ANTICIPER ET PRÉPARER
UN CONTRÔLE DE LA CNIL

A retenir :

La Commission nationale de l'informatique et des libertés (CNIL) a le pouvoir de contrôler les traitements de données personnelles effectués dans le cadre des activités des responsables de traitement ou de sous-traitant établis en France ainsi que les traitements réalisés pour le compte d'organismes non établis sur le territoire dès lors qu'ils visent des personnes résidant en France.

Dès lors qu'un organisme est soumis à un contrôle, il est tenu de répondre aux demandes de la CNIL.

La CNIL a rédigé une charte des contrôles qui a pour objectifs de :

- rappeler « *les droits et obligations des organismes faisant l'objet d'un contrôle, au regard notamment de la loi Informatique et Libertés et du RGPD* » ;
- préciser « *le déroulement et les suites d'un contrôle, quel qu'en soit sa forme, ainsi que les principes de bonne conduite à suivre dans ce cadre* ».

Préambule

Le règlement européen sur la protection des données (RGPD) repose prioritairement sur une logique de responsabilisation accrue des acteurs (responsables de traitement et sous-traitants), avec l'accompagnement et sous le contrôle de l'autorité de régulation : la Commission nationale de l'informatique et des libertés (CNIL).

Tout organisme qui traite des données personnelles doit ainsi pouvoir justifier **à tout moment** de sa conformité aux obligations imposées par le règlement (« *logique d'accountability* ») auprès de la CNIL. En application des pouvoirs qui lui sont confiés afin de s'assurer du respect de la règlementation en matière de protection des données personnelles, la CNIL peut notamment procéder à un contrôle *a posteriori* des traitements mis en œuvre.

Dans ce cadre, outre le rôle central du délégué à la protection des données personnelles (DPO) dans la mise en conformité au règlement européen, il est également le point de contact pour faciliter l'accès de l'autorité de contrôle aux documents et informations nécessaires à l'exécution de ses missions.

Pour accompagner les DPO dans l'exercice de leurs fonctions, le réseau SupDPO a souhaité mettre à leur disposition un document d'orientations sur diverses bonnes pratiques à mettre en œuvre afin de se préparer au mieux à un éventuel contrôle de la CNIL, et s'assurer du bon déroulement de celui-ci.

Ce document est susceptible d'évoluer en fonction de la règlementation, et pourra être enrichi des retours d'expérience des DPO membres du réseau.

Au préalable, nous invitons les DPO à prendre connaissance de la « Charte des contrôles » élaborée par la CNIL, accessible et annexée au présent document, pour leur permettre d'appréhender de la manière la plus concrète la procédure de contrôle de la CNIL.

Tout savoir sur les procédures de contrôle

Quel est le cadre légal ?

La CNIL a le pouvoir de contrôler les traitements de données personnelles effectués dans le cadre des activités des responsables de traitement ou de sous-traitant établis en France ainsi que les traitements réalisés pour le compte d'organismes non établis sur le territoire dès lors qu'ils visent des personnes résidant en France.

Les pouvoirs de contrôle de la CNIL sont prévus par différentes dispositions :

- **Le règlement européen sur la protection des données** prévoit que les autorités de protection des données peuvent « mener des enquêtes sous la forme d'audits sur la protection des données » (article 58-1), y compris de manière conjointe avec d'autres autorités de contrôle (article 62) ;
- **La loi du 6 janvier 1978 modifiée dite « loi informatique et libertés » (LIL)** prévoit que la CNIL peut « *procéder ou faire procéder* (…) *à des vérifications portant sur tous les traitements, et le cas échéant, d'obtenir des copies de tous documents ou supports d'informations utiles à ses missions* » (article 8-2°)g) ;
- **Le pouvoir de contrôle conféré à la CNIL** est également encadré par le décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (articles 16 à 37) qui précise notamment les conditions d'habilitations à

effectuer des contrôles des membres et agents de la CNIL ainsi que les différentes formes que peuvent prendre ces contrôles ;

- **Le code de la sécurité intérieure (CSI)** pour ce qui concerne les dispositifs de vidéoprotection (article L253-2) ;
- **Le code des postes et des communications électroniques (CPCE)** pour ce qui concerne la prospection directe utilisant les coordonnées d'un abonné ou d'une personne physique (L34-5).

La charte des contrôles de la CNIL

La CNIL a rédigé une charte[1] (voir Annexe) qui a pour objectifs de :

- rappeler « les droits et obligations des organismes faisant l'objet d'un contrôle, au regard notamment de la loi Informatique et Libertés et du RGPD » ;
- préciser « le déroulement et les suites d'un contrôle, quel qu'en soit sa forme, ainsi que les principes de bonne conduite à suivre dans ce cadre".

