



Aspects juridiques de l'externalisation

Journées Externalisation du CUME
Paris, 19 janvier 2010

Solenn Houssay

Animatrice du réseau SupCIL

Correspondant Informatique et Libertés de l'Université Jean Moulin – Lyon 3

Chargée de la Sécurité des Systèmes d'Information de l'Université Jean Moulin – Lyon 3

solenn.houssay@univ-lyon3.fr



Pourquoi parler des aspects juridiques ?

- Il y a des risques :
 - Risques de contentieux
 - Risque d'incident de sécurité
 - Risques d'atteinte à l'image de l'établissement
 - ...
- Il faut les étudier en amont :
 - Pour négocier les clauses du contrat
 - Eventuellement dire « non » d'emblée à un prestataire



Les points à étudier

- Applicabilité de la loi française
- Conditions de résiliation
- Protection des données à caractère personnel
- Engagement de mesures de sécurité, d'accès aux logs, sauvegardes...
- Etc.

- Liste exhaustive à constituer avec :
 - Le service juridique
 - Le RSSI
 - Le correspondant Informatique et Libertés (CIL)



Zoom sur la protection des données personnelles



La loi « Informatique et Libertés »

- Elle concerne tous les traitements de données à caractère personnel
- Donnée à caractère personnel = donnée qui permet d'identifier une personne physique, directement ou indirectement
- Sont donc concernées :
 - L'externalisation de la messagerie électronique
 - La sous-traitance d'une solution de vote électronique



Pour qui ?

- Responsable du traitement : celui qui décide de la finalité et des moyens
- En pratique :
 - Le Président d'université ou Directeur d'établissement
- Et si on externalise ?
 - Idem : le Président d'université !
 - Le prestataire est considéré « sous-traitant » au sens de la loi



Quelles obligations ?

- Issues de 5 principes fondamentaux :
 - Finalité
 - Pertinence des données
 - Durée limitée de conservation des données
 - Sécurité et confidentialité
 - Respect des droits des personnes (information, accès aux données, rectification, opposition)



En cas de sous-traitance

- Engagement du prestataire sur :
 - Respect de la finalité
 - Respect de la durée de conservation
 - Mesures de sécurité et de confidentialité
- Cf. modèle dans le guide « Informatique et Libertés » pour l'enseignement supérieur et la recherche
- Clauses d'autant plus exigeantes que les données sont sensibles



En cas de transfert à l'international (1)

- Principe d'interdiction si le pays destinataire n'assure pas un niveau de protection adéquat
 - OK pour l'Union Européenne et quelques autres pays
- Exception : l'entreprise destinataire apporte des garanties suffisantes
 - Grâce aux « Clauses contractuelles types » de la Commission Européenne, intégrées dans le contrat
 - Au travers de l'adhésion au « Safe Harbor » (Etats-Unis)

En cas de transfert à l'international (2)

- Carte interactive sur le site de la CNIL :

Protection des données dans le monde

Amérique du Nord

- Antigua-et-Barbuda
- Bahamas
- Barbade
- Belize
- Canada
- Costa Rica
- Cuba
- Dominique
- Etats-Unis
- Grenade
- Guatemala

Revenir à la carte

- Niveau adéquat ou équivalent de protection des données.
- Niveau adéquat de protection des données sous certaines conditions.
- Niveau non adéquat de protection des données.
- # Pays disposant toutefois d'une autorité de contrôle.



En cas de transfert à l'international (3)

- Safe Harbor = « sphère de sécurité »
 - Ensemble de principes de protection des données personnelles, auquel peut adhérer une société américaine
 - Liste sur le site web du Safe Harbor
- Attention ! L'adhésion au Safe Harbor ne dispense pas d'un contrat de service avec des clauses suffisantes



Les formalités (1)

- Selon la sensibilité des traitements
- En général, régime de déclaration
- Cas particuliers :
 - Transfert de données hors de l'Union Européenne > demande d'autorisation auprès de la CNIL
 - Télé-service de l'administration électronique > demande d'avis auprès de la CNIL



Les formalités (2)

- Télé-service de l'administration électronique si :
 - Service via site internet
 - Avec identifiants propres à chaque utilisateur
 - Mis à disposition par l'administration
 - Pour les usagers du service public

- Exemples :
 - ENT
 - Solution de vote électronique pour les étudiants
 - Mais pas : solution de vote électronique pour les personnels



L'aide apportée par le CIL

- Recommandations sur les caractéristiques du traitement
- Contenu des clauses du contrat de service
- Formalités
 - Demande d'avis
 - Demande d'autorisation
 - Inscription dans le registre des traitements de l'établissement (allègement de formalités du fait de la désignation du CIL)



Les accès privilégiés du CIL

- Au Service des correspondants de la CNIL
- A l'extranet de la CNIL
- Au réseau national SupCIL (CIL de l'enseignement supérieur et de la recherche), issu du partenariat CNIL-CPU



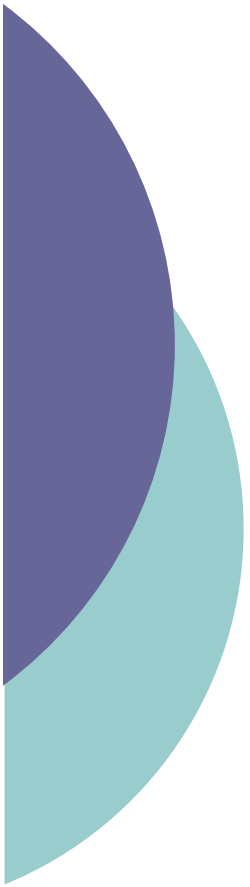


Le cas de la mutualisation



Ce qui change... ou pas

- Ce qui change :
 - Pays d'hébergement des données
 - Sans doute moins de clauses à négocier avec le prestataire
- Ce qui ne change pas :
 - Le chef d'établissement est toujours responsable de traitements
 - Il doit prendre des garanties suffisantes : convention inter-établissements à négocier



Conclusion



Evaluer les risques dès le début

- Etudier les aspects juridiques
 - Avec le service juridique
 - Avec le CIL (si existant)
 - Avec le RSSI
- Les garanties ont un coût... mais la prise de risques peut elle aussi coûter cher