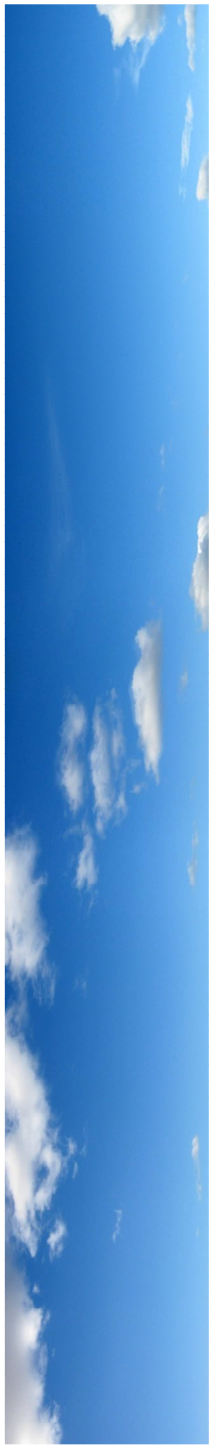
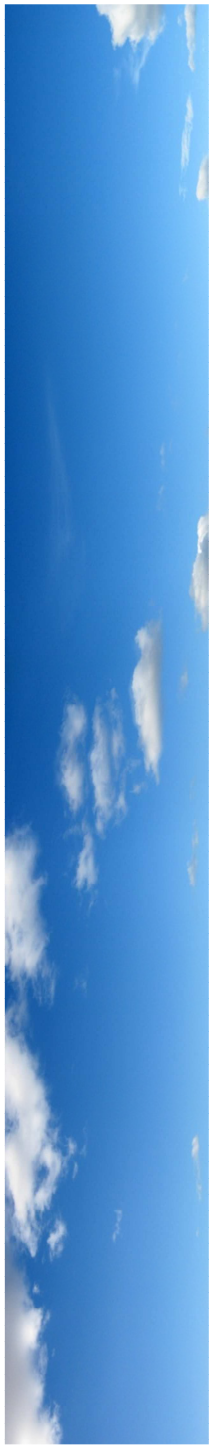


Recommandations sur le Cloud computing

EuroCloud, Paris, 25 septembre 2012

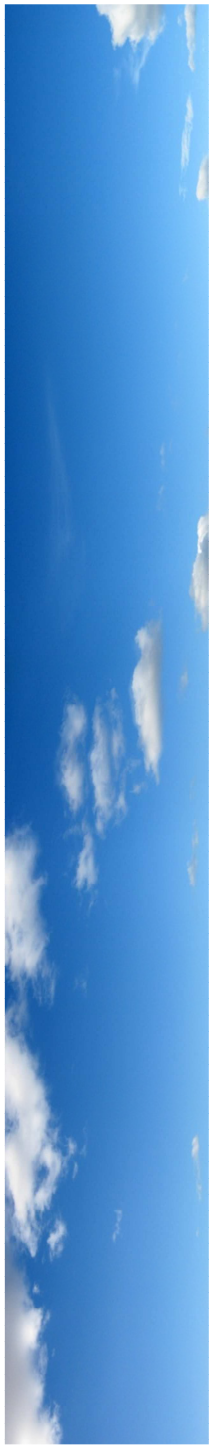
Didier GASSE, membre de la Commission nationale de l'informatique et des libertés
Myriam GUFFLET, Juriste au Service des affaires européennes et internationales
Amandine JAMBERT, Ingénieur expert au Service de l'expertise



La CNIL face au Cloud computing

- **Historique**
  - ✓Les précédents
  - ✓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 l'élaboration de nouvelles normes (27017/27018)
  - ✓Participation aux groupes de travail du *Cloud Security Alli*ance



