Rapport

Date de la séance du CE : 24 juin 2026
Direction : Direction de l'intérieur et de la justice
N° d'affaire : 2024.DIJ.1317
Classification : Non classifié

Ordonnance cantonale sur la protection des données (OCPD)

Table des matières

1. Synthèse 2

2. Contexte 3

3. Nouvelle réglementation 3
3.1 Caractéristiques de la nouvelle réglementation 3
3.2 Dispositions de l'OPD non reprises dans l'OCPD 4
3.2.1 Mesures techniques et organisationnelles 4
3.2.2 Obligations avant la mise en service 4
3.2.3 Publication sous forme électronique (communication à l'étranger) 5
3.2.4 Devoir d'information dans le cas d'une communication à l'étranger 5
3.2.5 Disposition sur les autorités communales de surveillance de la protection des données 5
3.2.6 Consultation de données de personnes décédées 6

4. Commentaire des articles 6
4.1 Traitement de données personnelles 6
4.1.1 Traitement par des tiers mandatés 6
4.1.2 Communication à l'étranger 9
4.2 Obligations des autorités et des tiers mandatés 11
4.2.1 Droits de la personne concernée 14
4.3 Autorité de protection des données, conseillère ou conseiller à la protection des données 16
4.4 Dispositions transitoires 19
4.5 Dispositions finales 19
4.6 Modifications indirectes 19
4.6.1 Ordonnance du 22 février 1995 fixant les émoluments de l'administration cantonale (ordonnance sur les émoluments ; OEmo) 20
4.6.2 Ordonnance du 21 décembre 2022 sur les procédures de consultation et de corapport (OPC) 20
4.6.3 Ordonnance cantonale du 11 novembre 2015 sur la géoinformation (OCGéo) 20
4.6.4 Ordonnance du 30 juin 2021 sur l'organisation et les tâches de la Direction de la santé, des affaires sociales et de l'intégration (ordonnance d'organisation DSSI, OO DSSI) et ordonnance du 18 octobre 1995 sur l'organisation et les tâches de la Direction des travaux publics et des transports (ordonnance d'organisation DTT, OO DTT) 20
4.6.5 Ordonnance du 5 décembre 2012 sur l'exercice de la prostitution (OEP) 20
4.6.6 Adaptations liées au nouveau titre de l'acte 21
4.6.7 Adaptation du nom de l'autorité de protection des données 21
4.6.8 Adaptation de la terminologie française concernant les données sensibles 22
4.6.9 Ordonnance du 20 janvier 2021 sur la plate-forme des systèmes des registres communaux (art. 8, al. 2 et annexe 2, ch. 2 O GERES) 22

4.7 Abrogation d'actes législatifs 25

5. Place du projet dans le programme gouvernemental de législature (programme législatif) et dans d'autres planifications importantes 25

6. Répercussions financières 25

7. Répercussions sur le personnel et l'organisation 26

8. Répercussions sur les communes 26

9. Répercussions sur l'économie 26

10. Résultat de la consultation 26
10.1 Transposition des dispositions sur la sécurité des données dans l'OSID 26
10.2 Ampleur du contrat avec des tiers mandatés 27
10.3 Définition des systèmes algorithmiques de prise de décision 27
10.4 Participation des communes aux frais de l'autorité cantonale de protection des données 28

1. Synthèse

La révision totale de l'ordonnance du 22 octobre 2008 sur la protection des données (OPD)[1] vise à créer les dispositions d'exécution nécessaires à la suite de la révision totale de la loi cantonale sur la protection des données (LCPD). Le titre de l'acte est changé, devenant l'ordonnance cantonale sur la protection des données, ainsi que le titre court (OCPD au lieu de OPD).

La matière réglée par l'ordonnance reprend dans une large mesure les dispositions de l'OPD : les normes concernant le blocage des données, le registre des fichiers, le droit d'accès, l'autorité de surveillance de la protection des données et les organes de contact pour la protection des données restent en substance inchangées.

Les nouveautés concernent notamment des dispositions d'exécution pour le traitement des données personnelles par des tiers mandatés et la communication à l'étranger. L'OCPD règle en outre le contenu minimal des contrats liant les autorités et les tiers par elles mandatés. Elle donne aussi les contours concrets des « garanties suffisantes », telles que requises par la LCPD lorsque des autorités communiquent des données à un État tiers dont le niveau de protection des données n'a pas été jugé adéquat par le Conseil fédéral. Ces prescriptions faciliteront l'application de la législation sur la protection des données pour les autorités. D'autres dispositions d'exécution de l'OCPD portent sur l'obligation d'inscrire au registre des fichiers et au registre des activités de traitement ainsi que sur l'obligation d'informer. Les systèmes algorithmiques de prise de décision au sens de la LCPD sont davantage définis, de même que les circonstances où leur utilisation fait naître l'obligation d'informer ou d'inscrire au registre des fichiers.

Les dispositions d'exécution de l'OPD qui traitaient des mesures techniques et organisationnelles pour garantir la sécurité des données sont transposées dans la nouvelle ordonnance sur la sécurité de l'information et des données (OSID)[2], qui se fonde aussi bien sur la loi sur la sécurité de l'information et la cybersécurité (LSIC)[3] que sur la LCPD.

Somme toute, l'OCPD concrétise la sécurité du droit pour les autorités, tenues de l'appliquer.

[1] RSB 152.040.1.
[2] Entrée au RSB encore inconnue.
[3] Entrée au RSB encore inconnue.

2. Contexte

Le 3 décembre 2025, le Grand Conseil a adopté la révision totale de la loi du 19 février 1986 sur la protection des données (LCPD)[4] et le nouvel acte entrera en vigueur le 1er septembre 2026. Cette révision avait pour but premier d'adapter la législation en matière de protection des données aux directives européennes et de garantir ainsi un niveau de protection des données approprié. Les principes constitutionnels pour boussole, la LCPD reprend le droit fédéral à chaque fois que cela paraît judicieux. La protection des données doit concilier la protection des droits fondamentaux des citoyennes et citoyens, d'une part, et l'intérêt de la communauté à l'accomplissement des tâches publiques, d'autre part.

Conformément à l'article 57 LCPD, le Conseil-exécutif édicte les dispositions nécessaires à l'exécution de la loi. C'est ce qu'il entend faire en arrêtant la révision totale de l'ordonnance sur la protection des données. Le titre court de l'ordonnance prêtant à confusion avec celui de l'ordonnance fédérale sur la protection des données en allemand[5], la hiérarchie des normes a été mise en évidence dans l'intitulé complet par l'ajout de l'adjectif « cantonale » et le libellé bref a été modifié en conséquence (OCPD).

La systématique de l'ordonnance découle de la LCPD dans sa nouvelle forme. Les dispositions d'exécution se répartissent comme suit :

1. Traitement de données personnelles
2. Obligations des autorités et des tiers mandatés
3. Droits de la personne concernée
4. Autorité de protection des données, conseillère ou conseiller à la protection des données
5. Dispositions transitoires et dispositions finales

Par rapport à l'ordonnance actuellement en vigueur, l'ordre des éléments a été fondamentalement revu.

Les dispositions d'exécution qui concernaient les mesures techniques et organisationnelles visant à garantir la sécurité des données sont introduites dans une nouvelle ordonnance, l'OSID, qui procède aussi bien de la LSIC que de la LCPD.

3. Nouvelle réglementation

3.1 Caractéristiques de la nouvelle réglementation

La matière réglée par l'ordonnance reprend dans une large mesure les dispositions actuellement en vigueur : les normes concernant le blocage des données, le registre des fichiers, le droit d'accès, l'autorité de surveillance de la protection des données et les organes de contact pour la protection des données restent en substance inchangées. Des adaptations rédactionnelles et terminologiques sont toutefois apportées, voire des changements sur le fond, lorsque la technique législative en vigueur ou le droit supérieur l'exigent.

D'autres éléments sont nouveaux. La LCPD prévoyait leur caractérisation par voie d'ordonnance. Ils concernent surtout le traitement des données personnelles par des tiers mandatés et la communication à l'étranger, les obligations pour les autorités de constituer un fichier avant

[4] RSB 152.04.
[5] RS 235.11.

toute mise en service, les obligations d'inscrire au registre des fichiers et au registre des activités de traitement, les droits de la personne concernée ainsi que l'autorité de protection des données, les conseillères et les conseillers à la protection des données. Par ailleurs, différentes ordonnances font l'objet d'une modification indirecte afin de régler les contradictions, les lacunes ou les incertitudes créées par la présente révision dans la législation spéciale.

La LSIC, édictée en parallèle de la révision de la législation sur la protection des données, vise à garantir la sécurité des informations lors de leur traitement et la sécurité de l'utilisation d'outils TIC par les autorités (art. 1 LSIC). Mené par la Direction des finances (FIN), le projet législatif a été adopté par le Grand Conseil le 12 juin 2025 (la date de l'entrée en vigueur n'est pas encore connue). Là où la LSIC veille à la protection des informations factuelles d'intérêt public, la LCPD se concentre sur celle des données personnelles et sur la garantie du droit constitutionnel à la protection des données des personnes physiques et morales. Si les biens juridiques protégés par la LSIC et la LCPD ne sont pas les mêmes, les deux actes n'en restent pas moins liés l'un à l'autre, puisque les principes de la législation sur la sécurité de l'information et la cybersécurité s'appliquent par analogie dans le domaine couvert par la LCPD (art. 10, al. 2 LCPD). Les deux projets ont donc pour point commun la sécurité des données, raison pour laquelle leurs dispositions d'exécution respectives en la matière ont été réunies dans l'OSID. L'occasion a été saisie pour transposer bon nombre de dispositions figurant jusque-là dans l'OPD dans l'OSID plutôt que dans l'OCPD (voir à cet égard les explications du point 2.2).

3.2 Dispositions de l'OPD non reprises dans l'OCPD

3.2.1 Mesures techniques et organisationnelles

Les articles 4 à 6 OPD réglaient jusqu'à présent la manière dont l'autorité responsable devait assurer la confidentialité, la disponibilité et l'exactitude des données par des mesures techniques et organisationnelles. Vu que ces dispositions techniques portent sur la sécurité des données (voir à cet égard les explications du point 2.1), elles sont reprises dans l'OSID plutôt que dans l'OCPD.

L'obligation d'annoncer en cas de violations de la sécurité des données (art. 26 LCPD) a été introduite avec l'adoption de la révision totale de la LCPD. Compte tenu du rapport thématique étroit qui la lie aux mesures susmentionnées, les dispositions d'exécution traitant de ce point sont réglées dans l'OSID.

3.2.2 Obligations avant la mise en service

Jusqu'à présent, les articles 7 à 9 OPD réglaient la mise en œuvre de l'ancienne LCPD quant au devoir de l'autorité de consulter l'autorité de surveillance en vue d'un contrôle préalable lorsqu'était prévu le traitement de certaines données personnelles pour un nombre important de personnes (devoir que l'on nomme obligation avant la mise en service).