Vous trouverez ci-dessous un résumé de cette charte.

Le contrôle de la mise en œuvre des traitements par la CNIL

La CNIL rappelle l'objectif des missions de contrôle, à savoir vérifier la conformité des traitements aux règles relatives à la protection des données personnelles, ainsi que le respect des dispositions du CSI et du CPCE s'agissant des traitements pour lesquels la CNIL dispose d'un pouvoir de contrôle.

Il s'agit de procéder à un constat des pratiques au sein de l'organisme mais en aucun cas les agents de la CNIL n'ont vocation à se prononcer sur d'éventuels manquements, ou à l'inverse, sur la conformité du ou des traitements faisant l'objet de vérifications. La mission de contrôle n'a pas non plus pour objet de conseiller le responsable de traitement ou le sous-traitant sur les mesures à mettre en œuvre pour se mettre en conformité.

Différentes situations peuvent conduire la CNIL à procéder à des vérifications auprès d'un responsable de traitement ou d'un sous-traitant. Les contrôles peuvent être engagés soit à la suite d'une plainte, soit à la suite de publications dans la presse, soit à l'initiative de la Commission afin d'investiguer certains sujets considérés comme prioritaires et déterminés dans le programme annuel des contrôles de la CNIL par exemple.

Ces contrôles peuvent revêtir différentes formes : sur place, sur pièces, sur convocation ou en ligne.

Les pouvoirs et obligations des agents de contrôle

Sur décision de son Président, les contrôles sont menés par les membres de la Commission et/ou des agents des services habilités.

En principe, la délégation réalisant le contrôle est composée d'au moins un juriste et d'un auditeur des systèmes d'information appartenant au service des contrôles. Les agents des autres directions ou services peuvent également être amenés à participer à la mission de contrôle en raison notamment de l'objet de celui-ci. Par exemple, un agent du service des plaintes lorsque le contrôle réalisé fait suite à une plainte.

Les membres de la délégation, tenus au secret professionnel, peuvent se déplacer au sein de l'organisme afin de procéder aux constats nécessaires, demander à entendre les membres du

[1] https://www.cnil.fr/sites/default/files/atoms/files/cnil-charte_des_controles.pdf

personnel susceptibles de lui communiquer des informations utiles à sa mission et exiger la communication de tout document qu'ils estimeraient utile (contrats, notes de services, autorisation préfectorale pour la vidéo, tableaux Excel, copie d'écrans de logiciels, etc.).

Les droits et obligations des organismes contrôlés

Lors d'un contrôle sur place, les agents de la CNIL doivent être en mesure de démontrer leur identité, leur habilitation à procéder aux contrôles et présenter leur ordre de mission.

Le responsable des lieux peut se faire assister du conseil de son choix, ce qui n'a cependant pas pour effet de suspendre le contrôle jusqu'à son arrivée.

Dès lors qu'un organisme est effectivement soumis à un contrôle, il est tenu de répondre aux demandes de la CNIL. Toute action empêchant la CNIL de réaliser le contrôle pour lequel elle a obtenu l'autorisation est susceptible de constituer un délit d'entrave à l'action de la CNIL (par exemple, en cas de refus de transmettre des informations ou en cas de destruction ou modification de documents utiles à la mission de la CNIL).
Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources de traitements journalistiques ou par le secret médical.

S'agissant du secret médical, celui-ci est opposable s'agissant des informations figurant dans certains traitements. Dans ce cas, la communication des informations ne pourra se faire qu'en présence d'un médecin.

Le déroulement des contrôles de la CNIL

La Charte décrit les différentes phases d'un contrôle selon la forme qu'il prend (sur place, en ligne, sur pièces ou sur convocation).

À l'issue des contrôles (à l'exception du contrôle sur pièces), un procès-verbal est rédigé par les agents de la CNIL dans lequel sont consignées, de manière factuelle, l'ensemble des informations qui ont été portées à leur connaissance pendant le contrôle ainsi que les constatations qu'ils ont effectuées.

Le procès-verbal énonce la nature, le jour, l'heure et le lieu des vérifications ou des contrôles effectués. Il indique également l'objet de la mission, les membres de celle-ci présents, les personnes rencontrées, le cas échéant, leurs déclarations, les demandes formulées par les membres de la mission ainsi que les éventuelles difficultés rencontrées.

