Check-list
pour contrats de services « cloud »
Version finale

Titre:	Check-list pour contrats de services « cloud »
Statut:	**FINAL**
Version:	2.0
Date de dépôt:	octobre 2015
Dernière révision:	26 février 2016
Auteur:	InterPARES Trust Project
Rédaction:	Jessica Bushey, Marie Demoulin, Elissa How et Robert McLelland
Domaine de recherche:	North American Team – Legal – NA14

La présente check-list pour contrats de services cloud est le fruit de recherches effectuées par l'InterPARES Trust Project sur des contrats de services cloud actuellement en usage, et ce du point de vue de la gestion d'archives, de l'archivistique et du droit. InterPARES Trust (2013-2018) est un projet de recherche plurinational et interdisciplinaire sur des sujets tels que la confiance faite aux archives et aux données numériques dans un environnement en ligne. Pour de plus amples informations veuillez consulter https://interpares.org.

Le public cible de ce document est constitué de gestionnaires d'archives, d'archivistes, de directeurs des systèmes d'information, et d'autres acteurs susceptibles d'utiliser des services cloud pour leur organisation. Le but de ce document est de fournir un outil qui sert à:

- Comprendre les contrats-type pour services cloud;
- Vérifier si des contrats cloud potentiels répondent aux besoins;
- Faire comprendre les besoins en archivage aux départements IT et affaires légales;
- Communiquer les besoins en archivage aux prestataires de services cloud.

Cette check-list est un outil de référence et ne constitue pas un conseil juridique. Nous ne recommandons ou déconseillons aucun prestataire de services cloud en particulier (ou l'usage de services cloud en général). Les personnes et organisations concernées devraient faire appel à un conseiller juridique pour des avis juridiques sur des contrats spécifiques.

Check-list pour contrats de services « cloud » Public cible: Gestionnaires d'archives et archivistes[1]				
Question	**O**	**N**	**?[2]**	**Remarques**
1. Contrat				
▪ La date d'entrée en vigueur du contrat est-elle mentionnée?				
▪ Les circonstances dans lesquelles le service pourrait être suspendu sont-elles expliquées?				
▪ Les circonstances dans lesquelles le service peut être résilié définitivement sont-elles expliquées? (Voir aussi section 8)				
▪ Y a-t-il une note explicative ou la possibilité de souscrire à une notification en cas de changement des conditions du service?[3]				
2. Droits d'auteur et usage des données				
▪ Possédez-vous les droits d'auteur des données que vous conservez, transmettez et/ou créez à l'aide du service cloud?				
▪ Est-ce que le prestataire de service se réserve le droit d'utiliser vos données à des fins opérationnelles et d'amélioration du service?				
▪ Est-ce le prestataire de service se réserve le droit d'utiliser vos données à des fins publicitaires?				
▪ Est-ce que le prestataire de service se réserve le droit d'utiliser vos données ou de les rendre accessibles sous forme de données ouvertes anonymes (via des interfaces de programmes d'application (API))?				

1 Cette check-list est principalement un outil pour aider les organisations à évaluer certains aspects récurrents de contrats-types de *cloud computing*, pour lesquels une organisation doit faire une appréciation des accords légaux proposés par le prestataire de service. La check-list sert également à fournir un aperçu de problèmes d'archivage relatifs aux services de *cloud computing* qui devraient être abordés dans les dispositions du contrat cloud. Il est fortement recommandé à toute organisation qui a recours à des services de *cloud computing*, pour lesquels un contrat spécifique est rédigé, de réviser les dispositions de ce contrat attentivement et de faire appel à tout conseil juridique nécessaire.

2 La colonne « ? » indique qu'un contrat n'est pas suffisamment clair ou que la question posée n'est pas d'application dans votre situation.

3 Certains contrats cloud, surtout ceux concernant des services cloud accessibles publiquement, comprennent des clauses qui permettent au prestataire de changer les dispositions du contrat à tout moment et à leur seule convenance. Une organisation devrait donc veiller à supprimer ce droit si possible, ou rendre chaque modification sujette à l'approbation de l'organisation, ou encore s'assurer que le prestataire de service est obligé d'informer l'organisation en avance de toute modification éventuelle.

