Protection des données

N° de la lecture individuelle : 4

Étudiant Laurent Térence, 802_1F

Sujet RGPD

Table des matières

1. Introduction à la loi sur la protection des données en Suisse

1.1 Contexte et importance de la protection des données personnelles.

La protection des données personnelles est devenue un enjeu majeur dans notre société de plus en plus connectée et numérisée. Dans ce chapitre, nous allons examiner le contexte dans lequel la loi sur la protection des données en Suisse a été élaborée, ainsi que l'importance de protéger les données personnelles.

Le développement rapide des technologies de l'information et de la communication a entraîné une augmentation exponentielle de la quantité de données personnelles collectées, stockées et traitées. Les progrès dans les domaines tels que l'internet, les médias sociaux, le commerce électronique, les objets connectés et l'intelligence artificielle ont créé de nouvelles possibilités, mais ont également soulevé des préoccupations en matière de protection des données.

La collecte et l'utilisation des données personnelles peuvent présenter des risques pour la vie privée et la sécurité des individus. Des informations sensibles telles que les données médicales, les informations financières, les données de localisation ou les préférences personnelles peuvent être exploitées à des fins malveillantes ou utilisées pour manipuler les individus.

La protection des données personnelles revêt donc une importance cruciale pour garantir la confiance des individus dans les services en ligne, les transactions commerciales et les échanges d'informations. Elle est essentielle pour préserver les droits fondamentaux à la vie privée, à l'autodétermination informationnelle et à la dignité humaine.

La législation sur la protection des données en Suisse vise à établir un cadre juridique clair et robuste pour encadrer la collecte, le traitement et la conservation des données personnelles. Elle garantit que les individus ont le contrôle sur leurs propres informations, en définissant des principes et des droits fondamentaux pour protéger leur vie privée et leurs données personnelles.

La protection des données personnelles favorise également la confiance dans l'économie numérique et les échanges transfrontaliers. Elle facilite les échanges de données avec d'autres pays et permet de renforcer la coopération internationale en matière de protection des données.

Dans les sections suivantes, nous explorerons en détail les dispositions de la loi sur la protection des données en Suisse, en mettant l'accent sur les principes clés, les droits des individus, les obligations des responsables de traitement, ainsi que les sanctions et les recours en cas de non-respect de la législation.

La protection des données personnelles est donc un aspect essentiel de notre société moderne, et la loi sur la protection des données en Suisse joue un rôle crucial dans la sauvegarde de ce droit fondamental.

1.2 Vue d'ensemble du cadre juridique suisse en matière de protection des données.

Le cadre juridique suisse en matière de protection des données est basé sur la Loi fédérale sur la protection des données (LPD) et d'autres lois connexes. Dans ce chapitre, nous allons explorer les principales lois et réglementations qui régissent la protection des données en Suisse.

La Loi fédérale sur la protection des données (LPD) constitue le fondement juridique principal en matière de protection des données personnelles en Suisse. Adoptée en 1992 et révisée en 2018, la LPD établit les principes fondamentaux de la protection des données et définit les droits et les obligations des parties concernées.

La LPD définit ce qu'est une donnée personnelle et établit les conditions dans lesquelles elles peuvent être collectées, traitées et utilisées. Elle précise également les droits des individus sur leurs données personnelles et les obligations des responsables de traitement.

En plus de la LPD, d'autres lois complètent le cadre juridique suisse en matière de protection des données. Parmi celles-ci, on trouve notamment :

La Constitution fédérale suisse : La Constitution garantit le droit à la protection de la sphère privée et personnelle, qui englobe la protection des données personnelles. Elle établit les principes généraux qui doivent être respectés dans le traitement des données.

Loi sur la protection des données dans le domaine des télécommunications (**LPDT**) : Cette loi spécifique réglemente la protection des données dans le secteur des communications électroniques, y compris les services de télécommunication et d'internet.

Loi sur les documents officiels (**LTrans**) : Cette loi réglemente l'accès aux documents officiels et la protection des données contenues dans ces documents.

Loi sur la surveillance de la correspondance par poste et télécommunication (**LSCPT**) : Cette loi vise à protéger la confidentialité des communications et établit les conditions dans lesquelles la surveillance des communications est autorisée.

