Séminaire

« *Le RGPD dans l'Enseignement supérieur et la Recherche : impacts et promesses* »

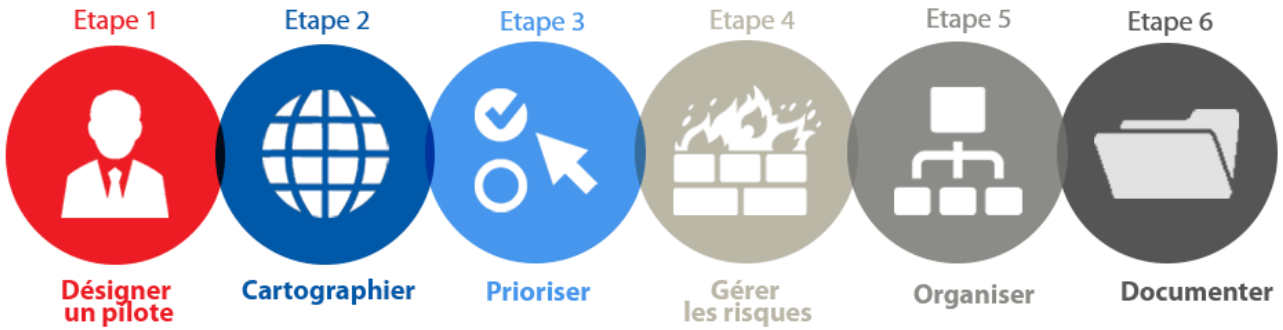
21 mars 2018

Règlement européen sur la protection des données
Les étapes conseillées par la CNIL pour s'y préparer

Florence Celen
Correspondant informatique et libertés (Toulouse III – Paul Sabatier)
Coordinatrice du réseau SupCIL

Victor Larger
Correspondant informatique et libertés (Paris Descartes)
Coordinateur du réseau SupCIL

RGPD - Les étapes conseillées par la CNIL pour s'y préparer



La CNIL préconise un plan en 6 étapes pour se préparer au RGPD. Ce plan est adaptable aux différents organismes des structures privées et publiques.

Il peut ainsi s'adapter aux établissements publics de l'enseignement supérieur et de la recherche. La présente présentation propose de **le mettre en perspective au regard de nos spécificités** (traditions universitaires, missions d'enseignement supérieur et de recherche,…), des situations constatées dans les différentes structures, et des freins susceptibles de freiner la mise en place rapide et efficace d'une conformité réelle au RGPD.

ETAPE
1
DÉSIGNER UN PILOTE

Désigner un pilote

Identifier et désigner un délégué à la protection des données (DPD/DPO).
> Choix du délégué interne, externe et/ou mutualisé
(art. 37 à 39 du RGPD, lignes directrices du G29 sur son statut, ses missions, les conflits d'intérêt…)

Dans les établissements qui ont fait le choix d'un **Correspondant informatique et libertés (CIL)**, celui-ci connaît déjà la réglementation, s'est tenu informé de la réforme européenne, a pu bénéficier de formations dédiées de la CNIL, dispose d'un accès privilégier à ses services, et peut accéder aux ressources et outils du réseau SupCIL.

Les organismes publics ont l'obligation de désigner un **délégué à la protection des données** à partir de mai 2018. Celui-ci pouvant être externalisé et/ou mutualisé, des organisations mixtes ou évolutives peuvent être décidées (externalisation d'un audit, puis désignation mutualisée, audit mutualisé puis désignations d'un DPD interne,…) en fonction de la stratégie de l'établissement.

Le DPD a vocation à être « le chef d'orchestre de la conformité » : **il n'agit pas seul** mais organise les opérations, fait rapport au Président, conseille les services et directions, forme les collègues, répond aux questions des extérieurs, met en relation les intervenants techniques et fonctionnels,…

ETAPE 2 CARTOGRAPHIER

Cartographier

Recenser les traitements de données mis en œuvre au sein de l'établissement.
> Cartographie de l'existant par finalités
(art. 30 du RGPD : responsable de traitement et sous-traitant, guide CNIL de la sous-traitance,…)

Dans les établissements qui ont fait le choix d'un **Correspondant informatique et libertés (CIL)**, celui-ci dispose d'ores et déjà d'un registre des traitements, qui peut servir de base à une nouvelle cartographie.

Cette cartographie doit également intégrer les traitements mis en œuvre au titre de la **sous-traitance réalisée pour d'autres** organismes.

En l'absence de CIL, l'établissement peut baser son registre sur les traitements déclarés à la CNIL par son établissement depuis le 1er janvier 1979, accessible depuis la plateforme **data.gouv.*fr***

Ce travail de recensement peut permettre d'identifier et d'harmoniser des traitements dont les finalités sont identiques et déclarés pour différentes composantes de son établissement.

Producteur
CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

ETAPE
3
PRIORISER

Prioriser

Identifier les chantiers prioritaires
> Analyse et décision au regard de la cartographie des traitements
(art. 39 du RGPD, lignes directrices du G29 sur les sanctions,…)

L'ampleur de la mise en conformité des traitements nécessite de hiérarchiser les opérations à mener.

