ETAT DE FRIBOURG
STAAT FREIBURG

Service de législation SLeg
Amt für Gesetzgebung GeGA

Grand-Rue 26, Case postale, 1701 Fribourg

T +41 26 305 14 45, F +41 26 305 14 08
www.fr.ch/sleg

Courriel: servicedelegislation@fr.ch

Fribourg, le 6 décembre 2022

Aide à la rédaction des bases légales sur le traitement des données personnelles

Ce document vise à fournir aux juristes de l'administration cantonale un outil et une méthode les aidant à rédiger les bases légales nécessaires au traitement des données personnelles. Le fait de suivre cette méthode doit, notamment, permettre de faciliter l'obtention d'un accès à la plateforme FriPers et au Référentiel cantonal. Ce document n'a toutefois pas pour ambition d'imposer une solution spécifique aux rédacteurs et aux rédactrices de projets qui conservent toute la latitude nécessaire dans l'élaboration des bases légales les plus adaptées aux situations qu'ils ont à régler. Il ne les dispense pas non plus de mener une analyse légistique complète tant sous l'angle matériel que formel. Ce document tient compte des nouveaux standards en matière de protection des données qui seront applicables au moment de l'entrée en vigueur de la loi révisée sur la protection des données. Une version très simplifiée de celui-ci sera, en outre, en principe intégrée dans les Directives de technique législative du Service de législation (la révision est en cours). Finalement, ce document peut être lu en parallèle du Guide de législation de la Confédération en matière de protection des données.

Table des matières

1. Principes

Les articles 13 al. 2 Cst. féd. et 12 al. 2 Cst. cant. consacrent le droit à la protection des données personnelles. Selon la jurisprudence et la doctrine dominante, ils ne protègent pas uniquement l'individu contre « l'emploi abusif » des données qui le concernent, mais couvrent toute intervention de l'État impliquant le traitement de données personnelles (par exemple leur collecte, leur communication, leur conservation, *etc.*). Ils incluent également le droit à l'« autodétermination informationnelle de chaque individu » (ATF 147 I 346, consid. 5 ; ATF 146 I 11, consid. 3.11 ; ATF 145 IV 42, consid. 4.2, in : JdT 2019 IV 177).

La LPrD (RSF 17.1) pose les règles générales en matière de protection des données. Une révision totale est actuellement en cours. La version de l'ap-LPrD (état août 2022) qui fait actuellement l'objet d'une dernière consultation interne devrait être finalisée durant le premier trimestre 2023, puis validée par le Conseil d'Etat et transmise au Grand Conseil pour une entrée en vigueur prévue le 1er janvier 2024. Elle contiendra des exigences plus claires sur la nécessité de bases légales sectorielles pour le traitement de données personnelles.

La rédaction de nouvelles bases légales sectorielles dans le domaine de la protection des données doit donc suivre un certain nombre de principes exposés ci-après et qui servent à concrétiser pareil droit. Ils viennent s'ajouter à d'autres principes du droit constitutionnel et administratif. En application du principe de la légalité, toute activité étatique doit ainsi, en règle générale, être prévue au moyen d'une loi (cf. art. 4 Cst. cant.), tandis que le respect des droits fondamentaux implique qu'une restriction portée à un tel droit soit justifiée au moyen d'une base légale, poursuive un intérêt public et soit proportionnée au but visé (art. 38 Cst. cant.).

2. Champ d'application de la législation sur la protection des données

Les exigences en matière de protection des données s'appliquent en présence d'un traitement de données personnelles.

Par ***données personnelles***, il faut entendre toute information qui se rapporte à une personne identifiée ou identifiable, physique ou morale (cf. art. 3 al. 1 let. a LPrD / 4 al. 1 let. a ap-LPrD). La notion est volontairement large et ne s'applique pas uniquement aux données qui peuvent être rapportées directement à une personne mais aussi aux données qui peuvent lui être rattachées sur la base d'informations connexes. Elle s'applique tant aux données des personnes physiques que morales. Même si elle est large, l'étendue de cette notion ne doit pas être étirée à l'extrême. Selon la doctrine et la jurisprudence, la simple possibilité théorique d'identifier une personne ne suffit pas pour entraîner l'application de la loi sur la protection des données si cette possibilité implique des efforts et des investissements excessifs (ATF 138 II 346, consid. 6.1, in : JdT 2013 I 71).

Nota bene : Les données qui sont anonymisées de manière irréversible ne sont plus considérées comme des données personnelles au sens de la législation sur la protection des données. Dans ce cas, les autres règles de protection des données décrites dans cette aide n'ont, en principe, plus besoin d'être suivies. Cela vaut en tout cas aussi longtemps que la technique d'anonymisation employée reste efficace au regard de l'évolution technologique. Les données pseudonymisées et les données cryptées restent pour leur part des données personnelles, même si c'est uniquement à l'égard des personnes qui disposent d'une clé de déchiffrement. Dans ce cas, les exigences en matière de légalité restent applicables pour les responsables de traitement.

Par ***traitement de données***, il faut entendre toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés –, notamment la collecte, la conservation, l'hébergement, l'exploitation, la modification, la communication, l'archivage ou la destruction de données (cf. art. 3 al. 1

let. d LPrD / 4 al. 1 let. d ap-LPrD). À nouveau, il s'agit d'une notion large. En pratique, elle s'applique sitôt qu'un organe public manipule des données personnelles.

Lors de l'élaboration de normes concernant le traitement de données personnelles, il est obligatoire de consulter l'Autorité de la transparence, de la protection des données et de la médiation (ci-après ATPrDM) en lui soumettant les propositions législatives envisagées (cf. art. 30a al. 1 let. b LPrD / 51 al. 1 let. c ap-LPrD). Dans tous les cas, cette consultation doit intervenir au plus tard au moment de la mise en consultation de l'acte, quel que soit le type de consultation choisi (ordinaire, restreinte ou interne). En vertu des articles 23 al. 1 et 32 al. 2 let. a du règlement du 24 mai 2005 sur l'élaboration des actes législatifs (REAL ; RSF 122.0.21), l'ATPrDM est une destinataire systématique de toutes les consultations législatives à l'intérieur de l'Etat.

3. Les différents types de normes en droit de la protection des données

On peut répartir les normes relatives au traitement de données personnelles en quatre catégories :

> ***Les normes-cadre***. Il s'agit principalement des dispositions des lois sur la protection des données mais on trouve aussi des normes-cadre dans d'autres types de loi présentant un caractère transversal et se rapportant au traitement de l'information au sens large. Dotées d'un champ d'application transversal, elles sous-tendent l'ensemble des activités de traitement de données. Les normes-cadre énoncent de façon générale les principes et les règles essentiels se rapportant à tous traitements de données sans égard au secteur d'activité en cause. Elles fixent les principes de licéité de chaque traitement (réserve de la loi, principe de finalité, principe de proportionnalité, bonne foi, etc.), posent des exigences spécifiques en lien avec certaines phases d'un traitement (collecte, communication, externalisation, destruction, *etc.*) et donnent des indications sur les mesures de sécurité à mettre en place par les auteur-e-s de traitement. Les normes-cadre de la protection des données n'autorisent en principe pas elles-mêmes le traitement de données personnelles mais elles disent à quelles conditions des données peuvent être traitées.

> ***Les normes habilitantes***. Il s'agit de normes qui contiennent une autorisation expresse de faire quelque chose qu'il ne serait, en principe, pas possible de faire en l'absence d'une norme. Les normes habilitantes sont l'expression même du principe de la légalité. En droit de la protection des données, elles satisfont à l'exigence d'une base légale prévue à l'article 4 al. 1, 1ère partie LPrD / 5 al. 1 ap-LPrD). Situées dans les lois sectorielles qui régissent les différentes activités de l'État, elles disent dans quelles circonstances un traitement de données est autorisé, à quelles fins, avec quelles données, avec quelles ressources et selon quelles modalités. L'introduction dans la loi de normes habilitantes est en principe une condition nécessaire du traitement.