Désormais, les obligations avant la mise en service sont réglées aux articles 18 à 20 LCPD : l'autorité vérifie par une analyse des risques si les traitements de données personnelles répétés qui sont envisagés entraînent un risque élevé pour les personnes concernées et, le cas échéant, une analyse d'impact relative à la protection des données personnelles doit être effectuée (art. 18 et 19 LCPD). Dans certains cas, l'autorité doit soumettre les traitements de données personnelles répétés qui sont envisagés à l'autorité de protection des données compétente en vue de sa prise de position, c'est-à-dire pour un contrôle préalable (art. 20 LCPD).

Les obligations avant la mise en service sont des instruments essentiellement pensés pour contrôler la sécurité des données. Par conséquent, elles ne sont pas concrétisées dans l'OCPD, mais dans l'OSID.

3.2.3 Publication sous forme électronique (communication à l'étranger)

L'article 15b de la loi du 2 novembre 1993 sur l'information et l'aide aux médias (LIAM)[6] crée la base légale habilitant les autorités à communiquer des données personnelles sur Internet dans la mesure où cela est nécessaire pour remplir leur mandat d'information. Il n'y a donc plus besoin qu'une base explicite de la législation sur la protection des données rende admissible la publication de données personnelles sur Internet. Le commentaire de l'article 15b LIAM établit en outre clairement que la communication de données personnelles en ligne n'est pas assimilée à une communication à l'étranger[7].

L'article 2 OPD n'a par conséquent plus de raison d'être.

3.2.4 Devoir d'information dans le cas d'une communication à l'étranger

L'article 17 du protocole[8] portant amendement à la convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après : STE n° 108+) prévoit pour l'adaptation de l'article 14, paragraphe 5 de la convention susmentionnée (STE n° 108) un devoir d'information à l'autorité de protection des données dans la mesure où les données sont communiquées à l'étranger sur la base des garanties du paragraphe 3, lettre *b*. La LCPD dans sa teneur avant révision instituait aussi un devoir d'information à cet égard (art. 14a, al. 3 aLCPD). Au niveau fédéral, la loi ne prévoit rien de plus que l'information, sur demande, des communications en relation directe avec la conclusion d'un contrat dans l'intérêt de la personne concernée, ainsi que celles nécessaires à la sauvegarde d'un intérêt public prépondérant, celles nécessaires pour la défense de droits ou celles nécessaires pour la protection de la personne concernée (art. 17, al. 2 LPD).

Quant au droit cantonal, il ne requerra pas non plus que l'autorité de protection des données soit informée de chaque communication à l'étranger. Une autorité pourra se contenter avant toute communication d'annoncer les clauses contractuelles selon l'article 3, alinéa 1, lettre *b* OCPD dès lors qu'elle y recourt. Si l'obligation d'annoncer à l'autorité de protection des données est remplie, toutes les communications subséquentes sont considérées comme avalisées dans la mesure où les mêmes garanties sont offertes (voir le commentaire de l'art. 3, al. 2).

De plus, l'autorité de protection des données peut elle-même recueillir des informations sur la base de l'article 46, alinéa 2, lettre *a* LCPD. Une disposition expresse dans l'OCPD au sens de l'article 17, alinéa 2 LPD n'est donc pas nécessaire.

3.2.5 Disposition sur les autorités communales de surveillance de la protection des données

Aujourd'hui, chaque commune et tout autre collectivité de droit communal dispose, pour son domaine, de sa propre autorité de surveillance qui assume le rôle d'autorité de protection des données. La présente révision doit offrir un cadre où les tâches de surveillance sont centralisées et

[6] RSB 107.1.
[7] Rapport sur la loi sur l'information du public, devenue la loi sur l'information et l'aide aux médias, p. 28.
[8] FF 2020 577.

la charge des communes allégée. En principe, les tâches de protection des données qui relevaient jusqu'à présent des autorités communales désignées à cet effet sont reprises par l'autorité cantonale. Font exception les quatre communes les plus peuplées du canton (Berne, Biel/Bienne, Köniz et Thoune) ainsi que d'autres collectivités de droit communal (voir l'art. 42 LCPD). Le niveau de la protection des données doit s'en trouver relevé et l'allocation des ressources gagner en efficience.

Les communes et les autres collectivités de droit communal fixent elles-mêmes l'élection et l'organisation de leur autorité de protection des données lorsqu'elles en désignent une pour leur domaine (art. 42, al. 2 LCPD), de sorte que la disposition sur les compétences en matière d'autorisation de dépenses des communes qui figurait à l'article 14 OPD n'a pas besoin d'être reprise.

3.2.6 Consultation de données de personnes décédées

La consultation de données de personnes décédées est actuellement régie par l'article 12 OPD. Le Tribunal administratif a jugé cet article contraire à la loi, les données des personnes décédées n'étant pas des données personnelles et n'entrant ainsi pas dans le champ d'application de la LCPD. La disposition ne découle donc d'aucune norme de délégation, c'est-à-dire d'aucune base dans la loi au sens strict[9].

La Confédération n'a d'ailleurs pas repris de disposition à cet égard dans sa nouvelle ordonnance (ordonnance du 31 août 2022 sur la protection des données, OPDo).

Au vu de ce qui précède, l'article 12 ne doit pas être transposé dans la nouvelle ordonnance.

4. Commentaire des articles

4.1 Traitement de données personnelles

4.1.1 Traitement par des tiers mandatés

Article 1 – Contenu du contrat

Alinéa 1

Si elle entend confier le traitement de données personnelles à des tiers, l'autorité conclut un contrat avec eux.

Le contrat doit être écrit. La forme écrite doit ici être comprise au sens de l'article 3 de l'ordonnance du 11 janvier 2023 sur l'administration numérique (OAN)[10] : elle est réputée respectée si la procédure est effectuée sous une forme numérique permettant d'établir la preuve par un texte. La présente disposition s'efface devant d'éventuelles conditions formelles plus strictes qui découleraient du droit des obligations (signature écrite à la main ou signature électronique qualifiée selon l'art. 14 du Code des obligations [CO][11]) ou du droit d'organisation de l'administration (p. ex. prescriptions en matière d'acquisition).

[9] Jugement du Tribunal administratif 100.2023.151U du 22 mai 2025, c. 4.1 ss.
[10] RSB 109.111.
[11] RS 220.

Alinéa 2

Le contrat doit prévoir l'objet et l'étendue du traitement des données (lit. *a*). Il doit aussi limiter le traitement à son but, excluant toute autre finalité, dont celles qui seraient propres aux tiers mandatés (lit. *b*). Les tiers mandatés ont le droit de traiter les données, mais de la même manière que l'autorité habilitée à le faire seulement (art. 12, al. 1, lit. *a* LCPD), ce qui explique l'importance des deux éléments précédents du contrat.

L'autorité doit prévoir contractuellement que les tiers mandatés sont soumis aux obligations de garder le secret (lit. *c*). Aucune de ces obligations ne doit s'opposer à la sous-traitance du traitement ; mandater des tiers serait sinon inadmissible (art. 12, al. 1, lit. *b* LCPD).

Les règles à suivre à la réception de demandes de renseignements (lit. *d*) figurent aussi au contrat. Une clause doit en particulier indiquer qu'il revient à l'autorité et non pas aux tiers mandatés d'administrer l'accès aux renseignements (voir l'art. 29, al. 3 LCPD). Il est par ailleurs nécessaire de définir à quel organe de l'autorité les tiers mandatés peuvent s'adresser à la réception d'une telle demande et qui compile les informations nécessaires.

Selon la lettre *e*, le contrat stipule en outre les mesures prises par les tiers mandatés afin de protéger les données personnelles. L'autorité peut ainsi s'assurer, par la force obligatoire du contrat, que les tiers mandatés garantissent la sécurité des données (voir l'art. 12, al. 2 LCPD). Il convient de noter que les éléments contractuels se rapportant à la sécurité des données sont régis par la LSIC et l'OSID, qui règlent le domaine dans le détail.

L'autorité restant responsable du traitement de données (art. 11 LCPD), il lui incombe d'en contrôler l'exécution. Ce principe est ancré à la lettre *f*. La lettre *g* ajoute au contenu obligatoire du contrat les aspects de sa durée et des conditions de sa résiliation.

Le contrat doit prévoir la forme et les conditions à respecter pour que les tiers mandatés puissent déléguer le traitement à d'autres personnes (sous-traitance). Selon le droit européen, le contrat doit revêtir la forme écrite, la forme électronique étant acceptée (art. 22 de la directive [UE] 2016/680)[12]. Quant aux conditions, il ne peut y avoir sous-traitance sans accord de l'autorité. Cet accord peut être de nature spécifique ou générale (voir le commentaire de l'art. 2).

Les autorités de protection des données contrôlent, de leur propre initiative ou à la suite d'une dénonciation, si les autorités et les tiers mandatés respectent les dispositions de protection des données, y compris de sécurité des données (art. 46, al. 1 LCPD). Dans le cas d'une sous-traitance, les obligations contractuelles et les droits de contrôle doivent aussi s'appliquer aux personnes auxquelles les tiers mandatés ont délégué des tâches. Ce point doit être stipulé dans le contrat passé par l'autorité et ces derniers (lit. *i*).

L'obligation de tenir un registre faite à une autorité conformément à l'article 22 LCPD s'impose également aux tiers mandatés (voir l'art. 8). Les parties contractantes doivent en convenir.

Dernier point, les sanctions en cas de manquements aux obligations doivent être prévues contractuellement. Les peines conventionnelles en sont un exemple typique. Il est aussi possible de prévoir qu'*aucune* peine conventionnelle ne sera infligée.

Tous ces aspects forment les éléments essentiels du contrat. Libre aux parties d'élargir le contenu de celui-ci.

L'article 1 porte sur des contrats innommés, c'est-à-dire des contrats qui ne font l'objet de règles expresses ni dans le CO ni dans une loi spéciale. La qualification de ces contrats, de droit privé ou administratif, et donc la définition du régime juridique applicable et des instances

[12] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

compétentes répondent aux critères déterminants du droit administratif[13]. Dans toute la mesure du possible, les autorités conviennent avec leurs partenaires au contrat, idéalement, que le droit suisse est applicable et que tout éventuel litige sera tranché par un tribunal suisse. L'article 17, alinéa 1 de l'ordonnance du 5 novembre 2014 sur l'organisation des marchés publics (OOMP)[14] doit en outre être observé : les conditions générales et les modèles de contrat du canton doivent être utilisés[15]. Ils prévoient l'ensemble des dispositions en matière de for et de droit applicable.

Alinéa 3

Il arrivera que l'autorité ne puisse pas fixer contractuellement l'ensemble des clauses de l'alinéa 2, en particulier lorsqu'elle sera sommée d'accepter les conditions générales non négociables des tiers mandatés. C'est pour ces cas qu'a été conçu l'alinéa 3 selon lequel expressément d'autres mesures doivent minimiser les risques (relevant du droit de la protection des données).

