice.

Anders Bennet (délégué à la protection des données suppléant, responsable informatique) est informaticien et assume depuis plus de dix ans une fonction de réviseur informatique 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 et de la Direction de l'économie, de l'énergie et de l'environnement ainsi que de la vidéosurveillance et des questions relatives aux paroisses.

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.

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

Michael Weber (collaborateur scientifique, domaine juridique) est avocat et travaille depuis avril 2020 pour le Bureau. 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.

En 2023, les charges d'exploitation du Bureau se sont élevées au total à quelque 230 000 francs. Environ 80 % de ces charges (environ 182 000 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'Office des affaires communales et de l'organisation du territoire 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 porte un soin tout particulier à son réseau de partenaires au sein de l'administration et s'applique à le développer. En 2023, il a organisé à nouveau deux réunions de tous les organes de référence pour la protection des données et une première rencontre avec les RSI BE des Directions et de la CHA dans le but de renforcer les échanges à la fois entre ces organes et avec le Bureau. Pour vérifier où en était la réalisation de ses objectifs stratégiques, le Bureau a mené une enquête de satisfaction auprès de ses interlocutrices et interlocuteurs principaux dans l'administration cantonale (secrétariats généraux, organes chargés de la transformation numérique, organes de référence pour la protection des données, RSI BE) ainsi qu'auprès des hautes écoles et des institutions de santé. Le taux de retour de 69 %, avec des réponses majoritairement positives et des suggestions constructives, a largement dépassé les attentes.

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 (CF) du canton de Berne et le Bureau ont mis en place une collaboration renforcée sur le plan stratégique.

Membre de privatim, la Conférence des préposé(e)s suisses à la protection des données, le Bureau est régulièrement en contact avec ses homologues des autres cantons et avec le PFPDT. Il s'agit, d'une part, de garantir l'échange de savoirs et d'expériences 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 2023 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

Nouvelle loi fédérale sur la protection des données

La loi fédérale sur la protection des données entièrement révisée est entrée en vigueur le 1er septembre 2023. Elle s'applique uniquement aux autorités fédérales et aux personnes privées qui traitent des données, en particulier à titre commercial, mais pas aux autorités cantonales et communales. Ces dernières sont en principe assujetties uniquement à la LCPD, qui est en cours de révision (cf. 6.2).

Les choses se compliquent lorsque le canton ou une commune délègue une tâche publique à une organisation de droit privé (en vertu de la loi ou d'un mandat de prestations). Dans ce cas, l'organisation devient une « autorité » au sens de la LCPD et elle est assujettie à cette dernière pour tous les traitements de données qu'elle effectue en vue d'accomplir la tâche qui lui a été déléguée. Par contre, parce qu'elle relève du droit privé, elle n'est pas assujettie à la LCPD en ce qui concerne le traitement des données relatives à son personnel.

La situation est encore différente lorsqu'une autorité cantonale ou communale fait appel à une entreprise de droit privé comme auxiliaire pour effectuer des traitements de données dont l'autorité conserve la responsabilité (travail sur mandat). Étant une personne privée, l'auxiliaire est en principe assujetti uniquement à la LCPD. Cependant, l'autorité doit lui imposer dans le contrat de prestation de services l'ensemble des obligations et des interdictions nécessaires pour que les dispositions de la LCPD soient respectées (p. ex. l'interdiction d'utiliser les données à ses propres fins). En effet, il ne faudrait pas que les droits fondamentaux des personnes concernées soient moins bien protégés parce que l'autorité responsable s'adjoint le concours de tiers pour accomplir ses tâches. C'est pourquoi l'article 28 de la nouvelle loi sur l'administration numérique (LAN) impose à l'autorité responsable de s'assurer que la personne mandatée traite les données de la même manière qu'elle-même est habilitée à le faire, que la sécurité des données est garantie et que la personne mandatée ne fait appel à des sous-traitants que si l'autorité responsable y a consenti au préalable. Dans sa version actuelle, la

LCPD prévoit à son article 16 que les personnes mandatées sont soumises au droit cantonal (et donc aussi à la LPD) de la même manière que leur mandant. C'est le seul dispositif légal de ce type en Suisse. Il est prévu de remanier cette disposition dans le cadre de la révision en cours pour aller dans le sens des explications qui précèdent (et de la nouvelle réglementation instaurée à l'art. 28 LAN).

Durant l'année sous revue, la question du droit de la protection des données applicable et donc de la compétence pour surveiller la protection des données a suscité un grand nombre de demandes de la part d'autorités cantonales et communales, de même que des échanges nourris entre les autorités cantonales chargées de la protection des données ainsi qu'entre ces autorités et le PFPDT.

Microsoft 365 dans l'administration cantonale

Les exigences légales à respecter pour faire appel à des auxiliaires s'appliquent également lorsqu'un mandataire fournit ses services à une multitude de clients sous une forme hautement standardisée en se servant de sa propre infrastructure, laquelle est souvent répartie sur plusieurs sites. Lorsqu'elle utilise les services en nuage de géants internationaux comme Microsoft (hyperscalers), l'autorité n'a en général que peu ou pas d'influence sur l'accord contractuel régissant ces services et elle n'a pas non plus les moyens de vérifier si cet accord est respecté. Même si l'accord est conforme à la législation sur la protection des données, ce qui est le cas du contrat-cadre 2022-2025 conclu par la Conférence suisse sur l'informatique auquel le canton a adhéré, l'autorité n'est plus en mesure de contrôler quelles données sont traitées (y c. celles collectées par le fournisseur sur les utilisatrices et les utilisateurs de son nuage), à quel endroit et à quelles fins ces données sont traitées, ni qui peut les consulter (p. ex. des sous-traitants). Lorsque le fournisseur est assujetti à une législation étrangère, par exemple la loi américaine Cloud Act, l'autorité suisse s'expose en outre au risque que des autorités étrangères accèdent aux données dans des conditions non conformes au droit suisse. Cela laisse subsister de multiples risques pour les droits fondamentaux des personnes concernées. Certains de ces risques peuvent être éliminés grâce à des mesures techniques et organisationnelles appropriées, d'autres pas.

Dans la perspective de l'introduction de Microsoft 365 (M365) dans l'administration cantonale, l'OIO et le Bureau se sont réunis à de nombreuses reprises pour discuter des différents risques et des mesures possibles pour les réduire ou les éliminer. Les risques qui subsistent malgré la prise de mesures, en particulier la perte de contrôle vis-à-vis de Microsoft et d'autorités étrangères, l'impossibilité de vérifier les assertions contractuelles, les changements rapides intervenant dans les services et parmi les sous-traitants ainsi que la dépendance accrue envers Microsoft, ont été exposés en détail et sincèrement par l'OIO dans un rapport à l'attention du Conseil-exécutif. Des garde-fous ont été définis pour l'utilisation de M365 : les applications Office (Word, Excel, PowerPoint et Outlook) restent

installées localement et les services en nuage (SharePoint, OneDrive et Teams) ne doivent pas être utilisés pour traiter des données personnelles particulièrement dignes de protection ni des données faisant l'objet d'une obligation particulière de garder le secret (p. ex. dans les domaines de la santé, de l'aide sociale et ou des assurances sociales).

Dans sa prise de position au sujet du rapport de l'OIO, le Bureau note que les risques résiduels ne peuvent être considérés comme supportables et donc être acceptés que si le Conseil-exécutif donne l'assurance que les services en nuage apportent des avantages essentiels par rapport à une solution locale et que ces avantages l'emportent sur les nouveaux risques encourus. Concernant l'exploitation de M365, le Bureau relève en outre que le modèle de la responsabilité partagée est porteur de nouveaux défis, pour lesquels il n'existe pas encore de stratégie éprouvée. Selon ce modèle, en effet, Microsoft peut faire évoluer ses services en permanence et leur apporter une succession rapide de modifications techniques tandis qu'il appartient au canton d'identifier, d'évaluer et de maîtriser les nouveaux risques.

En déclarant par voie d'arrêté qu'il reconnaît et accepte les risques résiduels mis en évidence dans le rapport de l'OIO, le Conseil-exécutif a engagé sa responsabilité, à la fois au regard de la législation sur la protection des données et sur le plan politique.

Lexique de la protection des données pour l'école obligatoire

L'Office de l'école obligatoire et du conseil a démarré en 2020 un projet de révision de ses lignes directrices sur la protection des données à l'école obligatoire, qui dataient de 2009. Dès le départ, le Bureau a participé avec voix consultative à ce projet, qui a demandé un gros investissement à toutes les parties et qui a été mené à bien fin 2023. Publié à l'adresse https://www.lp-sl.bkd.be.ch/fr/start/schulleitungen/datenschutzlexikon.html, le nouveau lexique de la protection des données à l'école obligatoire s'adresse au corps enseignant, aux directions d'école, aux administrations et autorités scolaires, aux spécialistes ainsi qu'aux parents qui ont des questions sur le traitement des données dans le domaine de l'école obligatoire. Il compte actuellement plus de 70 entrées classées par ordre alphabétique présentant l'essentiel des notions, des principes et des informations à connaître dans le domaine la protection des données. Il est accompagné d'une liste des questions les plus fréquemment posées dans la pratique. On trouve à la même adresse trois notices relatives aux services d'informatique en nuage de Microsoft, Google et Apple. Ce lexique a pour vocation d'aider les établissements de la scolarité obligatoire à trouver par eux-mêmes des réponses à leurs principaux questionnements concernant la protection des données dans leur domaine et de développer leurs compétences en la matière.

