Patrick Guillot, CIL des établissements universitaires de la ComUE Université Grenoble Alpes
CIL@grenet.fr

Prise en compte des données personnelles

Évolution de la règlementation

préliminaires

?

- qu‘est-ce qu’une donnée à caractère personnel ?
- quand a été créée la CNIL ?
- faut-il faire une déclaration ?
- le CIL, c’est quoi ?
- …

VRAI/FAUX ?

- l’@IP de mon ordinateur est une donnée personnelle
- un questionnaire sans «données nominatives» est «anonyme»
- les colloques, conférences, etc. sont des traitements à déclarer
- la législation sur les données personnelles est harmonisée au plan mondial
- ….

vrai / faux (1)

L'adresse de messagerie professionnelle (institutionnelle) est une donnée à caractère personnel	VRAI au même titre que l'adresse de messagerie privée
La redirection de la messagerie professionnelle sur la messagerie privée est tolérée	FAUX La sécurité des informations sensibles ou confidentielles n'est pas garantie
Le N+1 peut accéder (consulter) la messagerie ou l'espace professionnels d'un personnel	VRAI en ayant informé la personne sauf pour les informations privées conservées dans un répertoire clairement identifié «privé »
La fiche de paie est un justificatif pertinent de dépenses en personnel sur un projet	FAUX certaines informations confidentielles n'ont pas à être divulguées (NIR, primes, situation sociale, …)
Traiter des données sensibles doit être autorisé par la CNIL	VRAI ces traitements sont a priori interdits
L'annuaire interne des membres d'un laboratoire peut être publié sur le net	FAUX non conforme sans le consentement des personnes (admis sur intranet)
Le thésard est responsable des traitements de données personnelles utilisées pour son travail de thèse	FAUX la responsabilité juridique porte sur le laboratoire (UMR) ou l'établissement le directeur de thèse est responsable de mise en œuvre

la protection des données personnelles en recherche

loi informatique et libertés du 6/1/1978
règlement général européen du 27/4/2016

Logo labo

rappel : définitions et principes fondamentaux

- **la loi**
  - loi du 6 janvier 1978 modifiée (périmètre **national**)
  - règlement général **européen** (RGPD) du 27 avril 2016 **applicable le 25 mai 2018**
- **données à caractère personnel (personnelles) : informations qui**
  - prises isolément ou par regroupement, recoupement, permettent d'**identifier une personne** physique
    - directement (état civil, photo, numéro, biométrie, …)

    ou
    - **indirectement** (adresse, téléphone, situation familiale, profession, biens, …)
  - **quel(s) que soi(en)t le(s) moyen(s) utilisé(s)**
- **conformité d'un traitement de données personnelles**
  - défini et mis en œuvre pour une **finalité déterminée et explicite**
  - soumis au **consentement éclairé** des personnes concernées selon une **information préalable** complète et sincère
  - **collecte** et traite des **données pertinentes** et **non excessives**
  - garantit une **conservation des données** (hébergement , stockage) **limitée et sécurisée** (accès et confidentialité)
  - garantit l'**exercice des droits** des personnes concernées et le **contrôle** par chacune de ses données
- **nb : traitement de données pour les projets de recherche portant sur des personnes**
  - les protocoles de sélection et d'inclusion des personnes font partie du traitement des données

rappel : données personnelles sensibles

- **données révélant directement ou indirectement**
  - les origines raciales ou ethniques,
  - les opinions politiques, philosophiques ou religieuses
  - l'appartenance syndicale
- **données relatives**
  - à la santé
  - à la vie sexuelle
  - aux difficultés sociales
  - aux infractions ou condamnations
- **données biométriques et génétiques**
- **le numéro d'inscription des personnes au répertoire national**
  - NIR / n° Insee / **n° sécurité sociale**

enjeux : impacts sur la vie privée

I. la collecte des données

- les données d'inclusion/exclusion sont à prendre en compte
  - ce sont les **premières données collectée**s
  - ce sont **parfois** (souvent) **des données sensibles** (au sens de la loi)
  - ce sont des éléments de **l'analyse des risques et impacts** sur la vie privée
- impacts selon le type de données collectées (**pertinence**)
  - objectives ; confidentielles et/ou touchant à la vie privée ; sensibles
- impacts selon le volume de la collecte
  - nombre de personnes concernées ; nombre d'informations / personne
- impacts selon la source d'information
  - **la personne** ; un tiers ; fichier(s) constitué(s) ; **réseaux sociaux**
- impacts selon le protocole et les outils de collecte
  - enregistrement : interview, vidéo, capteurs, …
  - questionnaires : papier, en ligne (**! plate-forme**)
  - communication, extraction, requête sur un fichier
  - **par «moissonnage» (collecte massive, Big data)**

enjeux : impacts sur la vie privée

II. impacts selon la sécurité portée au données durant leur durée de conservation

- risques : fuite de données, accès illégitime, modification, suppression non souhaité ; …
- **analyse des risques**
  - maîtrise depuis la collecte à la production des résultats et à la suppression des données brutes

