Séminaire
« ***Le RGPD dans l'Enseignement supérieur et la Recherche : impacts et promesses*** »
21 mars 2018

Règlement européen sur la protection des données
Décryptage stratégique

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 / Impacts

Data Privacy

Éthique

Thèses

IT

Protection du patrimoine scientifique et technique

Publications

Homologation RGS

Financements européens

Cloud

Entrepôts de données

Unités de recherche

Données de recherche

Appels à projet

Droits des personnes

Relations contractuelles

Regroupements

Formalités CNIL…

Enquêtes administratives

Conformité « RGPD »

Ouverture des données

Analyse d'impact

Archivage des données

Pilotage de l'établissement

Gestion des accès

Sécurité des systèmes d'information

Données de gestion

Fondement juridique

RGPD / Objectifs

… Établir une règlementation européenne applicable dans les 28 états membres de l'UE, adaptée à l'évolution des technologies et garantissant la protection des données personnelles, et plus globalement, de la vie privée des citoyens européens.

- **Responsabiliser les acteurs traitant des données personnelles** ceux qui collectent, stockent, accèdent, échangent ou transfèrent des DCP (responsables de traitement et services opérationnels ; sous-traitants ; partenaires)

Accountability … de la logique déclarative CNIL à la capacité de s'autogérer et de prouver la conformité RGPD

- **Renforcer les droits des personnes**
- **Crédibiliser la régulation** (coopération renforcée entre autorités de protection des données)

RGPD / Champ d'application

Où ?

Un règlement qui touche tous les établissements (publics / privés) européens mais aussi les établissements basés hors UE qui collectent, hébergent, manipulent des données personnelles de citoyens européens.

Quand ?

Utilisation donnée à caractère personnel (DCP) / Sphère privée, professionnelle ou publique

Tous les aspects de la vie d'un individu identifié directement ou indirectement > éléments physiques, psychologiques, génétiques, mentaux, économiques, culturels, sociaux…

ESR directement concerné : en qualité de Responsable de traitement (RT) et de Sous-traitant (ST)

- ❑ Lien avec des usagers qui se renouvellent régulièrement,
- ❑ Collecte / Échange une grande masse de données, parfois sensibles liées à aux missions et activités : <u>enseignement, recherche et administration</u>.

DCP collectées : agents, étudiants, autres individus : lecteurs, enquêtés, patients, fournisseurs…

Principe ?

- ❑ Niveau de protection des DCP adapté à la sensibilité des DCP et aux risques sur la vie privée dès la conception des traitements, produits et services,
- ❑ Durant tout le cycle de vie de la DCP.

