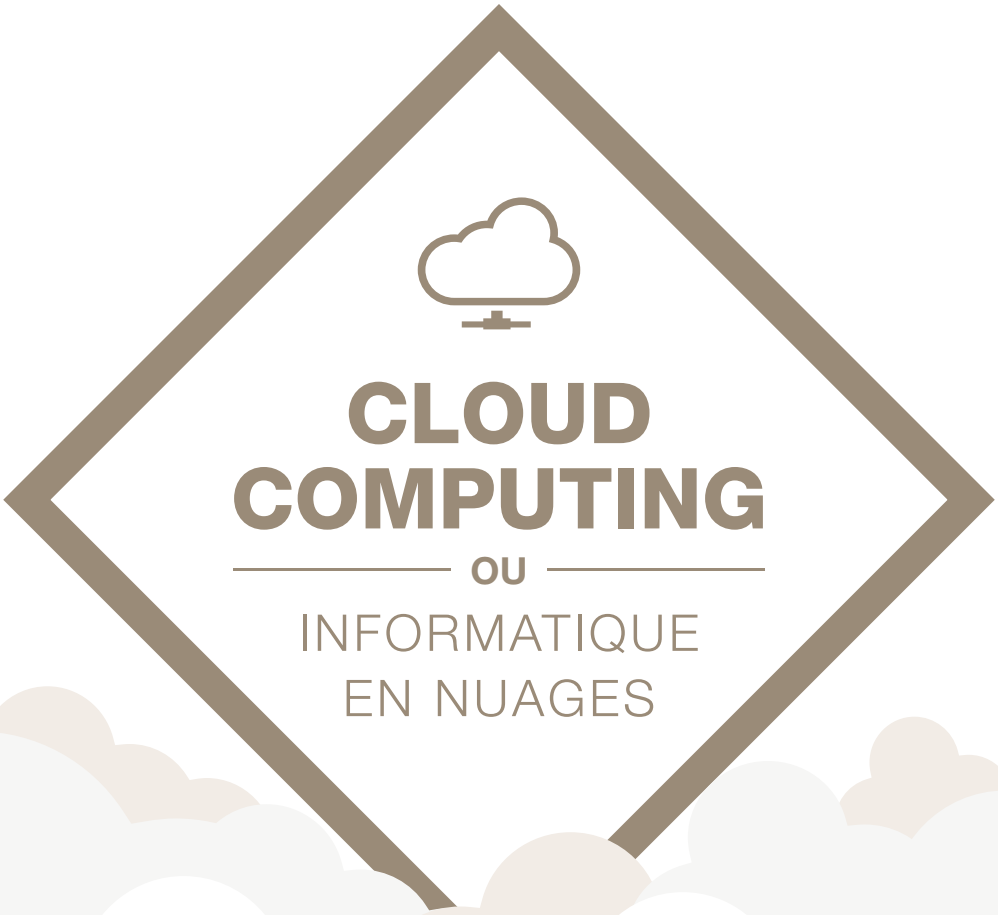
GUIDE DE LA PROTECTION
DES DONNÉES



CLOUD COMPUTING

OU

INFORMATIQUE
EN NUAGES

AD HOC RESOLUTION

Pragm@TIC
CONSULTING

Table des matières

1. Préambule 2
2. Définitions 3
3. Types de Cloud et responsabilités 4
3.1. Le Cloud privé ou interne 4
3.2. IaaS (Infrastructure as a Service) 4
3.3. PaaS (Platform as a Service) 5
3.4. SaaS (Software as a Service) 5
3.5. Responsabilités 5
4. Les principes applicables au traitement des données personnelles 6
5. Les risques 7
6. Recommandations : mesures organisationnelles et techniques 8
6.1 Catégorisation 8
6.2 Localisation 9
6.3. Sous-traitance 9
6.3.1 En général 9
6.3.2 Garanties à obtenir des fournisseurs 9
6.3.3 Privacy by design 10
6.4 Chiffrement 10
6.5 Suppression 11
6.6 Procédures 11
7. Recommandations spécifiques aux structures éducatives privées 12
7.1 Anonymisation 12
7.2. Cloud gratuit 12
7.3. Travaux d'élèves 12
7.4. Durée de conservation 12
8. Recommandations spécifiques aux données médicales 13
8.1. Localisation 13
8.2. Cloud gratuit 13
8.3. Consentement du patient 13

