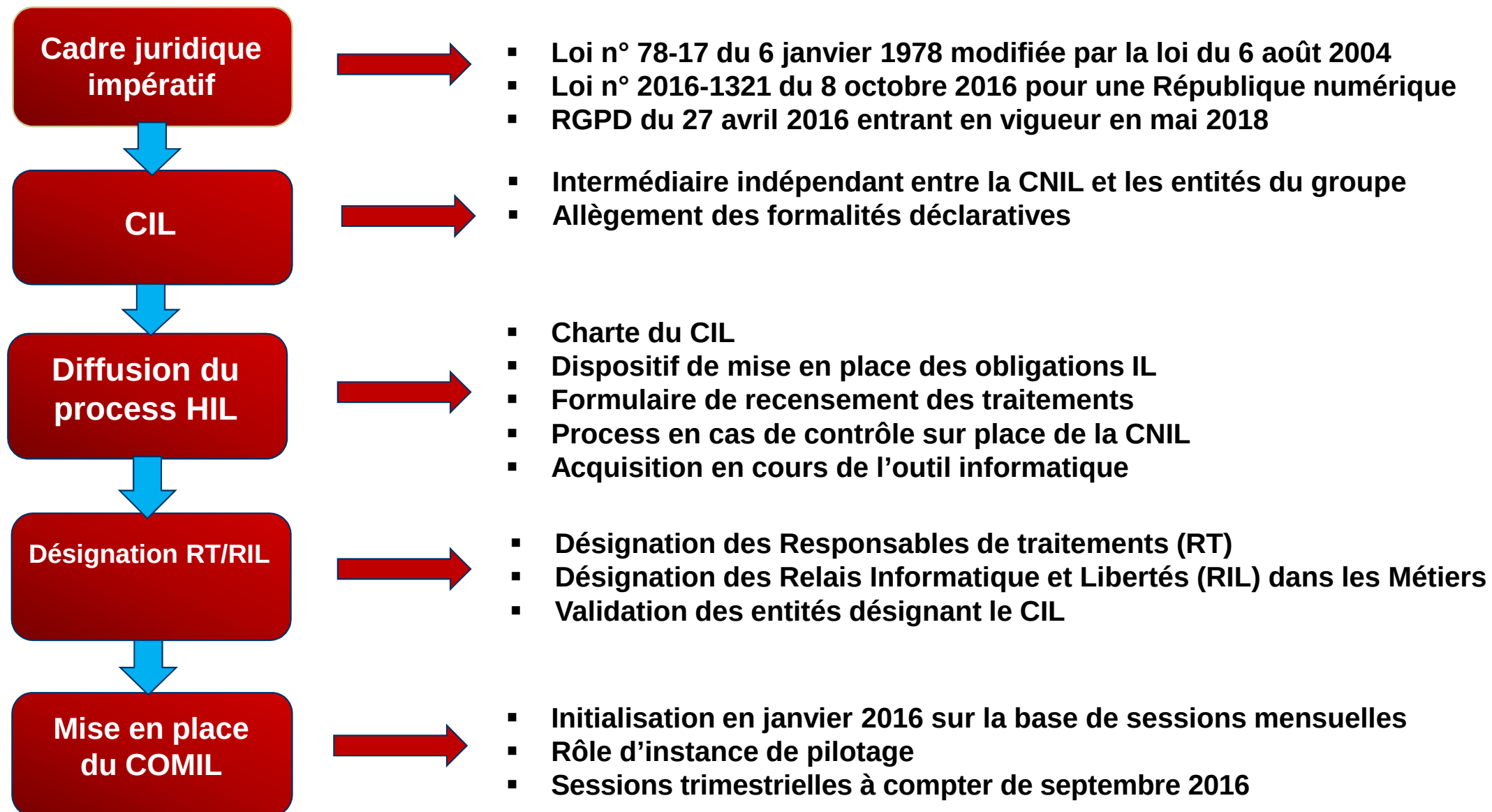


« Humanis Informatique et Libertés »

- 1.** Le dispositif HIL
- 2.** Les définitions essentielles
- 3.** Les principes légaux et réglementaires
- 4.** Règles relatives au consentement : NIR et opt-in /opt-out
- 5.** Mentions d'information et clauses IL
- 6.** Les principales actions 2016
- 7.** La trajectoire du dispositif HIL



➤ **Qu'est-ce qu'une donnée à caractère personnel (articles 2 et 8 de la loi du 6 janvier 1978)**

- ✓ Information relative à une **personne physique** (employés, candidats, affiliés)
- ✓ Identification **directe ou indirecte**, étant précisé que sont pris en compte l'ensemble des moyens utilisés en vue de permettre l'identification de la personne

Exemples : nom et prénoms, numéro adhérent, adresse IP, etc.

- ✓ Il existe des **données personnelles particulièrement sensibles dont le traitement est en principe interdit**, sauf consentement exprès des individus ou exceptions légales.

Exemples : numéro de sécurité sociale (NIR), données de santé, coordonnées bancaires, etc.

