CLUSIF

CLUSIR Rhône Alpes

Sécurité du Cloud

Cloud et conformité RGPD

Aurélie DUSONCHET

Consultante sécurité informatique / RGPD

SOMMAIRE

- Constats généraux sur les offres cloud
- Grands principes de mise en œuvre
- 7 recommandations de la CNIL
  - ✓ Identifier les données
  - ✓ Définir ses propres exigences de sécurité
  - ✓ Conduire une analyse de risques
  - ✓ Sélectionner le type de cloud pertinent
  - ✓ Choisir un prestataire avec des garanties
  - ✓ Revoir la politique de sécurité interne
  - ✓ Surveiller l'évolution dans le temps
- Ressources

Constats généraux

- Beaucoup d'offres standardisées = pas de négociation
- Manque de transparence
  - ✓ conditions de réalisation
  - ✓ transfert à l'étranger ? où ?
- Quelle sécurité « technique » ?
  - ✓ souvent supérieure à celle mise en œuvre en PME (CNIL)
  - ✓ mais quid de la pérennité des données ?
  - ✓ au prix de quelle perte de contrôle ?
- Quel respect de la législation relative à la protection des données personnelles ?

Grands principes de mise en œuvre

- Analyse de risques formelle
  - ✓ Attention ! un risque peut être remplacé par un autre… (ex. sécurité technique vs pérennité des données)
- Analyse des garanties offertes
  - ✓ droits des personnes
  - ✓ encadrement des transferts
  - ✓ sécurité des données
- Choix du prestataire
  - ✓ comparaison économique / technique / juridique

➔ 7 recommandations

1. Identifier clairement les données / traitements passant dans le cloud

- Pour chaque traitement, identifier les données passant dans le cloud :
  - ✓ données à caractère personnel
  - ✓ données sensibles au sens RGPD
  - ✓ données stratégiques
  - ✓ données utilisées par des applications métiers
- Pour chaque type de donnée, contrôler :
  - ✓ si réglementation spécifique
  - ✓ conditions minimales de transfert (ex. données de santé → HDS agréé)

2. Définir ses propres exigences de sécurité

- Sécurité technique ET juridique
- Nombreuses offres cloud « standard » = adaptées ?
- S'assurer que le niveau d'exigence minimal est atteint
- Prendre en compte dans les exigences les contraintes :
  - ✓ légales (localisation, garantie de sécurité, réglementations…)
  - ✓ pratiques (disponibilité, réversibilité, portabilité…)
  - ✓ techniques (interopérabilité)
- Evaluer les offres envisagées au regard de ces exigences

3. Conduire une analyse de risques

- Identifier les principaux risques de chaque usage cloud
  - ✓ Biens à protéger = données à caractère personnel
  - ✓ Impacts = pour l'entreprise **mais aussi** sur la vie privée des personnes

➔ Identifier les mesures de sécurité essentielles à mettre en œuvre

- Possible de s'appuyer sur
  - ✓ liste des 10 principaux risques identifiés par la CNIL
  - ✓ liste de ENISA : 35 risques

10 risques identifiés par la CNIL

Et leurs principaux impacts sur les critères de sécurité...

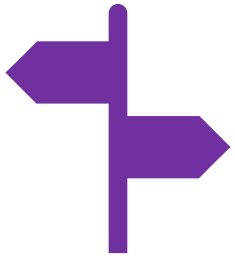
1. perte de gouvernance sur le traitement
2. dépendance technologique (changement de solution) [D]
3. faille dans l'isolation des données [I] [C]
4. réquisitions judiciaires (autorités étrangères...) [C]
5. faille dans la chaîne de sous-traitance [D] [I] [C] [P]
6. destruction ineffective / non-sécurisée, conservation trop longue
7. gestion des droits d'accès insuffisamment robuste [C] [I]
8. indisponibilité du service (et des moyens d'accès) [D]
9. fermeture du service ou acquisition tierce [D]
10. non-conformité réglementaire (cf. transfert internationaux)

Objectif : réduire les risques par :

- dispositions contractuelles
- mesures techniques prestataire et client
- mesures organisationnelles prestataire et client

4. Sélectionner le type de cloud pertinent

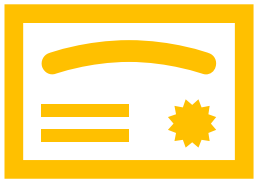
- SaaS / PaaS / IaaS
- Public / privé / hybride
- Sélectionner le type de cloud approprié **par traitement**
  - ✓ ex. IaaS français pour le site web, HDS pour données santé, SaaS européen privé pour la messagerie…
- Effectuer une migration cloud progressive, par traitement ou type de données par criticité croissante



