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

Les clauses « sécurité » d'un contrat SaaS

Paris, 21 janvier 2011

Frédéric Connes
Hervé Schauer
<Frederic.Connes@hsc.fr>
<Herve.Schauer@hsc.fr>

Sommaire

- Données personnelles
- Obligation de sécurité
- Envoi des données
- Confidentialité
- Localisation des données
- Convention de service attendu
- Réversibilité
- Audit de sécurité
- Résiliation
- Conclusion

Données personnelles

- SaaS : très souvent traitement de données personnelles
- Application de la loi du 6 janvier 1978
  - « Informatique et libertés »

- Personne responsable pénalement : responsable du traitement
  - Personne qui détermine les finalités et les moyens du traitement
  - Dans un contrat SaaS : prestataire
  - Risque pénal
    - 5 ans d'emprisonnement
    - 300 000 euros d'amende x 5 = 1,5 million d'euros
- Vérifier que le prestataire respecte ses obligations découlant de la loi de 1978

Données personnelles

- Obligations du responsable du traitement
  - Accomplir les formalités préalables (déclaration, autorisation)
  - Garantir la licéité de la collecte et du traitement
  - Informer les personnes concernées
  - Respecter la finalité du traitement
  - Garantir l'exactitude et la complétude des données
  - **Garantir la sécurité du traitement**
  - Communiquer les informations sur le traitement
  - Respecter la durée de conservation des données
  - Informer la CNIL en cas de suppression du traitement

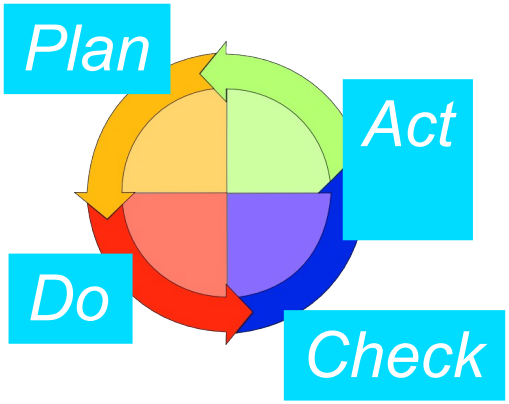
Obligation de sécurité

- A la charge du prestataire
- Loi informatique et libertés, article 34
  - Obligation de moyens
  - Renforcer la sécurité
    - Par des clauses spécifiques
    - 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

Obligation de sécurité

- Possibilité d'exiger contractuellement du prestataire qu'il soit certifié
  - Certification ISO 27001
    - SMSI
    - Périmètre
    - Organisme de certification
  - Label SAS 70 type II
    - AICPA, *Statement on Auditing Standards*
    - Audit de durée variable par plusieurs auditeurs
    - Vérification de l'efficacité des mesures de sécurité



- Possibilité d'exiger une expérience ou des certifications individuelles des personnels du prestataire les plus sensibles

Obligation de sécurité

- Le prestataire prend la responsabilité du maintien en conditions de sécurité pendant toute la durée du contrat
  - Mettre en œuvre des mécanismes de sécurité conformes à l'état de l'art
- Sur la sécurité et la mise à l'état de l'art
  - Conseil
  - Mise en garde
  - Recommandation

- Informer le client des risques de chaque opération envisagée par le prestataire
  - Incidents potentiels
  - Mise en œuvre d'actions de prévention ou correctives

Obligation de sécurité

- Responsable du traitement : peut faire appel à un sous-traitant
  - Critère : reçoit des instructions du responsable du traitement

- Vérifier si le responsable fait appel à la sous-traitance
  - Déclarer l'existence de sous-traitants du prestataire
    - Préciser la nature des relations entre eux
    - Préciser les conséquences en termes de responsabilité
  - Il doit exister un contrat entre le responsable et le sous-traitant précisant les obligations du sous-traitant en matière de sécurité (article 35 de la loi informatique et libertés)

Envoi des données

- Du client vers le prestataire
- Le prestataire
  - Doit garantir l'intégrité, la confidentialité et la disponibilité des données et des applications
  - Dès leur réception dans son système d'information
  - Le cas échéant, prévoir les autres obligations du prestataire pendant la période transitoire
- Moyens techniques
  - A préciser par le prestataire, mais non limitatifs
  - Exemple : sauvegardes immédiates des données du client

Confidentialité

- Nature des informations couvertes par la clause de confidentialité
  - Données hébergées
  - Autres informations sensibles (mots de passe...)
- Personnels soumis à l'obligation de confidentialité
  - Détailler les fonctions concernées
- Durée d'application de la clause
  - Pendant toute la durée du contrat
  - Après la fin du contrat ?

