FICHE INFO DU PPDT

Services collaboratifs gratuits en ligne et protection des données

PREAMBULE

La présente fiche informative intervient en complément de celle concernant le cloud computing (https://www.ge.ch/ppdt/fiches-info/doc/Cloud_computing.pdf).

En effet, le Préposé cantonal a constaté que des institutions publiques utilisent fréquemment des services gratuits en ligne (ex: Doodle, SurveyMonkey) ou proposent à des usagers de les utiliser; or, dans ce cadre, il n'est pas toujours facile de savoir si des données personnelles sont communiquées, lesquelles et, le cas échéant, quels sont les risques, les enjeux et les obligations incombant aux institutions publiques. La présente fiche informative a pour but de présenter les règles applicables en la matière, ainsi que les risques inhérents à l'utilisation de tels services.

Souvent, ces services gratuits en ligne sont faciles d'usage et pallient un manque de services similaires à l'interne. Il s'agit principalement d'offres dites de "software as a service" ou "logiciel en tant que service". Dans ce type d'offres, l'utilisateur n'est qu'un consommateur dans le cloud (nuage)[1]: il ne gère rien lui-même, ni les applications, ni les données, et a seulement accès aux fonctionnalités définies par le prestataire pour traiter les données dans le nuage.

En pratique, il s'agit par exemple de services permettant de

- ***Trouver une date pour une réunion qui convienne à plusieurs personnes (ex: Doodle)***
- ***Effectuer un sondage ou une enquête avec plusieurs questions (ex: SurveyMonkey, LimeSurvey)***
- ***Partager des documents (ex: Dropbox)***
- ***Travailler sur un même document (ex: Google Docs)***

L'utilisation de ces services par les institutions publiques genevoises, si elle implique des données personnelles au sens de l'art. 4 LIPAD[2], est soumise à la LIPAD; les règles topiques sont celles relatives à la sécurité des données et à la sous-traitance.

1 Pour rappel, le "cloud" ou "nuage" se définit comme l'exploitation de la puissance de calcul et/ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet.

2 Selon l'art. 4 litt. a LIPAD, on entend par données personnelles "toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable".

CADRE JURIDIQUE

Les art. 37 LIPAD et 13A RIPAD sont le siège de la matière; ils régissent respectivement la sécurité des données personnelles et la sous-traitance.

L'art. 37 LIPAD dispose:

[1] Les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées.

[2] Les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter.

[3] Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2. S'il implique l'exploitation de ressources informatiques et le traitement de données personnelles, ce contrôle doit s'exercer conformément à des procédures spécifiques que les instances mentionnées à l'article 50, alinéa 2, doivent adopter à cette fin, après consultation du préposé cantonal.

Services collaboratifs gratuits en ligne et protection des données

FICHE INFO DU PPDT

L'art. 13A RIPAD prévoit:

[1] Le traitement de données personnelles peut être confié à un tiers pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.

[2] L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même.

[3] La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant.

[4] Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article.

[5] S'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat.

[6] Le préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat.

L'al. 2 de cette disposition mérite d'emblée d'être souligné, puisqu'il précise que la responsabilité de l'institution en cas de sous-traitance est la même que si elle traitait les données elle-même.

Il convient encore de relever que la communication de données à un sous-traitant n'est pas considérée comme une communication de données personnelles à un tiers, conformément à l'art. 14 al. 4 RIPAD, qui renvoie à l'art. 13A RIPAD:

[4] Ne constitue pas une communication à un tiers de droit privé au sens de l'article 39, alinéa 9, de la loi la transmission d'informations à un mandataire, à un prestataire de service lié à une institution par un contrat de droit privé ou public ou à un représentant autorisé. L'article 13A du présent règlement est applicable.

L'UTILISATION D'UN "SOFTWARE AS A SERVICE"

Pour comprendre les risques liés à l'utilisation d'un service tiers en ligne, il faut avoir à l'esprit:

- Qui sont les parties prenantes liées à l'utilisation du service en ligne (ex: fournisseur d'accès, hébergeur, service web…)
- Quelles sont les données transmises (qu'elles soient activement transmises par l'utilisateur, par exemple une adresse e-mail, ou récoltées "à son insu", par exemple une adresse IP).

1. Les parties prenantes

Un service web (ex: Doodle, SurveyMonkey) fonctionne avec différents partenaires techniques; certains sont indispensables, indépendamment du service utilisé (ex: fournisseur d'accès à Internet, hébergeur) (1.1), d'autres sont nécessaires pour offrir le service spécifique (1.2) et certains peuvent avoir accès à des données, sans que leur intervention ne soit pourtant directement nécessaire au service offert (1.3). Un dernier type de parties prenantes qu'il convient de mentionner est extérieur au service offert mais lui impose des contraintes organisationnelles; il s'agit principalement des criminels.