> ***Les normes d'accompagnement (ou normes de sécurité)***. Les normes habilitantes qui autorisent un organe public à traiter des données personnelles ne suffisent pas toujours à respecter les exigences découlant du droit constitutionnel à la protection des données et à l'autodétermination informationnelle. Elles doivent dans ce cas être complétées par des règles supplémentaires qui imposent aux responsables du traitement un certain comportement en vue de garantir une protection adéquate des droits des citoyens et des citoyennes, et de prévenir les risques d'abus et d'arbitraire.

Dans le cadre de l'exploitation de plateformes telles que FriPers et le Référentiel cantonal, ce type de normes est en principe déjà posé dans l'acte qui traite de ces plateformes plutôt que dans la législation sectorielle. Les rédacteurs et les rédactrices peuvent donc généralement y renoncer, en tout cas dans le cadre d'un usage « ordinaire » de ces plateformes. Ponctuellement, une norme d'accompagnement (ou de sécurité) peut néanmoins se révéler nécessaire en présence de traitements présentant des risques particuliers, notamment en raison des finalités poursuivies, de la nature des données traitées, du type de traitement mis en œuvre ou de la participation de personnes extérieures à l'administration.

> ***Les normes indirectes*.** Vu la complexification des tâches administratives et l'omniprésence des traitements de données dans tous les secteurs d'activités de l'État, il est impossible pour le législateur d'envisager par avance toutes les situations où un traitement de données sera nécessaire à l'accomplissement d'une certaine tâche ni d'en réglementer tous les détails. C'est pourquoi le droit de la protection des données tolère qu'un traitement de données puisse tirer sa légitimité d'une base légale indirecte (cf. art. 4 al. 1, 2e partie LPrD / 5 al. 2 let. b ap-LPrD). Une telle base légale autorise à certaines conditions la réalisation de traitements de données même sans habilitation expresse parce que les traitements en cause sont jugés nécessaires, voire indispensables, à la réalisation d'une tâche qui, elle, est prévue au moyen d'une loi. L'admissibilité des normes indirectes est toutefois généralement subsidiaire à celle des normes habilitantes.

Ces notions sont par la suite développées et illustrées plus en détails au § 4.2 du présent document.

4. La rédaction des normes

4.1. Le rang des normes

Conformément à l'article 38 Cst. cant., toute restriction d'un droit fondamental doit être fondée sur une base légale. Les restrictions graves doivent être prévues par une loi adoptée par le Grand Conseil (loi au sens formel).

Selon la jurisprudence du Tribunal fédéral, tout traitement de données personnelles, quelles que soient les données en cause et quelles que soient les finalités poursuivies, induit généralement une atteinte au droit fondamental à la protection des données. Les traitements de données sensibles sont quant à eux réputés comme induisant une atteinte grave (ATF 143 I 253, consid. 3, in : JdT 2017 I 177). On peut ajouter à cette catégorie-là les activités de profilage ainsi que, plus largement, les traitements de données personnelles dont les finalités ou les modalités présentent un risque élevé d'atteinte.

La liste des données sensibles figure de manière exhaustive à l'article 3 al. 1 let. *c* LPrD / 4 al. 1 let. c ap-LPrD. Il s'agit des données personnelles sur :

1. les opinions ou activités religieuses, philosophiques ou syndicales ;
2. la santé, la sphère intime ou l'appartenance à une race ;
3. des mesures d'aide sociale ;
4. des sanctions pénales ou administratives et les procédures y relatives.

S'alignant sur le droit fédéral, l'avant-projet de révision de la LPrD élargit cette liste en y ajoutant les données génétiques et les données biométriques.

La notion de profilage sera intégrée dans la nouvelle loi sur la protection des données. Comme en droit fédéral, il s'agit de toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne.

Quant aux traitements de données personnelles dont les finalités ou les modalités présentent un risque élevé d'atteinte, il s'agit d'une notion juridique indéterminée qui doit être concrétisée au cas par cas. Les finalités d'un traitement peuvent présenter un risque élevé d'atteinte lorsqu'elles se rapportent à de la surveillance ou à de l'investigation, qu'elles limitent sensiblement l'autonomie de la personne ou qu'elles sont susceptibles d'affecter d'une autre manière sa situation personnelle de manière significative. Les modalités du traitement des données peuvent présenter un risque élevé d'atteinte

lorsqu'elles impliquent des moyens technologiques particulièrement intrusifs ou des techniques de traitement de données de masse. Tel peut être le cas, par exemple, du recours à des algorithmes soit pour prononcer certaines décisions individuelles, soit pour intervenir en soutien au prononcé de telles décisions. Peuvent aussi être concernées certaines catégories de traitements de données à large échelle via des plateformes (FriPers, Référentiel cantonal, *etc.*).

En application de ces principes, il s'ensuit que :

> pour les traitements de données non sensibles, une base légale prévue dans une ordonnance ou un règlement est généralement suffisante même si le choix d'une loi au sens formel n'est pas interdit ;

> pour les traitements de données sensibles, les activités de profilage ou les traitements induisant un risque élevé d'atteinte aux droits des personnes concernées, une base légale dans une loi au sens formel est généralement requise.

Ces règles ne sont toutefois pas absolues. Des traitements de données, y compris sensibles, peuvent en fonction des circonstances également reposer sur une autre justification, telle que l'existence d'une base légale indirecte dans la mesure où elle est admise (cf. § 4.2.4 ci-dessous) ou encore le consentement libre et éclairé de la personne concernée au traitement de ses données, lorsque rien ne s'y oppose.

On retrouve ces exigences formulées de manière imparfaite à l'article 4 de la LPrD de 1994. Selon cette disposition, **« [l]'organe public n'est en droit de traiter des données personnelles que si une disposition légale le prévoit, ou, à défaut, si les dispositions réglant l'accomplissement de sa tâche l'impliquent »**. Contrairement au standard actuel en Suisse en matière de protection des données, cette disposition ne fait pas de différence entre base légale au sens formel et base légale au sens matériel.

Dès lors, il est prévu de la remplacer dans le cadre de la révision totale de la LPrD par une règle plus claire et précise qui correspond au standard en Suisse dans ce domaine. C'est à la lumière de cette disposition que les nouvelles bases légales en matière de protection des données doivent dorénavant être pensées.

Avant-projet LPrD, août 2022[1]

Art. 5 Base légale

[1] L'organe public n'est en droit de traiter des données personnelles que si une disposition légale le prévoit ou si l'accomplissement d'une tâche légale l'exige.

[2] Le traitement de données sensibles ne peut avoir lieu que si :

a) une loi au sens formel le prévoit expressément, ou

b) l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument et la finalité du traitement ne présente pas de risques particuliers pour les droits fondamentaux des personnes concernées.

[3] Les activités de profilage et les traitements de données personnelles dont les finalités ou les modalités présentent un risque élevé d'atteinte aux droits fondamentaux des personnes concernées ne peuvent avoir lieu que si une loi au sens formel le prévoit expressément.

[4] Exceptionnellement, une base légale n'est pas exigée pour traiter des données personnelles lorsque le traitement est nécessaire pour sauvegarder les intérêts essentiels de la personne ou d'un tiers.

[1] La présente disposition est susceptible d'évoluer jusqu'à son adoption définitive par le Grand Conseil mais son esprit devrait rester identique.

Cette disposition envisage deux cas de figure différents :

> **Le traitement de données « non sensibles »** requiert en principe soit une base légale habilitante (« *si une disposition légale le prévoit* »), soit une base légale indirecte (« *si l'accomplissement d'une tâche légale l'exige* »). Le rang de la norme peut être soit celui d'une loi au sens formel, soit celui d'une loi au sens matériel. Le choix entre l'un ou l'autre type d'acte est avant tout une question d'appréciation et peut être guidé par des motifs d'opportunité (importance du traitement de données par rapport à la matière abordée, cohérence de l'acte, place à disposition, cosmétique législative, *etc.*).

> **Le traitement de données sensibles, les activités de profilage et les traitements de données dont les finalités et les modalités présentent un risque élevé d'atteinte** sont soumis à des exigences plus élevées. Ils doivent en principe reposer sur une base légale habilitante dans une loi au sens formel (« une loi au sens formel le prévoit expressément » [voir les normes habilitantes, § 4.2.2]). Le traitement de données personnelles sensibles peut toutefois également résulter d'une base légale indirecte, lorsqu'il se trouve dans un rapport de causalité étroit avec une tâche décrite dans une loi au sens formel (« le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel » [cf. voir les normes indirectes, § 4.2.4]).