III. impacts selon la possibilité d'identifier des personnes… Vous avez dit anonymat ?

- **différencier confidentialité et anonymat**
- les données brutes sont (toujours) des données personnelles
- l'anonymat strict n'existe (quasiment) pas !
- **des «données non nominatives» ne sont pas anonymes**
- recommandation systématique : «***pseudonymisation***»
  - **minimisation** du caractère identificateur (indirect) des données

IV. impacts selon la mise à disposition des données (destinataires)

- accès public auxrésultats : données de publication (agrégées)
- ouverture des données de recherche (**open access**) ; recherche ouverte (**open rech**erche)
  - aux publics scientifiques
  - obligation de la loi pour une république numérique si financement public
  - les données brutes doivent être ***pseudonymisées***
- **nb : toute réutilisation de données constitue un nouveau traitement soumis aux dispositions légales**

Évolution de la règlementation

de la loi I&L [06/01/1978 - …[
vers le RGPD [25/05/2018 - …[

Logo labo

Historique des principaux textes

- **1978 : Loi nº78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**
- **1995 : Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**
- **2004 : Loi nº2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés**
- **2012 : («loi Jardé») - Loi nº 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine**
- **2016 : (publication du RGPD) - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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**
- **2016 : («loi Lemaire»**) - Loi nº2016-1321 du 7 octobre 2016 pour une République numérique**
  - préfigure le RGPD
- **2017 : (Code de santé publique) - Décret nº 2017-884 du 9 mai 2017 modifiant certaines dispositions réglementaires relatives aux recherches impliquant la personne humaine**
- **2018 : application du RGPD immédiate et uniforme dans tous les pays de l'UE**
  - **s'impose aux lois nationales**
  - **la loi informatique et libertés sera amputée des dispositions du RGPD mais restera applicable pour notamment**
    - **les recherches en santé**
    - **les traitements relevant des intérêts de l'Etat**

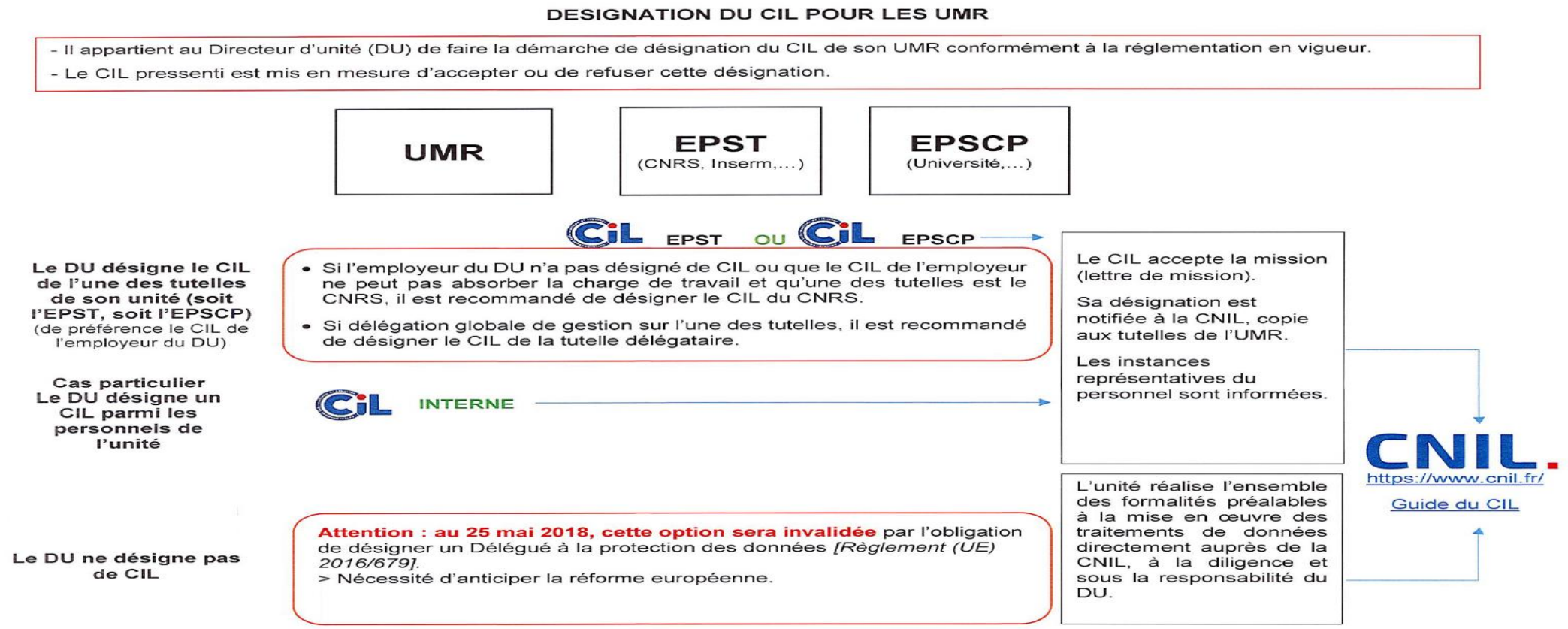
Renforcement des concepts fondamentaux. Évolution des obligations : principes

