



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



**CLUSIF 14 octobre 2010**

# **La désignation d'un CLIL : un retour sur investissement**

**Frédéric Connes**

<Frederic.Connes@hsc.fr>

- A première vue :
  - CIL = nouvelle fonction  $\Rightarrow$  nouveaux coûts
- Question :
  - La désignation d'un CIL est-elle rentable ?
- Comparer les coûts aux gains dans la durée
- Périmètre :
  - Entreprises
  - Administrations

- La désignation d'un CIL : un investissement réel
  
- L'action du CIL: un véritable retour sur investissement

- La désignation d'un CIL : un investissement réel
  - L'élément déclencheur
  - La désignation du CIL
  - La formation et l'accompagnement du CIL
  - L'organisation autour du CIL
  - Le temps consacré aux fonctions de CIL
  - Le respect des obligations légales

- Coût initial non nul :
  - Formalités de déclaration coûteuses
  - Dénonciation
  - Contrôle de la CNIL
  - Condamnation (directement liée ou non à informatique et libertés)
- Coût initial nul :
  - Impulsion de la direction
  - Démarche qualité
  - Sensibilisation réussie
  - Anticipation de problèmes
  - Obligation légale

- Information préalable des représentants du personnel :
  - Lettre recommandée
- Pas de frais à payer à la CNIL
- Peut se faire directement sur le web
- Principal coût : temps passé à préparer la désignation

- Déterminer :
  - Qui sera le responsable des traitements ?
  - Le CIL sera-t-il salarié, mutualisé, externe ?
  - La désignation sera-t-elle partielle, générale ou étendue ?
  - Combien de personnes approximativement
    - Sont chargées de la mise en œuvre des traitements
    - Ont directement accès aux traitements concernés par la désignation ?
  - Quelles mesures seront prises pour accompagner les missions du correspondant ?
- Peu prendre du temps

- Formation initiale :
  - Se former au droit pour les informaticiens
  - Se former à l'informatique pour les juristes
  - Sessions de sensibilisation gratuites (CNIL)
  - Organismes de formation reconnus
    - Investissent de plus en plus le marché du CIL
    - Durées et coûts très variables d'un organisme à un autre
    - Formations personnalisées: coût supplémentaire
  - Cabinets d'avocats
- Accompagnement :
  - Service CIL de la CNIL : gratuit
  - « Hot lines » spécialisées : coût à la question ou abonnement





- Recenser les traitements
- Se tenir informé
- Veiller au respect des obligations légales
- Recevoir les demandes et réclamations
- Conseiller et sensibiliser
- Préparer un éventuel contrôle de la CNIL
- Assister le responsable des traitements lors d'un contrôle
- Rédiger le bilan annuel

- Dégager des plages de travail dédiées aux fonctions de CIL :
  - Poste à temps partiel en complément d'autres responsabilités
    - DSI
    - RSSI
    - Directeur juridique...
  - Très grandes structures : poste à temps plein
- Dans tous les cas :
  - Personne connaissant bien l'entreprise
  - ⇨ ancienneté + larges compétences ⇨ salaire généralement élevé
  - Temps passé aux fonctions de CIL ⇨ coût important
- Petites structures : CIL externe possible

- Perte potentielle d'informations :
  - Données considérées comme
    - Inadéquates
    - Non pertinentes
    - Excessives
  - Exemple : zones de libre commentaires
    - Le CIL impose leur effacement
  - Durées de conservation excessives
    - Le CIL impose leur réduction
  - Peut apparaître comme un coût important pour certains organismes
  - Mais est-ce un véritable coût ?

- L'action du CIL : un véritable retour sur investissement
  - Alléger les formalités
  - Dormir tranquille
  - Disposer d'un conseil en interne
  - Démarche qualité
  - Lisser les coûts

- Traitements normalement soumis à déclaration dispensés
- Déclarations :
  - Pouvaient prendre du temps
  - Car effectuées par service souvent non spécialisé
- ⇒ Gain de temps important dans les structures ayant beaucoup de traitements déclarables
- Exception :
  - Transfert de données personnelles à destination d'un État non membre de l'Union européenne est envisagé
- Reste à faire :
  - Demandes d'autorisation

- **Audit informatique et libertés :**
  - Démarche initiée en interne par le CIL
    - Le recensement obligatoire des traitements n'est qu'une première étape
  - Auditeurs :
    - Internes (participation du CIL)
    - Externes (prestataire spécialisé)
      - Faire attention aux compétences du prestataire
      - Conseil juridique et ses limites
      - Projet de labellisation par la CNIL
  - Pas de certificat émis par la CNIL
  - Gains immédiats :
    - Identifier les traitements avec exhaustivité
    - Identifier les points de non-conformité légale