Publication d'anciens annuaires officiels sur Internet

Une question s'est posée suite à une dénonciation à l'autorité de surveillance : l'Université de Berne dispose-t-elle d'une base légale suffisante pour publier sur Internet des éditions anciennes de l'annuaire officiel du canton de Berne ? L'annuaire officiel contient des données sur les personnes employées par le canton l'année de sa publication, autrement dit des données personnelles. Or, la publication de ces données sur Internet expose les personnes concernées à un danger accru en raison de la possibilité que les données en question soient collectées par des systèmes automatisés n'importe où dans le monde et être réutilisées à n'importe quelles fins, y compris illégales. Au cours des échanges avec l'Université de Berne, il est apparu que la publication des annuaires officiels sur Internet ne reposait sur aucune base légale. L'université a donc cessé ces publications. En revanche, les anciens annuaires officiels peuvent toujours être consultés par tout un chacun à la Bibliothèque universitaire ou aux Archives de l'État.

Les annuaires officiels ne contenant plus de données personnelles peuvent être publiés sur Internet sans base légale. Il est donc possible de mettre en ligne une version anonymisée (caviardée) de ces annuaires. De plus, les droits de la personnalité s'éteignent au décès de la personne concernée. Or, à l'instar de la loi sur l'archivage, on peut présumer qu'après 110 ans les personnes concernées sont décédées. De ce fait, les annuaires officiels suffisamment anciens, même non caviardés, ne contiennent plus de données personnelles dignes de protection et peuvent donc être publiés sur Internet.

L'intelligence artificielle dans l'administration cantonale

Depuis que l'agent conversationnel ChatGPT a été mis gratuitement à la disposition du plus grand nombre fin 2022, l'utilisation de l'IA est sur toutes les lèvres. ChatGPT est un modèle de langage entraîné avec une multitude de textes préexistants pour fournir aux utilisatrices et aux utilisateurs qui conversent avec lui des réponses censées paraître naturelles et pertinentes. Cela a rapidement soulevé une question : dans quelle mesure l'administration cantonale peut-elle utiliser des systèmes d'IA dans le respect de la protection des données ? La version de ChatGPT accessible au grand public, de même que la variante gratuite du service de traduction DeepL, utilise les textes entrés par les utilisatrices et les utilisateurs pour son propre entraînement, c'est-à-dire dans un but non prévu. Par conséquent, il faut s'abstenir d'entrer des données personnelles lorsque l'on utilise ces agents. En outre, les données relatives à l'utilisation de l'agent sont enregistrées et exploitées pour améliorer le produit. Enfin, on ne peut pas partir du principe que les réponses fournies par les systèmes d'IA sont justes car ces systèmes ne comprennent pas les réponses qu'ils proposent ; ils ne font que les calculer sur la base de probabilités statistiques.

En concertation avec le Bureau, l'OIO a publié une information destinée au personnel expliquant les limites juridiques et les autres risques inhérents à l'utilisation de ces systèmes. Par ailleurs, des représentantes et des représentants de la CHA, du Secrétariat à l'administration numérique (qui est rattaché à la CHA), de l'Université de Berne, de la Haute école spécialisée bernoise, de la ville de Berne et du Bureau se sont réunis, sous la houlette du chancelier d'État, pour échanger au sujet de l'IA.

Communication de données par le biais de listes de destinataires visibles

Un citoyen a signalé au Bureau qu'un office envoyait des courriels groupés à un grand nombre de personnes sans masquer la liste des destinataires. En procédant ainsi, l'office communiquait à des tiers le nom de personnes physiques et de personnes morales ayant un rapport de droit avec le canton de Berne sans que cela repose sur une base légale ou soit nécessaire pour l'accomplissement de ses tâches, raison pour laquelle cette communication devait être considérée comme illicite. Étant donné la possibilité que ce procédé soit réutilisé et qu'il ait éventuellement un impact important sur les droits des personnes concernées, le Bureau a invité l'office à prendre des mesures organisationnelles appropriées afin que les courriels destinés à plusieurs personnes n'ayant rien à voir les unes avec les autres ne soient plus envoyés sans masquer la liste des destinataires et à lui exposer ces mesures. L'office a indiqué qu'il n'enverrait plus de courriels circulaires en affichant la liste des destinataires et qu'il sensibiliserait l'ensemble du personnel à la protection des données. Le Bureau a jugé ces mesures appropriées.

Modification de la loi sur la police et nouvelle loi sur la sécurité de l'information et la cybersécurité

Au cours de l'année sous revue, le délégué à la protection des données a été invité à deux reprises par une commission du Grand Conseil à des auditions concernant une affaire législative. La Commission de la sécurité a souhaité avoir un avis concernant une modification de la loi sur la police (LPol) que le Bureau avait largement commentée dans son rapport d'activité 2022 (p. 24 s.). Les deux problèmes de protection des données que le Bureau avait soulevés n'étaient pas résolus dans le projet présenté par le Conseil-exécutif. La durée de conservation des données issues de la recherche automatique de véhicules et de la surveillance du trafic dont la comparaison avec des banques de données policières n'a débouché sur aucune procédure (no hits) avait été ramenée de 100 à 30 jours, mais cela n'enlevait rien au caractère disproportionné de cette mise en réserve de données de citoyennes et de citoyens intègres. Le Grand Conseil, plutôt que de renoncer à la conservation de ces données, en a porté la durée à 60 jours, ce qui est hautement problématique du point de vue du droit constitutionnel. L'autre point critiqué par le Bureau, à savoir l'octroi à des autorités extracantonales d'un droit d'accès unilatéral aux données policières du canton, a été approuvé par le Grand Conseil sans modification.

Par ailleurs, la Commission des institutions politiques et des relations extérieures a examiné le projet de nouvelle loi sur la sécurité de l'information et la cybersécurité (LSIC). Les cyberattaques constituant une menace croissante, il est essentiel de régir de façon claire et contraignante les mesures visant à garantir la sécurité des données. C'est le but de la LSIC, qui apportera une réglementation moderne visant avant tout les données dont il faut assurer la confidentialité, la disponibilité et l'intégrité pour protéger des intérêts publics. Cependant, les principes prévus sont tout aussi adéquats pour protéger des données personnelles afin de garantir les droits fondamentaux des personnes concernées. C'est pourquoi il faut inscrire dans la LCPD révisée que les principes énoncés dans la LSIC sont également applicables à la protection des données.

6.1.2. Conseils à l'intention des personnes concernées

Renseignements sur la propriété foncière et la propriété de véhicules

Plusieurs personnes se sont adressées au Bureau parce qu'elles ne comprenaient pas que des tiers puissent apprendre sur Internet ou par SMS qui détient la propriété d'un bien-fonds ou d'un véhicule. Dans les deux cas, il existe une base légale à cet effet.

La législation fédérale sur le registre foncier prévoit que le nom et l'identité du propriétaire d'un immeuble sont communiqués à toute personne qui en fait la demande. Elle octroie en outre aux cantons la possibilité de publier ces données en ligne, tant que les données sont accessibles uniquement en relation avec un immeuble déterminé et que le système d'information est protégé contre les appels en série. Le canton de Berne a fait usage de cette possibilité en proposant le service GRUDIS public, accessible depuis le portail BE-Login. Il existe en effet un intérêt public à ce que les informations de base concernant la propriété soient accessibles à tous dans la mesure où la propriété foncière confère un droit exclusif d'utilisation et d'exploitation sur un bien à l'origine commun. Le registre foncier est le lieu où les rapports de propriété sont portés à la connaissance du public afin d'assurer la transparence juridique. Lorsque l'accès à un bien-fonds est interdit à des tiers, ceux-ci ont le droit de savoir qui leur impose cette restriction.

Par ailleurs, la loi fédérale sur la circulation routière habilite les cantons à communiquer les nom et adresse des détentrices et des détenteurs de véhicules si la communication officielle de ces données ne fait pas l'objet d'une opposition. Les détentrices et les détenteurs peuvent s'opposer à la diffusion des indications les concernant auprès de l'autorité cantonale, sans conditions et gratuitement. Pour sa part, la loi cantonale sur la circulation routière prévoit non pas une publication de ces renseignements, mais la possibilité de les demander par interrogation téléphonique individuelle soumise à émolument. Toute personne peut néanmoins

s'opposer à la communication de ces indications la concernant par une démarche sur le site Internet de l'Office de la circulation routière et de la navigation.

Erreur d'adressage de l'accusé de réception d'une déclaration d'impôt

Une personne domiciliée hors du canton de Berne a reçu un courriel accusant réception d'une déclaration d'impôt qu'elle n'avait jamais déposée et elle l'a signalé au Bureau. Renseignements pris auprès de l'Intendance des impôts, il est apparu que l'accusé de réception avait été envoyé à un homonyme du contribuable parce que celui-ci avait indiqué une adresse électronique erronée dans les informations de contact sur sa déclaration d'impôt. Pour s'assurer que les accusés de réception sont envoyés à la bonne adresse, l'Intendance des impôts va rajouter une étape de validation dans son système : les adresses électroniques indiquées dans les déclarations d'impôt seront vérifiées préalablement par l'envoi d'un autre courriel.

