Mise en conformité des activités pédagogiques et administratives d'une université: Cas de l'UTC

Rafia Berenguier
cil@utc.fr

Au commencement…

Parmi les obligations prévues par la loi du 6 janvier 1978 :

- une déclaration obligatoire des traitements

- l'information des personnes concernées par le traitement

- le respect des droits des personnes

- le respect des dispositions relatives à certaines catégories de données et de traitement
par exemple, données prévues aux articles 8, 9, 10 et traitements prévus aux articles 25, 26, 27 de la loi.

- …

mots clés « informatique & libertés »

Données à caractère personnel :
des données sont considérées comme à caractère personnel dès lors qu'elles permettent **d'identifier directement ou indirectement** des **personnes physiques**

Fichier : tout ensemble structuré et stable de données à caractère personnel

Traitement :
toute opération de collecte, enregistrement, organisation, conservation, modification, extraction, consultation, utilisation, communication, rapprochement, interconnexion, verrouillage, effacement, destruction portant sur de telles données

Le CIL

En 2004, la refonte de la loi du 6 janvier 1978 introduit la fonction de correspondant à la protection des données à caractère personnel, désormais connu sous l'acronyme de CIL (Correspondant Informatique et Libertés), chargé d'accompagner de manière indépendante, l'application des dispositions de cette loi dite « Informatique et Libertés ».

Le CIL : un outil de la conformité

Ses missions :

1- Tenir à jour le registre interne des traitements mis en œuvre au sein de l'université

2- Conseils et recommandations avant mise en œuvre des traitements

3- Contribuer à la diffusion de la culture Informatique et Libertés : sensibilisation et actions pédagogiques (site web, supports, formations…)

4- Veiller à l'effectivité des droits des personnes (information, d'accès, de rectification et d'opposition

5- Si nécessaire, procéder aux formalités auprès de la CNIL (demande d'avis ou d'autorisation)

6- Bilan annuel remis au RT et mis à disposition de la CNIL

La conformité pour une université

Comment la mettre en place?

Rôle du CIL (accompagner les personnes mettant en œuvre les traitement, veiller au respect des droits des personnes, procéder aux formalités déclaratives…)

Comment la maintenir?

- En respectant les 5 règles d'or de la protection des données

– En respectant un ensemble de bonnes pratiques

– En consultant le CIL en amont de chaque nouveau traitement

– …

→ **C'est une démarche collective**

Les 5 règles d'or de la protection des données

Finalité du traitement	Les données sont collectées pour des finalités **déterminées**, **explicites** et **légitimes** (art 6).
Pertinence des données	Données **adéquates**, **pertinentes** et **non excessives**
Durée de conservation limitée	Les données ne peuvent être conservées de manière indéfinies
Obligation de sécurité	Toutes les mesures doivent être prises pour empêcher que les données soient déformées, endommagées ou que des tiers non autorisés n'y aient accès
Respect des droits des personnes	Information des personnes - Droit d'accès, de rectification et d'opposition

Conformité : Quelles questions se poser ? (1/4)

1- Quelle(s) **finalité(s)** poursuit le traitement?

Etape primordiale car les données ne pourront pas être traitées de manière incompatible avec les finalités initiales. *Exemple: les traces informatiques*

La finalité déterminera aussi la durée de conservation.

2- Les données sont elles **pertinentes et non excessives?**

supprimer les champs qui ne sont plus nécessaires est une bonne pratique.

Sauf exceptions (consentement, intérêt public…), interdiction de collecter des données qui font apparaitre directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicales, les données de santé

Une protection particulière est accordée au traitement de données contenant le numéro de sécurité sociale.

Prendre contact avec le CIL

Conformité : Quelles questions se poser ? (2/4)

3- Quelle durée de conservation ?

Les données ne peuvent être conservées au-delà de la durée nécessaire à la réalisation de la finalité.
Au delà, elles ont vocation à être prises en charge par l'archiviste

définir une durée de conservation dès création du traitement-supprimer les listes expirées.
listes nominatives sur le poste de travail, extractions du SI (pointage, vérifications) dont l'utilité est limitée dans le temps.…

4- Sécurité des données : respect de l'intégrité et confidentialité des données.

gestion et mise à jour des habilitations et droits d'accès - limiter le stockage de DCP sur les clés USB– sécurité du mot de passe.
notes sur internet, gestion des droits dans moodle, vérification de la qualité de tiers autorisé…

Conformité : Quelles questions se poser ? (3/4)

-**Droit des personnes :** Information obligatoire (loyauté de la collecte) et garantie du droit d'accès, de rectification et d'opposition (s'il y a lieu pour ce dernier).

Tout formulaire traitant de données personnelles doit comporter une mention d'information (finalité, responsable, destinataire et exercice des droits).
Exemples: questionnaires, information préalable sur la page d'accueil du traitement, logiciel anti-plagiat…

Le droit d'opposition peut ne pas s'appliquer dans le cas de traitements « obligatoires ».

Un étudiant ne peut s'opposer à ce que ses données soient exploitées par le service scolarité. Il peut par contre, s'opposer au transfert d'informations le concernant au CROUS (carte multiservices).
L'étudiant peut aussi s'opposer à la publication de sa photo dans les application internes.

Conformité : Quelles questions se poser ? (4/4)

-Le traitement est-il un téléservice ?

téléservice : tout service permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives par le biais d'un identifiant qui lui est propre.

Exemple: ENT

-Données anonymes?

NON si :

- des données indirectement identifiantes sont collectées.

Exemple : Questionnaires en ligne avec enregistrement des données de connexion (identifiant, mdp, ip).

- des données peuvent être rattachées à des personnes par recoupement/combinaison

Cas des questionnaires adressés à un groupe de personnes pré-identifiées et susceptibles d'être identifiées.

Les régimes de formalités

- Dispense de déclaration

- Engagement de conformité à une norme simplifiée NS

NS 46 : gestion du personnel – NS 42: gestion des contrôles d'accès des horaires et de la restauration sur les lieux de travail

- Déclaration normale (ou registre CIL)

- Engagement de conformité à un cadre de référence (acte règlementaire unique « RU »)

RU13 : Apogée (organisation et gestion des enseignements et des étudiants) - RU03 : ENT

- **Demande d'avis auprès de la CNIL par l'établissement**

(art. 27 loi I&L) Vote électronique des usagers – gestion administrative et pédagogique des étudiants si l'établissement n'utilise pas apogée

- Engagement de conformité à un cadre de référence (appelé autorisation unique « AU »)

AU02 : Attribution d'aides ponctuelles aux étudiants

- **Demande d'autorisation auprès de la CNIL par l'établissement** *(art. 25 loi I&L)*