> En dérogation à ces règles, l'article 12f LPrD / art. 35 LCyb et art. 22 LPrD tels que proposé dans l'ap-LPrD offre la possibilité d'autoriser provisoirement dans une ordonnance dite « expérimentale », par le biais de **projets pilotes**, des traitements de données qui devraient en principe être prévus au niveau de la loi. La réalisation d'un projet pilote est soumise à un protocole strict. Elle requiert, en particulier, une tâche à accomplir, un besoin d'expérimentation, la nécessité d'une phase d'essai, la constitution d'un dossier complet, l'adoption par le Conseil d'Etat d'une ordonnance expérimentale d'une durée limitée et un rapport d'évaluation rétrospective. Pour les projets pilotes qui incluent le traitement de données sensibles ou d'autres types de traitement présentant un risque plus élevé d'atteinte aux droits fondamentaux, les dossiers et rapports d'évaluation relatifs à ces projets ainsi que le projet d'ordonnance expérimentale doivent être soumis pour avis à l'ATPrDM. Si les résultats du projet pilote sont concluants, le Conseil d'Etat lance la procédure législative destinée à transformer l'ordonnance expérimentale en projet de loi soumis au vote du Grand Conseil.

4.2. Le contenu des normes

L'exigence d'une base légale ne concerne pas que le rang de la norme mais s'étend à son contenu, qui doit être suffisamment clair et précis. Il faut que la base légale ait une densité normative suffisante pour que son application soit prévisible. Le degré de précision attendu d'une norme n'est toutefois pas identique pour n'importe quel traitement de données mais suit le principe de proportionnalité. Plus les risques d'atteintes à la personnalité ou aux droits fondamentaux sont élevés, plus le degré de précision de la disposition légale doit être élevé et la finalité du traitement définie de manière précise et reconnaissable pour la personne concernée.

4.2.1. Les normes-cadre

Les normes-cadre en matière de protection des données sont celles que l'on retrouve dans la législation générale. Dans le canton de Fribourg, il s'agit en premier lieu de la loi sur la protection des données (LPrD) et du règlement sur la sécurité des données (RSD ; RSF 17.15). Mais d'autres textes peuvent aussi être concernés comme la loi sur la cyberadministration (LCyb ; RSF 184.1) ; l'ordonnance relative à la plate-forme informatique contenant les données du registre des habitants (RSF 114.21.12) ou la législation sur le Référentiel cantonal (RSF 184.16).

Les normes-cadre ont une portée transversale et s'appliquent à l'ensemble des organes des collectivités publiques concernées. Elles posent les principes et les dispositions générales qui servent de fondement

au traitement des données par les collectivités publiques et dont la portée, le développement et la mise en œuvre sont précisés dans des lois sectorielles. Il s'agit en particulier des principes de finalité, de proportionnalité, d'exactitude, de transparence, de bonne foi et de sécurité. Elles peuvent aussi fixer un cadre général à certains échanges de données répondant à des règles standardisées applicables à toute l'administration comme c'est le cas, notamment, de FriPers ou du Référentiel cantonal.

En principe, la rédaction des normes-cadre en matière de protection des données n'est pas du ressort des juristes chargés de l'élaboration des dispositions sectorielles sur le traitement des données. Elles doivent néanmoins être connues de ces derniers, car elles fournissent les différents éléments à prendre en considération dans cette tâche.

4.2.2. Les normes habilitantes

Les normes habilitantes constituent l'expression même du principe de légalité. Dans le domaine qui nous occupe, elles contiennent une autorisation expresse de traiter des données personnelles. Suivant le contexte, elles donnent des indications sur les circonstances dans lesquelles un traitement de données peut être mis en œuvre, par qui, à quelles fins, avec quelles données, avec quelles ressources et selon quelles modalités.

Les normes habilitantes devraient en principe permettre de répondre aux questions suivantes :

> ***Qui sont les organes responsables du traitement des données*** : Cette indication permet notamment à la personne concernée de savoir quelle est l'autorité responsable du respect des principes de protection des données et auprès de qui elle peut faire valoir ses droits, en particulier son droit d'accès (art. 23 LPrD / 27 ap-LPrD). Il s'agit du responsable du fichier/traitement (« *Data Owner* »). S'il existe plusieurs responsables du traitement à raison de la matière, il convient de mentionner chacun d'eux (cf. p. ex. art. 34d al. 1 LASoc ; RSF 831.0.1). En revanche, il ne faut pas indiquer les éventuels sous-traitants (p. ex. en cas de recours à une solution de *Cloud Computing*), ni les organes responsables de la fourniture des infrastructures et des applications nécessaires aux traitements de données mis en œuvre (« System / Application Owner ») comme c'est souvent le cas du SITel. Une désignation trop générale (p. ex. l'État) n'est en principe pas admise si elle ne permet pas de savoir de qui on parle, ou alors elle devrait être précisée au niveau de la réglementation d'exécution.

> ***Quelles sont les finalités du traitement*** : L'indication d'une finalité suffisamment claire est une condition essentielle de toute norme autorisant un traitement de données. Sous réserve de l'existence d'un autre motif justificatif, tout traitement de données doit obligatoirement poursuivre une finalité qui est définie au niveau d'une loi ou d'une ordonnance. Pour atteindre son but, l'indication d'une finalité ne doit pas être trop vague. Les finalités indiquées doivent correspondre aux tâches qui sont fixées par le législateur dans l'acte en cause ou servir à leur réalisation. Une norme habilitante peut contenir une ou plusieurs finalités en fonction de l'acte en question. L'usage du terme « notamment » est autorisé (cf. p. ex. art. 143 LICD ; RSF 631.1), mais sa portée est limitée en pratique par les principes de la bonne foi et de loyauté. Dans les mêmes limites, une finalité inscrite peut également recouvrir d'autres sous-finalités très proches à condition d'être compatibles avec la première (« principe de compatibilité »). Cependant, il n'est généralement pas suffisant d'introduire dans un acte une base légale générale qui permettrait à l'organe compétent de traiter toutes les données nécessaires à l'accomplissement des tâches prévues dans cet acte. L'objectif est de trouver une formulation assez précise permettant aux personnes concernées – en s'entourant, au besoin, de conseils éclairés – de se représenter, à un degré raisonnable, à quelles fins leur données sont traitées.

> ***Quelles sont les données traitées*** : En principe, une énumération précise des données traitées pour chaque traitement n'est pas exigée. Des informations sur les données traitées peuvent ressortir de différentes manières avec un degré de précision plus ou moins élevé en fonction des circonstances. Pour le traitement de données non sensibles, une liste des données traitées n'est généralement pas requise si la

finalité indiquée est suffisante pour permettre à la personne concernée d'envisager sans grande surprise quelles données la concernant vont être traitées. On peut dans ce cas se contenter de quelques critères, voire d'un *listing* par catégories. Le besoin de précision peut toutefois évoluer en fonction des finalités poursuivies. Le traitement de données non sensibles peut requérir des indications plus précises si les finalités poursuivies présentent, de leur côté, un degré plus élevé de sensibilité et que les données traitées dépassent ce à quoi une personne raisonnable peut s'attendre. L'indication d'une liste exhaustive peut aussi se justifier dans des situations spécifiques où le fait de ne traiter qu'un nombre limité de données est un élément déterminant du traitement (cf. p. ex. art. 5 de l'ordonnance concernant la mise en place d'un essai pilote d'annonce électronique des déménagements ; RSF 114.21.22). Lorsqu'une énumération est proposée, il faut alors tenir compte du principe de minimisation des données, selon lequel il ne faut pas mentionner plus de données que nécessaire pour atteindre la finalité poursuivie. Pour le traitement de données sensibles, la situation est différente. Il est préférable de les mentionner clairement ou, au moins, par catégories. Il existe toutefois des exceptions, notamment au niveau des lois où le traitement de données sensibles est en quelque sorte inhérent à l'activité prévue dans l'acte en cause et où l'introduction d'une énumération aboutirait à un résultat contraire au but recherché (cf. p. ex. art. 30j al. 1 let. *b* de la loi sur la Police cantonale [RSF 551.1] ; art. 129 de la loi sur la santé [RSF 821.0.1]). Ce type d'exception doit toutefois être admis de manière restrictive. Dans certains cas, il est aussi possible, moyennant une délégation de compétence, de préciser la liste des données traitées dans la réglementation d'exécution (cf. art. 43 al. 2 LS ; RSF 411.0.1).