Par ailleurs, il convient de souligner que, selon la juridiction concernée, les autorités peuvent exiger d'avoir accès à certaines données. Par exemple, en vertu du "*CLOUD Act*" (Clarifying Lawful Overseas Use of Data Act – https://www.congress.gov/bill/115th-congress/house-bill/4943/text) signé le 23 mars 2018 par le Président des États-Unis, les entreprises américaines sont tenues, à certaines conditions, d'accorder un accès aux données aux autorités américaines, indépendamment du lieu de stockage de ces données.

1.1 Les parties prenantes indispensables

S'agissant des parties prenantes indispensables, l'on peut distinguer deux situations: lorsque les données sont *en transit* et lorsqu'elles sont au repos.

Lorsque les données sont *en transit*, c'est-à-dire transférées vers ou depuis un service web, il y a nécessairement des intermédiaires techniques:

- Le fournisseur d'accès Internet (ex: Swisscom, Sunrise, Citycable)
- Les intermédiaires lors de la transmission de données via Internet (routeurs, qui appartiennent à différents opérateurs)

En effet, une transmission de données via Internet passe souvent par de nombreux intermédiaires et ne prend pas toujours le même chemin (routage)[1].

[1] Voir l'annexe 1 pour un exemple de routage.

Services collaboratifs gratuits en ligne et protection des données

FICHE INFO DU PPDT

Ces intermédiaires sont autant de parties prenantes. Comme ils ne sont contrôlables sans frais démesurés ni par l'utilisateur/l'utilisatrice, ni par le service web, ce dernier – s'il est sérieux – fournira une sécurité de la couche de transport, autrement dit un chiffrement des données allant et venant vers son site. Cette sécurité est reconnaissable au "s" pour *secure* du https:// de l'adresse web (exemple: http**s**://www.google.ch). Ce chiffrement empêche une lecture ou une altération des données en transit par un intermédiaire ou un tiers observant la transmission. C'est aujourd'hui un standard; **par conséquent, un service en ligne qui ne procure pas cette sécurité ne doit pas être utilisé**.

Pour assurer que cette connexion sécurisée se fasse auprès du site authentique du service en ligne, elle est vérifiée par une autorité de certification, qui est donc également une partie prenante.

Lorsque les données sont *au repos*, elles sont stockées sur des serveurs pour leur sauvegarde ou leur utilisation. Dans le cas d'un service web, on parle d'hébergement. Seuls les plus grands services web disposent de leurs propres hébergements. Les autres font recours à un tiers spécialisé, l'hébergeur, soit une nouvelle partie prenante, qui met à disposition des serveurs et assure leur disponibilité constante.

Les serveurs d'un hébergeur ne sont pas toujours en Suisse. Il est à noter qu'un service web qui a une adresse qui finit en **.ch** (domaine de premier niveau pour la Suisse) n'est pas forcément hébergé en Suisse. En effet, il est possible de faire pointer une adresse web vers l'adresse IP d'un serveur web hébergé physiquement à l'étranger[2].

Par ailleurs, les services web recourent fréquemment aux techniques de *cloud computing* – directement ou via l'hébergeur – pour tout ou partie de leur infrastructure. Les mécanismes de réplication et de répartition automatique de la charge de trafic inhérents à ces techniques ont pour conséquence que les données ne sont pas forcément toujours stockées sur le même serveur dans un même pays.

Qu'il utilise un hébergeur ou non, le service web doit prendre des mesures organisationnelles et techniques pour protéger les données au repos.

Pour ce qui est de la protection contre l'accès illégitime d'un tiers, le chiffrement est ici aussi une solution commune. On distingue entre un chiffrement des données elles-mêmes et/ou du support sur lequel elles sont stockées.

La question de la gestion des clés de déchiffrement et de qui y a accès (l'hébergeur? le client? autre?) est alors essentielle.

Le site web www.ge.ch est accessible par défaut via une connexion sécurisée vérifiée par l'autorité de certification SwissSign AG, une joint venture entre les CFF, La Poste, Swisscom et plusieurs banques et assurances suisses.

Répartition géographique au 31.12.2018 des offres de cloud computing d'Amazon Web Services (actuellement leader de la branche).

