CORRESPONDANT INFORMATIQUE ET LIBERTÉS

GUIDE PRATIQUE DE LA PRISE DE FONCTION

DE LA DÉSIGNATION AU PILOTAGE

PRÉPARER LA DÉSIGNATION

Avant la désignation officielle, que doit faire un organisme pour organiser au mieux la prise de fonction du futur correspondant Informatique et Libertés (CIL) ?

PRÉ-INVENTAIRE

☐ **Faire réaliser une cartographie et un état des lieux**, même macroscopique, des traitements de données mis en œuvre par l'organisme (sur la base d'une liste « article 31 »[1]) : description, objectifs, origine et sensibilité des données traitées, estimation du nombre de personnes concernées, existence ou non de sous-traitance, transmission des données à des destinataires, transfert hors UE, historique des bilans et contrôles…).

☐ **Évaluer la charge de travail** du futur CIL sur la base de cet inventaire qui révélera l'ampleur des directions, fonctions, processus et métiers impactés.

CHOISIR VOTRE CIL

☐ **S'assurer de l'intérêt de la personne pressentie** et de ses qualifications dans le domaine de la conformité Informatique et Libertés[2].

☐ **Prévoir un rattachement** de la fonction de CIL à un membre de l'instance exécutive (dans l'idéal).

☐ **S'assurer qu'il n'y aura pas de conflit d'intérêt** empêchant la validation de la désignation. En effet, « *les fonctions ou activités exercées concurremment par le CIL ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission* »[3].

ACTER

☐ **Faire acter/valider la désignation** du CIL par un organe exécutif de l'organisation.

☐ **Formaliser** dans un document spécifique les missions confiées au CIL (lettre de mission, avenant au contrat…).

☐ **Mettre en place le processus de consultation de l'instance représentative du personnel compétente** (préparer le courrier, planifier la date de remise dudit courrier…).

☐ **Prévoir, si nécessaire, un budget spécifique** (formations du CIL et de son éventuel réseau de relais, déplacements à prévoir, création de supports de communication interne…).

☐ **Faire signer au CIL, si besoin, un engagement de confidentialité** spécifiquement lié à sa mission (accès à des informations confidentielles ou ne relevant pas de son périmètre habituel).

☐ **Permettre au CIL d'accéder dans l'organisme à toutes informations utiles** à ses missions et de bénéficier du nécessaire support de tous ses futurs interlocuteurs (ex : par envoi d'un courriel à toutes les directions). ›››

[1] *La liste des traitements déclarés auprès de la CNIL est communément appelée « liste article 31 »*
[2] *cf. guide du CIL, www.cnil.fr*
[3] *cf. article 46 du décret 2005-1309 du 20 octobre 2005 - cf Guide du CIL*

›››

SENSIBILISER RÉGULIÈREMENT

☐ **Informer l'exécutif des missions essentielles du CIL** et de son indépendance organisationnelle afin que sa mission soit soutenue et comprise au plus haut niveau.

☐ **Faire intervenir le CIL** avant ou après sa désignation officielle dans une instance de type comité de direction générale afin qu'il présente son rôle et la mission qui lui ont été confiés.

☐ **Informer la hiérarchie actuelle** du futur CIL de l'éventuelle nécessité d'alléger sa charge de travail liée à ses autres missions, si besoin (fonction à temps partiel).Cela est d'autant plus important pendant les 2 premières années d'exercice qui sont particulièrement importantes.

☐ **Mettre en place un plan de communication interne** pour informer l'ensemble des employés du rôle du CIL, de son statut et de ses missions.

CAS PARTICULIERS

☐ **Grands groupes** : anticiper la désignation et la mise en œuvre du plan de communication avec les dirigeants des filiales. Réaliser absolument l'état des lieux des traitements avant la désignation.

☐ **Secteur public** : étudier la mutualisation possible du CIL avec les organismes satellites dépendant de la collectivité d'origine et dont le Président, le Maire ou autres élus peuvent être aussi responsable de traitement.

