Guide pratique rédigé par la Conférence des gouvernements cantonaux (Guide pratique CdC)

Réforme européenne de la protection des données/Modernisation de la Convention du Conseil de l'Europe (Convention 108) :

Adaptation des lois cantonales sur (l'information et) la protection des données

Nouvelles sources :

P-Conv108	Convention (du Conseil de l'Europe) pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel; texte consolidé des propositions de modernisation de la Convention 108 suite à la réunion du CAHDATA (15-16 juin 2016), (https://www.admin.ch/ch/f/gg/pc/documents/2826/Revision-totale-de-la-loi-sur-la-protection-des-donnees_Convention_fr.pdf)
Dir. 2016/680	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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L119 du 4 mai 2016, 89 ss.
AP-LPD	Avant-projet relatif à une loi fédérale sur la protection des données entièrement révisée (version mise en consultation auprès des offices le 21 décembre 2016), https://www.admin.ch/ch/f/gg/pc/documents/2826/Revision-totale-de-la-loi-sur-la-protection-des-donnees_Projet-LPD_fr.pdf)

Référence :

Guide	Conférence des gouvernements cantonaux (CdC), Mise en œuvre Schengen/Dublin dans les cantons: protection des données, Guide pratique, 2006 (https://ius.unibas.ch/uploads/publics/7605/20100219145136_4b7e9768631b1.pdf)

Nécessité d'adaptation :

Aucune adaptation requise
Nécessité d'adaptation à vérifier
Adaptation requise

Contexte

Le présent état des lieux part du principe que des adaptations ont déjà eu lieu à la suite de l'association de la Suisse à l'espace Schengen (adaptations sur la base du Guide pratique 2006 et en raison de la reprise de la décision-cadre de 2008 (2008/977). Les cantons qui n'auraient pas encore procédé aux adaptations nécessaires devront le faire.

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
1	**Forme juridique : loi**				
1.1	**Forme juridique** (guide, ch. 1) Aucune adaptation requise	Art. 4 ch. 1 P-Conv108 Art. 63 al. 1 Dir. 2016/680	Chaque canton doit lui-même veiller à disposer des réglementations nécessaires en matière de protection des données, car la Confédération, faute de disposition constitutionnelle correspondante, n'a pas de compétence législative en la matière pour le traitement des données par des organes cantonaux et	Loi sur la protection des données, loi sur l'information et la protection des données	… il existe une loi cantonale sur la protection des données (loi sur l'information et la protection des données, ou

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			communaux.		similaires), qui réponde à toutes les exigences matérielles selon ch. 2-8
2	**Champ d'application de la loi**				
2.1	**Champ d'application** (guide, ch. 2.1) (uniquement le traitement automatisé des données ?)	Art. 2 al. 1 AP-LPD Art. 3 P-Conv108 Art. 2 Dir. 2016/680 Plus aucune restriction dans P-Conv108	Cette réglementation légale doit s'appliquer à tous les traitements de données effectués par des organes cantonaux et communaux avec tout au plus les exceptions ci-après (→ ch. 2.2-2.5) : Il n'est pas permis de limiter le champ d'application au traitement automatisé de données personnelles.	*« régit tout traitement de données personnelles par (des organes) publics (cantonaux et communaux), indépendamment des moyens utilisés et des procédures appliquées »*	… le champ d'application est décrit et aucune exception plus étendue que celles indiquées aux ch. 2.2-2.5 n'est prévue
2.2	**Exceptions au champ d'application** (guide, ch. 2.2) Adaptation requise	Art. 33 al. 1 AP-LPD	Il est permis de déclarer applicables au traitement des données d'organes publics agissant en droit privé les règles de la loi fédérale sur la protection des données prévues pour le traitement privé de données. Ces organes cantonaux publics n'étant pas privés mais agissant uniquement *comme* des privés, l'autorité cantonale de surveillance est compétente, en analogie avec la réglementation fédérale (art. 23 al. 2 LPD et art. 32 al. 2 AP-LPD).	*« Lorsqu'un organe public est soumis à la concurrence économique et agit en droit privé, les données qu'il traite sont soumises aux règles correspondantes de la loi fédérale sur la protection des données ; la surveillance relève de la loi en question. »*	… l'exception n'est pas décrite de manière plus étendue
2.3	Plus pour les procédures civiles et procédures pénales (guide, ch. 2.3) Adaptation requise	Art. 2 al. 3 AP-LPD Pas d'exception à l'art. 3 P-Conv108 (et art. 12bis ch. 9 C108 [09.16] : incompétence de l'autorité de surveillance pour les procédures judiciaires) Pas d'exception à l'art. 2 Dir. 2016/680	Changement par rapport au contexte actuel : il n'est plus permis de prévoir des exceptions générales au champ d'application dans le cadre de procédures pendantes civiles ou pénales. Cela ne signifie pas que les procédures ne s'appliquent plus : elles gardent leur validité en tant que législations sectorielles pour la protection des données, à l'instar d'autres lois comme la loi sur la police, la loi sur l'école ou la loi fédérale sur la partie générale du droit des assurances sociales (BEAT RUDIN, *Überholte Ausnahmen beim Geltungsbereich*, digma 2016, 122 ss). Autrement dit : les règles (p. ex. le code de procédure pénale), tout comme les principes de la loi sur la protection (de l'information et) des données (p. ex. les règles applicables aux autorités responsables, à la sécurité de l'information, etc.) continuent de s'appliquer. Il reste néanmoins deux domaines à réglementer : - afin d'éviter tout conflit entre les *droits à l'information relevant de la procédure et ceux relevant de la protection des données* des parties/personnes concernées, il devrait être prévu que les droits et les prétentions des personnes concernées dans le cadre de procédures pendantes civiles ou pénales soient régis exclusivement par le droit de procédure applicable. - par ailleurs, il devrait (et pourrait) être prévu que les travaux	*« Les droits et prétentions des personnes concernées dans le cadre de procédures pendantes civiles ou pénales (...) sont régis exclusivement par le droit de procédure applicable ».*	… l'exception n'est pas décrite de manière plus étendue

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			de traitement des procédures judiciaires pendantes échappent à la *surveillance* du préposé à la protection des données (→ ch. 8.2). La formulation « procédure de droit pénal » ne fait pas référence à la seule procédure devant le tribunal pénal ; elle débute par l'ouverture d'une enquête pénale par l'enquête du ministère public. La solution retenue par la Confédération dans le projet mis en consultation n'est pas conforme à la convention, dans la mesure où elle restreint le champ d'application de la LPD pour les procédures judiciaires pendantes. (→ ch. 8.2)		
2.4	Plus pour les procédures de juridiction constitutionnelle ou administrative (guide, ch. 2.4) Adaptation requise	Art. 2 al. 3 AP-LPD Pas d'exception à l'art. 3 P-Conv108 (et art. 12bis ch. 9 C108 [09.16] : incompétence de l'autorité de surveillance pour les procédures judiciaires) Pas d'exception à l'art. 2 Dir. 2016/680	Il en va de même (→ ch. 2.3) des procédures pendantes de juridiction administrative ou (si elles sont prévues dans le canton) constitutionnelle	*« Les droits et prétentions des personnes concernées dans le cadre de procédures pendantes (…) de droit public et de droit administratif (…) sont régis exclusivement par le droit de procédure applicable ».*	… l'exception n'est pas décrite de manière plus étendue
2.5	Traitement de données personnelles (guide ch. 2.5) Nécessité d'adaptation à vérifier	Art. 2 al. 2 let. a AP-LPD Art. 3 ch. 1bis P-Conv108 Pas d'exception dans la Dir. 2016/680	Prévoir une exception pour le traitement de données pour un usage personnel pose problème (l'exception prévue dans l'AP-LPD concernant les traitements de données pour un usage exclusivement domestique n'est pas pertinente pour les organes publics). Il ne saurait y avoir de « dossier caché ». Seuls les enregistrements compris comme des aide-mémoire sont autorisés ; cependant, ils ne devraient pas être exclus du champ d'application. On pourrait tout au plus envisager une exception pour les notes à caractère personnel comprises comme des aide-mémoire ; elles seraient exclues du droit d'accéder à ses propres données personnelles.	*Pas d'exception générale concernant le champ d'application. Tout au plus une exception précisément définie pour le droit d'accéder à ses propres données personnelles (Droit d'accès → ch. 5.4-5.6)*	… aucune exception n'est précisée dans le champ d'application pour les « outils de travail personnels » (« données personnelles pour un usage personnel »)
3	**Définitions**				
3.1	**Définitions** (guide ---)	Art. 3 AP-LPD Art. 2 P-Conv108 Art. 3 Dir. 2016/680	On retiendra les modifications ci-après :		

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
3.2	**Données personnelles** (guide ---) Nécessité d'adaptation à vérifier	Art. 3 let. a et b AP-LPD (« personne concernée ») Art. 2 let. a P-Conv108 Art. 3 ch. 1 Dir. 2016/680	Contrairement aux directives internationales (et à la plupart des États européens), les lois suisses sur la protection des données ne protègent pas uniquement les personnes physiques, mais aussi les personnes morales. Le Conseil fédéral a annoncé vouloir renoncer à cette spécificité dans le cadre de la révision LPD : les cantons ne sont pas tenus de procéder à cette adaptation, mais il serait préférable de le faire. Il suffit pour cela de retirer les personnes morales de la définition des « données personnelles ». Il faudra peut-être aussi adapter le but de la loi à supposer que les personnes morales y figurent ou y soient mentionnées (p. ex. en précisant que les droits fondamentaux des personnes [physiques et morales] dont les organes publics traitent les données [informations] doivent être protégés.	*Définitions :* *On entend par données personnelles :* *« - des informations sur des personnes physiques identifiées ou identifiables »* *But de l'article :* *La présente loi vise à protéger « les droits fondamentaux de personnes physiques dont les organes publics traitent les données personnelles. »*	... s'il ressort clairement de la définition (et, le cas échéant, du but) que la protection est réservée aux personnes physiques (si les personnes morales sont exclues, comme dans la loi fédérale)
3.3	**Données sensibles** Adaptation requise	Art. 3 let. c AP-LPD Art. 6 P-Conv108 Art. 3 en lien avec art. 10 Dir. 2016/680	Les données sensibles sont depuis toujours des informations sur la « race » ou « l'origine raciale ». Dans le cas des êtres humains, la race n'est pas une expression scientifique ; il faut protéger la personne contre toute discrimination due à sa race (exemples du passé : « juif », « nègre »). Les lois plus modernes parlent donc de « données sur l'ethnie » ou de « données sur l'origine ethnique ». On entend par là l'appartenance à un groupe d'individus qui se sentent liés entre eux par leur culture, leur histoire, leur langue, leurs us, leurs coutumes, leurs traditions, et qui se considèrent comme une communauté distincte du reste de la population et/ou sont considérés comme tels par le reste de la population. En plus de la race, la C108 mentionne l'ethnie comme critère à retenir dans la définition des données sensibles. Il est recommandé de remplacer « race » par « ethnie ».	*On entend par données sensibles :* *« - des données sur (la santé, le patrimoine génétique, la vie privée ou) l'origine ethnique »*	... la définition donnée dans la loi utilise le critère « ethnie » (origine ethnique, appartenance ethnique) (et si le critère « race » n'y figure, si possible, plus)
3.4	**Données sur la vie sexuelle ou sur l'orientation sexuelle** (guide ---) Nécessité d'adaptation à vérifier	Art. 3 let. ch. 2 AP-LPD Art. 6 al. 1 P-Conv108 Art. 10 Dir. 2016/680	Les données sur la vie sexuelle ou sur l'orientation sexuelle entrent désormais dans la catégorie des données sensibles. Si la « sphère intime » ou « la vie privée » figurent déjà dans la définition ou s'il n'y a pas d'énumération exhaustive des données sensibles (ajout p. ex. de « en particulier »), on peut se passer d'adapter la loi, en s'assurant cependant que les données sur la vie sexuelle ou sur l'orientation sexuelle font bien partie des données sensibles.	*On entend par données sensibles :* *« - des données sur la sphère intime » ou* *« - des données sur la vie sexuelle ou sur l'orientation sexuelle »*	... la définition figure dans la loi ou est sans la moindre ambiguïté (définition non détaillée des données sensibles)
3.5	**Données génétiques** (guide ---) Nécessité d'adaptation à	Art. 3 let. c ch. 3 AP-LPD Art. 6 ch. 1 P-Conv108 Art. 3 ch. 12 en lien avec art. 10 Dir. 2016/680	« Les données génétiques » entrent désormais dans la catégorie des données sensibles. Si le patrimoine génétique, p. ex., figure déjà dans la définition ou s'il n'y a pas d'énumération exhaustive des données sensibles (ajout p. ex. de « en particulier »), on peut se passer d'adapter la loi, en s'assurant cependant que les données génétiques font bien	*On entend par données sensibles :* *« - des données génétiques »*	... la définition figure dans la loi ou est sans la moindre ambiguïté (définition non détaillée des données sensibles)