▪ Est-ce que le respect des droits d'auteur et d'autres lois relatives à la propriété intellectuelle par le prestataire de service limite le type de contenu que vous pouvez sauvegarder dans le cloud?				
▪ Les stipulations contractuelles du prestataire de service s'appliquent-elles aux métadonnées?[4]				
▪ Devenez-vous propriétaire des métadonnées générées par le système cloud lors du téléchargement (upload et download), de la gestion ou de la migration des données?				
▪ Avez-vous un droit d'accès aux métadonnées pendant la durée d'application du contrat? (Voir aussi section 8)				
3. Accessibilité, récupération et utilisation				
▪ Existe-t-il des indicateurs précis concernant la disponibilité du service?				
▪ Est-ce que le degré d'accessibilité des données répond à vos besoins?				
▪ Est-ce que le degré d'accessibilité des données vous permet de respecter les lois sur le droit à l'information?[5]				
Est-ce que le degré d'accessibilité des données vous permet de respecter le droit des personnes d'avoir accès à leurs données personnelles?[6]				
Est-ce que le degré d'accessibilité des données vous permet de respecter le droit des autorités d'avoir accès à vos données pour des enquêtes, des contrôles ou à des fins judicaires?				
▪ Les procédures, délais et coûts pour la récupération de vos données suite à une interruption de service sont-ils clairement mentionnés?				
4. Stockage et conservation des données				
4.1. Stockage des données				
▪ Le prestataire de service effectue-t-il des copies de sauvegarde des données de votre organisation?				
▪ Le prestataire de service effectue-t-il des copies de sauvegarde des archives externes (par ex. données de clients)				

4 Les métadonnées facilitent la recherche d'archives, leur accessibilité et usage. Elles permettent d'assurer l'authenticité des documents à travers le temps. Elles peuvent être générés par votre organisation ou par le prestataire de service. Il est donc important de mentionner les métadonnées dans le contrat afin de clairement établir tous les aspects concernant le droit d'auteur, l'accès, la rétention, et le droit de disposer des données pendant la durée du contrat et au terme de celui-ci.

5 En général les lois sur le droit à l'information permettent au public d'avoir accès aux informations détenus par le gouvernement national.

6 Certains pays disposent de lois sur la protection de la vie privée par rapport aux informations personnelles des personnes détenues par le secteur public et/ou privé ; ces lois permettent aux personnes concernées d'avoir accès à leurs données personnelles.

	que votre organisation gère éventuellement?				
▪	Les dispositions du contrat conclu avec le prestataire s'appliquent-elles aux copies de sauvegarde?[7]				
▪	Le prestataire prend-il la responsabilité pour la récupération des données en cas de suppression accidentelle?				
4.2. Conservation des données					
▪	Existe-t-il des procédures qui permettent la gestion à long terme de vos données, de manière à assurer qu'elles restent utilisables, fiables, authentiques et intègres?[8]				
▪	Existe-t-il des procédures pour assurer l'intégrité des fichiers pendant le transfert de vos données vers et à partir du cloud (par ex. « checksum »)?				
▪	Existe-t-il une explication du développement futur du service (par ex. migration et/ou émulation)?				
▪	Le système permet-il l'accès à des pistes de vérification des activités liés au développement du service?				
▪	Serez-vous informé par le prestataire d'éventuels changements opérés sur vos données suite au développement du service?				
▪	Pouvez-vous demander à être informé de changements suite au développement du système qui pourraient avoir un impact sur vos données?				
5. Rétention et disponibilité des données					
▪	Etes-vous informé clairement sur la procédure et les conditions de destruction de vos données?[9]				
▪	Vos données (y compris copies simples et copies de sauvegarde) seront-elles détruites selon votre tableau de tri et de gestion?				
▪	Si oui, seront-elles détruites immédiatement et de manière irrévocable, ne permettant plus de récupération, et selon une procédure de destruction fiable qui assure la confidentialité des données jusqu'à leur destruction complète?				
▪	Disposez-vous d'informations sur la nature et				

[7] Concernant les droits d'auteur et d'accès, la sécurité, la rétention et le droit de disposer des données pendant la durée du contrat et au terme de celui-ci.

[8] Le caractère utilisable, fiable, authentique et intègre des données peut être défini dans le contrat (par ex. dans un alinéa « définitions » ou dans un glossaire). Il est recommandé de s'assurer que votre organisation et le prestataire de service ont la même compréhension de ces concepts.

[9] Par ex. : Cette procédure est-elle automatique ou nécessite-t-elle une autorisation? Est-ce que le prestataire propose une option « freeze » pour suspendre temporairement la destruction d'un ensemble de données et/ou de métadonnées contrairement aux directives du tableau de tri? Etes-vous informé de ou pouvez-vous spécifier la méthode de destruction?

le contenu des métadonnées associées qui sont générés par le système cloud?				
▪ Est-ce que le prestataire détruit aussi les métadonnées associées lors de la destruction de vos données?				
▪ Le prestataire donnera-t-il accès et/ou permettra-t-il l'accès à des pistes de vérification du processus de destruction?				
▪ Est-ce que le prestataire fournit une attestation, un rapport ou une déclaration de la destruction des données (si requis en vertu de votre politique de destruction interne ou légale)?				
6. Sécurité, confidentialité et respect de la vie privée				
6.1. Sécurité				
▪ Est-ce que le système est protégé contre l'accès, l'utilisation, la modification ou la destruction non autorisés de vos données?				
▪ Vos données sont-elles protégées lors des transferts vers et à partir du système cloud?				
▪ Le système cloud vous permet-il et offre-il l'accès à des pistes de vérification, aux métadonnées et/ou aux protocoles des accès pour vérifier les mesures de sécurité?				
▪ Serez-vous informé d'éventuelles infractions et violations de la sécurité et de dysfonctionnements du système?				
▪ Le prestataire a-t-il recours aux services d'un sous-traitant?				
▪ Le prestataire fournit-il des informations sur l'identité du sous-traitant et de ses tâches?				
▪ Est-ce que les sous-traitants doivent se conformer au même niveau d'obligations légales que le prestataire de services				
▪ Existe-t-il un plan de rétablissement après sinistre ou est-ce que le contrat prévoit les modalités à respecter en cas de sinistre?				
▪ Est-ce que le prestataire donne des informations sur la manière dont des procédures de rétablissement après sinistre se sont déroulées dans le passé?				
6.2. Confidentialité				
▪ Est-ce que le prestataire a une politique de confidentialité vis-à-vis de ses employés, partenaires et sous-traitants?				
6.3. Respect de la vie privée				