☐ **Remplacement d'un CIL** : organiser la passation de dossiers.

ORGANISER SA DÉSIGNATION

Quelles actions le futur CIL peut-il mettre en œuvre en amont pour préparer au mieux sa prise de fonction ?

S'INFORMER

☐ **Consulter la documentation en ligne** sur le site **www.cnil.fr** et télécharger le Guide du CIL pour s'informer sur le rôle du CIL.

☐ **Distinguer les différentes actions à lancer** selon qu'il s'agit de la 1ère nomination d'un CIL au sein de l'organisme ou d'un remplacement.

☐ **Prendre connaissance du pré-inventaire** (voir fiche 1) et évaluer le différentiel entre la liste des traitements déclarés et ce qui a été effectivement mis en œuvre par l'organisme.

☐ **Étudier les dossiers en cours** et consulter le bilan I&L[1] de l'année passée en cas de remplacement.

☐ **Identifier les moyens nécessaires à l'activité** (temps disponible, moyens humains, budget déplacement, espaces partagés de stockage, outil de cartographie de traitements, support pour le registre…).

ÉCHANGER AVEC LE RESPONSABLE DE TRAITEMENT

☐ **Rédiger une note** à destination du responsable de traitement* présentant notamment la procédure de désignation, les missions du CIL, les formations nécessaires, le budget prévisionnel, les modalités de fin de mission.

☐ **Organiser une réunion avec le responsable de traitement** pour échanger sur les conditions d'exercice de ses missions (outils et moyens mis à disposition), la mise en place d'un réseau de relais Informatique et Libertés.

☐ **Définir les modalités de travail** notamment en ce qui concerne les relations entre le CIL et le RT[2] (interlocuteurs relais identifiés par le RT, fréquence des réunions, circuit de communication, etc.).

☐ **Planifier l'organisation** de la procédure de désignation et la répartition des rôles (qui remplit le formulaire, qui l'envoie…).

IDENTIFIER SES FUTURS RELAIS INTERNES

☐ **Envisager l'opportunité** (selon la taille de l'entreprise) de mettre en place un réseau de personnes « relais » identifiées comme les interlocuteurs privilégiés du CIL.

☐ **Déterminer les interlocuteurs** internes et les directions qui pourront aider le CIL dans sa démarche (le secrétaire général pour la lettre de mission, la DRH[3] pour organiser la présentation aux IRP[4], etc.).

☐ **Rencontrer** les principaux représentants des directions et/ou les responsables des fonctions métiers et supports de l'organisme.

** Un responsable de traitement est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal. [1] Informatique et Libertés - [2] Responsable de traitement - [3] Direction des ressources humaines - [4] Instances représentatives du personnel.*

SE FORMER

Comment acquérir les connaissances nécessaires à l'exercice de la mission de CIL ?

LES OUTILS MIS À DISPOSITION DES CIL PAR LA CNIL

UN EXTRANET RÉSERVÉ AUX CIL

- ☐ **Tester** ses codes d'accès envoyés par courriel lors de la validation de la désignation.
- ☐ **Consulter** les rubriques « outils », « formation », « réseaux » sur l'extranet.
- ☐ **Parcourir** le forum de l'Extranet des CIL pour identifier les thématiques intéressant son secteur.

LE SITE DE LA CNIL

- ☐ **Identifier les fiches pratiques** vous concernant, lire/imprimer/classer.
- ☐ **Identifier les guides** relevant du secteur d'activité de l'organisme : à sauvegarder, imprimer et classer.
- ☐ **Identifier les cadres de référence pertinents** (norme simplifiée, autorisation unique, acte réglementaire unique).

LES ATELIERS CIL GRATUITS

- ☐ **Choisir ses ateliers** : sur l'extranet, partie « Ateliers », identifier les dates et le contenu des prochaines sessions.
- ☐ **Planifier son calendrier de formation** : pour les novices, assister idéalement aux ateliers « Fondamentaux partie I et II » dans le mois suivant la désignation ; pour les CIL déjà sensibilisés à la loi, possibilité de commencer par les ateliers spécifiques.

