ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

La Commission

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/atprd

Fribourg, 28 août 2017

Note de dossier relative à l'externalisation du traitement des données de l'Etat de Fribourg dans un Cloud

—

2017-PrD-77

I. Introduction

A titre préliminaire, il est important de relever que l'hébergement de la messagerie Outlook est une petite partie des demandes d'externalisation. En effet, plusieurs requêtes transmises en parallèle par différents collaborateurs du SITel sont actuellement en traitement au sein de notre Autorité. Elles portent notamment sur la refonte du registre fiscal, l'évolution de la plateforme informatique FRI-PERS, l'externalisation de l'hébergement, l'exploitation et la maintenance des sites Internet du canton de Fribourg, la gestion des appareils mobiles ainsi que l'introduction de l'Office 365 et Skype for business.

Afin de donner un fil rouge au SITel concernant les différents projets en cours et futurs, nous évaluons l'externalisation du traitement des données des organes publics dans les Clouds de manière générale. Cette analyse reprend en outre les recommandations du Préposé fédéral à la protection des données et à la transparence (PFPDT) et l'aide-mémoire de PRIVATIM concernant le Cloud computing dans le domaine scolaire.

II. Risques inhérents à l'externalisation[1]

A. Risques liés à la perte de maîtrise de son système d'information

L'interconnexion mondiale et l'utilisation de la mémoire virtuelle font qu'il est souvent impossible de localiser les données, notamment lorsqu'on a recours à des Clouds publics. Le maître des données ne sait pas où les données qu'il a déposées dans le Cloud sont enregistrées et traitées alors qu'il répond de leur utilisation. Il ignore souvent si des sous-traitants interviennent et s'ils veillent à une protection adéquate des données. L'utilisateur d'un Cloud ne peut donc pas assumer ses obligations en matière de protection des données (garantir la sécurité des données, accorder un droit d'accès, corriger ou effacer des données) ou uniquement en partie.

Il existe des risques liés :

> **à la sous-traitance** : vérifier que le sous-traitant dispose des capacités techniques et financières

[1] PFPDT, Explications concernant l'informatique en nuage (https://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=fr) ; Guide de l'externalisation des systèmes d'information de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), 2010 (http://www.ssi.gouv.fr/externalisation).

nécessaires à la bonne exécution des prestations ; s'assurer qu'une sous-traitance en cascade ne conduira pas à rendre inefficace les contraintes de sécurité exigées par le mandant ; le mandant doit se réserver le droit de récuser tout sous-traitant ne présentant pas les garanties suffisantes pour exécuter les prestations conformément aux exigences de sécurité identifiées ; tout traitement de données par un sous-traitant ne peut être réalisé que sur instruction du responsable du traitement et à condition qu'un contrat garantissent les mesures de sécurité et de confidentialité ;

> **à la localisation de données** : il peut arriver que certaines données soient enregistrées dans plusieurs centres situés dans le monde entier ; il faut s'assurer que l'ensemble des lieux d'hébergement répondent aux exigences de sécurité (niveau de protection adéquat de l'Etat) et de la législation ; une dissémination peut poser des problèmes du point de vue de la protection des données et de la sécurité des données mais également des problèmes pour le respect des obligations légales (conservation des données, droit d'accès, sauvegarde du secret, audit, etc.) ;

> **l'accès d'autorités étrangères aux données** : dans de nombreux cas, les données traitées dans le Cloud sont communiquées à l'étranger. Elles sont souvent enregistrées dans les pays qui ne leur assurent pas une protection suffisante. Les prestataires de services peuvent se voir ordonner par des autorités ou des tribunaux étrangers de donner accès aux données enregistrées dans le Cloud, même si ces données ne sont pas traitées ou enregistrées dans le pays en question ;

> **à la captivité** : les utilisateurs peuvent devenir dépendants du prestataire en raison de la faible portabilité et de la faible interopérabilité des services en nuage. En effet, si le prestataire n'a pas recours à une technologie et à une interface standardisées, le rapatriement des données dans le système informatique de l'utilisateur ou leur migration dans le nuage d'un autre prestataire peut être impossible ou extrêmement coûteux.

