Révision de la loi sur la protection des données (LPD)

Check-list pour un état des lieux en matière de protection des données

Cette check-list est destinée à aider les institutions à

- dresser un état des lieux de leur situation sur le plan de la protection des données;
- déterminer et évaluer la situation actuelle pour ce qui concerne le traitement des données personnelles des personnes physiques (en premier lieu les client·es et les collaborateur·trices; et
- en dégager les mesures et les modifications nécessaires dans la perspective de l'entrée en vigueur de la future LPD révisée (nLPD).

Le terme «client·es» utilisé dans le présent document désigne toutes les personnes ayant besoin de soutien qui vivent et/ou travaillent en institution, ou ont recours à des prestations institutionnelles individuelles.

Cette check-list doit être comprise et utilisée comme un support et une aide pratique. Elle ne prétend à aucune exhaustivité.

N'hésitez pas à nous adresser vos questions, les conseillers juridiques d'ARTISET se tiennent à votre disposition:

- Hans-Ulrich Zürcher | 031 351 58 85 | zuercher@advokatur-zuercher.ch
- Christian Streit | 031 385 33 39 | rechtsberatung@artiset.ch
- Yann Golay | 031 385 33 36 | yann.golay@artiset.ch

Synthèse des principales dispositions de la nouvelle loi sur la protection des données

1. La **protection des données** a pour objectif de protéger les **données personnelles**, c'est-à-dire «toutes les informations qui se rapportent à une personne physique identifiée ou identifiable».

   On entend par **données personnelles sensibles**
   - Les données relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales
   - Les données relatives à l'appartenance à un groupe ethnique ou à l'origine d'une personne
   - Les données relatives à la santé et à la sphère intime
   - Les données génétiques et biométriques (p. ex. l'ADN, les empreintes digitales, l'hémogramme résultant d'une prise de sang)
   - Les données relatives aux poursuites ou sanctions administratives et pénales.

2. Est considérée comme **traitement de données** «toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données».

3. Est considéré comme un **fichier** «tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée». La tenue **d'un registre des activités de traitement** devient obligatoire (cf. annexe 2).

4. **Profilage**
   Le profilage désigne le traitement *automatisé* de données personnelles dans le but d'établir des modèles de comportement et des profils de la personnalité (p. ex. situation économique, santé, préférences personnelles, intérêts, etc.)
   Lorsque le couplage de données permet d'évaluer des aspects essentiels de la personnalité (c'est p. ex. le cas lors du traitement de données personnelles sensibles), il existe un risque accru de violation des droits de la personnalité. Il est alors nécessaire d'obtenir le consentement exprès de la personne concernée.

5. **Analyse des risques/analyse d'impact sur la protection des données**
   Évaluation visant à déterminer si le traitement envisagé de données personnelles peut constituer un risque pour les droits de la personne concernée. Pour pouvoir évaluer ce risque potentiel, il est nécessaire d'apprécier au préalable le risque d'impact et la gravité du dommage potentiel. Il convient d'examiner et de décider si le traitement des données est justifiable au regard des risques qu'il implique et de quelle manière les risques identifiés peuvent, autant que possible, être minimisés. L'analyse doit être conservée pendant 2 ans.

6. Champ d'application de la LPD et application des lois cantonales sur la protection des données

La Confédération réglemente par des dispositions ad-hoc de la LPD les conditions régissant le traitement des données par les autorités fédérales et par les particuliers. Les cantons ont la compétence de réglementer eux-mêmes le traitement des données par des organes cantonaux.
De nombreuses législations cantonales désignent par analogie comme organes cantonaux également des personnes privées (associations de droit privé, fondations, etc.) chargées d'exécuter des tâches de droit public. C'est notamment le cas des institutions qui remplissent des tâches d'aide sociale institutionnelle sur la base d'un contrat de prestations avec le canton. Dans ce cadre, elles sont soumises non à la LPD mais à la législation cantonale en matière de protection des données.