DES FORMATIONS EXTÉRIEURES À LA CNIL

- ☐ **Possibilité de suivre des formations externes** aux « fondamentaux » de la protection des données dispensées par des organismes privés ou publics. Une liste indicative et non exhaustive figure sur l'extranet, partie « *Formations* ».
- ☐ **Assister à des conférences** et/ou tables rondes en rapport avec vos problématiques.
- ☐ Au sein de son organisme, **suivre des formations internes** sur des aspects juridiques ou techniques qui peuvent être nouveaux pour le CIL (ex : les notions de base des systèmes informatiques).

>>>

PRÉCISION : *Ces cadres de référence couvrent les grandes catégories de traitements les plus souvent mis en œuvre par les organismes (exemple : la norme simplifiée n° 46 encadre les traitements mis en œuvre pour la gestion du personnel). Vous devez vous assurer que le traitement envisagé est bien mis en œuvre dans les conditions décrites dans le cadre de référence. Le cas échéant, vous pourrez procéder à un « engagement de conformité » par lequel vous déclarerez mettre en œuvre ledit traitement comme décrit dans le cadre de référence.*

›››

☐ **Participer à des formations externes** pour se spécialiser sur un sujet spécifique à la protection des données personnelles concernant l'organisme. Éventuellement, suivre une formation diplômante qui permet d'appréhender de façon complète la matière.

SE DOCUMENTER ET METTRE EN PLACE UNE VEILLE

☐ **Organiser une veille** sur les sujets touchant aux données à caractère personnel (juridique, technique, sociétal, sectoriel…), à la sécurité (Clusif[1], Anssi[2]…), à son secteur d'activité.

☐ **S'abonner** à des revues, des newsletters, suivre des flux RSS divers tels que le fil d'actualité de la CNIL, de Légifrance.

☐ **Se familiariser** avec les principaux textes applicables à la protection des données personnelles (loi Informatique et Libertés n° 78-17 modifiée, décret d'application n° 2005-1309).

☐ **Constituer** une bibliographie de références.

METTRE EN PLACE SON RÉSEAU

☐ **Échanger les bonnes pratiques** avec les CIL d'autres organismes lors de groupes de travail, d'ateliers CIL, de réunions, d'échanges informels, conférences, déjeuners…

☐ **Étudier l'opportunité d'adhérer** à une association pour bénéficier de l'expérience de ses pairs.

☐ **Se rapprocher** de CIL situés dans la même zone géographique ou le même secteur d'activités et mettre en place des rencontres/déjeuners réguliers au niveau local.

[1] *Club de la Sécurité de l'Information Français*
[2] *Agence nationale de la sécurité des systèmes d'information*

RECENSER

Comment faire l'état des lieux des traitements de données mis en œuvre dans son organisme et le mettre à jour ?

PRÉPARER LA RENCONTRE AVEC LES SERVICES CONCERNÉS

Action préalable : demander la liste des traitements déclarés avant votre désignation par votre organisme, dite « liste article 31 »[1].

☐ **Collecter les organigrammes des directions** et si disponible un descriptif de l'activité des différents métiers.

☐ **Envoyer aux responsables opérationnels un questionnaire**[2] succinct pour savoir s'ils traitent des données à caractère personnel.

☐ **Mettre en place un planning de rendez-vous par grandes thématiques** (exemple de contenu : service concerné, date du rendez-vous, personne rencontrée, commentaires, personne référente indiquée par les responsables des directions/départements/services, date du rendez-vous avec ce référent, suivi).

☐ **Préparer des questionnaires**[2] qui vous serviront de fil rouge lors de vos entretiens avec les opérationnels. L'objectif : vous permettre d'identifier le besoin, à quoi ça sert, qui les utilise, sur quelle durée… ?