Collecte de données sur la conjointe ou le conjoint des externes assurant des cours

Les externes qui donnent des cours pour le canton de Berne, mais pas dans le cadre d'une activité indépendante, sont employés selon des modalités particulières afin que les cotisations sociales puissent être décomptées correctement. Le formulaire d'inscription prévoyait l'obligation de fournir des renseignements sur la conjointe ou le conjoint, notamment son numéro AVS, ce qui a fâché une formatrice. D'après les investigations menées par le Bureau auprès de l'Office du personnel, les renseignements en question sont nécessaires lorsqu'une personne employée doit cotiser à la caisse de pension, a droit à une allocation familiale voire à une allocation d'entretien ou est imposable à la source. Aucun de ces cas de figure ne concerne les externes assurant des cours, raison pour laquelle les données concernant leurs conjointes ou conjoints sont inutiles et ne peuvent donc pas être collectées. Le Bureau a également rappelé que, selon la loi fédérale sur l'AVS, il n'est possible de collecter et traiter systématiquement des numéros AVS que si cela répond à une nécessité de service clairement établie. Il a donc recommandé à l'Office du personnel de ne plus collecter de données sur les conjointes et les conjoints en lien avec les emplois concernés et de modifier en conséquence sa procédure d'inscription.

Divulgation des autres oppositions dans une procédure de permis de construire

Une personne concernée a demandé au Bureau comment l'autorité instruisant une procédure de permis de construire avait pu communiquer aux personnes

ayant déposé une opposition les nom et adresse de toutes les autres personnes ayant fait de même. Le Bureau lui a répondu que la législation sur la procédure administrative donnait aux parties le droit de consulter le dossier de la procédure, à moins que des intérêts publics ou privés prépondérants n'exigent que le secret soit gardé. Les oppositions faisant partie du dossier de la procédure, elles doivent donc en principe être communiquées à toutes les parties. Mais comme la norme légale en question (art. 23 de la loi sur la procédure et la juridiction administratives [LPJA]) peut sembler manquer de clarté dans le cas des procédures multipartites, le Bureau a recommandé, lors de la procédure de consultation sur la révision de la LPJA, que sa teneur soit précisée (lire le rapport d'activité 2022 du Bureau, p. 21).

Consultation du journal de bord d'un établissement pénitentiaire

Un détenu s'est adressé au Bureau parce que sa demande de consultation des entrées le concernant dans le journal de bord de l'établissement pénitentiaire avait été rejetée pour des raisons de principe. Il lui avait été opposé que le journal de bord était un outil de travail pour le personnel et qu'il n'était pas destiné aux détenus. L'établissement précisait que seuls les rapports d'exécution font partie du dossier d'exécution judiciaire et peuvent donc être consultés par les détenus. Pour le Bureau, il n'est pas justifié de refuser de manière générale la consultation du journal de bord. Toute personne a le droit de consulter les données la concernant : c'est un droit fondamental explicitement inscrit dans la Constitution cantonale. Pour pouvoir refuser à une personne la consultation de données la concernant, il faut qu'un intérêt public prépondérant ou un intérêt de tiers particulièrement digne de protection s'y oppose (art. 21, al. 4 LCPD). Une éventuelle restriction du droit de consultation doit en outre être proportionnée, c'est-à-dire ne pas dépasser la portée des intérêts effectivement prépondérants qui s'y opposent. Ainsi, la consultation ne peut pas être refusée de manière générale, mais uniquement en ce qui concerne les données dont la confidentialité doit être garantie (p. ex. pour protéger le personnel). Si cela n'est pas possible, l'autorité responsable reste tenue de fournir des renseignements indirects (art. 21, al. 1 LCPD). Dans tous les cas, la restriction du droit de consultation et de renseignement doit être justifiée de manière à ce que la décision soit compréhensible pour la personne concernée. La simple indication que le journal de bord n'est pas destiné aux détenus et que ceux-ci doivent se contenter des rapports d'exécution est tout à fait insuffisante. Le Bureau a recommandé à l'établissement pénitentiaire de revoir sa décision et il lui a proposé de participer, avec une fonction de conseil, à la recherche d'une solution qui soit conforme à la protection des données et applicable dans la pratique. L'Office de l'exécution judiciaire a cependant préféré que la DSE, en sa qualité d'autorité de surveillance, se prononce sur le recours de la personne concernée.

Remise par la poste de commandements de payer ouverts

Le Bureau reçoit régulièrement des signalements de personnes estimant qu'une atteinte a été portée à leur sphère privée parce qu'une collaboratrice ou un collaborateur de la poste leur a remis un commandement de payer ouvert et a pu ainsi en voir la teneur. La loi fédérale sur la poursuite pour dettes et la faillite (LP) dispose que le commandement de payer est rédigé en double, un exemplaire étant destiné au débiteur et l'autre au créancier (art. 70 LP). Le commandement de payer est notifié par un membre du personnel de l'office des poursuites ou par la poste. La personne qui procède à la notification doit attester sur chaque exemplaire du document le jour où la notification a été faite et la personne à laquelle l'acte a été remis (art. 72 LP). Cela explique pourquoi le commandement de payer ne peut pas être remis dans une enveloppe fermée. Aux yeux du législateur, la traçabilité de la notification, qui est importante pour la suite de la procédure, prime l'intérêt de la débitrice ou du débiteur à maintenir le secret.

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 2023 ne fait pas exception – que le Bureau enseigne la matière « Protection des données et sûreté de l'information » dans le cadre de la filière aboutissant au brevet de « Bernische Gemeindefachfrau/ Bernischer Gemeindefachmann » et de la formation du personnel administratif des écoles de langue allemande. Le cours à l'intention du personnel des secrétariats paroissiaux introduit en 2020 a lieu une fois par an et une formation consacrée à la protection des données dans les paroisses est proposée aux autorités paroissiales depuis 2021. Au cours de cette formation, les intervenantes et les intervenants du Bureau expliquent les principes généraux de la protection des données et leur application dans le domaine d'activité de leur auditoire. Ils s'attachent également à établir la discussion et à répondre aux questions concrètes des participantes et des participants en lien avec leur travail quotidien.

Le Bureau s'est en outre adressé à des employées et des employés communaux travaillant dans le domaine de la scolarité obligatoire à deux occasions : lors d'une réunion à l'école de Seedorf et lors de la rencontre de réseautage organisée par l'association des autorités scolaires du canton de Berne (Verband Schulbehörden Kanton Bern, VBS) sur le thème de la protection et de la sécurité des données.

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 des sujets spécifiques et plus généralement sur les principes de la protection des données (journée de réflexion du Secrétariat général des préfectures ; formation continue de la section Asile et réfugiés de l'Office de l'intégration et de l'action sociale ; rencontres de la Haute école pédagogique germanophone consacrées aux médias et à l'informatique à l'école obligatoire ; congrès de l'Association des établissements cantonaux d'assurance destiné aux juristes). La protection des données dans l'informatique en nuage a été un thème récurrent (formation continue à la préfecture de Frutigen – Bas-Simmental ; invitation à présenter un exposé dans le cadre du cours sur le droit de la protection des données de l'Université de Lucerne ; exposés lors de la Conférence Cloud de l'Administration numérique suisse ; colloque d'automne de l'association Vereinigung Gesundheit-sinformatik Schweiz ; équipe du Swiss Government Cloud de l'Office fédéral de l'informatique et de la télécommunication ; édition 2023 du colloque DINAcon). Le délégué à la protection des données a en outre prononcé des exposés sur la protection des données dans l'apprentissage et le travail avec l'IA (forum Schulthess consacré à l'importance du numérique pour la jeunesse) ainsi que sur le conseil et la surveillance dans le domaine de la protection des données (congrès de l'Université de Bâle sur l'avenir de la protection des données dans l'administration numérique).

6.2 Prises de position formelles

Révision totale de la loi cantonale sur la protection des données

La révision totale de la loi cantonale sur la protection des données qui est en cours a pour but de moderniser ce texte de loi et de l'adapter aux prescriptions européennes, notamment la Convention du Conseil de l'Europe pour la protection des données révisée et la directive de l'Union européenne relative à la protection des données dans le domaine du droit pénal. L'avant-projet de révision, auquel le Bureau a beaucoup contribué, a fait l'objet d'une consultation publique au cours de l'année sous revue. Dans sa prise de position, le Bureau s'est borné à donner son avis sur une disposition qui n'avait pas été discutée lors des travaux préparatoires et qui lui paraissait hautement problématique. Cette disposition permet aux autorités de communiquer des données personnelles à l'étranger afin qu'elles soient traitées par des auxiliaires même si le pays de destination n'offre pas un niveau de protection approprié et si cela ne peut pas être compensé par un

accord contractuel convenable, c'est-à-dire excluant tout accès par des autorités étrangères. À l'appui de cette proposition, le rapport invoque l'intérêt que l'utilisation de solutions en nuage étasuniennes présente pour l'administration cantonale, une utilisation qui n'est actuellement possible que de façon limitée car les États-Unis, avec leur législation sur la surveillance de masse par les services de renseignements, ne sont pas considérés comme un pays garantissant une protection des données appropriée. Pour être considéré comme garantissant une protection des données appropriée, un État n'a pas besoin d'avoir la même législation en la matière que la Suisse ou le canton de Berne. Il suffit que sa législation respecte les principes constitutionnels les plus fondamentaux : pas de restriction des droits fondamentaux sans base légale suffisamment précise ; garantie de la proportionnalité ; et protection juridique minimale pour les personnes concernées. Ces principes sont si élémentaires que la Convention du Conseil de l'Europe pour la protection des données stipule que des données personnelles ne peuvent être transférées dans des États étrangers que si une protection appropriée est garantie. Par conséquent, l'inscription dans la loi de la disposition proposée contreviendrait à la Constitution fédérale et à la Convention du Conseil de l'Europe, qui a force obligatoire pour le canton de Berne. Un recours auprès du Tribunal fédéral entraînerait son abrogation. Le Bureau a publié sa prise de position sur son site Internet (en allemand). Il y expose en détail les raisons pour lesquelles il s'oppose à cette disposition (www.be.ch/bpd > Actualités).

