AGENTIL

Déclaration sur la Protection des Données

27 Novembre 2024

Version 1.1

1. Introduction

AGENTIL SA (ci-après : AGENTIL) accorde une grande importance à un traitement des données personnelles responsable et conforme au droit. Le traitement des données personnelles s'effectue uniquement sur la base du droit applicable.

Dans la présente déclaration de protection des données, nous informons nos clients ainsi que les visiteurs de nos sites Internet (ci-après : clients) de la collecte, du stockage et du traitement des données personnelles.

Nous traitons les données uniquement sur la base du droit applicable. Le traitement des données est soumis à la nouvelle loi fédérale sur la protection des données (nLPD) et aux ordonnances relatives à la loi nouvelle fédérale sur la protection des données (OnLPD).

La consultation de nos sites Internet depuis l'étranger peut également être soumise aux législations étrangères sur la protection des données.

AGENTIL se réserve le droit de modifier en tout temps la présente déclaration de protection des données. La version en vigueur est celle publiée à l'adresse : www.agentil.com.

La présente déclaration de protection des données décrit nos pratiques et se compose des chapitres suivants :

- La collecte des données
- Les données
- Les traitements
- Les mesures de protection
- L'organisation

2. La Collecte des Données

Nous collectons et traitons les données qui sont nécessaires à notre activité, par exemple :

- Données personnelles (nom, prénom, fonction, adresse, etc.)
- Données de contact professionnelles (téléphone, adresse email, etc.)
- Données de société (toutes les données liées à votre société et vos collaborateurs, les données de votre progiciel, etc.)
- Données financières (relations de compte, vos coordonnées bancaires, votre référencement auprès d'assureur crédit, vos paiements, etc.)
- Données d'identification (p. ex. cookies, adresses IP, etc.),
- Données de localisation (déjà mentionné sur le site internet, etc.)
- Données liées à l'image (témoignages vidéo ou écrits de nos clients, référencement, etc.)
- Etc.

Nous distinguons plusieurs manières dont ces données sont sollicitées.

2.1. Fournies :

Ensemble des données que vous mettez à notre disposition lors de vos visites sur nos sites internet et l'usage de formulaires d'inscription.

2.2. Collectées :

Ensemble des données que nous collectons sur demande, lors, par exemple, de la conclusion d'un contrat. Pour la bonne gestion de notre relation commerciale, nous sollicitons un ensemble d'informations spécifiques ou documents de références.

2.3. Reçues : via tiers (partenaires / fournisseurs)

Ensemble des données vous concernant que nous recevons de tiers de confiance, notamment lors de procédures liées à des contrôles de solvabilité.

2.4. Automatique

Ensemble des données collectées par Cookies, monitoring, etc.

2.5. Le consentement

Avant toute action de collecte de données, AGENTIL respecte la notion de consentement préalable. Par consentement nous entendons : "toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle une personne concernée accepte par une déclaration ou par un acte positif clair que des données à caractères personnels la concernant fassent l'objet d'une collecte et d'un traitement".

2.6. Droits

2.6.1. Le droit d'accès

La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que ses données personnelles et/ou sensibles sont ou ne sont pas traitées et, lorsqu'elles le sont, elle a le droit d'obtenir l'accès auxdites données ainsi qu'à un certain nombre d'informations complémentaire. Ce droit comprend également celui d'obtenir une copie des données qui font l'objet d'un traitement.

2.6.2. Le droit de rectification

La personne concernée a le droit de demander que ses données soient rectifiées ou complétées, et ce dans les meilleurs délais.

2.6.3. Le droit d'effacement ou « droit à l'oubli »

La personne concernée a le droit de demander l'effacement de ses données, dans les meilleurs délais. Si les données de la personne concernée ont été transmises à d'autres entités, le mécanisme du « droit à l'oubli » s'enclenche : le responsable de traitement devra prendre toutes les mesures raisonnables pour informer les autres entités que la personne concernée a demandé l'effacement de tout lien vers ses données personnelles et/ou sensibles, ou de toute copie ou reproduction de celles-ci.

Sous réserve du respect des obligations relatives aux durées légales de conservation des données (voir article 8.1.4).