L'article 39 du RGPD attend du DPD qu'il tienne compte « *du risque associé aux opérations de traitement compte tenu de* ***la nature, de la portée, du contexte et des finalités*** *du traitement* ».

Les lignes directrices précisent les critères qui pourraient être pris en compte dans le montant des amendes administratives (« *the nature, gravity and duration of the infringement; the purpose of the processing; if the data subjects have suffered damage; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the damage; the degree of responsibility; the categories of the personal data affected,...* »).

Les traitements prioritaires pourraient donc être considérés **au regard du nombre de personnes concernées** (scolarité et ressources humaines), des **catégories de données traitées**, notamment les données sensibles (médecine préventive, recherches en santé,…), et de la position de l'établissement (sous-traitance,…).

ETAPE 4 GÉRER LES RISQUES

Gérer les risques

Réaliser des analyses d'impact relatives à la protection des données, ou *Data privacy impact assessment* (DPIA)
> Analyse et décision au regard de la cartographie des traitements
(section 3 du RGPD, lignes directrices du G29 sur les DPIA,…)

D'après la cartographie des traitements mis en œuvre dans l'établissement, certains vont pouvoir être identifiés comme susceptibles de présenter un risque élevé pour les droits et libertés des personnes, par exemple en cas de profilage, de traitement de leurs données personnelles, de croisement de données, ou d'exclusion du bénéfice d'un droit.

Une liste des traitements assujettis par défaut à une telle DPIA est en attente de la CNIL. L'analyse d'impact sur la protection des données s'ajoute aux analyses de risques sur le système d'information.

Dans ce cas, le RGPD prévoit la réalisation d'une analyse d'impact, qui permet d'établir un plan d'action pour réduire les risques.

L'opportunité d'une DPIA est décidée par le Président de l'établissement, sur conseil du DPD. Il associe les services supports, les sous-traitants, et le DPD.

Si le plan d'action ne permet pas d'écarter l'ensemble des risques, **la saisine de la CNIL est obligatoire**.

La CNIL met gratuitement à disposition un outil permettant de mener de telles analyses d'impact.

pia | analyse d'impact sur la protection des données
privacy impact assessment

ETAPE
5
ORGANISER

Organiser

Formaliser les procédures
> Étude des procédures actives, toilettage, compléments
(label « Gouvernance informatique et libertés » de la CNIL,…)

La conformité des traitements de données à caractère personnel peut s'organiser sans procédure. Toutefois, il est évident qu'une telle absence mènera nécessairement à un manque de clarté de l'organisation, à des confusions, et à des erreurs préjudiciables à l'organisme.

Le besoin de cadrage pourra dépendre de la taille de l'établissement, de son degré de maturité, des pratiques déjà en place, et de la volonté d'accompagnement des problématiques de protection des données.

Ainsi, une politique de gouvernance des données et la procédure amont décrivant la validation d'un nouveau traitement apparaissent nécessaires, afin qu'il soit validé par le responsable des traitements, après avoir été examiné par les acteurs concernés (DSI, DPD, service juridique,…) pour identifier les éventuels manquements.

Des procédures complémentaires peuvent être formalisées pour aider les services dans la protection des données au quotidien (marche à suivre pour faciliter l'exercice du droit d'accès, notification des violations de données, accompagnement d'un contrôle de la CNIL,…).

Enfin, le label « *Gouvernance informatique et libertés* », et la certification qui lui succèdera, identifient les procédures permettant un **haut niveau protection**.

ETAPE 6 DOCUMENTER

Documenter

Constituer un « dossier de conformité » pour chaque traitement
> Obtenir des services supports et utilisateurs les documents utiles
(art. 6 du RGPD,…)

L'article 6 du RGPD qui traite des « ***principes relatifs au traitement de données*** », pose le principe de l'*accountability*, et prévoit ainsi que le responsable des traitement est en mesure de démontrer le respect du traitement aux dispositions du Règlement européen.

Il convient donc de **documenter le respect de chaque exigence, pour chaque traitement** : licéité du traitement (c.a.d. instruction préalable), limitation des données collectées (c.a.d. privacy by default), identification des destinataires des données (c.a.d. politique d'habilitation), encadrement des opérations de sous-traitance (c.a.d. existence d'un contrat en cours comportant des clauses spécifiques),…

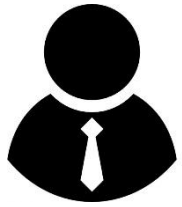
Ce lourd travail nécessite d'avoir priorisé les actions (cf. étape 3), de bénéficier d'un véritable appui de la gouvernance (par ex. avec une lettre de mission) et l'assistance effective des services supports et utilisateurs.

Il doit être régulièrement révisé (tous les trois ans ?) pour valider son exhaustivité et sa validité.

Des audits doivent être prévus et des outils mis en place pour permettre l'exercice effectif des droits et les réponses dans le délai RGPD.

RGPD - Les étapes conseillées par la CNIL pour s'y préparer

Les outils de la conformité



Délégué (DPD)

Packs sectoriels
Guide CNIL-CPU

Labels et certifications

Codes de conduite

Normes CNIL
Projet SupCIL-CPU ?

Registre des traitements

Analyses d'impact

Questions, commentaires, suggestions ?