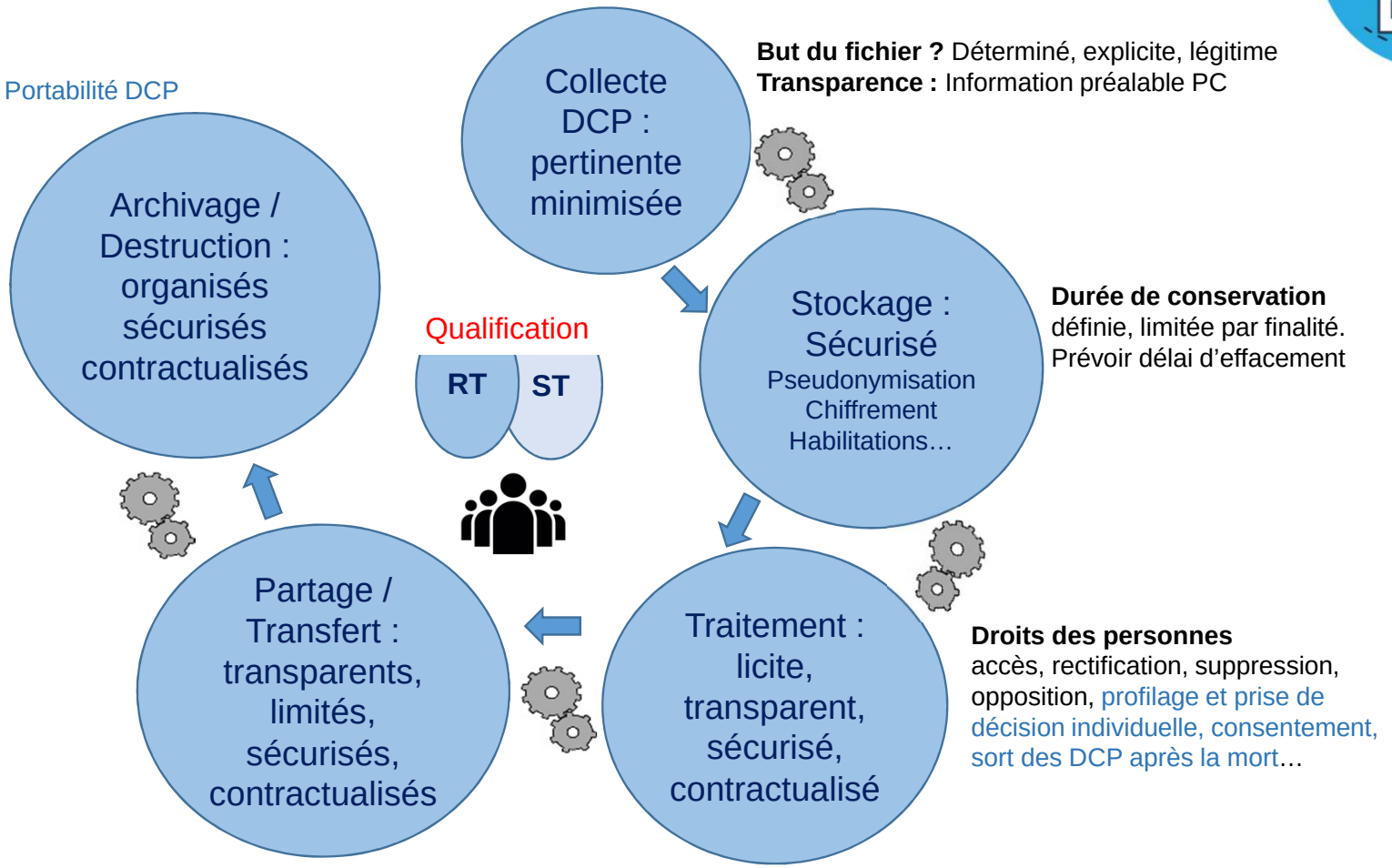
RGPD / Focus obligations des acteurs du TDCP : RT, ST, Co-RT

Obligations communes

Respecter les principes fondamentaux renforcés de la protection des DCP (Loi 1978, RGPD arts. 5 à 11)
Documenter / Tracer / Prouver les mesures organisationnelles et techniques prises = Accountability (arts. 24, 25)
Création / Maintenance registres des activités de traitement de DCP / Qualification RT et ST (art. 30)
Coopérer avec l'autorité de contrôle (art. 31)
Sécuriser les DCP et les traitements (art. 32)
Désigner un DPO (arts. 37 à 39)
Respecter les règles de transfert de DCP dans les pays tiers (arts. 44 à 50)

+ Obligations spécifiques RT : autorité qui détermine la finalité et les moyens, not. Informatiques, du traitement DCP	**+ Obligations spécifiques ST (agit pour le compte du RT) Responsabilité propre (art. 28)**	**+ Obligations spécifiques Co-RT**
Transparence / Information des personnes concernées (arts. 12 à 14)	Etre autorisé par le RT à sous-traiter (art. 28-2) Contractualiser la relation ST et ST (art. 28-3)	Obligations RT
Mettre en place les procédures organisationnelles et techniques de respect des droits des personnes concernées (arts. 15 à 21)	Respecter les instructions du RT (art. 28-3)	Contractualiser la relation RT conjoints (art. 26)
Respecter les principes de protection des données dès la conception et protéger les données par défaut (art. 25)	Engagement de confidentialité des personnes autorisées à traiter les DCP (art. 28-3)	Mettre à disposition des PC les termes de l'accord Co-RT (art. 26-2)
Pour les traitements de données sensibles : réaliser EIVP / PIA ▪ Analyser l'impact des TDCP sur la vie privée (arts. 35 à 36) ▪ Prendre les mesures de protection appropriées aux risques évalués	Coopérer et assister le RT (art. 28-3) dans ses obligations : ▪ Garantir la sécurité des DCP ▪ Alerter le RT en cas de manquement ▪ EIVP / PIA	
Contractualiser la relation RT / ST (art. 28) et auditer le ST	Supprimer les DCP ou remettre l'intégralité des DCP au RT au terme de la prestation (art. 28-3)	
Notifier violations de DCP à l'autorité de contrôle et aux personnes concernées (arts. 33, 34)	Notifier violations de DCP au RT ou à l'autorité de contrôle	