L'inventaire des pièces et documents dont les personnes chargées du contrôle ont pris copie est annexé au procès-verbal.

Le procès-verbal est notifié au responsable des lieux et au responsable des traitements et le cas échéant à son sous-traitant par lettre recommandée avec demande d'avis de réception. Lorsque seul le sous-traitant a fait l'objet d'un contrôle sur place, le procès-verbal lui est notifié, ainsi que, le cas échéant, au responsable du traitement et aux personnes mentionnées à l'alinéa précédent, selon les mêmes modalités.

Les suites d'un contrôle

Après examen des constats réalisés et des pièces éventuellement recueillies, différentes suites peuvent être apportées au contrôle :

- La clôture de la procédure : lorsque les constatations effectuées n'appellent pas d'observations particulières ou ne portent pas sur des manquements graves ;
- Avertir le responsable du traitement ou le sous-traitant du fait que les traitements envisagés sont susceptibles de violer les règles en matière de protection des données personnelles ou le rappeler à l'ordre lorsqu'ils ont effectivement entraîné une violation de ces règles ;

- L'organisme peut être mis en demeure de se mettre en conformité dans un délai imparti pour se mettre en conformité : lorsque les vérifications opérées conduisent à caractériser des manquements plus significatifs ;
- La transmission du dossier à la formation restreinte de la CNIL qui peut prononcer les sanctions : lorsque les vérifications opérées conduisent à caractériser des manquements selon leur gravité ;

En cas d'absence de réponse à la mise en demeure ou de non-respect de ses injonctions, le dossier peut également être transmis à la formation restreinte de la CNIL, qui peut prononcer des sanctions pécuniaires (amende administrative) ou non pécuniaires (rappel à l'ordre, injonction sous astreinte, etc.).

Les principes de bonne conduite

La CNIL fait part des principes de bonne conduite applicables aux contrôleurs de la CNIL tout en soulignant ceux attendus par les personnes faisant l'objet d'un contrôle, en particulier la coopération tout au long de la mission et jusqu'à la clôture du dossier.

C'est dans cette dernière optique, que le présent document décline les diverses bonnes pratiques qui pourraient être appliquées.

Comment anticiper et préparer un contrôle ?

Les mesures décrites ci-dessous sont des mesures organisationnelles à définir et mettre en place bien en amont de l'annonce d'un contrôle.

Comment préparer un contrôle ?

- Constituer une cellule de crise : prévoir la composition (responsable de traitement ou son représentant, responsable communication en fonction de l'objet du contrôle, DPO, RSSI, DSI, DAJ, DGS, etc.), identifier le rôle de chacun et fixer le mode de fonctionnement de la cellule ;
- Définir une procédure interne applicable en cas de contrôle de la CNIL (qui contacter, où s'installer, quelles actions entreprendre pendant et à l'issue du contrôle) ;
- Identifier les points de contact au niveau des différents services. Dans la mesure du possible, identifier au moins deux personnes pour chaque service afin de prévoir les cas d'absence : les contrôles de la CNIL sont inopinés, sauf exception (ex : contexte sanitaire) , et les agents sur place doivent pouvoir accompagner le contrôle lorsque la délégation se présente.
- Identifier le(s) éventuel(s) responsables des lieux : le responsable des lieux doit pouvoir répondre aux questions de la CNIL et être en mesure d'identifier les personnes idoines à contacter (DGS, par exemple). Un contrôle dure au minimum une journée et est susceptible de se poursuivre le jour suivant.: il convient donc que le responsable des lieux puisse neutraliser sa journée pour rester totalement disponible pendant la durée du contrôle.
- Sensibiliser et former les agents de l'accueil et de sécurité à la procédure à suivre en cas de contrôle, les consignes à appliquer : il est en particulier impératif que les agents ne s'opposent pas à la tenue du contrôle, et que tous les personnels collaborent en transparence avec la délégation ;
- Prévoir la mise à disposition de moyens matériels (salle de réunion, imprimante accessible pour faire une copie des documents à remettre à la CNIL) et logiciels (partage de fichiers sécurisé);
- Recréer les conditions d'un contrôle réel (s'inscrit dans le cadre des audits prévus par le RGPD) ;

- Prévoir l'accès à la documentation de la conformité : lors du contrôle, les agents sont susceptibles de demander toutes les informations utiles pour apprécier les conditions dans lesquelles sont mis en œuvre les traitements ainsi que les mesures prises par l'organisme pour se mettre en conformité.