7. Licéité du traitement de données

Un traitement de données est licite dans les cas suivants:

- lorsqu'il y a consentement libre et éclairé (possible sans condition de forme) de la personne concernée, ou
- s'il est prévu par la loi, ou
- si la personne concernée a rendu ses données accessibles et ne s'est pas expressément opposée à leur traitement, ou
- si le traitement se justifie par des considérations d'intérêt public ou privé prépondérantes. L'exécution d'un contrat existant (contrat de travail ou d'assistance, p.ex.) relève ainsi, entre autres, de l'intérêt privé.

8. Conseiller·ères à la protection des données en entreprise

Fonction/tâches:

- contrôle le traitement des données personnelles au sein de l'institution et intervient en cas de violation des dispositions légales en la matière
- a accès à tous les fichiers et traitements de données
- dresse un inventaire des fichiers
- élabore des directives et des instructions pour garantir la protection des données
- procède au préalable à des analyses des risques et des risques d'impact sur la protection des données, et les documente

Qualités/statut

- peut être un·e collaborateur·trice de l'institution ou une tierce personne mandatée
- dispose des connaissances techniques nécessaires
- occupe une place dans l'organisation/la hiérarchie de manière à éviter tout conflit d'intérêts (une solution possible est que la personne rapporte directement au comité/conseil de fondation)