> ***Quelles sont les modalités du traitement*** : Lorsque cela est nécessaire, les indications concernant les modalités du traitement fournissent des compléments d'information sur les types de traitement mis en œuvre et/ou sur les processus sous-jacents. De tels compléments d'informations peuvent être requis, par exemple, en cas d'appariement de données ou de profilage, lors du recours à des algorithmes, notamment dans le cadre de processus décisionnels, ou pour donner des précisions sur des traitements de données à grande échelle. A l'instar du profilage, certaines modalités du traitement impliquent obligatoirement l'adoption d'une base légale au sens formel (cf. art. 5 al. 3 ap-LPrD). Pour d'autres, c'est le plus souvent la combinaison des modalités et des finalités poursuivies qui déterminent le rang de la norme à adopter.

> Par ***appariement de données***, on entend l'opération consistant à relier entre elles des données provenant de sources différentes dans le but d'obtenir de nouvelles informations sur une situation ou une personne. Des appariements de données peuvent être réalisés, notamment, à des fins de vérification, d'investigation ou de recherche. La base légale devrait préciser l'opération d'appariement, les données ou les catégories de données appariées et le but de l'appariement. Par ***décision individuelle automatisée***, on entend une décision prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour la personne concernée ou l'affecte de manière significative. La nécessité et le rang de la base légale dépendent du besoin de légitimité requis par la décision, de sa complexité et de ses effets sur la personne. Selon l'ap-LPrD, ces décisions doivent, en outre, impérativement contenir une mention indiquant qu'elles ont été rendues sans intervention humaine (cf. art. A1-4a CPJA tel qu'introduit par l'ap-LPrD). Une mention de ce type est aussi requise en cas de recours à des ***outils automatisés d'aide à la décision***. Si une autorité recourt à des algorithmes de profilage pour l'assister dans la prise d'une décision, elle est tenue d'en faire mention systématiquement dans la partie de la décision qui contient la motivation (cf. art. 52a CPJA tel que proposé par l'ap-LPrD). Le recours au ***profilage*** implique à chaque fois l'adoption d'une base légale au sens formel. Celle-ci devrait indiquer au moins le but du profilage (le profilage ne constituant jamais une fin en soi) ainsi que les aspects de la personnalité qui sont évalués.

La communication de données personnelles doit, en principe, être prévue expressément au moyen d'une base légale (cf. art. 10 LPrD / 14 ap-LPrD). Dans ce cas, on distingue généralement entre les communications ayant lieu sur demande de l'autorité destinataire, celles qui ont lieu spontanément de la part de l'autorité communicante mais sans obligation, celles qui doivent avoir lieu d'office et de façon obligatoire et celles qui sont exécutées au moyen d'une procédure d'appel. On peut encore ajouter à

cette liste l'interfaçage entre plusieurs bases de données distinctes. Si une base de données ou un système d'information réglé dans un acte est interfacé avec une autre base de données ou un autre système d'information réglé dans un autre acte, l'interfaçage entre les deux systèmes nécessite une base légale spécifique ; celle-ci doit alors indiquer les finalités poursuivies, l'existence d'un interfaçage et les bases de données concernées (p. ex. : art. 5 OARSec ; RSF 712.11).

> Par ***procédure d'appel***, on entend le mode de communication automatisé des données par lequel les destinataires, en vertu d'une autorisation du responsable du fichier/traitement, décident de leur propre chef, sans contrôle préalable, du moment et de l'étendue de la communication (principe du « libre-service »). Par ***interfaçage***, on entend l'utilisation d'un programme permettant un échange ordonné de données entre deux sources où l'interface reformate les données pour assurer la compatibilité entre les deux sources. La notion de procédure d'appel inclut généralement celle d'interfaçage ainsi que les autres moyens de communication automatisés sans contrôle préalable.

Même si la LPrD précise que seule l'introduction d'une procédure d'appel doit être prévue expressément au moyen d'une base légale (cf. art. 10 al. 2 LPrD / 14 al. 2 ap-LPrD), il convient en principe de préciser autant que possible chaque type de communication (sur ces aspects, voir le Guide de législation de l'Office fédéral de la justice, 2019, n° 834 ss).

> ***Particularités dans le cadre de l'accès à FriPers et au Référentiel cantonal*** : Pour ces deux plateformes, les modalités d'accès aux données qu'elles hébergent sont réglées dans les actes qui les gouvernent. La nécessité d'introduire une base légale spécifique pour accéder à ces plateformes, soit par le biais d'une procédure d'appel, soit par le biais d'un interfaçage, est remplacée par un système d'autorisation décrit dans les actes concernés (cf. art. 16a LCH ; RSF 114.21.1 / art. 25 al. 2 LCyb ; RSF 184.1 *cum* art. A4-1 Ordonnance Référentiel cantonal ; RSF 184.16). Sauf cas particulier, les rédacteurs et les rédactrices de projets législatifs peuvent en principe ne pas aborder ces questions. Une base légale spécifique peut malgré tout devoir être introduite lorsque ces plateformes sont utilisées à certaines fins spécifiques présentant des risques particuliers pour les droits des personnes concernées, notamment en cas de profilage ou d'investigation (cf. art. 137 al. 3 LICD ; RSF 631.1).

4.2.3. Les normes d'accompagnement (ou de sécurité)

Les normes d'accompagnement (ou de sécurité) reposent sur l'article 22 LPrD / 41 ap-LPrD. Elles ont pour but d'assurer le respect des droits fondamentaux des personnes concernées et/ou la sécurité des données face à des traitements qui présentent des risques particuliers pour les personnes concernées ou pour l'État. Elles complètent les normes habilitantes qui autorisent l'exécution d'un traitement de données. Elles peuvent être intégrées soit dans une loi au sens formel, soit dans une loi au sens matériel. Une répartition entre les deux rangs est aussi possible (principes généraux formulés de manière technologiquement neutre au niveau de la loi et solutions de mise en œuvre formulées plus précisément et adaptables au niveau de la réglementation d'exécution).

Les normes d'accompagnement (ou de sécurité) peuvent soit prendre la forme d'engagements ou de garanties visant à écarter toute utilisation abusive des données (cf. art. 20 al. 2 et 21 LCyb ; RSF 184.1), soit instituer la mise en place de mesures techniques ou organisationnelles spécifiques (cf. art. A5-2 de l'ordonnance Référentiel cantonal ; RSF 184.16). Elles ne doivent pas nécessairement figurer dans des normes distinctes. Elles peuvent aussi être intégrées dans des normes habilitantes au moyen d'un ou plusieurs alinéa(s) spécialement consacré(s) à cette fin.