  Les demandes peuvent aussi bien porter sur les procédures et la politique générale de protection des données que sur les modalités de mise en œuvre d'un traitement en particulier.

  Les informations sollicitées doivent être transmises dans des délais raisonnables, aussi est-il primordial d'organiser la gestion et l'accès à la documentation.

  La documentation réalisée principalement par le DPO et le RSSI doit être centralisée, accessible et disponible aux intervenants (DAJ, DG notamment).

  La liste ci-dessous ne saurait être exhaustive et les éléments cités dépendront de votre organisme

  - **Documentation générale**

    - Présentation générale de l'organisme ;
    - Données générales chiffrées ;
    - Organigramme ;
    - Politique interne et externe de protection des données ainsi que les modalités de mise en place de ces politiques ;
    - Registre des traitements RT et ST ;
    - Registre des Violations de données personnelles ;
    - Registre des Demandes d'exercice de droits ;
    - La procédure interne de décision d'analyse d'impact ;
    - Actions de formations et sensibilisations réalisées ;
    - Feuilles de route, plan RGPD, etc.
    - Mesures de sécurités et procédures mises en place (PSSI, Politique de protection des données, PRA, etc.)
    - Charte informatique
    - Procédure de gestion des réclamations et demandes
    - Formulaires de consentement
    - Procédure violation de données
    - Cartographie des traitements

  - **Documentation relative à un traitement spécifique (le dossier de conformité)**

    - Formalités
      - Déclaration au registre et documentation justifiant les choix effectués s'agissant des modalités de mise en œuvre (base légale, moyens, durée de conservation, mesures de sécurité, ect.) ;
      - Analyse juridique préalable ;
      - Analyse de risque ou AIPD effectuée ;
      - Contrats et Annexes RGPD
    - Respects des droits des personnes concernées
      - Mentions d'information ;
      - Dans le cadre de l'exercice des droits : échanges avec les personnes concernées ;
      - Preuve de la notification aux personnes en cas de violation des données
    - Gestion des violations de données ou incidents
      - Preuve de la notification à la CNIL ;
      - Preuve de la notification aux personnes en cas de violation des données ;

        - Le cas échéant, l'historique incidents survenus et informations sur les mesures mises en place par pour éviter ce type de situation – sécurité, formation, maintenance, éthique…
    - Suivi des mesures techniques et organisationnelles de protection des données dans le temps
        - Procédure de contrôle interne de la conformité ;
        - Examen périodique de la conformité a posteriori ;
        - Notes de réunions, échanges, calendrier sur les éventuelles mesures correctives ;
        - Procédure de suivi du sort des données à échéance de la durée d'utilité administrative.

Quelles sont les premières actions à mener lors de l'annonce d'un contrôle par la CNIL ?

- Informer la direction et lui demander de désigner le **responsable des lieux**;
    - il est l'interlocuteur privilégié de la délégation de la CNIL au sein de l'organisme durant la totalité de la mission de contrôle. La responsabilité des lieux peut être transférée en cours de contrôle. Il en sera fait mention au procès-verbal. Le responsable des traitements, s'il est présent, a vocation à être responsable des lieux mais il peut s'agir de toute personne se désignant comme tel ou désignée par sa hiérarchie (par exemple le DGS ou le DGD-A ou le directeur ou directeur adjoint d'un laboratoire ou le DPO).
    - il sera amené à accompagner la délégation tout au long du contrôle et à signer le procès-verbal en fin de mission.
    - Avant de procéder aux vérifications, un premier échange avec le responsable des lieux permettra à la délégation d'avoir une vision plus précise de l'activité de l'organisme contrôlé et une meilleure compréhension de l'environnement et du contexte dans lequel il s'inscrit.
    - À cette occasion, les agents peuvent être amenés à interroger le responsable des lieux sur le fonctionnement de l'organisme, l'organigramme, les procédures mises en œuvre, les budgets alloués à certaines activités (DPO, RSSI, etc.) ou pour la mise en œuvre de certains dispositifs.
    - Les informations obtenues peuvent servir à orienter aux mieux les investigations.
- Désigner le responsable des lieux à la délégation;
- Activer la cellule de crise ;
- Informer les agents concernés par le contrôle en rappelant les bonnes pratiques (rester disponible, préparer la documentation utile, collaborer avec la délégation, rappeler aux équipes qu'il est strictement interdit de modifier les traitements de données jusqu'au contrôle de la CNIL) ;
- Réserver la salle de réunion dans laquelle la délégation pourra s'isoler pour rédiger le procès-verbal ;
- Suivre la procédure interne en cas de contrôle de la CNIL.