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
1	**Généralités / Situation de départ**				
1.1	L'institution planifie-t-elle et coordonne-t-elle la protection systématique des données à l'interne?		▪ Définir les principes directeurs du concept de protection des données. ▪ Intégrer la protection des données dès le départ pour chaque traitement de données.		
1.2	À quel moment et de quelle manière la thématique «protection des données» est-elle abordée et la situation évaluée par: ▪ le conseil de fondation/le comité? ▪ la direction?		▪ Adoption d'un concept de protection des données par le conseil de fondation/comité. ▪ Partie intégrante de la gestion des risques, la protection des données est régulièrement traitée au niveau de la direction.		
1.3	Les principes du traitement et de la protection des données sont-ils déjà documentés (concept de protection des données, règlements et directives internes, etc.)?		▪ Élaborer un concept de protection des données. ▪ Édicter une directive sur la protection des données.		
1.4	Des incidents ou problèmes notables concernant la protection des données se sont-ils déjà produits?		Tenir compte de l'expérience acquise.		
1.5	L'institution relève-t-elle (en tout ou en partie) de la législation cantonale en		▪ Déterminer la législation applicable. ▪ S'assurer que la situation effective est en conformité avec les exigences du droit cantonal et/ou fédéral s'appliquant en l'espèce.		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
	matière de protection des données?		▪ Dans le cas où le droit applicable est le droit cantonal, s'assurer d'être informé et de saisir les implications des potentiels futurs changements de législation.		
1.6	Sous quelle forme les données sont-elles traitées (électroniquement/sur papier)?		▪ Se déterminer en connaissance de cause sur la forme à adopter pour l'avenir. ▪ Assurer l'implémentation informatique selon une procédure bien définie.		
2	**Responsabilité de la protection des données au sein de l'institution**				
2.1	Évaluation critique des règles applicables/responsabilités en vigueur?		Intégrer l'expérience acquise dans la réglementation à venir.		
2.2	La responsabilité est-elle déjà définie?		▪ Désigner une personne responsable (collaborateur·trice ou personne externe). ▪ Définir le cahier des charges. ▪ Assurer à la personne responsable une formation initiale ainsi qu'une formation continue.		
3	**Collectes des données**				
3.1	Quelles sont les collectes de données existantes?		Établir un registre des collectes de données, à mettre régulièrement à jour. *Remarque:* La liste des exigences à respecter en ce qui concerne ce registre est détaillée dans l'annexe 2.		
3.2	Que contiennent ces collectes de données?		Dresser l'inventaire des dossiers existants.		
3.3	Comment et par qui sont-elles effectuées?		Coordination de l'exécution et de la standardisation des collections de données.		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
3.4	L'institution procède-t-elle à des traitements électroniques *automatisés* de données personnelles particulièrement sensibles en vue d'établir des modèles de comportement et des profils de personnalité (p. ex. situation économique, santé, préférences personnelles, intérêts, etc.)?		Obtenir le consentement explicite de la personne concernée.		
4	**Sécurité des données**				
4.1	Le traitement des données s'effectue-t-il par le biais de l'infrastructure de l'institution ou de celle d'un fournisseur d'accès?		Établir des règles contractuelles avec le prestataire en ce qui concerne le respect de la sécurité des données.		
4.2	Existe-t-il au sein de l'institution des mesures techniques et organisationnelles de protection des données traitées?		▪ Examiner les mesures existantes et, le cas échéant, en optimiser la sécurité. ▪ Réglementer les droits d'accès de manière appropriée. ▪ Bloquer l'accès aux personnes non autorisées.		
4.3	Comment est réglementé l'accès aux données personnelles au sein de l'institution? Existe-t-il des règles particulières pour l'accès aux données personnelles sensibles?		Définir l'accès à chaque collecte de données, de manière fonctionnelle mais aussi restrictive que possible en ce qui concerne les données personnelles sensibles.		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
4.4	Est-il garanti que toutes les données importantes sont disponibles dans un délai raisonnable?		▪ Contrôler et adapter les capacités techniques. ▪ Définir les règles d'accès de manière à assurer en permanence la présence d'au moins une personne autorisée.		
4.5	Les données sont-elles suffisamment protégées contre le vol, la falsification, la destruction, etc.?		Vérifier et, le cas échéant, adapter les autorisations d'accès et la configuration technique (au niveau informatique et physique, p. ex. la conservation des dossiers sous clé).		
4.6	Transfert de données: ▪ De quelle manière les données personnelles sont-elles transférées dans l'institution et vers l'extérieur? ▪ Le transfert de données par courrier électronique est-il sécurisé?		Garantir une transmission sécurisée des données par le biais de courriers électroniques cryptés ou par tout autre moyen approprié.		
5	**Admissibilité/licéité du traitement des données**				
5.1	Existe-t-il un consentement suffisant des personnes concernées ou une autorisation légale spécifique pour chaque traitement de données?		Actualiser les contrats de travail/d'hébergement existants ou compléter les nouveaux contrats avec le paragraphe suivant, par analogie: *«En signant le présent contrat, la personne concernée autorise expressément XXX [nom de l'INSTITUTION] à traiter les données personnelles communiquées, dans la mesure où cela est prévu et autorisé par la loi ou nécessaire à l'exécution du présent contrat, et tant que la personne concernée ne s'y oppose pas expressément.»*		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
5.2	Les données sont-elles traitées dans un but défini?		Définir les buts du traitement des données et les consigner par écrit.		
5.3	Les données recueillies sont-elles traitées dans le cadre du but défini?		Procéder à des contrôles périodiques (sondages ou contrôles aléatoires) du traitement de données.		
5.4	Est-ce que le·la client·e a rédigé des directives anticipées ou un mandat pour cause d'inaptitude?		▪ Classer les documents existants dans le dossier des client·es. ▪ Recommander aux client·es de rédiger des directives anticipées/un mandat pour cause d'inaptitude.		
6	**Utilisation/publication d'images/d'enregistrements sonores de client·es et de collaborateur·trices**				
6.1	L'institution réalise-t-elle et utilise-t-elle des enregistrements visuels/sonores? À quelles fins?		Faire figurer cette thématique dans l'inventaire des traitements de données.		
6.2	Comment le consentement des personnes concernées est-il obtenu pour une utilisation à des fins de publication?		Le consentement pour une utilisation à des fins de publication n'est juridiquement valable que s'il est donné librement et expressément, en toute connaissance des prises de vue ou enregistrements réalisés et de leur finalité dans chaque cas, et dans la mesure où il peut être révoqué. *Remarque* Un consentement formulé de manière générale dans le contrat de travail/d'hébergement est insuffisant.		
7	**Proportionnalité du traitement des données**				
7.1	Le traitement des données réalisé jusque-là se limite-t-il au strict nécessaire?		Limitation de la collecte de données à la finalité du traitement (p. ex. contrat de travail).		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