1. Préambule

Le présent guide s'adresse en priorité aux entreprises[1] *privées qui souhaitent externaliser tout ou partie de leurs données - **comprenant des données personnelles ou des données d'entreprise confidentielles** - en toute conformité. Fondé sur les dispositions légales en vigueur en Suisse, prévues par la loi fédérale sur la protection des données personnelles et son ordonnance, il n'a pas vocation à remplacer un avis juridique circonstancié, mais bien plutôt à accompagner, concrètement et de manière pragmatique, les entreprises qui s'aventurent sur le chemin de l'informatique en nuages, ou Cloud Computing. Les auteurs de ce guide, experts en protection des données personnelles, d'une part, et spécialistes en sécurité de l'information et analyse des risques, d'autre part, espèrent que ce guide permettra aux décideurs de prendre en connaissance de cause les décisions de base et de définir les grands axes de développement en pratiquant la privacy by design, seule manière de ne pas multiplier les coûts a posteriori par de laborieuses mesures correctives.*

[1] *Au sens du présent guide, le terme entreprise désigne tout organisme privé quelle que soit sa forme juridique.*

« On entend par donnée personnelle toute information permettant d'identifier une personne (ou une société, en droit suisse), même indirectement. »

2. Définitions

On entend par externalisation des données le fait de confier à un tiers, le sous-traitant, tout ou partie du traitement des données personnelles, par exemple la conservation (hébergement). Si le tiers ne conserve pas les données confiées sur ses serveurs, dans un lieu géographiquement circonscrit, mais au sein d'un réseau virtuel, on parle d'informatique en nuage (Cloud). L'environnement informatique n'est plus la propriété de l'entreprise ou de l'autorité et n'est plus géré en tout ou partie par elle, mais est loué à un ou plusieurs prestataires de services. Le nuage peut être privé ou public, voire les deux et peut être partagé par plusieurs organisations.

On entend par donnée personnelle toute information permettant d'identifier une personne (ou une société, en droit suisse), même indirectement.

Les données personnelles sensibles sont définies par la loi[2] et comprennent les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, les mesures d'aide sociale et les poursuites ou sanctions pénales et administratives.

Est considéré comme le maître de fichiers - ou responsable de traitement - terminologie utilisée dans le présent guide[3], la personne qui décide du but et du contenu d'un fichier.

Le terme « Cloud » étant largement utilisé et souvent de manière erronée, nous vous proposons la définition du Club des responsables d'infrastructure et de production[4] :