Les « autres mesures appropriées » à prendre seront déterminées dans chaque cas par les éléments de l'alinéa 2 qui n'auront pas pu faire l'objet d'une convention entre l'autorité et les tiers mandatés ainsi que par les potentielles conséquences relevant du droit de la protection des données. Une règle est inéluctable : les données personnelles peuvent être traitées par des tiers mandatés à la condition qu'elles le soient de la même manière que l'autorité elle-même est habilitée à le faire ; les tiers mandatés garantissent la sécurité des données et la délégation du traitement à d'autres personnes n'est pas possible sans l'accord préalable de l'autorité (art. 12 LCPD). Cela signifie qu'il leur incombe de respecter toutes les dispositions réglant la protection des données auxquelles l'autorité elle-même est soumise. Ces dispositions sont à chercher non seulement dans la LCPD, dans la LSIC et l'OSID (pour ce qui a trait à la sécurité des données), mais aussi dans le droit spécial (droit matériel de la protection des données). Si les autorités ne parviennent pas à garantir le respect de toutes les conditions de l'article 12 LCPD, seules des mesures de sécurité des données comme le chiffrement ou la pseudonymisation permettront d'assurer que les conditions en matière de protection des données sont réunies.

Article 2 – Délégation du traitement à une autre personne

L'article 1 prévoit que le contrat passé entre l'autorité et les tiers mandatés règle notamment les conditions qui permettent à ces derniers de déléguer le traitement des données à d'autres personnes.

L'article 12, alinéa 3 LCPD définit le cadre de la sous-traitance : les tiers mandatés ne peuvent pas déléguer le traitement à d'autres personnes sans l'accord préalable de l'autorité.

Selon l'article 22, paragraphe 2 de la directive (UE) 2016/680, l'accord peut être « spécifique » ou « général ». La Confédération met cette prescription en œuvre pour l'ensemble du secteur public par l'article 7 OPDo[16]. C'est aussi ce que prévoit l'article 2 OCPD. L'accord préalable peut être de nature générale (pour tous les cas de sous-traitance) ou spécifique (pour une sous-traitante ou un sous-traitant précis).

Si l'autorité et les tiers mandatés conviennent qu'un accord général est suffisant, ces derniers doivent informer l'autorité lorsqu'ils veulent remplacer la sous-traitante ou le sous-traitant ou recourir à d'autres personnes. L'autorité a alors la possibilité de s'opposer au changement envisagé.

[13] Blattmann Veronica in : Baeriswyl Bruno/Rudin Beat (édit.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), Zurich – Bâle – Genève, 2012, § 6, n. 19.
[14] RSB 731.22.
[15] Voir : https://www.kaio.fin.be.ch/fr/start/themen/oeffentliches-beschaffungswesen/rechtliches/allgemeine-geschaeftsbedingungen.html (dernière consultation : 19.05.2026).
[16] Voir à cet égard : rapport explicatif de l'ordonnance fédérale sur la protection des données, p. 30.

4.1.2 Communication à l'étranger

Article 3 – Garanties suffisantes

L'autorité peut communiquer des données personnelles à l'étranger si un niveau de protection approprié peut être garanti (art. 15, al. 1 LCPD). Elle peut partir du principe que c'est le cas dans les États tiers qui se trouvent dans le tableau de l'annexe 1 OPDo et pour lesquels une décision d'adéquation est donc disponible.

Selon la LCPD, l'autorité peut aussi communiquer des données personnelles à l'étranger si un niveau de protection approprié peut faire l'objet d'autres garanties suffisantes (art. 15, al. 1, lit. *c* LCPD).

Alinéa 1

Les clauses types de protection des données, approuvées en amont, établies et reconnues par le Préposé fédéral à la protection des données et à la transparence (PFPDT) offrent des garanties suffisantes au sens de l'article 15, alinéa 1, lettre *c* LCPD (lit. *a*). Le recours à ces clauses n'implique pas d'obligation d'informer l'autorité de protection des données.

Le PFPDT publie sur son site Internet des informations sur la communication de données personnelles à l'étranger[17]. Elle ou il y fait en particulier figurer la liste des clauses types de protection des données approuvées, établies ou reconnues par ses soins (à ce sujet, voir aussi l'art. 10, al. 2 OPDo)[18]. Actuellement, les éléments suivants font foi :

Les clauses types de protection des données correspondent aux clauses contractuelles types (CTT) de l'annexe de la décision d'exécution (UE) 2021/914 (*Standard Contractual Clauses*, SCC) [19]. Elles renvoient au règlement (UE) 2016/679 (ci-après : règlement général sur la protection des données)[20]. Le PFPDT reconnaît ces CTT, y compris leurs modules, sous réserve qu'elles soient modifiées et complétées si nécessaire dans des cas d'espèce. La manière de procéder à cet égard est décrite par le PFPDT dans son rapport intitulé « Transfert de données personnelles dans un pays ne présentant pas le niveau de protection des données adéquat, en application de clauses types de protection des données au sens de l'art. 16, al. 2, let. d, LPD »[21].

Le PFPDT reconnaît également comme clause type de protection des données le module de clauses contractuelles types pour le transfert de données à caractère personnel conformément à l'article 14, paragraphe 3, lettre *b* STE nº 108+ (*Model Contractual Clauses for the Transfer of Personal Data*, MCC)[22].

Lorsque des clauses types de protection des données sont élaborées par les autorités fédérales ou des personnes privées et que le PFPDT les approuve, elles sont publiées sur son site Internet[23].

Selon les circonstances, d'autres dispositions contractuelles que les clauses types mentionnées ci-dessus peuvent offrir le niveau de protection des données approprié (lit. *b*). Ces dispositions, décidées par l'autorité ou les tiers mandatés et la co-contractante ou le co-contractant, doivent

[17] Voir : www.edoeb.admin.ch/fr/communication-de-donnees-a-letranger (dernière consultation : 20.05.2026).
[18] Voir : PFPDT, Transfert de données personnelles dans un pays ne présentant pas le niveau de protection des données adéquat, en application de clauses types de protection des données au sens de l'art. 16, al. 2, let. d, LPD, téléchargeable à l'adresse suivante : www.edoeb.admin.ch/fr/communication-de-donnees-a-letranger (dernière consultation : 20.05.2026).
[19] La décision d'exécution (UE) 2021/914 du 4 juin 2021 est téléchargeable à l'adresse suivante : http://data.europa.eu/eli/dec_impl/2021/914/oj (dernière consultation : 20.05.2026).
[20] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[21] Voir : PFPDT, *op. cit.*, p. 3 s.
[22] Voir : PFPDT, *op. cit.*, p. 7.
[23] Voir à cet égard : rapport explicatif de l'ordonnance fédérale sur la protection des données, p. 35 s.

comprendre les éléments énoncés à l'article 4 et doivent être transmises à l'autorité de protection des données avant toute communication en vertu de l'alinéa 2.

L'énumération des garanties suffisantes à l'article 3, alinéa 1 est exhaustive. Elle s'inspire de celle fournie par l'article 16, alinéa 2, lettres *b* à *d* LPD, mais ne fait pas de distinction supplémentaire entre les « clauses de protection des données » et les « garanties spécifiques ». La raison en est la suivante : selon le rapport explicatif de l'OPDo, « [d]*ans le secteur privé,* [la] *garantie peut être fournie par des clauses de protection des données d'un contrat entre le responsable du traitement ou le sous-traitant et son co-contractant* » et « [d]*ans le secteur public, il peut s'agir de garanties spécifiques élaborées par l'organe fédéral compétent* »[24]. Or la LCPD n'est applicable que pour les traitements de données personnelles du fait des autorités cantonales. La distinction opérée dans le texte fédéral n'est donc pas nécessaire. L'OCPD n'utilise toutefois pas le terme de « garanties spécifiques », mais celui d'« autres clauses contractuelles ». Cette solution a été retenue dans différents cantons également (voir § 23, alinéa 1, lettre *b* de la loi sur l'information et la protection des données du canton de Bâle-Ville [Gesetzes über die Information und den Datenschutz des Kantons Basel-Stadt, Informations- und Datenschutzgesetz, IDG][25] et § 21, alinéa 1, lettre *b* de la loi sur l'information et la protection des données du canton de Bâle-Campagne [Gesetzes über die Information und den Datenschutz des Kantons Basel-Land, Informations- und Datenschutzgesetz, IDG][26]).

Alinéa 2

Si à l'heure d'élaborer un contrat une autorité se fonde sur des clauses au sens de l'article 3, alinéa 1, lettre *b* (voir le commentaire ci-dessus), elle doit le communiquer en amont à l'autorité de protection des données. Les dispositions ne sont toutefois pas soumises à l'approbation de cette dernière. La communication de données personnelles à l'étranger est admise dès que les clauses contractuelles ont été portées à la connaissance de l'autorité de protection des données, tant qu'elles sont au bénéfice de ces garanties.

Le devoir d'information ne s'applique pas à chacune des communications. Après que l'autorité de protection des données a pu prendre connaissance des clauses contractuelles selon l'article 3, alinéa 1, lettre *b*, l'existence des garanties est présumée sur le long terme, sauf modification des dispositions contractuelles néanmoins. Cette présomption implique donc que les catégories de données communiquées (art. 4, al. 1, lit. *b*), le type et la finalité du traitement (art. 4, al. 1, lit. *c*) et les catégories de destinataires (art. 4, al. 1, lit. *f*) demeurent inchangés par exemple.

Alinéa 3

L'exportatrice ou l'exportateur des données, c'est-à-dire l'autorité ou les tiers mandatés qui communiquent les données personnelles, prennent les mesures appropriées pour que les garanties suffisantes au sens de l'alinéa 1 soient respectées par les destinataires à l'étranger.

L'autorité peut notamment s'assurer que les tiers mandatés respectent effectivement les dispositions contractuelles par une vérification ou par des audits.

Cette prescription vise à assurer que les destinataires des données communiquées respectent effectivement le cadre régissant la protection des données en Suisse.

[24] Voir à cet égard : rapport explicatif de l'ordonnance fédérale sur la protection des données, p. 34.
[25] Recueil systématique du canton de Bâle-Ville : SG 153.260.
[26] Recueil systématique du canton de Bâle-Campagne : SGS 162.

Article 4 – Autres clauses contractuelles

Alinéa 1

Les garanties suffisantes au sens de l'article 3 peuvent être apportées par des clauses types de protection des données, mais aussi par des dispositions contractuelles entre l'autorité ou les tiers mandatés et leurs partenaires.

Les autorités doivent seulement communiquer les clauses de protection des données ou les garanties spécifiques à l'autorité de protection des données. Cette dernière n'a pas besoin d'approuver les dispositions contractuelles. Il existe donc un certain risque que les autorités et les tiers mandatés interprètent différemment le degré de protection que ces garanties doivent permettre d'atteindre. Le Conseil-exécutif juge donc pertinent de soumettre ces clauses à des standards déterminés. C'est à cet effet que l'article 4, alinéa 1 règle le contenu minimal des garanties suffisantes au sens de l'article 3, alinéa 1, lettre *b*. Dans un souci d'exhaustivité, cette disposition englobe tous les éléments, même ceux qui découlent obligatoirement de la LCPD (p. ex. lit. *a*). La teneur de la disposition est similaire au droit fédéral (art. 9 OPDo).