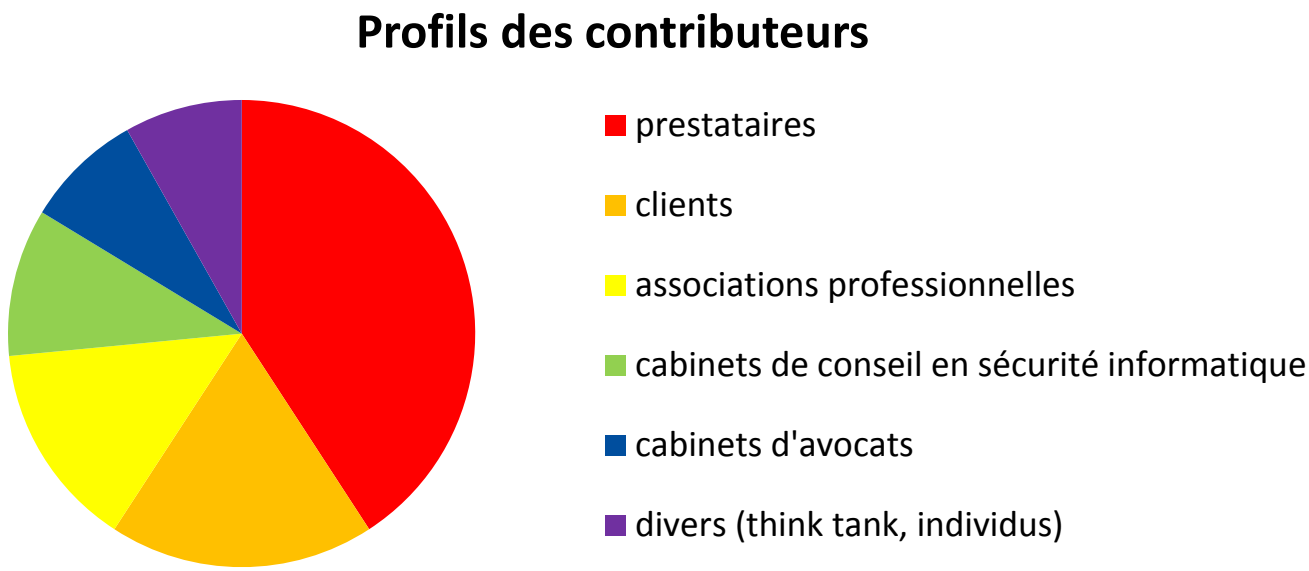
Enjeux et objectifs

- **Principaux enjeux du Cloud en termes informatique et liberté**
  - ✓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

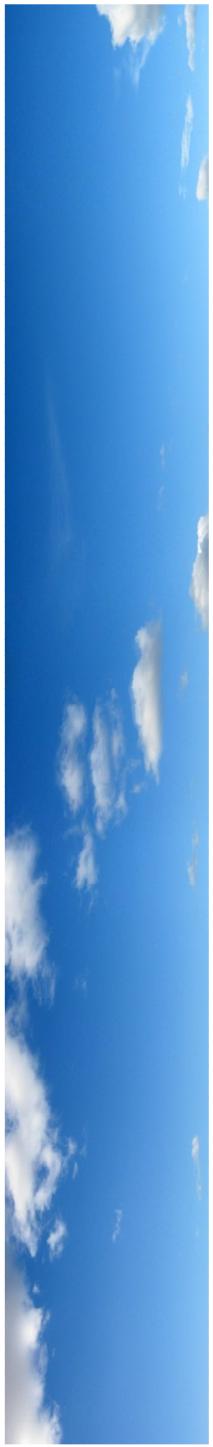
Résultats de la consultation publique

49 contributions



Points confirmés: définition du Cloud, droit applicable et encadrement des transferts

Points plus complexes: qualification du prestataire, sécurité du Cloud



Les 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

Déterminer la qualification du prestataire

- **Analyse factuelle :**
  - ✓ Faible niveau d'instructions
  - ✓ Absence de pouvoirs de contrôle
  - ✓ Offres standardisées
  - ✓ Contrats d'adhésion
- En cas de responsabilité conjointe: nécessaire partage des **responsabilités** entre les parties