> **à la perte de données** : les données peuvent être volées, effacées, écrasées par erreur ou subir d'autres modifications entraînant leur perte. Ainsi, il est impératif de recourir à un système de sauvegarde des données originales et que des systèmes de sécurité soient implémentés.

> **aux pannes de système et de réseau et non disponibilité des ressources et des services** : des pannes peuvent entraîner des pertes de données ou impliquer l'accès de personnes non autorisées aux données (la confidentialité, la sécurité et l'intégrité des données ne sont plus garanties). Ces pannes peuvent en outre paralyser le fonctionnement d'une entreprise ou d'une autorité : un tel scénario entraînerait non seulement des pertes financières, mais aussi de graves conséquences pour la réputation de l'organisation concernée.

> **à un usage abusif de données** : tous les prestataires de services n'indiquent pas comment les droits d'accès (physiques et virtuels) des employés sont réglés et surveillés. Souvent, les utilisateurs ne peuvent pas non plus consulter les clauses de confidentialité. Les nuages publics posent particulièrement problème à cet égard.

B. Risques liés aux interventions à distance

L'infogérance implique souvent la mise en place de liaisons permettant d'intervenir à distance. En évitant le déplacement d'un ou plusieurs techniciens, les interventions à distance permettent une réduction significative des coûts et des délais d'intervention. Des vulnérabilités peuvent apparaître selon le dispositif de télémaintenance : liaison établie de façon permanente avec l'extérieur, mots de passe par défaut (connu du monde entier) ou faibles, présence de failles dans les interfaces d'accès,

systèmes d'exploitation des dispositifs non tenus à jour, absence de traçabilité des actions, personnels responsables de ces dispositifs et collaborateurs non conscients des problèmes de sécurité ou mal formés, interconnexion de systèmes sécurisés de confiance à des système de niveau faible (internet par exemple).

Les risques liés aux dispositifs dédiés aux interventions à distance sont :

> l'intrusion dans le système d'information par une personne non-autorisée : indisponibilité de l'équipement voire du système d'information ; atteinte à la confidentialité ou à l'intégrité des données présentes sur le système d'information ;

> l'abus de droit d'un technicien du centre de support lors d'une intervention : accès à des données confidentielles ou téléchargement massif de ces dernières, modification de données, absence de traçabilité.

Il est recommandé de sécuriser la liaison par exemple par VPN, de restreindre l'accès par des droits d'accès, d'assurer une authentification des techniciens assurant le support, d'assurer une traçabilité des actions, d'effectuer des audits et d'assurer les mesures organisationnelles également.

C. Risques liés à l'hébergement mutualisé

L'informatique en nuage implique que les données de plusieurs utilisateurs qui n'ont aucun lien entre eux soient traitées dans le même nuage et par le même système. Cela augmente le risque qu'une attaque contre un des utilisateurs affecte également les autres. A la suite d'une attaque de hackers ou de déni de service, les données peuvent être indisponibles voire volées. Il est donc extrêmement important que le traitement des données des différents utilisateurs du Cloud soit strictement séparé et qu'il n'y ait pas de mélange de données.

Ainsi, l'hébergement sur un serveur spécifique doit être privilégié. Si le choix d'un hébergement mutualisé est retenu, il convient de bien analyser les conséquences de toutes les attaques potentielles et de prévoir dans le contrat les actions permettant un traitement efficace d'un incident, notamment la récupération de tous les journaux et l'isolement du réseau sans extinction des machines impliquées.

III. L'utilisation du Cloud du point de vue de la protection des données

Les organes publics, qui prévoient d'externaliser le traitement des données dans un Cloud, doivent veiller à respecter le droit sur la protection des données :

> selon l'article 10 LPrD, ils ne doivent transmettre des données personnelles à des tiers que s'il **existe une base légale** pour ce faire (communication systématique). Ainsi, le prestataire de services doit être contraint de se conformer entièrement aux dispositions sur la protection des données applicables en Suisse, de même que tout sous-traitant.