Source : https://aws.amazon.com/fr/about-aws/global-infrastructure/ - La description précise: " En plus de répliquer des applications et des données sur plusieurs centres de données de la même région à l'aide des Zones de Disponibilité (AZ), vous pouvez également choisir d'améliorer la redondance et la tolérance aux pannes en répliquant les données entre les régions".

[2] Voir l'annexe 2.

1.2 Les parties prenantes nécessaires au traitement des données pour l'offre du service

Au-delà des infrastructures essentielles de stockage et de communication, le service web a besoin d'un environnement informatique permettant de déployer le service spécifique qu'il offre ("les artefacts": base de données, scripts, etc.). Parfois, cet environnement est mis à disposition par l'hébergeur (voir par exemple les offres d'Infomaniak, qui est également hébergeur), parfois par le service web lui-même, parfois par des tiers.

Pour savoir quels sont cet environnement et ces artefacts, dans quelle mesure ceux-ci requièrent la transmission des données traitées à des tiers et, le cas échéant, à quelles conditions, l'utilisateur/l'utilisatrice devra consulter les conditions générales d'utilisation du service web, pour autant que ces aspects y soient mentionnés[3].

Or, la lecture des conditions générales des services offerts est souvent laborieuse, tant les clauses sont nombreuses et complexes.

> Exemple: le service web SurveyMonkey précise au point 15.4 de ses conditions générales qu'il travaille « *avec des partenaires de confiance pour certains éléments de nos Services. (« sous-traitants »)* ». La liste de ces sous-traitants n'est disponible que sur demande via un formulaire en anglais et sur condition de non- propagation. Par ailleurs, sa politique de confidentialité contient au point 16 des "informations spécifiques à d'autres services", qui sont certes mentionnés nommément, mais dont ni la nécessité technique ni le statut (propriété de SurveyMonkey?) ne sont clairs.

Par défaut, l'utilisateur/l'utilisatrice n'a donc souvent pas d'autre choix que de se fier à la bonne foi des services web. Hormis ce qu'ils veulent en dire, le traitement des données reste, dans le détail, une boîte noire.

L'on constate donc ici **la difficulté d'application des al. 3 et 4 de l'art. 13A RIPAD**, lorsque les conditions générales d'utilisation du service web font office de contrat au sens de ces dispositions. En particulier, la possibilité d'effectuer des audits sur le site du sous-traitant ne sera vraisemblablement jamais prévue par des conditions générales et il est impossible pour une institution publique genevoise de s'assurer du respect des prescriptions de la LIPAD.

1.3 Les parties prenantes supplémentaires

Les services web les plus connus appartiennent à des fournisseurs commerciaux. La gratuité de ces services découle la plupart du temps d'un modèle d'affaire en *freemium*, à savoir une offre de base gratuite sur laquelle se greffent des fonctions supplémentaires ou de meilleures performances payantes.

Cette offre de base gratuite s'accompagne très fréquemment d'un traitement des données des utilisateurs/utilisatrices **qui va au-delà du nécessaire requis pour le seul bon fonctionnement du service et qui fait intervenir d'autres services tiers en arrière-plan**. Il s'agit la plupart du temps de suivi publicitaire, qui permet de monétiser la gratuité du service. Ce traitement de données concerne aussi bien les utilisateurs/utilisatrices créant une nouvelle offre via ces services (le cas échéant en ouvrant un compte utilisateur[4]) que les destinataires[5] de cette offre ou les autres visiteurs/visiteuses. Le cas échéant, un transfert de leurs données personnelles dans des juridictions différentes de la Suisse n'est pas exclu. Les conditions d'utilisation et les politiques de confidentialité des services web décrivent ce traitement de données dans des termes plus ou moins clairs, et/ou en se référant aux conditions et politiques de chacun des autres services entrant en ligne de compte.

Ce transfert de données, potentiellement à l'étranger et dans des pays ne disposant pas d'une législation assurant un niveau de protection adéquat, est ici encore difficilement compatible avec la LIPAD, particulièrement avec l'art. 13A al. 5 et 6 RIPAD, ainsi qu'avec les grands principes de protection des données.

> Exemple: dans sa politique de confidentialité (disponible uniquement en anglais), le service web Doodle déclare recourir à six partenaires différents pour analyser son trafic[6]. Doodle utilise également les services de Google (AdSense et AdExchange Network) pour livrer de la publicité basée, entre autres, sur le contenu des sondages que l'utilisateur/l'utilisatrice crée via Doodle et son adresse IP (qui est une donnée personnelle[7]). Doodle dit également passer par "*d'autres entreprises publicitaires tierces*". Un lien vers plus d'informations à cet égard fait apparaître 86 requêtes vers autant de tels partenaires publicitaires, qui ont chacun leur propre politique de confidentialité. Doodle précise que la sienne peut changer à tout moment, et que son offre payante ne comprend pas de publicité.