5. Choisir un prestataire avec des garanties

- Garanties suffisantes en termes de :
  - ✓ mesures de sécurité / confidentialité
  - ✓ transparence sur les moyens employés

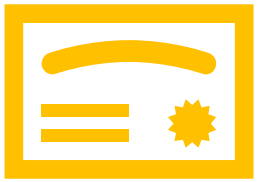
- Grille d'analyse en 2 parties
  1. Qualification juridique du prestataire ? (RT/ST)
  2. Evaluation du niveau de protection assuré par le prestataire



Qualification juridique

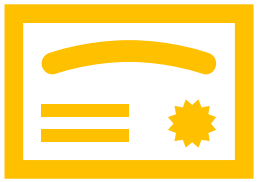
- Responsable de Traitement vs Sous-traitant
- selon le degré d'influence, d'autorité, de contrôle du client (contrats standards sans marge de négociation)
  → RT conjoint ?
- partage de responsabilités ? définir clairement les responsabilités de chaque partie

Hypothèse	Formalités déclaratives	Information des personnes	Obligation de confidentialité et sécurité	Exercice des droits des personnes concernées auprès du …
Le prestataire est conjointement responsable du traitement	Client[5]	Client[6]	Client + Prestataire	Client (avec le concours du prestataire)[7]



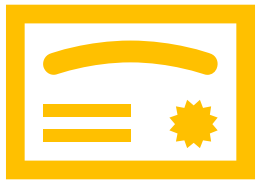
Evaluation du niveau de protection assuré

- responsabilité du choix du prestataire = client !
- liste des éléments essentiels devant figurer sur un contrat de service Cloud
- si garanties non offertes ou refus de négociation → risque élevé de non-conformité = éliminer le prestataire !



Eléments devant figurer dans un contrat

- **Informations relatives aux traitements**
  (respect des principes européens, moyens de traitement…)
- **Garanties mises en œuvre**
  (durée de conservation, modalités de restitutions…)
- **Localisation et transferts**
  (pays d'hébergement, modalités de transfert)
- **Formalités auprès de la CNIL**
  (facilitation des démarches, transmission d'infos…)
- **Sécurité et confidentialité**
  (politique de sécurité, certifications, traçabilité…)



➔ *cf. modèles de clauses en annexe du document CNIL*

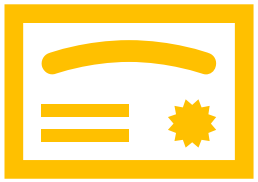
Exemple de modèle de clause

- **Continuité de service, sauvegardes et intégrité**

[Le modèle de clause suivant peut être utilisé que le prestataire soit sous-traitant ou responsable conjoint du traitement]

« Le Prestataire s'engage à prendre les mesures nécessaires pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du Contrat.

Il s'engage à utiliser un système de sauvegarde des Données et de continuité de service dont le détail est fourni dans l'accord de niveau de service annexé au Contrat. »

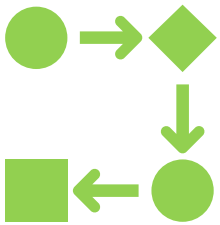


6. Revoir la politique de sécurité interne

- Cloud = changements profonds des modes opératoires

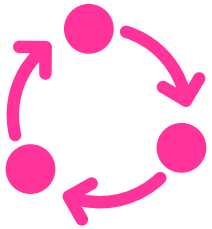
➔ Révision complète des procédures internes

- ✓ prise en compte des conclusions de l'analyse de risque
- ✓ modes de collectes, de transmission
- ✓ utilisation de terminaux nomades, mobiles
- ✓ mécanismes d'authentification



7. Surveiller les évolutions dans le temps

- Ré-évaluation périodique : amélioration continue
  - ✓ mise à jour de l'analyse de risques
  - ✓ changement de politiques
  - ✓ changement de procédures
  - ✓ nouvelles exigences
  - ✓ modification notable de service



Ressources

- CNIL
  - ✓ https://www.cnil.fr/cnil-direct/question/le-cloud-computing-cest-dangereux
  - ✓ https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

- ENISA
  - ✓ https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

CLUSIF

CLUSIR Rhône Alpes

Merci de votre attention !