Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Guide relatif aux mesures techniques et organisationnelles de la protection des données (TOM)

15 janvier 2024

TABLE DES MATIÈRES

1 Introduction 4
1.1 Loi sur la protection des données 4
1.2 Définitions 5
1.3 Principes généraux 6
1.4 Rôles 7
1.5 Mesures techniques et organisationnelles 7
1.6 Quelques outils 7
2 Traitement de données 9
2.1 Analyse d'impact 9
2.1.1 Obligation d'effectuer une AIPD 10
2.1.2 Exception à l'obligation d'effectuer une AIPD 10
2.1.3 Conseiller à la protection des données 10
2.1.4 Eléments constitutifs d'une AIPD 11
2.2 Registre 11
2.3 Annonces de violation 12
2.4 Responsables de traitement de données à l'étranger 13
3 Droits et devoirs 14
3.1 Devoir d'informer 14
3.2 Droits des personnes concernées 15
3.2.1 Droit d'accès aux données personnelles 16
3.2.2 Droit à la remise ou à la transmission des données personnelles 17
3.2.3 Droit à la destruction des données personnelles 18
3.2.4 Droit à la rectification des données personnelles 18
3.2.5 Droit à l'interdiction de traitement de données personnelles 18
3.2.6 Droit à l'interdiction de communiquer les données personnelles 19
3.2.7 Droit à la communication des mesures relatives aux données personnelles 19
3.3 Reproductibilité des procédures 19
4 Organes fédéraux 21
4.1 Bases légales 21
4.2 Traitements à des fins ne se rapportant pas à des personnes 21
4.3 Communication 22
4.4 Registre des activités de traitement 22
4.5 Annonces de violation de la sécurité des données 22
4.6 Décisions individuelles automatisées 22
4.7 Devoir d'informer 23
4.8 Droits des personnes concernées 23
4.9 Journalisation 23
4.10 Règlement de traitement 24
5 Protection des données 25

5.1 Protection dès la conception et par défaut 25
5.2 Pseudonymisation 26
5.3 Anonymisation 27
5.4 Généralisation 29
5.5 Minimisation 30
5.6 Randomisation 30
5.7 Chiffrement homomorphe 31
5.8 Données synthétiques 31
6 Infrastructure 32
6.1 Sécurité des locaux 32
6.2 Sécurité des salles de serveurs 33
6.3 Sécurité des places de travail 33
6.4 Utilisation du cloud 34
6.5 Approfondissements 35
7 Accès et traitements 36
7.1 Gestion des accès 36
7.2 Identification et authentification 36
7.3 Accès aux données 37
7.4 Accès à distance 38
7.5 Approfondissements 38
8 Cycle de vie des données 40
8.1 Saisie de données 40
8.2 Chiffrement des données 41
8.3 Sécurité des supports 42
8.4 Sauvegarde des données 42
8.5 Destruction des données 42
8.6 Niveau de sécurité et protection 43
8.7 Journalisation 44
8.8 Règlement de traitement 46
9 Partage et transfert 47
9.1 Sécurité du réseau 47
9.2 Chiffrement des messages 48
9.3 Signature des messages 49
9.4 Transmission des supports de données 50
9.5 Journalisation des transferts 50
9.6 Communication de données à l'étranger 51
9.7 Sous-traitance 52
10 Considérations finales 53
11 Références 54

1 INTRODUCTION

Ce guide est proposé par le Préposé fédéral à la protection des données et à la transparence (PFPDT). Il constitue une introduction aux risques et solutions liés à la protection des données dans les systèmes d'information actuels. Les thèmes principaux de la protection des données sont présentés sous l'angle des mesures techniques et organisationnelles envisageable, comme le chiffrement, l'anonymisation, l'authentification, etc. Ce guide est conçu comme une aide pour la mise en œuvre de mesures adéquates dans le but d'assurer une protection optimale et appropriée des données personnelles, en faisant les liens avec les règlementations et les standards actuels.

Ce guide est avant tout destiné aux personnes qui sont en charge des systèmes d'information, techniciens ou non, et qui sont confrontés directement au problème de la gestion des données personnelles, notamment des conseillers à la protection des données ou des représentants d'entreprises domiciliées en dehors de Suisse. Ce guide détaille principalement les obligations des responsables de traitement privés, mais les responsables de traitement d'un organe fédéral pourront également trouver des informations spécifiques les concernant dans la section « Organes fédéraux ».

Le guide est organisé en huit sections, qui concernent les traitements de données, les droits et devoirs, les organes fédéraux, la protection des données, l'infrastructure, les accès et traitements, le cycle de vie des données, et finalement le partage et transfert de données. Dans chaque section, nous rappelons les exigences légales et citons certains points auxquels il faut veiller lors de la conception d'un système et de sa mise en œuvre. Pour chaque point, des mesures sont proposées. Elles doivent être considérées comme des lignes directrices générales pour être ensuite adaptées aux spécificités de chaque projet et de chaque organisation. Des liens vers les standards suisses et internationaux sont aussi faits pour de plus amples informations.

Notons enfin qu'il ne s'agit pas d'un guide juridique. Si les règles essentielles de la LPD y sont présentées, c'est surtout à des fins informatives. Ce guide n'a pas pour vocation de développer, commenter ou préciser ces règles de droit et ne vise donc pas à servir de base à l'application et à l'interprétation de ces règles.

1.1 LOI SUR LA PROTECTION DES DONNÉES

La loi fédérale sur la protection des données (LPD) – en particulier les art. 7 et 8 – et l'ordonnance y relative (OPDo) – en particulier les articles 1 à 6 – sont les fondements de ce guide. Ces dispositions définissent les règles essentielles à observer. Notons également les art. 2 et 3 LPD qui en définissent le champ d'application : la LPD trouve application lorsque des données de personnes privées sont traités, avec des effets en Suisse, même si l'origine du traitement est à l'étranger.

Ce guide contient aussi les liens vers des éléments pertinents du RGPD et des standards internationaux. Bien que des liens soient souvent fait avec le RGPD, il est précisé que ce guide n'est pas une source complète pour la conformité au RGPD.

A souligner que, selon les dispositions transitoires de l'art. 69 LPD, les principes de protection des données dès la conception et par défaut (art. 7), l'analyse d'impact relative à la protection des données personnelles (art. 22) et la consultation préalable du préposé fédéral à la protection et données et à la transparence (art. 23) ne s'appliquent pas aux traitements qui ont

débuté avant l'entrée en vigueur de la LPD, soit le 1er septembre 2023, et dont ni les données traitées ni la finalité n'ont changé depuis.

Notons enfin qu'outre la LPD, il existe aussi des dispositions sur la protection des données dans la législation spécialisée, dérogeant parfois le régime de la LPD (par exemple les art. 32 et suivants de la loi sur la recherche sur l'être humain LRH). Il est donc important qu'un responsable de traitement se renseigne sur les lois spéciales qui lui sont potentiellement applicables en raison de son domaine d'activité.

1.2 DÉFINITIONS

Les termes suivants seront utilisés dans ce guide pour différencier certains concepts relatifs aux mesures organisationnelles et techniques : il s'agit de définitions propres à ce guide et qui ne sont pas directement reprises de la LPD.

- La ***sécurité des données*** regroupe toutes les mesures prises en vue d'assurer la confidentialité, l'intégrité et la disponibilité des données (ex. écoute ou modification des données en cours de transmissions).
- La ***protection des données*** regroupe toutes les mesures prises en vue de garantir les droits des personnes concernées sur leurs données personnelles (ex. sécurité des données, journalisation, *privacy by design*, …)
- Un **traitement automatisé** de données personnelles représente toute opération sur des données personnelles faite dans des systèmes de traitement automatisés.
- La notion de **risque élevé** dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Il est de la responsabilité du responsable de traitement de protéger la personnalité et les droits fondamentaux des personnes concernées, et donc de déterminer quand le risque devient élevé et de prendre les mesures nécessaires si tel est le cas.
  L'art. 22 al. 2 let. a et b LPD donne deux exemples concrets (le traitement de données sensibles à grande échelle et la surveillance systématique de grandes parties du domaine public), mais ceci n'est pas exhaustif.

Les termes suivants sont tirés de l'art. 5 LPD et seront utilisés tel quels dans ce guide.

- Les **données personnelles** sont toutes les informations concernant une personne physique identifiée ou identifiable.
- Une **personne concernée** est une personne physique dont les données personnelles font l'objet d'un traitement.
- Les **données personnelles sensibles** ou **données sensibles** sont
  - les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales,
  - les données sur la santé, la sphère intime ou l'origine raciale ou ethnique,
  - les données génétiques,
  - les données biométriques identifiant une personne physique de manière univoque,
  - les données sur des poursuites ou sanctions pénales et administratives,
  - les données sur des mesures d'aide sociale
- Un **traitement** représente toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données.
- La **communication** est le fait de transmettre des données personnelles ou de les rendre accessibles.

- Le **profilage** représente toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.
- Le **profilage à risque élevé** représente tout profilage entraînant un risque élevé pour la per-sonnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.
- Une **violation de la sécurité des données** représente toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données.
- L'**organe fédéral** est l'autorité fédérale, le service fédéral ou la personne chargée d'une tâche publique de la Confédération.
- Un ou une **responsable** du traitement est une personne privée ou un organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles.
- Un **sous-traitant** est une personne privée ou un organe fédéral qui traite des données personnelles pour le compte du responsable du traitement.

1.3 PRINCIPES GÉNÉRAUX

Le droit de la protection des données s'articule autour de certains principes généraux, applicables à tout traitement de données personnels (art. 6 LPD). Sans rentrer dans une description détaillée de ces principes – l'on renvoie sur ce point aux ouvrages juridiques spécialisés – l'on en présentera ici les grandes lignes :

- Tout traitement de données doit être licite (principe de licéité), c'est-à-dire qu'il ne doit pas enfreindre une règle de droit, y compris une règle hors de la LPD (en particulier le droit pénal, tels les art. 138 et suivants et 179 et suivants CP). En outre, un traitement de données ne doit pas porter atteinte à la personnalité de la personne concernée, sauf motif justificatif (art. 30 s. LPD). L'art. 31 al. 1 LPD cite comme motif justification le consentement de la personne concernée, la loi ou un intérêt prépondérant par rapport à celui de la personne concernée. L'al. 2 de cette disposition présente une liste non exhaustive de tels intérêts : il est important de souligner que ces intérêts entre en considération, mais ne sont pas automatiquement considérés comme prépondérant. Une analyse de cas en cas est à chaque fois nécessaire.
- Tout traitement de données doit se conformer au principe de la bonne foi et de la proportionnalité. Ce dernier principe implique de se limiter à ce qui est nécessaire pour chaque aspect du traitement : limiter la collecte aux données effectivement nécessaires pour atteindre la finalité visée, limiter les accès aux personnes qui en ont besoin pour l'accomplissement de leurs tâches, limiter les communications, la durée de conservation, etc.
- L'auteur d'un traitement de données ne peut pas faire plus avec ces données que ce qui est compatible avec le but annoncé ou reconnaissable pour la personne concernée au moment de la collecte (principe de finalité).
- Celui qui traite des données personnelles doit s'assurer qu'elles sont exactes et complètes en regard de la finalité du traitement (principe d'exactitude). Il doit donc être capable d'identifier les inexactitudes, mais aussi de les corriger.

1.4 RÔLES

En matière de protection des données, l'on identifie essentiellement les rôles suivants.

- Le ***responsable du traitement*** est la personne privée ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles (cf. ch. 1.2).
- Le ***conseiller à la protection des données*** est défini à l'art. 10 LPD (cf. aussi les art. 23 et 25 à 28 OPDo). Il a essentiellement pour tâches de conseiller et de former les responsables de traitement, ainsi que de concourir à l'application des prescriptions en matière de protection de données. C'est également l'interlocuteur privilégié des personnes concernées et des autorités en charge de la protection des données.
- Le ***sous-traitant*** est la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement. D'une manière générale, il est tenu aux mêmes principes et obligations que le responsable du traitement (principe de l'art. 6 LPD, privacy by design, …). Quelques dispositions règlent spécifiquement certains aspects de la relation sous-traitant – responsable du traitement (notamment les art. 9, 24 al. 3 et 25 al. 4 LPD, ainsi que les art. 7 et 17 al. 2 OPDo).
- Le ***préposé fédéral à la protection des données et à la transparence (PFPDT)*** effectue des tâches de surveillance et de conseil auprès des personnes privées et des organes fédéraux. Il tient également un registre public, auquel les organes fédéraux sont tenus de déclarer leurs propres registres d'activité en matière de protection des données (art. 12 al. 4 LPD).
- Le ***préposé cantonal à la protection des données (et à la transparence)*** effectue des tâches similaires auprès des organes cantonaux et communaux.

1.5 MESURES TECHNIQUES ET ORGANISATIONNELLES

Les mesures techniques et organisationnelles (art. 7 et 8 LPD, art. 3 OPDo) permettent de réduire les risques liés à un système d'information. Le responsable du traitement assume la mise en œuvre de telles mesures.

- Les ***mesures techniques*** se rapportent directement à l'aspect technique du système d'information (anonymisation, cryptage, authentification, etc.).
- Les ***mesures organisationnelles*** sont plus larges et se rapportent plutôt à l'environnement autour du système, aux personnes qui l'utilisent et à la manière dont il est utilisé (politique des habilitations, registre des traitements et des activités, etc.).

Les deux types de mesures sont indispensables. C'est de manière combinée qu'elles permettent d'éviter la destruction et la perte des données, ainsi que les erreurs, la falsification, les accès non autorisés, etc. Ces mesures sont à implémenter sur l'ensemble du cycle de vie des données contenues dans un système d'information et sont applicables à tous les niveaux du système.

1.6 QUELQUES OUTILS

La LPD propose notamment deux outils destinés à orienter les responsables de traitement et à les aider à satisfaire à leurs obligations :

- Codes de conduite (art. 11 LPD, art. 12 OPDo) : il s'agit de codes de bonnes pratiques en matière de protection des données, développés par les associations professionnelles, sectorielles ou économiques dont les statuts leur permettent de défendre les intérêts de leurs membres. Ces associations peuvent soumettre leur code au PFPDT, lequel émettra un avis qui sera publié. L'on souligne ici qu'il ne s'agit pas

d'une décision du PFPDT, par laquelle il validerait ou rejetterait le code de conduite, mais bien d'un simple avis.

- Les certifications (art. 13 LPD) : les fournisseurs de logiciels et de systèmes, ainsi que les responsables de traitement et leurs sous-traitants peuvent faire certifier leurs produits par un organisme agréé indépendant. Par ces certifications, ils démontrent ainsi satisfaire aux exigences de la LPD.

Outre de permettre la conformité aux exigences de la protection des données, ces outils donnent d'autres avantages. Aux conditions de l'art. 22 al. 5 LPD, le responsable du traitement qui suit un code de conduite ou dispose d'une certification, peut renoncer à réaliser une analyse d'impact selon l'art. 22 LPD. De plus, ces instruments peuvent également fonder des communications de données à l'étranger, quand bien même l'Etat considéré ne garantirait pas un niveau de protection des données adéquat (art. 16 LPD et art. 12 OPDo).

Standards					Mesures sur...	Lois / Règlements			Autres
COBIT	BSI	CH-MS	ISO 27001	ISO 27701		LPD	OPdo	RGPD	EDPB[1]
X	X	X	X		**Partage et transfert des données (externe)**	X	X	X	
X	X	X	X		**Traitement (interne)**	X	X	X	
X	X	X	X		**Infrastructure**	X	X	X	
				X	**Données elles-mêmes**	X	X	X	X
					Personnes concernées	X	X	X	X

Sécurité des données

Protection des données

Table 1: Mesures à prendre sur les éléments du traitement de données, les lois qui les exigent, ainsi que les normes qui les couvrent.[2] Par souci de clarté, l'on rappellera la distinction faite dans ce guide entre « protection des données » et « sécurité des données » (cf. ch. 1.2 ci-dessus).