Révision de l'ordonnance sur l'information

La loi sur l'information révisée par le Grand Conseil en 2022 est entrée en vigueur en 2024 sous la nouvelle appellation de loi sur l'information et l'aide aux médias (LIAM). L'ordonnance d'exécution de cette loi a donc été elle aussi entièrement révisée en 2023 et rebaptisée ordonnance sur l'information et l'aide aux médias (OIAM). Les publications des autorités pouvaient déjà inclure des données personnelles, pour autant qu'aucun intérêt prépondérant ne s'y oppose, notamment de la part des personnes concernées. Si cette condition est remplie, le nouvel article 15b LIAM permet de communiquer des données personnelles sur Internet également. Mais ces données doivent être retirées dès qu'il n'existe plus d'intérêt public à les rendre accessibles. La nouvelle OIAM devait apporter deux précisions à ce dispositif. Premièrement, la publication de données personnelles sur Internet peut exposer la personne concernée à des risques particuliers, par exemple celui d'être poursuivie ou de voir des membres de sa famille poursuivis à l'étranger ou celui d'être déchue de sa nationalité en raison de cette information. Par conséquent, une publication sur Internet doit être précédée d'une pesée des intérêts approfondie. Si la protection de la personne concernée répond à un intérêt prépondérant, il faut renoncer à une publication en ligne, sauf si l'information peut être publiée sous une forme anonymisée (document caviardé). Deuxièmement, l'ordonnance précise que le retrait de données personnelles publiées sur Internet peut être effectué en application de directives générales et par catégories de publication. Les autorités ont ainsi la possibilité de fixer des délais à l'expiration

desquels la publication ou les données personnelles qu'elle contient sont automatiquement retirées.

Révision de la loi sur l'archivage

Lors de la procédure de corapport en vue de l'adoption du projet de révision partielle de la loi sur l'archivage (P-LArch), le Bureau n'a rien eu à ajouter car il avait déjà apporté une contribution substantielle lors des travaux préparatoires et les questions intéressant la protection des données avaient pu être clarifiées dans le projet ou dans le rapport explicatif afférent. C'est notamment le cas de la gestion des données soumises à une obligation particulière de garder le secret, par exemple le secret professionnel du personnel de santé. Pour que les documents contenant des données protégées par le secret professionnel ou le secret de fonction puissent être proposés aux Archives de l'État, il faut que les personnes assujetties à l'obligation de garder le secret en soient libérées (art. 8, al. 3 P-LArch). Si les Archives de l'État recueillent des documents dont le délai de conservation court encore, elles deviennent auxiliaires de la personne astreinte au secret et y sont elles-mêmes tenues. Pour donner accès à des tiers à ces documents, elles doivent être libérées du secret par la même autorité que la personne qui a déposé les documents (art. 18a, al. 1 P-LArch). Les obligations particulières de garder le secret, que les personnes qui y sont assujetties doivent généralement observer jusqu'à leur décès, restent valables après l'expiration du délai de conservation (art. 17, al. 1 et art. 20 P-LArch). Même si les Archives de l'État ne sont plus soumises à une obligation particulière de garder le secret les visant directement, elles ne sont pas autorisées à donner plus facilement un accès aux documents que la personne assujettie à l'obligation de garder le secret. En d'autres termes, lorsque les Archives de l'État statuent sur une demande d'accès, par exemple à des fins scientifiques, elles doivent procéder à la même pesée des intérêts que l'autorité compétente pour libérer de l'obligation de garder le secret, c'est-à-dire en accordant une importance particulière au secret.

Nouveau système de gestion des cas : autorisation de dépenses

Le programme NFFS (de l'allemand Neues Fallführungssystem) de la DSSI vise à mettre en place un nouveau système informatique de gestion de cas au sein des services sociaux, des autorités de protection de l'enfant et de l'adulte ainsi que des services spécialisés dans l'insertion professionnelle. Il s'agit d'un projet de transformation numérique coûteux et de grande envergure pour le canton de Berne : plus de 80 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 requiert 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. Le Bureau, qui n'a eu aucune

observation à faire dans la procédure de corapport portant sur le crédit d'objet de 52 millions de francs demandé pour ce projet, est très heureux d'avoir été informé et consulté aussi complètement.

Convention visant à harmoniser l'informatique de la justice pénale

Le programme HIJP d'harmonisation de l'informatique de la justice pénale lancé en 2016 par la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) a pour but d'améliorer l'harmonisation et la mise en réseau des systèmes informatiques des autorités pénales. Durant l'année sous revue, la CCDJP a consulté les cantons sur un projet de convention administrative entre la Confédération et les cantons visant à créer une collectivité de droit public appelée HIJP Suisse ayant son siège à Berne. Il est écrit dans le projet que, si des questions juridiques se posent dans le cadre du fonctionnement de HIJP Suisse, c'est-à-dire concernant son organisation et son administration, le droit applicable est le droit bernois et plus spécialement la LCPD. Dans le rapport explicatif, le Bureau est désigné comme étant l'autorité de surveillance compétente pour la corporation HIJP Suisse. À la demande du Bureau, le canton de Berne a précisé un certain nombre de points dans sa prise de position au sujet du projet de convention. La LCPD dispose que le Bureau est soumis uniquement à la Constitution et à la loi (art. 33a). Contrairement à un concordat formel, une convention administrative intercantonale n'est pas apte à attribuer de nouvelles tâches au Bureau. Toutefois, le Bureau est autorisé à assumer des tâches relevant de la surveillance de la protection des données dans d'autres collectivités de droit public s'il a conclu un accord dans ce sens (art. 36a, al. 4 LCPD). Les prestations fournies dans ce cadre doivent être indemnisées convenablement afin de ne pas porter atteinte à l'indépendance financière du Bureau. C'est dans cet esprit que les organisations instituées par le Concordat sur les jeux d'argent au niveau suisse ont désigné le Bureau comme autorité de surveillance et conclu avec lui un accord comportant des règles d'indemnisation.

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 2023, le Bureau a traité 133 contrôles préalables concernant des projets informatiques (2022 : 134) et en a achevé 63 (2022 : 94). Si le taux de clôture des dossiers est plus bas que l'année précédente, c'est en raison de l'étendue et de la grande complexité de plusieurs dossiers, comme le projet SAP et ses différentes étapes, l'introduction de M365 dans l'administration cantonale (qui comprend plus de dix concepts SIDP nouveaux ou modifiés) et le projet de numérisation du Groupe de l'Île.

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.

Mise en place de M365 par différentes autorités

Comme expliqué sous le point 6.1.1 plus haut, 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). C'est pourquoi une autorité qui envisage de mettre en place M365 ne peut pas échapper à la nécessité de définir ses besoins concrets, de décrire les données qu'elle traite et leur besoin de protection, d'identifier l'ensemble des risques pour toutes les

personnes concernées et de prendre des mesures appropriées pour réduire ces risques ou les ramener à un niveau supportable, ce qui inclut d'évaluer d'autres produits possibles et, si les risques résiduels sont élevés, de renoncer totalement ou partiellement à utiliser certains services en nuage. Si les risques résiduels sont jugés supportables, il appartient à l'organe de direction le plus élevé d'en assumer la responsabilité au regard du droit de la protection des données. Toute autorité qui prévoit d'introduire M365 doit donc être consciente qu'elle s'engage dans une démarche complexe et chronophage.

C'est pourquoi il n'a pas été possible, en parallèle avec la préparation du rapport de l'OIO sur les risques à l'attention du Conseil-exécutif (cf. 6.1.1 plus haut), de mener à bien en 2023 le contrôle préalable des nombreux concepts SIPD présentés en vue de l'introduction de M365 dans *l'administration cantonale*. Le Bureau a néanmoins soumis l'ensemble des concepts à un premier examen et remis à l'OIO les ébauches de rapport de contrôle préalable contenant un ensemble de constatations et de recommandations afin qu'il prenne position et remanie ou complète la documentation SIPD. Un point important reste ouvert : il concerne les mesures organisationnelles, procédurales et techniques visant à garantir la sûreté de l'information et la protection des données dans le contexte de l'utilisation d'un bouquet de services en perpétuelle mutation technique, requérant de ce fait une réévaluation permanente des risques.

Un contrôle préalable a pu être achevé après quatre itérations (ébauches successives de rapport du Bureau incluant les constatations et les prises de position de l'autorité). Il concerne *l'Université de Berne*, qui prévoit de mettre en place M365 d'ici la fin 2024. Comme dans l'administration cantonale, les utilisatrices et les utilisateurs ne sont pas autorisés à traiter les données particulièrement dignes de protection ou visées par une obligation de garder le secret sur des services en nuage. Il n'en fallait pas moins documenter soigneusement et examiner les utilisations, les données traitées dans le cadre de chaque utilisation, la nécessité d'une externalisation partielle, l'intégration dans l'infrastructure informatique locale, les mesures visant à réduire le risque et l'engagement de la responsabilité de la direction de l'université pour les risques résiduels.