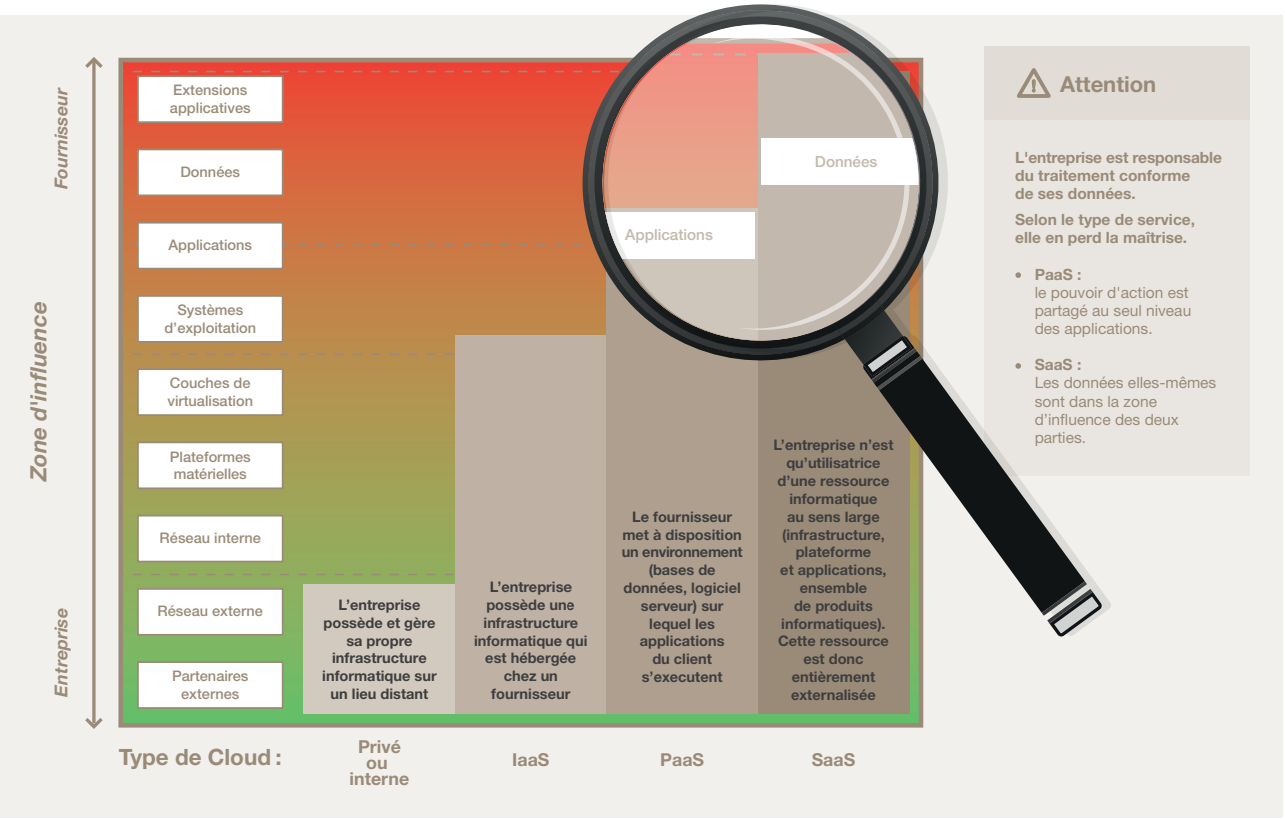
« Le Cloud Computing est un modèle d'accès simplifié à des ressources informatiques partagées et accessibles via le réseau Internet telles que des réseaux, des serveurs, du stockage, des applications et des services ».

[2] *Voir art. 3 de la Loi fédérale sur la protection des données, LPD RS 235.1* https://www.admin.ch/opc/fr/classified-compilation/19920153

[3] *La LPD parle de « maître de fichiers » mais le règlement européen comme certaines lois cantonales de « responsable de traitement »*

[4] *CRIP :* http://www.crip-asso.fr

3. Types de Cloud et responsabilités



3.1 Le Cloud privé ou interne

L'entreprise possède et gère sa propre infrastructure informatique sur un lieu distant. Elle partage, avec ses ayants droits, les données de l'entreprise à travers le réseau Internet.

› L'entreprise est donc responsable de son parc informatique, de son infrastructure, de ses données, de sa sécurité, etc.

› Le seul tiers intervenant est le fournisseur d'accès internet.

3.2 IaaS (Infrastructure as a Service)

Dans ce modèle, l'entreprise possède une infrastructure informatique qui est hébergée chez un fournisseur.

› L'entreprise gère et maintient ses applications, ses bases de données, ses logiciels, et ses serveurs.

› L'hébergeur du Cloud maintient l'infrastructure (les serveurs physiques, la virtualisation, le réseau et le stockage).