La « Norme minimale pour améliorer la résilience informatique » (notée CH-MS [1]) est un guide pratique, simple, et contient les liens vers les autres standards (ISO [2], COBIT [3], BSI [4], et NIST [5]). Nous nous référerons à la CH-MS dans les chapitres suivants pour des informations complémentaires.

[1] European Data Protection Board, anciennement appelé "Groupe Article 29".

[2] Ce guide concerne le traitement des données personnelles ; le traitement d'autres types de données n'est donc pas visé et peut être soumis à d'autres lois, non cité dans ce guide.

2 TRAITEMENT DE DONNÉES

Le responsable du traitement assume la responsabilité quant à la protection et à la sécurité des données personnelles qu'il traite ou fait traiter. La LPD lui impose notamment deux instruments spécifiques à mettre en œuvre si les conditions sont réunies : l'analyse d'impact relative à la protection des données et le registre des activités de traitement. En outre, le responsable du traitement peut avoir des obligations d'annonce en cas de violation de la sécurité des données, ou l'obligation de nommer un représentant en Suisse s'il est lui-même basé à l'étranger. Ces éléments seront abordés dans le présent chapitre.

D'autres obligations du responsable du traitement seront détaillées dans les sections « Droits et Devoirs » et « Protection des Données ».

2.1 ANALYSE D'IMPACT

Une analyse d'impact sur la protection des données est exigée par l'art. 22 LPD, respectivement l'art. 35 RGPD, « lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée ».

Suivant l'art. 23 LPD le responsable du traitement a en outre l'obligation de consulter le PFPDT lorsque l'analyse d'impact montre qu'un risque élevé subsiste malgré les mesures de mitigation envisagées.

L'élaboration d'une analyse d'impact sur la protection des données (AIPD ou PIA pour Privacy Impact Assessment) par un responsable du traitement a pour buts :

- l'identification et la résolution des problèmes de protection de données à une phase préliminaire, réduisant ainsi la complexité et le coût des solutions ;
- de démontrer le respect des principes de la protection des données, y compris sur les questions de droit d'accès des personnes concernées ;
- de prouver la conformité du traitement, s'agissant notamment de la conception du système, des mesures de mitigation des risques et des contrôle mis en œuvre pour s'assurer du respect des droits des personnes concernées ;
- de déterminer si le traitement présente malgré tout des risques pour la personnalité ou les droits fondamentaux des personnes concernées au sens de l'article 23 al. 1 LPD.

L'AIPD est un instrument important de la LPD. Elle fournit des informations sur la façon dont les risques ont été évalués et sur les mesures prévues pour les gérer. Ces éléments sont en outre particulièrement utiles pour la gestion et l'évaluation d'incidents telle une violation de la sécurité des données. On peut trouver un aide-mémoire sur l'AIPD sur le site du PFPDT[3]. Des guides et modèles sont également disponibles sur les sites de la CNIL[4] , de l'ICO[5] et de l'EDPB[6].

Dans cette section, nous aborderons les points suivants :

- Quand doit-on effectuer une analyse d'impact ?
- A quelles conditions une analyse d'impact est-elle facultative ?

[3] Analyse d'impact relative à la protection des données personnelles (admin.ch)
[4] L'analyse d'impact relative à la protection des données (AIPD) | CNIL
[5] Data protection impact assessments | ICO
[6] ARTICLE29 - Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)

- Comment effectuer une analyse d'impact ?

2.1.1 Obligation d'effectuer une AIPD

Avant de débuter un traitement de données, le responsable du traitement doit procéder à une analyse d'impact si le traitement est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées. A noter que, selon les dispositions transitoires (art. 69 LPD), une analyse d'impact doit également être réalisée pour des traitements ayant débuté avant l'entrée en vigueur de la nouvelle LPD, si la finalité du traitement change ou si de nouvelles données sont collectées.

L'article 22 al. 2 LPD précise que l'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque est notamment donné en cas de traitement de données sensibles à grande échelle ou lors de surveillance systématique de grandes parties du domaine public.

Si le responsable du traitement envisage d'effectuer plusieurs opérations de traitement semblables, il peut établir une analyse d'impact commune.

A noter enfin qu'un responsable du traitement privé n'est pas tenu à une AIPD s'il doit effectuer le traitement de données en vertu d'une obligation légale (art. 22 al. 4 LPD).

2.1.2 Exception à l'obligation d'effectuer une AIPD

Une analyse d'impact représente un investissement qui peut être important. Pour une entreprise qui effectue régulièrement des traitements de données impliquant une AIPD, il peut être intéressant d'envisager des mesures lui permettant de s'y soustraire.

L'article 22 al. 5 LPD offre ainsi deux possibilités au responsable du traitement privé :

Les certifications : Le responsable du traitement peut recourir à un produit, un système ou un service certifié, au sens de l'art. 13 LPD. Ces certifications sont délivrées par des organismes de certifications indépendants et agréés.

Les codes de conduite : Il peut également suivre un code de conduite au sens de l'art. 11 LPD, répondant en outre aux trois conditions suivantes : le code repose lui-même sur une analyse d'impact ; il prévoit des mesures pour protéger la personnalité et les droits fondamentaux ; il a été soumis au PFPDT. Ces codes sont élaborés par les associations professionnelles, sectorielles et économiques, autorisées de par leurs statuts à défendre les intérêts économiques de leurs membres.

Le recours à ces instruments justifie une dérogation, dès lors qu'en s'y référant, le responsable du traitement travaille dans un environnement dont la conformité à la protection des données a déjà été éprouvée.

2.1.3 Conseiller à la protection des données

A noter enfin le rôle du conseiller à la protection des données (art. 10 LPD et 23 OPDo). Lorsque malgré les mesures prévues, l'AIPD montre que les risques restent importants, le responsable du traitement doit normalement consulter le PFPDT (art. 23 LPD). Toutefois, si le responsable du traitement recourt à un conseiller à la protection des données « qualifié », cette consultation du PFPDT n'est pas nécessaire. Pour être « qualifié », le conseiller à la protection des données doit remplir les conditions suivantes (art. 10 al. 3 LPD) :

- Il doit exercer sa fonction de manière indépendante par rapport au responsable du traitement et sans recevoir d'instruction de celui-ci. Cela n'implique pas forcément qu'il

soit externe à l'entreprise. S'il est interne, il faudra toutefois prendre des mesures organisationnelles afin de lui garantir cette indépendance.
- Il n'exerce pas de tâches incompatibles avec sa fonction de conseiller à la protection des données (conflits d'intérêts).
- Il dispose des connaissances professionnelles nécessaires.
- Ses coordonnées sont publiées par le responsable du traitement et communiquées au PFPDT (qui mets à disposition un portail de notification pour ce faire)[7].

Mesures à envisager:

- Se renseigner sur l'existence d'outils certifiés correspond à ses besoins et comparer les conditions de leur usage avec l'investissement relatifs à l'élaboration répétée d'AIPD.
- Se renseigner sur l'existence d'un code de conduite répondant aux conditions requises et comparer l'investissement nécessaire pour en observer les prescriptions avec l'investissement relatifs à l'élaboration répétée d'AIPD.
- Envisager de nommer un conseiller à la protection des données, répondant aux conditions de l'art. 10 al. 3 LPD.

2.1.4 Eléments constitutifs d'une AIPD

Selon l'article 22 al. 3 LPD, une AIPD doit contenir :

- une description du traitement envisagé ;
- une évaluation des risques pour la personnalité et les droits fondamentaux des personnes concernées ;
- la description des mesures prévues pour mitiger les risques en question ;
- une évaluation du risque résiduel, tenant compte des mesures prises pour le limiter (art. 23 LPD).

L'AIPD est l'instrument de base pour la gestion du risque, c'est pourquoi elle doit être réalisée avec tout le soin et la rigueur nécessaire. Une AIPD bien menée permet non seulement d'identifier et de réduire ou éliminer les risques, mais aussi de mieux réagir en cas d'incident.

2.2 REGISTRE

En principe, le responsable du traitement a l'obligation de tenir un registre des activités de traitement (art. 12 al. 1 LPD). Les sous-traitants ont la même obligation.

Responsables de traitement

Suivant l'art. 12 al. 2 LPD, le registre du responsable du traitement contient au moins les informations suivantes :

- l'identité du responsable du traitement ;
- la finalité du traitement ;
- une description des catégories de personnes concernées ;
- une description des catégories de données personnelles traitées ;
- les catégories de destinataires ;
- dans la mesure du possible, le délai de conservation des données personnelles ; à défaut les critères pour en déterminer la durée ;

[7] Portail d'annonce : https://www.dpo-reg.edoeb.admin.ch

- dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données selon l'art. 8 LPD ;
- si les données vont être communiquées à l'étranger, le nom de l'Etat concerné et les garanties prévues (art. 16 al. 2 LPD), tel que détaillé dans la section Communication de données à l'étranger.

Sous-traitants
Les sous-traitants doivent tenir un registre comportant au moins les indications suivantes (art. 12 al. 3 LPD) :

- l'identité du sous-traitant ;
- l'identité du responsable du traitement ;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données selon l'art. 8 LPD ;
- si les données vont être communiquées à l'étranger, le nom de l'état concerné et les garanties prises (art. 16 al. 2 LPD), tel que détaillé dans la section Communication de données à l'étranger ;

Exceptions
Les entreprises et autres organismes de droit privé employant moins de 250 collaborateurs au 1er janvier d'une année, ainsi que les personnes physiques, sont exemptés de tenir un registre des activités, sauf si (art. 12 al. 5 LPD et 24 OPDo) :

- le traitement porte sur des données sensibles à grande échelle ;
- le traitement constitue un profilage à risque élevé.

Mesures à envisager:

- Vérifier régulièrement si les traitements de données (et le nombre d'employés) impliquent une obligation de tenir un registre.
- Lorsque l'on prévoit un nouveau traitement de données, envisager l'obligation de devoir tenir un registre dès le début du processus, afin que la saisie de données y soit facilitée.

2.3 ANNONCES DE VIOLATION

Si, malgré les mesures de protection mises en place, une violation de la sécurité survient et entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne, le responsable du traitement doit l'annoncer au PFPDT dans les meilleurs délais (art. 24 al. 1 LPD). Si la violation se produit chez un sous-traitant, celui-ci doit prévenir le responsable du traitement dans les meilleurs délais également (art. 24 al. 3 LPD).

Comme précisé à l'article 24 al. 2 LPD, l'annonce au PFPDT doit indiquer au moins la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées pour y remédier. De plus, le responsable du traitement doit informer la personne concernée lorsque cela est nécessaire pour sa protection ou lorsque le PFPDT l'exige. De plus amples détails sur les modalités de l'annonce sont indiqués à l'art. 15 OPDo.

Le responsable du traitement peut restreindre l'information à la personne concernée, la différer ou y renoncer dans les cas suivants (art. 24 al. 5 LPD) :

- l'intérêt prépondérant d'un tiers l'exige ;
- lorsque le responsable du traitement est tenu au secret de par la loi ;

- l'information est impossible à fournir ou exige des efforts disproportionnés ;
- l'information de la personne concernée peut être garantie de manière équivalente par une communication publique.

Mesures à envisager:

- Se renseigner sur les bonnes pratiques pour se prémunir des hackers ; ce guide en fait une présentation aux sections Accès et traitements et Partage et transfert. Il existe aussi des documents de bonnes pratiques spécialisés[8], ainsi que de nombreuses d'entreprises spécialisées qui pourront conseiller directement selon les besoins spécifiques.
- Préparer un document type ou un protocole pour le cas où une violation de la sécurité des données surviendrait, afin de réduire le délai d'annonce sur le portail de notification DataBreach.[9]
- Avoir un protocole clair pour la gestion de tels incidents, qui inclut une manière réaliste de contacter les personnes concernées.

2.4 RESPONSABLES DE TRAITEMENT DE DONNÉES À L'ÉTRANGER

Les articles 14 et 15 LPD concernent les responsables de traitements ayant leur siège ou leur domicile (soit des entreprises ou des personnes physiques) à l'étranger. Ceux-ci doivent désigner un représentant en Suisse lorsqu'il traite des données personnelles concernant des personnes en Suisse et que ce traitement rempli les conditions suivantes :

- le traitement est en rapport avec l'offre de biens ou de services ou le suivi de comportement de personnes en Suisse ;
- il s'agit d'un traitement à grande échelle ;
- il s'agit d'un traitement régulier ;
- le traitement présente un risque élevé pour la personnalité des personnes concernées.

Le responsable du traitement doit publier le nom et l'adresse de son représentant, celui-ci étant le point de contact pour le PFPDT et les personnes concernées. Le représentant doit tenir un registre similaire à celui d'un responsable du traitement (art. 15 al. 1 LPD) et fournit au PFPDT, sur demande, les indications qui y sont contenues. De même, il fournit aux personnes concernées des renseignements sur l'exercice de leurs droits sur demande.

Mesures à envisager :

- Tenir un registre comme détaillé dans la section Registre et disposer d'un protocole de transmission de l'information.
- Former un employé ou trouver un représentant qualifié pour assumer les tâches prescrites par les art. 14 et 15 LPD, notamment relatives aux droits des personnes concernées (Droits et devoirs).

[8] Small Business Guide: Cyber Security - NCSC.GOV.UK
[9] EDOEB DataBreach (admin.ch)

3 DROITS ET DEVOIRS

Tout traitement de données doit respecter les principes généraux définis à l'art. 6 LPD. Ces principes sont concrétisés par des droits dont bénéficient les personnes concernées, et notamment ceux-ci :

- *droit à être informé lors de la collecte de données (art. 19 à 21 LPD) ;*
- *droit d'accès et à la remise (portabilité) des données (art. 25 à 29 LPD) ;*
- *droit d'empêcher un traitement illicite, en demandant notamment l'arrêt du traitement, la rectification de données inexactes ou encore la destruction de données (art. 32 et 41 LPD).*

Ces aspects sont traités aux art. 13 à 20 du RGPD.

Toute personne dont les données personnelles sont traitées jouit d'un certain nombre de droits par rapport au traitement ; les responsables de traitement doivent être en mesure de garantir l'exercice de ces droits. Cette section détaille les différents droits des personnes concernées et les devoirs correspondant des responsables de traitement.

Dans ce chapitre, nous aborderons les points suivants :

- Quelles informations doivent être transmises aux personnes concernées ?
- Quels droits ont les personnes concernées sur leurs données ?
- Comment assurer que les personnes concernées puissent faire valoir leurs droits ?
- Comment assurer la reproductibilité des procédures d'exécution du droit d'accès ?

3.1 DEVOIR D'INFORMER

Les articles 19 à 21 LPD et 13 OPDo concernent le devoir d'informer et ses exceptions. Le responsable du traitement est tenu d'informer la personne concernée de manière adéquate s'agissant de la collecte de ses données personnelles, que cette collecte soit effectuée directement auprès d'elle ou non.

La personne concernée doit ainsi recevoir les informations nécessaires pour qu'elle puisse, au besoin, faire valoir ses droits et pour que la transparence des traitements soit garantie. Lorsque les données ne sont pas collectées auprès de la personne concernée, celle-ci doit recevoir l'information au plus tard un mois après la collecte ou, si cela intervient avant, au moment de la transmission des données.

Les informations doivent contenir au moins :

- l'identité et les coordonnées du responsable du traitement ;
- la finalité du traitement ;
- les destinataires ou catégories de destinataires auxquels les données sont transmises ;
- si les données ne sont pas collectées directement auprès de la personne concernée, les catégories de données traitées ;
- si ces données vont être communiquées en dehors de Suisse, le nom de l'Etat ou de l'organisme international auquel les données sont transmises, et, cas échéant, les mesures prises pour assurer une protection adéquate (art. 16 et 17 LPD).