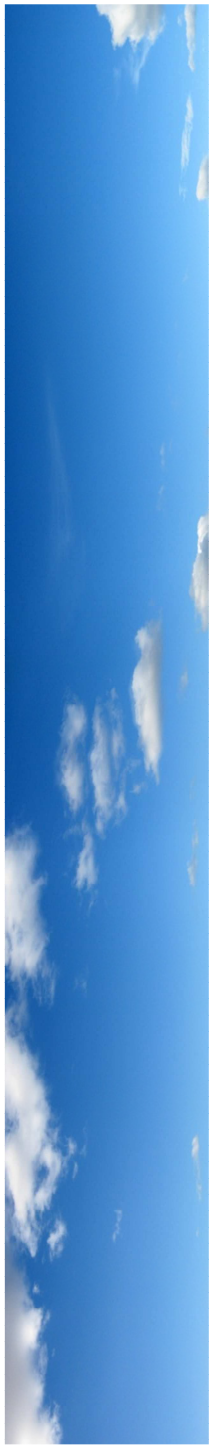
Sécurité : Principe de l'Analyse de risques

- SSI et protection de la vie privée n'ont pas le même objectif, une analyse des risques SSI ne permettra pas de répondre à toutes les questions relatives à la protection de la vie privée
  - Elle ne permettra pas d'étudier les impacts sur la vie privée et leur gravité.
  - Elle sera néanmoins utile à la réflexion sur les menaces et donnera une idée de la robustesse du dispositif.

- Méthode de Gestion des risques Vie Privée
  - Considérer les données à caractère personnel et 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

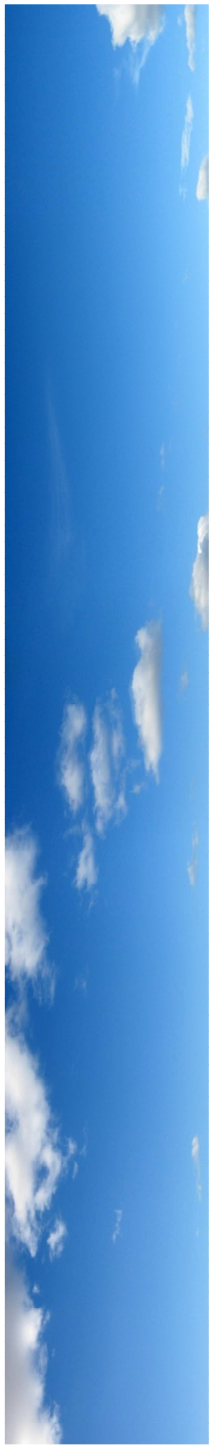
  ➢ Pour les sous-traitants



Sécurité : Coopération du prestataire

- Donner les moyens au client d'effectuer son 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 (futur droit à l'interopérabilité) ;
  - Traçabilité et information de toute anomalie détectée ;
  - Engagement de niveaux de services (« *Service Level Agreements* »)
  - ➢ Certifications (ex : 27001)
  - ➢ Engagement « vie privée » (ex : clauses, « *Privacy Level Agreement* » du CSA)