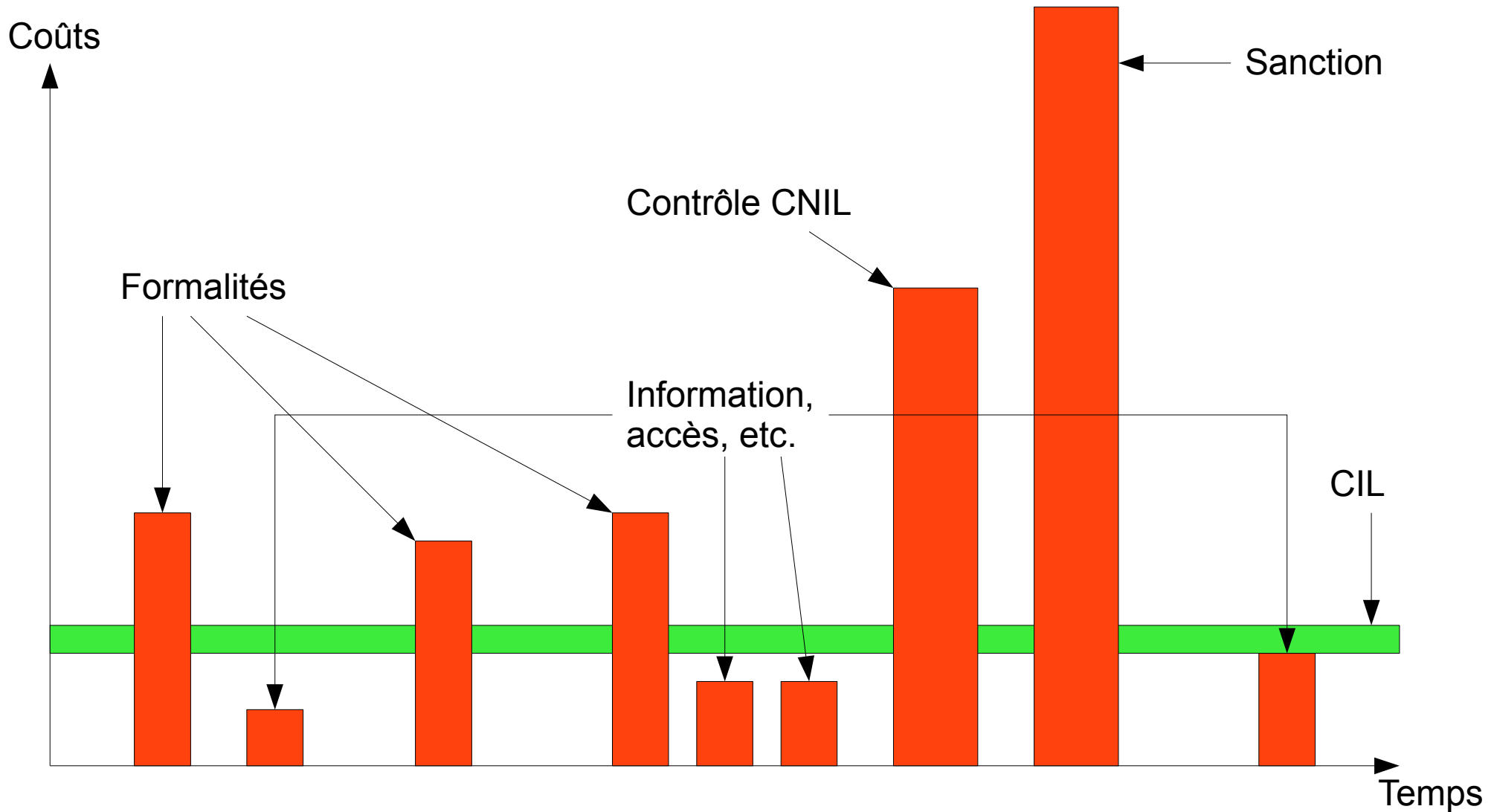
- Mise en conformité informatique et libertés :
  - Intégrer de nouveaux traitements dans la liste tenue par le CIL
  - Le cas échéant, faire les demandes d'autorisation
  - Garantir la licéité des collectes et des traitements
  - Garantir le respect de la finalité des traitements
  - Garantir le respect de la durée de conservation des données
  - Vérifier l'exactitude et la complétude des données
  - Vérifier les mesures de sécurité mises en place
  - Organiser l'information des personnes concernées
  - Organiser la communication des informations sur les traitements



- Gains d'une mise en conformité informatique et libertés :
  - Développement de l'activité sur des bases saines
  - Réduction du risque de dénonciation à la CNIL ou au parquet
  - Contrôle éventuel de la CNIL :
    - On ne craint pas le résultat du contrôle
  - En pratique :
    - Organismes ayant nommé un CIL et ayant été contrôlés :
      - Pas de non-conformité majeure constatée
      - Régularisation rapide de toutes les non-conformités mineures
      - Aucune condamnation
  - ⇒ Économies à moyen terme
  - ⇒ Faible risque de mauvaise publicité

- Le CIL peut remplacer les conseils d'un avocat
  - S'il a été correctement formé
  - Pour toutes les questions liées à l'informatique et aux libertés
- Peut devenir une référence dans l'organisme
  - Nouveau « commissaire aux données »
  - Aide le service juridique
- De plus : dispose de relais à la CNIL
  - Service dédié aux CIL
  - Répond gratuitement aux questions, même complexes
- ⇒ Économies pouvant être importantes
- ⇒ Gain de temps pour obtenir une réponse aux interrogations

- Désignation du CIL : peut être le point de départ d'une démarche qualité globale
- Processus d'amélioration continue
- Mise en conformité juridique globale
  - Au delà du périmètre informatique et libertés
- Obligation de sécurité : certification ISO 27001
- Plus généralement : certification ISO 9001
- A terme : ISO 29100
- ⇒ Gain en termes d'image
- ⇒ Gain de contrats grâce aux certifications



- Coûts :
  - Principalement en formation et en temps passé dans les fonctions
  - Assez facilement quantifiables
- Gains :
  - Gains de temps immédiats
  - Économies à moyen terme
  - Tranquillité d'esprit
  - Meilleure image
  - Contrats gagnés
  - Plus difficiles à quantifier : subjectifs
- ⇒ CIL = opportunité à saisir

# Questions