En outre, des ordonnances et des directives spécifiques complètent le cadre législatif suisse, fournissant des lignes directrices et des règles supplémentaires pour la mise en œuvre de la protection des données. Ces textes réglementaires précisent notamment les modalités de notification des violations de données, les mesures de sécurité requises, ainsi que les procédures de coopération internationale en matière de protection des données.

Il convient également de mentionner l'Office fédéral de la protection des données et de la transparence (OFDP) en tant qu'organisme de surveillance et de régulation de la protection des données en Suisse. L'OFDP est chargé de garantir le respect de la législation sur la protection des données et d'assurer la promotion de bonnes pratiques en matière de protection des données.

En résumé, le cadre juridique suisse en matière de protection des données repose sur la Loi fédérale sur la protection des données (LPD) et d'autres lois complémentaires. Ces lois établissent les principes fondamentaux de la protection des données personnelles, définissent les droits et les obligations des parties concernées, et prévoient des mesures de surveillance et de régulation pour garantir le respect de ces principes.

2. Champ d'application de la loi :

2.1 Définitions tiré du LPD

Le chapitre 2, section 1, de la loi sur la protection des données présente des définitions et des principes généraux. **L'article 5** énonce les différentes définitions utilisées dans la loi. Voici un résumé des principales définitions :

a. **Données personnelles** : Il s'agit de toutes les informations concernant une personne physique identifiée ou identifiable.

b. **Personne concernée** : C'est la personne physique dont les données personnelles font l'objet d'un traitement.

c. **Données personnelles sensibles** : Cela englobe plusieurs catégories de données spécifiques, telles que les opinions religieuses, philosophiques, politiques ou syndicales, les données de santé, les données relatives à la sphère intime, l'origine raciale ou ethnique, les données génétiques, les données biométriques permettant d'identifier une personne de manière unique, les données sur des poursuites ou sanctions pénales et administratives, ainsi que les données sur des mesures d'aide sociale.

d. **Traitement** : Il englobe toutes les opérations liées aux données personnelles, telles que la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction des données.

e. **Communication** : C'est le fait de transmettre ou de rendre accessibles des données personnelles.

f. **Profilage** : Il désigne toute forme de traitement automatisé de données personnelles visant à évaluer certains aspects personnels d'une personne, comme l'analyse ou la prédiction du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts, de la fiabilité, du comportement, de la localisation ou des déplacements.

g. **Profilage à risque élevé** : Il concerne le profilage qui présente un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, car il permet d'évaluer les caractéristiques essentielles de sa personnalité.

h. **Violation de la sécurité des données** : Il s'agit de toute violation de la sécurité entraînant accidentellement ou illégalement la perte, la modification, l'effacement, la destruction, la divulgation non autorisée ou l'accès non autorisé à des données personnelles.

i. **Organe fédéral** : Cela désigne l'autorité fédérale, le service fédéral ou la personne chargée d'une tâche publique de la Confédération.

j**. Responsable du traitement** : Il s'agit de la personne privée ou de l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.

k. **Sous-traitant** : C'est la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement.

Ces définitions sont essentielles pour comprendre les concepts et les principes de base régissant la protection des données en Suisse.

2.2 Les types de données personnelles couverts par la loi.

La loi sur la protection des données en Suisse couvre un large éventail de données personnelles. Dans ce chapitre, nous allons explorer les différents types de données personnelles qui sont protégés par la législation suisse.

Les données personnelles font référence à toute information se rapportant à une personne physique identifiée ou identifiable. Cela inclut des informations directement liées à une personne, telles que son nom, son adresse, son numéro de téléphone, son adresse e-mail, son numéro de sécurité sociale, ainsi que des informations plus spécifiques telles que sa localisation géographique, ses données biométriques, ses données de santé, ses données financières, ses préférences personnelles, etc.

La loi sur la protection des données reconnaît la sensibilité de ces informations et impose des règles strictes pour leur traitement. Elle vise à garantir que les individus ont le contrôle sur leurs données personnelles et que ces données sont utilisées de manière licite et légitime.

