Que faire quand la Cnil frappe à votre porte ?

Fiches pratiques pour anticiper et gérer un contrôle

Mathias Avocats

Janvier 2021

SOMMAIRE

AVANT-PROPOS

En diffusant ce livre blanc, nous souhaitons vous faire bénéficier de notre expertise, de notre pratique, de nos recommandations sur la gestion des contrôles de la Commission nationale de l'informatique et des libertés (Cnil).

En effet, les conséquences qui peuvent en résulter pour l'organisme contrôlé conduisent généralement les responsables du traitement et les sous-traitants à les redouter.

Deux stratégies peuvent être adoptées : l'une consiste à agir une fois que la Cnil est à la porte, l'autre vise à anticiper le contrôle par l'élaboration d'une procédure adaptée à la taille et à l'activité de l'organisme.

Mathias Avocats accompagne ses clients dans les deux cas y compris en sensibilisant les parties prenantes.

Nous vous souhaitons donc une bonne lecture, en espérant sincèrement que les fiches pratiques qui suivent vous seront utiles.

Bien à vous,

Garance Mathias

Avocat Associé
Mathias Avocats

Fiche 1 - Pourquoi mon organisme est-il contrôlé ?

Sur la décision de la Présidente de la Cnil, les agents de la Commission peuvent contrôler tout organisme traitant des données à caractère personnel dès lors qu'il dispose d'un établissement en France ou que le traitement concerne des personnes physiques résidant en France.

Les organismes peuvent faire l'objet d'un contrôle pour l'une (ou plusieurs) des raisons suivantes.

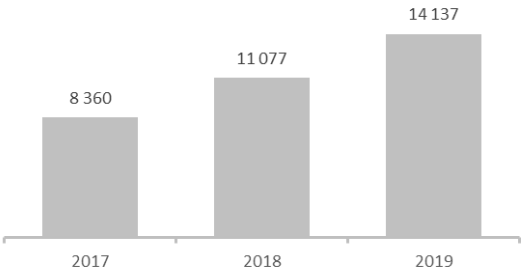
Mise en œuvre de traitements inscrits dans le programme annuel de la Cnil

La Cnil publie tous les ans un programme indiquant les secteurs et les activités de traitement de données pour lesquels des contrôles seront menés l'année suivante. Il est souvent élaboré en fonction de l'actualité ou d'une problématique ayant fait l'objet de nombreuses plaintes l'année passée.

Exemples de thématiques

RECRUTEMENT DU PERSONNEL	GESTION DES SERVICES DE STATIONNEMENT	COOKIES ET AUTRES TRACEURS
DONNEES DES MINEURS	SECURITE DES DONNEES DE SANTE	SERVICES DE GEOLOCALISATION

A la suite d'une plainte individuelle ou collective déposée auprès de la Cnil



Les plaintes sont en forte hausse ces dernières années. Selon la Cnil, elles représentent plus de 40 % des contrôles diligentés par ses agents.

Source: Cnil, Charte des contrôles, 5 août 2020, p.6

Délibération SAN-2019-001 du 21 janvier 2019

La formation restreinte de la Cnil a prononcé une sanction pécuniaire à l'encontre d'un éditeur de système d'exploitation à la suite des **plaintes collectives** déposées par deux associations, regroupant les **réclamations de 9 974 personnes concernées.**

Lorsque la Cnil reçoit un signalement de la part d'autres autorités

La Cnil peut diligenter un contrôle après avoir obtenu des informations de la part d'une autre autorité de contrôle européenne.

Opérations de contrôle conjointes (Article 62 du RGPD)

Lorsque l'organisme contrôlé dispose de plusieurs établissements dans l'Union européenne (UE) et/ou traite les données personnelles de plusieurs personnes concernées dans l'UE, un contrôle en coopération avec d'autres autorités de protection des données européennes peut être organisé.

Un contrôle peut également être réalisé à la suite d'informations transmises par toute autre autorité.