Note sur les cookies: lors de la visite d'un site web, il est fréquent qu'apparaisse une note signalant l'utilisation de cookies (c'est également le cas sur www.ge.ch). Un cookie est un petit fichier qui enregistre des informations sur l'appareil visitant actuellement le site, s'y télécharge et est envoyé par le navigateur de ce même appareil à chaque nouvelle visite du site web pour une durée

---

3 Il est certes possible de déterminer une partie des techniques utilisées de par le fait qu'elles doivent être exposées publiquement pour que le service fonctionne, mais cela ne permettra pas de comprendre ce fonctionnement en détail.

4 Par exemple, le membre de la fonction publique qui crée le compte utilisateur dans SurveyMonkey.

5 Les usagers interpellés par l'institution publique et dont les données sont traitées.

6 La confidentialité des données transmises à ces partenaires est évoquée de manière équivoque. Ainsi, Doodle prétend anonymiser les adresses IP fournies à Google Analytics; or ce service n'utilise pas les adresses IP pour identifier les visiteurs/visiteuses d'un site web de manière unique. Doodle dit utiliser le service HockeyApp de Microsoft en ne transmettant aucune donnée permettant d'identifier l'appareil mobile de l'utilisateur/l'utilisatrice de manière unique, mais la politique de confidentialité de HockeyApp mise en lien (en l'occurrence la "*Microsoft Privacy Statement*") fait explicitement référence à l'utilisation de données personnelles.

7 ATF 136 II 508.

déterminée. Il y a plusieurs types de cookies. Les uns sont parfois essentiels au bon fonctionnement de certaines parties du site web ou aident l'expérience de l'utilisateur/l'utilisatrice (en se souvenant de la langue dans laquelle elle a lu le site ou en se rappelant automatiquement de ses données de connexion, par exemple). D'autres appartiennent à des services tiers, comme les services de suivi publicitaire. À ce titre, une récolte d'informations permettant un profilage de l'utilisateur/l'utilisatrice est possible. Rares sont les sites qui décrivent **explicitement** combien de cookies s'installent, ainsi que leurs types[8]. Quand l'utilisateur/l'utilisatrice, faute de vrai choix, accepte l'utilisation des cookies, il/elle accepte de fait souvent un traçage (publicitaire). Ce dernier peut en outre utiliser d'autres techniques en plus des cookies[9].

En résumé, de l'infrastructure essentielle jusqu'à la monétisation des offres *freemium*, une pléthore de parties prenantes doivent ou peuvent intervenir dans l'utilisation d'un service web, impliquant *de facto* des relations contractuelles en cascade dont il est difficile d'avoir une vue d'ensemble.

Les institutions publiques doivent donc être très vigilantes dans le choix de leurs partenaires contractuels, afin de s'assurer que les règles de la LIPAD et du RIPAD seront respectées. De même, elles doivent être attentives à la communication qu'elles font aux usagers, lorsqu'elles utilisent des "*software as a service*".

2. Les données transmises

Si toutes les parties prenantes mentionnées ci-dessus traitent d'une manière plus ou moins directe des données, toutes **n'ont pas accès à des données personnelles, à savoir des informations qui se rapportent à une personne identifiée ou identifiable**[10], dont le traitement par une autorité publique genevoise est soumise à la LIPAD.

> Exemple fictif: une bibliothèque publique veut connaître l'avis de ses usagers/usagères sur ses services. Une collaboratrice ouvre un compte auprès d'un service web gratuit et crée un questionnaire en ligne. Ce dernier contient quelques questions fermées (oui/non/ne sait pas), quelques questions ouvertes – avec des champs permettant à l'utilisateur/l'utilisatrice d'écrire sa réponse – et une option facultative demandant à la répondante son nom et un moyen de la contacter pour plus d'informations et pour recevoir l'analyse des résultats une fois l'enquête terminée. L'adresse web de ce questionnaire est mise en lien sur le site de la bibliothèque, un petit tract en parle au guichet du prêt, etc. S'ensuivent les premières réponses des usagers/usagères jusqu'à une date limite, choisie par la bibliothèque.

