

« CONFORMITE CLOUD Editeurs 2017 »

Les recommandations du Conseil supérieur de l'Ordre des experts-comptables

Préambule

Cette liste de recommandations est à destination des fournisseurs de solutions cloud (dénommés les destinataires) pour leur permettre d'affirmer leur engagement sur le respect de la liberté, de l'autonomie, de l'indépendance et de la sécurité des structures d'expertise comptable et de leurs données. Cette première version ne concerne pas les seuls hébergeurs.

Elle est le résultat de la réflexion du groupe de travail de professionnels, membres de la commission innovation technologique, sous la responsabilité du Vice-Président de la commission Michel Bohdanowicz.

Article 1 : Engagements des destinataires

1 Liberté, autonomie, indépendance

1.1 Réversibilité

La réversibilité garantit à l'utilisateur du service la possibilité de changer de prestataire en récupérant ses données.

Aussi les destinataires s'engagent à :

- exporter toutes les données, documents et fichiers de l'expert en format libre ASCII ou selon des standards du marché ;
- permettre cette récupération immédiatement dossier par dossier, a minima ;
- ne pas facturer de supplément pour le téléchargement dossier par dossier ;
- permettre le retour en mode local, pendant les 3 mois suivant une souscription à l'offre cloud, pour les éditeurs proposant les deux modes d'exploitation de leurs solutions (local et cloud) ;
- informer clairement, dès la signature du contrat, de la durée de conservation des données par le prestataire après la fin de celui-ci ;
- informer obligatoirement et clairement dès la signature du contrat sur les services permettant de réexploiter les données après la fin du contrat (notamment en cas de contrôle fiscal).

1.2 Interopérabilité entre les solutions cloud

Le recours à des solutions cloud d'origines différentes nécessite que celles-ci communiquent entre elles au bénéfice de l'expérience-utilisateur.

Aussi les destinataires s'engagent :

- sur l'existence de « web services » ou connecteurs entrants ou sortants avec d'autres solutions éditeurs ; ou sur la possibilité d'importer et d'exporter des données principales et clés de toutes les applications (avec information préalable sur les données concernées) ;
- à informer les experts-comptables sur la politique de licences et de gestion de la compatibilité des versions de l'offre avec les différents logiciels bureautiques ;
- à mettre en œuvre un SSO (single sign on) permettant une navigation sans ré-authentification entre les applications d'un même éditeur et à intégrer les nouvelles offres développées ou acquises dans ce dispositif.

1.3 Durée et nature d'engagement

Le choix d'une solution cloud pour son système d'information porte les mêmes engagements en termes de formation des collaborateurs, d'ingénierie de migration et d'organisation interne qu'une solution en mode local. Le cloud offre cependant de nouvelles perspectives d'usages ponctuels ou dynamiques selon la croissance ou décroissance du cabinet et la nature des clients. Ces éléments doivent être pris en compte dans la durée et la nature des engagements.

Aussi les destinataires s'engagent :

- à ne pas imposer une durée d'abonnement de plus de 24 mois ;
- à rendre adaptables les dispositions contractuelles (options à destination des clients, notamment) relatives à la durée et au nombre de licences ;
- à limiter la durée de la tacite reconduction à 12 mois ;
- à respecter un préavis de 6 mois pour dénoncer le contrat ;
- proposer un processus de recettage permettant de marquer le début du contrat et à chaque évolution majeure de la prestation.

1.4 Accessibilité des données cabinet

Un des atouts du cloud réside dans la disponibilité des données dans le temps et l'espace, traduite par l'acronyme ATAWAD (Anytime, Anywhere, Anydevices).

Aussi les destinataires s'engagent à :

- proposer la solution cloud en mode : ATAW (Anytime, Anywhere) et prévoir dans ses plans de développements d'atteindre le niveau ATAWAD ;
- permettre au cabinet de mémoriser ponctuellement un dossier et le restaurer ultérieurement ;
- donner l'accès aux sauvegardes du fournisseur et à leur historique en précisant les modalités pratiques et juridiques (dossier par dossier, globalement, période de consultation) dans le contrat ;
- informer par avance des périodes d'indisponibilité programmées pour maintenance technique ;
- conserver une traçabilité de la dernière modification réalisée et des accès collaborateurs.

1.5 Accessibilité aux données cabinet par les clients

Le cloud est la base de processus collaboratifs ou d'informations entre le cabinet et ses clients.