Voici ce que le contrat doit prévoir au moins :

- l'application des principes de la licéité, de la finalité, de la proportionnalité, de la transparence et de l'exactitude, ces fondamentaux valant également pour les destinataires des données ;
- les catégories des personnes concernées ainsi que des données personnelles communiquées, dont les noms, les adresses, les données sur la santé et sur l'origine ethnique ;
- le type et la finalité d'une éventuelle communication des données personnelles ;
- les destinataires ou les catégories de destinataires ;
- le nom des États ou des organes internationaux, le cas échéant, auxquels sont destinées les données personnelles, et les conditions applicables à la communication ;
- les règles de conservation, d'archivage et de destruction des données personnelles ;
- les mesures visant à garantir la sécurité des données ;
- l'obligation qu'ont les destinataires d'annoncer les violations de la sécurité des données ;
- l'obligation pour les destinataires qui sont des autorités d'informer les personnes concernées par le traitement des données ;
- les droits de la personne concernée.

Si les destinataires ne peuvent pas se prévaloir d'une décision d'adéquation (voir les indications plus haut à ce propos) et s'il n'a pas non plus été possible de convenir de clauses types de protection des données ou de dispositions contractuelles au sens de l'article 4, il faut partir du principe que les garanties d'un niveau de protection approprié ne sont pas données (art. 15, al. 1, lit. *c* LCPD). L'exportation des données personnelles n'est alors pas admissible. Ces données peuvent être communiquées seulement si leur chiffrement est suffisant pour empêcher les destinataires d'y reconnaître un caractère personnel.

4.2 Obligations des autorités et des tiers mandatés

Le chapitre sur les obligations des autorités et des tiers mandatés comporte des dispositions sur l'obligation d'inscrire au registre des fichiers et au registre des activités de traitement (art. 21 ss LCPD) ainsi que sur l'obligation d'informer (art. 23 LCPD).

Article 5 – Portée de l'obligation d'inscrire au registre et de l'obligation des autorités de poursuite pénale et des tribunaux pénaux de tenir un registre

La disposition règle le contenu des registres en application de l'article 21, alinéa 3 LCPD et de l'article 22 en relation avec l'article 57 LCPD.

Alinéa 1

Le registre contient au moins des indications sur l'autorité responsable et ses coordonnées (lit. *a*), la base juridique et le but du fichier ou du traitement (lit. *b*), les données personnelles traitées ou leurs catégories ainsi que leur étendue (lit. *c*), les données personnelles qui sont régulièrement communiquées à d'autres autorités ou à des personnes privées ainsi que les destinataires de la communication (lit. *d*) et le délai de conservation (lit. *e*).

La disposition se fonde sur l'article 24 de la directive (UE) 2016/680 ainsi que sur la teneur actuelle de l'article 18 LCPD. La liste n'est pas exhaustive. Selon l'article 24 de la directive (UE) 2016/680, l'inscription au registre peut aussi comprendre le recours au profilage, la communication de données personnelles à l'étranger, le délai de conservation des données personnelles ou les mesures techniques et organisationnelles.

Article 6 – Exception à l'obligation d'inscrire au registre

L'article 6 désigne les fichiers qui n'ont pas besoin d'être inscrits au registre.

Conformément au droit en vigueur, les fichiers tenus à court terme et ceux déjà publiés autrement ne sont pas inscrits au registre. En raison de leur brève existence, les fichiers qui n'auront jamais plus de deux ans figurent au nombre des exceptions prévues (lit. *a*). L'ordonnance actuelle vise les fichiers qui sont « utilisés » pendant deux ans au plus. Ce verbe prête à confusion et pourrait induire en erreur, raison pour laquelle la formulation est revue. L'accent sera dorénavant mis sur la durée de la constitution du fichier, devant refléter la durée de sa gestion active. Ainsi, un fichier conservé plus de deux ans doit figurer au registre, qu'il soit utilisé ou non.

C'est le recueil qui est déterminant et non chacune des entrées de celui-ci. Si les fichiers sont de toute manière accessibles au public, il n'est pas nécessaire de procéder à une inscription au registre pour fournir les métadonnées de leur contenu (lit. *b*). Les lettres *a* et *b* portent sur les fichiers dans leur ensemble. Cela signifie qu'ils doivent être soit constitués pour une brève durée soit accessibles au public dans leur intégralité.

À la différence de la situation qui prévaut actuellement, les données qui seront finalement versées aux archives du canton ou d'une commune doivent aussi apparaître au registre. La lettre *b* est applicable pour autant que les données soient accessibles au public.

La lettre *c*, quant à elle, prévoit une nouvelle réglementation concernant les données personnelles au sens de l'article 4, alinéa 1 de l'ordonnance du 14 décembre 2005 sur la communication de données personnelles (OCDP)[27]. Ces données non plus ne doivent pas être inscrites au registre. Il s'agit exclusivement des données personnelles des autorités au sens de l'article 2, alinéa 1, lettre *i* LCPD qui sont listées de la lettre *a* à la lettre *l* OCDP (nom et prénom, fonction, formule d'appel et titre, langue officielle utilisée, adresse postale professionnelle, adresse électronique professionnelle, numéros de téléphone et de télécopie professionnels, place occupée dans l'organisation de l'administration ou de l'entreprise, indications sur la suppléance et le secrétariat, données techniques concernant les systèmes et services informatiques utilisés, notamment les clés, signatures ou certificats numériques publics, photos ou enregistrements vocaux). Le risque pour les personnes concernées étant nul ou tout au plus faible, l'obligation d'inscrire au registre n'a pas lieu d'être (art. 21, al. 4 LCPD).

[27] RSB 152.041.1.

Les exceptions de la disposition ne valent que pour le registre au sens de l'article 21 LCPD. Contrairement à ce que prévoit l'article 22 LCPD, l'article 24 de la directive (UE) 2016/680 ne permet pas d'exception concernant les autorités de poursuite pénale et les tribunaux pénaux.

Article 7 – Obligation d'annoncer et d'inscrire au registre en cas d'utilisation de systèmes algorithmiques de prise de décision

Selon l'article 21, alinéa 2, lettre *c* LCPD, il est obligatoire d'inscrire au registre les systèmes algorithmiques de prise de décision qui présentent un risque élevé pour les personnes concernées. De plus, l'autorité doit informer la personne concernée lors de la collecte de données personnelles de l'utilisation de systèmes algorithmiques de prise de décision présentant un risque élevé pour elle (art. 23, al. 2, lit. *c* LCPD).

À propos de ces systèmes, le rapport explicatif qui accompagnait la LCPD précisait : « L'intelligence artificielle au sens d'une machine capable de penser et d'agir d'elle-même comme un " être humain " n'existe pas pour l'heure et n'existera pas dans un avenir proche. En réalité, les systèmes de prise de décision sont conçus par des êtres humains et fonctionnent, à partir d'une analyse de données, en développant et proposant des solutions à des problèmes ou des domaines déterminés. »[28]

L'article 7 tient compte de ce qui précède, s'inspire notamment de la définition du Parlement européen[29] et décrit ce que sont les systèmes algorithmiques de prise de décision (*algorithmic decision-making*, ADM) au sens des articles 21, alinéa 2, lettre *c* et 23, alinéa 2, lettre *c* LCPD. Ces systèmes ont un fonctionnement automatisé, produisent ou précèdent des décisions à l'égard de personnes (en formulant des recommandations ou en exerçant une influence), qui relèvent du pouvoir d'appréciation quant aux conditions d'application ou aux conséquences juridiques. Une intervention humaine peut être nécessaire, mais un fonctionnement entièrement automatisé est aussi possible[30].

Si un système algorithmique de prise de décision se contente, par exemple, de vérifier qu'un dossier de candidature est arrivé dans les délais, il n'a aucune liberté d'action dans le processus de recrutement. Ce n'est par contre pas le cas s'il peut soumettre les profils à un contrôle en vue de déterminer s'ils remplissent les critères individuels définis par l'autorité. La liberté d'action porte alors sur le plan factuel. Il touche en outre aux conséquences juridiques dès lors que l'évaluation des candidates et des candidats décide de leur accession au reste du processus de sélection.

En présence d'un système algorithmique de prise de décision au sens de la définition donnée à l'article 7, alinéa 1, il convient de juger au cas par cas du degré de risque pour la personne concernée.

Le risque est élevé quand l'utilisation d'un tel système peut avoir un effet notable sur la personne concernée. Les circonstances du cas d'espèce sont les seules qui permettent de savoir si cet effet peut s'avérer notable. Par effet notable, on comprend notamment la possibilité que le système entraîne des conséquences juridiques négatives pour la personne concernée. Ce cas de figure se présente lorsque, selon l'évaluation, le profil d'une personne ne correspond pas à un poste et qu'elle se trouve exclue du processus de recrutement.

[28] Öktem, Rosa, Algorithmische Entscheidungssysteme, menschenrechtliche Vorgaben und Entwicklungen auf internationaler Ebene. In : Deutsches Institut für Menschenrechte (édit.), 2021, p. 1, disponible à l'adresse : https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/Publikationen/Information/Information_Algorithmische_Entscheidungssysteme.pdf (dernière consultation : 20.05.2026).

[29] Voir également pour la définition : European Parliamentary Research Service, Scientific Foresight Unit (STOA), Understanding algorithmic decision-making: Opportunities and challenges, 2019, p. 3 s., disponible à l'adresse : https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf (dernière consultation : 20.05.2026) ; Braun Binder Nadja/Obrecht Liliane, Transparenz über den staatlichen Einsatz algorithmischer Entscheidungssysteme, PJA 2024, p. 1069 ss, p. 1071 s. ; également : Kanton Appenzell Innerrhoden, Verzeichnis algorithmischer Systeme in der kantonalen Verwaltung Appenzell I.Rh., p. 1, disponible à l'adresse : https://publisher-ai.webcloud7.ch/themen/staat-und-recht/digitale-verwaltung/verzeichnis-algorithmischer-systeme (dernière consultation : 20.05.2026).

[30] Voir à cet égard : European Parliamentary Research Service, Scientific Foresight Unit (STOA), *op. cit.*, p. 1 ; Braun Binder Nadja/Obrecht Liliane, *ibid.*

Article 8 – Modalités de l'obligation des autorités de poursuite pénale et des tribunaux pénaux de tenir un registre

La disposition se fonde sur l'article 24 de la directive (UE) 2016/680, auquel les autorités de poursuite pénale sont soumises. Il en ressort que les tiers mandatés aussi doivent tenir un registre aux conditions de l'article 5 (al. 1). Par ailleurs, ce registre doit être mis à la disposition de l'autorité de protection des données qui le demande, par les autorités de poursuite pénale et les tribunaux pénaux comme par les tiers mandatés (al. 2).

Selon l'article 24 de la directive (UE) 2016/680, les registres se présentent sous une forme écrite, y compris la forme électronique. Il ressort de l'alinéa 2 que la forme du registre doit permettre aux autorités de poursuite pénale et les tribunaux pénaux de le mettre à la disposition de l'autorité de protection des données. Les critères du droit supérieur sont ainsi remplis sans que la manière de tenir le registre ne fasse l'objet d'une prescription expresse.

4.2.1 Droits de la personne concernée

Article 9 – Modalités de la communication des renseignements

Les modalités de la communication des renseignements sont réglées par voie d'ordonnance conformément à l'article 30, alinéa 2 LCPD. La disposition d'application de l'article 9 s'inspire de l'article 16 OPDo.