Voici quelques **exemples** de types de données personnelles couverts par la loi :

1. Données d'identification : Cela comprend les informations permettant d'identifier une personne, telles que le nom, l'adresse, la date de naissance, le numéro de passeport, etc.

2. Données de contact : Il s'agit des informations permettant d'entrer en contact avec une personne, comme l'adresse e-mail, le numéro de téléphone, l'adresse postale, etc.

3. Données financières : Cela inclut les informations liées aux transactions financières d'une personne, telles que les numéros de compte bancaire, les relevés bancaires, les informations de carte de crédit, etc.

4. Données de santé : Il s'agit des informations concernant l'état de santé d'une personne, les antécédents médicaux, les traitements médicaux, les informations génétiques, etc.

5. Données biométriques : Cela comprend les données relatives aux caractéristiques physiques uniques d'une personne, comme les empreintes digitales, la reconnaissance faciale, l'iris, etc.

6. Données de localisation : Il s'agit des informations permettant de déterminer la position géographique d'une personne, comme les données de localisation GPS, les adresses IP, etc.

7. Données professionnelles : Cela inclut les informations liées à l'emploi d'une personne, telles que l'employeur, le poste occupé, les qualifications professionnelles, etc.

Il convient de noter que la loi sur la protection des données reconnaît également les données sensibles, qui sont des catégories spécifiques de données personnelles nécessitant une protection accrue. Cela inclut des informations telles que l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques dans le but d'identifier de manière unique une personne, etc.

En résumé, la loi sur la protection des données en Suisse couvre un large éventail de données personnelles, allant des données d'identification et de contact aux données sensibles telles que les données de santé et les données biométriques.

2.3 Les exemptions et les exceptions applicables.

3 Référence : Article 4 et 13 de la LPD.

La Loi fédérale sur la protection des données (LPD) en Suisse prévoit certaines exemptions et exceptions concernant le traitement et la communication des données personnelles. Ces exemptions permettent de déroger à certaines obligations de protection des données dans des situations spécifiques. Deux articles importants de la LPD abordent ces exemptions et exceptions : l'article 13 et l'article 4.

Article 13: Évaluation et certification des fournisseurs de systèmes de traitement de données personnelles

L'article 13 de la LPD concerne l'évaluation et la certification des fournisseurs de systèmes ou de logiciels de traitement de données personnelles. Selon cet article, ces fournisseurs, ainsi que les responsables du traitement et les sous-traitants, ont la possibilité de soumettre leurs systèmes, produits ou services à une évaluation effectuée par des organismes de certification agréés et indépendants. Cette évaluation vise à vérifier la conformité de leurs systèmes de traitement avec les exigences de protection des données.

Le Conseil fédéral est chargé d'édicter des dispositions sur la reconnaissance des procédures de certification et sur l'introduction d'un label de qualité de protection des données. Ces dispositions tiennent compte du droit international et des normes techniques reconnues au niveau international.

Article 4: Préposé fédéral à la protection des données et à la transparence

L'article 4 de la LPD concerne le **Préposé fédéral à la protection des données et à la transparence** (PFPDT). Le PFPDT est chargé de surveiller la bonne application des dispositions fédérales de protection des données. Cependant, il existe certaines limitations à sa compétence de surveillance.

Le PFPDT ne peut exercer aucune surveillance sur l'Assemblée fédérale, le Conseil fédéral, les tribunaux fédéraux, et le Ministère public de la Confédération en ce qui concerne le traitement de données personnelles dans le cadre de procédures pénales. De plus, les autorités fédérales ne relèvent pas de sa compétence en ce qui concerne le traitement de données personnelles dans le cadre de leurs activités juridictionnelles ou dans le cadre de procédures d'entraide judiciaire internationale en matière pénale.

En résumé, l'article 13 de la LPD permet l'évaluation et la certification des fournisseurs de systèmes de traitement de données personnelles, tandis que l'article 4 établit les compétences et les limitations du Préposé fédéral à la protection des données et à la transparence.

3. Principes clés de la loi :

Référence : Article4, 6 et 7 de la LPD.