▪ Est-ce que les stipulations contractuelles établies par le prestataire comprennent des politiques de respect de la vie privée, de confidentialité ou de sécurité pour des données sensibles, confidentielles, personnelles ou d'autres types de données spéciales?				

▪ Le contrat mentionne-t-il clairement quelles informations (y compris informations personnelles[10]) sur votre organisation sont collectées, pourquoi elles sont collectés et comment elles sont utilisés par le prestataire?				
▪ Est-ce que le prestataire partage ces informations avec d'autres entreprises, organisations ou personnes sans votre consentement?				
▪ Est-ce que le prestataire mentionne les raisons légales pour lesquelles il partage ces informations avec d'autres entreprises, organisations ou personnes?[11]				
▪ Si le prestataire partage des informations avec ses affiliés pour le traitement des données, cela se passe-t-il conformément à une politique de respect de la vie privée, de la confidentialité et de sécurité ?				
6.4. Accréditation et audit				
▪ Est-ce que le prestataire est accrédité via un programme de certification d'un tiers ?				
▪ Est-ce que le prestataire est soumis à des audits de manière systématique, régulière et indépendante par des tiers afin de démontrer le respect des politiques de sécurité, confidentialité et respect de la vie privée?				
▪ De tels processus de certification ou d'audit sont-ils documentés?				
▪ Avez-vous accès à des informations sur l'identité de l'entité de certification ou d'audit et la date de validité de la certification?				
7. Localisation des données et flux de données transfrontaliers				
7.1. Localisation				
▪ Savez-vous où exactement vos données et copies sont (physiquement) localisés dans le cloud?				

▪ Cette localisation est-elle conforme aux dispositions de localisation qui régissent les données de votre organisation en vertu de la loi en général, et plus particulièrement celle sur le respect de la vie privée?				
▪ Pouvez-vous spécifier l'endroit où vos données et copies sont enregistrées?				
▪ Savez-vous où les métadonnées sont enregistrées et si elles sont enregistrées au même endroit que les données?				

[10] Egalement des informations personnelles sur vos employés, clients, partenaires, prestataires, collaborateurs, etc.
[11] Par ex.: Savez-vous que vos informations peuvent être accessibles aux autorités répressives et aux services de sécurité nationale de différentes juridictions?

7.2. Flux de données transfrontaliers				
▪ Vous informe-t-on de changements éventuels de localisation de vos données qui induisent un changement de juridiction?				
▪ Est-ce que la problématique de possibles injonctions de divulgation par des services de sécurité nationaux ou étrangers portant sur vos données stockées en cloud est-elle abordée?				
▪ Est-ce que le prestataire mentionne clairement la juridiction compétente sous laquelle le contrat est exécuté et devant laquelle d'éventuels différends seront réglés?				
8. Fin de prestation de service – terme du contrat[12]				
▪ Si le prestataire met fin au service, en serez-vous informé?				
▪ Existe-t-il une procédure fixe pour contacter le prestataire au cas où vous voudriez résilier le contrat?				
▪ En cas de résiliation de contrat, vos données seront-elles transférées vers votre organisation ou vers un autre prestataire de votre choix dans un format utilisable et inter-opérationnel?				
▪ Est-ce que le contrat mentionne clairement la procédure, le coût et le délai de retour/transfert de vos données à la fin du contrat?				
▪ Avez-vous le droit d'accéder aux métadonnées générées par le système cloud à la fin de votre contrat?				
▪ Vos données et métadonnées associées seront-elles détruites immédiatement et de manière irrévocable, ne permettant plus de récupération, à la fin du contrat et après avoir confirmé la bonne réception (le retour) de l'entièreté de vos données?				

▪	L'organisation a-t-elle la possibilité de confirmer la destruction de documents et de métadonnées avant la fin du service fourni par le prestataire?				
▪	Le client peut-il mettre fin au contrat sans pénalité si le prestataire de service cloud change?				

[12] La fin de prestation de service est un moment clé du contrat qui doit être détaillé afin de fixer la procédure à suivre, les obligations et les responsabilités des parties contractantes et la destination des données avant la cessation de la relation contractuelle.