Dans ce cas de figure courant, les transmissions de données qui entrent en compte sont les suivantes:

1. En ouvrant un compte auprès du service web, la collaboratrice a entré son nom et une adresse e-mail professionnelle qui l'identifie → ce sont **des données personnelles**.
2. Les réponses que l'utilisateur/l'utilisatrice fait aux questions fermées sont a priori de simples données[11]. Ses réponses aux questions ouvertes peuvent **potentiellement** contenir des données personnelles.
3. L'option facultative comprend **exclusivement des données personnelles**.

Ces données ont été fournies activement d'une part par la collaboratrice, d'autre part par le répondant/la répondante au questionnaire. Mais comme il y a de fortes probabilités que l'un/l'une comme l'autre n'ont pas lu les conditions générales et la politique de confidentialité du service web, **ils ont tous les deux fourni inconsciemment et passivement des données personnelles**[12] en acceptant plusieurs cookies ou d'autres méthode de traçage présents sur le service web.

LES RISQUES LIES A L'UTILISATION DE "SOFTWARE AS A SERVICE"

Comme mentionné ci-dessus, les services web tiers sont appréciés par les utilisateurs/utilisatrices individuel/le-s pour leur disponibilité, leur aisance d'utilisation et leur gratuité. Ils recèlent néanmoins des risques inhérents à leur nature et aux pratiques des entreprises les détenant.

Les risques principaux découlent de la délégation complète du contrôle sur les données de l'utilisateur/l'utilisatrice au service web.

---

8 Le cas échéant, il est possible de les déterminer à la visite du site ou après acceptation des cookies, mais cela requiert une connaissance approfondie des outils fournis avec le navigateur web.

9 Pour un aperçu, voir https://myshadow.org/fr/browser-tracking et amiunique.org.

10 Voir l'art. 4 LIPAD.

11 Toutefois, une réponse à une question fermée, si elle peut être liée à une adresse IP, peut constituer une donnée personnelle, puisqu'il s'agit d'une information se rapportant à une personne identifiable. Il pourrait même s'agir d'une donnée personnelle sensible si la question porte sur un élément lié à la santé ou à l'existence de poursuites pénales, par exemple.

12 Dans les faits, c'est moins le cas pour la collaboratrice de la bibliothèque qui utilise un ordinateur (partagé ?) de son institution que de l'utilisateur/l'utilisatrice qui répond probablement au questionnaire sur un appareil privé qui lui appartient.

Concrètement, les risques concernent:

1. ***La disponibilité***
   - Que faire si le service web n'est plus accessible, pour une raison technique ou autre, s'il ferme ou est acquis par un tiers qui en change les conditions d'utilisation ?
   - Comment récupérer les données (traitées) sans perte pour une utilisation par un autre service ou en interne (portabilité des données) ?
2. ***L'intégrité***
   - Comment gérer les droits d'accès aux données ? Comment s'assurer des mesures de protection vis-à-vis d'un accès, qu'il soit autorisé (sous-traitance) ou indu[13] ? Le cas échéant, comment être informé de l'accès par des autorités étrangères (dans leur juridiction) ?
   - Comment s'assurer des mesures de sauvegarde des données ?
   - Le cas échéant, comment identifier des failles dans la chaîne de sous-traitance ?
3. ***Le stockage***
   - Comment s'assurer de la localisation des serveurs et, le cas échéant, des contrats de sous-traitance qui y sont liés ?
   - Comment s'assurer de l'isolation des données[14] ?
4. ***La conformité réglementaire***
   - Comment s'assurer du respect des normes légales, des bonnes pratiques et des standards techniques ?
   - Comment s'assurer que les données ne sont pas conservées au-delà de ce qui est nécessaire à leur traitement et, le cas échéant, qu'elles ont bien été effacées[15] ?

Les obligations prévues par les art. 37 LIPAD et 13A RIPAD ont pour but de remédier à ces risques. L'aide-mémoire intitulé "Risques et mesures spécifiques à la technologie de Cloud computing" émis par Privatim souligne également les points d'attention[16].

Toutefois, dans les faits, un contrôle indépendant en tout temps relatif à ces questions n'est pas possible, même s'il est requis par l'art. 13A al. 3 RIPAD. Pour autant que les conditions générales des services web y répondent **de manière précise**, elles sont la seule assurance.

Ces conditions générales constituent par ailleurs un contrat standard souvent non négociable, contrairement à ce qu'implique un mandat pérenne entre un prestataire privé et l'État. Il est à noter qu'il existe des accords-cadres dans certains domaines[17].