COLLECTER L'INFORMATION

☐ **Centraliser les dossiers de formalités** figurant sur la « liste article 31 ».

☐ **Récupérer auprès de la Direction informatique (ou DSI[3]) et du service qualité**, les documents existants pouvant aider au recensement : cartographie fonctionnelle et applicative du Système d'Information, cartographie des flux, cartographie des risques, si elle existe, liste des applications métiers et techniques, existence de vidéosurveillance…

IDENTIFIER LES TRAITEMENTS

☐ **Analyser le site web de votre organisme** pour identifier les données collectées dans les formulaires, les mentions d'informations, l'utilisation de cookies, etc.

☐ **Passer en revue** les normes simplifiées et autorisations uniques publiées par la CNIL et correspondant à l'activité de votre organisme : cet exercice vous donnera un panorama des traitements existants les plus courants et vous aidera à les identifier http://www.cnil.fr/documentation/deliberations/.

☐ Se rapprocher de CIL désignés par un organisme similaire au vôtre (ex : via le forum de l'extranet réservé aux CIL ou via l'annuaire) afin qu'il vous communique la liste des finalités qui figurent à son registre.

›››

[1] Faire cette demande au service des correspondants en précisant votre nom et qualité, celui de votre organisme, ainsi que le n°Siren/Siret de votre structure.
[2] Modèle disponible sur l'Extranet réservé aux CIL
[3] Direction des systèmes d'information

›››

ANALYSER ET SYNTHÉTISER

☐ **Mettre en place un tableau de suivi des traitements identifiés par service**. Vous porterez dans ce tableau les traitements identifiés par finalité (et non par logiciel utilisé, car un même logiciel peut être utilisé pour différents traitements et inversement) lors de vos entretiens.

☐ **Classer les traitements** en distinguant ceux pour lesquels une formalité a été réalisée (cf. « liste article 31 »), ceux qui doivent être régularisés et ceux qui ne sont plus d'actualité.

METTRE EN CONFORMITÉ - RÉGULARISER

☐ **Analyser la conformité** des traitements identifiés sur la base des principes de la protection des données personnelles étudiés (atelier, formation, etc.).

☐ **Établir des priorités** pour les régularisations, eu égard à la sensibilité des dossiers et des risques encourus.

☐ **Analyser la pertinence des formalités** déjà effectuées pour chaque traitement déclaré auprès de la CNIL.

☐ **Se rapprocher de la CNIL** pour un éventuel accompagnement dans la démarche.

PORTER AU REGISTRE

☐ **Créer votre modèle de fiche de registre** (vous disposez d'un exemple accessible sur l'extranet).

☐ **Structurer le registre**, en distinguant notamment les traitements liés au fonctionnement de l'organisme (ex : RH, sécurité des locaux) et ceux liés à son cœur d'activité (ex : gestion des clients).

☐ **Porter à ce registre les nouveaux traitements, les traitements modifiés depuis la désignation du CIL** et ceux qui n'ont pas fait l'objet de formalités, si et seulement s'ils sont soumis à déclaration normale ou s'ils sont conformes à une norme simplifiée.

COMMUNIQUER

Comment informer les publics internes ?

SE FAIRE CONNAÎTRE

☐ Créer une adresse de messagerie spécifique et un numéro de téléphone dédié au CIL.

☐ Intégrer le logo CIL dans son adresse électronique, ses cartes de visite, sur son bureau, sur l'intranet (cf. règlement d'usage du logo sur l'extranet des CIL).

IDENTIFIER ET EXPLOITER LES SUPPORTS INTERNES DE COMMUNICATION

☐ **Rencontrer la direction de la communication** (ou équivalent) : lui présenter votre rôle, votre activité et identifier le soutien qu'elle peut vous apporter ainsi que les supports que vous pourriez mettre à profit pour communiquer.