Le *Groupe de l'Île* prévoit lui aussi de mettre en place M365 d'ici la fin 2024. Son projet porte principalement sur la bureautique, même si des informations particulièrement dignes de protection sur la santé de la patientèle pourront aussi être traitées sur cette plateforme dans certains cas. Le contrôle préalable en cours met donc l'accent sur les mesures techniques et organisationnelles prévues pour protéger la confidentialité de ces données, qui doivent répondre à des exigences accrues.

Utilisation du nuage AWS pour le traitement d'images médicales

L'institut de médecine tissulaire et de pathologie a le projet de numériser les images d'échantillons pathologiques et le processus diagnostique associé, y

compris les éléments d'aide à la décision fournis par des systèmes d'IA. Étant donné les importantes capacités de stockage et de calcul que ce projet requiert, l'institut envisage de passer par les services Web d'Amazon (AWS) pour exploiter le système de gestion de ces images. Le contrôle préalable a permis de constater que les images étaient pseudonymisées avant d'être traitées dans les services en nuage. Ainsi, les données ne peuvent pas être rattachées par des tiers à des personnes identifiées ou identifiables si bien qu'elles ne constituent pas des données personnelles pour des personnes extérieures. Le contrôle préalable a donc pu être clôturé sans que l'institut ait à présenter des mesures particulières pour accroître la protection des données de santé.

Transfert aux États-Unis de données personnelles ou potentiellement personnelles

Une nouvelle application pour smartphone de l'Office de l'agriculture et de la nature (OAN) permet aux personnes intéressées qui pénètrent dans une réserve naturelle d'être averties des interdictions en place et, indépendamment de cela, de recevoir des informations sur les réserves naturelles. Pour des raisons techniques, l'adresse IP du smartphone doit être envoyée au fournisseur aux États-Unis. Les adresses IP sont considérées comme des données personnelles lorsque leur destinataire, qu'il s'agisse de la personne voulue ou d'un tiers non autorisé, peut les rattacher à une personne identifiée ou identifiable. Le Bureau recommande à l'OAN de traiter les adresses IP comme des données personnelles et de s'assurer que leur transfert aux États-Unis respecte les dispositions légales. En raison de leur législation sur la surveillance de masse par les services de renseignements, les États-Unis ne sont actuellement pas considérés comme un pays garantissant une protection des données appropriée, raison pour laquelle il est en principe interdit d'y transférer des données personnelles (art. 14a, al. 1 LCPD). Toutefois, le transfert de données personnelles dans ce pays est permis si la personne concernée en a été informée et y a consenti préalablement. L'OAN a donc prévu qu'une information s'affiche à la première ouverture de l'application et que l'utilisatrice ou l'utilisateur doive donner son consentement pour pouvoir utiliser l'application.

Plateforme de participation numérique

Le canton de Berne voulait que toutes les consultations publiques, notamment concernant les projets de loi, se déroulent sur la plateforme de participation numérique. Cette plateforme est mise à disposition par un fournisseur suisse sous la forme d'un logiciel en tant que service *(Software as a Service*). Grâce à l'attitude constructive de la CHA, qui est responsable du dossier, et à la coopération du fournisseur, qui était disposé à apporter des modifications à la plateforme, toutes les recommandations du Bureau ont pu être mises en application au stade du contrôle préalable. Le Bureau avait notamment déploré qu'au début les membres

du personnel cantonal aient la possibilité de voir quelles personnes avaient participé à l'élaboration des prises de position en utilisant la fonction de collaboration de la plateforme. Les opinions et les actions politiques sont considérées comme des données particulièrement dignes de protection. Elles ne regardent pas les autorités, sauf si elles sont indiquées lors du dépôt de la prise de position. Pour résoudre le problème, le fournisseur a masqué ces données pour les autorités, données dont il a besoin pour autoriser les personnes participantes à accéder à la plateforme. L'envoi de courriels indiquant le statut de la prise de position, par exemple l'accusé d'enregistrement sur la plateforme ou l'accusé de réception, passait au départ par un fournisseur aux États-Unis, qui a ensuite pu être remplacé par un fournisseur européen. Enfin, le Bureau a recommandé à la CHA de nombreuses adaptations aux dispositions régissant l'utilisation et la protection des données, adaptations qui ont été intégralement réalisées.

Numérisation des échanges postaux avec l'administration cantonale

Durant l'année sous revue, l'administration cantonale a franchi de nouvelles étapes dans sa démarche de numérisation des échanges postaux, ce qui a occasionné un certain nombre de contrôles préalables. Le projet Digipost@BE a permis de mettre en place le traitement numérisé des courriers entrants dans plusieurs offices. Le courrier est ouvert dans un lieu central pour y être scanné puis transmis sous forme numérique à l'autorité compétente pour qu'il le traite. Il fallait s'assurer que les enveloppes portant la mention « secret », « personnel », « confidentiel » ou « privé » ne soient pas ouvertes et soient remises par courrier postal séparé aux services indiqués. En outre, le dispositif Digipost@BE utilise un module d'apprentissage basé sur l'IA, qui peut être entraîné pour classer les documents entrants de manière plus efficace, par exemple en apprenant les coordonnées de certains champs de contenu. Lors de la configuration de ce module, chaque autorité destinataire définit les données qui peuvent être utilisées pour l'entraînement ; elle doit veiller à ce qu'il ne s'agisse pas de données personnelles.

Inversement, l'administration a la possibilité de remettre des documents aux citoyennes et aux citoyens par voie numérique. À cet effet, le canton, avec le concours de la Poste, met à disposition une boîte aux lettres électronique (BE-ePost), dont l'utilisation est facultative. Lors du contrôle préalable, le Bureau a vérifié que les bases légales requises existaient, que la confidentialité était garantie, que la sécurité de la transmission des données était assurée et qu'il était possible de revenir à tout moment à une remise des documents par voie postale. Les personnes intéressées pourront étrenner ce service en s'inscrivant via leur compte BE-Login pour recevoir les tranches d'impôt.

Transformation numérique du Groupe de l'Île

Le Groupe de l'Île prévoit de remplacer plusieurs systèmes informatiques par le nouveau système d'information clinique du fournisseur américain EPIC, un système de documentation des traitements associé à un système de pilotage permettant de gérer l'occupation des lits, les plans de service, le nettoyage des chambres, etc. Les institutions de santé du groupe passeront ainsi d'une gestion des dossiers médicaux par cas à une gestion par patient, ce qui facilitera la prise en charge interdisciplinaire. Afin que l'ensemble des sites, des cliniques, des domaines médicaux et des catégories professionnelles puissent collaborer, la documentation de l'ensemble des traitements sera regroupée dans un dossier central pour chaque patiente ou patient au lieu d'être éparpillée dans des dossiers par cas ou par clinique. Il est prévu d'accorder au personnel médical des droits d'accès étendus. Étant donné l'ampleur et la grande complexité du projet ainsi que du nouveau concept de conservation et d'accès aux données, le Bureau a demandé à être impliqué à un stade précoce pour dispenser des conseils. Il a ainsi pu, avant même le contrôle préalable, échanger sur les étapes du projet à venir et les points à surveiller du point de vue de la protection des données, mais aussi avoir une démonstration détaillée du système sur place. En ce qui concerne les droits d'accès, le Bureau a souligné dès le départ la nécessité de prendre des mesures appropriées pour garantir le respect du principe de proportionnalité. En 2023, le contrôle préalable a donné lieu à deux itérations, qui ont permis de ramener le nombre de points à régler de 86 à 25.

En raison de son interdépendance avec le système d'information clinique EPIC, l'application spécialisée Medical Content Plattform, le futur système de gestion des contenus du domaine de la santé du Groupe de l'Île, a également été soumise à un contrôle préalable. Cette application, qui est intégrée dans le système EPIC, sera utilisée pour mettre à la disposition du personnel médical une grande partie des contenus médicaux, c'est-à-dire concrètement des clichés, documents, signaux biologiques, fichiers audio et vidéo produits par des systèmes experts externes ou mis à disposition par des médecins traitants externes ou des institutions partenaires. Durant l'année sous revue, le Bureau a rendu ses troisième et quatrième avis sur la volumineuse documentation SIPD en vue de son remaniement. L'examen du quatrième remaniement n'est pas encore achevé.

Enregistrements audio et vidéo dans les services de l'emploi

L'ordonnance cantonale sur le marché du travail permet depuis 2022 à l'Office de l'assurance-chômage (OAC) de procéder à des enregistrements audio et vidéo des entretiens menés avec la clientèle à des fins d'assurance de la qualité et de formation du personnel, à condition que l'ensemble des personnes participant à l'entretien y aient expressément consenti. L'OAC a remis au Bureau les documents SIPD pour contrôle préalable en 2023. Le Bureau a contrôlé notamment l'application des prescriptions relatives au consentement, qui doit être libre, la plateforme

de sauvegarde des enregistrements pendant le délai de conservation et la destruction des données à l'issue du délai de conservation. Comme il est en outre prévu d'utiliser les données pour réaliser des études dans le cadre de l'assurance de la qualité, le Bureau a également vérifié les conditions régissant la transmission des données à des fins de recherche et la procédure à respecter pour cette transmission.