DES ALTERNATIVES ECONOMES EN DONNEES

Il existe des offres gratuites plus respectueuses de la protection des données que d'autres. Elles découlent essentiellement des mouvements pour les **logiciels libres** et ceux **à code source ouvert**. Ces deux mouvements ont en commun la volonté de développer des logiciels en licence libre, c'est-à-dire permettant à chaque utilisateur/utilisatrice – sans autorisation explicite individuelle préalable – de les copier, de les étudier, de les modifier, de les réutiliser et de les redistribuer, parfois même de manière commerciale, par opposition aux logiciels dits propriétaires. Plus ces logiciels sont utilisés, plus il se trouve de personnes prêtes à les améliorer.

---

13 Les cas de manquement à la sécurité de l'information en ligne sont fréquents. De nombreuses listes de données de connexion (noms d'utilisateurs et mots de passe) circulent en ligne. En janvier 2019, une des plus grandes listes de telles informations agrégées a été rendue disponible : elle compte pas moins de 773 millions de combinaisons uniques d'adresses e-mail et de mots de passe. Le site https://haveibeenpwned.com suit l'actualité des bases de données en ligne qui sont compromises et permet à chacun de tester si son adresse e-mail se trouve dans de telles listes.

14 Les services web en cloud public "mutualisent" souvent les données sur les serveurs qu'ils utilisent, c'est-à-dire qu'ils hébergent les données et services de clients différents sur des serveurs identiques. Le risque d'un accès indu accidentel d'un tiers en est d'autant plus grand. Par ailleurs, une attaque contre une ressource mutualisée peut avoir des répercussions sur toutes les autres.

15 A l'exemple de Dropbox, qui a conservé des données prétendument effacées de manière permanente pendant des années: https://www.zdnet.com/article/dropbox-bug-kept-users-deleted-files-on-its-servers-for-six-years/

16 http://www.privatim.ch/fr/aide-memoire-sur-les-risques-et-les-mesures-specifiques-au-cloud-computing/

17 Par exemple entre educa.ch et microsoft pour Office 365: https://dsb.zh.ch/internet/datenschutzbeauftragter/de/publikationen/anleitungen/_jcr_content/contentPar/form_1/formitems/office_365_in_volks_/download.spooler.download.1548063864789.pdf/Leitfaden-Office-365-in-den-Schulen.pdf

Par exemple:

- Un de ces logiciels les plus répandus est Linux, un noyau de système d'exploitation qui équipe dans ses diverses variantes des ordinateurs personnels, une grande partie des serveurs web publics et de nombreux appareils connectés. Le système d'exploitation pour téléphones mobiles Android, développé principalement par Google, a été créé à partir du noyau Linux et d'autre logiciels dont le code source est ouvert, et est lui-même distribué sous une licence similaire
- Le site web le plus connu qui est issu de ce courant est assurément Wikipédia et ses nombreuses variantes linguistiques, comme fr.wikipedia.org pour sa principale offre francophone. Ses ressources sont non seulement libres d'accès, mais elles doivent l'être impérativement pour être complétées, corrigées et améliorées par tout/toute utilisateur/utilisatrice le souhaitant. Le logiciel permettant l'utilisation de Wikipédia – nommé MediaWiki – est aussi open source et sous licence libre; chacun peut donc se l'approprier pour créer sa propre encyclopédie ou pour tout autre usage que rend possible ce logiciel. Le tout est géré par une organisation à but non lucratif, la Wikimedia Foundation

L'association française Framasoft, dont le but principal est l'éducation aux logiciels libres, propose sur son site web https://degooglisons-internet.org de nombreux services web que chacune peut utiliser gratuitement.

Par exemple:

- "Framadate" ou "findmind.ch" pour trouver une date ou faire un sondage
- "Framaforms" pour créer des formulaires

Ces alternatives n'exploitent pas de données personnelles au-delà du strict nécessaire ni ne suivent ultérieurement leurs utilisateurs/utilisatrices. Dans une optique de respect de la protection des données, elles sont donc à préférer aux offres commerciales gratuites, même si elles ne s'affranchissent pas des risques mentionnés ci-dessus.

L'on peut également se référer à divers documents émis par le Préposé à la protection des données du canton de Zurich qui liste des solutions qui tiennent compte de la protection des données des utilisateurs et utilisatrices[18].

Il faut toutefois souligner que les solutions à privilégier sont les solutions "sur mesure" ou internes à l'institution publique concernée.