« L'objectif pour le responsable de traitement est de ne pas perdre la maîtrise de ses données »

3.3 PaaS (Platform as a Service)

Dans ce modèle, l'hébergeur met à disposition un environnement (bases de données, logiciels, serveurs) dans lequel les applications s'exécutent.

- L'entreprise maintient donc uniquement ses applications.
- L'hébergeur maintient la plateforme d'exécution des applications et l'infrastructure.

3.4 SaaS (Software as a Service)

Il s'agit cette fois d'un modèle où l'entreprise n'est qu'utilisatrice d'une ressource informatique au sens large (infrastructure, plateforme et applications, ensemble de produits informatiques). Cette ressource est entièrement externalisée.

- L'entreprise s'abonne simplement en ligne.
- Le fournisseur maintient l'ensemble de la structure.

3.5 Responsabilités

A la lecture de ce qui précède, il apparaît clairement que les responsabilités diffèrent selon le modèle de service choisi. Or, l'objectif pour le responsable de traitement est de ne pas perdre la maîtrise de ses données. Rien n'empêche de confier tout ou partie du traitement des données à un fournisseur, comme dans le modèle PaaS, pour autant que le responsable de traitement en garde la maîtrise et que le fournisseur (sous-traitant) s'engage contractuellement à respecter les principes légaux applicables exposés ci-dessous. Tel n'est pas le cas avec le modèle SaaS. Il est cependant possible d'utiliser ce dernier modèle en filtrant les données qu'on y dépose, après les avoir catégorisées.

4. Les principes applicables au traitement des données personnelles

Toute donnée personnelle doit être traitée par le responsable de traitement selon les 7 principes suivants[5] :

- LICÉITÉ (base légale, consentement, intérêt prépondérant)
- FINALITÉ (n'utiliser les données qu'aux fins indiquées)
- PROPORTIONNALITÉ (traitement apte, adéquat, le moins intrusif possible ; suppression à terme)
- EXACTITUDE (tenir à jour le fichier)
- BONNE FOI
- TRANSPARENCE DE LA COLLECTE (la personne concernée est informée)
- SÉCURITÉ (confidentialité, disponibilité, intégrité)

S'y ajoute le droit d'accès de toute personne concernée à ses données personnelles. Ce droit est absolu même s'il peut être restreint dans certaines circonstances. Pour respecter ces principes et être conforme, le responsable de traitement doit garder la main sur les données qu'il traite, qu'il s'agisse de la collecte, de l'exploitation, de la communication, de la conservation ou de la destruction, comme sur celles qu'il sous-traite, par exemple à des fins de conservation (stockage). Il doit également s'assurer que le sous-traitant garantira le droit d'accès, cas échéant, ce qui suppose que la législation du pays concerné reconnaisse ce droit. Par exemple, tel n'est pas le cas à ce jour (février 2016) de la législation américaine.

A noter que ces principes se retrouvent, parfois sous une autre dénomination, dans la législation applicable sur le territoire de l'Union européenne. A ce jour, il s'agit de la directive européenne 95/46, qui sera remplacée par le règlement général sur la protection des données personnelles, adopté le 15 décembre 2015 pour une entrée en vigueur prévue en 2018.

[5] *Voir art. 4, 5 et 7 LPD*

« Un nouveau cadre de sécurité existe désormais. »

5. Les risques

Les risques généraux de la sous-traitance sont la perte de données, les pannes de systèmes, l'indisponibilité des données, ainsi qu'un usage abusif des données. S'y ajoutent avec l'informatique en nuage : la perte de contrôle sur les données, le manque de séparation et d'isolation des données, l'accès d'autorités étrangères aux données, la captivité et le non-respect des dispositions légales[6].

Dans tous les cas, le responsable de traitement répond de la conformité du traitement des données personnelles, et le sous-traitant en répond dans la mesure de son contrat.