7.2	Est-il possible de garantir que les données collectées à des fins autorisées, ne sont traitées que dans ce but, et ne seront pas utilisées à d'autres fins?		Intégrer l'obligation de préciser l'affectation et la finalité dans le concept de protection des données.		
7.3	Les données sont-elles collectées et stockées «préventivement» (sans objectif clair et concret)?		Intégrer l'interdiction de la collecte «préventive» dans le concept de protection des données.		
7.4	Peut-on garantir que les données recueillies ne seront conservées que le temps nécessaire à leur traitement?		Faire figurer une limite de conservation à ne pas dépasser dans le concept de protection des données. *Remarque* Voir également, en ce qui concerne la notion de traitement nécessaire ou requis, les rubriques «Archivage» et «Suppression des données».		
8	**Communication/transmission de données à des tiers**				
8.1	Les données concernant une curatelle sont-elles communiquées?		Documenter la notification ou établir un procès-verbal.		
8.2	Des données sont-elles transmises à des tiers (autorités, médecins/hôpitaux, assureurs, etc.)?		▪ Informer la personne concernée. ▪ Prévoir un transfert sécurisé des données.		
8.3	Des données sont-elles communiquées à l'étranger?		▪ Procéder à une évaluation des risques (spécifiques à chaque pays) avant de transférer des données (le cas échéant, après en avoir discuté avec votre prestataire TIC). ▪ En informer les personnes concernées.		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
			Remarque Est également considéré comme transfert de données hors de Suisse le fait de stocker des données dans un cloud sur une infrastructure de serveur qui se trouve physiquement à l'étranger.		
9	**Information des personnes concernées sur le traitement des données**				
9.1	Quand et comment les personnes concernées sont-elles informées du traitement de leurs données?		▪ Veiller à ce que les personnes concernées soient informées, le cas échéant adapter les procédures existantes. ▪ Dans le cas d'une collecte planifiée de données, les informations suivantes doivent être communiquées au moment où la collecte est réalisée: - Le nom/les données de contact de la personne en charge de la protection des données. - La finalité du traitement des données. - La période d'utilisation des données. - Le ou la destinataire, dans le cas où les données sont communiquées à des tiers. *Remarque* «Collecte de données planifiée» indique que la collecte de donnée est voulue. Recommandation: l'information sur le traitement des données est toujours donnée par écrit (dans le contrat de travail/d'établissement ou dans un document annexe à ces contrats).		
9.2	Une déclaration de confidentialité figure-t-elle sur le site Internet de l'institution?		Vérifier la déclaration de confidentialité existante, le cas échéant en intégrer une au site de l'institution.		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
10	**Droits d'accès/de consultation des personnes concernées**				
10.1	Comment sont garantis les droits d'une personne à accéder et à consulter les données la concernant?		Intégrer les droits d'accès/de consultation dans le concept de protection des données en tenant compte des exigences suivantes: ▪ Les droits d'accès/de consultation sont en principe garantis à tout moment et sans condition. ▪ Gratuité de principe (sauf en cas d'effort disproportionné; la facturation des frais doit alors être communiquée à l'avance). ▪ La limitation ou le refus en cas d'intérêt public ou privé prépondérant constitue l'exception, et ses conditions sont clairement définies.		
11	**Transfert de données aux personnes concernées**				
11.1	Comment leurs données sont-elles transmises aux personnes concernées?		Donner un aperçu et documenter la manière dont le transfert aux personnes concernées s'est fait jusqu'à présent.		
11.2	L'institution est-elle en mesure de transmettre à l'avenir des données personnelles «dans un format électronique courant»?		Prendre les mesures nécessaires pour pouvoir transmettre des données par voie électronique.		
12	**Dossiers du personnel**				
12.1	Le service du personnel tient-il un dossier unique et complet pour chaque collaborateur·trice?		Toutes les données pertinentes d'un·e collaborateur·trice doivent être rassemblées dans un seul et même dossier.		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
12.2	Qui y a accès?		Réglementer l'accès de manière claire et éventuellement différenciée.		
12.3	Les données particulièrement sensibles sont-elles protégées de manière spécifique/conservées séparément?		Vérifier la protection existante et l'améliorer le cas échéant. *Remarque* Les certificats et rapports médicaux, les informations de l'assurance accidents, de l'assurance d'indemnités journalières en cas de maladie et de l'assurance invalidité, les informations sur les activités syndicales, etc. sont à protéger tout particulièrement.		
12.4	Existe-t-il des «dossiers secrets» (auprès de la hiérarchie)?		Les «dossiers secrets» doivent impérativement être proscrits et détruits.		
13	**Dossiers des client·es**				
13.1	Un dossier complet est-il établi pour chaque client·e?		Fournir un aperçu et documenter la manière dont ces dossiers sont actuellement gérés.		
13.2	Qui gère ces dossiers?		Fournir un aperçu et documenter la manière dont ces dossiers sont actuellement gérés.		
13.3	Qui a accès aux dossiers?		Réglementer l'accès de manière claire et éventuellement différenciée.		
13.3	Les données particulièrement sensibles sont-elles protégées de manière spécifique/conservées séparément?		Vérifier la protection existante et l'améliorer le cas échéant. *Remarque* Les certificats et rapports médicaux, les informations sur les traitements médicaux, les médications et les thérapies, les informations de l'assurance accidents, de l'assurance d'indemnités journalières en cas de maladie et de		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
			l'assurance invalidité, les informations relatives à la confession, la sphère intime, etc. sont à protéger tout particulièrement.		
14	**Archivage des données**				
14.1	Sous quelle forme les données sont-elles conservées actuellement?		Encourager par principe un archivage numérique. *Remarque* La conservation de documents sur papier n'est que rarement obligatoire (p. ex. pour le rapport de gestion et le rapport de révision; art. 958 f al. 2 CO). Les données doivent être conservées séparément selon leur nature, de manière structurée, datée et chronologique.		
14.2	Combien de temps les données sont-elles conservées actuellement?		Définir les standards d'archivage à appliquer (dans le concept de protection des données ou dans un concept d'archivage dédié) en tenant compte des délais de conservation légaux ou en se basant sur les délais de prescription généraux fixés par la législation fédérale et les dispositions cantonales (p.ex. dans la loi sur l'archivage, celle relative à l'aide sociale, etc.). *Remarque* Les dispositions fédérales en matière de conservation et les délais de prescription sont exposés dans l'annexe 1.		
14.3	Qui a accès aux archives?		Réglementer clairement l'accès (selon le principe: autant de personnes que nécessaire, aussi peu que possible).		
14.4	La sécurité des données archivées est-elle garantie?		▪ Vérifier ce qui touche à la sécurité de manière générale. ▪ Mesures de protection des données archivées contre le vol, la destruction (par l'eau, le feu, la vermine, etc.). ▪ Protection des données archivées électroniquement contre la modification, la suppression, etc.		