Alinéa 1

L'alinéa 1 porte sur les demandes de renseignement. La personne concernée doit en principe faire sa demande par écrit. Conformément aux travaux préparatoires au niveau fédéral, la forme écrite comprend toutes les formes qui permettent d'établir la preuve par le texte. On n'entend pas plus ici qu'à l'article 1 la forme écrite simple au sens des articles 13 à 15 CO[31]. Une demande électronique est possible.

Certaines personnes sont tenues d'effectuer leurs transactions avec les autorités par voie électronique en vertu de l'article 8 de la loi du 7 mars 2022 sur l'administration numérique (LAN)[32]. La disposition de la LAN prime alors et les demandes au sens de la LCPD ne peuvent émaner d'elles sous une autre forme. Les personnes morales doivent donc transmettre leur demande de renseignement par la voie électronique (art. 30 LCPD en relation avec l'art. 9 OCPD et l'art. 8 LAN).

Avec l'accord de l'autorité, la personne concernée peut formuler sa demande oralement.

Alinéa 2

L'alinéa 2 porte sur la communication des renseignements. L'autorité doit communiquer les renseignements à la personne concernée de manière compréhensible et, en principe, par écrit. Les exigences posées à l'écrit sont les mêmes que celles de l'alinéa 1. L'autorité peut donc fournir les renseignements par la voie électronique (voir le commentaire ci-dessus). Selon l'article 30, alinéa 1, lettre *a* LCPD, l'autorité envoie à la personne concernée les données personnelles traitées « en tant que telles ». Il en ressort que les renseignements ne se rapportent pas aux documents mais aux données personnelles[33]. Cela signifie que l'autorité peut par exemple envoyer des renseignements écrits réunis dans un tableau ou dans une liste[34].

[31] Voir à cet égard : rapport explicatif de l'ordonnance fédérale sur la protection des données, p. 40.
[32] RSB 109.1.
[33] Voir Gramigna Ralph in : Blechta, Gabor P. / Vasella David (édit.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, Bâle : Helbing Lichtenhahn Verlag, art. 25, n. 20 LPD et renvoi aux débats du Parlement fédéral.
[34] Stengel Cornelia/Stäuble Luca in : Bieri Adrian/Powell Julian (édit.), DSG Kommentar, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zurich, 2023, art. 25, n. 15 LPD (droit d'accès).

S'il s'agit d'images ou d'enregistrements audio, l'autorité pourra les envoyer à la personne concernée dans leur forme originale (lit. *a*). La transmission orale des informations, par exemple par téléphone, est également prévue, pour autant que la personne concernée y ait consenti (lit. *b*). Les deux parties peuvent aussi s'entendre en vue d'une consultation sur place des données (lit. *c*). L'autorité peut produire des copies au lieu d'originaux, en particulier si les informations doivent être anonymisées.

Alinéa 3

Conformément à l'alinéa 3, l'autorité prend des mesures adéquates pour identifier la personne qui a déposé la demande. Ce point revêt une importance particulière lorsque les demandes se font de vive voix ou par voie électronique. Pour savoir quand des mesures s'imposent et lesquelles, il convient de se fonder sur les circonstances du cas d'espèce. La personne concernée est tenue de coopérer. La règle veut qu'elle présente à l'autorité un document d'identification officiel ou une copie de celui-ci. Lorsqu'il s'agit d'une petite collectivité, il peut suffire que la personne soit personnellement connue de l'autorité du traitement ; aucune mesure supplémentaire n'est alors requise.

Tout envoi numérique est soumis aux règles de l'article 9 OAN.

Article 10 – Délais en matière de renseignement

La teneur de l'article 10 reprend les règles fixées à l'article 18 OPDo.

Selon l'alinéa 1, l'autorité a 30 jours pour fournir les renseignements ou, sinon, pour rendre une décision fondée restreignant le droit d'accès.

L'alinéa 2 relativise ce délai. Si l'autorité ne peut pas donner les renseignements dans les 30 jours, elle en informe la personne concernée en lui indiquant le délai dans lequel ils lui seront fournis.

Article 11 – Droit de blocage de la communication à des personnes privées

Le contenu de la disposition est substantiellement le même que celui de l'article 1 actuellement en vigueur. Si la demande est admise, les tiers voient tout accès aux données personnelles bloqué.

Une décision attaquable est rendue pour ordonner ou refuser le blocage (voir l'art. 54 LCPD).

Alinéa 1

À l'instar de la demande de renseignements (art. 9, al. 1), la demande de blocage doit être déposée par écrit par la personne concernée. Les exigences relatives à la forme écrite sont précisées plus haut, au commentaire de l'article 9, alinéa 1. Pour les personnes tenues d'effectuer leurs échanges par voie électronique avec les autorités en vertu de l'article 8 LAN, la demande de blocage au sens de la LCPD ne peut pas être envoyée autrement que par voie électronique (voir le commentaire de l'art. 9, al. 3).

Avec l'accord de l'autorité, la personne concernée peut formuler sa demande oralement.

Alinéa 2

Le but de la disposition est de garantir que la personne concernée obtienne une réponse à sa demande. L'autorité doit communiquer avec elle de manière compréhensible et, en principe, par écrit. Pour la forme écrite, il convient de se référer aux conditions de l'alinéa 1. C'est à ce titre que l'autorité peut répondre à la personne concernée par voie électronique (voir le commentaire de l'al. 1).

Alinéa 3

Conformément à l'alinéa 3, l'autorité prend des mesures adéquates pour identifier la personne concernée. Cette dernière est tenue de coopérer (voir à propos des mesures adéquates le commentaire de l'art. 9, al. 3).

4.3 Autorité de protection des données, conseillère ou conseiller à la protection des données

Avec l'entrée en vigueur de la LCPD, l'autorité de surveillance de la protection des données devient l'autorité de protection des données.

En outre, la notion d'organe de contact pour la protection des données est remplacée au profit de la terminologie retenue dans le droit fédéral (conseillère ou conseiller à la protection des données).

Voilà pourquoi le chapitre « Autorité de surveillance de la protection des données, organes de contact pour la protection des données » actuellement en vigueur doit être modifié en « Autorité de protection des données, conseillère ou conseiller à la protection des données ».

Article 12 – Documentation

L'article 12 reprend les dispositions de l'article 13 en vigueur.

Alinéa 1

L'alinéa 1 précise que les autorités communiquent les projets d'acte législatif et les mesures prévues à l'autorité cantonale de protection des données, qui prend position à leur sujet conformément à l'article 43, alinéa 1, lettre *f* et alinéa 3 LCPD.

Il est rédigé dans le «seul» but de souligner que l'autorité de protection des données n'a pas à s'enquérir des projets auprès des autorités, mais que ces dernières doivent d'elles-mêmes lui remettre les documents selon l'article 43, alinéa 1, lettre *f* et alinéa 3 LCPD. Il appartient ensuite à l'autorité de protection des données d'examiner le dossier et de retenir les parties sur lesquelles elle souhaite prendre position.

La disposition n'a aucune répercussion matérielle sur l'obligation de documenter. Ainsi, l'autorité cantonale de protection des données s'exprime sur les projets d'acte législatif et les mesures des communes et collectivités de droit communal ne disposant pas de leur propre autorité de protection des données seulement s'ils touchent *de manière importante* à la protection des données (art. 43, al. 3 LCPD). S'agissant des autorités cantonales, leur obligation selon l'article 43, alinéa 1, lettre *f* LCPD concerne les projets d'acte législatif et les mesures qui sont liés à la protection des données. Il faut que ce lien soit d'une certaine importance, comme l'entend déjà la réglementation actuelle.

La définition de ce qu'est un projet d'acte législatif a déjà été fournie dans le rapport accompagnant la LCPD. Ce sont tant les projets de loi ou d'ordonnance que les projets de modification législative. Quant aux mesures en font principalement partie les instructions d'exécution, les dispositions prises pour garantir la sécurité informatique, les enquêtes, la création de processus et leur réagencement comme, par exemple, l'émission de certificats électroniques.

Alinéa 2

En vertu de l'alinéa 2, les décisions sur recours concernant la protection des données sont anonymisées par les Directions et la Chancellerie d'État avant d'être envoyées à l'autorité cantonale de protection des données.

L'alinéa se rapporte aux décisions sur recours qui concernent directement la protection des données, c'est-à-dire, par exemple, celles rendues à propos de la consultation ou de la communication de données personnelles. L'article 4 LCPD exige une base légale pour chaque traitement, ce qui comprend la communication de données personnelles. De telles bases légales peuvent être trouvées dans les lois spéciales, comme la LIAM ou la loi du 10 février 2019 sur la police (LPol)[35]. Ainsi, des demandes d'accès fondées sur la LIAM concernent directement la protection des données ; l'autorité cantonale de protection des données doit donc en avoir connaissance. Par contre, des décisions sur recours qui peuvent avoir des effets en termes de protection des données mais qui se rapportent aux bases de la législation spéciale n'ont pas besoin d'être envoyées. C'est le cas notamment des décisions de la Direction de la santé, des affaires sociales et de l'intégration en matière de devoir de discrétion du corps médical conformément à la loi du 2 décembre 1984 sur la santé publique (LSP)[36].

Article 13 – Participation des communes aux frais de l'autorité cantonale de protection des données

La disposition découle de l'article 44, alinéas 3 et 4 LCPD et concrétise le montant de la participation aux frais de l'autorité cantonale de protection des données dont les communes soumises à la surveillance de cette dernière doivent s'acquitter.

Il faut partir du principe qu'à moyen terme le financement par capitation ne devrait pas changer. Une réaction rapide doit rester possible en cas de remaniement inattendu ou de modification à long terme du budget de l'autorité de protection des données, c'est pourquoi le montant de la participation par personne est fixé par voie d'ordonnance.

Le nombre des habitantes et des habitants est calculé sur la base de la population résidante moyenne déterminée en vertu du principe du domicile civil conformément au registre des habitantes et des habitants des communes (voir l'art. 7 de la loi du 27 novembre 2000 sur la péréquation financière et la compensation des charges [LPFC])[37]. Fera foi pour la première fois le nombre de personnes figurant au dernier relevé à la date d'entrée en vigueur de la présente ordonnance. Le décompte pour les périodes suivantes sera actualisé au moment de la facturation. La FIN publie en août environ les chiffres concernant la population au 31 décembre de l'année écoulée sur son site Internet[38]. À titre d'exemple, la facturation 2025 se fonde sur les données au 31 décembre 2024, qui ont été rendues disponibles en septembre 2025.

Le calcul qui a abouti au montant par habitante et habitant retenu dans l'ordonnance repose sur les chiffres de la population résidante du canton de Berne au 31 décembre 2023 :

Population résidante du canton de Berne au 31 décembre 2023	1 063 533
Population résidante de Berne, Bienne, Köniz, Thoune	279 783
Population résidante sans Berne, Bienne, Köniz, Thoune	783 750

Les coûts supplémentaires induits par la centralisation des tâches au sein de l'autorité cantonale de protection des données sont évalués à un montant annuel de 720 000 francs dans le budget et le plan intégré mission-financement publiés. À plus vaste échéance, le montant hypothétique s'établit à environ 800 000 francs, soit à une participation de chaque commune à hauteur d'un franc par habitante et habitant (CHF 800 000 ÷ 783 750 = CHF 1,020 ≈ CHF 1,00).