Les mesures organisationnelles et techniques de sécurité à mettre en place dépendent de chaque type de traitement et doivent faire l'objet d'une analyse au cas par cas. De manière très résumée, elles peuvent porter sur :

> ***La disponibilité***. Cette propriété vise à assurer qu'un système d'information et les données qu'il contient peuvent être utilisés par les personnes autorisées au moment voulu conformément aux

performances prévues (cf. p. ex. art. 8a al. 2 LPAL ; RSF 124.1 même si hors contexte de la protection des données) ;

> ***L'intégrité***. Cette propriété vise à assurer qu'une information n'a pas été modifiée, détruite ou altérée d'une quelconque manière que ce soit, notamment de façon involontaire, depuis sa création (cf. p. ex. art. 61 al. 3 LGC ; RSF 121.1 ; voir aussi art. 11 RPAL ; RSF 124.11 même si hors contexte de la protection des données) ;

> ***L'authenticité***. Cette propriété vise à assurer que l'auteur-e d'une information nouvelle ou modifiée a été identifié et qu'il ou elle dispose des droits nécessaires pour ce faire (cf. p. ex. art. 6 LArch ; RSF 17.6) ;

> ***La traçabilité***. Cette propriété permet d'établir quelle personne a eu accès à une donnée, à quel moment et quel traitement est concerné (cf. p. ex. art. A5-2 de l'ordonnance Référentiel cantonal ; RSF 184.16) ;

> ***La pérennité***. Cette propriété vise à assurer qu'un système d'information et les données qu'il contient pourront continuer d'être exploités dans le temps malgré la possibilité de changement dans les formats et les supports de données utilisés (cf. p. ex. art. 12d al. 1 LPrD / 19 al. 1 ap-LPrD) ;

> ***La résilience***. Cette propriété vise à assurer qu'un système d'information est capable de faire face à des perturbations internes ou externes tout en permettant la poursuite de son exploitation (cf. p. ex. art. 4 al. 1 de l'ordonnance fédérale sur les cyberrisques ; RS 120.73) ;

> ***La confidentialité***. Cette propriété vise à assurer que seules les personnes dûment autorisées disposent d'un accès aux données leur permettant de les consulter et, le cas échéant, de les diffuser. Elle s'appuie sur différentes techniques telles que l'anonymisation, la pseudonymisation et le chiffrement des données (cf. p. ex. art. 103 al. 2 RLS ; RSF 411.0.11 / art. 12e al. 1 LPrD ; RSF 17.1).

Il n'est pas obligatoire de prévoir des mesures de sécurité dans chaque cas au niveau de la loi ou d'une ordonnance. Mais des mesures de sécurité peuvent quand même s'avérer nécessaires par rapport à certains types d'activités présentant des risques particuliers, notamment lorsqu'elles impliquent l'interconnexion de plusieurs bases de données entre elles, la réunion de plusieurs données sensibles ou le recours à des algorithmes. Le besoin de telles normes peut émerger au moment de l'élaboration d'un concept SIPD (Concept de sécurité de l'information et de protection des données) ou d'une analyse d'impact relative à la protection des données (cf. art. 42 ap-LPrD). Le présent document peut à cet effet se montrer utile pour déterminer les exigences en matière de protection des données, pour évaluer les risques et pour déterminer les mesures à prendre en vue de l'élaboration du concept ou de l'analyse d'impact.

> Dans certaines situations, les mesures à prendre sont déjà énoncées spécifiquement dans un autre acte à titre de norme-cadre. Il n'est donc pas nécessaire de les répéter une deuxième fois comme norme d'accompagnement (voir, par exemple, les mesures particulières énoncées à l'article 21 RSD s'agissant de la mise en place d'une procédure d'appel).

Si un projet législatif requiert l'insertion de normes de sécurité, se pose alors la question du type d'acte où insérer ces normes (loi au sens formel ou matériel). Idéalement, les lois au sens formel devraient le plus possible être rédigées avec des termes ouverts qui ne font pas référence à une technologie ou une technique particulière mais qui se concentrent surtout sur un ou plusieurs objectifs de sécurité à atteindre (principe de neutralité technologique). Si des précisions doivent être apportées sur la manière d'atteindre ces objectifs, il est préférable de les insérer dans un acte d'exécution plutôt que dans une loi. Ainsi les objectifs de sécurité qui sont fixés au niveau de la loi restent en principe stables, mais la manière de les atteindre peut plus facilement être adaptée aux évolutions de la technique.

Dans le cadre de l'accès aux données provenant de la plateforme FriPers ou du Référentiel cantonal, les normes d'accompagnement (ou de sécurité) sont insérées directement dans la législation relative à ces plateformes. Les rédacteurs et les rédactrices de projets peuvent donc en principe ne pas aborder ces questions. Dans l'hypothèse où l'introduction de telles normes se révélerait nécessaire dans un cas particulier, il est possible de demander conseil auprès des organes spécialisés de l'État dans ces questions (ATPrDM et SITel).

Quand bien même les rédacteurs et les rédactrices de projets législatifs ne sont peut-être pas les personnes les mieux informées sur ces questions, la rédaction de normes d'accompagnement (ou de sécurité) implique de tenir compte de l'évolution des technologies dans le temps. Il est donc particulièrement recommandé de s'entourer de spécialistes de ces questions au moment de rédiger ce type de normes et de procéder ponctuellement à une réévaluation de leur efficacité et de leur pertinence.

4.2.4. Les normes indirectes

Les normes indirectes ne constituent pas à proprement parler des normes de protection des données. Elles énoncent une tâche légale dont la réalisation implique néanmoins un traitement de données personnelles. Comme elles ne contiennent pas les différentes indications se rapportant à un traitement de données, elles sont moins transparentes pour les personnes concernées et elles sont aussi moins faciles à appréhender pour les organes qui traitent des données.

L'admissibilité des normes indirectes comme motif justificatif à un traitement de données requiert pour cette raison une certaine prudence et, dans tous les cas, une analyse circonstanciée qui doit porter tant sur les risques du traitement, les catégories de données pouvant être traitées que sur les modalités de leur traitement et les organes à qui elles peuvent profiter. Une attention particulière doit être portée à la mise en œuvre des principes de finalité et de proportionnalité. En outre, il faut garder à l'esprit que l'admissibilité des normes indirectes est généralement subsidiaire à celle des normes habilitantes. Une norme indirecte peut suppléer l'absence d'une norme habilitante de manière ponctuelle. Un traitement de données qui se caractérise par une certaine régularité ou durabilité devrait, en revanche, pouvoir s'appuyer sur une norme habilitante.

Les exigences concernant les normes indirectes varient selon qu'on se trouve en présence de données « non sensibles » ou de données « sensibles » :

> S'agissant **des données « non sensibles »**, une base légale indirecte est généralement considérée comme admissible dès lors qu'il existe un lien factuel suffisant et reconnaissable entre une tâche et les données nécessaires à son accomplissement. La tâche peut être mentionnée soit dans une loi au sens formel, soit dans une loi au sens matériel (ordonnance). Quand bien même les normes indirectes ne prévoient pas expressément un traitement de données, elles devraient néanmoins être accompagnées de suffisamment d'éléments permettant aux personnes concernées d'envisager quelles catégories de données feront l'objet d'un traitement (p. ex. si l'octroi d'une prestation est subordonnée à la condition que plusieurs personnes fassent partie du même ménage, le traitement des données visant à connaître la composition du ménage peut être couvert par une norme indirecte).

> S'agissant **des données « sensibles »,** les exigences sont plus élevées. D'une part, la tâche légale nécessitant un traitement de données doit être prévue dans une loi au sens formel et le traitement visant sa réalisation doit être « indispensable » à celle-ci. Le mot indispensable n'a pas la même largesse qu'« utile » ou même « nécessaire ». Pour justifier le traitement de données sensibles sur la base d'une norme indirecte, il faut qu'en l'absence dudit traitement, la tâche ne puisse quasiment plus être réalisée ou uniquement au prix d'efforts disproportionnés. Le caractère indispensable doit porter sur tous les aspects du traitement (catégories de données traitées, modalités du traitement, organes autorisés à traiter des données, *etc.*). D'autre part, la finalité du traitement ne doit pas présenter de risques particuliers pour les droits fondamentaux de la personne concernée. L'expression « risque particulier » est moins fort que

risque élevé requérant l'adoption d'une base légale au sens formel. Mais il est plus fort qu'un simple risque théorique propre à chaque traitement de données. Dans tous les cas, une norme indirecte autorisant le traitement de données sensibles devrait être accompagnée de suffisamment d'éléments permettant aux personnes concernées de se représenter quelles données sensibles les concernant feront l'objet d'un traitement (p. ex. l'utilisation de la religion pour la détermination de l'impôt paroissial).