3. Les Données

AGENTIL traite les données à caractère personnel de ses clients qui sont en contact direct ou indirect avec elle. Nous utilisons le terme « données » comme synonyme du terme « données à caractère personnel ». Les données sont des informations qui se rapportent directement à un client ou que nous pouvons attribuer directement à un client.

Au chiffre 3.2, AGENTIL informe sur les catégories de données traitées conformément aux informations contenues dans la présente déclaration sur la protection des données.

Lorsque des données concernant d'autres personnes nous sont communiquées, l'expéditeur confirme qu'il est habilité à le faire et que les données sont correctes. Avant de nous communiquer ces données, l'expéditeur doit s'assurer que les tiers en question savent que nous traitons leurs données.

La présente déclaration de protection des données s'applique par conséquent aux données que nous avons déjà collectées ou que nous collecterons à l'avenir.

3.1. Quelles données font l'objet d'un traitement ?

Selon la situation et la finalité, nous traitons diverses données à caractère personnel provenant de différentes sources. Nous collectons et obtenons ces données en premier lieu directement auprès de nos clients notamment lors de la mise en place de relations contractuelles, lorsqu'ils utilisent nos produits et services ou dans le cadre de communications générales.

Nous pouvons également obtenir des données à partir d'autres sources, par exemple de registres publics ou d'autres sources accessibles au public, des autorités ou de tout autre tiers. Dans ce cadre, AGENTIL traite différentes catégories de données. Les principales catégories de données sont décrites ci-après :

3.1.1. Données de base :

Les données de base sont des données ayant trait à l'identité ainsi qu'à la situation et aux caractéristiques, comme le nom, l'adresse ou la date de naissance. Ces données peuvent également concerner des tiers (fondés de procuration) et comprennent aussi les droits de signature, les procurations et les déclarations de consentement.

3.1.2. Données contractuelles :

Lorsqu'un contrat est conclu avec nous, nous traitons, outre les données de base, d'autres données, telles que des informations sur l'achat et l'utilisation de produits et de services. Ces données comprennent des informations sur le traitement et l'exécution des contrats ainsi que des retours d'information de nos clients concernant les services.

3.1.3. Données de communication :

Les données de communication sont les données liées à la communication avec nos clients, que cette communication ait lieu sous forme d'échange de courriers, par téléphone ou par le biais de canaux

électroniques (p. ex. via e-mail, SMS etc…). Elles comprennent également les données d'authentification (p. ex. les données d'authentification, les données biométriques etc…) ainsi que les enregistrements vidéo et audio. Lors de la vérification de l'identité (p. ex. en cas de demande de renseignement), nous collectons en outre des données afin de vous identifier (p. ex. au moyen d'une copie d'un document d'identification).

3.1.4. Données techniques :

- Les données techniques sont des données que nous collectons lors de l'utilisation d'une de nos prestations électroniques. Ces données comprennent également l'adresse IP d'un terminal et les journaux dans lesquels nous enregistrons l'utilisation de nos systèmes.
- Afin de garantir le fonctionnement de ces offres, nous pouvons attribuer un code individuel aux terminaux (p. ex. sous la forme d'un cookie). Les données techniques ne permettent pas de tirer des conclusions sur l'identité d'une personne.
- En les combinant avec les données des comptes utilisateurs, des enregistrements, des contrôles d'accès ou de l'exécution des contrats, nous pouvons, le cas échéant, associer d'autres données à des personnes physiques.

3.1.5. Données d'enregistrement :

Les données d'enregistrement sont des données concernant les clients qui sont transmises lors d'un enregistrement ou d'une activation afin d'utiliser certaines offres et services ou de pouvoir y participer (p. ex. les newsletters et les formulaires).

3.1.6. Autres données :

Nous collectons d'autres données relatives aux clients dans différents contextes. Ainsi, des données sont collectées dans le cadre de procédures administratives ou judiciaires (p. ex. des pièces, des moyens de preuve, etc.). Nous pouvons également collecter des données pour des raisons de prévention des fraudes.

3.2. Type de données – définitions

3.2.1. Données à caractère personnel : identification

Les données personnelles se réfèrent à toute information qui permet d'identifier une personne physique ou morale et d'établir une relation univoque.

Cela peut inclure des informations telles que le nom, l'adresse, le numéro de téléphone, l'adresse e-mail, l'adresse IP, le numéro de sécurité sociale, le numéro de carte de crédit, etc.