Article 14 – Rapport

L'article 14 est une disposition nouvelle et règle, en application de l'article 51 LCPD, le contenu obligatoire du rapport de l'autorité cantonale de protection des données. Cette dernière doit

[35] RSB 551.1.
[36] RSB 811.01.
[37] RSB 631.1.
[38] Voir : https://www.fin.be.ch/fr/start/themen/OeffentlicheStatistik/bevoelkerungsstatistik/publikationen.html (dernière consultation : 21.05.2026).

rendre compte en particulier des lacunes constatées et des améliorations souhaitables dans la mesure où cela ne porte atteinte à aucun intérêt public au sens de la législation sur la sécurité de l'information et la cybersécurité, et plus précisément de l'article 1, alinéa 2 LSIC. Ainsi, le signalement d'une lacune ne doit pas être rapporté lorsqu'il rendrait public des brèches du dispositif TIC et, donc, des vulnérabilités de l'administration publique. La diffusion de l'information présenterait une menace pour la sécurité publique.

L'autorité de protection des données peut consulter les Directions ou la Chancellerie d'État avant la publication du rapport.

Article 15 – Conseillère ou conseiller à la protection des données

La disposition est reprise de la législation en vigueur, mais connaît quelques adaptations.

L'alinéa 1 étend l'obligation de désigner une conseillère ou un conseiller à la protection des données à la Direction administrative de la magistrature.

Pour le reste, l'alinéa 1 reprend la liste existante des tâches, à l'exception de la mention du soutien aux organes responsables ainsi qu'aux utilisatrices et aux utilisateurs. Cette obligation ne disparaît pas réellement, mais découle déjà logiquement des lettres *a*, *c* et *d*, qui prévoient des activités de conseil, la promotion de l'information et de la formation du personnel ainsi que le concours à l'application des prescriptions relatives à la protection des données. Conformément à la législation fédérale et à l'article 34, lettre *e* de la directive (UE) 2016/680, les conseillères et les conseillers à la protection des données sont en outre l'organe de contact pour l'autorité cantonale de protection des données (lit. *e*).

Alinéa 2

Les Directions, la Chancellerie d'État et la Direction administrative de la magistrature ont le choix entre le fait de désigner une personne concrète ou de se contenter de déléguer les tâches à un organe de leur unité administrative. Elles disposent donc d'une grande liberté dans la manière dont elles entendent s'organiser en termes de structure et de personnel pour garantir la protection des données au sein de leur champ d'activité. Sur le fond, il serait tout à fait judicieux qu'une personne soit désignée conseillère ou conseiller à la protection des données. Celle-ci posséderait de surcroît déjà des connaissances adéquates en la matière et les approfondirait en les mettant en pratique conformément à l'alinéa 1.

L'alinéa 2 fixe un régime supplétif de compétence pour les cas où les Directions, la Chancellerie d'État ou la Direction administrative de la magistrature ne désigneraient pas de conseillère ou de conseiller à la protection de données et se trouveraient en porte-à-faux avec l'article 32 de la directive (UE) 2016/680.

Dans les Directions et à la Chancellerie d'État, ce sont les juristes des offices qui interviennent dans leur domaine dans la mesure où personne n'a concrètement été retenu pour ce faire. À défaut, le service juridique règle en interne qui assume la charge.

S'agissant de la Direction administrative de la magistrature, la responsabilité revient subsidiairement à l'État major des ressources selon l'article 19 de la loi du 11 juin 2009 sur l'organisation des autorités judiciaires et du Ministère public (LOJM)[39].

Alinéa 3

L'alinéa 3 établit que les questions spécifiques des communes et des autres collectivités de droit communal en matière de protection des données peuvent être adressées à la conseillère compétente ou au conseiller compétent et, s'il n'y en a pas, au service juridique compétent de la Direction ou de la Chancellerie d'État ou, le cas échéant, aux juristes des offices. L'Office des

[39] RSB 161.1.

affaires communales et de l'organisation du territoire (OACOT) pourra aussi notamment être amené à répondre aux demandes en lien avec le droit communal.

4.4 Dispositions transitoires

Article 16 – Contrats en cours avec des tiers mandatés

L'adaptation en fonction de l'article 1 n'a pas besoin d'avoir lieu immédiatement après l'entrée en vigueur de l'ordonnance pour les contrats en cours conclus avec des tiers mandatés. Elle peut attendre la prochaine acquisition ou modification, mais doit intervenir au plus tard le 1er octobre 2030.

Article 17 – Enquêtes pendantes devant l'autorité de protection des données

La LCPD ne s'applique pas aux enquêtes des autorités de protection des données qui sont pendantes au moment de son entrée en vigueur (art. 59 LCPD). L'article 17 est rédigé dans l'intention d'établir clairement ce que recoupe la notion d'enquête pendante, à savoir les affaires en cours en matière de protection des données, notamment des procédures de contrôle préalable, des dénonciations relevant du droit de la surveillance ainsi que des prises de position sur les projets d'acte législatif et les mesures. Les enquêtes pendantes devant l'autorité de surveillance communale au moment de l'entrée en vigueur de l'ordonnance sont poursuivies par celle-ci jusqu'à leur clôture. Un délai transitoire s'applique également aux contrôles préalables.

Ce qui relève du conseil informel n'est pas visé par la disposition.

Article 18 – Sécurité des données et contrôle préalable

Jusqu'à présent, les aspects de la sécurité des données et des contrôles préalables étaient réglés aux articles 4 à 6, respectivement 7 à 9 OPD. Ils seront repris dans la législation sur la sécurité de l'information et la cybersécurité (voir le commentaire des points 2.1 et 3.2.1). Comme la LSIC et l'OSID entreront en vigueur après la LCPD et l'OCPD, les articles 4 à 9 OPD continueront de s'appliquer jusqu'à ce moment.

4.5 Dispositions finales

La présente révision totale entraîne indirectement la modification de différentes autres ordonnances (art. 19 ; voir ci-dessous). Par ailleurs, deux ordonnances doivent être abrogées : l'actuelle OPD et l'ordonnance du 4 juillet 2018 portant introduction de la directive (UE) 2016/680 relative à la protection des données à caractère personnel (OiDPD)[40] (art. 20).

4.6 Modifications indirectes

Les dispositions qui suivent doivent faire l'objet d'une modification indirecte en raison de la révision de la législation sur la protection des données.

[40] RSB 152.043.

4.6.1 Ordonnance du 22 février 1995 fixant les émoluments de l'administration cantonale (ordonnance sur les émoluments ; OEmo)[41]

Les renvois figurant dans les articles 31 à 33 OEmo sont adaptés à la nouvelle législation sur la protection des données.

De surcroît, l'article 31, alinéa 2 conformément à l'article 56, alinéa 2 LCPD prévoit un nouvel émolument : l'autorité peut le percevoir lorsque la personne exerce ses droits en faisant preuve de mauvaise foi ou en agissant à la légère. La disposition vise avant tout les requêtes procédurières.

4.6.2 Ordonnance du 21 décembre 2022 sur les procédures de consultation et de corapport (OPC)[42]

Le Bureau pour la surveillance de la protection des données change de nom et devient le Bureau pour la protection des données. Ce terme doit être repris aux articles 4, alinéa 2, lettre *r*, et 18 OPC. Il est précisé que les projets d'acte législatif et les mesures ne doivent être soumis à l'autorité de protection des données que lorsqu'ils touchent la protection des données de manière importante.

4.6.3 Ordonnance cantonale du 11 novembre 2015 sur la géoinformation (OCGéo)[43]

En premier lieu, le renvoi figurant à l'article 15, alinéa 2 OCGéo est adapté à la nouvelle législation sur la protection des données. En deuxième lieu, l'expression « sont en cause » est remplacée par « s'y opposent », qui est le verbe utilisé à la fois dans la LCPD (art. 14, al. 3) et dans la LIAM (art. 27, al. 1)[44]. En dernier lieu, le renvoi à la LIAM est modifié afin qu'il corresponde à la nouvelle législation.

4.6.4 Ordonnance du 30 juin 2021 sur l'organisation et les tâches de la Direction de la santé, des affaires sociales et de l'intégration (ordonnance d'organisation DSSI, OO DSSI)[45] et ordonnance du 18 octobre 1995 sur l'organisation et les tâches de la Direction des travaux publics et des transports (ordonnance d'organisation DTT, OO DTT)[46]

Vu la teneur de l'article 15 OCPD, il convient d'adapter l'article 8, alinéa 2, lettre *a* OO DSSI et l'article 7, alinéa 1, lettre *e* OO DTT. Les termes à retenir sont ceux de conseillère ou conseiller à la protection des données.

4.6.5 Ordonnance du 5 décembre 2012 sur l'exercice de la prostitution (OEP)[47]

Selon l'article 9, alinéa 2 OEP, l'Office des services et des ressources de la Direction de l'intérieur et de la justice (DIJ) est responsable de la protection des données. Par arrêté du 24 novembre 2021, le Conseil-exécutif a modifié l'ordonnance sur l'organisation et les tâches de la

[41] RSB 154.21.
[42] RSB 152.025.
[43] RSB 215.341.2.
[44] RSB 107.1.
[45] RSB 152.221.121.
[46] RSB 152.221.191.
[47] RSB 935.901.

Direction de l'intérieur et de la justice (ordonnance d'organisation DIJ, OO DIJ)[48], marquant la dissolution de l'Office des services et des ressources et la réorganisation des domaines d'activité[49]. L'article mentionné doit donc être modifié : l'Office juridique de la DIJ assume la responsabilité de la protection des données dans le cadre de l'ordonnance.

