Procédure en cas de contrôle CNIL

PRÉAMBULE

Conformément aux dispositions réglementaires, et notamment à la loi 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, la CNIL peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 44 *(contrôle sur place)*, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions.

Selon l'Article 44, les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 *(habilitation par la Commission)* ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Le procureur de la République territorialement compétent en est préalablement informé.

Les membres de la commission et les agents mentionnés au premier alinéa du I peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie; ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles; ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Ils peuvent, à la demande du président de la commission, être assistés par des experts désignés par l'autorité dont ceux-ci dépendent.

Seul un médecin peut requérir la communication de données médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion de service de santé, et qui est mis en œuvre par un membre d'une profession de santé.

Il est dressé contradictoirement un procès-verbal des vérifications et visites menées en application du présent article.

LES PHASES DE LA PROCÉDURE

1. Diffusion de l'information au Responsable des Lieux et au DPO par le Standard ou l'accueil des différents établissements après authentification des identités des contrôleurs de la CNIL.

2. Déclenchement de la procédure par le Responsable des Lieux ou le DPO.

3. Diffusion de l'information par le Responsable des Lieux ou le DPO avec l'aide du Standard et activation des fiches consignes.

4. Accueil des contrôleurs de la CNIL par le Responsable des Lieux.

5. Mise en place de la Cellule de Crise autour du Responsable des Lieux et du DPO.

6. Organisation de la mission de contrôle de la CNIL.

7. Réunion de la Cellule de Crise chaque jour après le départ des agents de la CNIL.

8. Réunion de debriefing à la fin de la visite de la CNIL.

9. Information du Directeur Général du déroulement du contrôle par le Responsable des Lieux et le DPO.

LA CELLULE DE CRISE

a. Sa composition

1. Le Délégué à la Protection des Données
2. Le Directeur Général
3. Toute autre personne compétente de la structure

b. Sa mission

La Cellule de Crise coordonne le suivi et l'organisation de la mission de contrôle de la CNIL. Chaque agent de la CNIL (entre 2 minimum et 6 personnes) sera accompagné dans ses déplacements par une personne de la Cellule de Crise afin qu'il ne soit jamais laissé seul dans leur déplacement à l'intérieur des locaux.
La Cellule de Crise se réunira en fin de journée afin de faire le point sur le déroulement du contrôle de la CNIL et pour répondre au mieux aux demandes éventuelles de la CNIL.

Chaque accompagnateur des agents de la CNIL tiendra un journal du déroulement du contrôle et permettra ainsi au Responsable des Lieux de centraliser toutes les informations et de valider ou d'apposer des remarques au procès-verbal de fin de visite de la CNIL.

FICHE CONSIGNE N° 1

TITULAIRE : STANDARD, ACCUEIL

Missions :
✓S'assurer de l'authentification de l'information.
✓Diffuser l'information au DPO

1. Authentifie l'information :

- S'assure des identités des visiteurs (CNI, cartes d'accréditation CNIL) et de la présence d'une lettre de mission de la CNIL.
- Les faire patienter dans un lieu neutre et ne pas les laisser seuls.

2. Diffuse l'information :

Appelle le standard au poste : …. ou sinon le standardiste au poste : …., ligne interne abrégée : ….

FICHE CONSIGNE N° 2

TITULAIRE : DELEGUE A LA PROTECTION DES DONNEES

Missions :
Le DPO est Désigné par l'entité pour être l'interlocuteur privilégié auprès de la CNIL afin d'assurer d'une manière indépendante le respect des obligations prévues dans la loi Informatique et Libertés. Il suivra la mission de contrôle de la CNIL.

Suivi de la mission de contrôle de la CNIL :
✓ Prend connaissance de l'ordre de mission notamment sur l'origine de la vérification (initiative de la CNIL ? Plainte ?) et son périmètre. L'information quant à la cause du contrôle n'est pas une obligation pour la CNIL néanmoins l'objet doit être inscrit dans le PV ;
✓ Vérifie tous les documents et données qu'emportent les agents de la CNIL ;
✓ Accompagne les agents de la CNIL dans les différentes visites ;
✓ Tient un journal du déroulement du contrôle ;
✓ Participe à la réunion chaque fin de journée de la Cellule de Crise afin de faire le point sur le déroulement du contrôle de la CNIL et pour répondre au mieux aux demandes éventuelles de la CNIL ;
✓ Vérifie le procès-verbal de fin de visite de la CNIL (la liste exhaustive des données prélevées doit figurer au procès-verbal) ;
✓ Garde une copie du procès-verbal de fin de visite de la CNIL,
✓ Participe à la réunion de debriefing à la fin de la visite pour faire un CR et répondre aux demandes éventuelles de la CNIL.
✓ Informe le Directeur Général du déroulement du contrôle avec le Responsable des Lieux.

FICHE CONSIGNE N° 3

TITULAIRE : DIRECTEUR GENERAL

Missions :

✓Suivre le déroulement du contrôle de la CNIL

✓Répondre aux demandes de la CNIL : mise en demeure, convocation devant la formation restreinte

✓ Suivi du déroulement du contrôle de la CNIL

✓ Réponse aux demandes de la CNIL

✓ Informe le DPO de toute demande de la CNIL

DEMANDES ÉVENTUELLES DE LA CNIL

A retenir :
Les agents de la CNIL sont des professionnels aguerris au contrôle. Il faut de la vigilance et de la prudence et se méfier du caractère sympathique des entretiens.
Il ne faut pas en dire plus que ce qui est demandé. Il ne faut répondre qu'aux questions de manière simple et claire car sinon, il peut y avoir des incompréhensions et le doute est créé.
Il n'y a pas d'obligation à répondre immédiatement donc il faut s'accorder le temps de la réflexion pour répondre ou trouver le bon document.

Recensement des demandes éventuelles de la CNIL :
Liste des thèmes :
- Présentation organisme ;
- Liste des traitements ou processus de recensement des traitements
- Architecture du système informatique ;
- Activité du DPO : moyens accordés pour réaliser sa mission ;
- Licéité des traitements : finalité et fondement légal, données pertinentes et non excessives, qualité de la méthode de recueil des données ;
- Politique de Sécurité de l'entité
- Politique d'habilitation : Recensement et catégorisation de l'ensemble du personnel ainsi que la gestion des Autorisations
- Contrats des sous-traitants

A retenir :
Après une mise en demeure de la CNIL, le responsable de traitement dispose d'un délai fixé allant de 10 jours minimum à 3 mois maximum pour faire part de ses observations écrites (si nécessaire) et se conformer.

En cas de non-respect de la mise en demeure, une sanction est susceptible d'être prononcée. Un rapport est rédigé et le responsable des traitements dispose d'un délai d'un mois pour transmettre à la commission ses observations écrites. Ce délai peut être porté à 15 jours en cas de procédure d'urgence.

Avant que la formation restreinte ne se réunisse, le rapporteur peut entendre le responsable des traitements ou toute autre personne s'il l'estime utile. Le responsable de traitement est informé par lettre recommandée de la date de la séance de la commission et de la faculté qu'il a d'être entendu, un mois avant cette date.