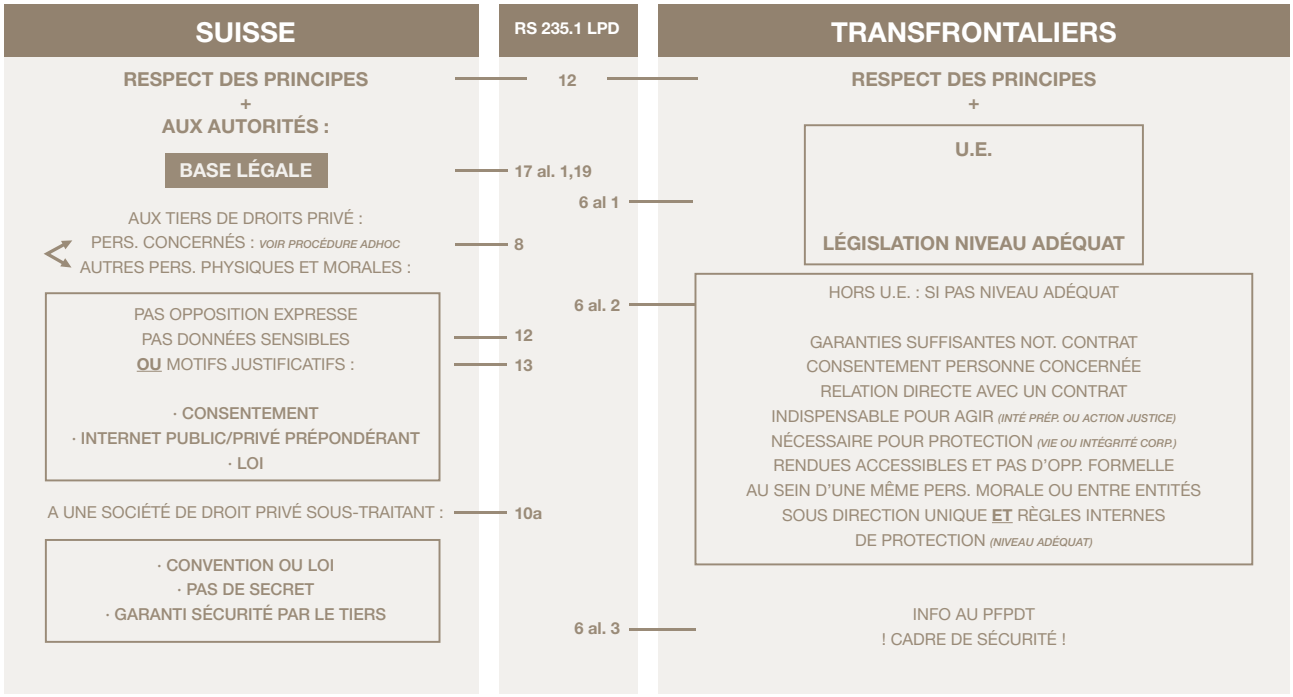
Lorsqu'on transfère des données personnelles en dehors du territoire suisse, on doit s'assurer que le traitement ainsi transféré répondra bien aux mêmes conditions que celles prévalant sur notre territoire (la législation est alors dite de niveau adéquat). De manière générale, tout flux transfrontière à destination d'un pays de l'Union européenne ou d'un pays disposant d'un niveau de traitement adéquat (voir la liste du préposé fédéral[7]) ne nécessitera pas la prise de mesures supplémentaires, au contraire des flux transfrontières à destination des autres pays, pour lesquelles des mesures organisationnelles et techniques garantissant un traitement conforme seront exigées.

C'est le lieu de rappeler que s'agissant du territoire des Etats-Unis, il n'est pas, a priori, considéré comme étant de niveau adéquat. Jusqu'en octobre dernier, ce manquement était corrigé par un cadre de sécurité appelé Safe Harbor, convention agréée par la commission européenne. Un tel Safe Harbor avait également été mis en place en Suisse. En date du 6 octobre 2015, la cour de justice de l'union européenne a invalidé ce système, créant du même coup une insécurité pour les entreprises suisses. Un nouveau cadre de sécurité existe désormais. On peut se référer, pour une meilleure compréhension des conditions applicables aux flux des données, au schéma ci-après.