4.6.6 Adaptations liées au nouveau titre de l'acte

Les ordonnances citées ci-après mentionnent soit la LCPD ou l'OPD de manière générale, soit des dispositions précises de ces actes législatifs. Dans la mesure du possible, il convient de renvoyer au texte et de manière dynamique, sans référence à des articles concrets. Des modifications ultérieures de la législation s'en trouvent ainsi simplifiées. La modification du titre de l'acte législatif entraîne celle des renvois ; ainsi, les modifications indirectes suivantes sont nécessaires :

- Article 18 OPC
- Articles 31 à 33 OEmo
- Article 6 de l'ordonnance du 18 mai 2005 sur le personnel (OPers)[50]
- Articles 4 et 9 de l'ordonnance du 20 mai 2020 sur le traitement des données dans le domaine de l'asile, des réfugiés et des étrangers (ODARE)[51]
- Articles 2, 7, 9, 12, 13, 15 et 32 de l'ordonnance du 20 janvier 2021 sur la plate-forme des systèmes des registres communaux (O GERES)[52]
- Article 28 de l'ordonnance cantonale du 3 novembre 2021 sur l'état civil (OCEC)[53]
- Articles 2, 4, 13 et 19 de l'ordonnance du 20 janvier 2021 sur le système de gestion centrale des personnes (O GCP)[54]
- Préambule de l'OCDP
- Article 14 de l'ordonnance du 27 octobre 2010 sur l'assurance immobilière (OAIm)[55]
- Article 9 OEP
- Article 11b de l'ordonnance du 18 décembre 2002 concernant le système d'information sur les données relatives aux immeubles (ordonnance GRUDIS)[56]
- Article 15 OCGéo
- Article 86 de l'ordonnance du 7 novembre 2007 sur les écoles moyennes (OEM)[57]
- Article 3 de l'ordonnance du 14 novembre 2018 sur les expulsions (Oex)[58]
- Article 27a de l'ordonnance du 20 septembre 2017 sur le droit de cité cantonal et le droit de cité communal (ordonnance sur le droit de cité, ODC)[59]

4.6.7 Adaptation du nom de l'autorité de protection des données

La notion de « surveillance de la protection des données » est présente dans un certain nombre d'ordonnances et doit être abandonnée au profit de la nouvelle désignation. À teneur de la LCPD, il s'agit désormais d'autorités de protection des données. Le changement d'appellation

[48] RSB 152.221.131.
[49] Voir : rapport de la modification (disponible en allemand : Vortrag zur Änderung der Verordnung über die Organisation und die Aufgaben der Direktion für Inneres und Justiz [Organisationsverordnung DIJ, OrV DIJ], p. 1).
[50] RSB 153.011.1.
[51] RSB 861.112.
[52] RSB 152.051.
[53] RSB 212.121.
[54] RSB 152.052.
[55] RSB 873.111.
[56] RSB 215.321.5.
[57] RSB 433.121.
[58] RSB 222.100.
[59] RSB 121.111.

reflète clairement le fait que ces autorités sont avant tout là pour conseiller, guider et former, plutôt que pour contrôler et sanctionner ; il appelle la modification des dispositions suivantes :

- Articles 13 et 19b OAN
- Articles 4 et 18 OPC
- Article 11 OPers
- Article 9 ODARE
- Article 20 O GERES
- Article 11 O GCP
- Article 11 de l'ordonnance du 20 novembre 2019 sur les données secondaires de communication (ODSC)[60]

4.6.8 Adaptation de la terminologie française concernant les données sensibles

Comme dans le cas des lois, les « données particulièrement dignes de protection » connaissent une adaptation d'ordre terminologique. Il convient de reprendre le terme de données sensibles. Cette adaptation est à l'origine de plusieurs modifications indirectes :

- Articles 15, 20 et 21 de l'ordonnance du 15 novembre 2023 sur l'information et l'aide aux médias (OIAM)[61]
- Article 9 OAN
- Articles 9 à 13 O GERES
- Articles 9 et 13 à 15 O GCP
- Articles 6, 6a et 203 OPers
- Articles 3 et 10 de l'ordonnance du 15 septembre 2021 sur l'exécution de la surveillance électronique (OESurvE)[62]
- Article 85 de l'ordonnance du 28 mars 2007 sur le statut du corps enseignant (OSE)[63]
- Article 12b de l'ordonnance du 28 octobre 1998 sur l'imposition des véhicules routiers et la facturation par l'office compétent (ordonnance sur l'imposition des véhicules routiers, OIV)[64]
- Article 8 ODARE

4.6.9 Ordonnance du 20 janvier 2021 sur la plate-forme des systèmes des registres communaux (art. 8, al. 2 et annexe 2, ch. 2 O GERES)[65]

Contexte

Certaines autorités déterminées ont besoin de pouvoir suivre l'historique des changements d'état civil ou d'autres événements annoncés (p. ex. mariage ou déménagement) depuis 2010, soit l'année de mise en service de la plate-forme GERES, afin de garantir l'exactitude des données personnelles. Une révision de l'O GERES s'impose donc à ce titre.

La loi du 10 mars 2020 sur les fichiers centralisés de données personnelles (LFDP)[66] régit les principes du traitement des données de personnes physiques ou morales contenues dans des fichiers centralisés de données personnelles ainsi que la mise en œuvre de la loi fédérale du

[60] RSB 153.011.5.
[61] RSB 107.111.
[62] RSB 341.12.
[63] RSB 430.251.0.
[64] RSB 761.611.1.
[65] RSB 152.051.
[66] RSB 152.05.

23 juin 2006 sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes (loi sur l'harmonisation de registres, LHR)[67]. Selon l'article 18, le canton exploite un fichier centralisé de données personnelles pour accomplir les tâches prévues par la LHR.

Dans l'O GERES, le Conseil-exécutif a édicté les règles concernant la plate-forme des systèmes des registres communaux, qui est un fichier centralisé de données personnelles, en application de l'article 7, alinéa 1 LFDP. L'étendue des données de la plate-forme GERES est déterminée par des limites territoriales et temporelles :

> *1 La plate-forme GERES permet d'interroger ou d'annoncer des données relatives à des personnes d'une commune municipale ou d'une paroisse, d'un ensemble de communes municipales ou de paroisses ou de tout le territoire cantonal.*
>
> *2 Grâce à l'historisation, la plate-forme GERES permet d'afficher les annonces d'événements antérieurs, dans la limite de celles des cinq années précédant la plus récente.*

Les fonctionnalités les plus importantes permettant un profilage ou l'édition de données sensibles sous une autre forme sont indiquées dans l'article 10, alinéa 1 O GERES. L'annexe 2 fournit la liste des fonctionnalités restantes de la plate-forme GERES accompagnées de leur description, en donnant également des détails sur l'historisation (ch. 2 de l'annexe 2) :

N°	Fonctionnalité	Descriptif	Etendue
1.	Droit de modification	Saisir et modifier des données dans GERES	Toutes
2.	Historisation	Afficher les événements et leur modification par personne	Par année, 5 dernières années au plus

Les droits d'accès à la plate-forme sont réglés par les Directions et la Chancellerie d'État ainsi que par la Direction administrative de la magistrature. Chacune d'entre elles édicte une ordonnance ou un règlement à cet effet (art. 18 ss O GERES).

Modification (art. 8, al. 2 et annexe 2, ch. 2 O GERES)

L'autorité peut traiter des données personnelles lorsqu'une base légale suffisante l'autorise expressément, que le but du traitement est défini et que le traitement est approprié et nécessaire à l'accomplissement de sa tâche (art. 4, 6 et 7 LCPD). Selon l'article 8 LCPD, les données personnelles traitées doivent en outre être exactes et complètes. L'historisation des données est limitée aux cinq années précédant l'événement le plus récent (art. 8, al. 2 O GERES).

À l'occasion de la récente révision de l'ordonnance de Direction du 13 août 2021 sur les droits d'accès aux fichiers centralisés de données personnelles délivrés par la Direction des finances (FDP OD FIN)[68], entrée en vigueur au 1er octobre 2025, il est apparu que GERES permettait dans certains cas de consulter l'historique des événements (p. ex. mariage ou déménagement) sur une période plus longue que les cinq ans prévus. En effet, il est possible de remonter jusqu'en 2010 si la personne était déjà née à cette époque et si la commune à laquelle avaient été annoncés les événements a transféré son registre sur la plate-forme GERES.

Or, les exemples ci-dessous montrent que les autorités chargées d'assurer l'exactitude des données GERES ont besoin de consulter l'historique jusqu'en 2010, ce qui légitimise le but, l'adéquation et la nécessité d'une historisation des données jusqu'en 2010.

a) Gestionnaire de services GERES de l'Office d'information et d'organisation (OIO) et sa suppléance : actuellement, l'accès aux données est limité aux cinq dernières années. Dorénavant, il devra être possible de remonter jusqu'en 2010, car les communes en ont besoin pour analyser les erreurs et les corriger. L'OIO ne corrige pas lui-même les données, mais c'est lui qui détecte les erreurs et les signale aux communes pour qu'elles les rectifient.

[67] RS 431.02.
[68] RSB 152.053.1.

b) Support aux communes, GERES-clearing : tout comme les gestionnaires de services, le contrôle de GERES incombant au service de support aux communes de l'Intendance des impôts (ICI) ne peut pour le moment porter que sur les cinq dernières années. Là aussi, la durée doit être étendue jusqu'en 2010, car l'examen de la qualité des données repose essentiellement sur une vérification exhaustive et traçable des changements d'état civil et des autres événements.

   Le service de support aux communes ne peut évidemment pas demander aux communes de corriger des données qu'il ne peut pas repérer du fait que la règlementation actuelle limite ses droits d'accès aux périodes dont la fin remonte à moins de cinq ans. Sans un historique exhaustif et traçable des données, certains problèmes de qualité ne seront jamais détectés.

c) Secteurs Impôts périodiques et Impôts spéciaux et services de l'ICI : le secteur Impôts périodiques procède notamment à la taxation du revenu et de la fortune ainsi qu'à la perception des montants dus à ce titre par l'ensemble des personnes du canton. Il mène les procédures jusque devant la Commission des recours en matière fiscale. Ces procédures durent parfois beaucoup plus de cinq ans, notamment si des voies de droit sont saisies. Il faut par conséquent que les données et modifications remontant à plus de cinq ans dans GERES puissent être consultées.

   Le secteur Impôts spéciaux et services procède notamment à la taxation des gains immobiliers, des successions et des donations ainsi qu'à la perception des montants dus à ces titres par l'ensemble des personnes concernées dans le canton. Il mène aussi les procédures de rappel d'impôt. Ces dernières aussi se prolongent parfois largement au-delà du délai de cinq ans, de sorte que l'accès aux données ne doit pas être limité à cette période.

d) Adaptateur GERES-NESKO : la limite de cinq ans s'applique actuellement aussi à l'adaptateur GERES-NESKO, qui est un système de l'ICI. Or cette limite empêche de transmettre via sedex (routage) des corrections d'événement remontant à plus de cinq ans. Ainsi, il n'est actuellement pas possible de corriger des événements plus anciens au moyen du routage.

   Le traitement des annonces de GERES exige toujours une lecture de l'ensemble de la « Basedelivery », autrement dit du premier jeu de données de la personne dans GERES à la date de l'événement. Or celle-ci peut être antérieure à la période de cinq ans prévue. L'accès doit donc être rendu possible jusqu'en 2010 pour garantir la régularité du flux de données.

e) Bedag Informatique SA : l'entreprise est chargée du développement, de la maintenance, de l'exploitation et du support de l'adaptateur GERES-NESKO. À cette fin, elle a elle aussi besoin d'un accès illimité à l'historique des données pour programmer l'adaptateur. Elle n'a toutefois accès qu'aux données des domaines développement, analyse d'affaires et centre de calcul, et ne dispose pas des droits de modification des données GERES.

Vu ce qui précède, la consultation des changements d'état civil et des autres événements enregistrés sur la plateforme GERES depuis 2010 peut, selon la tâche de l'autorité requérante, respecter les principes de la proportionnalité et de la finalité au sens des articles 6 et 7 LCPD. Pour que cet accès soit licite, l'O GERES doit être adaptée. Il appartient aux Directions, à la Chancellerie d'État et à la Direction administrative de la magistrature, ou aux communes municipales et aux communes bourgeoises ainsi qu'aux paroisses de désigner dans une règlementation ad hoc les autorités qui peuvent effectivement faire usage de cette historisation. Elles doivent ensuite soumettre leur proposition à l'autorité de protection des données pour confirmation.

4.7 Abrogation d'actes législatifs

L'OCPD étant le fruit d'une révision totale, il convient d'abroger l'OPD en sa forme actuelle.