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	vérifier		partie des données sensibles.		
3.6	**Données biométriques** (guide ---) Adaptation requise	Art. 3 let. c ch. 4 AP-LPD Art. 6 ch. 1 P-Conv108 Art. 3 ch. 13 en lien avec art. 10 Dir. 2016/680	Les données biométriques, c'est-à-dire les données à caractère personnel *résultant d'un traitement technique spécifique* relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique (images faciales, données relatives à un visage obtenues par un programme de reconnaissance faciale (pas n'importe quelle photo !), données dactyloscopiques, empreintes vocales, iris), entrent désormais dans la catégorie des données sensibles.	*On entend par données sensibles :* *« - des données à caractère personnel résultant d'un traitement technique spécifique relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique (données biométriques) »*	... la définition figure dans la loi
3.7	**Traitement** (guide ---) Nécessité d'adaptation à vérifier	Art. 3 let. d AP-LPD Art. 2 let. b P-Conv108 Art. 3 ch. 2 Dir. 2016/680	La définition du traitement de données est nettement plus précise. Dans le projet mis en consultation par la Confédération, mais aussi dans la Dir. 2016/680, « effacement » et « destruction » sont utilisés ensembe, sans explication sur le lien qui les unit. « Destruction » a un sens physique. Quant à savoir si « effacer » signifie « faire disparaître du processus actif » (comme on radie les inscriptions au casier judiciaire) ou simplement supprimer de l'environnement électronique, il appartient au canton de le dire. On ignore si le projet de loi final du Conseil fédéral contiendra une explication à ce sujet.	*« Traitement de données : toute opération ou ensemble d'opérations, indépendamment du procédé utilisé, effectuées sur des données personnelles, telles que la collecte, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données »*	... la définition, plus précise, figure dans la loi ou est sans la moindre ambiguïté et implique toutes les nouvelles formes de traitement mentionnées.
3.8	**Profilage** (guide ---) Adaptation requise	Art. 3 let. f AP-LPD Art. 3 ch. 4 Dir. 2016/680	La directive UE juge le profilage comme un nouveau mode de *traitement* (considéré comme particulièrement « dangereux »). Il exige le respect des mêmes conditions que celles appliquées au traitement des données personnelles particulièrement dignes de protection (en d'autres termes, une base légale est nécessaire en règle générale). Les lois cantonales doivent en tenir compte. « Profilage » doit être repris dans les définitions afin de faciliter la formulation et la compréhension. Le « profil de la personnalité », qui revient souvent dans les lois cantonales et qui peut être assimilé aux données sensibles, peut être supprimé ou conservé. En résumé : - il faut ajouter le terme « profilage », en tant que mode de traitement, - on peut supprimer *le terme* « profil de la personnalité » (= catégorie de données personnelles), comme à la Confédération, ou le conserver ; il est tout à fait possible de conserver la définition « assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique », élément de la définition des données sensibles, sans utiliser « profil de la personnalité » ; - les principes du traitement de données doivent être modifiés (→ ch. 4.2) et	*Ajout d'un nouveau terme :* *« profilage : tout traitement automatisé de données, personnelles ou non, consistant à analyser ou à prédire les caractéristiques personnelles essentielles d'une personne, notamment son rendement au travail, sa situation économique, sa santé, sa sphère intime ou ses déplacements »*	... la définition du profilage figure dans la loi

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			- ces modifications apparaissent aussi dans les législations sectorielles.		
3.9	**Organe public responsable du traitement** (guide ---) Nécessité d'adaptation à vérifier	Art. 3 let. h AP-LPD Art. 2 let. d P-Conv108 (« controller ») Art. 3 ch. 8 Dir. 2016/680	Le droit supérieur définit ce qu'on entend par « personne responsable du traitement ». Cette définition peut être reprise *ou* précisée dans la réglementation de la responsabilité. On utilisera à l'échelon cantonal l'expression « *organe public responsable du traitement* » (autorité, etc.), le traitement par des privés n'étant pas réglementé.	*« organe public responsable du traitement : organe public qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données, de même que son étendue, ou mise en œuvre directe (→ ch. 4.9)*	... la définition est reprise ou l'expression figure déjà dans les règles applicables à la responsabilité (→ ch. 4.9)
3.10	**Sous-traitant** (guide ---) Nécessité d'adaptation à vérifier	Art. 3 let. i AP-LPD Art. 2 let. f P-Conv108 Art. 3 ch. 9 Dir. 2016/680	Le droit supérieur définit ce que l'on entend par « sous-traitant». Cette définition peut être reprise *ou* précisée dans la réglementation de la responsabilité.	*« sous-traitant : personne privée ou autorité publique qui traite des données pour le compte du responsable du traitement » ou mise en œuvre directe (→ ch. 4.12)*	... la définition est reprise ou l'expression figure déjà dans les règles applicables à la responsabilité (→ ch. 4.12)
4	**Principes relatifs au traitement des données**				
4.1	**Légalité** (guide ch. 3.1) Aucune adaptation requise	Art. 4 al. 1 AP-LPD Art. 5 ch. 3 P-Conv108 Art. 4 al. 1 let. a et art. 8 Dir. 2016/680	Le traitement de données personnelles doit être licite. Pour le traitement administratif de données, cela signifie en particulier que des données ne peuvent être traitées que moyennant une base légale. Une telle base légale peut ressortir d'une obligation expresse, d'une habilitation à traiter d'une certaine manière des données ou d'une tâche légale dont l'exécution exige un traitement particulier de données. Au regard de la législation publique sur la protection des données (principe de la légalité ci-dessous), on peut se demander s'il suffit qu'une personne donne son *consentement* à une autorité pour que celle-ci procède au traitement des données qui la concernent. Comment justifier, par exemple, que les services d'aide sociale soient habilités à traiter les données d'un demandeur moyennant uniquement le consentement de ce dernier ? Les contraintes devaient être de toute évidence plus poussées que celles relevant d'une simple base légale indirecte (p. ex. se procurer des données de l'administration fiscale afin de vérifier les indications que le demandeur a fournies sur sa situation personnelle). Le consentement peut, le cas échéant, permettre de libérer du secret professionnel ou du secret de la fonction la personne ou le service devant communiquer des données aux services de l'aide sociale (il peut s'agir, p. ex., d'un médecin devant évaluer une capacité à travailler), ou de procéder à une pesée des intérêts. Par ailleurs, le consentement est le moyen de justifier la com-	*Pour le **traitement** de données :* *p. ex. « licite », « conforme à la loi », « s'il existe pour cela une base légale (expresse) » (dans le sens de base légale directe)* *« ou si l'exécution d'une tâche légale l'exige » (dans le sens de base légale indirecte)* *Pour la **communication** de données :* *p. ex. « communique des données personnelles si une disposition légale l'exige ou l'autorise » (dans le sens de base légale directe) « ou si cela est nécessaire à l'exécution d'une tâche légale » (dans le sens d'une base légale indirecte) « ou si, dans le cas d'espèce, la personne concernée a donné son consentement explicite ou, si elle n'est pas en mesure de le faire, la communication des données est dans son intérêt et le consentement est supposé de bonne foi. »*	… … l'exigence de la légalité (conformité à la loi) est inscrite dans la loi

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			munication de données. En ce qui concerne les exigences spécifiques au traitement des données sensibles et au profilage, se reporter → ch. 4.2		
4.2	**Conditions qualifiées au traitement des données personnelles sensibles et au profilage** (guide ch. 3.7) Adaptation requise (profilage)	Art. 27 al. 2 et art. 29 al. 1 AP-LPD Art. 6 ch. 1 P-Conv108 Art. 10 Dir. 2016/680	Le traitement de données personnelles qui concernent de près la personnalité et qui présentent un fort potentiel de stigmatisation et de discrimination (données dites sensibles, dignes de protection) exige une protection qualifiée. L'usage veut que l'on exige une base légale formelle ou que l'on pose des exigences plus élevées à la nécessité d'exécuter une tâche (« nécessité absolue », « nécessité impérative », « indispensable »). Si, dans un cas d'espèce, le consentement de la personne concernée doit servir de base de justification, il doit alors s'agir d'un *informed consent* (accord donné en connaissance de cause, librement et sans menace [expresse ou dissimulée] de subir des torts en cas de refus). À noter par ailleurs que la définition « profil de la personnalité » peut être supprimée, mais que la question du **profilage** doit être réglée ici. (→ ch. 3.8)	*Pour le **traitement** de données :* *« Il ne peut y avoir traitement de données personnelles sensibles ou réalisation d'un profilage que si l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument (dans le sens de base légale directe) ou si cela est indispensable pour l'exécution d'une tâche clairement spécifiée dans une loi au sens formel (dans le sens de base légale indirecte).* *Pour la **communication** de données :* *« ne communique des données personnelles sensibles ou les résultats d'un profilage que si une loi l'exige ou l'autorise expressément » (*dans le sens de base légale directe*), « si cela est absolument indispensable à l'exécution d'une tâche clairement spécifiée par une loi » (*dans le sens de base légale indirecte*) « ou si, dans le cas d'espèce, la personne concernée a donné son consentement explicite ou, si elle n'est pas en mesure de le faire,* la communication des données est dans son intérêt et le consentement est supposé de bonne foi *»).*	… le traitement de données personnelles sensibles et le profilage sont liés à des conditions qualifiées
4.3	**Bonne foi** (guide ch. 3.2) Aucune adaptation requise	Art. 4 al. 2 AP-LPD Art. 5 ch. 4 let. a P-Conv108 Art. 4 al. 1 let. a Dir. 2016/680	Le traitement de données personnelles doit être effectué dans le respect du principe de la bonne foi. Il découle de ce principe notamment l'interdiction de collecte de données secrètes (identification ou collecte de données). Le principe perd donc de sa signification en raison du devoir d'information auquel sont tenus les organes publics responsables du traitement des données (→ch. 5.2).	*« doit respecter le principe de la bonne foi »*	… l'exigence du traitement respectueux du principe de la bonne foi est inscrite dans la loi ou elle découle clairement des principes constitutionnels
4.4	**Finalité** (guide ch. 3.3) Aucune adaptation requise	Art. 4 al. 3 AP-LPD Art. 5 ch. 4 let. b P-Conv108 Art. 4 al. 1 let. b Dir. 2016/680	La finalité (ou l'interdiction de changer la finalité) est un élément-clé du droit de la protection des données. Des données personnelles ne peuvent être traitées que dans le but qui est indiqué lors de la collecte, qui ressort manifestement des circonstances ou qui est prévu par la loi, alors que la définition de la finalité par la loi reste prioritaire dans le domaine du droit public.	*« Le traitement de données personnelles doit correspondre au but qui est indiqué lors de la collecte, pour autant qu'une autre base légale ne prévoie expressément une autre finalité ou que la personne concernée ait donné son consentement dans le cas d'espèce. » ou « Le traitement de données personnelles ne doit avoir lieu que pour des finalités déterminées (expli-*	… l'exigence de la finalité est inscrite dans la loi