Par exemple, dans le contexte d'une entreprise, les données personnelles peuvent être les informations des employés, des clients ou des partenaires commerciaux.

3.2.2. Données à caractère privé : identification forte

Les données privées font référence à des informations personnelles qui ne sont pas accessibles au public en général et qui sont considérées comme privées pour une personne ou une entité spécifique.

Cela peut inclure des données de nature financière, telle que les relevés bancaires, les numéros de compte bancaire, les données de carte de crédit, les informations médicales, les dossiers juridiques, les informations

relatives à la vie personnelle, etc. Par exemple, les données privées d'une entreprise pourraient inclure les informations financières internes, les contrats confidentiels, les rapports de recherche et développement non publiés, etc.

3.2.3. Données à caractère sensible : profilage

Les données sensibles sont une sous-catégorie des données privées qui nécessitent une protection renforcée en raison de leur nature extrêmement confidentielle.

Ces données sont considérées comme étant particulièrement sensibles, car leur divulgation ou leur utilisation abusive pourrait causer un préjudice grave à une personne ou une organisation.

Les exemples courants de données sensibles comprennent les informations médicales ou de santé mentale, les données génétiques, les opinions politiques ou religieuses, les orientations sexuelles, les origines ethniques ou raciales, les données biométriques, etc.

Dans le contexte d'une entreprise, les données sensibles peuvent être les informations relatives aux brevets, les secrets commerciaux, les plans de produits futurs, les informations sur la sécurité nationale, etc.

3.3. Analyse d'impact

Pour l'analyse d'impact des données à caractère personnel stocké sur nos systèmes, nous utilisons un outil d'analyse d'impact : PIA (Privacy Impat Assesment), Analyse d'impact sur la Protection des données (AIPD).

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Le logiciel PIA s'inscrit dans une démarche d'accompagnement des responsables de traitement dans la mise en œuvre des obligations de la nLPD. Il permet et accompagne la conduite d'une analyse d'impact relative à la protection des données , qui est obligatoire pour certains traitements.

3.4. Temps de conservation des données

3.4.1. Données hébergées sur notre BCS :

Nous supprimons les données à caractère personnel de notre base de données deux (2) semaines après l'arrêt du contrat. Les données sauvegardées sont quant à elles supprimées un (1) mois après la suppression des données de la base.

3.4.2. Données présentes dans notre ERP :

Les comptes clients sont basculés en statut « inactifs » car il ne nous est pas possible de supprimer intégralement les données pour des raisons de contrôle et d'intégrité des systèmes et d'archives.

3.4.3. Données présentes sur nos supports marketing :

Les données utilisées, diffusées sur nos contenus marketing sont régies par une autorisation de diffusion signée par le client qui est valable 3 ans à partir de la date de signature, cet accord doit être renouvelé à

l'échéance pour qu'AGENTIL puisse continuer à utiliser ces données. Le client peut faire la demande à tout moment de leur suppression.

3.4.4. Données stockées localement :

Les données stockées localement ne sont conservées que le temps nécessaire au traitement qui en est fait. Chaque client peut en demander la suppression à tout moment.

3.5. Date et champ d'application

La présente déclaration de protection des données s'applique à partir du moment ou des données personnelles et/ou sensibles sont mises à notre connaissance.

La présente déclaration de protection des données s'applique à tous les processus durant lesquels nous traitons vos données notamment lors de :

- Consultation de notre site web
- Prise de contact avec nous
- Processus d'avant-ventes, de démonstrations ou de rendez-vous commerciaux,
- Processus contractuel (passage de commande de produits et/ou services, facturation, règlement)
- Processus de livraison des produits et/ou services,
- Processus de diffusion de documents, informations ou communications de notre part,
- Processus marketing,
- Processus de recrutement,
- Etc.

4. Les Traitements

Le traitement désigne toute opération relative à des données, par exemple la collecte, l'enregistrement, l'utilisation, la communication ou l'effacement.

La présente déclaration sur la protection des données décrit comment nous traitons les données lorsque les clients utilisent nos services ou produits, sont en relation avec nous dans le cadre d'un contrat ou communiquent avec nous de manière générale.

La présente déclaration de protection des données s'applique par conséquent au traitement des données que nous avons déjà collectées ou que nous collecterons à l'avenir.