RGPD / Bouleversement des pratiques… Pas des principes



Transverse

Organisation et suivi RGPD :
DPO
RT : Politique de gouvernance DCP / Accountability / Procédures internes
Registres des activités de traitements : RT/ST

Conception et contrôle des TDCP :
PSSI / Procédures internes
Privacy by design / Privacy by default
EIVP
Études de risques SI / RGS
Contrôle des mesures de sécurité
Droits des personnes renforcés
Notification des violations DCP
Audits
Contractualisation

Documentation / Traçabilité

… De l’obligation de moyen à l’obligation de résultat… (1/2)

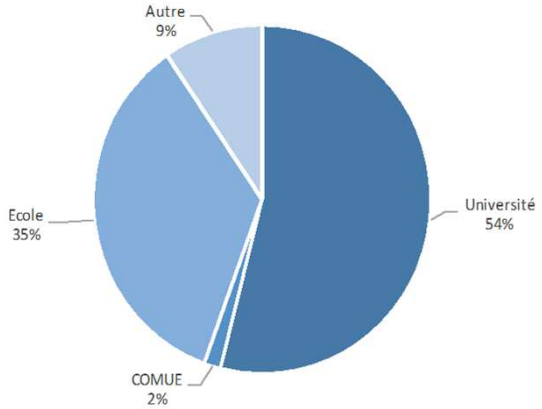
Le Responsable de Traitement (RT) : - Président université ou Directeur grande école
- DU pour les UMR et UMS (Note CPU 09/2017)

Premier pas vers la responsabilisation : **Désigner un DPO** *articles 37 à 39 RGPD ; Lignes directrices du G29 (statut, mission, conflit d’intérêt…)*

« Le passage du CIL au DPO reste aujourd’hui du choix de chaque entreprise, mais il est clair que le CIL a vocation à devenir DPO.

Et cette fonction prendra sa pleine dimension une fois le règlement adopté ».

AFCDP 2015, Isabelle Falque-Pierrotin, Présidente de la CNIL



ESR (CPU / CGE) : la majorité des organisations disposent d’un CIL, soit 145 (03/2018), chargé de l’analyse de conformité des TDCP

Statuts CIL / DPO similaires
Pas de changement majeur dans les missions, la pratique a été consacrée par le RGPD

- ✓ Informe et conseille le RT, les agents et les usagers sur la protection des DCP
- ✓ Contrôle le respect du RGPD et des procédures internes (analyse de conformité)
- ✓ *Dispense des conseils pour l’analyse d’impact des traitements sur la vie privée* (NOUVEAU)
- ✓ *Accède aux DCP*

IMPORTANT **Choix du DPO** interne, externe et/ou mutualisé **MAIS** désignation **expresse** par chaque RT

La manière de le désigner, les moyens et le soutien qui lui seront attribués démontreront l‘engagement de l’établissement pour la protection des DCP

… De l’obligation de moyen à l’obligation de résultat… (2/2)

L’organisation, les processus de gestion et de conservation des données doivent évoluer pour atteindre le niveau de conformité RGPD exigé.

Quelle démarche de mise en conformité initier ?

Mise en place d’une gouvernance de protection DCP *(sur le modèle du label CNIL « Gouvernance I et L »)*

Mise en place d’un comité ad hoc pour la définir et la mener

Une décision hiérarchique forte : initiée par la gouvernance pour entraîner l’ensemble des structures (enseignement, recherche, administration) vers une nouvelle culture d’établissement et un changement des pratiques.