Quelles sont les actions à réaliser pendant le contrôle ?

Organisation

- Préparer la salle pour recevoir la délégation et dans laquelle les contrôleurs peuvent s'isoler pour rédiger le procès-verbal ;
- Choisir l'outil informatique adéquat (partage de fichiers sécurisé) pour transmettre les documents demandés par la délégation ;
- Outre la présence des participants permanents à ce contrôle (responsables des lieux, DPO, RSSI, etc), prévoir la disponibilité des personnes susceptibles de répondre aux interrogations de la délégation selon l'objet des vérifications (DAJ, DCOM, DSI, DRH, etc.), il est possible de demander à la délégation si elle peut préciser l'ordre de passage de ces personnes ;
    - Le cas échéant, demander à la délégation son conseil pour le choix de ces personnes ;
- Désigner la personne qui coordonnera la collecte des documents à remettre sur place à la délégation ou à lui transmettre ultérieurement ;
- Informer les agents concernés par le contrôle de ne pas détruire ou modifier les informations faisant l'objet du contrôle de la CNIL et en informer le personnel ;
- Préparer une ou deux diapos de synthèse sur le traitement qui fait l'objet du contrôle afin de le présenter à la délégation.

Suivi du contrôle

- Vérifier le respect du cadre légal : information, conditions horaires du contrôle, habilitation des agents de contrôle, établissement du procès-verbal, etc. ;
- Prendre connaissance de leur ordre de mission ;
- Répondre de manière factuelle claire, synthétique et précise aux questions posées par la délégation, sans anticiper sur d'éventuelles futures questions ou pointer des problématiques qui n'auraient pas été abordées ;
- Veiller à noter au fur et à mesure les documents demandés par la délégation en précisant les pièces transmises sur place et celles à communiquer ultérieurement ;

A la fin de chaque journée de contrôle

- La délégation remet au responsable des lieux une copie du procès-verbal en fin de journée. Le responsable de traitement en recevra une copie par lettre recommandée avec accusé de réception dans les jours qui suivent le contrôle.
- Le responsable des lieux avec les participants au contrôle relit le procès-verbal très attentivement avant de le signer le procès-verbal (un des éléments constitutifs du dossier de sanction). L'organisme contrôlé a toujours la possibilité d'adresser des observations sur ce procès-verbal à la CNIL après le contrôle tant que la procédure de contrôle est ouverte.
- Si vous estimez que des éléments de la retranscription dans ce procès-verbal ne sont pas fidèles à vos échanges, demander à ce qu'ils soient reformulés. N'hésitez pas à pointer chaque élément à préciser ou reformuler, même s'ils sont nombreux. En cas de refus par la délégation, précisez-le dans la zone commentaires du procès-verbal ;

- Transmettre à la délégation les documents à donner sur place et listés dans le procès-verbal. Des pièces peuvent également devoir être communiquées à la CNIL à la suite du contrôle. Elles seront mentionnées au procès-verbal avec un délai pour leur communication ;
- Signer le procès-verbal ;
- Veiller à obtenir une copie de la version finale du procès-verbal incluant toutes les pièces et informations recueillies ;

Quelles sont les actions à mener après le contrôle ?

- Transmettre à la délégation les documents à communiquer ultérieurement en utilisant une solution de partage de fichiers sécurisée (par exemple FileSender[2] de Renater). Les agents de la CNIL disposent d'une plateforme d'échange de fichiers sécurisées au besoin.;
- Avant le retour de la CNIL :
    - Organiser des réunions en interne pour un premier bilan du contrôle ;
    - Envoyer à la direction un rapport suite au contrôle avec des propositions d'actions associées ;
    - Identifier les enjeux et les éléments de langage pour la phase de communication ;
    - Le cas échéant, anticiper l'éventuel retour de la CNIL en faisant connaître les irrégularités mises en lumière, en interne, par ce contrôle, et les mesures correctives déjà mises en œuvre ou envisagées selon un calendrier défini ;
    - Afin de respecter les délais
        - Suivre les réponses aux demandes de la CNIL ;
        - ou bien suivre le respect des échéances du plan d'action dans le temps.

[2] https://filesender.renater.fr/

Annexe – Charte des Contrôles de la CNIL

La page présentant la Charte se trouve à l'adresse : https://www.cnil.fr/fr/controles-de-la-cnil-une-charte-pour-tout-comprendre

La Charte est accessible en cliquant sur le lien :
https://www.cnil.fr/sites/default/files/atoms/files/cnil-charte_des_controles.pdf