L'article 4 présente les principes fondamentaux qui régissent le traitement des données personnelles. Voici un résumé de ces principes :

1. Licéité du traitement : Tout traitement de données personnelles doit être effectué conformément à la loi.

2. Bonne foi et proportionnalité : Le traitement des données doit être réalisé de manière honnête et équitable, en respectant le principe de proportionnalité entre les objectifs poursuivis et les données collectées.

3. But spécifique du traitement : Les données personnelles ne doivent être traitées que dans le but spécifié lors de leur collecte, prévu par la loi ou évident compte tenu des circonstances.

4. Transparence de la collecte des données : La collecte de données personnelles, ainsi que les finalités du traitement, doivent être clairement identifiables pour la personne concernée.

5. Consentement éclairé : Lorsque le consentement de la personne concernée est requis pour justifier le traitement de ses données personnelles, ce consentement n'est valable que s'il est donné librement, après que la personne a été dûment informée. Dans le cas de données sensibles et de profils de la personnalité, le consentement doit être explicite en plus d'être libre et éclairé.

Ces principes visent à assurer la protection des données personnelles en garantissant leur traitement légitime, éthique et respectueux des droits des individus.

L'article 6 de la LPD énonce les principes fondamentaux du traitement des données personnelles. Tout traitement de données personnelles doit être licite et se conformer aux principes de la bonne foi et de la proportionnalité. Les données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée. De plus, elles doivent être traitées ultérieurement de manière compatible avec ces finalités. Il est également précisé que les données doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement.

L'article 6 souligne également que le responsable du traitement est tenu de s'assurer de l'exactitude des données personnelles. Il doit prendre toutes les mesures appropriées pour rectifier, effacer ou détruire les données inexactes ou incomplètes, en tenant compte du type de traitement, de son étendue et du risque que le traitement présente pour la personnalité ou les droits fondamentaux des personnes concernées.

En ce qui concerne le consentement, l'article 6 de la LPD stipule que lorsque le consentement de la personne concernée est requis, celui-ci ne peut être valable que s'il est donné librement et après que la personne ait été dûment informée. Le consentement doit être exprès dans certains cas, notamment lorsqu'il s'agit d'un traitement de données sensibles, d'un profilage à risque élevé effectué par une personne privée ou d'un profilage effectué par un organe fédéral.

Par ailleurs, l'article 7 de la LPD aborde la protection des données dès la conception et par défaut. Il impose au responsable du traitement de mettre en place des mesures techniques et organisationnelles appropriées dès la conception du traitement, afin de garantir le respect des prescriptions de protection des données, en particulier les principes énoncés à l'article 6. Ces mesures doivent être adaptées à l'état de la technique, au type de traitement, à son étendue et au risque que le traitement présente pour la personnalité ou les droits fondamentaux des personnes concernées. De plus, le responsable du traitement est tenu de limiter le traitement des données personnelles au minimum requis par la finalité poursuivie, à moins que la personne concernée en dispose autrement.

En résumé, le consentement libre, éclairé et spécifique de la personne concernée est essentiel pour la collecte des données personnelles, conformément aux articles 6 et 7 de la LPD. Le traitement des données doit être effectué dans le respect des finalités déterminées, en veillant à leur exactitude et en mettant en place des mesures de protection appropriées dès la conception du traitement. Les responsables du traitement doivent donc se conformer à ces dispositions légales pour garantir le respect des droits des personnes concernées et assurer la protection des données personnelles.

3.1 Sécurité des données et obligations de confidentialité.

L'article 8 de la LPD, intitulé "Sécurité des données", stipule ce qui suit :

Les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru.

Les mesures doivent permettre d'éviter toute violation de la sécurité des données.

Le Conseil fédéral édicte des dispositions sur les exigences minimales en matière de sécurité des données.

Cet article met en évidence la responsabilité des acteurs impliqués dans le traitement des données personnelles de garantir la sécurité appropriée de ces données. Cela signifie qu'ils doivent prendre des mesures concrètes, tant au niveau organisationnel que technique, pour protéger les données contre les risques potentiels de violation de la sécurité.

Les mesures organisationnelles comprennent la mise en place de politiques de sécurité des données, la désignation de responsables de la protection des données, la formation du personnel sur les bonnes pratiques en matière de protection des données, ainsi que l'établissement de procédures de contrôle et de surveillance.