5. L'accès aux données personnelles de base

Il est globalement admis que certaines données personnelles de base, non sensibles, sont pratiquement nécessaires à tout organe des collectivités publiques sur une base régulière ou ponctuelle (cf. Stratégie numérique de la Confédération 2020-2023, § 2.1). Il s'agit de données permettant d'identifier et de prendre contact avec une personne comme ses noms, ses prénoms, sa raison sociale (pour les personnes morales), ses adresses, sa date de naissance (ou de fondation pour les personnes morales) et ses dirigeants et représentants (pour les personnes morales). Peuvent aussi faire partie de cette catégorie de données le numéro de téléphone ou l'adresse de courriel de la personne pour autant qu'elle consente à partager ces données.

En soi, ces données non sensibles peuvent en principe être collectées et traitées sur la base d'une norme indirecte même relativement vague, car l'existence d'un lien factuel suffisant et reconnaissable entre l'accomplissement d'une certaine tâche se rapportant à une personne et les données qui permettent d'identifier cette dernière et/ou de la contacter peut quasiment toujours être démontrée.

Le besoin et la gestion centralisée des données de base est un élément de plus en plus central des différentes politiques en matière de cyberadministration. Une de ses composantes est l'introduction du principe « *Once-Only* » en vertu duquel certaines informations de base qui servent à la grande majorité des unités administratives ne devraient être collectées et traitées qu'une seule fois avant d'être mises à disposition plus largement des unités administratives de l'État et des communes. La mise en place d'un tel système doit servir à la fois les intérêts des administré-e-s et de l'administration. Aux premiers, il évite d'avoir à communiquer régulièrement les mêmes données aux différentes unités administratives de l'État. A la seconde, il épargne des tâches redondantes et lui permet de concentrer ses efforts et ses ressources sur ses tâches légales.

S'inscrivant dans cette démarche du *Once-Only*, une disposition générale visant à accorder un accès à un certain nombre de données de base à l'ensemble des unités administratives de l'État sera prochainement intégrée dans la loi traitant du Référentiel cantonal. Le socle des données concernées devrait être aussi restreint que possible. Le but est de réunir des données de base, toutes non sensibles, comparables à celles qu'on trouve dans un annuaire. Ce faisant, les unités administratives concernées traiteront les données en question sur le fondement d'une base légale qui les y autorise formellement. Elles n'auront plus besoin de contourner l'absence de base légale en se tournant vers des sources de données non officielles et moins fiables disponibles sur Internet. En outre, elles auront l'assurance de disposer à chaque fois de données actualisées et correspondant aux informations officielles en possession de l'État, ce qui est conforme au principe d'exactitude prévu dans la loi sur la protection des données.

6. L'utilisation systématique du numéro AVS

Depuis le 1er janvier 2022, l'article 153*c* de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS ; RS 831.10) permet aux autorités de la Confédération, des cantons et des communes d'utiliser systématiquement le numéro AVS (ci-après : le NAVS) dans l'exécution de leurs tâches légales en vertu d'une autorisation générale, sans avoir besoin à cette fin d'une disposition spécifique dans une loi spéciale pour chaque nouvel usage. Il n'est dès lors plus nécessaire d'inscrire une norme habilitante dans la loi spéciale correspondante pour chaque but d'utilisation et chaque catégorie d'utilisateurs et utilisatrices systématiques du NAVS.

L'utilisation du NAVS est réputée systématique lorsque l'intégralité, une partie ou une forme modifiée de ce numéro est traitée en étant liée à des données personnelles collectées et stockées de manière structurée (cf. art. 153*b* LAVS). Tel est le cas lorsque le NAVS est stocké, même modifié, dans un fichier de données. Par fichier on entend tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée. Sont aussi concernés les cas où le NAVS est sauvegardé de manière cryptée, réversiblement ou irréversiblement – via une fonction de hachage par exemple. En revanche, il n'y a pas d'utilisation systématique du NAVS lorsque celui-ci est échangé de manière transitoire sans stockage dans une base de données non structurée.

Les nouvelles possibilités d'usage du NAVS ne valent toutefois qu'à l'égard des organes habilités à traiter celui-ci de manière systématique. Pour être habilités à traiter systématiquement le NAVS, les organes de l'administration doivent préalablement s'annoncer auprès de la Centrale de compensation de la Confédération (CdC) et mettre en place une série de mesures organisationnelles et techniques destinées à garantir une utilisation conforme du NAVS. Il en résulte que la communication systématique du NAVS n'est autorisée par le droit fédéral qu'entre organes habilités à traiter celui-ci systématiquement ; la communication du NAVS à un organe non-habilité à traiter systématiquement ce numéro ne peut pas se fonder sur l'article 153*c* LAVS.

En outre, l'autorisation générale de traiter systématiquement le NAVS ne s'applique pas non plus aux personnes ou aux organisations de droit public et privé qui accomplissent une tâche administrative sans faire partie de l'administration, ni aux organismes intercantonaux ou intercommunaux établis en dehors de l'administration. Pour ces catégories de personnes ou d'organismes, l'adoption d'une base légale correspondante reste également toujours requise (cf. art. 153*c* al. 1 let. a, ch. 4).

Bien que l'adoption d'une base légale ne soit généralement plus exigée pour le traitement systématique du NAVS, cela peut cependant demeurer nécessaire dans certaines situations pour des raisons de cohérence, de transparence et de bonne foi. Tel peut être le cas, par exemple, lorsqu'une disposition énumère quelles sont les données collectées et enregistrées (cf. art. 19 LCyb ; RSF 184.1). Si le NAVS en fait partie, ce pourrait être contraire aux règles de la bonne foi de ne pas l'indiquer. L'usage du NAVS peut aussi exceptionnellement devoir être mentionné si celui-ci occupe une fonction clé dans le déroulement d'une procédure ou d'un processus nécessitant d'être décrit dans un acte législatif.

Selon les articles 153*d* à 153*h* LAVS, pour être reconnu utilisateur ou utilisatrice systématique du NAVS, il faut satisfaire aux conditions suivantes :

1. Annoncer à la Centrale de compensation l'utilisation systématique du NAVS au moyen du formulaire prévu à cet effet.
2. Désigner une personne responsable de l'utilisation systématique du NAVS (RUSN).
3. Limiter l'accès au numéro AVS aux personnes qui ont besoin de ce numéro pour accomplir leurs tâches légales.
4. Informer les personnes autorisées à utiliser le numéro AVS que celui-ci ne peut être utilisé qu'en rapport avec leurs tâches et communiqué que conformément aux prescriptions légales.
5. Garantir la sécurité de l'information et la protection des données (SIPD), notamment en veillant à crypter les fichiers de données qui comprennent le numéro AVS et qui transitent par un réseau public.
6. Définir la manière de procéder en cas d'accès non autorisé aux banques de données ou d'utilisation abusive de celles-ci.
7. Permettre à la Centrale de compensation (ci-après : la CdC) d'effectuer des contrôles des numéros AVS utilisés et faire les corrections ordonnées par la CdC.

7. Check-List de questions à examiner lors de l'élaboration de bases légales servant au traitement de données personnelles

1. Questions préalables	
Est-on en présence de données personnelles (non-anonymisées)?	Non ☐ -> LPrD pas applicable Oui ☐
Est-ce que la finalité du traitement est connue ?	Non ☐ -> Nécessite l'interruption du traitement Oui ☐
Est-ce que le catalogue des données nécessaires au traitement est connu et tient-il compte du principe de proportionnalité et de minimisation des données ?	Non ☐ -> Nécessite des investigations complémentaires Oui ☐
Les données appartiennent-elles à la catégorie des données dites de base ?	Non ☐ -> Requiert une analyse juridique complète Oui ☐ -> Voir si accès possible via FriPers ou le Référentiel cantonal aux conditions particulières fixées dans les lois y relatives
Le traitement requiert-il une base légale ?	Non ☐ -> Existe-t-il un autre motif justificatif valable, en particulier une base légale indirecte ? Voir section 2 Oui ☐ -> Voir section 3
Plusieurs organes ou personnes prennent-ils part au traitement ?	Non ☐ Oui ☐ -> Voir section 4
Des garanties particulières ou des mesures d'accompagnement ou de sécurité sont-elles requises afin de prévenir les risques d'abus ou de traitements illicites	Non ☐ Oui ☐ -> Voir section 5
Le traitement inclut-il le NAVS ?	Non ☐ Oui ☐ -> Voir section 6
2. Normes indirectes	
Le traitement de données sert-il à l'exécution d'une tâche « accessoire » ou de peu d'importance prévue dans une loi au sens formel ou dans une ordonnance (norme indirecte) ?	Non ☐ -> Le traitement n'est pas en rapport avec la loi et doit être interrompu Oui ☐ -> Voir questions suivantes
Le traitement se caractérise-t-il par une certaine régularité ou durabilité ?	Non ☐ Oui ☐ -> Penser à insérer une norme habilitante