L'absence de conformité aux règles génère des risques financiers (procédures judiciaires, refonte d'applications informatiques inadaptées aux besoins) et réputationnels.

[6] *La communication transfrontière doit respecter certaines règles, voir en particulier art. 6 LPD*

[7] *Sur le site du Préposé fédéral à la protection des données et à la transparence (PFPDT), la liste se trouve à l'adresse :* http://www.edoeb.admin.ch/datenschutz/00626/00753



© AD HOC RESOLUTION 2014

6. Recommandations : mesures organisationnelles et techniques

Les recommandations ci-contre sont à prendre en complémentarité les unes des autres, de manière à garantir la sécurité sous ses trois aspects, soit disponibilité, intégrité, et confidentialité.

6.1 Catégorisation

Avant de faire un choix sur les offres de service, il convient de catégoriser les données de l'organisme et de mesurer les impacts en cas de perte de celles-ci.

Par souci de simplicité, nous proposons ici de considérer deux catégories de données :

cat.1 Les données stratégiques, confidentielles, personnelles ou sensibles (clients, fournisseurs, contrats, données comptables, ressources humaines, etc.)

cat.2 Les données générales (documentation, catalogues, caractéristique des produits, etc.)

Ces deux types de données étant fondamentales pour l'organisme, il convient d'en mesurer les impacts (DIC – Disponibilité, Intégrité et Confidentialité) si :

- Les données sont indisponibles (panne, destruction, etc.)
- Les données sont modifiées par autrui (interne ou externe)
- Les données sont accessibles par des personnes non légitimées

« Il convient de s'assurer que le service choisi ne conduise pas à une perte de maîtrise des données »

De manière générale, en termes de gouvernance de la protection des données, il conviendrait de mettre en place un programme soutenu par la direction, notamment une politique de sécurité. Par ailleurs, tout nouveau projet impliquant en particulier l'utilisation du Cloud en lien avec des données personnelles devrait faire l'objet d'une analyse de risque de type Privacy Impact Assessment.

6.2 Localisation

Au vu des niveaux différents d'adéquation en termes de protection des données entre les pays, il convient de choisir un lieu de traitement (par exemple de conservation) situé en Suisse ou sur le territoire de l'Union européenne[8].

6.3 Sous-traitance

6.3.1 En général

Comme exposé ci-dessus, il convient de s'assurer que le service choisi ne conduit pas à une perte de maîtrise des données[9]. Par conséquent, le modèle SaaS est à exclure pour les données de catégorie 1.

6.3.2 Garanties à obtenir des fournisseurs

- Réversibilité en cas de rupture de contrat, de faille ou d'absorption du fournisseur de service
- Qualité du support utilisateur pour les applications ou services en mode SaaS (catégorie 2)
- Traçabilité des accès aux données en cas d'audit ou de procédure judiciaire
- Exclusion de toute sous-traitance sans accord préalable de l'entreprise
- Droit de faires des audits
- Respect des Accords de Niveau de Services (SLA) du fournisseur de service (niveau suffisant de disponibilité, réactivité d'intervention, …)
- Pérennité/Fiabilité des fournisseurs de services de Cloud Computing
- Possibilité d'avoir des services ou des infrastructures dédiés

[8] L'Irlande, bien que de niveau législatif adéquat, n'est pas à recommander. Voir arrêt C-362/14 sur http://curia.europa.eu. *Certains pays hors UE sont adéquats, comme le Canada, voir la liste précitée*

[9] Attention à ne pas sous-traiter de données soumises à un secret, voir art. 10a LPD

- Localisation des sociétés fournissant les services de Cloud Computing et des services associés (support)
- Respect des principes applicables en matière de protection des données y compris droit d'accès (Clause de responsabilité)
- Applicabilité du droit suisse et for juridique en Suisse