Quant aux mesures techniques, elles englobent l'utilisation de mécanismes de cryptage, de pare-feu, de sauvegardes régulières, d'accès restreint aux données, ainsi que la mise en place de protocoles de sécurité informatique.

Par ailleurs, il est important de souligner que la LPD impose également des obligations de confidentialité. Les responsables du traitement et les sous-traitants sont tenus de respecter la confidentialité des données personnelles qu'ils traitent. Cela signifie qu'ils ne doivent pas divulguer ces données à des tiers non autorisés et doivent les utiliser uniquement dans le cadre des finalités pour lesquelles elles ont été collectées.

3.2 Transfert international des données.

Référence : Article 16 , 17 et 18 de la LPD.

Article 16 de la LPD : Cet article énonce les principes généraux du transfert international des données personnelles. Il stipule que des données personnelles peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que l'État destinataire dispose d'une législation assurant un niveau de protection adéquat, ou si un organisme international garantit un tel niveau de protection. En l'absence d'une telle décision du Conseil fédéral, des garanties appropriées doivent être mises en place pour assurer un niveau de protection adéquat.

" *En l'absence d'une décision du Conseil fédéral au sens de l'al. 1, des données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti par:*

a. un traité international;

b. les clauses de protection des données d'un contrat entre le responsable du traitement ou le sous-traitant et son cocontractant, préalablement communiquées au PFPDT;

c. des garanties spécifiques élaborées par l'organe fédéral compétent et préalablement communiquées au PFPDT;

d. des clauses type de protection des données préalablement approuvées, établies ou reconnues par le PFPDT;

e. des règles d'entreprise contraignantes préalablement approuvées par le PFPDT ou par une autorité chargée de la protection des données relevant d'un État qui assure un niveau de protection adéquat.

3 Le Conseil fédéral peut prévoir d'autres garanties appropriées au sens de l'al.2»

Article 17 de la LPD : Cet article énumère les dérogations aux principes énoncés à l'article 16. Il spécifie les cas dans lesquels des données personnelles peuvent être communiquées à l'étranger, tels que le consentement exprès de la personne concernée, la relation directe avec la conclusion ou l'exécution d'un contrat, la nécessité de sauvegarder un intérêt public prépondérant, la protection de la vie ou de l'intégrité corporelle, etc.

Article 18 de la LPD : Cet article traite spécifiquement de la publication de données personnelles sous forme électronique. Il précise que la publication de telles données via des services d'information et de communication automatisés, dans le but d'informer le public, n'est pas considérée comme une communication à l'étranger, même si ces données peuvent être consultées depuis l'étranger.

4. Les droits des individus :

4.1 Droit à l'information et accès aux données personnelles.

Référence : Article 25 de la LPD

Cet article énonce le droit fondamental d'une personne à être informée sur le traitement de ses données personnelles. Il précise les informations que le responsable du traitement doit fournir à la personne concernée, telles que l'identité du responsable, la finalité du traitement, la durée de conservation des données, etc. Il souligne également le droit d'accéder aux informations sur les destinataires des données et sur l'existence de décisions automatisées.

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

Référence : Article 28 de la LPD

Cet article confère à la personne concernée le droit de récupérer les données personnelles qu'elle a préalablement communiquées au responsable du traitement. Elle peut demander ces données dans un format électronique couramment utilisé. De plus, si la personne souhaite transférer ses données à un autre responsable du traitement, elle peut également en faire la demande, sous réserve des conditions énoncées.

Le responsable du traitement est tenu de remettre ou de transmettre ces données gratuitement, sauf exceptions prévues par le Conseil fédéral en cas d'efforts disproportionnés.

5. Les obligations des responsables de traitement :

5.1 Notification des violations de données.

Référence : Article 24 de la LPD

Cet article énonce les obligations du responsable du traitement en matière d'annonce des violations de la sécurité des données personnelles. Il spécifie les informations qui doivent être fournies lors de l'annonce, les cas dans lesquels l'information de la personne concernée peut être restreinte ou différée, ainsi que l'interdiction d'utiliser cette annonce dans le cadre d'une procédure pénale sans le consentement de la personne tenue de faire l'annonce.