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
				cites) et licites »,	
4.5	**Proportionnalité** (guide ch. 3.4) Aucune adaptation requise	Art. 4 al. 2 AP-LPD Art. 5 ch. 1 et art. 5 ch. 4 let. c P-Conv108 Art. 4 al. 1 let. c Dir. 2016/680	Le traitement de données personnelles doit être proportionnel, à l'instar de tout acte administratif. Les données traitées doivent être adéquates eu égard aux finalités recherchées ; le traitement de données doit constituer la mesure la plus clémente permettant d'atteindre le but recherché, et la finalité (tâche) ainsi que l'ingérence dans l'auto-détermination informationnelle (traitement de données) doivent se tenir réciproquement dans un rapport adéquat (proportionnalité dans une affaire). Pour la dimension temporelle de la proportionnalité → ch. 4.6. Pour les contraintes qualifiées relatives à la proportionnalité lors du traitement de données personnelles sensibles et au profilage → ch. 4.2.	*« doivent être adéquates et pertinentes eu égard aux finalités pour lesquelles elles sont traitées (...) », « peuvent être traitées pour autant (et aussi longtemps) qu'elles sont adéquates et pertinentes eu égard aux finalités recherchées », « peuvent être traitées pour autant qu'elles sont adéquates et pertinentes par rapport au but recherché (…) »*	… l'exigence de la finalité est inscrite dans la loi
4.6	**(délai)** (guide ch. 3.4) Nécessité d'adaptation à vérifier	Art. 4 al. 4 AP-LPD Art. 5 Dir. 2016/680	La proportionnalité prévoyait déjà que le traitement des données personnelles doit être limité dans le temps. Désormais, l'effacement (ou l'anonymisation) des données personnelles, ou la vérification régulière de la nécessité de conserver ces données pour l'exécution d'une tâche sont soumis à des délais et des règles procédurales doivent garantir que ces délais sont respectés. Il faut donc prévoir au moins une directive relative à l'effacement (ou à res à l'exécution d'une tâche, à supposer qu'elles ne soient pas soumises à la législation sur l'archivage. L'obligation de proposer des données selon la loi sur l'archivage en vigueur ne peut suffire ; on peut en revanche envisager un délai par défaut si aucun délai de conservation, de vérification ou d'effacement n'est prévu dans la législation sectorielle. Les modalités de mise en œuvre peuvent être définies dans le droit d'application ou réglées dans un SGPD (→ ch. 4.10). Utilisation des termes « destruction » et « effacement » → ch. 3.7.	*« doivent être adéquates et pertinentes eu égard aux finalités pour lesquelles elles sont traitées et ne peuvent être conservées plus longtemps que les finalités ne l'exigent », « peuvent être traitées pour autant et aussi longtemps qu'elles sont adéquates et pertinentes eu égard aux finalités recherchées », « peuvent être traitées pour autant qu'elles sont adéquates et pertinentes par rapport au but recherché, et doivent être détruites (rendues anonymes) dès qu'elles ne sont plus nécessaires à l'exécution de la tâche ». Disposition distincte : « les données personnelles qui ne sont plus nécessaires, qui sont considérées sans valeur archivistique par l'organe en charge de l'archivage, doivent être détruites (ou rendues anonymes) par l'organe public », en précisant dans la législation sectorielle un délai par défaut pour la proposition de données aux archives.*	… l'exigence d'un délai de conservation pour le traitement de données est considérée par le droit cantonal comme un aspect relevant de la proportionnalité (loi sur la protection des données et/ou législation sectorielle)
4.7	**Exactitude** (guide ch. 3.5) Aucune adaptation requise	Art. 4 al. 5 AP-LPD Art. 5 ch. 4 let. d P-Conv108 Art. 4 al. 1 let. d Dir. 2016/680	Les données personnelles traitées par des organes publics doivent être exactes ; premièrement parce que le droit à l'auto-détermination informationnelle l'exige et deuxièmement parce que le traitement de données inexactes pour l'exécution de tâches administratives ne saurait être proportionnel. Par conséquent, l'exigence de l'exactitude doit être ancrée dans la loi, soit à titre de principe d'exactitude, soit comme un devoir du maître de fichier de s'assurer de l'exactitude des données, soit	*« L'organe public responsable est tenu de s'assurer de l'exactitude des données personnelles traitées. Il prend toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. »*	… l'exigence de l'exactitude est inscrite dans la loi dans l'une des formes mentionnées

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			au minimum comme un droit de rectification pour la personne concernée. Il ne suffit plus d'en rester au seul droit de rectification accordé à la personne concernée. L'exhaustivité des données est un aspect de l'exactitude. Elle ne doit être critiquée que si le fait que les données ne sont pas complètes a conduit à une inexactitude. Elle ne doit donc pas figurer expressément dans la loi.		
4.8	**Sécurité de l'information** (guide ch. 3.6) Adaptation envisageable	Art. 11 AP-LPD Art. 7 P-Conv108 Art. 4 al. 1 let. f et art. 29 Dir. 2016/680	Les données personnelles doivent être protégées par des mesures techniques et organisationnelles contre tout traitement non autorisé (la destruction accidentelle ou non autorisée, la perte accidentelle ainsi que l'accès, la modification et la diffusion non autorisés). On devrait préférer la notion de sécurité de l'information à celle de sécurité des données.	*« doivent être protégées par des mesures techniques et organisationnelles adéquates contre tout traitement non autorisé », « veille à les protéger contre la perte, le vol, le traitement et l'accès non autorisés », à cela s'ajoutent des réglementations au niveau, p. ex., de l'ordonnance (ordonnance sur la sécurité de l'information).*	… l'exigence de la sécurité de l'information est inscrite dans la loi
4.9	**Responsabilité** (guide ---) Adaptation envisageable	Art. 26 AP-LPD Art. 8 ch. 1bis P-Conv108 Art. 19 et 21 Dir. 2016/680	Les nouvelles bases légales insistent sur la nécessité d'attribuer clairement la responsabilité du traitement des données. Ceci en particulier lorsque les données sont traitées conjointement par plusieurs organes ; les responsabilités doivent être dans ce cas réglées de manière transparente (un point de contact unique, p. ex., pour les personnes concernées).	*«^{x} L'organe public qui traite des données personnelles (informations) pour s'acquitter de ses tâches légales est responsable du traitement desdites données (à des fins d'information).* *^{x} Si plusieurs organes publics traitent conjointement des informations communes, ils s'engagent à en régler la responsabilité.»*	... l'attribution de la responsabilité (en cas, notamment, de traitement conjoint des données) est inscrite dans la loi
4.10	**Preuve du respect des dispositions PD** (guide ---) Adaptation requise	Art. 10 AP-LPD Art. 19 let. a AP-LPD (insuffisant car la *compliance* selon C108 et Dir. n'y figure pas) Art. 8bis ch. 1 P-Conv108 Art. 4 al. 4 Dir. 2016/680	Les nouvelles dispositions légales exigent que l'organe public responsable ou le sous-traitant en charge du traitement des données doivent être en mesure de respecter les dispositions relatives à la protection des données. La preuve peut être fournie par un système de gestion de la protection des données (SGPD). Les SGPD reposent sur les normes ISO relatives à la gestion de la qualité (ISO 9001) et à la sécurité de l'information (ISO 27001, etc.). S'il est renoncé à cette certification, il convient de préciser quels documents sont requis pour fournir ladite preuve (il peut s'agir d'un concept de sécurité de l'information, d'un concept d'accès, etc.). Il y a suffisamment d'instruments. Il apparaît plus judicieux de définir par ordonnance dans quels cas un SGPD est obligatoire (p. ex. lorsque le traitement porte sur des données sensibles).	*Alinéa additionnel :* *«^{x} L'organe public responsable du traitement doit être en mesure de prouver qu'il respecte les dispositions relatives à la protection des données. Le Conseil d'État en spécifie les détails dans l'ordonnance afférente.»*	... si l'obligation de prouver le respect des dispositions en la matière est inscrite dans la loi
4.11	**Conseiller à la protection des données**	Art. 32-34 Dir. 2016/680	Seule la directive relative à la protection des données traitées dans le cadre de la coopération policière et judiciaire prévoit la fonction de conseiller. Il n'est pas nécessaire d'inscrire cette obligation dans la loi sur la protection des données – on le fera éventuellement en droit cantonal sur la police.	*À inscrire éventuellement dans les législations sectorielles*	

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	(guide ---) Adaptation requise dans les législations sectorielles				
4.12	**Sous-traitance** (guide ---) Adaptation requise	Art. 7 AP-LPD Art. 22 s. Dir. 2016/680	La nouvelle directive précise les conditions de sous-traitance des données par des tiers. Il ne sera fait appel qu'à des sous-traitants qui présentent des *garanties suffisantes* quant à la mise en œuvre de mesures techniques et organisationnelles, de manière que le traitement réponde aux exigences du droit et garantisse la protection des droits de la personne concernée. Le sous-traitant ne recrutera pas un autre sous-traitant sans *l'autorisation écrite préalable* de l'organe public mandataire. Le traitement par un sous-traitant est régi par un *contrat* ou un autre acte juridique, qui lie le sous-traitant au responsable du traitement (loi, ordonnance, arrêté du Conseil d'État, etc.). L'acte juridique définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données personnelles et les catégories de personnes concernées et les obligations et les droits du sous-traitant et de l'organe public mandataire. Il s'agit notamment de garantir - que le sous-traitant n'agit que sur instruction de l'organe public mandataire, - que les personnes autorisées à traiter les données s'engagent à respecter la confidentialité ou soient soumises à une obligation légale de confidentialité, - que les droits des personnes concernées soient pleinement respectés, - qu'au terme du contrat les données personnelles soient supprimées, une fois la sélection opérée par l'organe public mandataire, ou renvoyées à l'organe, - que le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable de l'organe public mandataire.	*« L'organe public peut faire appel à des tiers pour traiter des données personnelles :* *- si aucune disposition juridique ou arrangement contractuel ne s'y oppose ou que* *- s'il garantit que seuls les traitements que l'organe public serait en droit de faire lui-même sont effectués.* *L'organe fait en sorte que le traitement des informations soit conforme à cette loi.* *Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable de l'organe public mandataire. »* *Les différentes conditions applicables au recrutement de tiers et à la garantie que seuls les traitements de données personnelles que l'organe public serait en droit de faire lui-même seront effectués peuvent être réglées en détail au niveau de l'ordonnance (voir « Commentaire »).*	... la loi précise les conditions s'appliquant à la sous-traitance, à la garantie que seuls les traitements que l'organe public seraient en droit de faire lui-même sont effectués, à l'interdiction de recruter un autre sous-traitant sans l'autorisation écrite préalable de l'organe public mandataire
5	**Droits des personnes concernées**				
5.1	**Transparence du traitement** (guide ch. 4.1) Nécessité d'adaptation à vérifier	Art. 13, 20 et 36 AP-LPD Art. 5 ch. 4 let. A P-Conv108 Art. 13 ss. Dir. 2016/680 Art. 24 Dir. 2016/680	La transparence dans le traitement des données personnelles est l'un des principaux objectifs de la législation sur la protection des données. Seront établis en vertu du principe de transparence : - l'obligation des organes publics de tenir et de rendre accessible un registre (dans le domaine de la justice et de la police) des « activités de traitement » (des procédures de traitement des données personnelles) (→ ch. 6.7) ;		… le principe de transparence est détaillé dans la loi (ch. 5.2-5.6)