Exceptions
L'article 20 al.1 et 2 LPD permet au responsable du traitement d'être délié de ses obligations d'informer de la collecte de données personnelles si l'une des conditions suivantes est remplie :

- la personne concernée possède déjà les informations correspondantes ;
- le traitement des données personnelles est prévu par la loi ;
- le responsable du traitement est un privé et il est lié par une obligation légale de garder le secret ;
- si les données personnelles ne sont pas collectées auprès de la personne concernée et que l'information est impossible à donner ou nécessite des efforts disproportionnés à donner.

A noter que, s'agissant des médias, il peut également être renoncé à l'information aux conditions de l'art. 27 LPD.

Restrictions
L'article 20 al. 3 et 27 LPD permettent au responsable du traitement de restreindre ou différer la communication des informations, ou y renoncer, si l'une des conditions suivantes est remplie :

- les intérêts prépondérants d'un tiers l'exigent ;
- l'information empêche le traitement d'atteindre son but ;
- ses propres intérêts prépondérants l'exigent et qu'il ne communique pas les données à des tiers.

Des exemples d'intérêts prépondérants de tiers ici seraient par exemple pour remplir son contrat avec la personne concernée ou pour garantir la sécurité du traitement. Un exemple d'intérêt prépondérant propre serait pour faire du marketing direct à la personne concernée (sans communication à des tiers).

Il existe des possibilités supplémentaires dans l'article 27 LPD pour les médias.

Décisions individuelles automatisées
L'article 21 LPD oblige également le responsable du traitement d'informer la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données automatisé et qui a des effets juridiques sur elle ou l'affecte de manière significative.

La personne concernée doit pouvoir, à sa demande, faire valoir son point de vue. Elle peut en outre exiger qu'une personne physique revoit la décision.

Des exceptions à ces règles existent dans deux cas de figure :

- lorsque la décision automatisée est en relation directe avec un contrat entre la personne concernée et le responsable du traitement et que la décision satisfait la demande de la personne concernée ;
- lorsque la personne concernée consent expressément à ce que la décision soit prise de manière automatisée.

3.2 DROITS DES PERSONNES CONCERNÉES

Outre le droit à être informé, les personnes concernées ont plusieurs autres droits concernant leurs données personnelles. Ceux-ci sont décrits aux articles 25 à 29 ainsi que 32 LPD.

Concrètement, ces droits peuvent être mis en œuvre dans le cadre d'une action civile, fondée généralement sur les art. 28 et suivants du Code civil ou sur le droit des contrats.

S'agissant des droits que peuvent faire valoir les personnes concernées à l'endroit des organes fédéraux, ils sont dans leur essence similaires à ceux décrits dans ce chapitre ; pour de plus amples informations, il est renvoyé à la section « Droits des personnes concernées ».

3.2.1 Droit d'accès aux données personnelles

L'article 25 LPD permet à toute personne de demander au responsable du traitement si des données personnelles la concernant sont traitées. Elle reçoit les informations nécessaires pour qu'elle puisse faire valoir ses droits et pour que la transparence du traitement soit garantie. Ses informations contiennent au moins :

- l'identité et les coordonnées du responsable du traitement ;
- les données personnelles traitées ;
- la finalité du traitement ;
- la durée de conservation des données personnelles ou, si elle n'est pas encore déterminable, les critères permettant de la fixer ;
- si les données n'ont pas été récoltées chez la personne concernée, l'origine des données ;
- cas échéant, l'existence d'une décision individuelle automatisée ainsi que la logique sur laquelle elle repose ;
- cas échéant, les destinataires ou les catégories de destinataires à qui les données personnelles sont transmises et les informations visées à l'art. 19 al. 4 LPD.

S'il s'agit de données personnelles sur la santé de la personne concernée, elles peuvent lui être transmises, avec son accord, par l'intermédiaire d'un professionnel de la santé qu'elle aura désigné (art. 25 al. 3 LPD).

Ces renseignements doivent être fournis en principe gratuitement, dans les 30 jours. Si les données sont traitées par un sous-traitant, celui-ci est tenu d'aider le responsable du traitement à satisfaire au droit d'accès. Au surplus, les modalités du droit d'accès sont réglées aux art. 16 à 19 OPDo.

Restrictions

L'article 26 LPD permet au responsable de traitement de refuser, restreindre ou différer l'accès dans les cas suivants :

- une loi au sens formel le prévoit, notamment pour protéger un secret professionnel ;
- les intérêts prépondérants d'un tiers l'exigent ;
- la demande d'accès est manifestement infondée parce qu'elle poursuit un but contraire à la protection des données ou est manifestement procédurière ;
- les intérêts prépondérants du responsable de traitement l'exigent et il ne communique pas les données à des tiers.

Le responsable du traitement doit indiquer dans un délai de 30 jours le motif pour lequel il refuse, restreint ou diffère la communication des informations.

A noter encore que les médias peuvent bénéficier de dérogations supplémentaires, aux conditions de l'art. 27 LPD.

Mesures à envisager :

- Une information claire et compréhensible doit être donnée. Elle est nécessaire pour que chacun puisse connaître et exercer ses droits.
- Une procédure pour les demandes d'accès doit être mise en place et connue des collaborateurs.
- Le système est organisé de manière à pouvoir répondre à la demande : la recherche doit permettre de trouver rapidement l'intégralité des données de la personnes concernée.
- Les données dont les droits d'accès pourraient être restreints sont clairement indiquées comme telles, ainsi que le motif.
- En cas de sous-traitance, une procédure de transmission des données par celui-ci doit également être définie.

3.2.2 Droit à la remise ou à la transmission des données personnelles

L'article 28 LPD permet à une personne concernée de demander au responsable du traitement de lui remettre, dans un format électronique couramment utilisé, les données personnelles la concernant qu'elle lui a communiquées, si les deux conditions suivantes sont réunies :

- le responsable du traitement traite les données personnelles de manière automatisée ;
- les données personnelles sont traitées avec le consentement de la personne concernée ou en relation directe avec la conclusion ou l'exécution d'un contrat entre elle et le responsable du traitement.

Aux mêmes conditions, la personne concernée peut demander au responsable du traitement de transmettre directement les données en question à un autre responsable du traitement, pour autant que cela n'exige pas d'effort disproportionné.

La remise et la transmission des données personnelles est en principe gratuite. Les restrictions de ce droit sont les mêmes que pour le droit d'accès (art. 29 LPD).

Les détails, notamment techniques, relatif à d'exercice de ce droit sont décrits aux art. 20 à 22 OPDo.

L'Union Européenne a publié des directives sur la « portabilité des données » qui peuvent servir de base pour la concrétisation de ces droits[10].

Mesures à envisager :

- lors de la conception d'un traitement de données automatisé, utiliser un format courant, de manière à ce qu'une extraction soit aisée ;
- alternativement, prévoir une méthode de transformation des données personnelles en format couramment utilisable ;
- se renseigner sur l'existence de standards ou de modèles pour la transmission de types de données personnelles spécifiques (biométriques, génétiques, …) ;
- établir des protocoles de remise et de transmission des données personnelles et les faire connaître aux collaborateurs ;
- considérer la faisabilité d'importer des données personnelles depuis les systèmes d'autres responsables de traitement qui procèdent à des traitements similaires.

[10] ARTICLE29 - Guidelines on the right to "data portability" (wp242rev.01) (europa.eu)

3.2.3 Droit à la destruction des données personnelles

L'art. 32 al. 2 let. c LPD prévoit que la personne concernée peut demander l'effacement ou la destruction de ses données personnelles. Ce droit, concrétisé par l'effacement ou l'anonymisation des données personnelles, peut être complexe à mettre en œuvre pour des traitements à grande échelle, en raison de l'aspect souvent international de tels traitement et des avancées de la technologie actuelle, par exemple avec l'utilisation du cloud sur des serveurs dispersés sur plusieurs continents.

Lors de la destruction des données, le système doit garantir que l'entier des données concernées par la demande (qui ne sont pas forcément l'entier des données personnelles de la personne concernée) soient effacées/anonymisées par l'opération (Destruction des données). Ceci est grandement facilité si le système a été conçu selon les principes de protection dès la conception (*privacy by design)* et de protection par défaut (Protection dès la conception et par défaut).

3.2.4 Droit à la rectification des données personnelles

L'art. 32 al. 1 LPD prescrit que les personnes concernées peuvent exiger que des données personnelles inexactes soient rectifiées, sauf si leur modification est interdite par une disposition légale ou que ces données sont traitées à des fins archivistiques dans un intérêt public.

Cas échéant, le responsable du traitement doit s'assurer que les données soient modifiées dans l'ensemble de ses systèmes et bases de données, et vérifier si elles ont servi à rendre des décisions. Selon les cas, il pourrait être pertinent de vérifier si des décisions ont été prises sur la base de ces données erronées.

Pour le cas où ni l'exactitude ni l'inexactitude d'une donnée ne peut être prouvée, la personne concernée peut exiger que l'on y ajoute une mention relative à son caractère litigieux (art. 32 al. 3 LPD)

Il est recommandé de se préparer à ce type de situations en mettant en place des processus clairement définis et en préparant les instruments adéquats (notamment prévoir des champs pour indiquer le caractère litigieux de la données).

3.2.5 Droit à l'interdiction de traitement de données personnelles

L'art. 32 al. 2 let. a LPD indique que la personne concernée peut demander qu'il soit fait interdiction de traiter ses données personnelles.

Outre des situations où la personne souhaite interdire un traitement qu'elle considère injustifié dans sa totalité, ce droit est aussi utile dans des situations hybrides, notamment lorsque les données sont traitées à des fins multiples. Par exemple, une adresse e-mail est utilisée pour l'enregistrement d'un compte et pour la newsletter hebdomadaire du site ; la personne concernée peut demander l'arrêt de l'utilisation de son adresse pour la distribution de la newsletter.

De même, certaines données personnelles doivent être conservées pour des raisons légales (dossiers médicaux pas exemple), mais la personne concernée souhaite que le responsable du traitement ne les utilise pas à d'autres fins ; il peut ainsi faire interdire tout traitement qui irait au-delà de ce but.

Pour faire suite à de telles demandes, le responsable du traitement doit pouvoir séparer ses différents traitements. Prévoir un processus simple pour mettre fin à certains traitements

spécifiques est donc recommandé (se désabonner à la newsletter en décochant une case, par exemple).

3.2.6 Droit à l'interdiction de communiquer les données personnelles

L'article 32 al. 2 let. b LPD prévoit que la personne concernée peut demander l'interdiction d'une communication déterminée de données personnelles à des tiers.

La mise en place d'un attribut d'autorisation de partage est une manière de respecter les demandes d'interdiction de communiquer sans pour autant effacer les données. Ces mesures peuvent être couplées à celles relatives à la limitation des finalités, évoquées ci-dessus.

3.2.7 Droit à la communication des mesures relatives aux données personnelles

A noter enfin que la personne concernée peut demander à ce que les mesures évoquées aux ch. 3.2.3 à 3.2.6 soient publiées ou communiquées à des tiers (art. 32 al. 4 LPD).

Mesures à envisager :

- Les systèmes de traitements sont organisés de manière à pouvoir répondre aux différentes demandes sans compromettre l'ensemble des traitements.
- Les procédures pour répondre à ces demandes sont prédéfinies, claires et connues des collaborateurs.
- Les procédures relatives aux différentes demandes sont aisément accessibles et faciles à mettre en œuvre pour les personnes concernées, par exemple dans une section « Protection des Données » ou « Mon Compte ».
- Dans le cas de données personnelles mises en ligne, il peut être judicieux de désindexer certaines pages des moteurs de recherche afin de simplifier le respect des droits des personnes concernées.

3.3 REPRODUCTIBILITÉ DES PROCÉDURES

Les procédures qui permettent de mettre en œuvre les différents droits des personnes concernées doivent être clairement définies et reproductibles. Si les mécanismes sont préprogrammés dans le système qui traite les données, tous les collaborateurs avec les autorisations adéquates auront la possibilité d'effectuer les différentes actions sur les données demandées par les personnes concernées. Un mécanisme préprogrammé est également bénéfique lors d'un contrôle effectué par une autorité de surveillance puisqu'il démontre que les divers droits des personnes concernées peuvent être respectées en cas de demande.

Mesures à envisager :

- La procédure d'exécution du droit d'accès est préprogrammée dans le système.
- Tous les collaborateurs utilisent la même procédure.
- L'autorité de surveillance peut effectuer son travail si nécessaire en testant la procédure intégrée au système.

Lectures supplémentaires :

	CNIL [6]
Exercice des droits de limitation du traitement	Ch. 11
Exercice des droits de rectification et d'effacement	Ch. 12
Exercice des droits d'accès et à la portabilité (RGPD)	Ch. 13
Finalités: déterminées, explicites et légitimes	Ch. 14

Fondement: licéité du traitement, interdiction du détournement de finalité	Ch. 15
Formalités préalables	Ch. 16
Information des personnes concernées	Ch. 22
Recueil du consentement	Ch. 30

4 ORGANES FÉDÉRAUX

Globalement, les organes fédéraux sont soumis aux mêmes règles et principes que les privés, bien que des variations existent. Les articles 33 à 42 LPD exposent des règles applicables spécifiquement à ces organes. De même, ponctuellement, l'OPDo règle les choses un peu différemment pour les organes fédéraux (art. art. 4 al. 2 ou art. 6 OPDo par exemple). Le présent guide s'adressant avant tout aux personnes privées, les spécificités relatives aux organes fédéraux ne seront présentées que brièvement. Vous pourrez trouver des informations supplémentaires sur le site de l'OFJ[11].

4.1 BASES LÉGALES

En principe, les organes fédéraux n'ont le droit de traiter des données personnelles que s'ils disposent d'une base légale appropriée (art. 34 LPD).

Si le traitement concerne des données sensibles ou des profilages, ou peut potentiellement causer une grave atteinte aux droits fondamentaux de la personne concernée, la base légale doit en plus être une loi au sens formel (art. 34 al. 2 LPD).

Dans l'hypothèse d'un traitement de données sensible ou d'un profilage, une base légale au sens matérielle peut néanmoins suffire si le traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée et que le traitement est indispensable à l'accomplissement d'une tâche, elle-même définie dans une loi au sens formel (art. 34 al. 3 LPD).

Enfin, en dérogation à ce qui précède, les organes fédéraux sont en droit de traiter des données personnelles dans trois hypothèses (art. 34 al. 4 LPD) :

- si le Conseil fédéral autorise le traitement, considérant que les droits des personnes concernées ne sont pas menacés ;
- si la personne concernée a consenti au traitement en l'espèce ou a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement ;
- si le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable.

4.2 TRAITEMENTS À DES FINS NE SE RAPPORTANT PAS À DES PERSONNES

L'article 39 LPD permet aux organes fédéraux de traiter des données personnelles à des fins de recherche, de planification ou de statistique si :

- les données sont rendues anonymes dès que la finalité du traitement le permet ;
- l'organe fédéral ne communique des données sensibles à des personnes privées que sous une forme ne permettant pas d'identifier les personnes concernées ;
- le destinataire ne communique les données à des tiers qu'avec le consentement de l'organe fédéral qui les lui a transmises ; et
- les résultats du traitement ne sont publiés que sous une forme ne permettant pas d'identifier les personnes concernées.

[11] Informations destinées aux organes fédéraux (admin.ch)

Cet article institue une exception au principe de finalité et représente aussi un assouplissement des exigences en matière de base légale nécessaire au traitement et la communication des données (cf. art. 39 al. 2 et les articles qui y sont cités).

4.3 COMMUNICATION

Globalement, la communication de données personnelles est soumise aux mêmes conditions que le traitement en lui-même (voir art. 36 al. 1, renvoyant à l'art. 34 al. 1 à 3 LPD, voir ci-dessus). Des dérogations spécifiques sont toutefois prévues à l'art. 36 al. 2 LPD : il s'agit essentiellement de situation où cela est nécessaire à l'accomplissement d'une tâche, ou lorsqu'il s'agit de sauvegarder des intérêts supérieurs, ou encore si la personne si oppose de manière contraire à la bonne foi. Le consentement de la personne concernée est aussi un motif pouvant justifier une communication.