> S'il existe une obligation légale ou contractuelle de garder le secret, les données **ne doivent pas être confiées** à un prestataire de Cloud (art. 11 let. b LPrD), de sorte qu'il est possible que seule une partie des données puissent être externalisées.

> Le traitement de données personnelles découlant de l'utilisation de l'informatique en nuage relève du traitement sur mandat au sens de l'article 18 LPrD. Le traitement de données personnelles ne peut être confié à un prestataire de services pour autant que l'organe public qui fait traiter des données personnelles demeure responsable de la protection des données, en lui

donnant les instructions nécessaires et en veillant à ce que celui-ci n'utilise les données ou ne les communique que pour l'exécution du mandat. Lorsque le prestataire de services n'est pas soumis à la LPrD, comme c'est le cas pour des entreprises privées, l'organe public assure la protection des données par un contrat. Ainsi, la sécurité des données doit être garantie au sens de l'art. 22 LPrD et du Règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD). Ces dispositions prévoient que **l'organe public qui traite des données personnelles doit prendre les mesures d'organisation et les mesures techniques appropriées contre tout traitement non autorisé des données et qu'il faut assurer la confidentialité, la disponibilité et l'intégrité des données.** Le prestataire doit protéger les données contre les risques suivants : destruction accidentelle ou non autorisée ; perte accidentelle ; erreurs techniques ; falsification, vol ou utilisation illicite ; modification, copie, accès ou autre traitement non autorisés. Ces mesures doivent faire l'objet d'un examen périodique sur place. La mise en œuvre concrète des mesures de protection des données dépend de l'entreprise ou de l'autorité, du type de données, de l'organisation du nuage et de son découpage. Selon la nature des prestations, voici une liste non-exhaustive des exigences de sécurité : gestion de la sécurité ; protection antivirale ; mises à jour, correctifs de sécurité ; sauvegardes et restauration ; continuité d'activité ; authentification ; confidentialité et intégrité des flux ; contrôle ; imputabilité et traçabilité ; personnels en charge des prestations ; exigences de sécurité concernant le personnel extérieur. **Si les données sont confidentielles, secrètes ou sensibles, leur délocalisation dans un nuage, à l'étranger, n'est pas autorisée.** Le Préposé fédéral à la protection des données donne les mêmes recommandations aux organes publics fédéraux. Il est ainsi également envisageable que seule une partie du traitement des données puisse être externalisée. De plus, la transmission à l'étranger de données personnelles des visiteurs de site Internet peut notamment permettre aux autorités étrangères d'accéder aux données situées dans leur pays, sur la base de leur législation nationale.

> Le maître du fichier doit s'assurer que le mandataire n'effectue le traitement de données que de la manière dont il serait lui-même en droit d'effectuer. Il incombe alors à l'organe public de vérifier régulièrement le respect de traitement des données, ce qui implique un important contrôle.

> L'utilisation de services en nuage implique dans de nombreux cas de communiquer des données à l'étranger, puisque leur traitement a souvent lieux sur des serveurs disséminés dans le monde entier. Les pays concernés connaissent très souvent un niveau de protection des données inférieur à celui de la Suisse. Des données personnelles ne peuvent être communiquées à l'étranger **que dans les Etats qui garantissent un niveau de protection adéquat** (art. 12a al. 1 LPrD). Toutefois, des données personnelles peuvent être communiquées dans les Etat n'offrant pas une telle garantie, lorsque l'une des conditions suivantes est réalisée : a) des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger ; b) la personne concernée a, en l'espèce, donné son consentement explicite ; c) le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat, et les données traitées concernent le cocontractant ; d) la communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, à l'exercice ou à la défense d'un droit en justice ; e) la communication est, en l'espèce, nécessaire la protection de la vie ou de l'intégrité corporelle de la personne concernée. La transmission à l'étranger de données personnelles peut notamment permettre aux autorités étrangères d'accéder aux données situées dans leur pays, sur la base de leur législation nationale. Ce point est particulièrement délicat pour les organes publics qui doivent protéger les données de leurs

citoyens notamment contre les accès non autorisés. **Il est important de relever qu'il revient à celui qui transmet les données à l'étranger de prouver qu'il a pris toutes les mesures nécessaires pour garantir un niveau de protection adéquat.**