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			- l'obligation des organes publics d'informer les personnes concernées sur la collecte de données personnelles (→ ch. 5.2-5.3); - le droit pour toute personne de se faire communiquer, le cas échéant, les données traitées par un organe public (droit d'accès à ses données personnelles) (droit à l'information) (→ ch. 5.4-5.6).		
5.2	**Devoir d'informer** (guide ---) Adaptation requise	Art. 13 AP-LPD Art. 7bis P-Conv108 Art. 13 Dir. 2016/680	Est exigée une information (active) sur la collecte de données personnelles – *ne concerne plus seulement le traitement de données sensibles.* Information sur : - organe public responsable (coordonnées incluses) ; - base légale du traitement des données ; - finalités du traitement des données ; - teneur et catégories des données ; - destinataires des données ou catégories de destinataires (si les données sont communiquées à des tiers) ; - droits de la personne concernée. Si les données font l'objet d'un relevé systématique (formulaire d'inscription ou de demande, sur papier ou en ligne), il serait judicieux de les indiquer directement dans le formulaire. Pour tout autre collecte de données, la personne concernée sera informée individuellement, excepté si, et seulement si, une limitation est admise (→ immédiatement ci-après ch. 5.3).	*Devoir d'informer lors de la collecte de données* *L'organe public responsable informe la personne concernée chaque fois que des données sont collectées ; ce devoir d'information s'applique aussi lorsque les données sont collectées auprès de tiers.* *Éléments que doit contenir l'information :* - *organe public responsable (coordonnées incluses) ;* - *teneur et catégories des données ;* - *base légale et finalité du traitement ;* - *destinataires des données ou catégories de destinataires (si les données sont communiquées à des tiers) et* - *droits de la personne concernée.*	... le devoir d'informer (teneur minimale) est inscrit dans la loi
5.3	**Exceptions au devoir d'informer** (guide ---) Adaptation requise	Art. 14 AP-LPD Art. 7bis ch. 1bis P-Conv108	L'obligation d'informer ne s'applique pas, - lorsque la personne concernée dispose déjà des informations (en particulier si elle a déjà été informée à un stade antérieur de la collecte) ; - lorsque l'enregistrement ou la communication sont expressément prévus par la loi (donc lorsque la base légale apporte suffisamment de précisions sur les finalités de la collecte de données concernant ces personnes) ; ou - lorsque le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés. En outre, la communication des informations peut être restreinte (en tout ou partie, ou différée), pour les mêmes motifs que ceux prévus pour l'accès à ses propres données personnelles (droit d'accès) (→ ch. 5.6). Dès que le motif de la restriction n'a plus lieu d'être, l'information est communiquée.	L'obligation d'informer ne s'applique pas, lorsque - *lorsque la personne concernée dispose déjà des informations au sens de § ■■ [→ ch. 5.2],* - *lorsque le traitement des données personnelles est expressément prévu par la loi ou* - *lorsque le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés.* *La communication des informations peut être restreinte pour les mêmes motifs que ceux prévus pour l'accès à ses propres données personnelles.*	... les exceptions au devoir d'informer ne sont pas précisées dans la loi.
5.4	**Droit de chacun de savoir si et, le cas échéant, quelles données le concernant sont traitées (droit d'accès)**	Art. 20 AP-LPD Art. 8 ch. 1 let. b C 108 (09.16) Art. 14 Dir. 2016/680 Art. 12 Dir. 2016/680 pour les modalités	Le droit de toute personne de savoir si et, le cas échéant, quelles données la concernant sont traitées par un organe public – que l'organe public traite lui-même ou fasse traiter les données – est un élément-clé du droit de la protection des données. De ce droit découlent les autres droits et prétentions de la personne concernée. Il faut régler, outre le droit, certaines modalités (dépôt d'une requête par la personne concer-	*« Toute personne a le droit de savoir si des données la concernant sont traitées par un organe public, et, le cas échéant, avoir accès à ces données.* *Sont communiqués :* - *les éléments énumérés au § ■■ [→ ch. 5.2],*	… le droit d'être informé (accès à ses propres données personnelles) est inscrit dans la loi

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	(guide ch. 4.2) Nécessité d'adaptation à vérifier		née, forme de la diffusion des informations). Il est permis, pour simplifier la procédure, de prévoir un accès direct aux données pertinentes sur demande de la personne concernée. Les données communiquées comprennent les éléments énumérés au chapitre Devoir d'informer (→ cf. 5.2) et des informations : - sur la durée de conservation des données personnelles et - sur l'origine des données. Il pourra être précisé au niveau de l'ordonnance comment on compte accorder l'accès aux données personnelles (en règle générale par écrit, ou garantie de consultation avec l'accord du demandeur, ou par oral).	- *des informations sur la durée de conservation des données personnelles et* - *des informations sur l'origine des données personnelles. »*	
5.5	(**Coûts**) (guide ch. 4.3) Nécessité d'adaptation à vérifier	Art. 20 al.1 AP-LPD Art. 8 ch. 1 let. b P-Conv108 Art. 12 al. 4 Dir. 2016/680	Le droit d'être renseigné (et de consulter) est l'un des droits les plus importants découlant du droit constitutionnel de la protection de la personnalité. Les renseignements (l'accès à ses propres données personnelles) sont fournis, par principe, gratuitement. Une exception est admise lorsque la demande a un caractère excessif.	« Les renseignements sont fournis gratuitement. » *(avec év. une exception si la demande a un caractère excessif, ou si une nouvelle demande est déposée dans un court intervalle de temps [p. ex. une année] sans qu'il y ait un intérêt particulier ; un intérêt légitime est établi, lorsque les données de la personne concernée ont été modifiées à son insu).*	… si la loi prévoit que les renseignements sont fournis gratuitement (avec év. des exceptions si la demande a un caractère excessif)
5.6	**Exceptions au droit d'accès** (guide ch. 4.4) Aucune adaptation requise	Art. 21 AP-LPD Art. 9 P-Conv108 Art. 15 Dir. 2016/680	La communication des renseignements (garantie de consultation) ne peut être aisément restreinte (refusée, limitée ou différée). Il faut préciser dans la loi que les renseignements peuvent être tout au plus restreints pour autant qu'une loi le prévoie ou que la restriction soit justifiée par la protection d'intérêts publics prépondérants (p. ex. pour ne pas compromettre une instruction pénale), d'intérêts privés prépondérants de tiers (p. ex. pour protéger d'autres personnes concernées) ou de la personne concernée elle-même. Le dernier cas d'application (protection de la personne concernée) ne justifie pas l'obligation de confidentialité ; il faut en tout cas prévoir des procédures particulières qui permettent de répondre au besoin de protection sans pour autant refuser la communication des renseignements (p. ex. communication par une personne de confiance de la personne qui le demande).	*« peut être restreinte, refusée, limitée ou différée pour autant que cela soit justifié par la protection d'intérêts publics prépondérants ou d'intérêts prépondérants de tiers. »*	… les restrictions au droit d'être informé (et d'avoir accès à ses données personnelles) sont clairement délimitées par la loi
5.7	**Droit à la rectification de données inexactes** (guide ch. 4.5) Nécessité d'adaptation à	Art. 34 al. 3 let. a AP-LPD Art. 8 ch. 1 let. e P-Conv108 Art. 16 Dir. 2016/680 Art. 12 Dir. 2016/680 pour les modalités	Les données personnelles traitées par des organes publics doivent être exactes (→ ch. 4.7). La personne concernée a le droit d'obtenir gratuitement et dans les meilleurs délais la rectification de données inexactes. Le droit à la rectification peut être éventuellement restreint *par une loi spéciale* et dans une *finalité particulière* (art.16 al. 4 Dir. 2016/680, protection de la sécurité publique, non-entrave	*« Toute personne concernée a le droit d'obtenir gratuitement et dans les meilleurs délais la rectification de données inexactes »*	… le droit de rectification de la personne concernée est prescrit dans la loi en conséquence (y c. la réglementation sur le fardeau de la preuve et la possibilité d'ajouter une mention du caractère

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	vérifier (gratuité !) (fardeau de la preuve) (guide ch. 4.5) Aucune adaptation requise (si l'exactitude ou l'inexactitude ne peuvent être déterminées) (guide ch. 4.5) Aucune adaptation requise	Art. 34 al. 2 AP-LPD Art. 16 al. 3 let. a Dir. 2016/680 (restriction si l'exactitude ou l'inexactitude ne peuvent être déterminées)	à à une instruction publique ou judiciaire, etc.; id. art. 9 P-Conv108). En principe, il revient à l'organe public d'apporter la preuve de l'exactitude des données, et non pas à la personne concernée de prouver leur inexactitude. On peut prévoir une exception pour le cas où la preuve peut raisonnablement et sans autre être exigée de la personne concernée. Dans certaines circonstances (p. ex. en présence de jugements de valeur ou de données transmises à l'organe public par un tiers), il n'est pas possible, de par la nature des données, de déterminer si elles sont exactes ou non (il ne s'agit pas ici de l'échec de la preuve par l'organe public, mais de l'impossibilité de la preuve en raison de la nature des données). Dans ce cas, l'organe public mentionne le caractère litigieux et restreint le traitement des données personnelles concernées. Une restriction pourrait consister à n'autoriser la transmission des données qu'assortie de la mention du caractère litigieux.	*« Si l'organe public conteste l'inexactitude, c'est à lui de prouver l'exactitude »* *« Si, en raison de leur nature, il ne peut être déterminé si les données personnelles sont exactes ou non, l'organe public doit mentionner le caractère litigieux des données et restreindre leur traitement »*	litigieux en présence de jugements valeur [cf. champs suivants]). … le fardeau de la preuve revient en premier lieu à l'organe public … la loi précise que, lorsque ni l'exactitude ni l'inexactitude des données personnelles ne peuvent être prouvées en raison de leur nature, l'organe public doit mentionner le caractère litigieux et restreindre le traitement des données personnelles
5.8	**Droit à la cessation, à l'élimination et à la constatation** (guide ch. 4.6) Adaptation requise (droit à l'effacement)	Art. 34 al. 1 AP-LPD Art. 8 P-Conv108 Art. 54 Dir. 2016/680 (droit à un recours juridictionnel)	Si des données sont traitées de manière illicite, la personne concernée peut faire valoir plusieurs droits : la cessation du traitement illicite des données (p. ex. par effacement, interdiction de communication), la réparation des conséquences d'un traitement illicite (p. ex. par effacement, communication aux destinataires des données, publication, dommages-intérêts, réparation du tort moral) et la constatation de l'illicéité d'un traitement. Il y aura examen de l'intérêt légitime, pour autant que la demande de rectification n'émane pas de la personne concernée mais d'un tiers (sans procuration de la personne concernée) ; cet intérêt est toujours présumé chez la personne concernée en raison des droits de la personnalité. Le droit de constatation peut éventuellement être subordonné à l'existence d'un intérêt légitime ; pour les autres droits, le risque d'un autre traitement ou le risque de transmission est un motif suffisant. La révision prévoit un nouvel élément ; le droit à l'effacement des données qu'une personne peut faire valoir si le traitement de ses données personnelles est illicite. Il peut être renoncé à l'effacement uniquement lorsque les données personnelles doivent être conservées à titre de preuve. Le devoir de documentation dans le cadre d'une intervention de l'État admet dans la plupart des cas de don-	*« Toute personne peut exiger de l'organe responsable* *- qu'il mette fin à tout traitement illicite de données personnelles,* *- qu'il supprime les effets d'un traitement illicite ;* *- que l'illicéité d'un traitement soit constatée.* *La personne peut demander notamment que les données la concernant soient effacées ou communiquées à des tiers. »*	… le droit de la personne concernée à la cessation d'un traitement illicite, à la réparation des conséquences d'un traitement illicite (droit à l'effacement y c.) et à la constatation de l'illicéité d'un traitement est inscrit dans la loi