Nous informons séparément de certains traitements de données, par exemple dans d'autres mentions sur la protection des données, dans des CG, dans des descriptions de produits et de services, sur nos sites Internet, dans des déclarations de consentement, des contrats et des formulaires.

4.1. Responsabilités

AGENTIL est responsable du traitement des données conformément à la présente déclaration de protection des données ; elle est également le service compétent en matière de protection des données, sauf indication contraire dans un cas particulier.

Pour exercer vos droits et nous contacter pour toute question concernant la protection des données à caractère personnel, vous pouvez nous joindre :

- par écrit à l'adresse suivante : AGENTIL SA, Protection des données, Rue du Pré-de-la-Fontaine 19, 1242 Satigny - GE,
- par e-mail : dpo@agentil.com,
- par téléphone au +41 (0)22 595 04 04.

4.2. Objectifs / finalités

La présente déclaration a pour objectif de vous informer de façon transparente sur l'utilisation de vos données. Nous utilisons vos données pour :

4.2.1. Conclure / Exécuter d'un contrat :

Dans le cadre de la relation contractuelle, nous procédons à tous les traitements nécessaires à la préparation, la conclusion, l'exécution ou la mise en œuvre du contrat. Avant la conclusion d'un contrat, nous nous renseignons sur votre solvabilité (informations sur votre capacité de paiement et votre conduite en matière de paiements), afin de déterminer si nous pouvons effectivement conclure le contrat et, le cas échéant, sous quelle forme. Pour vous livrer une marchandise commandée, nous pouvons être amenés à transmettre vos données à un prestataire tiers (p. ex. la Poste). De plus, pour le trafic des paiements, nous échangeons vos données avec un prestataire de services financiers.

4.2.2. Communiquer :

Dans le cadre de la relation clientèle, nous échangeons des informations (contrat, documents, etc.) pour la réalisation de nos prestations, l'amélioration de nos services, …

C'est le cas lorsque vous remplissez l'un de nos formulaires de contact, que vous vous adressez à nous par mail, par courrier, par téléphone ou par un autre moyen ou encore lorsque nous prenons contact avec vous. À cet effet, nous traitons en particulier les données suivantes (données personnelles et/ou sensibles, de contact, financières). Nous pouvons exécuter toutes les opérations nécessaires à la communication avec vous, notamment répondre à vos demandes ou vous contacter si nous avons des questions.

Nous attirons votre attention sur le fait que nous enregistrons de manière aléatoire des communications téléphoniques ou des vidéoconférences pour des raisons d'amélioration qualité ou de preuve (certification, audit, etc.) ou sur demande exprès du client.

4.2.3. Des actions marketing et commercial :

Dans le cadre de campagne marketing ou d'action de référencement, nous traitons les informations nous permettant de vous informer sur nos offres de manière appropriée. Nous pouvons vous adresser des informations et des offres par courrier ou par voie électronique (newsletters, emails, ou d'autres messages électroniques et de l'envoi postal de brochures publicitaires, de magazines ou d'autres imprimés, etc.), vous faire part de recommandations de produits ou de services.

Nous pouvons vous remettre des bons ou vous inviter à des événements, des tirages au sort et des concours.

Nous personnalisons ces offres et informations à l'aide des données que vous nous confiez.

4.2.4. Être conforme aux exigences légales :

Dans le cadre de, nous sommes tenus de respecter les exigences légales et, en cas d'infractions, de collaborer avec les autorités.

C'est le cas lorsqu'il s'agit d'appliquer les dispositions relatives à l'ensemble des lois auxquelles nous sommes soumis (RGPD, nLPD, loi informatique et libertés, etc.) et au respect d'autres exigences réglementaires (Certification, audit, etc.).

Nous pouvons être, dans le cadre de la prévention et l'explication d'actes pénaux ou de comportements fautifs, requis de transmettre des informations ou des documents aux autorités ou collaborer à des enquêtes menées par des autorités (p. ex. poursuites pénales ou autorité de surveillance, etc.).

4.2.5. Autres finalités :

Dans le cadre de nos processus internes et de notre administration, nous pouvons exploiter vos données personnelles.

C'est le cas, pour des opérations menées à des fins administratives, statistiques ainsi que l'évaluation et l'amélioration de nos processus internes.

4.3. Lieu de traitement

Vos données sont traitées en Suisse, en France, en Europe ou en dehors de ces zones géographiques. Toujours via des canaux sécurisés.