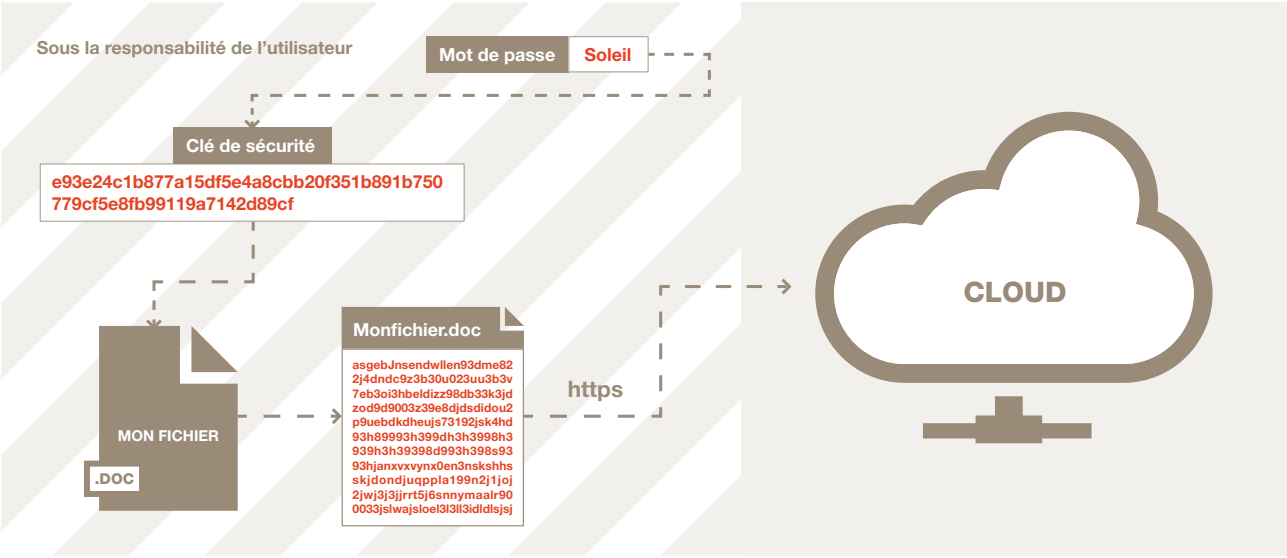
6.3.3 Privacy by design

Cette pratique facilite grandement le traitement de telles requêtes. Pensez-y dans la rédaction des cahiers des charges

Tout projet informatique impliquant le traitement de données personnelles devrait prendre en considération les principes ci-dessus dès leur conception. Il devrait en particulier permettre la suppression de données, manuelle ou automatique, l'anonymisation et l'accès aux données de la personne concernée (sous forme d'extraction lisible par ex.).

6.4 Chiffrement

En règle générale, nous recommandons de chiffrer les données de catégorie 1 (voir paragraphe 6.1), à savoir les données confidentielles, personnelles et stratégiques que vous déposez dans le Cloud.



Certains fournisseurs offrent le chiffrement, toutefois il est difficile de savoir si vous êtes les seuls à pouvoir déchiffrer vos données, ce qui est essentiel. Assurez-vous d'avoir des clés de chiffrement uniques et d'être les seuls à les détenir.

A ce jour, les bonnes pratiques recommandent un chiffrement AES 256 bits. S'agissant du risque d'accès de tiers non légitimés, incluant les services de renseignements (hors procédure judiciaire), il peut être qualifié de faible lorsque tant la donnée que sa transmission sont cryptées. La solidité de la chaîne de sécurité est égale au maillon le plus faible : Un haut niveau de chiffrement sera inefficace, par exemple, si la clé de chiffrement est échangée de manière non sécurisée.