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			nées rendues anonymes ; cf. arrêt du Tribunal administratif du canton de Berne du 15.4.2014 (100.2013.156U) ; SANDRA HUSI, *Widerrechtlich bearbeitete Daten ins Archiv?*, digma 2015, 24 ss. Pour certaines finalités (art. 16 Abs. 4 Dir. 2016/680, p. ex. protéger la sécurité publique, éviter de gêner des enquêtes officielles ou judiciaires ; idem art. 9 P-Conv108), on peut prévoir une restriction du droit à l'effacement dans une loi spéciale. Utilisation des termes « destruction » et « effacement » → ch. 3.7.		
5.9	**Droit à l'interdiction de communication** (guide ch. 4.7) Aucune adaptation requise	Art. 30 AP-LPD Art. 8 al.1 let. d C108	La personne concernée par le traitement administratif de données peut exiger de l'organe public responsable que la communication de certaines données personnelles (à des personnes privées) soit interdite (blocage). Ce droit doit être garanti sans condition, sauf s'il est rendu vraisemblable qu'il existe un intérêt légitime. La loi doit aussi préciser à quelles conditions l'interdiction de publication peut être levée (p. ex. lorsqu'une loi prescrit la communication ou que celle-ci est impérative pour l'accomplissement par l'organe responsable des tâches prévues par la loi ou pour la défense d'un droit).	*« la personne concernée (qui rend vraisemblable l'existence d'un intérêt légitime) peut exiger de l'organe responsable qu'il s'oppose à la communication de certaines données personnelles »,* *« Malgré l'opposition, la communication est licite* *- si l'organe public est tenu légalement de le faire* *- si la communication est impérative pour l'accomplissement des tâches prévues par la loi ou* *- si la personne qui demande la publication rend vraisemblable que les données sont nécessaires à la défense d'un droit. »*	… le droit de s'opposer à la communication est inscrit dans la loi, avec tout au plus trois exceptions
5.10	**« Plainte » auprès de l'autorité de surveillance en matière de protection des données** (guide ---) Adaptation requise	Art. 41 al. 5 AP-LPD (insuffisant) Art. 12bis ch. 3 P-Conv108 Art. 52 f. Dir. 2016/680 Art. 17 Dir. 2016/680	Sans préjudice de tout autre recours administratif ou juridictionnel, il faut prévoir que toute personne concernée a le « droit de se plaindre » auprès du délégué à la protection des données, si elle considère que le traitement de données à caractère personnel constitue une violation des dispositions de la loi sur la protection des données. Il devrait s'agir d'une « dénonciation à l'autorité de surveillance » de droit administratif. Le délégué à la protection des données est tenu de traiter la dénonciation et d'informer la personne de son issue dans un délai de trois mois. En cas d'incompétence de l'autorité de surveillance, la dénonciation sera transmise sans délai au délégué compétent. Si l'autorité de surveillance ne traite pas la dénonciation, la personne a le droit de former recours (également sous forme de dénonciation de droit administratif) contre l'autorité de surveillance en défaut (art. 53 al. 2 Dir. 2016/680). L'exercice des droits de la personne concernée par le délégué à la protection des données au sens de l'art. 17 Dir. 2016/680	*Prévoir la possibilité d'une dénonciation à l'autorité de surveillance en matière de protection des données – pour autant que cela ne soit pas prévu d'une façon générale par la législation sur la procédure administrative :* *(Le délégué à la protection des données)* *«- traite les plaintes concernant la violation des prescriptions légales en tant que dénonciation à l'autorité de surveillance relevant du droit administratif et informe la personne dans les trois mois de l'état d'avancement et de l'issue de sa plainte. »* Il s'agit en outre de prévoir les ressources nécessaires.	... la loi dispose que le délégué à la protection des données doit traiter les dénonciations (« plaintes ») des personnes concernées dans un délai raisonnable (trois mois au maximum) et qu'il doit prévoir les ressources nécessaires

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			(cf. cas prévus à l'art. 13 al. 3, l'art. 15 al. 3 et l'art. 16 al. 4 Dir. 2016/680) peut être précisée par domaine (comme le fait jusqu'ici la Confédération à l'art. 18 al. 3-5 LMSI).		
6	**Dispositions spéciales**				
6.1	**Décision individuelle automatisée** (guide ch. 5.1) Adaptation requise	Art. 15 et 20 al. 3 AP-LPD Art. 8 al. 1 let. a et al. 2 P-Conv108 Art. 11 Dir. 2016/680	La P-Conv108 prescrit que la personne concernée a le droit de ne pas être soumise à une décision prise uniquement sur le fondement d'un traitement automatisé de ses données, sans qu'elle puisse faire valoir son point de vue. La solution minimale envisageable serait que - que la personne concernée soit informée de l'existence d'une décision individuelle automatisée lorsque cette dernière a des effets juridiques pour elle ou l'affecte de manière significative ; - que la personne concernée ait la possibilité de faire valoir son point de vue sur la décision individuelle automatisée et sur les données traitées. Ces règles sont importantes, notamment en droit privé. En droit public, les décisions individuelles qui produisent des effets juridiques prennent en général la forme d'une décision de l'administration. Comme celle-ci doit être notifiée, les personnes concernées sont obligatoirement informées. Elles ont le droit de donner leur point de vue avant que la décision ne soit rendue, si bien qu'elles peuvent se prononcer sur la décision individuelle. On peut donc en déduire que les lois cantonales sur la protection (de l'information et) des données n'ont pas besoin d'intégrer des normes spéciales. Si des décisions individuelles automatisées devaient être introduites à l'avenir dans certains domaines, sans qu'elles débouchent sur une décision, mais qu'elles déploient quand même des effets juridiques ou des effets majeurs sur la personne concernée, il faut veiller à ce que la loi pose une base formelle claire et qu'il soit garanti à la personne concernée qu'elle a la possibilité de donner son point de vue sur la décision individuelle automatisée et sur les données traitées.	*Règles superflues s'il peut être garanti que la personne concernée est informée en cas de décision individuelle automatisée (p. ex. en cas de notification de la décision) et qu'elle a la possibilité de donner son point de vue (en vertu, p. ex, du droit d'être entendu).*	... si des règles sont superflues, parce qu'il est garanti que la personne concernée est informée en cas de décision individuelle automatisée (p. ex. en cas de notification de la décision) et qu'elle a la possibilité de donner son point de vue (en vertu, p. ex, du droit d'être entendu).
6.2	**Analyse d'impact relative à la protection des données** (guide ---) Adaptation requise	Art. 16 al. 1 et 2 AP-LPD Art. 8bis ch. 2 P-Conv108 Art. 27 Dir. 2016/680	Les nouvelles dispositions du droit supérieur prescrivent qu'une analyse d'impact relative à la protection des données est réalisée par l'organe public responsable. L'analyse contient au moins une description des procédures de traitement prévues, une évaluation des risques pour les droits fondamentaux des personnes concernées et l'exposition et l'évaluation des mesures prises pour y remédier, des garanties, des mesures de sécurité et des dispositifs permettant de respecter les droits fondamentaux des personnes concernées et de fournir la	*« L'organe public responsable est tenu de réaliser une analyse d'impact relative à la protection des données, dès lors qu'il entend traiter des données personnelles. »* *« L'analyse d'impact relative à la protection des données contient au moins :* - *une description générale des procédures de traitement prévues,* - *une évaluation des risques pour les*	... la loi prévoit que l'organe public responsable est tenu de réaliser une analyse d'impact relative à la protection des données, dès lors qu'il entend traiter des données personnelles.

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			preuve que cette loi est appliquée. L'analyse d'impact revient, pour l'organe public responsable, à préparer les éléments justifiant le respect des règles de protection des données (→ch. 4.10). Par ailleurs, elle touche les points qui doivent être évoqués dans le cadre de la consultation préalable (→ch. 6.3) qui a lieu dès lors que le traitement envisagé est susceptible d'entraîner un risque accru pour les droits fondamentaux des personnes concernées.	*droits fondamentaux des personnes concernées et* - *l'exposition et l'évaluation des mesures prises pour y remédier, des garanties, des mesures de sécurité et des dispositifs permettant de respecter les droits fondamentaux des personnes concernées et de fournir la preuve que cette loi est appliquée. »* *Les détails pourront être précisés par ordonnance.*	
6.3	**Consultation préalable** (guide ch. 5.2, « Contrôle préalable ») Adaptation requise	Art. 16 al. 3 et 4 AP-LPD Art. 28 Dir. 2016/680 (« Consultation préalable de l'autorité de contrôle »)	La directive 2016/680 (et le règlement général sur la protection des données) prévoient que certains projets sont soumis au délégué à la protection des données pour consultation préalable (« contrôle préalable », dans la législation antérieure). Il s'agit - de projets pour lesquels l'analyse d'impact a relevé des risques élevés pour les libertés et les droits des personnes, - de projets pour lesquels le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les droits fondamentaux des personnes concernées, - de projets législatifs qui touchent le traitement de données. Le délégué à la protection des données devra établir une liste des opérations de traitement, qui fera l'objet d'une consultation préalable. Les critères sont par exemple le nombre de personnes enregistrées, le nombre d'organes publics participants, la sensibilité des données (art. 28 al. 3 Dir. 2016/680). L'objectif de cette consultation est de garantir à temps la protection des données, notamment : - en tenant compte, lors de projets législatifs, des dispositions constitutionnelles et de celles relatives à la protection des données, - en détectant et en évaluant les risques et les mesures prévues, lors d'autres projets (TI), afin de réduire les risques à un minimum tolérable, d'examiner l'éventualité et de faire en sorte, le cas échéant, que des mesures d'ordre juridique, organisationnel ou technique soient prises pour réduire encore ce risque. Le délégué à la protection des données peut prendre position sur les projets législatifs. Pour d'autres projets, le délégué à la protection des données peut formuler des recommandations (→ ch. 8.5b), lorsque le traitement des données prévu viole les dispositions légales en matière de protection des données, en particulier lorsque	*« Consultation préalable du délégué à la protection des données* *L'organe public responsable soumet au délégué à la protection des données les objets suivants :* - *projets législatifs touchant à la protection des données, et* - *projets pour lesquels le type de traitement en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les droits fondamentaux des personnes concernées.* *Le délégué à la protection des données peut établir une liste des opérations de traitement, qui fera l'objet d'une consultation préalable. »*	… la loi prévoit l'obligation de réaliser une consultation préalable pour les projets législatifs ou pour les projets qui comportent un risque élevé pour les droits fondamentaux des personnes concernées par le traitement des données

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			l'organe public responsable n'a pas suffisamment évalué les risques pour les droits fondamentaux des personnes concernées et engagé des mesures pour les atténuer. Tous les documents requis une fois rassemblés, le délégué à la protection des données a six semaines (prolongement d'un mois envisageable) pour livrer son évaluation (recommandation) ou pour exercer les compétences qui lui sont conférées (→ ch. 8.5). Il n'est pas vraiment utile de prescrire un délai fixe. Les consultations préalables de moindre importance devraient se dérouler rapidement – sachant que les projets de longue haleine supposent toujours une consultation préalable à différents stades d'avancement. La loi pourrait préciser, le cas échéant, « dans un délai raisonnable ». La réglementation que propose la Confédération dans le projet mis en consultation ne tient pas pleinement compte des exigences posées par la Dir. 2016/680. La consultation préalable est un moyen efficace de prévention ; il évite qu'il faille après coup améliorer les projets au prix d'efforts considérables ou même les abandonner.		
6.4	**Obligation de notification des violations de la protection des données** (guide ---) Adaptation requise	Art. 17 AP-LPD Art. 7 ch. 2 P-Conv108 Art. 30 Dir. 2016/680 (à l'autorité de surveillance) Art. 31 Dir. 2016/680 (aux personnes concernées)	Les violations de la protection des données (définition légale → prochaine rubrique) doivent être notifiées sans délai au délégué à la protection des données, à moins que la violation ne présente vraisemblablement pas de risques pour la personnalité et les droits fondamentaux de la personne concernée. Le contenu de la notification (détails de la violation, de ses effets les plus probables et des mesures effectives/prévues pour rétablir la protection et atténuer les effets de cette violation) peut être défini par ordonnance. L'organe public responsable informe en outre les personnes concernées lorsque les circonstances l'exigent ou lorsque le délégué à la protection des données le demande. La communication est obligatoire lorsque les personnes concernées peuvent prendre les dispositions nécessaires pour éviter un préjudice. L'organe public peut renoncer à la communication, dès lors que des dispositions sont prises ultérieurement afin d'éliminer le plus sûrement le risque élevé pour les droits fondamentaux des personnes concernées. Par ailleurs, l'organe public peut renoncer, en tout ou partie, à cette information ou l'ajourner si un intérêt public ou privé prépondérant l'exige. En cas de **sous-traitance :** Si la violation a lieu dans le cadre de la sous-traitance, le sous-traitant la notifiera sans délai à l'organe public responsable qui la signalera au délégué à la protection des données (règlement à cet endroit ou au chapitre consacré au sous-	*Notification des violations de la protection des données* *«[x] L'organe public responsable notifie au délégué à la protection des données, sans délai indu, toute violation de la protection des données.* *[x] Il y a violation de la protection des données .....» [→ voir ci-dessous en fin de rubrique]* *«[x] Il n'existe pas d'obligation de notification, dès lors que la violation de la protection des données ne présente vraisemblablement pas de risques pour les droits fondamentaux de la personne concernée.* *[x] L'organe public responsable informe en outre les personnes concernées, lorsque les circonstances l'exigent ou lorsque le délégué à la protection des données le demande.* *[x] Par ailleurs, l'organe public peut renoncer, en tout ou partie, à cette information ou l'ajourner si un intérêt public ou privé prépondérant l'exige » (ou renvoi à une réglementation générale régissant les restrictions).* *Régler en lien avec la **sous-traitance**, ou*	... la loi prévoit une obligation de notification en cas de violation de la protection des données (notion à définir).