Extension de VacMe à la vaccination contre le mpox et à d'autres vaccinations

La DSSI a développé l'application VacMe, mise en place durant la pandémie de COVID-19, afin de pouvoir répondre à d'autres besoins, par exemple pour la vaccination contre le mpox, la grippe ou les tiques. Le contrôle préalable a relevé un défaut significatif : les données des personnes souhaitant se faire vacciner ou ayant été vaccinées auraient pu être consultées et traitées non seulement par les prestataires publics du système de santé, mais aussi par les autorités de l'administration cantonale alors qu'il n'y a pas de base légale suffisante pour cela. La DSSI a donc procédé à des adaptations techniques et modifié le concept des rôles et des droits d'accès afin que les autorités administratives n'aient plus accès aux données. Le Bureau a ainsi pu clôturer le contrôle préalable avec un avis positif.

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).

Surveillance de la caserne militaire

Il est beaucoup plus facile pour le Bureau d'appréhender les installations de vidéosurveillance, notamment l'emplacement des caméras et les espaces couverts, ainsi que les besoins auxquels répondent ces installations lorsqu'il peut visiter les lieux avec l'autorité responsable pour se faire une idée concrète de la situation. Après une visite de la caserne militaire de Berne, il a reçu pour contrôle préalable la documentation SIPD portant sur la modernisation du dispositif de vidéosurveillance. Huit caméras étaient prévues pour surveiller en temps réel le contrôle des accès tandis que 18 autres caméras devaient enregistrer des images en divers endroits afin de protéger le bâtiment et les véhicules, militaires et civils, garés sur le périmètre. L'examen auquel chaque caméra est soumise individuellement par principe a montré que la vidéosurveillance était utilisée de manière conforme au but et proportionnée.

Nouveau bâtiment principal de l'Hôpital de l'Île

Un dispositif de vidéosurveillance étendu était prévu pour le nouveau bâtiment principal de l'Hôpital de l'Île, baptisé Maison Anna-Seiler. Il se composait de 75 caméras qui devaient, conformément à la LPol, enregistrer des images pour protéger le bâtiment, le personnel et la patientèle contre les infractions. Un autre ensemble de 63 caméras devait servir à l'accomplissement de tâches dans le domaine des soins hospitaliers, en assurant la surveillance en temps réel de lieux déterminés dans le but de protéger la santé des patientes et des patients. Il est apparu au Bureau que les deux ensembles de caméras étaient utilisés de manière proportionnée à leur but et que la durée de conservation des images était appropriée. Le Bureau reviendra sur une recommandation relative à la protection technique des images contre l'accès par des tiers non autorisés lorsqu'il examinera l'ensemble de l'infrastructure vidéo.

6.4 Audits

Le Bureau a pour mandat légal de surveiller l'application des prescriptions relatives à la protection des données et à la sûreté de l'information. Alors que le contrôle préalable porte sur *une situation future*, c'est-à-dire sur la conformité au droit et la sécurité des modalités prévues pour un nouveau traitement de données, l'audit SIPD porte sur une *situation existante*, c'est-à-dire sur la manière dont le nouveau traitement de données fonctionne. Les audits constituent donc, dans l'activité de surveillance du Bureau, un complément important aux contrôles préalables.

Au cours de l'année sous revue, le Bureau a mené neuf audits, dont un en collaboration avec le CF. Le Bureau et le CF prévoient d'ailleurs de poursuivre leur excellente collaboration. Un audit prévu n'a pas pu être réalisé en raison du contexte difficile dans lequel évolue le service concerné. Conformément à sa stratégie axée sur les risques, le Bureau s'est concentré sur les services TIC de base, les applications spécialisées essentielles et le domaine de la santé (hôpitaux), où il a contrôlé plus spécialement la protection de base des TIC et les équipements médicaux. Il a également suivi l'avancement de la mise en œuvre des recommandations qu'il avait formulées lors des audits des années précédentes. L'accompagnement de la mise en œuvre des actions correctives est une tâche normale du Bureau, gage d'efficacité et d'obtention des résultats souhaités.

Enseignements généraux

Les contrôles a posteriori permettent au Bureau d'établir de manière transparente si les autorités responsables ont remédié de manière efficace et vérifiable aux lacunes relevées. Or, si des progrès ont pu être observés, force est de constater que les autorités auxquelles des mesures sont préconisées s'emploient à les réaliser avec une diligence variable. Le manque d'attention et les retards qui en découlent dans la mise en œuvre des mesures SIPD augmentent le risque de ne pas pouvoir faire face suffisamment vite et de manière adéquate aux dangers de la cybercriminalité, qui évoluent constamment. Il faut donc que l'identification systématique des risques dans ce domaine et la rapidité de réaction face aux risques identifiés reçoivent une attention accrue. Cela vaut également pour l'examen périodique des risques et des mesures requis par l'ordonnance sur la protection des données (OPD ; art. 4, al. 3) pour s'assurer que les systèmes TIC conservent de manière générale leur capacité de résistance face aux risques de cybersécurité.

En ce qui concerne les hôpitaux, il est apparu que la gestion des équipements médicaux était en grande partie déterminée par les fournisseurs. Ceux-ci étant en position de force sur le marché, les hôpitaux ont relativement peu de contrôle sur l'infrastructure médicale et sur la sécurité de son exploitation. Les travaux de maintenance supplémentaires destinés à maintenir ou à accroître la sécurité ont souvent un coût élevé.

De manière générale, les autorités laissent les prestataires et les fournisseurs impliqués, sur lesquels elles n'ont pas d'influence ni de contrôle direct, assumer leur responsabilité en matière de protection des données et de sûreté de l'information. Il est important que les autorités améliorent le pilotage et la surveillance des prestataires et des fournisseurs et surtout qu'elles en assument la responsabilité de manière vérifiable.

Application spécialisée socialweb

Plusieurs foyers scolaires cantonaux utilisent l'application socialweb pour gérer leur administration et la prise en charge de leur clientèle. Socialweb est un logiciel modulaire basé sur le Web conçu pour le travail social et le travail socio-éducatif. Le Bureau a choisi le centre pédagogique de logopédie et d'entraînement auditif de Münchenbuchsee pour y réaliser un audit représentatif. L'évaluation a porté sur les domaines suivants : gouvernance SIPD (pilotage des tâches SIPD), concepts et mesures de protection SIPD, processus de gestion des utilisatrices et des utilisateurs, externalisation, conservation des données et interfaces, gestion de la continuité de l'exploitation, gestion de la continuité des services TIC, gestion des crises et des situations d'urgence.

L'audit a mis en évidence des lacunes dans tous les domaines contrôlés, avec un risque associé jugé moyen dans la majeure partie des cas. L'application spécialisée se prêtait mal à un audit en raison de l'ancienneté de la documentation et des incertitudes en découlant concernant la situation à viser dans le domaine de la protection des données et de la sûreté de l'information. Il n'a donc pas été possible de produire un résultat complet et qualifié. Le Bureau suivra activement la mise en œuvre des actions correctives.

Réseau sans fil BE-NET

En 2019, le Bureau avait vérifié si le réseau sans fil BE-NET proposé par l'OIO dans le cadre des services de base TIC respectait les exigences en matière de protection des données et de sûreté de l'information. L'examen avait mis en évidence des lacunes associées à des risques moyens et faibles. Un audit de suivi a été mené pour vérifier si les actions correctives préconisées avaient été mises en œuvre de manière complète et vérifiable et si elles étaient efficaces.

Il est apparu que seuls six des 14 problèmes identifiés avaient été totalement résolus. Une solution partielle avait été trouvée pour six autres problèmes ; sa mise en œuvre avait débuté, mais il restait des adaptations à apporter. Deux problèmes étaient encore entiers, de même que les risques associés. Cependant, il était prévu que les mesures préconisées soient réalisées d'ici la fin juillet 2024. Compte tenu du temps écoulé depuis le premier audit, ce résultat n'est pas satisfaisant. La rapidité de réalisation des actions correctives mérite de recevoir une plus grande attention. Le Bureau suivra la mise en œuvre des mesures restant à réaliser.

Centre de calcul de la POCA

Le CF et le Bureau ont audité conjointement l'exploitation du centre de calcul de la POCA. Les applications informatiques et les applications de communication sont hébergées sur deux sites de la POCA à Berne. Leur exploitation est assurée

en interne. L'audit a porté sur les aspects suivants : existence d'un cadre de référence approprié pour les contrôles dans le domaine SIPD, assurant la traçabilité du pilotage de l'exploitation du centre de calcul ; adéquation de la sécurité physique avec la criticité des applications exploitées ; mesures prises pour garantir la sécurité du réseau. La préparation à des interventions en cas d'urgence ou de crise a également été évaluée.

Il est apparu que le centre de calcul est hébergé dans des locaux anciens, qui ont évolué au fil du temps mais dont les installations techniques n'ont pas été conçues pour l'exploitation d'une infrastructure TIC. Globalement, l'audit a conclu que le centre de calcul actuel, notamment parce qu'il exploite des applications critiques, n'était pas conforme aux exigences élevées dans le domaine SIPD, aux normes courantes pour les centres de calcul ni aux bonnes pratiques. Il est donc associé à des risques élevés pour la protection des données et la sûreté de l'information. Il est prévu, dans le cadre de la construction du nouveau Centre de police Berne, que la POCA soit dotée d'un centre de calcul conçu à neuf.