5. Mesures de Protection

5.1. Accès

Qui a accès à vos données chez AGENTIL et à qui les transmettons-nous ?

5.1.1. Collaborateurs AGENTIL :

Notre organisation défini des rôles, responsabilités et profils précis pour chacune des activités de nos collaborateurs (finances, administration, ventes, etc.). Dans ce cadre nous définissons les règles permettant l'accès à vos données et le type de traitement autorisé. Ces règles sont contrôlées et revues à échéance régulières et peuvent être, en tout moment, modifiées.

5.1.2. Partenaires AGENTIL :

Dans le cadre de la relation avec certains partenaires (éditeurs, sous-traitants, etc.) nous sommes amenés à transmettre certaines données. Par exemple lorsqu'il s'agit de traiter une commande nécessitant de renseigner le nom de l'utilisateur final (gestion des licences).

Dans le cadre de l'hébergement de données sur notre Cloud, notre partenaire est soumis aux mêmes règles et exigences de protection des données.

Dans tous les cas, AGENTIL en contrôle la bonne application.

Nous avons vérifié auprès de nos fournisseurs et partenaires le respect de cette exigence.

Chacun de partenaires ou sous-traitants est tenu de signer un accord de confidentialité mutuel ainsi qu'un engagement sur le respect sur la loi de protection des données.

5.2. Processus

5.2.1. Contrôle des sous-traitants

Nous vérifions auprès de nos fournisseurs et partenaires le respect de cette exigence sur la base d'un contrôle.

5.2.2. Consentement explicite

AGENTIL vous demande un consentement explicite dès le début des échanges car nous accordons une importance fondamentale au consentement explicite de tous nos clients pour la collecte de leurs données personnelles.

Conformément aux principes énoncés par la nLPD, le consentement doit être libre, spécifique, éclairé et univoque. Il est essentiel que nous obtenions une autorisation claire et affirmative de votre part, de manière à garantir la transparence et le respect de votre vie privée.

5.2.3. Sensibilisation des collaborateurs AGENTIL

Nos collaborateurs sont sensibilisés sur la protection des données qu'ils sont amenés à traiter et s'engagent à respecter des règles, principes et devoirs notamment au travers du règlement du personnel, de communications régulières ainsi que d'une charte informatique détaillant les bonnes pratiques.

5.3. Solutions logicielles

5.3.1. PIA (voir article 3.3)

5.3.2. 2FA

Nous utilisons un outil de double authentification pour le contrôle d'accès à nos systèmes.

5.3.3. Safe PW

Nous utilisons un outil de gestion des mots de passe pour la création, le suivi, la mise à jour, le stockage.

5.3.4. Antivirus

Nous utilisons un antivirus pour l'ensemble de nos systèmes, cet antivirus est régulièrement contrôlé et mis à jour par la personne en charge de l'administration de nos systèmes.

5.3.5. Anonymisation

Nous procédons régulièrement à l'anonymisation des données à caractère personnelle dès lors que nous sommes tenus de transmettre des données à des tiers.

5.4. Solutions Matérielles

5.4.1. Hébergement privé

Sélection d'un Datacenter professionnel certifié. Le Datacenter qui héberge les données des clients ayant fait le choix de notre solution BCS remplit toutes les conditions optimales en matière de protection des données et est certifié selon les normes en vigueur. Les certifications et informations complémentaires sont disponibles sur notre site internet.

6. Organisation

6.1. Responsable des traitements

Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément à la législation.

Ces mesures sont réexaminées et actualisées si nécessaire.

6.2. Délégué à la protection des données

Un Délégué à la protection des données a été désigné pour assurer la réception des demandes éventuelles concernant les données traitées et y apporter une réponse.

Il/Elle est également responsable de la communiquer et des interactions avec les autorités en charge de la protection des données.

Ce/Cette délégué est joignable à l'adresse dpo@agentil.com.

6.3. Responsable sécurité IT

Il/Elle a la charge de la gestion des solutions logicielles et matérielles et plus particulièrement des mises à jour y relatives.

6.4. Direction financière

Il/Elle est responsable de l'attribution des droits d'accès aux données financières.

6.5. Direction des Ressources Humaines

Il/Elle est responsable de l'attribution des droits d'accès aux données à caractère personnel.