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	(définition légale) (guide ---) Adaptation requise		traitant → ch. 4.12). Donner une définition de la « violation de la protection des données. *[La définition qu'en donne l'art. 17 AP-LPD (« traitement non autorisé ») est trop générale ; elle obligerait à communiquer toute violence ou atteinte, même mineure.]*	*de la façon suivante :* *«[x] Le sous-traitant notifiera sans délai toute violation de la protection des données à l'organe public responsable. »* *« Il y a violation de la protection des données dès lors que l'atteinte à la sécurité est telle qu'elle a entraîné la suppression définitive ou la perte des données traitées, leur modification ou leur divulgation non intentionnelle ou illicite, ou que des personnes non autorisées ont accès à ces données personnelles. »*	
6.5	**Destinataires des données personnelles informés des rectifications, effacements/destructions, violations de la protection des données ou limitations de traitement** (guide ---) Adaptation requise	Art. 19 let. b AP-LPD Art. 16 al. 5 Dir. 2016/680	Du moment que le traitement des données n'est pas (plus) légitime, les services et les personnes qui ont reçu préalablement les données personnelles sont informés de leur rectification, de leur effacement ou destruction, de leur violation (→ ch. 6.4) ou de leur limitation de traitement (→ ch. 5.7, vers la fin), afin que les tiers à qui les données ont été communiquées ne puissent plus les retravailler, parce qu'ils ignorent la procédure. Il peut être fait abstraction d'une information seulement si elle se révèle impossible ou exige des efforts disproportionnés. La situation doit être appréciée avec soin. L'organe public compétent doit avoir fait une tentative au moins et avoir rencontré de sérieuses difficultés, surmontables uniquement au prix d'efforts considérables.	*L'organe public informe les destinataires des données personnelles de chaque rectification, effacement ou destruction (→ ch. 6.4), ou limitation de traitement conformément à l'art. ■■ (→ ch. 5.7, vers la fin), sauf si cela se révèle impossible ou exige des efforts disproportionnés.*	... la loi prévoit l'obligation d'information
6.6	**Règles de traitement des données personnelles à des fins sans lien avec la personne** (guide, ch. 5.3) Aucune adaptation requise	Art. 32 AP-LPD Art. 5 ch.4 let. b P-Conv108 Art. 4 al. 3 Dir. 2016/680	La finalité du traitement des données peut être sans lien avec la personne lorsque, bien que ces données concernent une personne identifiée ou identifiable, celle-ci n'est pas visée en tant que telle, puisque les données sont utilisées à des fins statistiques, de planification ou de recherche (parfois dites « finalités scientifiques », bien que « scientifiques » ne recouvre que la méthode). Il est permis de privilégier ce type de traitement (p. ex., se passer de base légale spéciale pour le traitement ou la communication de données), s'il est certain que les données sont rendues anonymes du moment que la finalité du traitement l'autorise et si les résultats publiés ne permettent pas d'identifier la personne concernée. Il peut être utile, dans certaines circonstances, d'assortir la communication de données personnelles à des destinataires hors de l'administration de conditions supplémentaires (garanties, interdiction de diffusion, peines conventionnelles, etc.). La *première* collecte de données personnelles à des fins non liées à la personne exige en revanche une base légale sépa-	*P. ex. : **traitement** des données à des fins sans lien avec la personne (par l'organe public compétent) :* *« Un organe public est en droit de traiter des données personnelles à des fins sans lien avec la personne, notamment dans le cadre de la recherche, de la planification ou de la statistique, aux conditions suivantes :* - *les données ne sont plus utilisées ou communiquées à des fins en lien avec la personne, et* - *les données sont rendues anonymes ou un pseudonyme est utilisé, si la finalité du traitement le permet, et* - *les résultats du traitement sont publiés sous une forme ne permettant pas d'identifier la personne concernée. »*	… la loi prévoit que du moment que la finalité du traitement est sans lien avec la personne, les données personnelles sont rendues anonymes et les résultats sont publiés seulement s'il est impossible d'identifier la personne concernée

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			rée et elle n'est pas incluse dans la liste des tâches. Il est envisageable de renforcer, par une disposition pénale, la communication de données dans une finalité sans lien avec la personne, dans l'éventualité où le destinataire qui a reçu les données d'un organe public à des fins de traitement sans lien avec la personne les traite à d'autres fins ou les fait suivre intentionnellement ou par négligence à des tiers, enfreignant ainsi ses obligations.	*P. ex : **communication** des données à des fins sans lien avec la personne :* *« Un organe public est en droit de communiquer à d'autres organes publics de son canton, d'autres cantons ou de la Confédération des données qui seront traitées à des fins sans lien avec la personne, notamment dans le cadre de la recherche, de la planification ou de la statistique, tant que cela n'est pas exclu par une disposition sur la confidentialité.* *Le destinataire s'engage :* *- à rendre les données anonymes ou à utiliser un pseudonyme, pour autant que la finalité du traitement le permette, et* *- à publier les résultats sous une forme ne permettant pas d'identifier la personne concernée.* *L'organe public peut communiquer des données à des personnes privées qui les traiteront à des fins de recherche, tant que cela n'est pas exclu par une disposition sur la confidentialité et que le destinataire est tenu, en sus, en vertu de l'al. 2,* *- de ne pas traiter les données à d'autres fins, et* *- de ne pas communiquer les données à des tiers, et* *- de veiller à la sécurité de l'information. »* *Aménagement éventuel d'une **disposition pénale** :* *« Quiconque traite ou communique à des tiers, intentionnellement ou par négligence, des données personnelles qu'il a reçues d'un organe public à des fins de traitement sans lien avec la personne et qui enfreint ce faisant l'obligation prévue à § ■■ est puni d'une amende. » (Renvoi éventuel à la loi sur les contraventions pénales pour connaître le montant des amendes, la façon de les calculer, etc.).*	
6.7	**Registre des activités de trai-**	Art. 36 AP-LPD Art. 24 Dir. 2016/680 (pas de	L'obligation de tenir un registre des activités de traitement, prévue par la directive 2016/680, concerne uniquement les	*L'obligation de tenir un registre des activités de traitement n'existe que pour le*	... l'obligation de tenir un registre sur les activités de

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	tement (guide, ch. 5.4) Nécessité d'adaptation à vérifier	registre public)	autorités judiciaires et la police. Il est donc possible de l'appliquer à des domaines précis (p. ex. loi sur la police, loi d'introduction du code de procédure pénale (CPP) ; il est probable que la Confédération maintiendra dans la LPD l'obligation de tenir un registre pour les organes fédéraux, mais pas dans le CPP ; les cantons ne seront donc pas tenus de la respecter). Ce registre n'est pas équivalent à la preuve du respect des dispositions sur la protection des données (→ ch. 4.10) ; il est, tout au plus, un « pis-aller ». *Dans un souci de transparence*, les cantons peuvent, p. ex., maintenir un registre des procédures ayant trait au traitement de données personnelles (p. ex. ; § 24 IDG/BS, (http://www.staatskanzlei.bs.ch/oeffentlichkeitsprinzip/verfahren.html).	*domaine d'application de la directive 2016/680 (justice, police) → inscription de l'obligation dans la loi sur la police et dans la loi d'introduction du code de procédure pénale CPP.* *Dans un souci de transparence, il est possible de maintenir un registre des procédures ayant trait au traitement de données personnelles (p. ex. § 24 IDG/BS).*	traitement est prévue par le droit réel pour les autorités judiciaires et la police
6.8	**Flux transfrontières de données** (guide, ch. 5.5) Aucune adaptation requise	Art. 5 et 6 AP-LPD Art. 12 P-Conv108 Art. 35-39 Dir. 2016/680	La loi doit prévoir, outre les modalités de communication des données, que le transfert transfrontière de données personnelles à des destinataires qui échappent à la Convention (108) pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel n'est autorisé que si un niveau de protection adéquat est garanti par l'État où se trouvent ces destinataires (au sens de l'art. 12 C108). Il est utile de mentionner (éventuellement dans l'ordonnance d'exécution) que les organes publics qui s'interrogent sur le niveau de protection des données dans un État se réfèrent à la liste établie par le Conseil fédéral sur la base de l'art. 5 al.7 AP-LPD.	*Inscriptions des conditions dans la loi, conformément à l'art. 12 C108*	… la loi prévoit que la communication de données à l'étranger n'est autorisée qu'aux conditions figurant à l'art. 12 C108
7	**Voies de droit, responsabilité, sanctions**				
7.1	**Voies de droit (garantie des voies de droit)** (guide, ch. 6.1) Aucune adaptation requise	Art. 34 al. 5 AP-LPD Art. 8 let. f P-Conv108 Art. 10 P-Conv108 Art. 12bis ch. 6 P-Conv108 Art. 53 et 54 Dir. 2016/680	Toute personne concernée par le traitement de ses données doit pouvoir saisir une instance judiciaire par voie de droit si elle estime que ses droits ont été violés, le cas échéant après la procédure interne de recours administratif. (Annulabilité des décisions de l'organe de contrôle → ch. 8.10)	*(En lien avec les droits et les prétentions de la personne concernée [→ ch. 5.4 ss.)* *« Si un organe public ignore une demande sur la base de cette loi, il justifie sa décision » → annulable en vertu, p. ex., de la loi de procédure administrative ou de la loi sur l'organisation procédurale administrative*	… en fin de compte, la personne concernée (le cas échéant après avoir épuisé les voies de recours administratives internes) peut s'adresser à une instance judiciaire
7.2	**Responsabilité** (guide, ch. 6.2) Aucune adaptation requise	Art. 10 P-Conv108 Art. 56 Dir. 2016/680	Si une personne subit un préjudice en raison du traitement illicite de ses données, elle a droit à des dommages-intérêts.	*P. ex. : loi sur la responsabilité, loi sur la responsabilité des organes de l'État*	… une base légale permet de faire valoir des dommages-intérêts en cas de traitement illicite des données
7.3	**Sanctions**	Art. 55 ss AP-LPD (dispositions pénales) Art. 10 P-Conv108	Une loi doit prévoir des sanctions en cas de violation des dispositions sur la protection des données.	*P. ex. : disposition pénale en cas de violation du secret de fonction ; disposition pénale en cas d'utilisation contraire au*	… une loi prévoit des sanctions en cas de violation des dispositions sur la

