Le Cloud computing et les données à caractère personnel

Club EBIOS, Paris, 11 décembre 2012

Amandine JAMBERT, Ingénieur expert au Service de l'expertise

Le Cloud et la Loi Informatique et Libertés

Sujet	Loi I&L	Cloud
Contrôle et sécurité	*"Les données à caractère personnel ne peuvent faire l'objet d'un **traitement** de la part d'un sous-traitant que **sur instruction** du responsable du traitement."*	Prestataire: *"Nous nous occupons de tout"*
Responsabilité du traitement	*"'**Le responsable** d'un traitement de données à caractère personnel **est l'organisme qui détermine ses finalités et ses moyens**."*	Prestataire: *"Nous nous occupons de tout et nous ne sommes responsables de rien"*
Localisation	Le **transfert hors UE** et pays adéquat est **interdit** par défaut, peut être autorisé SI les garanties sont suffisantes. Les personnes doivent **être informées des pays** dans lesquels les données sont traitées.	Prestataire: *"Nous nous occupons de tout mais nous ne pouvons pas garantir la localisation des données"*
Durée de conservation	"[Les données] *sont conservées pendant une durée qui n'excède pas la **durée nécessaire aux finalités** pour lesquelles elles sont collectées et traitées"*	Les politiques de suppression des données sont définies indépendamment du client et du traitement

La CNIL face au Cloud computing

- **Historique**
  - ✓Entretiens et première communication à la Commission
  - ✓Consultation publique
  - ✓Synthèse de la consultation et recommandations
  - ✓Présentation et publication de nos recommandations

- **Actions entreprises en parallèle par la CNIL**
  - ✓Contribution à l'Avis WP196 du G29
  - ✓Participation à des groupes de travail (CSA, ISO 27017/27018, etc.)

- **Principaux enjeux du Cloud en termes Informatique et Libertés**
  - ✓Juridiques
  - ✓En matière de sécurité

- **Objectifs des recommandations de la CNIL**
  - Aider les entreprises clientes de services de Cloud computing, notamment les PME, à faire les bons choix au regard de la loi Informatique et Libertés
  - Fournir des pistes de réflexion
  - Proposer des outils pratiques (modèles de Clauses / méthode)

Les recommandations de la CNIL : 7 étapes clés

1. **Cartographie** des données et des traitements
2. Définition des **exigences de sécurité technique et juridique**
3. **Analyse de risques***
4. **Choix des modèles** de services et de déploiement pertinents
5. Choix d'un prestataire présentant des **garanties suffisantes***
6. **Révision** de la politique de sécurité interne
7. **Surveillance** des évolutions

Etape 3 : Analyse de risques

- SSI et protection de la vie privée :
  - Protéger l'organisme VS Protéger les personnes concernées

- Méthode de Gestion des risques Vie Privée
  - Considérer les données à caractère personnel ;
  - Considérer les processus légaux ;
  - Ajouter les impacts sur la vie privée des personnes concernées ;
  - Déterminer des mesures respectueuses de la vie privée.

➢ Pour les Responsables de Traitement

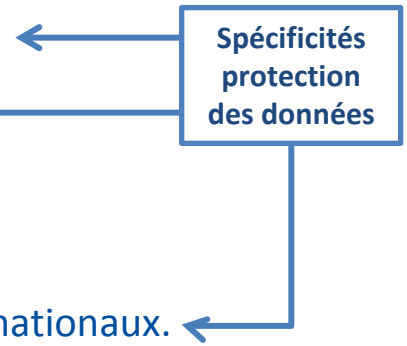
➢ Pour les sous-traitants

Etape 3 : Analyse de risques

35 risques ENISA : http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

CNIL : 10 en particulier

- **perte de gouvernance** sur le traitement ;
- **dépendance technologique**
- faille dans **l'isolation des données** (système virtualisé)
- **réquisitions judiciaires**, notamment par des autorités étrangères ;
- faille dans la **chaîne de sous-traitance** ;
- **destruction** ineffective ou non sécurisée des données ;
- insuffisance de moyens de **gestion des droits d'accès** ;
- **indisponibilité du service** du prestataire ;
- **fermeture du service** du prestataire ou acquisition par un tiers ;
- **non-conformité réglementaire**, notamment sur les transferts internationaux.



Etape 5 : Choix d'un prestataire présentant des **garanties suffisantes**

- **Déterminer la qualification juridique du prestataire:**
  - Le client seul responsable OU responsabilité conjointe
  - Répartition différente de la responsabilité

- **Analyse factuelle (pour SaaS et PaaS public) :**
  - Faible niveau d'instructions
  - Absence de pouvoirs de contrôle
  - Offres standardisées
  - Contrats d'adhésion

➢ **SaaS et PaaS public : Responsabilité conjointe (généralement)**

Etape 5 : Choix d'un prestataire présentant des **garanties suffisantes**

- Des **garanties juridiques** :
  - Conformité à la loi I&L
  - Sous-traitants (nouveau règlement : responsabilité du sous-traitant ?)
  - Transferts (diapo suivante)

- Avoir les **moyens de faire l'analyse de risque** :
  - Accès à la **politique de sécurité** ;
  - Mesures de sécurité et sûreté physique sur **le site d'hébergement** ;
  - Mesures assurant la disponibilité, l'intégrité et la confidentialité des données ;
  - Système de **remontée des plaintes** et des failles de sécurité ;
  - **Réversibilité/portabilité** (nouveau règlement : futur droit à l'interopérabilité ?);
  - **Traçabilité** et information de toute anomalie détectée ;
  - Engagement de niveaux de services (« **Service Level Agreements** »)
- ➢ Certifications (ex : 27001)
- ➢ Engagements « vie privée » (ex : clauses, « Privacy Level Agreement » du CSA)

- Avoir la possibilité de **faire des audits** (si sous-traitant).

Etape 5 : Choix d'un prestataire présentant des **garanties suffisantes**

- Information sur la **localisation** des centres de données
- Encadrement des transferts :
  - Adéquation : les pays avec une protection des données satisfaisantes
  - Les **BCR « sous-traitants »**, un outil adapté au Cloud
  - Les clauses contractuelles types de la CE
  - Safe Harbor (…)
  - Autorisation de la CNIL
- Information immédiate en cas de demande **d'accès par des autorités étrangères**

Etape 5 : Choix d'un prestataire présentant des **garanties suffisantes**

- Modèles de clauses :
  - ce ne sont que des modèles !

- *Mais conserver le principe, page 11 :*

  « les prestataires qui n'offrent pas ces garanties essentielles dans leurs contrats et qui refusent toute négociation avec leurs clients potentiels ne devraient pas être sélectionnés. »

Conclusion

- Les **besoins du client** doivent constituer la base du processus :
  - Passer au Cloud ne doit pas être un acte de foi
  - Rationaliser autant que possible

- C'est possible d'être conforme !
  - Services européens
  - Les géants américains évoluent (Google Apps for Government, Office 365 de Microsoft)

Merci de votre attention!