CONCLUSION

L'utilisation de "*software as a service*" n'est pas anodine en terme de protection des données. En effet, l'institution publique reste responsable des données personnelles ainsi sous-traitées comme si elle les traitait elle-même. Or, comme cette fiche informative l'explique, l'institution publique perd souvent tout contrôle sur les données personnelles selon le sous-traitant choisi. C'est pourquoi il importe que les institutions publiques soient vigilantes dans le choix des sous-traitants et favorisent, autant que faire se peut, des solutions *ad hoc* internes, leur permettant de respecter les dispositions prévues par la LIPAD en la matière. En effet, tant l'art. 37 LIPAD que l'art. 13A RIPAD posent des exigences en matière de sécurité et de sous-traitance qui permettent aux institutions publiques de se prémunir face aux risques liés à cette perte totale de contrôle sur les données.

Précisons finalement un point essentiel, à savoir que le traitement de données personnelles ne peut être confié à un tiers que pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

[18] https://dsb.zh.ch/internet/datenschutzbeauftragter/de/publikationen.html#anleitungen

FICHE INFO DU PPDT

Services collaboratifs gratuits en ligne et protection des données

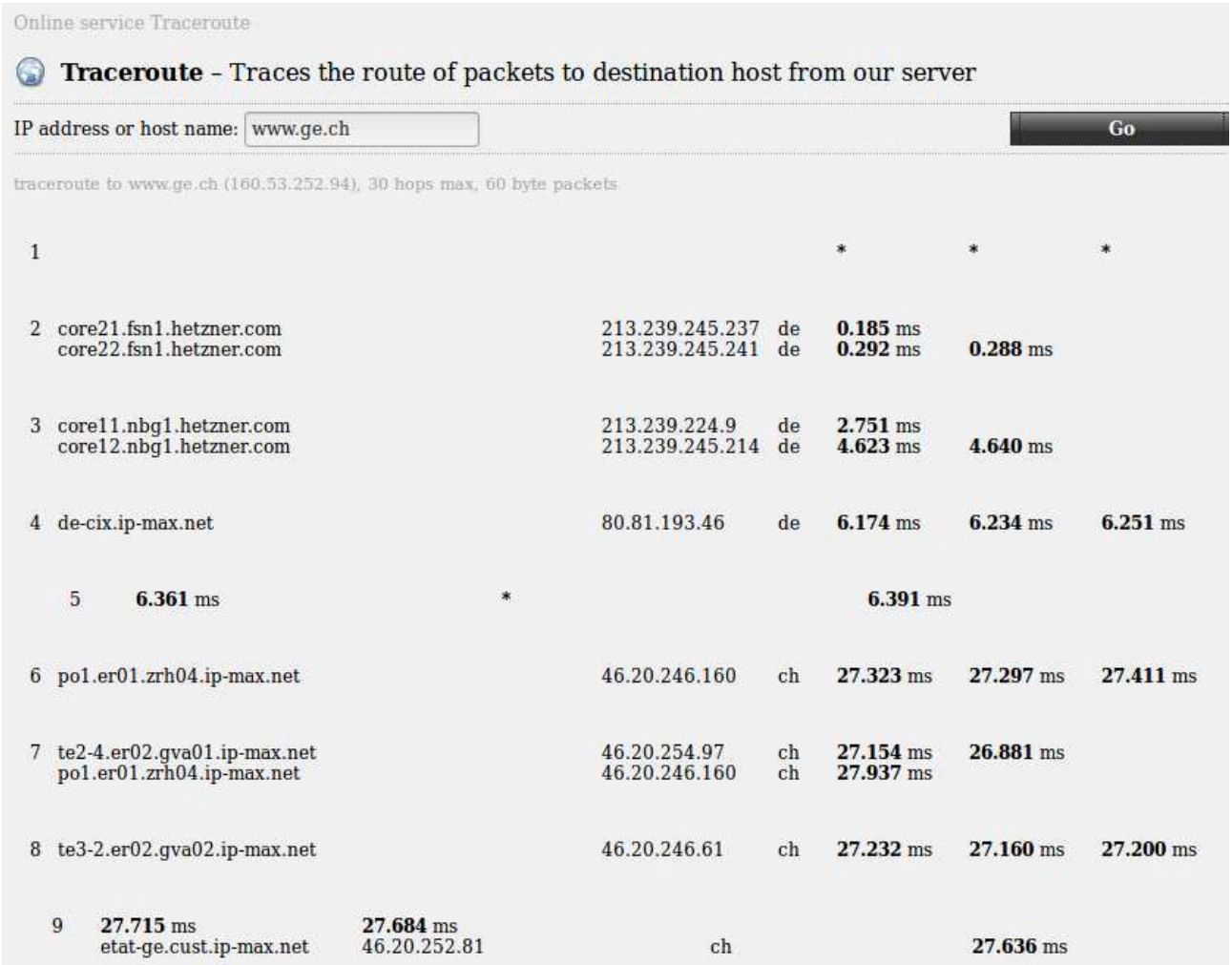
La présente fiche informative a été réalisée avec le concours de M. Julien Clavel, consultant en techniques du web.