D'une manière générale, les organes fédéraux ont en outre le droit de communiquer sur demande le nom, prénom, adresse et date de naissance d'une personne (art. 36 al. 4 LPD). Il s'agit cependant d'un droit et non d'une obligation : l'organe doit toujours procéder à une pesée des intérêts, à la lumière des principes de la protection des données. Les organes fédéraux peuvent également informer le public ou rendre les données publiquement accessibles dans les cas visés à l'art. 36 al. 3 et 5 LPD.

Enfin, et d'une manière générale, les organes fédéraux peuvent refuser la communication s'ils sont tenus par une obligation légale de secret ou en présence d'un intérêt public ou privé significatif (art. 36 al. 6 LPD). A noter encore que la personne concernée peut également former opposition à la communication de ses données ; l'organe fédéral statue ensuite sur l'opposition (art. 37 LPD).

4.4 REGISTRE DES ACTIVITÉS DE TRAITEMENT

Les organes fédéraux doivent tenir un registre des activités de traitement, dont le contenu est similaire à celui qui doit être tenu par les personnes privées (art. 12 LPD, cf. Registre). Ils doivent en outre déclarer leurs registres au PFPDT (12 al. 4 LPD). Ils peuvent le faire sur le portail d'annonce dédié.[12]

4.5 ANNONCES DE VIOLATION DE LA SÉCURITÉ DES DONNÉES

Les organes fédéraux sont soumis au même régime d'annonce de violation de la sécurité de données que les privés (art. 24 LPD). Une nuance existe néanmoins dans les motifs leur permettant de restreindre, différer ou renoncer à l'information de la personne concernée : il n'est ici pas question de l'intérêt d'un tiers, mais de la préservation d'un intérêt public prépondérant ou pour garantir la pertinence d'une enquête, d'une instruction ou d'une procédure (art. 24 al. 5 let. a, renvoyant à l'art. 26 al. 2 let. b LPD).

4.6 DÉCISIONS INDIVIDUELLES AUTOMATISÉES

Globalement, le régime en matière de décisions individuelles automatisées est le même pour les organes fédéraux et les personnes privées. A noter cependant deux différences introduites par l'art. 21 al. 4 LPD :

[12] DataReg: http://datareg.edoeb.admin.ch/

1) lorsqu'un organe rend une décision individuelle automatisée, il doit la qualifier comme telle ;
2) la personne concernée ne peut pas faire valoir son point de vue et demander à ce qu'une personne physique revoit la décision si, selon sur la base d'une loi fédérale (art. 30 al. 2 PA par exemple), la personne n'a pas à être entendue avant que la décision ne soit rendue.

4.7 DEVOIR D'INFORMER

A nouveau, un organe fédéral est pour l'essentiel soumis aux mêmes conditions qu'un privé (Devoir d'informer). A la différence d'un privé, un organe fédéral ne pourra cependant pas retreindre, différer ou renoncer à l'information pour ses intérêts propres (art. 20 al. 3 let. c LPD), mais pour sauvegarder des intérêts publics ou la pertinence d'une enquête, d'une instruction ou d'une procédure (art. 20 al. 3 let. d LPD).

4.8 DROITS DES PERSONNES CONCERNÉES

De façon générale, les organes fédéraux doivent se plier aux mêmes exigences que les privés pour ce qui est des droits de personnes concernées (Droits et Devoirs).

A noter que s'agissant du droit d'accès, un organe fédéral ne peut pas refuser, restreindre ou différer celui-ci pour ses intérêts propres, mais pour sauvegarder un intérêt public prépondérant ou la pertinence d'une enquête, d'une instruction ou une procédure (art. 26 al. 2 let. b LPD).

S'agissant de la mise en œuvre de ses droits, la personne concernée dispose matériellement plus ou moins des mêmes prétentions que contre des personnes privées (art. 41 à comparer avec l'art. 32 LPD). L'art. 41 LPD détaille certaines nuances dans la nature ou la mise en œuvre de ces prétentions. A noter en particulier qu'une telle procédure serait régie par la PA (art. 41 al. 6 LPD).

Enfin, l'art. 42 LPD règle la coordination entre les procédures selon la loi sur la transparence et les droits conférés par l'art. 41 LPD.

Mesures à envisager :

- Indiquer clairement la base légale et/ou motif pour tout traitement de données personnelles.
- Indiquer les données personnelles affectée par les exceptions aux différents droits des personnes concernées.
- Préparer des procédures similaires à celles recommandées dans la section Droits et devoirs.

4.9 JOURNALISATION

Pour les organes fédéraux et leurs sous-traitants, une journalisation doit être faite dans tous les cas lorsqu'ils effectuent des traitements automatisés de données personnelles. La journalisation doit porter au moins sur l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données.

Aux surplus, les exigences concernant la journalisation par des responsables de traitement privés sont également valables (Journalisation).

4.10 RÈGLEMENT DE TRAITEMENT

En présence de certains types de traitements automatisés (cf. art. 6 al. 1 OPDo), les organes fédéraux sont tenus d'élaborer un règlement de traitement. Le contenu de ce règlement correspond à ce qui est demandé pour les règlements de privés (Règlement de traitement). Le PFPDT mets également à disposition un modèle de règlement de traitement pour les organes fédéraux[13].

[13] Règlement de traitement (Offices fédéraux) (DOCX)

5 PROTECTION DES DONNÉES

La protection des données dès la conception ainsi que la protection des données par défaut, prescrite par l'art. 7 de la LPD et l'art. 25 du RGPD, implique de prendre des mesures pour minimiser la collecte de données personnelles, ainsi que leur exposition.

Le principe de la proportionnalité, art. 6 al. 2 LPD, et l'art. 5 al. 1 let. c RGPD, implique notamment la limitation des accès aux données personnelles.

Le principe de l'exactitude des données est ancré par l'art. 6 al. 5 LPD et l'art. 5 al. 1 let. d RGPD.

Cette section suggère des mesures à prendre pour protéger le contenu des données personnelles. Diverses techniques et pratiques sont décrites pour améliorer la protection des données en affectant directement leur contenu.

L'article 7 al. 1 et 2 LPD explicite le devoir du responsable du traitement consistant à mettre en place, dès la conception du traitement, des mesures techniques et organisationnelles, afin que le traitement respecte les prescriptions de protection des données. L'utilisation de chiffrement des messages (Chiffrement des messages) ou de pseudonymisation (Pseudonymisation) à certaines étapes du traitement, par exemple, permet de mieux protéger les données personnelles des personnes concernées.

Dans cette catégorie, nous incluons des mesures (techniques) qui touchent aux contenus des données, afin de les rendre moins précises, moins sensibles, en les adaptant aux finalités visées. Ces mesures visent à adapter (minimiser) l'information que les données fournissent. En d'autres termes, la quantité de données pourrait rester la même (par ex. ID, genre, adresse exacte), mais les informations fournies varieront en fonction de la finalité visée (par ex. ID, genre, canton).

Cette adaptation de l'information sert également à :

- Adapter l'information aux finalités visées (principe de la proportionnalité).
- Sécuriser l'information (principe de la sécurité). Si les données tombent dans les mauvaises mains, l'information dévoilée serait moins précise et moins sensible.
- Éventuellement anonymiser les données.

5.1 PROTECTION DÈS LA CONCEPTION ET PAR DÉFAUT

La protection des données dès la conception (art. 7 al. 1 LPD) demande la prise en compte par le responsable du traitement des principes de protection des données dès la conception même du système, et non après seulement. Une réflexion avant la mise en œuvre du traitement sur les justifications de la collecte des données, de leur utilisation, leur gestion et leur organisation permet d'assurer le respect des normes de protection des données, notamment la mise en œuvre des recommandations faites dans le présent guide.

La protection des données par défaut (art. 7 al. 3 LPD), est l'une des expressions du principe de proportionnalité. Il s'agit pour le responsable du traitement de prendre des mesures dès la collecte de données pour faire en sorte que, par défaut, via notamment des préréglages, seule la quantité de données strictement nécessaire à la finalité du traitement ne soient collectées et utilisées. Par exemple, lors de la récolte de cookies sur un site internet, ceux qui ne sont

pas nécessaires à la consultation du site devraient être désactivés par défaut ; aussi, l'utilisateur qui accepte l'utilisation de cookies supplémentaire doit activement y consentir.

Ce concept s'étend également aux étapes suivantes du traitement : pour le responsable, il s'agit de faire en sorte que chaque étape du traitement puisse être mené avec le strict minimum d'information nécessaire.

Les différentes mesures prises dans le cadre de la protection dès la conception et par défaut figurent typiquement dans le détail d'une AIPD (Analyse d'impact).

Mesures à envisager :

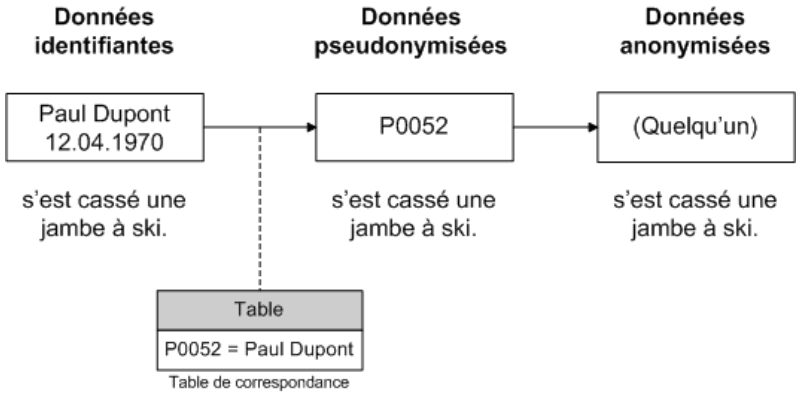
- Lorsque des données non-nécessaires au traitement sont également collectées, prévoir une valeur par défaut nulle ou négative (ex. « NA »).
- Clairement indiquer et séparer les données nécessaires et non-nécessaires au traitement.
- Prendre en compte les effets des informations non-obligatoires sur l'efficacité de l'anonymisation et de la pseudonymisation.

5.2 PSEUDONYMISATION

Au sens juridique, la pseudonymisation consiste à modifier les données personnelles de manière à ce qu'elles ne puissent plus être reliées à une personne spécifique sans informations supplémentaires ou sans efforts disproportionnés. Les données pseudonymisées restent cependant à risque de réidentification et sont de ce fait toujours considérées comme des données personnelles.

La pseudonymisation consiste en la création d'un pseudonyme qui remplace typiquement le nom, la date de naissance, etc. de la personne concernée dans les bases de données. Simultanément, une table de correspondance séparée est créée afin de lier le nom à ce pseudonyme. Ainsi, seules les personnes ayant accès à cette table peuvent aisément lier les données avant le nom, et de ce fait reverser la pseudonymisation.

Le schéma suivant donne un aperçu de ce processus :



Il existe divers moyens de faire la correspondance entre les données identifiantes et leurs pseudonymes, notamment :

- L'établissement de tables de correspondance, comme dans l'exemple de la figure ci-dessus.
- L'utilisation de « fonctions » dont les entrées sont les données identifiantes, et les sorties sont les pseudonymes correspondants.

A noter que ces correspondances, qu'elles soient faites avec des tables ou des fonctions, ne devraient pas être réversibles (sans passer par la table par exemple). Dans l'exemple ci-dessus, il ne doit pas être possible d'inverser P0052 pour obtenir « Paul Dupont » sans utiliser la table de correspondance. Pour que les correspondances ne soient pas réversibles :

- L'établissement des correspondances dans la table doit être aléatoire, ou basé sur un « secret » inconnu pour les personnes qui utilisent les données pseudonymisées.
- Si la correspondance est faite par des « fonctions », celles-ci ne doivent pas être réversibles. C'est typiquement le cas des fonctions de hachage cryptographique, tels que SHA256, MD5 etc. Par exemple, SHA256(« Paul Dupont ») produit « 671fee34b2bd82aec7bd60d757ebf3fd8f395d61b1dd70279d416e18b20937e1 », et il est pratiquement impossible de deviner l'entrée à partir de cette sortie.
- Cependant, puisque ces fonctions de hachage sont publiques, la personne utilisant les pseudonymes peut facilement vérifier ce que donne SHA256(« Paul Dupont ») (ou toute la liste de noms possibles, comme ceux des collègues d'entreprise par exemple), pour établir le lien entre « Paul Dupont » et son pseudonyme « 671…7e1 ». Pour éviter cela, il faut utiliser une clé secrète en combinaison avec les données identifiantes, avant de faire le hachage. Par exemple, SHA256(« Paul Dupont », « TopSecret ») donne un pseudonyme que l'utilisateur est incapable d'inverser tant qu'il n'a pas accès au « TopSecret ». C'est-ce qu'on appelle hachage avec clé secrète.
- En détruisant la table de correspondance, ou la clé secrète du hachage, on élimine la possibilité de revenir du pseudonyme à la donnée identifiante correspondante, que ce soit pour celui qui a établi la table ou le hachage de correspondance, ou pour celui qui utilise les pseudonymes. Cependant, cette destruction des liens n'est pas suffisante pour que les données deviennent anonymes, comme il sera expliqué ci-dessous.

5.3 ANONYMISATION

Au sens juridique, l'anonymisation consiste à modifier de façon irréversible les données personnelles de sorte à ce qu'elles ne puissent plus être liées à une personne spécifique, sans efforts disproportionnés[14]. Les données anonymisées ne sont plus considérées comme des données personnelles, et de ce fait sortent du champ d'application de la LPD.

Pour s'assurer de l'anonymité des données, supprimer une table d'identifiants utilisé pour masquer le nom ne suffit souvent pas. Par exemple, dans la liste des patients d'un hôpital, [ID 8128136, Femme, 42 ans, habite (petit village), traitée pour le SIDA, date d'opération 12.07.2021] ne remplit pas les conditions d'anonymité. Même sans avoir le nom caché derrière l'ID, il serait aisé de savoir qui est cette personne par exemple pour son employeur, ou même n'importe quelle personne connaissant son âge et son village de résidence. Plus le nombre de personnes concernées est petit, et plus le nombre de données restent, plus il est facile de réidentifier la personne.

[14] Il faut comprendre par-là que « *l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre […]. Il convient de prendre en compte dans chaque cas d'espèce l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne. Le caractère raisonnable des moyens en question doit être évalué au regard de l'ensemble des circonstances, telles que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de leur évolution »* (Message LPD, FF 2017 p. 6639).

Il existe plusieurs techniques d'anonymisation, qui seront décrites ci-dessous. Elles ne suffisent cependant pas toujours à anonymiser tous les jeux de données. Chaque jeu de données différent requière une réflexion individuelle, et certains ne peuvent tout simplement pas être rendus anonymes sans perdre leur utilité (ce qui met alors le responsable de traitement devant le choix de traiter des données personnelles ou de renoncer purement et simplement au traitement). De plus, certains types de données requièrent des techniques différentes, par exemple l'anonymisation des personnes dans des vidéos ou des photographies, qui exige des techniques adaptées.

Pour pouvoir estimer le niveau d'anonymisation, au-delà de sa définition juridique, il y a plusieurs modèles de risques. Selon les définitions du Groupe Article 29[15] donnée dans son Avis sur les Techniques d'anonymisation [7]:

- *l'individualisation*, qui correspond à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données;
- *la corrélation,* qui consiste dans la capacité de relier entre elles, au moins, deux enregistrements se rapportant à la même personne concernée ou à un groupe de personnes concernées (soit dans la même base de données, soit dans deux bases de données différentes). Si une attaque permet d'établir (par exemple, au moyen d'une analyse de corrélation) que deux enregistrements correspondent à un même groupe d'individus, mais ne permet pas d'isoler des individus au sein de ce groupe, la technique résiste à l'«individualisation», mais non à la corrélation;
- *l'inférence*, qui est la possibilité de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs.