Application spécialisée GERES

La plateforme des systèmes des registres communaux (GERES) sert à l'accomplissement des tâches du canton qui découlent des législations fédérale et cantonale régissant l'harmonisation des registres, les personnes étrangères ainsi que l'établissement et le séjour des Suissesses et des Suisses. Elle sert également de source de données centrale pour l'accomplissement de nombreuses tâches publiques ainsi que pour la compilation de statistiques. Les données qu'elle contient sont fournies par les communes et consolidées au niveau cantonal. L'exploitation de GERES relève de la responsabilité de l'OIO. L'audit du Bureau a porté sur la sécurité de l'information, la gestion du changement et des droits d'accès ainsi que l'externalisation. Le Bureau a également vérifié si des contrôles sont réalisés pour s'assurer du respect des prescriptions imposées par la réglementation en ce qui concerne le traitement des données personnelles.

Des lacunes ayant une significativité moyenne ou faible ont été identifiées dans seulement deux des cinq domaines audités, ce dont il faut se féliciter. Elles concernaient les contrôles visant à s'assurer que les utilisatrices et les utilisateurs ne bénéficient pas de droit d'accès dont ils n'ont pas besoin pour accomplir les tâches qui leur sont dévolues et des retards dans la suppression des données. Le Bureau suivra la mise en œuvre des actions correctives nécessaires.

Protection de base de l'infrastructure informatique du Centre hospitalier Bienne

Le Centre hospitalier Bienne (CHB) dessert Bienne, le Seeland et le Jura bernois. Cet établissement de soins aigus propose une gamme élargie de soins médicaux

de base. Son offre revêt une importance suprarégionale pour l'approvisionnement en soins de la population dans quatre domaines phares à caractère interdisciplinaire. Le CHB a la forme juridique d'une société anonyme, détenue à 99 % par le canton de Berne. L'audit a porté essentiellement sur le respect des exigences SIPD dans la protection de base de l'infrastructure informatique. La protection de base englobe l'ensemble des mesures (organisation, procédures, outils, infrastructures et systèmes techniques, données, dispositifs, etc.) mises en place pour assurer la sécurité des processus opérationnels (y c. le traitement des données personnelles) et leur conformité avec les prescriptions en matière de protection des données.

L'audit a mis en évidence des lacunes dans presque tous les domaines contrôlés, avec un risque associé jugé moyen ou élevé pour la protection des données et la sûreté de l'information. Cela tient notamment au fait que des procédures et des contrôles importants visant à sécuriser les données personnelles ainsi que les systèmes TIC en fonction de leur classification et de leur criticité et à les exploiter de manière conforme au droit étaient encore en cours d'élaboration au moment de l'audit. De ce fait, il y a un risque accru que les prescriptions imposées par la réglementation ne soient pas respectées de manière traçable et que les systèmes TIC ne garantissent pas la protection voulue. Le Bureau suivra la mise en œuvre des actions correctives.

Infrastructure informatique des équipements médicaux de l'hôpital SRO AG

L'hôpital régional de Haute-Argovie (SRO AG) est le centre hospitalier de la région. L'hôpital de Langenthal, ses deux centres de santé de Huttwil et Niederbipp et le Panorama Park à Herzogenbuchsee offrent une couverture médicale complète à la population de la région. L'infrastructure informatique est exploitée en majeure partie avec des ressources internes. Il arrive que l'établissement fasse appel à des spécialistes externes pour certains projets ou services. En 2019, le Bureau avait examiné la protection de base de l'infrastructure informatique de SRO AG. C'est pourquoi l'audit réalisé en 2023 a porté essentiellement sur la gestion des équipements médicaux ayant une dimension informatique. Il a consisté à réaliser une série de contrôles dans les domaines de la gestion du risque, de l'exploitation des TIC et de l'externalisation ainsi qu'à examiner le rôle du Chief Information Security Officer. Enfin, la réalisation des actions correctives préconisées suite au premier audit de la protection de base de l'infrastructure informatique a été vérifiée.

Dans le domaine des équipements médicaux, des lacunes ont été identifiées dans tous les domaines audités, dont certaines associées à des risques élevés pour la protection des données et la sûreté de l'information. Le Bureau a notamment constaté que les processus de gestion des équipements médicaux et de leur cycle de vie n'étaient pas encore documentés ni coordonnés de manière optimale. Les consignes et les instructions d'utilisation étaient incomplètes Un test visant à identifier les points faibles a mis en évidence un nombre élevé de lacunes

de sécurité patentes et connues, présentant des degrés de criticité variés, dans les équipements reliés au réseau. Cela s'explique notamment par le fait que les responsables TIC n'avaient pas la possibilité de mettre à jour les logiciels anciens des équipements. De manière générale, la mise à jour doit être autorisée ou effectuée par le fabricant ou le fournisseur, ce qui, dans certains cas, n'est pas fait systématiquement mais seulement à la demande de SRO AG. En outre, les coûts facturés pour ces opérations sont souvent très élevés. Cela constitue un déficit de sécurité notable, sur lequel SRO AG n'a qu'un contrôle indirect dans une partie des cas alors que c'est lui qui assume la responsabilité de l'ensemble des risques SIPD. Les fabricants ou les fournisseurs des équipements médicaux doivent apporter leur contribution pour que SRO AG puisse assumer sa responsabilité en matière de sûreté de l'information et de protection des données. Le Bureau suivra la mise en œuvre des actions correctives.

Infrastructure informatique des équipements médicaux de l'hôpital STS AG

L'hôpital Simmental-Thun-Saanenland AG (STS AG) assure la couverture médicale dans l'Oberland bernois, avec un établissement à Thoune et un établissement à Zweisimmen. STS AG est le plus grand centre hospitalier régional public du canton de Berne. Il propose une large gamme de soins de base et de spécialités médicales. L'infrastructure informatique est exploitée en majeure partie avec des ressources internes. Il arrive que l'établissement fasse appel à des spécialistes externes pour des services dédiés. Le Bureau avait audité la protection de base de l'infrastructure informatique de STS AG en 2020. L'audit mené en 2023 a porté sur les mêmes points d'attention et sur les mêmes domaines que l'audit de SRO AG, même s'il n'a pas été possible de pratiquer des contrôles d'ampleur égale dans tous les domaines.

L'audit des équipements médicaux a mis en évidence des lacunes, dont certaines sont associées à des risques élevés pour la protection et la sécurité des données. Il est apparu en particulier que les contrôles visant à analyser, évaluer, identifier et représenter les risques pour l'infrastructure informatique et pour la protection des données n'étaient pas encore intégralement implémentés. Le processus de gestion des équipements médicaux et les responsabilités en place n'étaient pas encore documentés ni coordonnés de manière optimale, en particulier en ce qui concerne la mise hors service d'équipements médicaux. Les consignes et les instructions d'utilisation documentées étaient lacunaires. Un test visant à identifier les points faibles a mis en évidence des lacunes de sécurité présentant un degré de criticité élevé dans les équipements reliés au réseau. Comme SRO AG, STS AG n'a qu'un contrôle limité sur cette situation et doit compter sur la contribution des fabricants et des fournisseurs (notamment en ce qui concerne la mise à jour régulière des logiciels des équipements médicaux) pour pouvoir assumer sa responsabilité dans le domaine SIPD. Le Bureau suivra la mise en œuvre des actions correctives.

Protection de base de l'infrastructure informatique du groupe hospitalier Lindenhofgruppe AG

L'hôpital Lindenhof à Berne est un établissement privé. Avec les hôpitaux Engenried et Sonnenhof, il forme le groupe Lindenhof. Il s'agit de l'un des groupes hospitaliers privés les plus importants à l'échelle de la Suisse pour ce qui est des établissements répertoriés. Il propose une large gamme de soins interdisciplinaires ainsi que des prestations de médecine spécialisée et de médecine hautement spécialisée. L'audit s'est concentré sur le respect des exigences SIPD dans le domaine de la protection de base de l'infrastructure informatique. La protection de base englobe l'ensemble des mesures (organisation, procédures, outils, infrastructures et systèmes techniques, données, dispositifs, etc.) mises en place pour assurer la sécurité des processus opérationnels (y c. le traitement des données personnelles) et leur conformité avec les prescriptions en matière de protection des données.

L'audit a mis en évidence, dans cinq des six domaines principalement visés, des lacunes associées à des risques moyens, mais aussi élevés dans certains cas. Le Bureau a notamment constaté que les responsabilités nécessaires n'étaient pas définies clairement. Cela complique la mise en place de mécanismes permettant de s'assurer de manière vérifiable que les données classifiées sont traitées exclusivement en accord avec les prescriptions imposées par la réglementation en vigueur. Il a été constaté également que certains processus formalisés n'étaient pas appliqués de manière systématique. En outre, il manque dans certains domaines des instructions et des procédures claires pour guider et faciliter la mise en œuvre des processus. Le Bureau suivra la mise en œuvre des actions correctives.

Contrôles en application de l'ordonnance VIS

En application de l'ordonnance VIS, le Bureau est tenu de contrôler régulièrement les accès des autorités cantonales au système central d'information sur les visas des États Schengen. En 2023, le Bureau a réalisé le premier contrôle de ce type en utilisant un échantillon aléatoire des accès du personnel du Service des migrations de l'Office cantonal de la population. Il est apparu que les accès avaient eu lieu dans le cadre de l'accomplissement des tâches et dans le respect des prescriptions en matière de protection des données. Le Bureau a néanmoins recommandé de renforcer continuellement la formation et la sensibilisation du personnel.

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, 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. Il est prévu d'étendre cette obligation à l'ensemble des tâches publiques dans le cadre de la révision de la LCPD. 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, ce qui peut inclure, dans des cas déterminés, d'informer les personnes concernées.