#	Thématique / Points à contrôler	Résultat de l'évaluation Situation actuelle	Mesures recommandées	Délai	Personne responsable
			▪ Assurer la lisibilité future des données archivées électroniquement.		
15	**Suppression des données**				
15.1	La suppression des données s'effectue-t-elle dans le respect des dispositions légales?		▪ S'assurer que les données électroniques effacées sont effectivement définitivement supprimées. ▪ Détruire les données physiques sur place (en les passant à la déchiqueteuse) ou dans des conteneurs spéciaux pour contenu à déchiqueter.		
15.2	Les délais de suppression sont-ils réglementés et définis de manière différenciée?		Réglementer les délais de suppression (dans le concept de protection des données ou dans un concept spécifique dédié à l'effacement des données), en tenant compte ▪ des délais de conservation définis par la loi, ▪ du principe selon lequel la durée d'archivage doit être limitée de manière appropriée.		
16	**Formation et sensibilisation des collaborateur·trices**				
16.1	De quelle manière le personnel est-il formé et sensibilisé à la protection des données ▪ de manière générale? ▪ concrètement?		▪ S'assurer que les règles internes relatives à la protection des données (concept de protection des données, directives, etc.) soient connues et comprises. ▪ Assurer de manière régulière une formation et une sensibilisation sur un plan général, dans le cadre d'une formation continue à l'interne. ▪ Assurer un conseil et un soutien individuel en situation pour le personnel, guider et conseiller l'encadrement, resp. la personne en charge de la protection des données dans l'entreprise sur les précautions correctes à respecter, en se basant sur les erreur/les lacunes constatées.		