Une solution résistant à ces trois risques offrirait par conséquent une protection fiable contre les tentatives de réidentification utilisant les moyens les plus susceptibles d'être raisonnablement mis en œuvre par le responsable du traitement des données ou par des tiers.

A noter qu'il est de plus en plus difficile de parler d'une réelle anonymisation (au sens technique), absolument irréversible. Ceci est dû à :

- la croissance des volumes de données pouvant être utiles pour la réidentification ;
- l'accessibilité de plus en plus aisée à ces données ;
- de nouveaux algorithmes plus performants et plus précis, pouvant être utilisés pour la réidentification ;
- des avancées en cryptographie qui pourraient rendre les techniques existantes moins robustes.

[15] Maintenant European Data Protection Board (EDPB)

Bonnes pratiques d'anonymisation du Groupe Art. 29[15]

En général :
- Ne pas se contenter de « publier et oublier ». Compte tenu du risque résiduel d'identification, les responsables du traitement des données devraient :

1. identifier les nouveaux risques et réévaluer régulièrement le(s) risque(s) résiduel(s) ;

2. examiner si les contrôles des risques identifiés sont suffisants et les ajuster en conséquence ;

3. surveiller et contrôler les risques.

- Parmi ces risques résiduels, la possibilité d'identifier la partie non anonymisée d'un ensemble de données devrait (le cas échéant) être prise en considération, surtout en combinaison avec la partie anonymisée, ainsi que les corrélations possibles entre les attributs (par exemple entre les données relatives à la localisation géographique et celles concernant le niveau de prospérité).

Mesures à envisager:

- Privilégier l'utilisation de données anonymisées dans les limites des possibilités du projet. Si les données sont correctement anonymisées, alors la loi sur la protection des données ne s'applique plus.
- En cas d'anonymisation, aucune information identifiante indirecte n'est conservée. Une information identifiante indirecte est une information qui, lorsque mise en relation avec d'autres informations qui, prises séparément, ne sont pas significatives, permet d'identifier une personne.
- Si l'anonymisation n'est pas envisageable, les collaborateurs travaillent si possible sur des données pseudonymisées.
- La table de correspondance et/ou la clé secrète du hachage doit être sécurisée. Elles ne doivent être accessibles qu'à un nombre restreint de collaborateurs et si possible être chiffrées.

5.4 GÉNÉRALISATION

La généralisation consiste à remplacer certaines valeurs d'attributs par des valeurs plus génériques ou par marges de valeurs. Par exemple :

- Remplacer une certaine date de naissance (ex. 8.03.1980) par l'année de naissance (ex. 1980), ou encore par une marge d'âge (ex. [40-50] ans).
- Remplacer une certaine adresse exacte par sa ville, région ou canton (on peut très bien hiérarchiser).
- Remplacer une certaine nationalité par sa région géographique, ou continent.

La généralisation rend les attributs moins utiles pour la réidentification des personnes. Par exemple :

- [Sexe : Femme, Age : 32, Nationalité : Moldave, Résidence : Morges] peut facilement être identifiable. Sous forme généralisée, [Sexe : Femme, Age : 30-40, Nationalité : Europe de l'Est, Résidence : Région Lausannoise] rendrait l'identification plus difficile.
- Pour un service météo, une granularité GPS (~2m) n'est pas nécessaire, et son utilisation pourrait identifier l'utilisateur inutilement. Une généralisation au niveau de la localité est plus appropriée.

La généralisation des données contribue à :

- L'anonymisation éventuelle des données (sortant ainsi du cadre de la LPD et du RGPD).
- La proportionnalité de l'information collectée, que les données soient anonymes ou pas.
- La sécurisation des données, que les données soient anonymes ou pas.

5.5 MINIMISATION

Application concrète du concept de protection dès la conception, la minimisation consiste en la récolte du strict minimum de données nécessaires. En effet, certaines données, ou leurs combinaisons, peuvent contribuer à l'identification des personnes concernées, même si individuellement elles ne sont pas personnelles ou sensibles

Exemples:

- Pour analyser les moyens de transport des utilisateurs d'une certaine application, l'exclusion des données GPS autour des domiciles des utilisateurs permettrait de mieux cacher leurs identités.
- Une application qui propose certains services (ex. transports publics) dans un certain pays, durant certaines heures d'ouverture, ne devrait pas récolter la localisation de l'utilisateur dans d'autres pays, ni hors des heures de service.

Comme pour la généralisation, le filtrage des données contribue à :

- La proportionnalité, que les données soient anonymes ou pas.
- La sécurisation des données, que les données soient anonymes ou pas.

5.6 RANDOMISATION

Certaines finalités cherchent des résultats statistiques plutôt qu'individuels à partir des données collectées. C'est typiquement le cas où on peut appliquer la randomisation, soit le changement aléatoire des valeurs des attributs. Par exemple : si on cherche la moyenne d'âge d'une certaine population, on peut changer les valeurs individuelles collectées, tout en gardant (presque) la même moyenne originale.

Plusieurs techniques s'inscrivent dans cette catégorie, notamment :

- l'ajout de bruit, soit la modification de catégories d'information sans changer les informations pertinentes pour la mesure (par ex. ajouter cinq ans à une personne et en retirer cinq à une autre) ;
- la permutation, soit l'inversion de données entre différents jeux de données sans changer les informations pertinentes pour la mesure (par ex. permuter échanger l'âge entre deux personnes) ;
- la confidentialité différentielle, qui est une technique de randomisation spécifique qui détermine la quantité de bruit à ajouter lors du transfert de données au lieu de directement sur les données.

A noter que la randomisation change les valeurs des attributs, sans pour autant anonymiser les personnes concernées. Par exemple, les noms/prénoms des personnes pourraient être gardés en clair, mais les âges indiqués seraient incorrects, et inutiles s'ils sont pris individuellement. C'est une manière de diminuer les risques sans changer les identifiants.

Par contre, en l'absence d'autres identifiants, les attributs randomisés contribuent indirectement à l'anonymisation. Par exemple, en ajoutant du bruit à l'âge [Homme, 39 ans, Morat], où 39 = 34 + bruit, on a moins de certitude sur l'identité de la personne.

5.7 CHIFFREMENT HOMOMORPHE

Un algorithme de chiffrement homomorphe est capable de crypter des données de façon à garder les propriétés mathématiques des données histoire qu'il soit possible d'encore mesurer certaines informations sur ces données en ayant accès uniquement à la version cryptée.

Cette méthode, relativement récente, est limitée dans les opérations que l'on peut mener dessus et peut se révéler relativement couteuse à mettre en œuvre mais peut rendre possible un traitement de données sensibles par un tiers sans risque d'accès de celui-ci.

Il existe également des algorithmes dits partiellement homomorphiques, qui permettent typiquement une seule opération, mais à moindre coût.

5.8 DONNÉES SYNTHÉTIQUES

Des données synthétiques sont des données créées artificiellement à partir de vraies données, par exemple avec un algorithme d'apprentissage machine (*machine learning*). Ces données seraient suffisamment similaires à des vraies données personnelles pour pouvoir entraîner d'autres modèles dessus (des fausses images de tumeurs pour un système d'aide en médecine, par exemple).

L'utilisation de telles données permet en principe de sortir du champ d'application de la LPD, mais il convient de faire très attention au processus de création de ces données. Il doit être impossible de recréer les données originales ou de réidentifier les personnes concernées dans les données personnelles originelles (cf. Anonymisation). Si ce n'est pas le cas, ces données doivent tout de même être considérées comme des données personnelles.

6 INFRASTRUCTURE

La sécurité des données, déduite de l'art. 8 de la LPD, de l'art. 3 OPDo, et des art. 5 al. 1 let. f et art. 32 du RGPD, implique, entre autres, la sécurisation des locaux, des serveurs, et des locaux de travail.

Les mesures décrites précédemment se concentrent sur le contenu des données ; elles n'abordent pas l'environnement de ces données, soit les infrastructures et les comportements des personnes appelées à travailler sur ces données. L'emplacement physique des données doit être soigneusement étudié : où se trouvent les serveurs de données et comment assurer leur sécurité en tenant compte de tous les acteurs impliqués ?

Les aspects suivants sont traités en détails et accompagnés de mesures concrètes :

- Comment assurer la sécurité des locaux ?
- Comment assurer la sécurité des serveurs ?
- Comment assurer la sécurité des places de travail ?
- Quels sont les risques de l'utilisation du cloud ?

6.1 SÉCURITÉ DES LOCAUX

Les locaux sont définis comme les lieux où les utilisateurs du système travaillent et, par conséquent, ont accès aux données. Les données sont physiquement stockées dans les salles de serveurs (cf. section suivante) et les ordinateurs personnels sont des périphériques qui permettent d'accéder à ces données. L'accès à ces machines, en tant qu'interfaces vers les données, doit être contrôlé. Seules les personnes autorisées doivent accéder aux bâtiments et aux bureaux. Les fonctions de ces personnes peuvent être variées et il faut toutes les prendre en compte pour définir des droits d'accès spécifiques : les collaborateurs de l'organisation en font partie, évidemment, mais également le personnel de maintenance, de nettoyage, etc.

Il faut tenir compte du contexte global pour prendre les mesures adéquates. Si plusieurs organisations partagent un même bâtiment, elles n'ont pas forcément les mêmes besoins en matière de protection des données. La sécurité doit alors être adaptée, par étage par exemple. De plus, les serveurs de données peuvent être externalisés et leur sécurité par conséquent confiée à des tiers.

Mesures à envisager :

- L'accès au(x) bâtiment(s) est réglementé. Un badge, éventuellement associé à un code d'accès, permet l'authentification des personnes qui souhaitent entrer dans le bâtiment.
- Si plusieurs organisations partagent le même bâtiment, il faut, si nécessaire, également réglementer l'accès aux locaux privatifs de l'organisation : un système d'accès électronique est installé à l'étage ou dans la section réservée à l'organisation.
- Une réglementation particulière ainsi qu'une procédure d'accueil pour les visiteurs est établie afin d'éviter qu'ils ne se déplacent seuls et librement dans le bâtiment.
- Les bureaux sont verrouillés en dehors des heures de présence.
- Des alarmes sont éventuellement placées dans les locaux les plus sensibles et sont activées en dehors des heures de présence.

6.2 SÉCURITÉ DES SALLES DE SERVEURS

Les salles de serveurs sont les lieux les plus sensibles d'une organisation puisque les données sont physiquement stockées sur ces machines. L'intégrité et la disponibilité des données sont garanties si la perte définitive des données est impossible grâce à la mise en place de mesures appropriées. Il est important de déterminer là aussi qui est autorisé à accéder à ces salles. Avec un nombre restreint d'autorisations accordées, la sécurité est améliorée. Il faut éviter de mauvaises manipulations sur les serveurs, intentionnelles ou non, qui mènent à une destruction ou une modification des données. Ainsi, des mesures particulières doivent être prises pour sécuriser les salles de serveurs.

Mesures à envisager :

- Un nombre restreint de personnes est autorisé à pénétrer dans les salles de serveurs. Autoriser l'accès à toutes les personnes qui partagent une fonction identique est trop laxiste. L'accès à des fins de maintenance des systèmes est autorisé à un nombre restreint de techniciens. De même, il est judicieux de toujours confier le nettoyage des salles aux mêmes employés.
- Les accès aux salles de serveurs sont journalisés.
- Une alarme est installée et fonctionne en continu pour éviter toute intrusion frauduleuse.
- Idéalement, la salle de serveurs se trouve au sous-sol afin de minimiser le nombre d'accès physiques (portes, fenêtres, etc.).
- Les incidents naturels, tels que les incendies ou les inondations, sont détectables de manière automatique et signalés par des alarmes.

6.3 SÉCURITÉ DES PLACES DE TRAVAIL

Les collaborateurs accèdent et traitent les données depuis leur place de travail. L'ordinateur personnel du collaborateur y est installé. L'environnement de travail doit être sécurisé par une disposition stratégique des différents périphériques. Un nombre suffisant de rangements qui peuvent être fermés à clé doit être mis à disposition du collaborateur.

L'ordinateur personnel doit être protégé par un mot de passe connu du collaborateur seul. Il doit également être protégé par les logiciels nécessaires pour éviter les intrusions. La protection doit couvrir tous les types de virus, de logiciels malveillants (malwares) et d'attaques au sens large.

Ces mesures doivent être étendues également aux collaborateurs en travail à distance. Vous trouverez des conseils sur ce sujet sur le site de l'OFCS[16].

Mesures à envisager :

- Les places de travail sont aménagées de telle sorte que les écrans d'ordinateurs ne sont pas visibles depuis la porte. Les visiteurs, extérieurs à l'organisation, ne peuvent ainsi pas observer le travail des collaborateurs.

[16] Home Office - Sécuriser son accès à distance (admin.ch)

- Les documents imprimés ne restent pas sans surveillance autour de l'imprimante. Par exemple, le collaborateur introduit un code dans l'imprimante pour libérer l'impression de ses documents.
- Le collaborateur dépose ses documents imprimés et tout le matériel sensible (clés USB, CD-ROM, etc.) dans des rangements qu'il peut fermer à clé.
- Les ordinateurs portables, éventuellement les ordinateurs fixes également, sont enchaînés au bureau afin d'éviter les vols à l'intérieur des locaux.
- Un logiciel antivirus est disponible et activé sur toutes les machines. Il est mis à jour régulièrement.

6.4 UTILISATION DU CLOUD

Les raisons principales de l'utilisation des systèmes d'informatique en nuage (cloud) sont la réduction des coûts d'infrastructure informatique et de logiciels, la gestion externalisée des programmes intermédiaires ou de haut niveau, une plus grande capacité de calcul, un espace de stockage des données dynamique (la mémoire louée dans le nuage augmente ou diminue en fonction des données qui y sont enregistrées), la mobilité, la simplicité et la rapidité de l'accès aux données, l'extensibilité du système et, dans certains cas, l'amélioration de la sécurité.

La délocalisation de données est toujours risquée. À cet égard, l'informatique en nuage pose entre autres les problèmes énumérés ci-dessous :

- Perte de contrôle sur les données.
- Manque de séparation et d'isolation des données des différents clients du fournisseur.
- Non-respect des dispositions légales par le fournisseur.
- Accès par des autorités étrangères aux données.
- Captivité.

Même s'ils sont en principe diminués, les risques ci-dessous continuent d'exister, que les données soient traitées dans un nuage ou pas :

- Perte de données.
- Pannes de système et de réseau et non-disponibilité des ressources et des services.
- Usage abusif des données.

Recourir au cloud n'est pas une fin en soi, mais un moyen de répondre à des besoins. Il faut donc en premier lieu identifier ces besoins et se demander si l'on a vraiment besoin d'un cloud, cas échéant pour quelle partie de son activité.

Par ailleurs, en choisissant le type de nuage entrant en considération (nuage privé, nuage public propre à l'entreprise ou nuage hybride), il faut procéder suffisamment tôt à une analyse approfondie des exigences en matière de protection des données, en veillant tout particulièrement au traitement des données personnelles (de leur enregistrement à leur effacement en passant par leur traitement ultérieur), afin que la configuration du nuage respecte dès le départ ces exigences. Si à la suite de l'analyse des risques, il existe des doutes sur la manière dont les données personnelles sont traitées dans le nuage, il ne faudrait pas les délocaliser sans autres mesures de mitigation des risques.