PPDT - 18.02.2019

Services collaboratifs gratuits en ligne et protection des données

ANNEXES

Annexe 1



Online service Traceroute

Traceroute – Traces the route of packets to destination host from our server

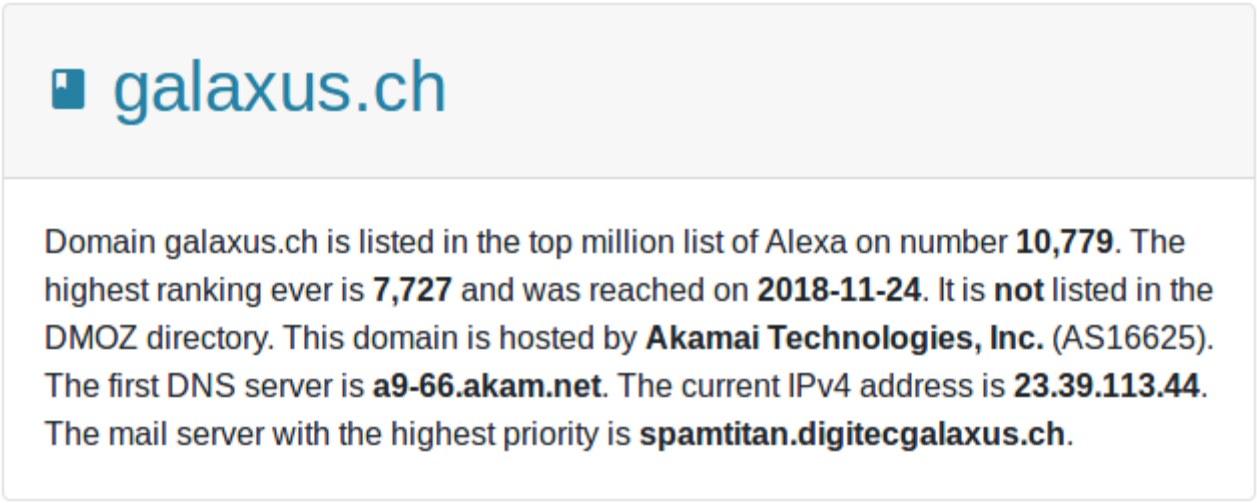
IP address or host name: www.ge.ch Go

traceroute to www.ge.ch (160.53.252.94), 30 hops max, 60 byte packets

1				*	*	*
2	core21.fsn1.hetzner.com core22.fsn1.hetzner.com	213.239.245.237 213.239.245.241	de de	**0.185** ms **0.292** ms	**0.288** ms	
3	core11.nbg1.hetzner.com core12.nbg1.hetzner.com	213.239.224.9 213.239.245.214	de de	**2.751** ms **4.623** ms	**4.640** ms	
4	de-cix.ip-max.net	80.81.193.46	de	**6.174** ms	**6.234** ms	**6.251** ms
5	**6.361** ms	*		**6.391** ms		
6	po1.er01.zrh04.ip-max.net	46.20.246.160	ch	**27.323** ms	**27.297** ms	**27.411** ms
7	te2-4.er02.gva01.ip-max.net po1.er01.zrh04.ip-max.net	46.20.254.97 46.20.246.160	ch ch	**27.154** ms **27.937** ms	**26.881** ms	
8	te3-2.er02.gva02.ip-max.net	46.20.246.61	ch	**27.232** ms	**27.160** ms	**27.200** ms
9	**27.715** ms etat-ge.cust.ip-max.net	**27.684** ms 46.20.252.81	ch		**27.636** ms	

L'utilitaire *traceroute* du site ping.eu montre les étapes du chemin que prend une requête partant du serveur de ping.eu (qui se trouve en Allemagne) pour un site web donné, ici: www.ge.ch. Essayez par vous-même pour un site donné, plusieurs fois de suite, et comparez les résultats. Vous verrez qu'ils ne sont pas toujours exactement les mêmes.

Annexe 2



Le site web dnslytics.com donne des informations sur des domaines, ici, galaxus.ch, dont l'hébergeur est Akamai Technologies. L'adresse IP du serveur (23.39.113.44 au moment de cette requête)…

… permet de le localiser géographiquement, en l'occurrence: aux Pays-Bas, bien que l'adresse du site soit dans le domaine de premier niveau pour la Suisse (.ch).