Par la révision totale de sa législation sur la protection des données, le canton de Berne met définitivement en œuvre les exigences de la directive (UE) 2016/680. L'OiDPD, limitée de toute manière au 31 août 2026, peut donc être abrogée au 1er septembre 2026.

5. Place du projet dans le programme gouvernemental de législature (programme législatif) et dans d'autres planifications importantes

La révision correspond à l'objectif stratégique n° 2 du programme gouvernemental de législature, selon lequel « *le canton de Berne* […] *exploite les opportunités de la transition numérique et fournit* […] *des services efficaces, de haute qualité et efficients.* » Le projet législatif contribue à cet objectif par le transfert à l'autorité cantonale de protection des données des tâches qui incombaient aux autorités communales compétentes dans le domaine (et qui incomberont encore aux quatre communes les plus peuplées). Les communes se trouveront déchargées des défis actuels et prochains que présente le monde numérique, et la surveillance sera professionnalisée. Le savoir-faire ainsi concentré garantira non seulement une meilleure efficience, mais donnera aussi accès à un service professionnel tant aux autorités communales qu'à la population.

6. Répercussions financières

Les adaptations obligatoires au droit supérieur des dispositions de la législation cantonale sur la protection des données ont des répercussions financières. Toutefois, c'est la révision totale de la loi qui en est à l'origine. En principe, la révision totale de l'ordonnance ne devrait pas grever les finances au-delà de ce qui découlerait éventuellement de l'exécution des dispositions de la loi. Les explications qui suivent se rapportent donc essentiellement à la révision totale de la loi.

Des moyens supplémentaires devront être mis en œuvre, en particulier parce que l'autorité de protection des données aura la possibilité de rendre des décisions et que la surveillance relevant du droit communal sera pour la plus grande partie centralisée et assumée par le canton. Les charges supplémentaires du canton sont toutefois remboursées par une participation des communes aux coûts (voir l'art. 44, al. 3 et 4 LCPD).

L'analyse d'impact relative à la protection des données personnelles, nouvelle, correspond pour l'essentiel aux instruments actuels, c'est-à-dire l'analyse SIPD et le concept SIPD, de sorte qu'elle n'engendre en principe aucune augmentation significative des frais. Certes, les autorités, qui n'étaient jusque-là soumises à aucune obligation en la matière, devront aussi procéder à cette analyse, mais, en fin de compte, leur charge de travail ne s'en trouvera pas accrue. Elles doivent en effet déjà se soumettre à un contrôle préalable et évaluer les risques d'un traitement des données. Le fait de formaliser l'analyse des risques et l'analyse d'impact relative à la protection des données personnelles n'a que pour conséquence de standardiser la procédure et de l'ancrer dans la loi.

Les nouvelles obligations en matière d'information et d'annonce peuvent alourdir les charges des autorités, mais les coûts ne devraient pas excéder les moyens disponibles. Par ailleurs, il appartient aux autorités d'empêcher tout incident en prenant les mesures techniques et organisationnelles appropriées.

7. Répercussions sur le personnel et l'organisation

En raison de la centralisation de la surveillance relevant du droit communal, l'autorité cantonale de protection des données a besoin d'environ 400 % de poste supplémentaires. Le surcoût est compensé par un système de participation (art. 44, al. 3 et 4 LCPD, art. 13 OCPD).

Les Directions et la Chancellerie d'État disposent déjà d'un organe de contact pour la protection des données. L'obligation est maintenue, tout comme l'essentiel du cahier des charges. Le changement notable est d'ordre terminologique : au lieu d'organe de contact, on parlera de conseillères et de conseillers à la protection des données. Rien n'indique donc que le projet engendrera des mesures en matière de personnel et d'organisation.

8. Répercussions sur les communes

La révision implique une diminution de charge pour les communes – sauf pour les quatre communes les plus peuplées – en raison de la centralisation des tâches relevant de la protection des données au sein de l'autorité cantonale. Les communes dont les tâches sont centralisées contribuent financièrement aux frais supportés par l'autorité cantonale de protection des données. La participation, fixée à l'article 13 OCPD, est d'un franc par habitante et habitant. Le montant peut donc dépasser celui que les communes allouaient jusqu'à présent à la surveillance de la protection des données.

9. Répercussions sur l'économie

La législation sur la protection des données ne s'adresse directement qu'aux autorités du canton de Berne. Les tiers sont seulement indirectement concernés, en particulier les entreprises, lorsqu'ils agissent sur mandat du canton. Dans un tel cas, les tiers mandatés ne peuvent traiter des données personnelles autrement que dans la mesure où le ferait l'autorité. Ils doivent ainsi également se conformer aux dispositions relatives à la protection des données.

10. Résultat de la consultation

L'OCPD a fait l'objet d'une procédure de corapport et d'une consultation du 8 décembre 2025 au 31 janvier 2026. Les personnes qui ont pris part à la consultation ont souscrit dans une large mesure au projet. Quelques propositions matérielles ont été formulées.

10.1 Transposition des dispositions sur la sécurité des données dans l'OSID

À l'occasion de la consultation, il a plusieurs fois été reproché que le projet d'ordonnance ne reprendrait pas les dispositions de l'OPD en matière de sécurité des données et qu'elles seraient transposées dans l'OSID.

Une coordination des dispositions d'exécution de la LSIC et de la LCPD relevant de la sécurité des données est logique pour plusieurs raisons. Ces deux lois sont étroitement liées l'une à l'autre. Ainsi, l'article 10 LCPD en tant que tel ne règle pas la sécurité des données, mais renvoie aux principes de la législation sur la sécurité de l'information et la cybersécurité applicables par analogie. La sécurité des données est à la jonction des législations sur la protection des données et sur l'information. Les mesures de sécurité de l'information et des données étant les

mêmes, il est pertinent de les régler dans une seule ordonnance d'exécution. Si la LCPD et l'OCPD prévoyaient des règles en matière de sécurité des données, on courrait le risque de voir certaines mesures abordées deux fois ou de laisser certains points en suspens. Une couverture complète du domaine de la sécurité des données et de l'information est possible dès lors que la LCPD et l'OCPD renvoient à la législation sur l'information tant en matière de sécurité des données qu'au sujet des obligations avant la mise en service.

10.2 Ampleur du contrat avec des tiers mandatés

Quelques participantes et participants à la consultation déploraient la densité du contenu minimal du contrat à passer avec les tiers mandatés selon l'article 1 OCPD, en particulier pour le traitement de données personnelles « courantes ». À leur sens, l'étendue du contrat ne se justifierait pas.

Avant la conclusion d'un contrat, la première étape consiste toujours à vérifier si l'autre partie se voyant confier des tâches de droit public est considérée comme une autorité au sens de l'article 2, alinéa 1, lettre *i* LCPD. En pareil cas, elle doit se charger de manière indépendante de la protection des données. L'article 1 OCPD n'est alors pas applicable.

Là où l'autorité fait appel à des tiers pour le traitement des données (tiers mandatés), ces derniers doivent remplir les conditions de l'article 12 LCPD et les données doivent être traitées de la même manière que l'autorité est habilitée à le faire. L'autorité conserve toutefois la responsabilité sur le traitement, raison pour laquelle il est important qu'un contrat fixe les obligations des tiers mandatés. Cela signifie également que les tiers mandatés n'ont pas plus d'obligations à respecter que celles qui s'imposeraient à l'autorité remplissant elle-même les tâches déléguées. Le degré de détail de la liste sert aussi à garantir la sécurité du droit et à assurer l'uniformité des procédures.

Ce qui précède éclaire sur la nécessité de maintenir le projet en la forme. Un délai transitoire de quatre ans est en outre accordé aux autorités pour adapter les contrats existants aux conditions de l'article 1 OCPD si nécessaire. La disposition transitoire de l'article 16 OCPD renvoie ainsi à l'article 39, alinéa 5 OSID, selon lequel les autorités adaptent leurs outils TIC et contrats aux exigences relatives à la protection de base dès la prochaine acquisition ou modification, mais au plus tard quatre ans après l'entrée en vigueur de l'ordonnance.

10.3 Définition des systèmes algorithmiques de prise de décision

Des participantes et des participants craignaient que la disposition sur les systèmes algorithmiques de prise de décision n'aille trop loin. En substance, leur conclusion était que seuls ceux ayant un impact notable sur la prise de décision devaient en principe entrer dans cette catégorie.

L'article 7 OCPD n'est pas une disposition d'exécution de l'article 25 LCPD. Pour rappel, ce dernier prévoit que l'autorité informe la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative (décision individuelle automatisée). L'article 7 OCPD ne détermine pas non plus quand l'emploi d'un système algorithmique de prise de décision est admissible. La LCPD non plus ne prescrit rien en ce sens.

La « seule » chose que définit l'article 7, c'est ce que recouvrent le terme de système algorithmique de prise de décision et celui de risque élevé au sens de l'article 21 et 23 LCPD (respectivement : obligation d'inscrire au registre et obligation d'informer). Il apporte ainsi des réponses au moment de déterminer les utilisations qui impliquent une inscription au registre et une information. Un système algorithmique de prise de décision n'est pas défini par son degré d'influence sur la personne qui décide, mais sur son existence même. La définition s'appuie sur différentes définitions existantes, dont celle du Parlement européen. L'alinéa 1 est maintenu en tant que tel. Le jugement lié à la notion de significativité joue seulement un rôle lorsqu'il s'agit d'apprécier le risque pour la personne concernée. Ce point est réglé l'alinéa 2.

10.4 Participation des communes aux frais de l'autorité cantonale de protection des données

Différentes communes étaient d'avis que la participation aux frais de l'autorité cantonale de protection des données qui leur incombe (sauf aux quatre disposant de leur propre autorité), fixée à un franc par habitante et habitant, était trop élevée. À cet égard, il y a lieu de relever que la centralisation partielle occasionne des coûts. La LCPD fixe donc au niveau de la loi que les communes dont les tâches de surveillance sont centralisées doivent participer aux frais de l'autorité cantonale de protection des données.

Le rapport de la LCPD laissait déjà supposer que la hauteur du montant serait peu ou prou d'un franc par habitante et habitant. Les coûts supplémentaires induits par la centralisation avaient en effet été estimés à environ un million de francs et il était indiqué que toutes les communes y participeraient par l'intermédiaire de la compensation des charges. Il était donc déjà possible de prévoir que la participation serait approximativement d'un franc par habitante et habitant.

À ce sujet, le Grand Conseil a rejeté le système de financement par la compensation des charges et décidé que seules les communes ne possédant pas leur propre autorité de protection des données devraient participer aux frais du Bureau pour la protection des données. À cela s'ajoute que les coûts supplémentaires effectifs sont de quelque 720 000 francs par an selon les données du budget et du plan intégré mission-financement qui ont été publiées depuis les délibérations. La hauteur de la participation reste stable. Si le montant est arrondi selon les règles usuelles, de 720 000 à 800 000 francs, chaque commune sur laquelle l'autorité cantonale de protection des données exerce sa surveillance doit verser une somme d'un franc par habitante et habitant.

La participation d'un franc par habitante et habitant est ainsi justifiée.