Ensuite, il faut choisir soigneusement le sous-traitant (en procédant notamment à une analyse complète des risques des points de vue organisationnel, juridique et technique), lui donner des instructions précises et le surveiller attentivement, comme précisé à l'article 9 al. 2 LPD. Il faut bien choisir les applications et les données qui peuvent être délocalisées dans un nuage et celles qui doivent rester sur ses propres serveurs. En fin de compte, l'utilisateur du service reste responsable du respect des prescriptions en matière de protection des données, puisqu'il mandate un sous-traitant, et il continue de répondre vis-à-vis des personnes concernées.

Plus d'explications sur le sujet du « cloud » se trouvent sur le site du PFPDT[17].

6.5 APPROFONDISSEMENTS

D'autres aspects importants à prendre en compte pour l'infrastructure :

	CH-MS [1]	CNIL [8]	ISO 27002 [9]
Configuration des appareils mobiles	Sec. 1.6.9	Fiche 6	Sec 6.7
Éléments d'une stratégie de défense en profondeur	Sec. 1.6		
Gestion des cycles de vie du matériel	Sec. 1.6.8	Fiche 13	Sec. 7.14
Gestion des postes de travail		Fiche 5	Sec. 7.6 – 7.8
Gestion des risques	Sec 1.6.3, 2.2.4-6		
Maintenance	Sec. 2.3.5		Sec. 7.13
Sécurité des hôtes	Sec. 1.6.13		
Sécurité du réseau		Fiche 7, 8	Sec 8.20 – 8.22
Sécurité physique / des matériels	Sec. 1.6.7, 2.3.3	Fiche 16	Sec. 7.3 – 7.5

[17] Informatique en nuage (admin.ch)

7 ACCÈS ET TRAITEMENTS

La sécurité des données, déduite de l'art. 8 de la LPD, de l'art. 3 OPDo, et des art. 5 al. 1 let. f et art. 32 du RGPD, implique, entre autres, la sécurisation de l'accès aux données.

La destruction ou l'anonymisation des données quand elles ne sont plus nécessaires au regard des finalités du traitement est prescrite aux art. 6 al. 4 de la LPD et art. 17 al. 1 let. a du RGPD.

Parallèlement à la sécurisation de l'infrastructure, des mesures doivent aussi être prise au niveau de l'utilisation et la gestion des données. Dans ce chapitre nous traiterons :

1. de la gestion des accès ;
2. du cycle de vie des données et journalisation.

7.1 GESTION DES ACCÈS

Il s'agit ici de savoir qui a accès aux données, qui peut les manipuler et dans quelle mesure. Ceci implique plusieurs niveaux de sécurité : les ordinateurs qu'utilisent les collaborateurs doivent être accessibles aux seules personnes à qui l'on a accordé un accès et doivent être protégés contre les tentatives d'intrusion extérieure. Ces tentatives peuvent être locales – une personne non autorisée pénètre dans les locaux – ou distantes – une personne non autorisée accède au système à travers le réseau. Finalement, il faut décider de la trace que l'on souhaite conserver des accès physiques et électroniques :

1. Comment assurer l'identification et l'authentification des utilisateurs ?
2. Comment sécuriser l'accès aux données des utilisateurs ?
3. Comment gérer les accès à distance ?

7.2 IDENTIFICATION ET AUTHENTIFICATION

L'identification permet de connaître l'identité d'un individu, de le distinguer des d'autres. L'authentification permet de vérifier qu'un individu est bien celui qu'il prétend être. L'authentification se fait à l'aide de preuves que l'individu présente au système. Ces preuves sont de trois types. Il peut s'agir d'un objet que l'individu *possède* (un badge par exemple) ou d'une information que l'individu *connaît* (un mot de passe par exemple) ou alors d'une *propriété qui caractérise* l'individu (une propriété comportementale, telle que la signature, ou une propriété morphologique telle qu'une empreinte digitale). On parle d'authentification forte ou authentification à multiple facteurs (MFA) quand au moins deux modalités sont combinées (badge et mot de passe, mot de passe et application Authenticator, …).

Une politique de mot de passe est un outil important dans la gestion de l'authentification, et permet de diminuer les risques d'un choix de mot de passe trop simple par les employés. Des critères sont par exemple la longueur minimale, l'ancienneté maximale, l'usage de caractères spéciaux et majuscules, le nombre de fausses entrées avant un blocage, etc.

L'utilisation de programmes de génération et de gestion de mots de passe peut faciliter le respect de ces consignes pour les employés.

La CNIL propose une fiche de conseil sur l'authentification[18], qui contient également un outil de calcul de complexité pour votre politique de mot de passe[19]. Vous trouverez également des revues de technologies spécifiques sur le site de l'OFCS (uniquement en allemand pour l'instant)[20].

Mesures à envisager :

- Les comptes utilisateurs qui permettent l'authentification sont uniques. Les collaborateurs ne partagent pas de compte. Un compte comprend un identifiant (nom d'utilisateur) associé à un mot de passe, ou un badge, etc.
- Idéalement, chaque individu possède des comptes différents pour s'authentifier sur sa machine de travail puis sur les différentes applications qu'il utilise. Ainsi, si une personne mal intentionnée accède à la machine, elle n'est pas encore en mesure d'accéder aux données par le biais des applications installées.
- Si une authentification unique est utilisée (SSO), les mesures de sécurité sont adaptées en conséquence puisque qu'avec ce mécanisme, l'accès à la machine autorise également l'accès aux applications.
- Une politique de mot de passe est détaillée et tenue à jour selon l'évolution des recommandations de sécurité.
- La fréquence de changement du mot de passe est inversement proportionnelle à la complexité exigée pour celui-ci.
- L'authentification à l'aide de données biométriques doit être réalisée dans le respect des mesures présentées dans le « Guide relatif aux systèmes de reconnaissance biométrique »[21].

7.3 ACCÈS AUX DONNÉES

Toutes les données sont stockées sur les serveurs centraux. La plupart des collaborateurs n'ont pas besoin d'avoir accès à l'ensemble des données. En restreignant l'accès aux seules données utiles à chaque collaborateur, les risques d'une mauvaise utilisation des données – volontaire ou non – sont diminués. Les abus peuvent également être prévenus. Des règles d'accès et un mécanisme d'autorisation doivent donc être définis par rapport aux fonctions de chaque collaborateur.

Mesures à envisager :

- Le système d'information est organisé d'une manière permettant des accès différenciés en fonction des utilisateurs.
- L'organisation interne définit les droits d'accès de chaque collaborateur en élaborant une matrice des droits d'accès. Cette matrice est régulièrement mise à jour et vérifiée avec les changements de personnel.
- Le collaborateur s'authentifie à la mise en marche du système. Plus la sensibilité des données qu'il traite est grande, plus l'authentification est forte.
- Une journalisation est effectuée sur les accès au système suivant les conditions abordées dans la section « Journalisation ».

[18] Sécurité : Authentifier les utilisateurs | CNIL
[19] Vérifier sa politique de mots de passe | CNIL
[20] Technologiebetrachtungen (admin.ch)
[21] Guide relatif aux systèmes de reconnaissance biométrique (PFPDT)

7.4 ACCÈS À DISTANCE

Les accès à distance peuvent être de plusieurs types et des mesures de protection doivent être envisagées pour chaque situation distincte.

Un accès aux données peut être demandé par un collaborateur qui souhaite travailler depuis l'extérieur et souhaite un accès distant à son ordinateur du bureau. Suivant la politique de l'organisation et la sensibilité des données, ce type d'accès doit être réglementé. Une méthode sûre d'authentification doit être mise en place. L'accès aux données peut aussi être demandé par un tiers autorisé, comme un sous-traitant, par exemple. Le cas doit être clairement réglé et une authentification forte doit être requise. Finalement, avant toutes choses, ce sont les accès frauduleux qui doivent être absolument évités.

La section « Sécurité du réseau » apporte des compléments en matière de sécurité des communications entre un tiers distant et l'organisation.

Mesures à envisager:

- Un accès sécurisé est proposé aux personnes qui souhaitent ou doivent se connecter à distance.
- La méthode d'authentification choisie est forte et donc composée de deux modalités au moins.
- Les ordinateurs personnels sont protégés par un pare-feu (firewall).
- Sous les conditions abordées dans la section « Journalisation », les accès peuvent être journalisés.

7.5 APPROFONDISSEMENTS

D'autres aspects importants à prendre en compte pour les traitements en interne :

	CH-MS [1]	CNIL [8]	ISO 27002 [2]
Analyse des incidents	Sec. 2.5.3		Sec. 5.24, 5.25
Analyse des risques	Sec. 2.2.4		
Authentifier les utilisateurs		Fiche 2	Sec. 8.5
Circonscrire les dommages (Mitigation)	Sec. 2.5.4		
Communication	Sec. 2.5.2, 2.6.3		
Contrôle d'accès physique	Sec. 2.3.1		Sec. 7.1, 7.2
Contrôle de l'implémentation et efficacité des mesures	Sec. 3		Sec. 5.35
Contrôle des accès logiques	Sec. 2.3.1	Fiche 3	
Définition des environnements	Sec. 2.2.2		Sec. 8.31
Gestion des incidents et des violations de données	Sec. 2.4.1, 2.4.3	Fiche 4	Sec. 5.26
Gestion des risques	Sec. 1.5.4		
Gestion des risques liés à la chaîne d'approvisionnement	Sec. 2.2.6		Sec. 5.19
Gouvernance	Sec. 2.2.3		
Inventaire et organisation	Sec. 2.2.1		
Maintenance	Sec. 2.3.5		
Organisation et responsabilités	Sec. 1.5.2, 1.5.3		Sec. 5.4
Plan d'intervention	Sec. 2.5.1		

Plan de restauration (Recovery)	Sec. 2.6.1		
Sécurité des données	Sec. 2.3.3		
Sensibilisation des collaborateurs	Sec. 1.6.17, 2.3.2	Fiche 1	
Stratégie pour gérer les risques	Sec. 2.2.5		Sec. 5.24
Surveillance	Sec. 2.4.2		Sec 8.15, 8.16
Sécurité des sites Web		Fiche 9	
Sauvegarde et archivage		Fiche 10, 11	Sec 8.15
Sécurité des échanges		Fiche 15	

8 CYCLE DE VIE DES DONNÉES

Avec la mise en œuvre des mesures décrites aux sections précédentes, l'accès aux données peut être considéré comme sûr, tant du point de vue physique (accès aux serveurs centraux) que du point de vue du traitement (accès aux ordinateurs personnels et aux applications). La phase suivante consiste à assurer la sécurité des données durant leur cycle de vie. Elles doivent rester intègres et fiables durant l'entier de ce cycle, c'est-à-dire depuis leur introduction dans le système jusqu'à leur destruction, leur anonymisation ou leur archivage, en incluant évidemment toutes les phases de traitement qu'elles vont subir.

Les traitements peuvent être effectués au sein de l'organisation par les collaborateurs autorisés. Toutefois, ils peuvent également être sous-traités à des organisations tierces.

De plus, dans le cadre des traitements, les données sont régulièrement transférées sur des supports mobiles, tels que des clés USB, des disques durs externes, etc. Finalement, garder une trace des différents traitements permet, en cas de problèmes, de mieux comprendre d'où ils proviennent.

Tous ces aspects et situations doivent être étudiés afin d'éviter des abus.

Pour cette thématique, nous abordons les questions suivantes :

- Comment gérer l'introduction des données dans le système?
- Comment chiffrer les données?
- Comment assurer la sécurité des différents supports de données?
- Comment assurer la sauvegarde les données?
- Comment détruire de manière définitive les données?
- Comment gérer la sécurité de l'information et la protection des données?
- Comment surveiller les traitements sur les données (journalisation)?
- Comment établir un règlement de traitement?

8.1 SAISIE DE DONNÉES

La saisie de données dans le système est une étape délicate. En plus des différents problèmes de sécurité (notamment vus dans Infrastructure et Accès et traitements), il s'agit d'éviter d'introduire dans le système des données incomplètes ou erronées. Une fois les données saisies, les traitements qui seront effectuées sur cette base pourraient conduire à des résultats incorrects et des décisions inappropriées.
Le choix de la plateforme d'entrée, la politique d'accès aux données, la validation et la vérification sont autant d'éléments importants dans la saisie des données.
De plus, il faut distinguer la saisie de données dans un système en phase de test en phase productive.

Mesures à envisager :

- Les données sont introduites uniquement par du personnel formé et autorisé.
- Des mécanismes d'aide sont mis en place dans le système. Ces mécanismes repèrent les informations manquantes et effectuent éventuellement des contrôles de vraisemblance sur les saisies.
- Les données utilisées pour les tests sont soit des données fictives, soit des données anonymisées.
- L'introduction des données est journalisée (Journalisation).

8.2 CHIFFREMENT DES DONNÉES

Les données sont habituellement mémorisées sur un disque dur sous forme de fichiers ou dans une base de données. Une méthode pour protéger les données personnelles et éviter qu'elles ne soient lues et modifiées de manière abusive consiste à chiffrer ces données. À l'aide d'une clé, les données sont transformées en un code non compréhensible. Ainsi, le chiffrement rend les données inintelligibles pour celui qui ne possède ou ne connaît pas la clé.

Niveaux de chiffrement

Le chiffrement peut se faire à différents niveaux. Les données stockées (« at rest ») doivent idéalement être chiffrées en tout temps. Le chiffrement à ce niveau protège contre les accès extérieurs à l'organisation, par exemple contre la perte de l'infrastructure physique (disque dur volé ou mal effacé avant d'être jeté).

Comme les utilisateurs et applications ont besoin des données déchiffrées pour travailler, il est recommandé de faire un niveau de chiffrement supplémentaire à l'interne. Les données peuvent être séparées en différentes zones, chacune ayant leur propre chiffrement et autorisant uniquement les utilisateurs et applications agrées à accéder aux données déchiffrées. Ce niveau protège les données contre des accès internes non autorisés, par exemple par des membres de l'organisation malveillants ou piratés.

Il existe également la possibilité du chiffrement au niveau du fichier, ou les parties sensibles des données sont chiffrées séparément du reste, ce qui permet une protection très granulaire et donc la possibilité d'exploiter les données non sensibles sans mettre à risque les autres données, ce qui est néanmoins plus complexe à mettre en œuvre.

Il faut donc choisir le niveau approprié de chiffrement selon l'utilisation prévue des données et leur sensibilité.

Il est également important de choisir une méthode de chiffrement appropriée, spécifiquement de ne pas utiliser des méthodes maintenant obsolètes. Différents algorithmes recommandés au moment de l'écriture de ce guide sont par exemple :

- AES (avec une clé de 128 ou 256 bits) avec un mode de construction approprié (CCM, GCM, ou EAX) ou ChaCha20 (avec Poly1305) pour le chiffrement symétrique
- RSA-OAEP, ECIES-KEM ou DLIES-KEM pour le chiffrement asymétrique ;
- SHA-256, SHA-512 ou SHA-3 comme fonctions de hachage

Vous pourrez trouver des informations plus détaillées sur le site de l'ANSSI[22]

Mesures à envisager :

- L'algorithme de chiffrement et plus particulièrement la longueur de la clé sont proportionnels à la sensibilité des données.
- Sur un même support de données, différents groupes de données peuvent être chiffrés avec des clés propres.
- Les clés de chiffrement sont sécurisées.
- L'accès aux clés est limité à un nombre restreint de collaborateurs.

[22] Mécanismes cryptographiques | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

8.3 SÉCURITÉ DES SUPPORTS

Les données ne sont pas seulement mémorisées sur les serveurs centraux et les ordinateurs personnels. De nombreux supports externes permettent de transférer de l'information entre collaborateurs ou vers l'extérieur sans avoir à passer par le réseau. Des sauvegardes temporaires et limitées sont également possibles sur ces supports.

Parmi les supports externes, les clés USB, les disques durs externes, les CD-ROM, etc. ont des fonctions diverses puisqu'ils n'ont pas tous les mêmes propriétés. Certains sont réinscriptibles, comme les clés USB, d'autres ne le sont pas, comme les CD-ROM. Il est possible de stocker une quantité de données toujours plus importante sur un support toujours plus petit. Il faut garder cela à l'esprit pour ne pas sous-estimer les risques liés à ces supports.