> Enfin, l'utilisateur répond du droit d'accès (art. 23ss LPrD) et du droit d'effacer ou de rectifier les données (art. 26 LPrD). Ces droits doivent être garantis en tout temps et leur mise en œuvre doit respecter les prescriptions en matière de protection des données, ce qui peut poser de grandes difficultés si l'utilisateur ne sait pas où sont stockées les données.

Au vu de ce qui précède, nous relevons une absence de base légale concernant l'externalisation du traitement de données des organes publics dans un Cloud. Dès lors, c'est la LPrD qui est applicable. Cependant, l'externalisation doit tenir compte de la révision de la Loi fédérale sur la protection des données (LPD) et de la révision de la LPrD qui va en découler. En outre, la législation sur le dossier électronique du patient exige que le support de données soit en Suisse et soit régi par le droit suisse (art. 25 al. 6 ODEP).

IV. Cas particuliers – hébergement dans un Cloud en Suisse ou dans un Cloud à l'étranger

En l'espèce, l'organe public concerné demeure responsable de ses données et le SITel reste responsable de la sécurité informatique. Il donne les instructions nécessaires au prestataire de services suisse ou étranger. Il veille également à ce que ces dernières soient respectées (Ordonnance du 3 novembre 2015 sur la gestion de l'informatique et des télécommunications dans l'administration cantonale ; RSF 122.96.11). Ainsi, la mise œuvre concrète des mesures organisationnelles et techniques appropriées dépend du type de données, de l'organisation du nuage, de l'étendue des risques et du degré de confidentialité des données.

Dans la mesure où l'externalisation des données touche pratiquement tous les services de l'Etat et qu'elle va être appliquée dans un premier temps à la messagerie, puis aux autres logiciels, nous sommes d'avis qu'un Cloud étatique fribourgeois est nécessaire. Cela permettrait de limiter tous les risques précités et de garder la maîtrise intacte de toutes les données traitées par l'Etat.

A défaut de Cloud fribourgeois, romand ou national, des mesures techniques et organisationnelles strictes doivent être appliquées dans la mesure où l'Etat traite des données sensibles et soumises au secret de fonction/professionnel.

Il est important, avant de mettre des données dans un nuage, de choisir soigneusement le prestataire en procédant notamment à une analyse d'impact, lui donner des instructions précises et le surveiller attentivement. Dans la mesure où l'organe public reste responsable du respect de la protection des données, il répond des infractions en la matière auprès des personnes concernées, de sorte qu'il doit bien choisir les applications et les données qui peuvent être délocalisées dans un nuage et celles qui doivent rester sur ses propres serveurs.

Voici les conditions à respecter :

> le nuage privé est obligatoire ;

> les données doivent être localisées en Suisse ou dans un Etat dont la législation offre un niveau de protection des données élevé ;

> les données soumises au secret de fonction/professionnel ne peuvent pas être externalisées et

doivent être stockées sur un serveur sécurisé de l'Etat ;

> les données sensibles doivent être chiffrées au niveau du transfert et du stockage des données ; la clé de chiffrement doit être auprès de l'organe public, de sorte que le prestataire de services n'a pas accès aux données. En outre, ces données peuvent être hébergées seulement par les prestataires de services soumis exclusivement au droit suisse, détenus en majorité par des propriétaires suisses et fournissant toutes leurs prestations sur le territoire suisse ;