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	(guide, ch. 6.3) Aucune adaptation requise	Art. 57 Dir. 2016/680		*mandat ou de communication de données personnelles par des tiers mandatés pour traiter ces données*	protection des données
8	**Préposé à la protection des données**				
8.1	**Préposé à la protection des données** (guide, ch. 7.1) Aucune adaptation requise	Art. 37-49 AP-LPD Art. 12bis ch. 1 P-Conv108 Art. 44 Dir. 2016/680	Le traitement administratif des données est contrôlé par un organe totalement indépendant. La loi doit donc prévoir expressément la présence d'un préposé à la protection des données, indépendant (→ ch. 8.7 f.) et capable d'exercer un contrôle efficace (→ ch. 8.9).		… la loi prévoit la création d'un poste de préposé à la protection des données (elle précise ses tâches (ch. 8.4), ses compétences (ch. 8.5), ses devoirs (ch. 8.6), son indépendance (ch. 8.7 f) et la garantie d'un contrôle efficace (ch. 8.9)
8.2	**Exceptions au contrôle** (guide ---)	Art. 2 al. 3 et 4 AP-LPD Art. 12bis ch. 9 P-Conv108 Art. 45 al. 2 Dir. 2016/680	Les opérations de traitement des procédures judiciaires pendantes devraient échapper à la surveillance du préposé à la protection des données, pour faire contrepoint à l'applicabilité de la loi sur la protection des données dans les procédures judiciaires en cours (→ ch. 2.3 et 2.4). Il y a donc lieu d'aménager une exception. Tout au plus, le parlement cantonal et les exécutifs cantonaux peuvent être exclus de la surveillance du préposé à la protection des données, en raison de la séparation des pouvoirs.	*« Échappent à la surveillance du préposé :* - *les opérations de traitement des procédures pendantes civiles ou pénales ;* - *les opérations de traitement des procédures pendantes de juridiction constitutionnelle ou administrative »*	... les opérations de traitement des procédures pendantes civiles ou pénales échappent à la surveillance du préposé à la protection des données
8.3	**Qualification** (guide ---) Adaptation requise	Art. 43 al. 2 Dir. 2016/680	Pour exercer ses fonctions, le préposé à la protection des données doit justifier des qualifications, de l'expérience et des compétences nécessaires, en particulier dans le domaine de la protection des données.	*L'organe de contrôle « est dirigé par un spécialiste de la protection des données (le préposé) », « peut être nommé préposé un spécialiste de la protection des données »*	
8.4	**Tâches** (guide, ch. 7.2) Adaptation requise	Art. 40 al. 1, art. 49 AP-LPD Art. 12bis ch.2 let. b, e, P-Conv108 Art. 12bis ch. 2^{bis,} 3, 5bis, 7 P-Conv108 Art. 45 Dir. 2016/680	Le préposé à la protection des données doit accomplir au moins les tâches suivantes :		
8.4a	Contrôle	Art. 40 al. 1 AP-LPD Art. 46 al. 1 let. a Dir.	Contrôle - contrôle indépendant et inopiné sur la base d'un plan établi	*Le préposé à la protection des données « surveille la mise en œuvre des disposi-*	… la mission de contrôle est inscrite dans la loi

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	(guide, ch. 7.2a) Aucune adaptation requise	2016/680	par le préposé à la protection des données lui-même - contrôle au cas par cas du traitement concret des données, en particulier des « recours » des personnes concernées (dénonciations à l'autorité de surveillance)	*tions sur la protection des données », il « contrôle leur application sur la base d'un plan qu'il établit lui-même »*	
8.4b	Conseil (guide, ch. 7.2b) Aucune adaptation requise	Art. 49 let. a AP-LPD Art. 12bis ch. 2bis P-Conv108 Art. 46 al. 1 let. c et e Dir. 2016/680	Conseil aux organes publics - dans l'activité législative et - dans l'application du droit et conseil aux personnes concernées	*Le préposé à la protection des données « donne son avis sur les actes législatifs importants pour la protection des données » ; « l'organe de contrôle conseille les organes publics sur les questions ayant trait à la protection des données (et la sécurité de l'information) », « il conseille les personnes concernées sur leurs droits ».*	… la mission de conseil est inscrite dans la loi
8.4c	Sensibilisation des organes publics responsables et de la population (guide ---) Adaptation requise	Art. 49 let. c AP-LPD Art. 12bis ch. 2 let. e P-Conv108 Art. 46 al. 1 let. b et d Dir. 2016/680	C'est l'une des tâches du préposé à la protection des données de sensibiliser les organes publics responsables aux obligations qui sont les leurs et le public aux questions liées à la protection des données (notamment à la responsabilité des personnes concernées).	*Le préposé à la protection des données « sensibilise les organes publics à leur mission de protection des données et le public à l'importance de la protection des données ».*	… la mission de sensibilisation est inscrite dans la loi
8.4d	Suivi des évolutions pertinentes (guide ---) Adaptation requise	Art. 46 al. 1 let. j Dir. 2016/680	Suivi des évolutions pertinentes dans le domaine des technologies de l'information et de la communication, dans la mesure où elles ont une incidence sur la protection des données personnelles	*Le préposé à la protection des données « suit les évolutions pertinentes pour la protection des données personnelles ».*	… la mission de suivre les évolutions pertinentes afin de protéger les données personnelles est inscrite dans la loi
8.4e	Collaboration (guide ---) Nécessité d'adaptation à vérifier	Art. 49 let. b AP-LPD Art. 46 al. 1 let. h Dir. 2016/680	Les autorités de surveillance collaborent étroitement avec d'autres autorités de surveillance ; elles se prêtent mutuellement assistance.	*Le préposé à la protection des données « collabore avec les organes d'autres cantons, de la Confédération ou étrangers, qui accomplissent les mêmes tâches que lui ».*	... l'obligation de collaborer est inscrite dans la loi
8.4f	Frais (guide ---) Nécessité d'adaptation à vérifier	Art. 46 al. 3 Dir. 2016/680	Le préposé à la protection des données accomplit ses missions gratuitement pour les personnes concernées. Si les demandes sont manifestement infondées ou trop fréquentes, l'autorité de contrôle peut facturer des frais équitables, calculés sur la base des frais de gestion, ou elle refusera d'accomplir le mandat, auquel cas elle devra prouver que celui-ci est manifestement infondé ou excessif.	*Il n'est pas prévu de facturer des frais, mais il n'est pas exclu de le faire non plus : « L'accomplissement des missions du préposé à la protection des données est gratuit pour les personnes concernées. » Possibilité de prévoir explicitement une exception (frais facturés ou non-recevabilité d'une demande manifestement infondée ou excessive)*	… l'accomplissement des missions par le préposé à la protection des données est gratuit en vertu de la loi (exception faite éventuelle des demandes manifestement infondées ou excessives)
8.4g	Autres	Art. 49 let. f AP-LPD	L'organe de contrôle peut se voir accorder d'autres tâches, p. ex. celle de médiation entre les personnes concernées et les	*Le préposé à la protection des données « fait office de médiateur entre les organes*	… aucune autre mission n'est confiée au préposé à

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	(guide, ch. 7.2c) Aucune adaptation requise		organes publics (pour autant que les deux parties y consentent). Il faut veiller cependant à ce que ces missions ne compromettent pas l'indépendance du contrôle. La réserve qui entend faire approuver certains traitements de données par le préposé à la protection des données pose problème, dans la mesure où l'organe public n'est plus responsable (→ ch. 4.9) du traitement des données. Une mission de conciliation peut poser problème si l'on considère le principe de transparence dans l'administration, car elle exclut pratiquement toute discussion préalable avec l'organe public et éventuellement la personne de qui émane la demande (il se peut aussi que l'impartialité de la conciliation ne soit plus garantie après la discussion).	*publics et les personnes concernées ».*	la protection des données qui puisse compromettre l'indépendance du contrôle
8.5	**Compétences** (guide, ch. 7.3)	Art. 12bis ch. 2 let. a, b-d P-Conv108 Art. 47 Dir. 2016/680	L'organe de contrôle (le préposé à la protection des données) doit disposer au moins de compétences suivantes :		
8.5a	Investigation (guide, ch. 7.3a) Aucune adaptation requise	Art. 41 AP-LPD Art. 12bis ch. 2 let. a P-Conv108 Art. 47 al. 1 Dir. 2016/680	Pouvoir d'investigation complet : pouvoir de mener des enquêtes indépendamment de toute obligation de discrétion, d'obtenir toutes les informations sur le traitement des données nécessaires à l'accomplissement de sa mission de contrôle, de consulter tous les documents, de procéder à des visites et d'assister à des démonstrations sur la façon dont s'effectuent les traitements	*Le préposé à la protection des données « est autorisé, indépendamment de toute obligation de discrétion, à mener des enquêtes, à obtenir toutes les informations sur le traitement des données nécessaires à l'accomplissement de sa mission de contrôle, à consulter tous les documents, à procéder à des visites et à assister à des démonstrations sur la façon dont s'effectuent les traitements*	… la loi reconnaît au préposé à la protection des données un pouvoir d'investigation complet, tel que décrit, indépendamment de toute obligation de discrétion éventuelle
8.5b	Intervention (guide, ch. 7.3b) Nécessité d'adaptation à vérifier	Art. 43 AP-LPD Art. 12bis ch. 2 let. a P-Conv108 Art. 47 al. 2 Dir. 2016/680	Le préposé à la protection des données doit disposer d'un pouvoir d'intervention réel. Il a le droit de s'exprimer sur le projet (consultation préalable, cf. ch. 6.3), de faire des *remarques* sur le traitement des données et d'émettre des *recommandations* concrètes (formelles) sur le traitement lui-même. L'organe public auquel la recommandation est adressée donne son avis et déclare s'il compte suivre ou non la recommandation.	*P. ex.* *« Le préposé à la protection des données peut émettre des recommandations sur la manière de traiter des données personnelles.* *L'organe public auquel la recommandation est adressée déclare au préposé à la protection des données s'il compte suivre sa recommandation. »*	… la loi reconnaît au préposé à la protection des données un pouvoir d'intervention réel, tel que décrit
8.5c	Injonction (décision) Nécessité d'adaptation à vérifier	Art. 43 AP-LPD Art. 12bis ch. 2 let. c et art. 12bis ch. 6 P-Conv108 Art. 47 al. 2 let. b et c Dir. 2016/680	En présence d'une infraction aux dispositions légales de protection des données, l'organe de contrôle doit pouvoir *enjoindre* (par décision), p. ex., de suspendre le traitement illicite de données ou de renoncer à leur communication illicite. L'injonction peut être qualifiée de « directive », p. ex., à moins que ce terme ne recouvre une autre réalité dans le droit cantonal (dans le canton de ZH, il est utilisé pour adresser un projet au parlement, alors que la Confédération parle de « message »). Cette injonction peut être émise après le rejet d'une recom-	*« Si un organe public déclare ne pas vouloir suivre la recommandation du préposé à la protection des données ou qu'il ne la suit effectivement pas, le préposé à la protection des données peut décider (ordre) de faire appliquer tout ou partie de la recommandation si l'intérêt de sa mise en œuvre est prépondérant.* *Aucune injonction (directive) ne peut être émise à l'encontre du tribunal cantonal*	... si le préposé à la protection des données a le pouvoir, en cas d'infraction au droit à la protection des données, d'émettre des injonctions (directives) susceptibles de recours devant un tribunal