En cas de traitement de données « ordinaires », les données traitées présentent-elles un lien factuel et reconnaissable suffisant avec la tâche à accomplir ?	Non ☐ -> Le traitement n'est pas en rapport avec la loi et doit être interrompu ou de nouvelles bases légales doivent être élaborées Oui ☐ -> Se demander si une base légale habilitante ne serait pas souhaitable
En cas de traitement de données sensibles, les données traitées sont-elles indispensables à l'exécution d'une tâche prévue dans une loi au sens formel et le traitement ne présente pas de risque particulier pour les droites des personnes concernées ?	Non ☐ -> Soit renoncer au traitement, soit créer une base légale adéquate Oui ☐ -> Se demande si une base légale habilitante ne serait pas souhaitable
3. Normes habilitantes	
La base légale habilitante envisagée donne-t-elle des indications sur les auteurs du traitement, les finalités du traitement, sur les (catégories de) données traitées et sur les modalités du traitement ?	Non ☐ -> Des précisions sont probablement à apporter Oui ☐
Est-on en présence de données sensibles ou d'activité de profilage ?	Non ☐ Oui ☐ -> Peut avoir un impact sur le rang de la base légale à élaborer
Les finalités ou les modalités du traitement présentent-elles un risque accru d'atteinte aux droits des personnes concernées ?	Non ☐ Oui ☐ -> Peut avoir un impact sur le rang de la base légale à élabore
Le traitement prévu implique-t-il des appariements de données, un interfaçage entre plusieurs bases de données, un accès à une base de données par procédure d'appel, le recours à des algorithmes, le prononcé d'une décision individuelle automatisée ou présente-t-il d'autres particularités ?	Non ☐ Oui ☐ -> Une mention expresse de ces éléments doit être envisagée dans une disposition idoine
4. Responsabilités	
Le ou les responsable(s) du fichier/traitement ont-ils été clairement identifiés ?	Non ☐ -> Besoin de clarification Oui ☐ -> Le ou les responsables du fichier/traitement doivent apparaître comme tels dans les dispositions légales. En cas de co-responsabilité entre plusieurs organes, définir les différentes responsabilités dans la déclaration de

	traitement (art. 19 LPrD / 39 ap-LPrD)
Existe-t-il d'autres participants au fichier/traitement, notamment des sous-traitants ou des fournisseurs de service cloud ?	Non ☐ Oui ☐ -> Possibilité prévue par la loi mais avec des conditions particulières ; nécessite généralement de régler la question des responsabilités de manière contractuelle.
5. Normes d'accompagnement et de sécurité	
Des mesures de sécurité particulières sont-elles requises ?	Non ☐ Oui ☐ -> Un concept SIPD a-t-il été élaboré ?
Quelles mesures de sécurité sont particulièrement requises ?	Disponibilité ☐ Intégrité ☐ Authenticité ☐ Traçabilité ☐ Pérennité ☐ Résilience ☐ Confidentialité ☐ Autres garanties ☐
Les mesures de sécurité requises figurent-elles déjà dans une autre loi ou une ordonnance applicable au traitement de données ?	Non ☐ -> Si une telle base légale semble nécessaire, la créer avec au besoin l'appui de l'ATPrD et/ou du SITel Oui ☐
6. Utilisation systématique du NAVS	
Le NAVS est-il stocké en intégralité, en partie ou sous une forme modifiée en étant lié à des données personnelles collectées de manière structurée ?	Non ☐ Oui ☐ -> Les organes de l'administration cantonale et communale sont autorisés à utiliser systématique le NAVS à condition de s'annoncer à la CdC et d'appliquer les mesures de sécurité spécifiques prévues aux art. 153d ss LAVS. Cette autorisation ne s'applique pas aux organisations ou aux personnes de droit public ou de droit privé extérieures à l'administration chargée d'une tâche administrative au sens de l'article 153c al. 1 let. a ch.

	4 LAVS. Pour ces personnes une base légale reste requise.
Le NAVS est-il échangé systématiquement en intégralité, en partie ou sous une forme modifiée en étant lié à des données personnelles collectées de manière structurée ?	Non ☐ Oui ☐ -> Un organe habilité à traiter systématiquement le NAVS est habilité à communiquer celui-ci de manière systématique (c'est-à-dire lié à des données personnelles collectées de manière structurée) à un autre organe habilité à traiter systématiquement le NAVS. Dans ce cas, seule la communication des données personnelles souhaitées doit être prévue au moyen d'une base légale, mais pas la communication du NAVS qui sert uniquement à des fins techniques et est prévue par le droit fédéral. En revanche, la communication du NAVS à un organe qui n'est pas habilité à traiter systématiquement le NAVS requiert une base légale.

8. Liste d'exemples de normes sur le traitement des données personnelles

Ce dernier chapitre offre une liste d'exemples de différentes bases légales en droit cantonal concernant le traitement des données personnelles. Son but n'est pas d'imposer une manière spécifique de rédiger des normes, mais d'offrir un certain nombre d'exemples pouvant servir d'inspiration aux rédacteurs et aux rédactrices de projets dans leurs domaines d'activité.

> Exemples de ***normes habilitantes***

Loi sur la santé (LSan ; RSF 821.0.1)

Art. 129 Traitement de données personnelles

[1] Les organes chargés d'appliquer la présente loi sont habilités à traiter et à faire traiter les données personnelles, y compris des données sensibles et les profils de la personnalité, qui leur sont nécessaires pour accomplir leurs tâches.

[2] Ils peuvent notamment communiquer ces données :

a) à d'autres autorités et organes cantonaux, intercantonaux, fédéraux, étrangers ou internationaux lorsqu'elles sont nécessaires à l'accomplissement de leurs tâches ;

b) à des organes ou des personnes privés lorsqu'elles sont nécessaires à l'accomplissement d'une tâche qui leur est confiée par la législation ou d'un devoir légal qui leur incombe.

[3] La Direction peut ouvrir aux autorités et organes mentionnés à l'alinéa 2 l'accès aux données du registre des professionnels de la santé au moyen d'une procédure d'appel, notamment par un accès en ligne.

Loi sur la Police cantonale (LPol ; RSF 551.1)

Art. 30i Organisation – Réseau d'annonce et partenariat

[1] Les partenaires suivants et l'unité de gestion des menaces partagent toute information relative à un risque important de commission d'un acte de violence susceptible de porter atteinte à l'intégrité physique, psychique ou sexuelle de tiers :

a) les services de l'Etat, des communes et des autres corporations de droit public ainsi que des établissements de droit public ;

b) les autorités du Pouvoir judiciaire ;

c) les institutions privées, lorsqu'elles accomplissent des tâches de droit public ;

d) les professionnels de la santé ;

e) les associations poursuivant un but social, de prévention ou de soutien ainsi que les associations religieuses.

[2] Les fonctionnaires et les membres des autorités sont déliés de leur secret de fonction dans les relations entre l'unité de gestion des menaces et les partenaires.

[3] Les professionnels de la santé sont déliés de leur secret professionnel aux conditions fixées par la loi sur la santé.

[4] Les ecclésiastiques et leurs auxiliaires sont déliés du secret professionnel dans leurs relations avec l'unité de gestion des menaces.

Loi sur les impôts cantonaux directs (LICD ; RSF 631.1)

Art. 143 Traitement des données

[1] Le Service cantonal des contributions gère, pour l'accomplissement des tâches qui lui incombent en vertu de la présente loi, des systèmes d'information. Ceux-ci peuvent contenir des données sensibles portant notamment sur des sanctions administratives ou pénales importantes en matière fiscale.