➤ **Qu'est-ce qu'un traitement de données (article 2 de la loi du 6 janvier 1978)**

Traitement automatisé ou non automatisé, quel que soit le procédé utilisé, notamment la collecte, l'enregistrement, l'organisation, l'enregistrement, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

➤ **Les rôles respectifs du Responsable de Traitement (RT) et du Relais Informatique et Libertés (RIL)**

- ✓ **Le RT** définit les finalités et les moyens du traitement ;
- ✓ **Le RIL** garantit l'exactitude des traitements recensés et assiste le RT dans sa mission. Ainsi, il aide le CIL à veiller à la conformité I&L au quotidien.

❑ Les grands principes traditionnels de la loi Informatique et Libertés du 6 janvier 1978 :

- Finalité du traitement (déterminée, explicite et légitime)
- Proportionnalité (données adéquates, pertinentes et non excessives, limitation des destinataires, données exactes, complètes et mises à jour)
- Durée de conservation limitée des données
- Sécurité, intégrité et confidentialité des données
- Respect des droits des personnes (information, accès et rectification, suppression, opposition)

❑ Les nouveaux principes consacrés par la loi pour une République numérique du 7 octobre 2016 :

Le règlement européen relatif à la protection des données personnelles (RGPD) adopté le 27 avril 2016 sera directement applicable à compter du 25 mai 2018. **La loi pour une République numérique prévoit par anticipation une série de dispositions modifiant la loi Informatique et Libertés et s'articulant autour du nouveau droit général à la maîtrise de ses données personnelles.**

- Certaines mesures sont entrées en vigueur dès le 9 octobre 2016 :
 - droit d'organiser le sort post mortem de ses données personnelles par des directives générales et particulières ;
 - droit à l'oubli pour les personnes qui étaient mineures lors de la collecte de leurs données
 - renforcement de l'information des personnes concernées (délai de conservation, droit d'organiser le sort post mortem de ses données personnelles).
- Des mesures transitoires seront abrogées le 25 mai 2018 étant donnée que le RGPD les prévoit lui-même :
 - facilitation de l'exercice des droits des personnes concernées par voie électronique ;
 - renforcement du pouvoir de sanction de la CNIL.
- D'autres mesures renvoient au RGPD et entreront donc en vigueur le 25 mai 2018 :
 - consécration du droit à la récupération et à la portabilité des données personnelles.

❑ **Les nouveaux principes du RGPD applicables à compter du 25 mai 2018 :**

- **Accountability** : responsabilisation et charge de la démonstration de la conformité
- **Analyses d'impact sur la vie privée**
- **Privacy by design** : respect de la vie privée dès la conception du projet
- **Droit à la portabilité des données personnelles**
- **Droit à la limitation de l'utilisation des données personnelles**
- **Droit d'organiser le sort post mortem de ses données personnelles**
- **Droit à l'oubli pour les personnes qui étaient mineures lors de la collecte de leurs données**
- **Responsabilité des sous-traitants**
- **Fort pouvoir de sanction, notamment financière, de la CNIL** : le montant maximal de l'amende passera de 150 000€ à 3M€ en 2017 et à 20M€ ou 4% du CA annuel mondial de l'entreprise en 2018.

À compter du 25 mai 2018, **le groupe devra appliquer une gestion par les risques** qui remplacera le régime légal actuel des formalités préalables auprès de la CNIL. Cette gestion se traduira notamment par la réalisation d'études d'impact sur la vie privée, le renforcement de l'information des personnes ou encore la révision des contrats de sous-traitance.

Le groupe devra également nommer **un Data Protection Officer (DPO)** dont les missions seront plus larges que celles dévolues actuellement au CIL.

Le NIR est une donnée dont l'utilisation et la consultation sont très contrôlées et strictement limitées à certaines hypothèses définies par les textes légaux et réglementaires.

Il n'est pas possible de collecter et/ou d'exploiter le NIR dans un traitement dès lors que ce traitement n'a pas pour finalité :

- La tenue des comptes d'épargne salariale (article L444-5 Code du travail) ;
- L'établissement du bulletin de paie et les différentes déclarations sociales obligatoires (décret n° 91- 1404 du 27 décembre 1991) ;
- Les activités d'assurance maladie, maternité et invalidité complémentaire (articles R115-1 et R115-2) que la CNIL interprète strictement, en excluant la gestion commerciale de ces activités ;
- La poursuite d'un intérêt général (service public).

- ⇒ **Il est interdit d'utiliser le NIR des clients en qualité d'identifiant unique à des fins de gestion de la relation commerciale**
- ⇒ **L'interconnexion de fichiers contenant notamment le NIR, en vue d'effectuer un traitement ayant, à terme, une finalité « commerciale » est soumise à demande d'autorisation auprès de la CNIL. Elle a peu de chance d'aboutir à autorisation et est donc fortement déconseillée**
- ⇒ **Bonne pratique: occulter le NIR en le remplaçant par un autre numéro d'identifiant**

- ❑ **L'opt-in** est le principe par lequel un individu doit donner son consentement préalable avant d'être la cible d'une prospection commerciale directe effectuée par un canal marketing automatisé (email, sms, tel).
 - La récolte préalable de l'opt-in est une obligation imposée par la loi et les recommandations d'application émises par la CNIL.
 - La loi prévoit deux exceptions au principe de l'opt-in. L'une pour les individus déjà clients de l'entreprise à qui il est possible de faire une offre « analogue » et l'autre pour les adresses email professionnelles.
 - La CNIL précise l'exigence liée au consentement préalable. Elle estime notamment que cette autorisation doit se faire de manière active par une case à cocher, en vue de garantir un consentement exprès, libre et éclairé.