Mesures à envisager :

- Les collaborateurs sont formés aux dangers d'introduire un support inconnu (clé USB, …) dans son ordinateur.
- Les supports externes contenant des données personnelles sensibles ou des profilages sont chiffrés.
- Les supports externes doivent être mis sous clé.
- Une procédure de destruction des supports est mise en place et les outils nécessaires à cette destruction sont disponibles.
- Une revue régulière de la configuration et des mises à jour est prévue.

8.4 SAUVEGARDE DES DONNÉES

Il est essentiel d'assurer l'intégrité et la disponibilité des données contenues dans le système. Il faut donc définir une procédure pour la sauvegarde des données. Ainsi, si les données sont détruites à la suite d'une mauvaise utilisation ou d'un traitement frauduleux ou si elles sont corrompues, il doit être possible de les récupérer dans l'état le plus récent possible. La fréquence de sauvegarde doit être proportionnelle à la quantité de traitements effectués journellement sur les données.

Mesures à envisager:

- Une stratégie de sauvegarde est définie de manière appropriée en fonction des données elles-mêmes, de leur quantité et de leur fréquence de modification.
- La stratégie de sauvegarde est communiquée aux collaborateurs.
- Les serveurs de sauvegarde doivent être soumis aux mêmes mesures de sécurité que les serveurs centraux.
- La récupération des données est effectuée par du personnel formé à cette tâche.

8.5 DESTRUCTION DES DONNÉES

Comme cela ressort de l'article 6 al. 4 LPD, les données personnelles n'ont pas pour vocation à être conservées sans aucune limite de temps. Leur durée de conservation doit être définie et des mécanismes pour la destruction définitive de ces données doivent être établis. Ainsi, il ne suffit pas d'effacer simplement ses données d'un disque dur pour considérer qu'elles sont détruites. Il faut véritablement s'assurer qu'elles ne seront plus jamais accessibles. Il en va de même pour les données qui sont contenues sur papier ou sur des supports mobiles. Les copies de sauvegardes doivent également être détruites.

Mesures à envisager :

- Une stratégie de suppression est définie de manière appropriée pour assurer une destruction graduelle et complète des données personnelles, y compris dans les sauvegardes après la fin de leur utilité.
- Les données sont effacées à l'aide de programmes spéciaux qui garantissent un effacement total et définitif des données (en nettoyant les espaces vides, par exemple).
- Les données papier sont détruites par une déchiqueteuse de papiers.
- Les CD-ROM et autres supports mobiles sont également détruits physiquement s'ils ne peuvent pas être complètement nettoyés d'une autre manière.

8.6 NIVEAU DE SÉCURITÉ ET PROTECTION

Pour sécuriser les données de manière optimale, il peut être utile de mettre en relation la nature des données personnelles liée à un niveau de risque et à la classification de l'information (par exemple « non classifié, interne, confidentiel »). Une matrice de classification est proposée ci-dessous. S'agissant d'un instrument générique, cette matrice ne sera pas toujours adéquate pour tous les cas de figure ; elle doit ainsi être adaptée selon les besoins spécifiques de l'organisation.

Tableau 1: Matrice de mesures selon la confidentialité et le risque lié aux données personnelles

Protection des données / Prot. de l'information	Données non personnelles	Données personnelles non sensibles	Données personnelles sensibles	Données personnelles "ultrasensibles"
		Risque: minimal/moyen	Risque: élevé	Risque: très élevé
Information non classifiée		**Protéger l'accès**	Protéger **+ Chiffrer** **+ Journaliser le traitement**	Protéger Chiffrer Journaliser **+ Numéroter (*)**
Information INTERNE	**Protéger l'accès**	Protéger	Protéger Chiffrer Journaliser	Protéger Chiffrer Journaliser Numéroter
Information CONFIDENTIELLE	Protéger **+ Chiffrer**	Protéger Chiffrer	Protéger Chiffrer Journaliser	Protéger Chiffrer Journaliser Numéroter
Information SECRÈTE	Protéger Chiffrer **+ Numéroter (*)**	Protéger Chiffrer Numéroter	Protéger Chiffrer Journaliser Numéroter	Protéger Chiffrer Journaliser Numéroter

(*) La numérotation des copies du document est une mesure en relation avec la protection de l'information.

Dans l'exemple de matrice ci-dessus, nous utilisons les définitions du risque suivantes :

1. ***Risque minimal*** : données personnelles dont l'abus ne semble pas, en règle générale, avoir de conséquence particulière pour la personne concernée. Il s'agit par exemple du nom et du prénom, ou alors d'informations publiques.
2. ***Risque moyen*** : données personnelles dont l'abus peut affecter la situation économique ou la place dans la société de la personne concernée. Il s'agit par exemple de données relatives à la situation d'un locataire, aux relations professionnelles, ou un profilage.
3. ***Risque élevé*** : données personnelles dont l'abus peut gravement affecter la situation économique ou la place dans la société de la personne concernée. Il s'agit par exemple de données sensibles ou de profilages à risque élevé.
4. ***Risque très élevé*** : données personnelles « ultrasensibles » dont l'abus peut mettre en danger la vie de la personne concernée. Il s'agit par exemple d'adresses d'hommes de liaison de la police, d'adresses de témoins dans certaines poursuites pénales ou d'adresses de personnes qui sont menacées suite à l'expression de leurs opinions ou de leur appartenance religieuse ou politique.

Mesures à envisager :

- Le système est élaboré en fonction d'une matrice adaptée.
- Les mesures mise en œuvre sont en adéquations avec la matrice.

8.7 JOURNALISATION

Il est généralement utile de garder une trace de tous les traitements effectués sur les données. Il peut s'agir en particulier de la consultation des données, de l'ajout de nouvelles données, de modifications de données existantes ou de la destruction de données. En conservant une trace de ces différentes actions, il est possible, en cas de problèmes, de remonter à la source d'un incident (accès frauduleux, traitement non autorisé sur les données, …).

Ces actions peuvent être journalisées : un enregistrement séquentiel de tous les événements qui sont liés au système d'informations est effectué et ces fichiers de journaux (ou « logs ») sont conservés sur une période adaptée à la sensibilité des données et des traitements et à leurs finalités.

L'art. 4 OPDo règle la question de la journalisation. Il y est ainsi prescrit qu'en présence de traitements automatisés de données sensibles à grande échelle ou de profilage à risque élevé et si les mesures préventives ne suffisent pas à garantir la protection des données, le responsable privé et son sous-traitant doivent journaliser au moins les événements suivants : l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données.

La journalisation doit fournir des informations sur l'identité de la personne qui a effectué le traitement, la nature, la date et l'heure du traitement et, cas échéant, l'identité du destinataire des données.

Les fichiers de journaux doivent répondre à des exigences spécifiques :

- ils doivent être conservés dans un système séparé de celui dans lequel les données personnelles sont traitées ;
- ils doivent être conservés durant au moins un an ;

- ces fichiers ne doivent être accessibles qu'à cercle restreint de personnes, soit celles chargées de vérifier l'application des dispositions relatives à la protection des données personnelles ou de préserver ou restaurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ils ne peuvent être utilisés qu'à ces fins.

Pour les données personnelles généralement accessibles au public, l'enregistrement, la modification, l'effacement et la destruction des données doivent au moins être journalisés.

Journaliser tous les traitements de données personnelles demande un investissement important. Pour faciliter la mise en place d'un protocole de journalisation, ainsi que pour mieux identifier si une telle obligation existe, voici quelques réponses à des questions fréquemment posées :

- Il n'est pas attendu que la journalisation des données personnelles soit séparée de la journalisation de sécurité des informations. La redondance n'est donc pas nécessaire.
- L'obligation de journalisation s'applique uniquement aux données personnelles dans des systèmes de traitement automatisé des données. Par exemple, un accès manuel à un document texte contenant des informations personnelles n'a donc, du point de vue de l'art. 4 OPDo, pas forcément besoins d'être journalisé. Au contraire, l'exécution d'un script qui efface les données personnelles dans le même document doit l'être.
    - Néanmoins, il est important de noter qu'il peut être dans l'intérêt du responsable de traitement de journaliser quand même ces activités, ou de ne pas permettre le traitement de certaines données personnelles sur des documents non journalisés.
- Par « généralement accessible au public », on entend des données dont l'accès ne requiert aucune identification, ou accessible par un grand nombre de personnes.

Des informations supplémentaires au sujet de la journalisation sont disponibles sur le site du PFPDT[23].

Un protocole de journalisation peut aussi être intégré au système sur une base volontaire. Cela étant, la nécessité de cette journalisation doit être claire et associée à des buts précis ; il s'agit en effet d'éviter de simplement créer des données supplémentaires – et donc des risques supplémentaires – sans justification. De plus, la journalisation doit être proportionnelle en termes de quantité d'informations journalisées et de durée de conservation des fichiers de logs.

Mesures à envisager :

- Le contenu des fichiers de logs et la durée de conservation de ces fichiers sont proportionnels aux données et aux traitements effectués.
- Les collaborateurs sont informés qu'une trace des actions qu'ils effectuent sur les données est conservée.
- Les fichiers issus de la journalisation (journaux) sont sécurisés.
- Les droits d'accès sur les journaux sont clairement définis et limités à certaines fonctions au sein de l'organisation.
- Le protocole est protégé contre des éventuelles attaques ou des accès frauduleux.

[23] Recommandations techniques du PFPDT relative à la journalisation prévue à l'art. 4 OPDo (PDF)

8.8 RÈGLEMENT DE TRAITEMENT

Le règlement de traitement est un outil prévu aux articles 5 et 6 OPDo. Le règlement (sous forme de manuel ou de documentation) donne des indications sur l'organisation interne, par exemple la description de l'architecture du système ; sur les procédures de traitement des données, en particulier la communication des données et l'exercice des droits d'accès ; sur les procédures de contrôle (autorisations) et sur les mesures techniques et organisationnelles de sécurité des données.

Le règlement de traitement doit être élaboré par le responsable du traitement et son sous-traitant. S'il est obligatoire, il doit être régulièrement l'actualisé et être mis à disposition du conseiller à la protection des données.

Contenu du règlement et obligation

Le responsable du traitement privé est tenu d'élaborer un tel règlement s'il opère des traitements automatisés sur des données sensible à grande échelle ou en lien avec de profilages à risque élevé. Le règlement doit contenir notamment des informations sur l'organisation interne, sur les procédures de traitements et de contrôle des données, ainsi que les mesures visant à garantir la sécurité des données (art. 5 OPDo).

Si le responsable du traitement est un organe fédéral (art. 6 OPDo), le règlement de traitement est obligatoire pour les traitements automatisés en cas :

a. de traitement de données sensibles ;
b. de profilage ;
c. de traitement de données personnelles au sens de l'art. 34, al. 2, let. c, LPD ;
d. d'accès aux données personnelles accordé aux cantons, aux autorités étrangères, aux organisations internationales ou aux personnes privées ;
e. d'ensembles de données interconnectés ;
f. d'exploitation d'un système d'information ou de gestion d'ensembles de données conjointement avec d'autres organes fédéraux.

Un modèle de règlement de traitement est disponible sur le site du PFPDT[24].

[24] Règlement de traitement (personnes privées) (DOCX)

9 PARTAGE ET TRANSFERT

Le principe de la proportionnalité, art. 6 al. 2 LPD, et art. 5 al. 1 let. c RGPD, implique la limitation des accès aux données personnelles.

Les art. 9 LPD et 7 OPDo contiennent des prescriptions générales relatives au recours à un sous-traitant dans le cadre de la protection des données personnelles.

Les moyens de communications actuels permettent de travailler à distance, d'échanger de l'information facilement et rapidement. Ainsi, les données ne restent pas simplement à l'intérieur de l'organisation mais sont souvent transmises à l'extérieur. Des contacts avec des tiers sont réguliers. La protection des données durant leur transfert doit également être garantie.

Nous abordons ici les questions suivantes :

- Comment assurer une sécurité suffisante ?
- Comment chiffrer un message que l'on envoie à un tiers ?
- Comment signer un message que l'on envoie à un tiers ?
- Comment transmettre les supports mobiles de manière sécurisée ?
- Comment garder une trace des différentes communications ?
- Quelles sont les spécificités du transfert de données à l'étranger ?

9.1 SÉCURITÉ DU RÉSEAU

Les communications au sein du réseau interne d'une organisation sont nombreuses. Il peut s'agir de collaborateurs qui travaillent à distance et souhaitent se connecter au réseau interne ou de tiers qui accèdent aux données par ce biais. La sécurité du réseau et des communications doit être garantie. Les accès se font généralement via Internet. Il est donc indispensable d'utiliser des protocoles de communication sécurisés. Le protocole TLS (Transport Layer Security), successeur de SSL (Secure Sockets Layer), permet d'établir un canal de communication chiffré sécurisé entre un client et un serveur. Les algorithmes et les clés cryptographiques sont négociés entre le client et le serveur. TLS permet également aux deux parties de s'authentifier à l'aide de certificats. Ce protocole est une sous-couche des protocoles de communications usuels (HTTP, FTP, etc.). Il est transparent pour l'utilisateur et son utilisation peut être remarquée par l'apparition d'un cadenas fermé dans la fenêtre de la plupart des navigateurs.

De plus, la mise en place de connexions VPN (Virtual Private Network – réseau privé virtuel) permet de sécuriser l'accès au réseau interne. Il permet d'encapsuler les données chiffrées à transmettre. Un réseau VPN est basé sur des protocoles cryptographiques forts, tels que TLS, IPSec ou SSTP.

Mesures à envisager :

- Les communications via Internet du réseau interne vers l'extérieur doivent être limitées au strict nécessaire.
- Vérifier que la mise en place d'un protocole de communication sécurisé (par ex. TLS) soit prévue pour les traitements à effectuer sur les données.

- Mettre en place un VPN si des collaborateurs ou des tiers sont amenés à se connecter à distance au réseau local de l'organisation
- Vérifier quotidiennement les mises à jour des différents logiciels utilisés et s'assurer de les faire pour maintenir un niveau de sécurité maximal.

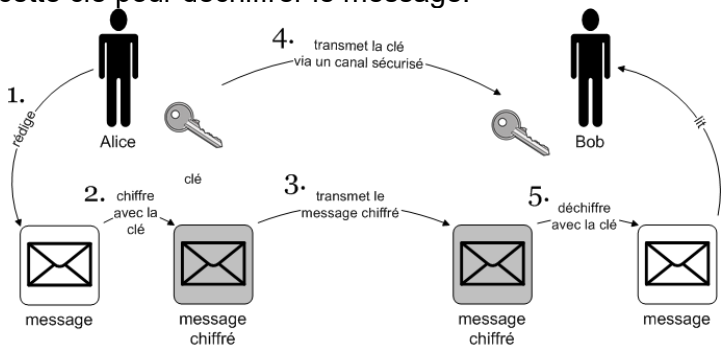
9.2 CHIFFREMENT DES MESSAGES

Parallèlement au chiffrement des disques durs et des fichiers pour empêcher les accès indésirables aux données, il est nécessaire de chiffrer les messages afin d'éviter qu'une tierce partie écoute la communication et soit en mesure de lire, de modifier ou de supprimer le message.

Il existe deux méthodes pour le chiffrement de message : le chiffrement symétrique et le chiffrement asymétrique.

Le chiffrement symétrique fonctionne selon le schéma ci-dessous:

1. Alice rédige un message pour Bob.
2. Alice chiffre son message au moyen d'une clé.
3. Alice transmet le message chiffré à Bob.
4. Alice transmet la clé à Bob de manière sécurisée.
5. Bob utilise cette clé pour déchiffrer le message.