Exemples de support de communication :

- Newsletter : pour publier des articles ou des brèves sur le thème « Informatique et Libertés » (actualités I&L du secteur, la journée de la protection des données personnelles…).
- Intranet : créer un espace thématique dédié à l'échange d'informations avec le CIL.
- Réseau social d'entreprise : création d'une communauté.
- Événements dédiés : jeu-concours, quizz.
- Parcours d'intégration d'un nouvel arrivant : programmer un rendez-vous avec les responsables des RH pour prévoir une sensibilisation aux bonnes pratiques.

☐ **Identifier le contenu disponible**, exemple : affiches de la CNIL, fiches juridiques de la CNIL, site internet de la CNIL, extranet CIL, affiches spécifiques déjà réalisées en interne sur les thématiques « Informatique et Libertés ».

☐ **Identifier les publics cibles en interne et leurs besoins** : tout service amené à manipuler des données à caractère personnel (ex : Direction informatique, direction RH, direction commerciale, etc.).

☐ **Créer du contenu** : élaborer et publier des mémos ou des fiches thématiques qui concernent le monde professionnel ou personnel (exemple : comment bien remplir une zone de commentaire ? quels conseils pour protéger ses données personnelles avant de partir en vacances ? qu'est-ce que le droit d'accès ? etc.).

☐ **Communiquer aux moments opportuns :**

- **Les contrôles de la CNIL ou l'actualité** sont des leviers d'actions pour sensibiliser sur des problématiques qui sont similaires à celles de votre organisme.
- S'il existe des **opérations internes de sensibilisation** sur la sécurité des informations, intégrer les bonnes pratiques concernant la protection des données.
- **La journée européenne de protection des données (28 janvier).**

›››

›››

ORGANISER UN RÉSEAU DE RELAIS INFORMATIQUE ET LIBERTÉS

☐ **Établir une fiche de mission type** pour un RIL : profil, missions, % estimé du temps à y consacrer.

☐ **Identifier une personne relais « Informatique et Libertés » (RIL) pour chaque direction** métier ou filiales parmi les collaborateurs ayant une bonne connaissance de la loi Informatique et Libertés, des pratiques métiers et/ou des systèmes d'information (SI) utilisés par sa direction.

☐ **Communiquer sur la présence d'un RIL et son rôle.**

☐ **Réunir régulièrement** son réseau de RIL (échanges d'info – point d'avancement des actions en cours).

FOCUS

☐ **Valoriser** les actions menées en s'associant à la communication vers les clients, membres, usagers…

☐ *Pour les CIL très expérimentés* : **intervenir** dans des formations, conférences, répondre à des interviews, écrire des articles dans des revues spécialisées.

PILOTER

Quelles procédures mettre en place pour veiller à la conformité Informatique et Libertés ?

ORGANISER LA REMONTÉE DE L'INFORMATION

☐ **Participer aux réunions transversales** (comité de direction, comité stratégique…) **et créer une synergie** (ex : création d'un comité de pilotage I&L) avec les services achats, juridique, RH, informatique par exemple.

☐ **Faire inscrire régulièrement** un point « Informatique et Libertés » à l'ordre du jour d'une réunion de direction (ex : état d'avancement des activités du CIL).

☐ **Formaliser la consultation du CIL par les directions concernées** (ex : juridique, achats, informatique, sûreté, marketing, communication, archives, urbanisme, etc.) dès l'initialisation d'un projet impliquant un traitement de données.
Exemple : Pour une direction juridique : associer/faire valider par le CIL la mise en place de clauses types «Informatique et Libertés» dans les contrats, les conventions («*privacy by design*» et «*by default*»).

☐ **Mettre en place un « Comité I&L »** composé des RH, du juridique, des services achats, de l'informatique, de la qualité et des moyens généraux. Programmer des réunions régulières avec ces directions métiers pour les grandes orientations et projets impliquant un traitement de données personnelles ou ayant un impact sur la sécurité des données.

☐ S'associer à l'**élaboration ou à la mise à jour des documents de gouvernance** (politique de sécurité du système d'information - PSSI, chartes, etc.).