> les conditions d'externalisation doivent être traitées dans un contrat qui doit être validé par l'ATPrD. L'organe public responsable des données doit en outre approuver le contrat d'externalisation. Quant à lui, le SITel ne doit pas signer un contrat-type qu'il est impossible de personnaliser mais doit négocier un contrat pour l'ensemble de l'Etat de Fribourg en y intégrant des clauses particulières en matière de sécurité. Le contrat traite des points suivants : confidentialité ; profilage non autorisé ; finalité ; pas de communication à des tiers ; hébergement et stockage ; portabilité ; durée de conservation et sauvegarde des données originales ; droit d'accès ; contrôles (effectuées par l'ATPrD notamment) ; sécurité des données : antivirus, mises à jour, traçabilité, destruction des données, etc.

> la sous-traitance doit être autorisée par l'organe public qui doit faire valider le contrat y relatif à l'ATPrD.

En outre, nous relevons que le traitement de données proposé par Swisscom n'est pas conforme à la LPrD dans la mesure où la description de services renvoie, à la prestation de Microsoft, selon les conditions de Microsoft, ce qui n'est pas acceptable.

V. Conclusion

En l'absence de base légale relative à l'externalisation du traitement de données des organes publics, la LPrD est applicable.

Dans la mesure où l'Etat traite des données sensibles et soumises au secret de fonction/professionnel, en particulier en ce qui concerne l'hôpital, la prison, la police cantonale, les instances judiciaires, le service cantonal des contributions, etc., un Cloud étatique fribourgeois, romand ou national doit être développé afin de garder la maîtrise totale de toutes les données traitées par l'Etat. Ainsi, les données resteraient en main de l'Etat.

Si le SITel évoque principalement des raisons financières à l'externalisation du traitement des données, le contrôle des mesures techniques et organisationnelles des données externalisées ajouté à l'hébergement des données soumises au secret de fonction et/ou professionnel au sein de l'Etat ne permet pas d'être plus rentable, de sorte qu'un Cloud étatique permettrait de répondre entièrement et à satisfaction aux conditions légales de protection des données. De plus, ce dernier pourrait être mis à disposition des cantons voisins contre rémunération ou développé avec en collaboration des autres cantons.

A défaut de ce Cloud, des mesures techniques et organisationnelles strictes doivent être impérativement appliquées par le SITel et les conditions suivantes respectées :

> le nuage privé est obligatoire ;

> les données doivent être localisées en Suisse ou dans un Etat dont la législation offre un niveau de protection des données élevé ;

- les données soumises au secret de fonction/professionnel ne peuvent pas être externalisées et doivent être stockées sur un serveur sécurisé de l'Etat ;
- les données sensibles doivent être chiffrées au niveau du transfert et du stockage des données ; la clé de chiffrement doit être auprès de l'organe public, de sorte que le prestataire de services n'a pas accès aux données. En outre, ces données peuvent être hébergées seulement par les prestataires de services soumis exclusivement au droit suisse, détenus en majorité par des propriétaires suisses et fournissant toutes leurs prestations sur le territoire suisse ;
- les conditions d'externalisation doivent être traitées dans un contrat qui doit être validé par l'ATPrD. L'organe public responsable des données doit en outre approuver le contrat d'externalisation. Quant à lui, le SITel ne doit pas signer un contrat-type qu'il est impossible de personnaliser mais doit négocier un contrat pour l'ensemble de l'Etat de Fribourg en y intégrant des clauses particulières en matière de sécurité. Le contrat doit traiter des points suivants : confidentialité ; profilage non autorisé ; finalité ; pas de communication à des tiers; hébergement et stockage ; portabilité ; durée de conservation et sauvegarde des données originales ; droit d'accès ; contrôles (effectuées par l'ATPrD notamment) ; sécurité des données : antivirus, mises à jour, traçabilité, destruction des données, etc.
- la sous-traitance doit être autorisée par l'organe public qui doit faire valider le contrat y relatif à l'ATPrD.

Laurent Schneuwly
Président