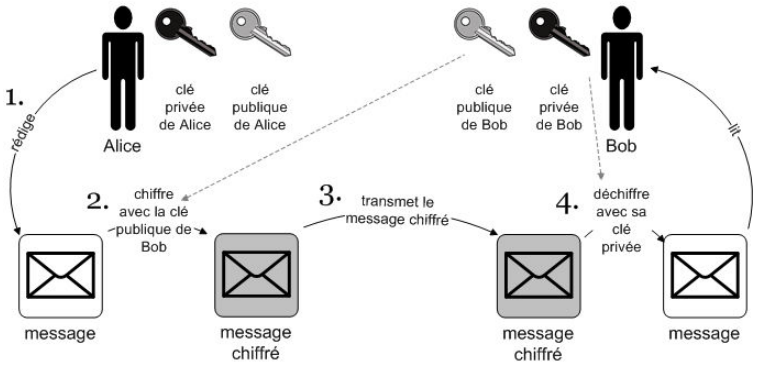


Le chiffrement symétrique est plus simple à mettre en œuvre car il ne comprend qu'une seule clé. Toutefois, la transmission de cette clé doit être effectuée de manière sûre.

Le chiffrement asymétrique est plus complexe mais il évite les problèmes liés à la transmission de la clé. Ce n'est pas une clé qui est utilisé mais deux. Chaque utilisateur génère une paire de clés : l'une est publique et rendue disponible à tous, la seconde est privée et connue de l'utilisateur seulement. La clé publique est utilisée pour chiffrer le message et la clé privée pour le déchiffrer. Cette technique permet également de signer les messages (cf. section « Signature des messages »).

Le déroulement illustré ci-dessous est le suivant :

1. Alice prépare un message pour Bob.
2. Alice utilise la clé publique de Bob pour chiffrer le message – elle s'assure ainsi que seul Bob – en utilisant sa clé privée – pourra le lire.
3. Alice envoie le message à Bob.
4. Bob utilise sa clé privée pour déchiffrer le message.



De nombreuses applications aujourd'hui utilisent pas un chiffrement asymétrique pur, mais chiffrent les données avec un algorithme symétrique et additionnellement chiffrent la clé de chiffrement symétrique avec un algorithme de chiffrement asymétrique. Cette méthode de chiffrement hybride combine les avantages de la vitesse du chiffrement symétrique avec la sécurité du chiffrement asymétrique.

Mesures à envisager :

- Déterminer quel type de chiffrement est le plus adéquat, suivant la sensibilité des données et les tiers avec qui l'organisation traite.
- Si le chiffrement symétrique est utilisé, il faut définir un protocole sûr pour la transmission de la clé (l'email, par exemple, n'est pas sûr).
- Si on choisit le chiffrement asymétrique, il faut mettre en place un mécanisme de chiffrement des messages. Il convient de le coupler avec la signature des messages (cf. section « Signature des messages »).

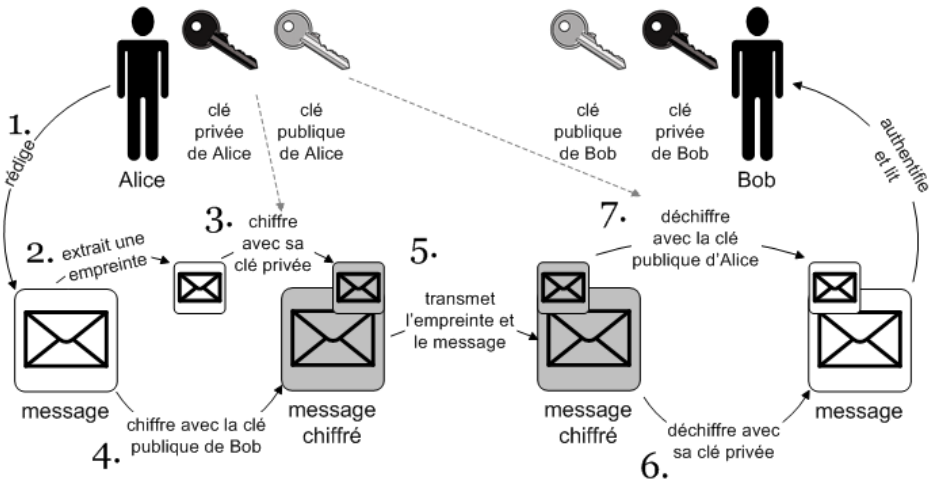
Reste à Alice de vérifier que la clé publique qu'elle a est vraiment celle de Bob, et non pas celle d'un « intermédiaire » entre eux (man-in-the-middle). Pour ceci, la clé publique de Bob peut être signée par une autorité supérieure, dont la clé publique peut être aussi signée, et ainsi de suite jusqu'à un niveau connu et vérifiable par Alice. Les signatures de messages, ou des clés publiques, sont expliquées dans la section suivante.

9.3 SIGNATURE DES MESSAGES

En chiffrant un message (cf. section « Chiffrement des messages »), il est possible de s'assurer que seule la personne en possession de la clé nécessaire au déchiffrement sera capable de lire le message. Il peut également être nécessaire que le destinataire du message soit en mesure de s'assurer que l'expéditeur est bien celui qu'il prétend être. En signant le message, l'expéditeur peut transmettre cette information de manière sûre.

Cette action est habituellement effectuée préalablement au chiffrement du message selon le protocole suivant :

1. Alice rédige un message.
2. Alice extrait une empreinte de ce message. Cette empreinte sert de signature au message.
3. Alice signe cette empreinte avec sa clé privée.
4. Elle chiffre ensuite le message selon la procédure décrite plus haut.
5. Alice transmet l'empreinte et le message à Bob.
6. Bob déchiffre le message.
7. Il vérifie ensuite l'empreinte avec la clé publique d'Alice et s'assure ainsi qu'elle est bien l'expéditrice du message.



Mesures à envisager :

- Les collaborateurs sont sensibilisés aux situations dans lesquelles une communication doit être signée et chiffrée.
- Les collaborateurs connaissent la manière de chiffrer et de signer les messages.

9.4 TRANSMISSION DES SUPPORTS DE DONNÉES

La transmission des supports de données mobiles est un problème délicat puisque cela implique qu'une partie des données sort de manière physique de l'organisation et est transportée vers un autre lieu. Il est essentiel que ces supports soient protégés durant leur transport afin d'éviter qu'en cas de perte ou – plus grave – de vol, les données ne deviennent accessibles. Plus les données contenues sur les supports mobiles sont sensibles, plus la transmission doit être sécurisée.

Mesures à envisager :

- Les destinataires à qui sont remis les supports peuvent être authentifiés de manière sûre.
- La mise sous pli des supports avant la transmission est effectuée de manière sécurisée.
- Si nécessaire, les supports sont chiffrés.
- Un protocole de transport est défini. Par exemple, les supports peuvent être transportés dans des valises fermées à clé.
- Le principe des quatre yeux permet d'assurer que la remise et la réception des données est effectuée correctement.

9.5 JOURNALISATION DES TRANSFERTS

L'envoi de données via le réseau et la transmission de supports mobiles peuvent être protocolés et enregistrés dans un journal. Ce mécanisme de journalisation permet de tracer les expéditeurs et les destinataires des données et la manière dont les supports ont été transmis. Ainsi, en cas d'abus, de mauvaise utilisation ou d'action malencontreuse, ces

informations permettent de retracer le parcours des données depuis l'expéditeur jusqu'à la survenance du problème.

Les considérations développées dans la section « Journalisation » s'appliquent également pour les journalisations de transfert.

Mesures à envisager :

- Définir une journalisation très précise qui recense les expéditeurs, les destinataires, le trajet effectué et tous les points intéressants du trajet.
- Il est préférable de confier toujours les transferts de supports aux mêmes collaborateurs.
- Il est nécessaire d'appliquer le principe de proportionnalité à la journalisation des transferts, suivant leur ampleur, la durée, etc.

9.6 COMMUNICATION DE DONNÉES À L'ÉTRANGER

La transmission de données personnelles à l'étranger peut comporter des risques importants : elle fait donc l'objet d'une réglementation assez détaillées aux articles 16 à 18 LPD et 8 à 12 OPDo. Par défaut, les données personnelles ne devraient pas être transmises à l'étranger. Schématiquement, il existe trois types de situations autorisant néanmoins ces transferts :

Approbation du Conseil Fédéral

Le premier cas est détaillé aux art.16 al.1 LPD et art. 8 OPDo. Le Conseil fédéral établit une liste positive d'Etats dont la législation sur la protection des données est considérée comme adéquate. Si un Etat ne s'y trouve pas, c'est soit que sa législation est jugée insuffisante, soit qu'elle n'a pas encore été examinée. A noter qu'outre les Etats, il peut aussi s'agir d'organismes internationaux. La liste peut être trouvée dans l'annexe 1 de l'OPDo[25].

Instruments spécifiques

Le second cas est détaillé aux art. 16 al. 2 LPD et art. 9 et suivants OPDo. Si l'Etat concerné ne figure pas dans la liste précitée, il existe plusieurs outils de protection de données qui, s'ils sont utilisés, permettent malgré tout des communications de données vers cet Etat. La loi mentionne les outils suivants :

- un traité international ;
- une clause de protection des données d'un contrat entre le responsable du traitement ou le sous-traitant et son co-contractant, préalablement communiqué au PFPDT ;
- des garanties spécifiques élaborées par un organe fédéral compétent et préalablement communiquées au PFPDT ;
- des clauses-types de protection des données préalablement approuvées, établies ou reconnues par le PFPDT ;
- des règles d'entreprise contraignantes préalablement approuvées par le PFPDT ou par une autorité chargée de la protection des données originaire d'un Etat qui assure un niveau de protection adéquat.

A cette liste, l'art. 12 OPDo ajoute encore les codes de conduite et les certifications qui, à certaines conditions, peuvent fonder une communication de données à l'étranger.

[25] États, territoires, secteurs déterminés dans un État et organismes internationaux dans lesquels un niveau de protection adéquat des données est garanti

Situations dérogatoires
Le troisième cas est détaillé dans l'art. 17 LPD. Hors des situations exposées ci-dessus, une communication à l'étranger peut être admissible dans certains cas particuliers : il s'agit essentiellement de situations où la personne concernée est d'une certaine manière associée à cette transmission, ou que la transmission vise à préserver des intérêts importants. Les situations envisagées par la LPD sont les suivantes :

- si la personne concernée a donné son consentement à la transmission ;
- si la personne concernée a rendu les données personnelles accessibles à tous et ne s'est pas expressément opposée au traitement ;
- si la transmission est en relation directe avec la conclusion ou l'exécution d'un contrat entre le responsable et la personne concernée ;
- si la transmission est en relation directe avec la conclusion ou l'exécution d'un contrat entre le responsable et son cocontractant dans l'intérêt de la personne concernée ;
- si la transmission est nécessaire à la sauvegarde d'un intérêt public prépondérant ;
- si la transmission est nécessaire à la constatation, à l'exercice ou à la défense d'un droit devant un tribunal ou une autre autorité étrangère compétente ;
- si la transmission est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et qu'il n'est pas possible d'obtenir l'accord de la personne concernée dans un délai raisonnable ;
- si les données personnelles proviennent d'un registre prévu par la loi, accessible au public ou à toute personne justifiant un intérêt légitime, pour autant que les conditions légales dans ce cas soient réunies.

En outre, selon les cas, le responsable du traitement doit, sur demande, informer le PFPDT des communications qu'il effectue (art. 17 al. 2 LPD).

Mesures à envisager :

- Prendre en compte dès la conception, et avant de procéder à tout transfert, les exigences et risques d'un transfert de données à l'étranger.
- Vérifier régulièrement la liste des pays figurant dans l'annexe 1 de l'OPDo.
- Si nécessaire, examiner la possibilité et l'adéquation de recourir à l'un des outils évoqués ci-dessus.

9.7 SOUS-TRAITANCE

Il arrive régulièrement qu'une organisation recourt à des sous-traitants en relation avec la gestion des données qu'elle traite. A titre d'exemple, l'on peut citer le stockage de données auprès de tiers, le recours à des solutions IT fournies et entretenues par des entreprises tierces (notamment via le cloud) ou plus largement, le fait de leur confier une tâche déterminée, telle la facturation, le démarchage, etc. L'organisation qui fournit le mandat doit s'assurer que le sous-traitant est en mesure de garantir la protection des données de manière adéquate (art. 9 al. 2 LPD). En outre, elle reste responsable du traitement et donc responsable vis-à-vis des personnes concernées et des autorités.

Le responsable du traitement peut uniquement transférer des données personnelles si cela est prévu par la loi ou un contrat. En outre, le tiers ne peut effectuer que des traitements que le responsable serait lui-même en droit d'effectuer. Enfin, aucune obligation légale ou

contractuelle de garder le secret ne doit l'interdire (art. 9 al. 1 LPD). A noter encore qu'un sous-traitant ne peut lui-même sous-traiter qu'avec l'autorisation du responsable du traitement (art. 9 al. 3 LPD).

Mesures à envisager :

- Vérifier la fiabilité de l'offre des sous-traitants, leur réputation et leur expertise dans le cadre de la sécurité et protection des données.
- Établir un contrat avec le sous-traitant qui encadre le traitement de données par celui-ci et permette d'assurer le respect les obligations du responsable du traitement vis-à-vis des personnes concernées (confidentialité des données, conditions de restitution et destruction, gestion des incidents, demandes d'accès, …).
- Prévoir des mécanismes permettant de s'assurer que le sous-traitant respecte ses engagements en matière de protection des données (audits de sécurité, chiffrement des données selon leur sensibilité…).

Vous pourrez trouver des recommandations et outils supplémentaires sur la page de l'OFCS[26].

10 CONSIDÉRATIONS FINALES

L'application des mesures techniques et organisationnelles présentées dans ce guide permet d'assurer une protection des données appropriée. Toutefois, il est nécessaire de toujours prendre en compte le contexte global dans lequel s'inscrit un projet, sa sensibilité, la quantité de données nécessaires, etc.

La responsabilité de la protection des données incombe au responsable du traitement. Aborder ce problème le plus tôt possible lors du développement d'un projet est le meilleur moyen de non seulement gérer les différents risques, mais aussi d'être en mesure de respecter ses diverses obligations vis-à-vis des demandes que peuvent formuler les personnes concernées.

[26] Collaborer avec des prestataires externes de services informatiques (admin.ch)

11 REFERENCES

[1] Office fédérale de l'approvisionnement économique du pays OFAE, «Norme minimale pour les TIC,» 2023. [En ligne]. Available: https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html. [Accès le 25 08 23].

[2] ISO, «Normes,» [En ligne]. Available: https://www.iso.org/fr/standards.html. [Accès le 29 août 2023].

[3] ISACA, «COBIT | Control Objectives for Information Technologies | ISACA,» [En ligne]. Available: https://www.isaca.org/resources/cobit. [Accès le 29 août 2023].

[4] Federal Office for Information Security - BSI, «Technical Guidelines,» [En ligne]. Available: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/technische-richtlinien_node.html. [Accès le 29 août 2023].

[5] NIST, «National Institute of Standard and Technology,» [En ligne]. Available: https://www.nist.gov/. [Accès le 29 août 2023].

[6] CNIL, «Analyse d'impact relative à la protection des données - Les bases de la connaissance,» Février 2018. [En ligne]. Available: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf. [Accès le 25 août 2023].

[7] Groupe Article 29, «Avis 05/2014 sur les Techniques d'anonymisation,» 10 avril 2014. [En ligne]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf. [Accès le 25 août 2023].

[8] CNIL, «Guide pratique RGPD - Sécurité des données personnelles,» Mars 2023. [En ligne]. Available: https://www.cnil.fr/sites/cnil/files/2023-04/cnil_guide_securite_des_donnees_personnelles-2023.pdf [Accès le 25 août 2023].

[9] Organisation internationale de normalisation, «ISO/IEC 27002:2022 Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information,» 2022. [En ligne]. Available: https://www.iso.org/fr/standard/75652.html. [Accès le 09 2023].