Durant l'année sous revue, le Bureau a reçu le signalement de plusieurs incidents qui s'étaient produits chez des prestataires externes (à savoir Xplain AG, Concevis AG et Unico Data AG), dont certains avaient entraîné la divulgation de données à des personnes non autorisées. Ces incidents, dont les médias se sont emparés, ont montré que les autorités qui externalisent des traitements de données ne doivent pas négliger leur responsabilité dans le choix, l'instruction et le contrôle de leurs auxiliaires.

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 2023, 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 et il est l'interlocuteur des services de surveillance de la protection des données des collectivités de droit communal (art. 15, al. 3 OPD).

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

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

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 sur le recours à l'IA dans l'administration (technologie, premières applications pratiques, exigences au regard du droit constitutionnel). Privatim a rédigé un total de dix prises de position en réponse à des consultations de la Confédération, de la Conférence des gouvernements cantonaux et de la CCDJP. Elle en a mis certaines à la disposition de ses membres comme modèle de réponse. La conférence a eu des échanges avec des organisations ayant une activité intercantonale, notamment Administration numérique suisse, l'agence Educa, la nouvelle Organisation dommages sismiques, le groupe de travail Droit dans l'exécution des peines de la CCDJP et la corporation Technique et informatique policières Suisse, 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 avec le PFPDT sur des questions relatives au droit de la protection des données applicable et à la compétence en matière de surveillance de la protection des données qui en découle ainsi que sur les incidents de protection des données survenus chez des prestataires informatiques qui concernaient à la fois les autorités fédérales et les autorités cantonales (cf. 6.5.1 plus haut).

Groupes de travail de privatim

Le *groupe de travail Cyberadministration* a institué un sous-groupe dédié à l'IA, à qui il a demandé d'élaborer un référentiel propre à assurer la protection des données lors de l'utilisation de l'IA et d'identifier les éventuelles lacunes à combler au niveau législatif, en se basant sur la législation en vigueur dans le domaine de la protection des données et en tenant compte des travaux en cours au niveau de l'UE visant à réglementer l'IA.

Le *groupe de travail Sécurité* a accompagné la CCDJP dans ses travaux d'élaboration d'un concordat sur l'échange de données dans le domaine policier. Le Bureau juge que la formule du concordat est nettement mieux adaptée que l'approche consistant à prévoir dans les législations cantonales sur la police des habilitations unilatérales à communiquer automatiquement des données policières aux autres cantons. Il faut toutefois que ce concordat définisse les échanges de données prévus avec une précision suffisante et de manière proportionnée. Un blanc-seing qui laisserait aux organes d'exécution le soin de concrétiser la majeure partie du dispositif ne serait pas conforme aux exigences fondamentales de la Constitution en matière d'atteinte aux droits fondamentaux. Au cours de l'année sous revue, le groupe de travail a donné son avis sur un

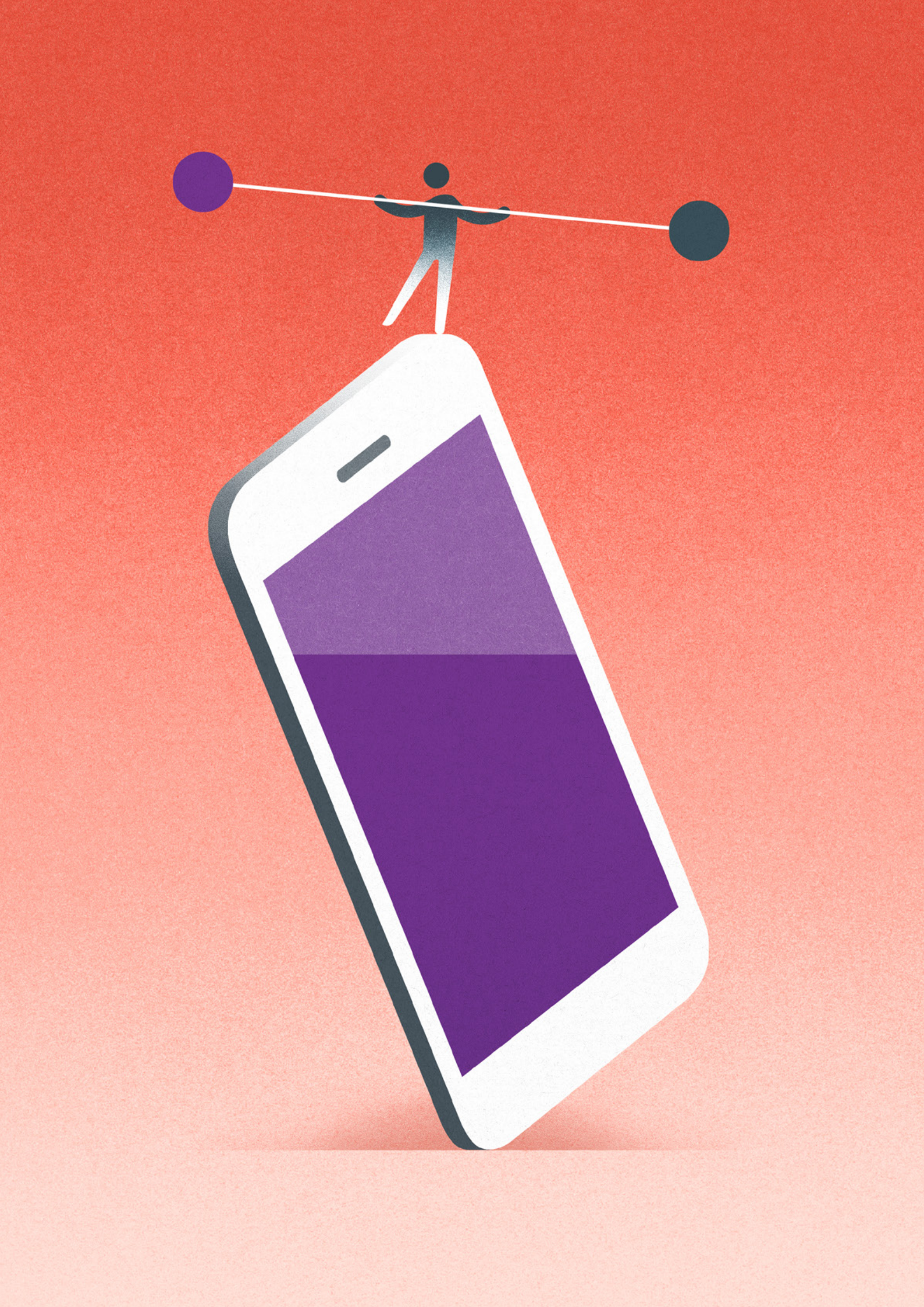
avant-projet lors d'une consultation restreinte informelle et il a réuni les éléments en vue de l'élaboration de la position formelle de privatim en réponse à la consultation publique ouverte par la CCDJP en novembre.

En 2023, le *groupe de travail Santé* s'est réuni sous la direction de la déléguée à la protection des données suppléante et responsable juridique, une fois à distance et une fois en présentiel. Les échanges ont porté notamment sur des projets de recherche et des registres médicaux (souvent en lien avec les projets de recherche discutés). Il a été question des champs de compétence de la législation fédérale et de la législation cantonale sur la protection des données, de l'articulation entre les commissions d'éthique et les autorités de protection des données au niveau cantonal ainsi que de la définition des cas dans lesquels un contrôle préalable est obligatoire. Ces questions complexes resteront à l'agenda du groupe de travail en 2024, qui réfléchira en outre à l'IA dans le secteur de la santé (p. ex. lorsqu'elle est utilisée comme aide aux diagnostics radiologiques).

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

Al.	Alinéa
Art.	Article
AVS	Assurance-vieillesse et survivants
AWS	Amazon Web Services
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CF	Contrôle des finances
CHA	Chancellerie d'État
CHB	Centre hospitalier Bienne
DSE	Direction de la sécurité
DSSI	Direction de la santé, des affaires sociales et de l'intégration
Fr.	Francs
GERES	Plateforme des systèmes des registres communaux
HIJP	Harmonisation de l'information dans la justice pénale
IA	Intelligence artificielle
IP	Internet Protocol
LAN	Loi sur l'administration numérique
LIAM	Loi sur l'information et l'aide aux médias
LCPD	Loi cantonale sur la protection des données
LP	Loi fédérale sur la poursuite pour dettes et la faillite
LPD	Loi fédérale sur la protection des données
LPJA	Loi sur la procédure et la juridiction administratives
LPol	Loi sur la police
LSIC	Loi sur la sécurité de l'information et la cybersécurité

M365	Microsoft 365
NFFS	Nouveau système de gestion des cas
OAC	Office de l'assurance-chômage
OAN	Office de l'agriculture et de la nature
OIAM	Ordonnance sur l'information et l'aide aux médias
OIO	Office d'informatique et d'organisation
OPD	Ordonnance sur la protection des données
VIS	Ordonnance sur le système central d'information sur les visas et sur le système national d'information sur les visas
PFPDT	Préposé fédéral à la protection des données et à la transparence
P-LArch	Projet de modification de la loi sur l'archivage
POCA	Police cantonale
privatim	Conférence des préposé(e)s suisses à la protection des données
RSI BE	Responsable de la sécurité de l'information
SIPD	Sûreté de l'information et protection des données
SRO AG	Spital Region Oberaargau (hôpital régional de Haute-Argovie)
STS AG	Hôpital Simmental-Thun-Saanenland
TIC	Technologies de l'information et de la communication
UE	Union européenne

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

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

www.be.ch/bpd