Une nécessité (principe d’accountability) : En cas de contrôle, l’établissement devra être en capacité de démontrer qu’il a mis en œuvre les mesures organisationnelles et techniques pour respecter le RGPD.

❑ **Désigner un DPO :**

- o Garantir l’effectivité de ses missions (lettre de mission)
  + Organiser sa désignation expresse en cas de mutualisation entre plusieurs RT (UMR, UMS)
  + Désigner des référents protection des DCP (réseau)
- o Indépendant / Absence de conflit d’intérêt (pas de cumul avec des fonctions nécessitant de déterminer finalité/moyens des traitement de DCP)
- o Saisir le DPO de manière appropriée et en temps utiles

… De l’obligation de moyen à l’obligation de résultat… (2/3)

Quelle démarche de mise en conformité ?

❑ Définir les politiques et les process de gestion des DCP

- o Mettre en place l’outil de suivi et de vérification de la conformité des traitements au RGPD : Registres RT / ST (responsabilité RT)
- o Modifier le process de pilotage des projets : tenir compte de la protection DCP dès la conception des traitements et des services (Privacy by design / by default)
  - ▪ Définir les règles exécutoires des politiques de confidentialité et de sécurité (pseudonymisation, chiffrement par défaut)
  - ▪ Mettre en place les mesures et les outils internes garantissant une protection optimale des personnes dont les données sont traitées (Évaluer les risques : EIVP et risques SI ; outiller la gestion/suivi des réclamations, des violations de DCP (délais RGPD), archivage / purge du SI
- o Contractualiser la conformité RGPD avec les sous-traitants et les partenaires (adaptation et revue des contrats, conventions, marchés)
- o Organiser la traçabilité des mesures garantissant le respect RGPD en continu / Coopération avec l’autorité de contrôle

❑ Campagnes de communication / formation / sensibilisation des acteurs au respect des obligations (Plan de formation)

- o Impliquer les métiers dans les processus de conformité définis
- o Intégrer la protection des DCP dans les objectifs des agents

RGPD / Bénéfices attendus…

La conformité au RGPD, une opportunité pour l'université, les grandes écoles à différents niveaux :

Image / Réputation	Instaurer/Restaurer la confiance des usagers et des personnels de l'université dans la gestion de leurs DCP
Juridique	Améliorer la responsabilité numérique de l'université Limiter les risques : plaintes / contentieux
IT	Sécuriser et assainir les traitements et le stockage de la donnée « Accountability », « Privacy by design » ou « by default » apportent qualité et fiabilité des processus et des outils Limiter les risques de violation des DCP
Métier	Maitriser l'utilisation de la donnée et augmenter sa valorisation = Qualité des processus de gestion
RH / Etudiants / Extérieurs	Responsabiliser les acteurs de l'université sur la question des DCP

Éviter les sanctions dont les montants dissuadent la non-conformité :

- Impact sur l'image (niveau de maitrise des données et des outils)
- Impact financier de 10 à 20 M€ ou 2 % du CA annuel mondial
- Sanctions pénales

RGPD / Régulation renforcée

- Tout traitement mis en œuvre en UE ou hors UE MAIS qui concerne des citoyens UE est soumis au droit de l'UE
  - Comité européen de la protection des données
  - Coordination des autorités de contrôle européennes (CNIL, …)
- La plupart des formalités déclaratives CNIL sont supprimées, le régime d'autorisation est maintenu (loi I et L)
  - Du temps libéré pour opérer des contrôles
- Notification de violations de données à l'autorité de contrôle (CNIL)
- Transferts hors UE encadrés
  - Règles, accords ou contrats contraignants (normes UE)
  - ou consentement de la personne
  - ou vérification CNIL (autorisation)

Comment la CNIL contrôle-t-elle la conformité au RGPD ?