Annexe 1 : Délais de conservation / Délais de prescription généraux, selon la législation fédérale

Objet	Délai de prescription (maximum)	Base légale	Remarques
Livres de comptes, rapport de gestion, pièces comptables importantes	10 ans	Art. 957ss. CO	La comptabilité «enregistre les transactions et les autres faits nécessaires à la présentation du patrimoine, de la situation financière et des résultats de l'entreprise (situation économique)» (art. 957a al. 1 CO). Les obligations qui en découlent impliquent de conserver en particulier les livres de comptes et les pièces comptables, qui peuvent, selon les cas, inclure également la correspondance commerciale relative à une transaction. Le cas échéant, les contrats de travail et les contrats d'hébergement peuvent aussi être considérés comme des pièces justificatives essentielles.
Obligations générales relevant du droit du travail	5 ans	Art. 128 CO	
Données importantes pour le certificat de travail	10 ans		Délai fixé par la jurisprudence
Données salariales et documents relevant du droit du travail qui peuvent également être importants au regard des dispositions légales en matière de fiscalité	10 ans	Art. 958f al. 1 CO ; art. 126 al. 3 LIFD	
Documentation relative au respect des obligations découlant de la législation sur le travail (en particulier les contrôles du temps de travail)	5 ans	Art. 73, al. 2, de l'ordonnance 1 relative à la loi sur le travail	
Dommages et intérêts/réparation en de lésions corporelles ou décès d'une personne	3/20 ans	Art. 60 al. 1bis et art. 128a CO	Peut concerner d'ancien·nes collaborateur·trices et d'ancien·nes client·es
Infractions relevant de la discrimination en fonction du genre	3 mois	Art. 8, paragraphe 2, de la loi sur l'égalité (LEg)	

Prestations ou cotisations aux assurances sociales, resp. obligation de restitution.	5 ans	Art. 24 et 25 LPGA	Il est toutefois recommandé de conserver les dossiers personnels pendant 10 ans en cas d'*accident* survenu pendant les rapports de travail, et pendant 30 ans en cas d'accident grave ou de maladie professionnelle (recommandation ad hoc LAA n° 09/87 ; https://www.koordination.ch/fileadmin/files/ad-hoc/1987/09-87.pdf).

Annexe 2 : Exigences relatives à la tenue d'un registre des activités de traitement

Le/La responsable de la protection des données dans l'entreprise doit tenir un registre de tous les traitements de données, avec les indications minimales suivantes:

- Identité du/de la responsable de la protection des données dans l'entreprise
- Finalité du traitement
- Catégories de personnes concernées
- Catégories de données personnelles traitées
- Catégories de destinataires des données
- Durée de conservation des données personnelles ou critères de détermination de cette durée
- Description générale des mesures prises pour assurer la sécurité des données (mesures de protection techniques et organisationnelles appropriées)
- Indication de l'État concerné en cas de communication de données à l'étranger et indication des garanties permettant d'assurer une protection appropriée de ces données