7. Notification violation des données

7.1. Description violation

Une violation de données survient lorsque les données dont nous sommes responsables subissent un incident de sécurité qui entraîne une violation de la confidentialité, de la disponibilité ou de l'intégrité.

7.2. Délai notification

Si la violation engendre un risque pour les droits et libertés d'une personne, nous notifions l'autorité de contrôle compétente dans les meilleurs délais, et au plus tard 72 heures après avoir pris connaissance de la violation.

Si la violation de données engendre un risque élevé pour les personnes affectées, ces dernières seront alors également informées dans les meilleurs délais après avoir pris connaissance de la violation, à moins que des mesures de protection techniques et organisationnelles efficaces ou d'autres mesures qui garantissent que le risque n'est plus susceptible de se matérialiser aient été prises.

7.3. Processus de notification

Le processus de notification va se réaliser en plusieurs phases :

Investigation :

Nous procéderons à une investigation interne complète sur l'incident déterminant :

- la nature de la violation
- si possible, les catégories et le nombre approximatif de personnes concernées par la violation
- les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
- la description des conséquences probables de la violation de données ;
- la description des mesures prises ou à prendre pour éviter que cet incident se reproduise ou atténuer les éventuelles conséquences négatives.

Protection :

Nous mettrons en place immédiatement des mesures correctrices pour empêcher que la faille perdure et/ou se reproduise.

Information :

Les personnes concernées par la violation seront informées de façon proactive, afin de leur donner ainsi la possibilité de prendre des mesures appropriées.

Elles seront informées au fur et à mesure de nos investigations, de toute information utile sur la nature et l'étendue des Données Personnelles éventuellement déjà touchées et les mesures correctrices prises ou envisagées pour y remédier.

Notification :

Si la violation engendre un risque pour les droits et libertés d'une personne, une notification de violation sera ouverte auprès des autorités de contrôle compétentes selon la localisation :

- Pour des données personnelles dépendantes de la législation suisse :

Conformément à l'art. 24 de la nouvelle loi sur la protection des données qui entre en vigueur le 1er septembre 2023, les violations de la sécurité des données devront désormais être annoncées au Préposé fédéral à la protection des données et à la transparence (PFPDT) si elles entraînent un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées par la fuite de données. Cette obligation d'annoncer est valable pour les particuliers, les entreprises et les organes fédéraux et doit être satisfaite dans les meilleurs délais, sur le formulaire d'annonce ici: https://databreach.edoeb.admin.ch/report

Déposition d'une dénonciation pénale à la police cantonale de notre siège, celle-ci procédera aux investigations nécessaires. Site https://www.suisse-epolice.ch/#/search-station les postes de police proches et leurs données de contact.

En fonction du lieu d'établissement de l'entreprise, le règlement général de l'Union européenne sur la protection des données est également applicable lorsque les données qui ont fuité sont ou comprennent des données personnelles.

- Pour des données personnelles dépendantes de la législation française et/ou européenne :

La notification sera transmise à la CNIL dans les meilleurs délais à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.

Si nous ne pouvons pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, nous procéderons à une notification en deux temps :

1. Une notification initiale dans un délai de 72 heures si possible à la suite de la constatation de la violation ;
2. Si le délai de 72 heures est dépassé, nous expliquerons, lors de notre notification, les motifs du retard ;
3. Enfin, une notification complémentaire dès lors que les informations complémentaires sont disponibles.

Si nous sommes un sous-traitant des données, nous notifions chaque violation de données au responsable du traitement des données.

8. Références

8.1. Cadre légal

nLPD

Loi Fédérale sur la protection des données (LPD) du 25 Septembre 2020 (FF 2020 7397).

https://www.fedlex.admin.ch/eli/fga/2020/1998/fr

8.1.1. Loi Informatique et liberté

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

8.1.2. RGPD

Le règlement général sur la protection des données – RGPD du 23 mai 2018.

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

8.1.3. Autres références règlementaires

Pour toutes informations concernant les autres références règlementaires, se référer aux sites suivants :

https://entreprendre.service-public.fr/vosdroits/F10029#:~:text=Les%20livres%2C%20registres%2C%20documents%20ou,un%20d%C3%A9lai%20de%206%20ans.

https://www.fedlex.admin.ch/eli/cc/1999/354/fr