Aussi les destinataires s'engagent à :

- s'interdire la consultation ou l'exploitation directe ou indirecte des données des clients du cabinet dans un strict respect du secret professionnel ;
- tenir compte du fait que le cabinet doit pouvoir proposer à son client des accès distincts des droits du cabinet avec des droits différenciés pour les utilisateurs du client ;
- permettre la gestion par le cabinet des périodes consultables par le client ;
- offrir un accès ATAWAD en consultation ;
- fournir une information claire pour le cabinet et son client sur l'origine des informations échangées avec celui-ci. (Le client a-t-il accès à la base de données du cabinet ou à une base dédiée et donc à sa fréquence de mise à jour) ;
- conserver la traçabilité des accès des clients et de leur dernière modification réalisée ;
- permettre un verrouillage de la saisie par le cabinet ;
- fournir un support technique aux utilisateurs ;
- proposer une interface spécifique pour le client en saisie et en restitution (tableaux de bord...).

1.6 Confidentialité et propriété des données

Les enjeux de propriété des données sont plus prégnants dans les solutions cloud.

Aussi les destinataires s'engagent :

- à respecter et faire respecter par leurs collaborateurs et leurs fournisseurs le secret professionnel des experts-comptables ;
- à ne pas facturer directement le client du cabinet pour ses options sans l'accord de l'expert-comptable ;
- à inscrire dans le contrat que la propriété des données est dévolu au cabinet ;
- à ne pas diffuser ni exploiter les données des clients du cabinet.

2 Sécurité

La contrepartie du cloud est une plus grande vulnérabilité aux menaces de pertes et vols des données ou à l'indisponibilité des services. Les paragraphes suivants expriment les dispositifs devant être mis en œuvre par les destinataires pour garantir un minimum de sécurité aux cabinets.

2.1 Cryptage des données

- Les destinataires s'engagent à utiliser un tunnel sécurisé entre le client et les serveurs du prestataire avec un cryptage 128 bits au minimum.

2.2 Sauvegardes des données par le prestataire

Les destinataires s'engagent à :

- fournir une information claire dans le contrat à propos de la politique de sauvegarde et d'historisation ;
- communiquer le taux minimum annuel de disponibilité du service cloud ;
- limiter à 24 heures maximum, après destruction totale du site principal et des éventuels sites « miroirs » (avec une antériorité de 24 heures), le plan de reprise d'activité, éventuellement sur un périmètre fonctionnel réduit ;
- indiquer dans le contrat le montant du plafond d'assurance responsabilité professionnelle ou d'une clause pénale en cas d'indisponibilité du service.

2.3 Sécurité physique des sites

- Les destinataires s'engagent à proposer des data center sécurisés par certification ISO 27001 ou par une déclaration de conformité à un référentiel reconnu de sécurité des datacenters.

2.4 Localisation des données hébergées, responsabilités

Les destinataires s'engagent à :

- ce que les données soient hébergées dans l'Union Européenne ou dans un pays avec qui la France a un accord de coopération fiscale. Cette règle est appliquée au serveur principal et à tous les dispositifs de secours ou secondaires. Elle est maintenue pendant toute la durée du contrat et adaptée selon les changements de la réglementation et des relations entre pays. Le client est informé des évolutions réalisées ;
- ce qu'en cas de litige, seuls les tribunaux français soient compétents et le droit français soit applicable ;
- informer les cabinets de la sous-traitance et d'éventuelles clauses de porte fort.

2.5 Authentification des utilisateurs

Les destinataires s'engagent à mettre en place :

- une authentification avec gestion différenciée des droits d'accès ;
- des procédures de révocation programmée et en cas d'urgence.

3 Garanties et données financières

Les destinataires s'engagent à :

- mentionner dans le contrat les garanties et assurances proposées ;
- publier leurs données financières, notamment leur cotation Banque de France ;
- informer leurs clients en cas changement de contrôle (exclusif ou conjoint) ou d'influence notable (dans le sens de la norme IAS 28) et rendre possible la résiliation du contrat avec respect des délais de préavis prévus ;
- informer de l'existence d'un club utilisateurs d'experts-comptables.

Article 2 : Communication

Les destinataires de la présente liste sont autorisés à apposer sur leurs supports de communication leur engagement de respecter l'ensemble des recommandations du Conseil supérieur de l'ordre des experts-comptables « Conformité cloud » suivi de l'année de validité.

Les destinataires bénéficieront par ailleurs de la promotion de la liste de recommandations « Conformité cloud » assurée par le Conseil supérieur.