5.2 Évaluation de l'impact sur la protection des données (EIPD).

Référence : Article 22 de la LPD

En résumé, cet article établit l'obligation pour le responsable du traitement de réaliser une analyse d'impact relative à la protection des données personnelles lorsque le traitement présente un risque élevé. L'analyse d'impact doit évaluer les risques potentiels et prévoir des mesures de protection adéquates. Toutefois, certaines situations, telles que les obligations légales ou l'utilisation de systèmes certifiés ou de codes de conduite approuvés, peuvent exempter le responsable du traitement de cette obligation.

6 Nouvelle loi sur la protection des données « nLPD »

« *La nouvelle loi sur la protection des données (nLPD) entrera en vigueur le 1er septembre 2023. Elle instaurera des nouveautés non seulement pour les personnes traitant des données et pour les personnes concernées, mais aussi pour le PFPDT, dont elle modifie les tâches et les pouvoirs, et qui va donc intensifier son activité de surveillance et augmenter le nombre d'enquêtes*. » src. « Rôle du PFPDT (admin.ch) »

La Suisse a adopté une nouvelle loi fédérale sur la protection des données (nLPD) afin de mieux

protéger les données de ses citoyens. Cette loi entrera en vigueur le 1er septembre 2023 et apporte plusieurs changements importants pour les entreprises. Les principaux changements comprennent :

1. Limitation de la couverture aux données des personnes physiques plutôt que des personnes morales.

2. Inclusion des données génétiques et biométriques dans la catégorie des données sensibles.

3. Introduction des principes de "Privacy by Design" et de "Privacy by Default" pour garantir la protection des données dès la conception des produits et services.

4. Obligation de réaliser des analyses d'impact en cas de risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.

5. Extension du devoir d'information préalable à la collecte de toutes les données personnelles, pas seulement les données sensibles.

6. Obligation de tenir un registre des activités de traitement des données, avec une exemption pour les petites et moyennes entreprises à faible risque.

7. Notification rapide en cas de violation de la sécurité des données au Préposé fédéral à la protection des données et à la transparence (PFPDT).

8. Introduction de la notion de profilage dans la loi, qui concerne le traitement automatisé de données personnelles.

Ces changements visent à garantir une protection adéquate des données personnelles des individus et à assurer la compatibilité avec le droit européen, en particulier le Règlement européen sur la protection des données (RGPD). Les entreprises suisses doivent se conformer à ces nouvelles obligations afin de maintenir la libre circulation des données avec l'Union européenne et éviter une perte de compétitivité.

6.1 Différences avec l'UE

« *Les entreprises qui s'étaient déjà conformées au règlement général de l'UE sur la protection des données (RGPD) auront peu de changements à entreprendre. L'association SwissPrivacy.Law a publié un tableau de comparaison entre la nLPD et le règlement européen à consulter à cette adresse (en français): https://swissprivacy.law/55/* », src : « Nouvelle loi sur la protection des données (nLPD) (admin.ch) »

Bibliographie

données, L. f. (s.d.). Récupéré sur https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2020/1998/fr/pdf-x/fedlex-data-admin-ch-eli-fga-2020-1998-fr-pdf-x.pdf

juridique, A. (s.d.). *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/4*. Récupéré sur http://data.europa.eu/eli/reg/2016/679/oj/fra

PME, & Portail. (s.d.). *Nouvelle loi sur la protection des données (nLPD)*. Récupéré sur https://www.kmu.admin.ch/kmu/fr/home/fakten-und-trends/digitalisierung/datenschutz/neues-datenschutzgesetz-revdsg.html

RS 235.1 - Loi fédérale du 25 septembre 2020 sur la protection des données (LPD). (s.d.). Récupéré sur https://www.fedlex.admin.ch/eli/cc/2022/491/fr#art_23

transparence, P. f. (s.d.). *Bases légales protection des données*. Récupéré sur https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/grundlagen.html

transparence, P. f. (s.d.). *Déclaration de protection des données sur Internet*. Récupéré sur https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/arbeit_wirtschaft/datenschutzerklaerung.html