



HERVÉ SCHAUER CONSULTANTS  
Cabinet de Consultants en Sécurité Informatique depuis 1989  
Spécialisé sur Unix, Windows, TCP/IP et Internet



Openday 23 juin 2011

# Les clauses sécurité dans un contrat de cloud

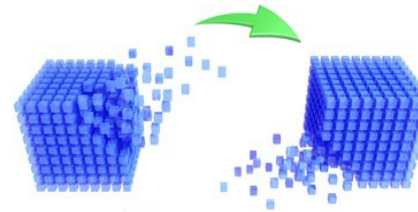
**Frédéric Connes**

<Frederic.Connes@hsc.fr>

- Société de conseil en sécurité des systèmes d'information depuis 1989
- Prestations intellectuelles d'expertise en toute indépendance
  - Pas de distribution, ni intégration, ni infogérance, ni investisseurs, ni délégation de personnel
- Prestations : conseil, études, audits, tests d'intrusion, formations
- Domaines d'expertise
  - Sécurité technique
  - Sécurité organisationnelle
  - Sécurité juridique (qualification OPQCM)

- Envoi des données
- Obligations du client
- Prérrogatives du prestataire
- Données à caractère personnel
- Obligations de sécurité
- Confidentialité
- Convention de service attendu
- Audits de sécurité
- Réversibilité
- Résiliation
- Effacement des données

- Du client vers le prestataire
- Le prestataire
  - doit garantir l'intégrité et la confidentialité des données et des applications
  - dès leur réception dans son système d'information (avant la bascule)
- Moyens techniques
  - A préciser par le prestataire, mais non limitatifs
  - Exemple : sauvegardes immédiates des données du client
- Garantir la continuité avec le système antérieur
  - Lors de la bascule
  - Notamment au niveau des mesures de sécurité mises en place



- Respecter les dispositions légales et réglementaires en vigueur
  - Intrusion dans un système informatique, *spamming*, *phishing*...
  - Propriété intellectuelle, vie privée, infractions de presse...
- Garantir la confidentialité des mots de passe attribués
- Agir promptement en cas de notification
  - Responsabilité pénale en tant qu'hébergeur si en a la qualité
  - Possibilité pour le prestataire de se substituer au client
- Agir promptement en cas d'attaque (déni de service...)
  - Notamment : avertir le prestataire
- Sanctions
  - Suspension, suppression du service, avec ou sans préavis

- Intervenir sur les données ou les applications du client
  - En cas d'attaque ou de dysfonctionnement
  - En cas de problème légal
  - A l'occasion d'une maintenance ?
- Si le client ne peut pas agir lui-même
  - Urgence, client ne répond pas
  - Client n'a pas la compétence technique pour intervenir
- Selon quelles modalités ?
  - Conditions à remplir pour accéder aux données et applications
  - Indemnisation éventuelle du client en cas de dysfonctionnement consécutif à l'intervention ?



- Préciser qui est responsable du traitement
  - Le cas échéant, envisager d'avoir des co-responsables
  - Préciser les sous-traitants
- Déterminer la loi applicable
  - Préciser le lieu d'établissement et la localisation des moyens de traitement
- Prévoir les éventuels transferts de données hors UE
  - Donc : savoir avec précision où sont et où vont les données
- Reprendre les obligations du responsable du traitement
  - Formalités préalables, information, droit d'accès...

- A la charge du responsable de traitement
- Obligations de moyens
  - Loi informatique et libertés, art. 34 et 35
  - Difficile d'imposer des obligations de résultat
    - Le coût risquerait d'être prohibitif
  - Mais prévoir des obligations de moyens renforcées
    - Par des clauses spécifiques à la sécurité
    - Précisant les moyens devant être mis en œuvre contractuellement
    - Mettre « tous les moyens en œuvre pour garantir la sécurité »
- Apporter tout le soin et la diligence nécessaires à la fourniture d'un service conforme aux usages de la profession et à l'état de l'art



- Possibilité pour le personnel du prestataire d'intervenir sur les machines ou les données du client
  - Avec ou sans son accord
  - Conditions d'accès aux données
  - Personnes soumises à l'obligation de confidentialité
- Durée d'application de la clause
  - Pendant toute la durée du contrat
  - Combien de temps après la fin du contrat ?
- Quels contrôles sont réalisés par le prestataire ?
  - Sur l'information des personnels
  - Sur le respect des obligations de confidentialité



- *Service Level Agreement (SLA)*
- Taux global de disponibilité
  - En heures ouvrées/non ouvrées
  - Durée cumulée des indisponibilités
  - Nombre maximum d'indisponibilités
  - Période retenue (jour, semaine, mois, trimestre, année...)
  - GTI, GTR
- Exclusions
  - Force majeure
  - Maintenances et interventions programmées ?
    - Prévoir le délai de prévenance permettant l'exclusion
- Indemnisation prévue



- Possibilité de faire des audits de sécurité
  - Dépend du rapport de force entre le client et le prestataire
  - Le client qui ne fait pas d'audits prend des risques
    - Il doit faire entièrement confiance au prestataire
    - Sa direction doit être informée des risques pris
- Définition du périmètre de l'audit et détermination de la périodicité
- Délai de prévenance
  - Possibilité de le réduire en cas d'urgence
  - Audits périodiques
- Modalités de l'audit (tests d'intrusion...)



- Permettre au client de reprendre possession des données
  - A tout moment, sans justification
- Délai de prévenance à prévoir
- Obligations du prestataire
  - Apporter l'assistance nécessaire pour faciliter le transfert des données et des moyens de sécurité matériels et logiciels vers le client ou tout autre prestataire
  - Garantir le service attendu et la sécurité des données et des applications pendant le transfert
  - Assurer la prestation de service jusqu'au terme du contrat



- Prévoir les motifs de résiliation du contrat
- Manquement grave du prestataire à l'une des obligations de sécurité mises à sa charge par le contrat
  - Disponibilité, confidentialité, intégrité
  - Liste non exhaustive des manquements graves
  - Mise en demeure du client de mettre fin au manquement
    - Prévoir le délai
  - Si le manquement n'est pas réparé dans le délai, le client peut résilier le contrat de plein droit
    - Avec ou sans préavis
- Prévoir aussi des pénalités



- Prévoir

- Lors de la résiliation
- En cours de contrat
  - A l'expiration d'un délai
  - A la demande du client



- Problèmes

- L'effacement physique est rarement complet (aucunes garanties)
  - Sauf à utiliser des outils spécifiques (passes multiples)
- Il est difficile d'effacer dans
  - Les architectures redondantes (combien de copies ? localisation ?)
  - Les sauvegardes (nombre ? localisation ?)
  - Les archives (où sont les données ? En reste-t-il ailleurs ?)

- Le contrat est fondamental pour la sécurité juridique
  - Il doit être adapté aux parties et donc être rédigé sur mesure
  - Il doit intégrer des clauses sécurité détaillées
- Ne pas faire confiance aux exemples de clauses que l'on trouve sur Internet
  - Idéalement, faire appel à un juriste pour rédiger les clauses
- Réviser périodiquement les clauses sécurité du contrat en fonction
  - De l'évolution de la relation contractuelle
  - De l'évolution des techniques et de l'état de l'art en matière de cloud