- ❑ **L'opt-out** est le principe par lequel un individu ne donne pas son autorisation à l'utilisation de ses données personnelles.
 - Pratique consistant à envoyer un email commercial à un individu sans lui avoir demandé auparavant son autorisation mais en lui permettant cependant, dans le cadre du message, de demander à ne plus être dans la liste des destinataires.

- ❑ **Typologie d'opt-in/opt-out devant être gérés dans nos SI (y compris hors prospection commerciale)**
 - opt-in/opt-out '**SMS**' ;
 - opt-in/opt-out **abonnement conseil spécifique** pour chaque type de communication (rendez-vous thématiques/newsletter) ;
 - opt-in/opt-out **commercial** (emails de prospection commerciale) ;
 - opt-in/opt-out **contrat et information institution contractante** (emails de services analogues au contrat souscrit et information institution) ;
 - opt-in/opt-out **groupe** (emails d'actualité du groupe Humanis) ;
 - opt-in/opt-out **profilage obligatoire à compter du 25 mai 2018** (conformément à l'article 22 du RGPD précité).

Des règles impératives doivent être respectées en matière de protection des données à caractère personnel collectées et traitées au sein du groupe :

- ☐ Les **mentions légales CNIL** doivent contenir les informations énumérées par les textes en vigueur. Elles doivent figurer sur tous les supports de collecte de données à caractère personnel et peuvent faire l'objet d'adaptations en fonction notamment de la finalité poursuivie par le traitement et des destinataires concernés.
- ☐ Les **mentions spécifiques d'opt-in** sont nécessaires en vue de recueillir le consentement préalable de la personne visée par une action commerciale (une charte des bonnes pratiques relatives à la collecte des emails sera prochainement diffusée).
- ☐ Les **mentions d'opt-out** doivent notamment apparaître sur tous les emails commerciaux sortants à destination des personnes physiques (clients et prospects).

Compte-tenu de l'évolution réglementaire, ces différentes mentions devront être revues au fil de l'eau. Une périodicité de révision doit être établie afin de permettre d'anticiper l'application du RGPD précité. A cette fin, un process global de communication et de mise à jour des mentions légales structures/CNIL/opt-in est en cours de rédaction.

- ☐ Des **clauses IL** doivent être insérées notamment dans les contrats de sous-traitance et de partenariat ainsi que dans les CGU des plateformes numériques et des différents espaces accessibles sur internet.

➤ **Mise en conformité du Registre de traitement**

➤ **Actions de sensibilisation aux enjeux Informatique et Libertés**

Les RT et les RIL ont été respectivement invités à des réunions de sensibilisation organisées conjointement par le CIL, la DAJF en collaboration avec le cabinet d'avocats Courtois-Lebel.

Les actions organisées respectivement à l'attention des RIL et des RT sont désormais closes.

➤ **Initialisation et réunions du COMIL**

Depuis le 01/01/16, le COMIL réunit des représentants de la DAJF, la DRCC, la DSI et la Transformation pour accompagner le CIL et prendre les décisions requises dans le cadre du dispositif « HIL ».

À compter de 2017, des Directions supplémentaires intégreront le COMIL en tant que membres permanents. De plus, des RIL seront ponctuellement invités en vue de traiter des problématiques spécifiques à leur Direction.

➤ **Création d'un formulaire dématérialisé pour l'exercice des droits des personnes**

Faciliter et garantir l'exercice des droits des personnes est l'une des priorités du dispositif « HIL ». En raison des défaillances de la boîte mail contact-CNIL, un formulaire de contact accessible depuis les mentions légales a été créé. Il permet à la personne concernée de préciser la nature de sa demande (accès, suppression, opposition etc,) et de joindre, le cas échéant, les éléments d'identification requis.

➤ **Création d'un espace Informatique et Libertés sur ForHum**

➤ **Diffusion mensuelle des Flashs Informatiques & Libertés**

Rappel de la trajectoire 2017 :

- **1^{er} jalon : mise en place du dispositif HIL**
- **2^{ème} jalon : sensibilisation des acteurs et mise en conformité du registre de traitements**

Trajectoire 2017/2018 :

- **3^{ème} jalon : intégration des dispositions du nouveau règlement européen dans le dispositif HIL**
 - Définition et mise en œuvre d'une procédure de contrôle du suivi de la conformité I&L afin de permettre une traçabilité des actions.
 - Rédaction et diffusion de la Charte Ethique de données personnelles.
 - Ouverture de l'accès au registre des traitements et au Registre des demandes I&L à l'ensemble des RT et des RIL.
 - Mise en place d'un outil pour réaliser les études d'impact sur la vie privée.