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			mandation (→ ch. 8.5b) ou directement, s'il est prévisible que l'organe public rejettera la recommandation ou qu'il ne lui donnera pas suite. Cette injonction, qui prend la forme d'une décision, est susceptible de recours (→ ch. 8.10) directement devant le tribunal cantonal (tribunal administratif).	*(tribunal administratif).* *Le préposé à la protection des données peut émettre directement une injonction (directive) s'il est prévisible que l'organe public rejettera la recommandation ou qu'il ne lui donnera pas suite.* *L'organe public auquel l'injonction (directive) est adressée peut déposer un recours devant le tribunal cantonal (tribunal administratif) conformément aux règles en vigueur. »*	
8.5d	Mesures provisoires (guide ---) Adaptation requise	Art. 42 AP-LPD Art. 47 al. 2 let. c Dir. 2016/680	Si des intérêts dignes de protection sont visiblement menacés ou lésés, le préposé à la protection des données doit pouvoir interdire à titre préventif le traitement des données.	*« Si des intérêts dignes de protection sont visiblement menacés ou lésés, le préposé à la protection des données peut, à titre préventif, ordonner des mesures provisoires pour limiter ou suspendre le traitement des données par l'organe public jusqu'à ce que le cas ait été examiné par le tribunal cantonal. »*	... si le préposé à la protection des données a le pouvoir d'ordonner des mesures provisoires pour limiter ou suspendre le traitement des données dans l'éventualité où des intérêts dignes de protection sont visiblement menacés ou lésés
8.5e	Plainte, dénonciation (guide, ch. 7.3c) Nécessité d'adaptation à vérifier	Art. 45 AP-LPD Art. 12bis ch. 2 let. d P-Conv108 Art. 47 al. 5 Dir. 2016/680	Pouvoir d'ester en justice, de dénoncer : droit d'intenter une action devant les instances judiciaires ou de déposer une dénonciation en cas de violation de la loi sur la protection des données. Le droit de dénoncer une infraction résulte de l'art. 301 CPP. L'*obligation* de dénoncer (art. 302 al. 2 CPP) n'est pas à établir, du moins dans le cadre de la fonction. Si l'infraction persiste, une injonction doit être envisagée (→ ch. 8.5c). Dans les cas où ni une plainte pénale, ni une directive n'entrent en ligne de compte, il doit néanmoins être possible de déposer une dénonciation devant l'autorité supérieure à l'organe public qui a enfreint les dispositions légales sur la protection des données, comme le permet en principe le droit administratif. Sinon, il y a lieu de mentionner cette possibilité dans la loi sur la protection des données.	*Si le droit de déposer une dénonciation devant l'autorité supérieure à l'organe public qui a enfreint les dispositions légales sur la protection des données n'est pas prévu par le droit administratif :* *« Le préposé à la protection des données peut dénoncer une telle infraction à l'autorité supérieure à l'organe public qui a enfreint les dispositions légales sur la protection des données. »*	… un pouvoir d'ester en justice ou de dénonciation est reconnu par la loi au préposé à la protection des données
8.5f	Sanctions (guide ---) Nécessité d'adaptation à vérifier	Art. 50 ss. AP-LPD Art. 12bis ch.. 2 let. c P-Conv108 Art. 57 Dir. 2016/680	En cas d'infraction à la législation sur la protection des données, l'organe de contrôle doit pouvoir infliger des sanctions administratives (on pense ici à des amendes). Les sanctions sont efficaces, proportionnées et dissuasives. Des amendes au sein de l'administration, autrement dit d'un même budget, ne riment presque à rien. Chaque canton doit réfléchir à la nécessité de mettre en place un règlement ad hoc.	*Si le préposé à la protection des données doit pouvoir infliger des sanctions à l'organe public qui enfreint la législation sur la protection des données ; mettre en place un règlement ad hoc (p. ex. amendes, critères d'appréciation).*	... un pouvoir de sanction est prévu par la loi (assorti d'un règlement ad hoc), pour autant qu'il soit souhaité par le canton
8.6	**Devoirs**	Diff. art. AP-LPD	Mention expresse dans la loi au moins des obligations sui-		

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	(guide, ch. 7.4)	Art. 12 ch. 3, 5bis, 5ter, 7 P-Conv108 Art. 44 al. 2 et art. 49, 50, 52 Dir. 2016/680	vantes de l'organe de contrôle (du préposé à la protection des données) :		
8.6a	Traitement des requêtes (guide, ch. 7.4a) Adaptation requise	Art. 12bis ch. 3 P-Conv108 Art. 52 Dir. 2016/680	Traitement des requêtes : obligation d'entendre le plaignant (→ ch. 5.10) au sujet de la protection de ses droits et de ses libertés fondamentales en lien avec le traitement de données personnelles, et de traiter sa demande	→ *Ch. 5.10*	→ Ch. 5.10
8.6b	Entraide administrative (guide, ch. 7.4b) Aucune adaptation requise	Art. 46 et 47 AP-LPD Art. 12bis ch. 7 P-Conv108 Art. 50 Dir. 2016/680	Entraide administrative : obligation, dans l'accomplissement des tâches de contrôle, de collaborer avec les organes de contrôle (préposés à la protection des données) des autres cantons, de la Confédération et des pays étrangers	*Le préposé à la protection des données « travaille avec les organes de contrôle des autres cantons, de la Confédération et des pays étrangers. »*	… le préposé à la protection des données a l'obligation légale de collaborer avec les autres organes de contrôle
8.6c	Devoir de discrétion (guide, ch. 7.4c) Aucune adaptation requise	Art. 12bis ch. 5ter P-Conv108 Art. 44 al. 2 Dir. 2016/680	Secret professionnel : obligation de respecter les dispositions relatives au secret professionnel, même après la fin de l'activité, au même titre que les organes publics amenés à traiter des données personnelles	*« Les membres et les collaborateurs du préposé à la protection des données sont tenus de garder le secret sur les données personnelles dont ils ont connaissance dans le cadre de leur travail, au même titre que l'organe public qui traite ces données.»* *Pouvoir d'investigation : « Le préposé et ses collaborateurs sont tenus de garder le secret sur les informations dont ils ont connaissance dans le cadre de leur travail, au même titre que l'organe public qui traite ces informations. »*	… le préposé à la protection des données a l'obligation légale de respecter le secret professionnel (même après la fin de l'activité)
8.6d	Compte-rendu (guide, ch. 7.4d) Aucune adaptation requise	Art. 48 AP-LPD Art. 12bis ch. 5bis P-Conv108 Art. 49 Dir. 2016/680	Compte-rendu : obligation, d'une part, de rendre compte à l'organe de nomination des activités, de la gestion financière, etc. et, d'autre part, d'informer périodiquement ou chaque fois que cela est nécessaire l'organe de nomination et le public des résultats de ses activités (de contrôle), autrement dit des constatations et des évaluations qu'il a faites et des conséquences des dispositions relatives à la protection des données (succès et échecs)	*Le préposé à la protection des données « rend compte de ses activités à l'organe de nomination et il informe celui-ci et l'opinion publique, périodiquement ou chaque fois que cela est nécessaire, des constatations et des évaluations qu'il a faites et de la mise en œuvre des dispositions sur la protection des données. »*	… le préposé à la protection des données a l'obligation légale de rendre compte de sa gestion financière et de ses activités
8.7	**Garantie d'indépendance totale** (guide, ch. 7.5 + annexe)	Art. 37 al. 3 AP-LPD Art. 12bis ch. 4 P-Conv108 Art. 42 et 43 Dir. 2016/680	Les dispositions légales exigent un organe de contrôle qui accomplisse ses tâches en toute indépendance, ce qui implique, d'une part, que cette indépendance soit inscrite dans la loi et, d'autre part, qu'elle obtienne des garanties institutionnelles (cf. ch. 8.8).	*P. ex. : utilisation des termes « indépendance », « organe de contrôle indépendant » ou autres dans le titre du paragraphe ou dans le texte de loi*	… l'indépendance est garantie expressément par la loi
8.8	(Garanties institutionnelles d'indé-	Art. 37-39 AP-LPD Art. 12bis ch. 4 P-Conv108	Il est nécessaire de prévoir des garanties institutionnelles en plus de postuler l'indépendance totale de l'organe de contrôle.	*Indépendance :* *« accomplit ses tâches sans recevoir*	… l'indépendance, l'incompatibilité, la procé-

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
	pendance totale) (guide, ch. 7.6 + annexe) Nécessité d'adaptation à vérifier	Art. 42 al. 2 Dir. 2016/680 (indépendance) Art. 42 al. 3 Dir. 2016/680 (incompatibilité) Art. 42 al. 5 Dir. 2016/680 (choix de ses propres agents) Art. 42 al. 6 Dir. 2016/680 (budget) Art. 43 al. 1 Dir. 2016/680 (nomination) Art. 43 al. 3 Dir. 2016/680 (choix de la durée du mandat) Art. 43 al. 4 Dir. 2016/680 (révocation)	Les garanties contiennent au moins les éléments suivants : - indépendance - incompatibilité : autre charge publique, fonction dirigeante dans un parti politique, autre activité lucrative ? - procédure de nomination (afin d'éviter une « nomination des contrôleurs par les contrôlés » : si possible par le parlement seul ou par une procédure à laquelle il participe [approbation de la nomination faite par l'exécutif, nomination par le parlement sur proposition de l'exécutif, etc.]) - choix d'une durée de mandat fixe de quatre ans au moins - révocation : incapacité permanente de remplir ses fonctions ou faute grave (en règle générale par décision à la majorité qualifiée de l'autorité de nomination) - propre budget - choix de ses propres agents (dans le cadre du budget approuvé)	*d'instructions »* *Incompatibilité :* *« Le préposé ne peut assumer aucune autre charge publique, aucune fonction dirigeante au sein d'un parti politique, aucune autre activité lucrative. L'organe de nomination peut accorder des dérogations. Si le préposé travaille à temps partiel au sein de l'organe de contrôle, l'autorisation d'exercer l'autre activité lucrative ne peut lui être refusée dans la mesure où cette activité lucrative ne l'empêche pas de remplir sa fonction et qu'elle n'influence ni son indépendance, ni sa réputation. »* *Procédure de nomination (organe de nomination, procédure de nomination) et durée du mandat* *Révocation :* *« Le préposé ne peut être relevé de ses fonctions que s'il est incapable de remplir ses fonctions de façon permanente ou s'il commet une faute grave. La décision est prise par l'organe de nomination, à la majorité des deux tiers. »* *Budget :* *L'organe de contrôle établit son propre budget, dont il dispose librement une fois celui-ci approuvé par le Parlement.* *Recrutement du personnel :* *« Le préposé décide, dans les limites du budget approuvé par le Parlement, de la gestion du personnel de l'organe de contrôle et prend les décisions juridiques le concernant. »*	dure de nomination, la durée du mandat, la révocation, le budget et le choix des propres agents sont précisés dans la loi
8.9	**Garantie d'un contrôle efficace** (guide, ch. 7.7) Nécessité d'adaptation à vérifier	Art. 12bis ch. 5 P-Conv108 Art. 47 al. 4 Dir. 2016/680	Les prescriptions légales exigent un contrôle actif et efficace. Il doit pouvoir être inopiné et intervenir sur la base d'un programme de contrôle établi de façon autonome après une évaluation des risques. Cela suppose - premièrement, que l'organe de contrôle possède les compétences requises (cf. ch. 8.5), - deuxièmement, qu'il dispose des ressources financières et en personnel nécessaires et - troisièmement, que lui ou sa direction justifient de compétences techniques élevées (qualification → ch. 8.3 ; formation continue).	*Attribution de ressources suffisantes dans les petits et les moyens cantons pour financer plusieurs postes au sein de l'organe de contrôle (droit, [révision] informatique) ; taux d'occupation de 50 %-100 % dans les petits cantons* *Alternative : des solutions régionales communes à plusieurs (petits) cantons*	… contrôle efficace assuré si les ressources financières et en personnel sont suffisantes et les compétences techniques élevées

	Rubrique	Base légale	Commentaire	Solutions possibles	Réalisé si …
			Un contrôle réel ne peut en aucun cas être assuré par un organe de contrôle cantonal si la seule chose que celui-ci puisse faire, en raison de son faible taux d'occupation (30-40 % pour les petits cantons), soit de réagir à une sollicitation, p. ex. En outre, le temps partiel soulève la question des activités (lucratives) accessoires (ou de leur autorisation), ce qui pose un problème d'indépendance.		
8.10	**Annulabilité des décisions de l'organe de contrôle** (guide, ch. 7.8)	Art. 44 AP-LPD Art. 12bis ch. 6 P-Conv108 Art. 53 Dir. 2016/680	Les décisions de l'organe de contrôle doivent pouvoir faire l'objet d'un recours juridictionnel. Dans la mesure où ses actes juridiques (p. ex. injonctions, mesures provisionnelles ; → ch. 8.5c+d) ont un effet contraignant, ils doivent pouvoir être soumis à un contrôle judiciaire.	Pas de réglementation explicite dans la LPD, du moment que les règles de protection juridique des cantons ou de la Constitution stipulent clairement que les décisions du préposé à la protection des données sont annulables.	… l'annulabilité judiciaire des décisions de l'organe de contrôle est garantie proportionnellement à leur caractère contraignant