6.5 Suppression

Comment vous assurer que toutes vos données ont bien été effacées, par exemple en fin de contrat, notamment dans les différentes sauvegardes ? Une preuve négative ne pouvant être rapportée, la seule solution consiste à chiffrer vos données, de sorte que même si elles ne sont pas toutes effacées, il sera difficile, voire impossible d'y accéder.

6.6 Procédures

Le règlement européen renforce également la nécessité de documenter tout processus ou procédure et préconise l'élaboration de codes de conduite (bonnes pratiques).

- Informer le Préposé fédéral de la communication de données hors du territoire suisse (art. 6 LPD)
- Déclarer le fichier au Préposé fédéral en cas de traitement de données sensibles, de profil de la personnalité ou de communication régulière de données personnelles à des tiers[10]
- Elaborer un règlement de traitement. Le règlement de traitement vise en premier lieu à rendre le développement de systèmes et le traitement de données aussi transparents que possible[11]. L'exemple mis en lien peut être simplifié en fonction de votre contexte.
- En cas de mise à disposition d'une plateforme collaborative à des usagers ou des clients, élaborer des conditions générales d'utilisation afin notamment de remplir l'obligation de transparence et de délimiter les rôles et responsabilités.

[10] *Voir* http://www.edoeb.admin.ch/datenschutz/00626/00743/00858/index.html?lang=fr
[11] *Voir* http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr

« Il convient d'être attentif à l'utilisation faite des données stockées sur le Cloud »

7. Recommandations spécifiques aux structures éducatives privées

7.1 Anonymisation

Privilégier en toute circonstance l'anonymisation ou la pseudonymisation des données personnelles des élèves, en particulier lors de la création de compte de messagerie, ou pour la reddition de travaux

7.2 Cloud gratuit

Il convient en outre d'être attentif à l'utilisation faite des données stockées sur le Cloud et d'éviter tout Cloud privé ou éducatif utilisant les données à des fins commerciales. Tel peut être le cas de sites gratuits, par opposition aux sites payants.

7.3 Travaux d'élèves

Considérer les travaux d'élèves de type dissertations comme des documents pouvant contenir des données personnelles sensibles (opinions personnelles, récits et témoignages). Ces documents sont particulièrement à sécuriser, à moins de couper totalement le lien entre le document et l'élève concerné.

7.4 Durée de conservation

Si les documents scolaires au format papier sont à conserver en raison d'exigences légales, il est recommandé de supprimer tout document scolaire au format numérique à la fin du cycle scolaire concerné.

8. Recommandations spécifiques aux données médicales

8.1 Localisation

Pour un accompagnement à la conformité, consultez nos experts.

Les données de santé sont de par la loi des données sensibles, qui requièrent un traitement dont la sécurité soit concrètement garantie, de la collecte à la suppression. Le lieu de conservation comme les canaux de communication ou d'accès à ces données doivent être propres à garantir la disponibilité, l'intégrité et la confidentialité des données. Le présent guide ne traite pas du e-dossier médical prévu par la loi fédérale et mis en œuvre par certains cantons, qui répond à des conditions spécifiques auxquelles il est renvoyé.

8.2 Cloud gratuit

Vu ce qui précède, il convient là aussi d'être attentif à l'utilisation faite des données stockées sur le Cloud et d'éviter tout Cloud privé utilisant les données à des fins commerciales. Tel peut être le cas de sites gratuits, par opposition aux sites payant.

8.3 Consentement du patient

Hormis de rares cas prévus par la loi, le traitement des données de santé réclame le consentement du patient. Par ailleurs, le droit à l'information de la personne concernée, en général, prend de l'importance en particulier avec le règlement européen. C'est pourquoi l'utilisation d'un Cloud dans ce domaine devrait faire l'objet d'un consentement explicite.

Ce guide a été élaboré par Isabelle Dubois, AD HOC RESOLUTION et Charly Delay et Vincent Ottinger de Pragm@TIC - Consulting Sàrl et est protégé par le droit d'auteur – avril 2016.

www.pragmatic-consulting.ch
www.adhocresolution.ch