Confidentialité

- Possibilité pour le personnel du prestataire d'intervenir sur les données ou la configuration du client ?
  - Avec ou sans son accord ?
  - En cas d'attaque ou de dysfonctionnement
  - En cas de réquisition judiciaire
  - A l'occasion d'une maintenance
  - Lecture pour des motifs commerciaux (publicité ciblée...)
  - Autres cas ?

- Selon quelles modalités ?
  - Conditions à remplir pour accéder aux données
  - Indemnisation éventuelle du client en cas de dysfonctionnement consécutif à une intervention ?

Localisation des données

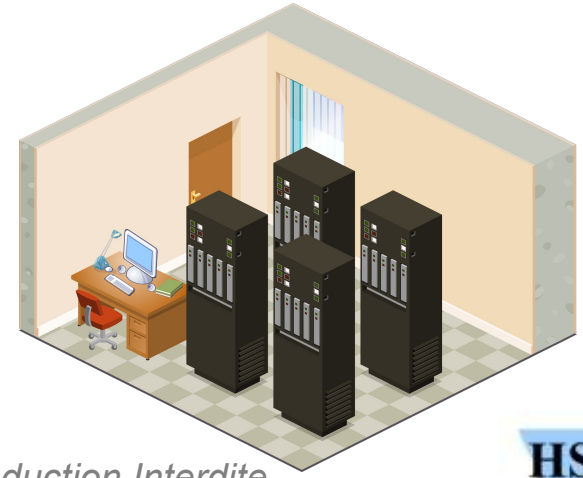
- Des transferts hors Union européenne sont-ils prévus ?
  - Régime particulier de la loi informatique et libertés
  - Interdits par principe

- L'État destinataire doit assurer un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux, ou :
  - Consentement de la personne concernée
  - Décision de la CNIL
  - Diverses exceptions
- Toujours s'assurer que les éventuels transferts de données hors Union européenne sont licites

Localisation des données

- Obligations du prestataire
  - Communiquer la liste de tous les lieux de stockage
    - Y compris les sites de secours
    - Important si l'architecture est distribuée
  - Être en mesure de localiser le lieu de stockage d'une donnée
    - Si pas en permanence, au moins *a posteriori* après un incident

- Possibilité de prévoir un accès aux locaux du prestataire par le client
  - A tout moment ou sur rendez-vous



Convention de service attendu

- *Service Level Agreement* (SLA)
- Taux global de disponibilité (en heures ouvrées/non ouvrées)
  - Durée et nombre maximum des indisponibilités avec la période retenue (jour, semaine, mois, trimestre, année...)
  - Force majeure
- Maintenances
  - Informer le client avant toute opération entraînant une indisponibilité ou une dégradation des performances
  - Délai de prévenance
  - Entrent dans le temps d'indisponibilité ?

- Temps maximal de réalisation de certaines opérations

Convention de service attendu

- Garanties liées à l'intégrité des données
  - Moyens techniques mis en œuvre (RAID, système de fichiers distribué...)
  - Périmètre des sauvegardes, durée de conservation
  - Temps garanti de restauration à partir des sauvegardes en cas de défaillance
- Indemnisation prévue (pénalités)
  - Par exemple en jours non facturés
  - Limite (sur le mois, le trimestre, l'année)
  - Exclusions (fait d'un intermédiaire sur Internet...)
- Conditions de révision de la convention de service

Réversibilité

- Permettre au client de reprendre possession des données
  - A tout moment, sans justification
  - Mais délai de prévenance à prévoir
- Prévoir la durée de la transition à partir de son déclenchement
- 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

Audits de sécurité

- Pour du SaaS spécifique
- Définition du périmètre de l'audit et détermination de la périodicité
- Délai de prévenance
  - Possibilité de le réduire en cas d'urgence

- Possibilité pour le client de contrôler à tout moment le respect des exigences de sécurité
  - Dispositions prises pour assurer la sécurité
  - Attaques constatées et arrêtées
- Possibilité pour le client de déléguer l'audit à un tiers de son choix
- Modalités de l'audit (visites, entrevues, accès aux machines)

Résiliation

- 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

Conclusion

- Points liés à la sécurité nombreux
  - Se protéger grâce au contrat
  - Couvrir toute la vie du SaaS
- Législation est un atout
  - Importance de la loi de 1978
- Implication du RSSI indispensable
  - Voir aussi avec le service juridique

Questions ?

www.hsc.fr