[2] Le Service cantonal des contributions et les autorités visées à l'article 141 échangent les données qui peuvent être utiles à l'accomplissement de leurs tâches dans la mise en œuvre de la présente loi ou d'autres lois fiscales cantonales ou fédérales. Les autorités citées à l'article 142 communiquent aux autorités chargées de l'exécution de la présente loi les données qui peuvent être importantes pour son exécution.

[3] Les données sont communiquées dans des cas d'espèces ou sous forme de liste ou encore sur des supports de données électroniques. Elles peuvent également être rendues accessibles au moyen d'une procédure d'appel lorsqu'une base légale le prévoit.

[4] Est obligatoire la communication de toutes les données qui peuvent servir à la taxation et à la perception des impôts, notamment :

a) l'identité ;

b) l'état civil, le lieu de domicile ou de séjour, l'autorisation de séjour et l'activité lucrative ;

c) les opérations juridiques.

[5] Les données personnelles communiquées et les équipements utilisés tels que les supports de données, les programmes informatiques et la documentation concernant ces programmes doivent être protégés de toute manipulation, modification ou destruction non autorisées ainsi que du vol.

[6] Le Conseil d'Etat édicte des dispositions d'exécution sur l'accès aux données ainsi que sur les autorisations de traitement, la durée de conservation, l'archivage et la destruction des données. Il arrête en outre les modalités d'application de la communication de données électroniques par procédure d'appel.

Loi sur les bourses et les prêts d'études (LBPE ; RSF 44.1)

Art. 14a Accès aux données du SCC

[1] Le Service chargé des subsides de formation peut accéder, par une procédure d'appel, aux données du Service cantonal des contributions (SCC) relatives aux conditions de revenu et de fortune nécessaires au calcul du revenu déterminant des requérants et des personnes légalement tenues à leur entretien, dans le respect des règles découlant de la protection des données.

[2] Il informe les personnes dont les données fiscales ont été collectées conformément à l'alinéa 1.

Ordonnance d'application de la législation fédérale sur les résidences secondaires (OARSec ; RSF 712.11)

Art. 5 *Plate-forme informatique – Contenu et buts*

[1] Il est mis en place une plate-forme informatique comprenant les données issues d'un croisement du registre cantonal FriPers et du registre fédéral des bâtiments et logements (RegBL).

[2] La plate-forme poursuit notamment les buts suivants :

a) servir de référence aux organes et autorités cantonales compétents pour l'examen et la délivrance des autorisations de construire en indiquant pour chaque commune, en cours d'année, la proportion effective de résidences secondaires ;

b) servir de moyen d'annonce en mettant à la disposition des préfets les informations relatives aux changements de séjour des personnes ;

c) servir d'aide à l'exécution pour les préfets qui doivent s'assurer de la bonne mise en œuvre par les communes de leurs tâches de police des constructions.

> Exemples de ***normes d'accompagnement (ou de sécurité)***

Loi sur la cyberadministration (LCyb ; RSF 184.1)

Art. 20 al. 2 Utilisation systématique du NAVS

[2] L'utilisation du numéro AVS à d'autres fins que celles qui sont décrites à l'alinéa 1 est prohibée. En particulier, il est interdit de faire usage du numéro AVS comme moyen d'apparier des données entre elles à des fins de profilage ou d'investigation. Les lois spéciales sont réservées.

Ordonnance concernant la mise en œuvre du Référentiel cantonal de données de personnes, organisations et nomenclatures (projet pilote ; RSF 184.16)

Art. a5-2 Journalisation et traçabilité des opérations de traitement

[1] Les opérations de traitement sur les données du Référentiel cantonal font l'objet d'une procédure de journalisation permettant d'analyser les accès aux données, de mettre en évidence la survenance de dysfonctionnements et de répondre aux besoins de surveillance.

Ordonnance concernant l'exécution des relevés statistiques cantonaux (RSF 110.11)

Art. 13 Destruction des éléments d'identification des personnes et du matériel d'enquête

[1] Les organes responsables détruisent les éléments d'identification des personnes et les documents d'enquête dès qu'ils n'en ont plus besoin pour saisir, compléter, contrôler et apurer les données ou pour établir des séries chronologiques.

Règlement d'exécution de la loi sur l'aide sociale (RELASoc ; RSF 831.0.11)

Art. 21 Rapport sur la situation sociale et la pauvreté

[1] …
[2] …
[3] La transmission de données en vue de la production du rapport se fait en concertation avec le Service de l'informatique et des télécommunications par des moyens organisationnels et techniques adéquats pour assurer la sécurité des données (disponibilité, intégrité et confidentialité). Le traitement et la conservation des données se font dans un espace de stockage dont les accès sont protégés et peuvent être audités.
[4] Le Service de la statistique nomme ses collaborateurs et collaboratrices habilités à traiter les données. Ces derniers sont soumis au secret fiscal pour les données fiscales proprement dites.
[5] …

> Exemples de ***normes indirectes***

Loi sur l'exercice des droits politiques (LEDP ; RSF 115.1)

Art. 2a Exercice des droits politiques (citoyenneté active) – En matière communale

[1] Ont le droit de voter et d'élire en matière communale, s'ils sont âgés de 18 ans révolus :
a) les Suisses et Suissesses domiciliés dans la commune ;

b) les étrangers et étrangères domiciliés dans la commune qui sont domiciliés dans le canton depuis au moins cinq ans et au bénéfice d'une autorisation d'établissement (permis C).

[2] La commune procède à l'enregistrement dans le registre électoral. En cas de doute sur la qualité de citoyenneté active, l'étranger ou l'étrangère, dont la qualité est en question, est tenu-e de collaborer à l'établissement des faits justifiant l'octroi de cette qualité.

[3] …

[4] Les étrangers ou étrangères inscrits au registre électoral d'une commune qui quittent le canton sont, à leur retour, réinscrits dans le registre électoral de leur commune de domicile, pour autant qu'ils soient au bénéfice d'une autorisation d'établissement.

Loi sur les bourses et les prêts d'études (LBPE ; RSF 44.1)

Art. 10 Bénéficiaires

[1] Peuvent bénéficier des subsides, sur requête et à la condition que le domicile déterminant se trouve dans le canton :

a) les citoyens et citoyennes suisses ;
b) les personnes de nationalité étrangère bénéficiaires d'un permis d'établissement en Suisse ou d'un permis de séjour annuel;
c) les réfugié-e-s ou les apatrides résidant en Suisse et reconnus par elle ;
d) les ressortissants et ressortissantes d'Etats membres de l'Union européenne et de l'Association européenne de libre-échange (AELE), à condition qu'ils soient assimilés aux citoyens et citoyennes suisses dans le domaine des bourses et prêts d'études par les accords internationaux.

[2] Le règlement d'exécution précise la notion de domicile déterminant en matière de subsides.

Loi sur le registre foncier (LRF ; RSF 214.5.1)

Art. 23 Convocation

[1] Le conservateur ou la conservatrice convoque aux séances de reconnaissances :

a) les propriétaires des biens-fonds compris dans le périmètre ;
b) les titulaires de droits distincts et permanents immatriculés ;
c) dans la mesure où ils doivent consentir à une modification ou une radiation envisagées ou à l'inscription d'un droit produit, les autres titulaires de droits réels limités, et
d) au besoin, les personnes qui ont produit des droits non inscrits ainsi que les propriétaires des biens-fonds limitrophes du périmètre.

Règlement sur l'agriculture (RAgri ; RSF 910.11)

Art. 40 Vérification de la reconnaissance

[1] Le Service vérifie périodiquement si les exploitations et les communautés reconnues satisfont aux conditions posées par l'ordonnance fédérale sur la terminologie agricole et la reconnaissance des formes d'exploitation.

[2] Il vérifie sans délai la reconnaissance des communautés d'exploitation, notamment lorsque les circonstances laissent supposer :

a) qu'il y a eu un changement des exploitants ou exploitantes impliqués, ou,

b) pour les unités de production concernées, qu'une modification des rapports de propriété s'est produite depuis la reconnaissance, ou

c) que les contrats de bail à ferme agricole existant au moment de la reconnaissance sont modifiés.