☐ **Entretenir un contact régulier** avec les opérationnels traitant des données à caractère personnel, savoir être à l'écoute, en soutien.

☐ **Organiser un reporting régulier** des relais « Informatique et Libertés » pour les projets et les actions engagés.

☐ **Préparer la rédaction et la communication du bilan annuel** au responsable de traitement : définir le calendrier (exercice en année civile, fiscale, universitaire, etc.), enregistrer au fur et à mesure les actions réalisées pour alimenter le bilan.

☐ **Établir un rapport d'activité régulier** à destination de l'instance exécutive : définir le calendrier (exercice en année civile, fiscale, universitaire, etc.), enregistrer au fur et à mesure les actions réalisées pour alimenter le rapport d'activité.

ANTICIPER LES RISQUES

☐ **Prévoir une procédure interne en cas de contrôle de la CNIL** (ex : définition des règles d'accueil de la délégation, qui solliciter selon l'objet du contrôle…).

☐ **Intégrer**, dans les procédures d'expression de besoins ou de validation de contrat, une ligne indiquant la collecte ou non de données à caractère personnel et, le cas échéant, l'information obligatoire du CIL pour consultation.

☐ **En cas de failles de sécurité et violations de données à caractère personnel, mettre en place une procédure d'information du CIL dans un délai de 24 heures.**

☐ **En cas de situation de blocage interne** pour le CIL, prévoir une procédure d'alerte du responsable de traitement et/ou de résolution du conflit. ›››

>>>

CRÉER DES DOCUMENTS SUPPORT

☐ **Créer des FAQ** pour mise à disposition des RIL, modèles de courriers de réponse (ex : droit d'accès).

☐ **Créer une documentation décrivant le processus de mise en conformité I&L** et diffuser via un espace/support accessible aux salariés concernés (affichage, intranet…).

GÉRER LES DEMANDES DE DROITS D'ACCÈS/RECTIFICATION

☐ **Proposer une méthode de réponse aux services** : fixer un délai de traitement, présenter un courrier-type, « que faire en cas de demande incomplète ? », etc.

☐ **Préparer des modèles de réponse** aux demandes des personnes, en fonction des métiers.

☐ **Mettre en place un tableau de pilotage** des demandes de droit d'accès et délais de réponse **et informer les services en relation avec le public** (service clients, accueil physique et/ou téléphonique etc.) qu'ils peuvent être contactés directement.

☐ **Veiller à ce qu'une adresse électronique générique dédiée** à ces demandes soit clairement indiquée sur le site Web de votre organisme et que tous les emails envoyés à cette adresse vous soient bien transmis.

☐ **Établir une procédure visant à informer ces services** que le CIL doit être informé de toute demande, plainte ou courrier concernant l'exercice des droits d'accès, d'opposition et de rectification. Mettre à disposition cette procédure sur un espace accessible à toute personne (intranet, affichage, etc.).

☐ **En cas de congés**, prévoir une personne « relais ».

FORMER

☐ **Identifier** les services/directions auprès desquels il faudra mener des **démarches ciblées** avec la mise en place d'animations ou de formations régulières en interne.

☐ **Organiser la formation** spécifique et l'animation du réseau de « RIL » (point d'actualité, mise à jour sur les solutions de sécurité (chiffrement des données, etc.).

AUDITER

☐ **Réaliser ou faire réaliser** régulièrement des audits I&L.

☐ **Diffuser et suivre** le plan d'actions correctives ou évolutives.

ORGANISER LE SUIVI DE SON ACTIVITÉ

☐ **Tenir un tableau de bord** de ses activités qui permettra ensuite de rédiger le bilan d'activité.

☐ **Réaliser un suivi mensuel** de l'activité I&L avec le responsable de traitement, au début surtout.

☐ **Établir un rapport d'activité régulier** qui alimentera la présentation du point « Informatique et Libertés » à l'ordre du jour d'une réunion de direction.