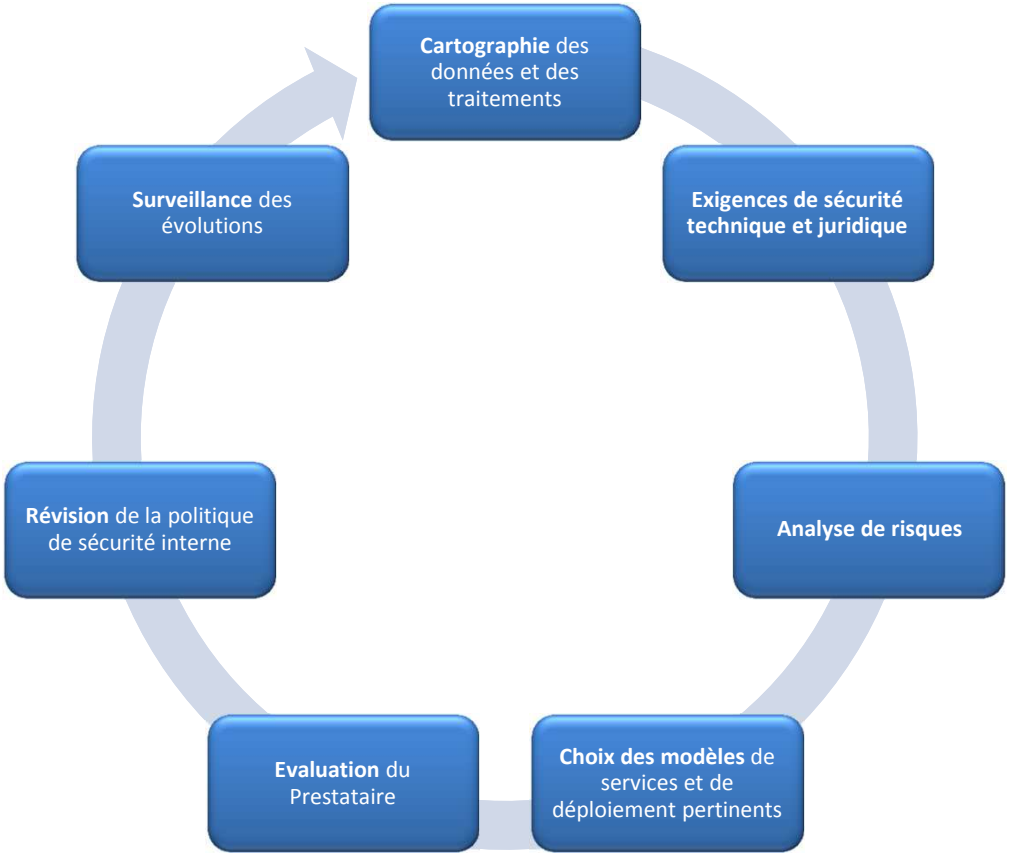
- Lorsque le prestataire est sous-traitant, le client doit pouvoir procéder (ou faire procéder) à des audits.

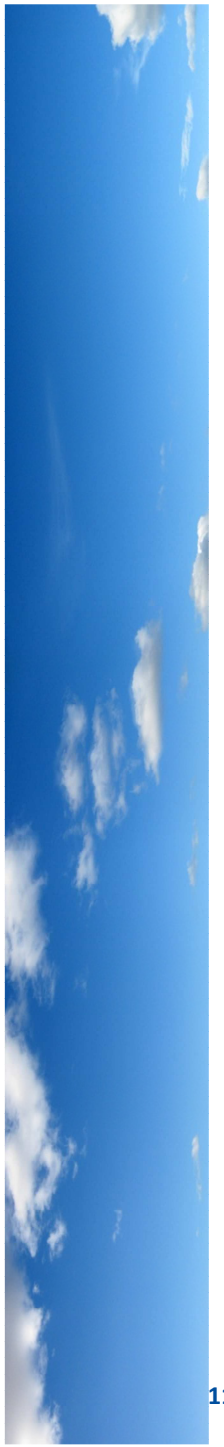


Encadrer les transferts de données hors EEE

- Information sur la **localisation** des centres de données
- Encadrement des transferts : les **BCR « sous-traitants »**, un outil adapté au Cloud
- Information en cas de demande d'**accès par des autorités étrangères**

Conclusion


Cartographie des données et des traitements
Exigences de sécurité technique et juridique
Analyse de risques
Choix des modèles de services et de déploiement pertinents
Evaluation du Prestataire
Révision de la politique de sécurité interne
Surveillance des évolutions



Merci de votre attention!