- **Accountability**
  - passage d'une **logique déclarative** à une **logique de responsabilité** et de **preuve de conformité**
  - **preuve par la documentation (protocole, DMP, analyse de risque, cahier de labo, autorisation CNIL, …)**
  - **responsabilité des sous-traitants**
- **Privacy by design**
  - **prise en compte** des aspects informatique et libertés et **des impacts dès le début du projet (cahier des charges)**
  - **principe de minimisation** selon le protocole de la recherche
    - la **pertinence** des (catégories de) données
    - les **durées de conservation**
    - le niveau de **sécurité** à porter aux données
  - **information** complète, loyale, explicite **et consentement éclairé**
- **Privacy & security by default**
  - **principe de minimisation** par défaut
  - mesures techniques **et** organisationnelles
    - sur les outils : infra, applications, anonymisation, chiffrement, …
    - sur les processus métiers : méthodes, protocoles, habilitations, …
- **Privacy impact assessment (PIA) ou étude d'impact sur la vie privée (EIVP)**
  - analyse de risques
  - élément de preuve de conformité
  - détermine la nécessité de soumission préalable à la CNIL.

Renforcement des principes fondamentaux. Évolution des obligations

- **Responsabilités**
  - renforcement et extension aux sous-traitants
  - **extension aux UMR** (quid des autres unités mixtes ?)
- **Sécurisation juridique**
  - Loi I&L (2004) : **Correspondant informatique et libertés** (CIL)
    - non obligatoire
    - situation actuelle sur le site (CNRS/universités)
      - 2012 : CIL du CNRS et CoSIL de la DR11
      - 2007 : CIL mutualisé des établissements (UGA, USMB, INP, IEP, COMUE UGA)
      - aucune UMR n'a désigné de CIL
  - RGPD (2016) : **DELEGUE à la protection des données** (DPO ?)
    - **obligation pour tout organisme public (25 mai 2018)**
    - processus de désignation en cours de formalisation (CNIL)
    - situation actuelle sur le site (CNRS/universités)
      - transition «naturelle» CIL → DELEGUE
      - **obligation de désignation pour les UMR (demande CPU/CNRS sept 2017)**

Quel CIL pour les UMR ? recommandations CNIL/CPU/CNRS



Les différentes options sur le site

tutelles concernées : EPST (CNRS) - EPSCP (UGA, USMB, INP, IEP)

1. Cas particulier : un membre (personnel) de l'unité

si le contexte le permet (compétence interne)

2. Le CIL de l'établissement employeur du DU

préconisation CNIL relayée par CPU et CNRS (chaine de responsabilité administrative et pénale)
sur le site : CIL du CNRS ou CIL mutualisé (UGA, USMB, INP, IEP)

3. Le CIL de la tutelle dont l'UMR a reçu une DGG

y en a-t-il ?
position CNIL réservée (< 50 chercheurs)

4. Le CIL de la tutelle «préférée»* (préconisation locale)

culture de mutualisation, relations métier
hébergement par la tutelle

5. Le CIL du CNRS (option finale)

en cas de refus du CIL mutualisé**
autres situations non résolues

vrai / faux (2)

La voix est une donnée personnelle biométrique	**FAUX** **c'est bien une donnée personnelle mais elle peut être déformée ou contrefaite**
un questionnaire sans «données nominatives» est «anonyme»	**FAUX** **beaucoup d'autres informations permettent d'identifier une personne**
les colloques, conférences, etc. sont des traitements à déclarer	**VRAI** **on gère des listes de contacts, de participants, d'intervenants, la restauration, l'hébergement, etc.**
Les recherches en santé sont soumises à des obligations spécifiques	**VRAI** **relèvent d'un chapitre particulier de la loi informatique et libertés et du Code de la santé publique**
Ne pas s'opposer vaut consentement	**FAUX** **le consentement est un acte volontaire marqué.** **toute autre attitude vaut opposition**
Le transfert (la communication) de données personnelles dans l'UE est autorisé	**VRAI : l'UE est un périmètre de confiance pour la sécurité des données** **le transfert hors UE non autorisé par la CNIL est interdit**
Le mail n'est pas un moyen de communication sécurisé	**VRAI** **équivaut à la carte postale pour le corps du message** **A MINIMA : CHIFFRER LES PIECES JOINTES CONFIDENTIELLES ou SENSIBLES**

Merci de votre attention

Questions ?