- Les modalités de contrôle de la CNIL restent inchangés : Sur place / En ligne / Sur audition et sur pièces
- Déclenchements : programmes annuels de contrôle, sur plaintes, infos médias, à la suite d'un premier contrôle

2 types d'obligations distinguées :

- Respect non négociable des principes fondamentaux de la protection des DCP (Pertinence collecte, finalité, conservation, sécurité, droits)
- Nouvelles obligations et nouveaux droits : les contrôles auront pour but d'accompagner, dans un premier temps, les établissements vers la mise en œuvre opérationnelle du RGPD (EIVP, notifications des violations de DCP…)

RGPD / Mises en demeure, jugements, sanctions,…

2004-2013 : Contrôles dans les établissements de l'ESR (vidéosurveillance, thématique annuelle, actualités…)

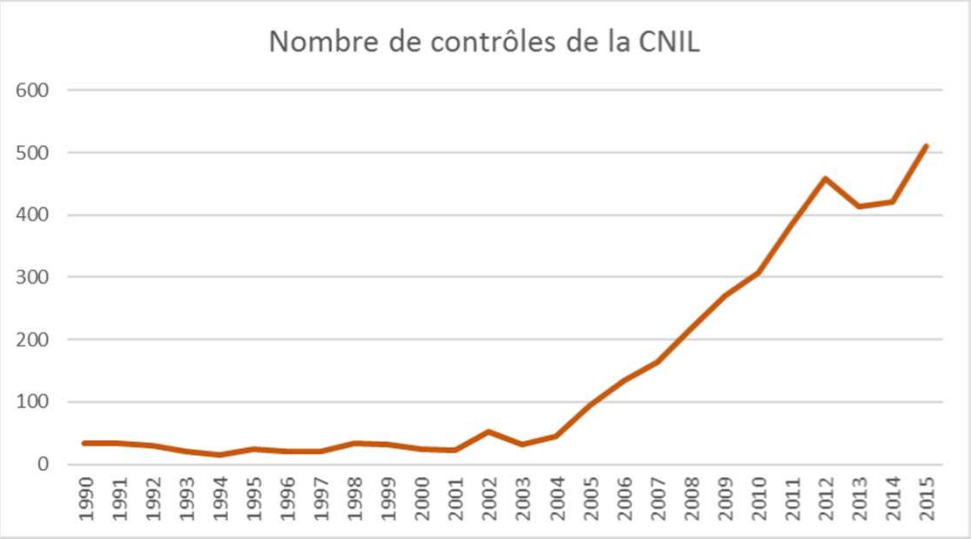
2014 : Contrôles en ligne de 6 universités - Contrôle sur place

2016 - 2017

HERTZ : Sanction CNIL de 40.000 euros (sous-traitance).

CGE : Contrôles sur les traitements de gestion administrative et pédagogique et sur les traitements réalisés à partir de données collectées via APB

DARTY : Sanction CNIL de 100.000 euros (sous-traitance)



Ministère : Mise en demeure relative à APB

CNOUS / IZLY : Géolocalisation des porteurs et renseignements auprès de sociétés publicitaires

TGI de Marseille : Un médecin pédiatre de l'AP-HM condamné au versement 5000 euros d'amende.

2018

CNAMTS : mise en demeure pour sécurité insuffisante des données (établissement public susceptible de faire l'objet de l'une des sanctions prévues par l'art. 45 de la loi I&L ainsi que, selon les dispositions du Code pénal, d'une amende pouvant atteindre 1,5 M€).

RGPD / Pour aller plus loin…

Texte complet du Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

- ❑ Sur le site de l'UE : http://eur-lex.europa.eu/
- ❑ Sur le site de la CNIL

Site CNIL https://www.cnil.fr/

- ❑ Les principales orientations de la réformes et les évolutions à anticiper (lignes directrices CNIL)
- ❑ Se préparer en 6 étapes + Guides CNIL, recommandations et outils de conformité

Particularité ESR

- ❑ Réseau SupCIL en évolution
- ❑ Lettre CPU 04-09-2017, conformité légale des traitements de DCP - Désignation CIL dans les unités mixtes
- ❑ Lettre CNIL aux RT via les CIL ESR 22-11-2017

Questions, commentaires, suggestions ?