Délibération SAN-2019-001 du 21 janvier 2019

La Cnil a été informée par le client d'une société intermédiaire en assurance que les données d'autres clients étaient accessibles sans procédure d'authentification aux espaces personnels des clients sur le site web de la société. La Cnil a également reçu un **signalement de la part de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)** qui l'avisait de la possibilité d'accéder aux données des clients de la société depuis un moteur de recherche sans contrôle préalable.

La Cnil et la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) - autorité chargée de la protection des consommateurs - a conclu en 2012 un protocole de coopération, mis à jour en 2019. Par le biais de ce protocole, la Cnil et la DGCCFR ont renforcé leur collaboration, afin notamment de réaliser des contrôles communs.

Enquête conjointe sur l'IP Tracking

La Cnil et la DGCCRF ont mené des contrôles communs de sites de commerce en ligne sur les pratiques de fluctuation des tarifs en fonction de l'adresse IP des internautes. Les conclusions de cette enquête, publiées en janvier 2014, n'ont toutefois pas permis de constater l'existence de telles pratiques dites également « *behaviour pricing* ».

Lorsque l'attention des médias s'est portée sur l'organisme

La Présidente de la Cnil peut décider de faire un contrôle lorsque des problématiques et enjeux relatifs à la protection des données à caractère personnel sont évoqués par les médias.

Délibération SAN-2021-003 du 12 janvier 2021

Après la **publication de plusieurs articles de presse** révélant l'utilisation de drones équipés de caméras par la police et la gendarmerie pour surveiller le respect du confinement, la Présidente de la Cnil a décidé de diligenter un contrôle sur pièces, suivi par un contrôle sur place. A la suite de ces vérifications, une procédure de sanction a été engagée et la formation restreinte de la Cnil a prononcé un rappel à l'ordre ainsi qu'une injonction à l'encontre du ministère de l'intérieur.

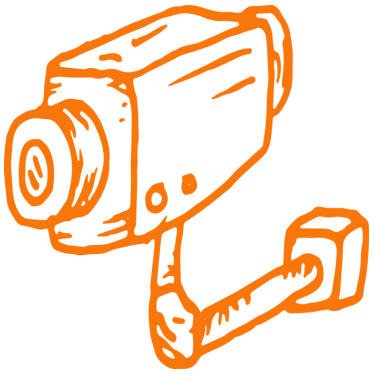
A la suite d'un contrôle dans les locaux d'un client, ou au sein d'une filiale

Si un contrôle a lieu dans une société faisant partie d'un groupe, il est possible que les agents de la Cnil souhaitent effectuer un contrôle de la conformité d'une autre entité du même groupe. Cela peut être le cas, par exemple, lorsque l'entité initialement contrôlée n'est pas, après premières investigations, le responsable de traitement de l'activité visée par la Cnil.

Un tel scénario peut également se produire dans le cadre des relations client-prestataire. A la suite d'un contrôle diligenté auprès d'un client responsable de traitement, les agents de la Cnil peuvent procéder à un contrôle auprès du prestataire auquel le client a confié tout ou partie de ses activités de traitement, ou inversement.

Dans le cadre du contrôle des dispositifs de vidéoprotection

La Cnil est compétente pour contrôler les conditions de mise en œuvre et d'utilisation des systèmes de vidéoprotection dans des lieux ouverts au public (Article L.253-2 du Code de la sécurité intérieure).



Fiche 2 - Quels sont les types de contrôle ?

Il existe quatre types de contrôle : sur place, sur pièces, sur audition et en ligne.

En général, deux agents habilités seront désignés par la Présidente de la Cnil, à savoir un juriste et un auditeur des systèmes d'information. Il peut toutefois arriver, selon la nature du contrôle, qu'un seul agent soit chargé du contrôle.

Quelle que soit la forme qu'il prenne, l'objectif d'un contrôle est de vérifier la conformité d'un traitement mis en œuvre par une entité (Cnil, Charte des contrôles, 5 août 2020). A ce titre, les agents de la Cnil peuvent notamment demander la communication de toute information ou de tout renseignement qu'ils estiment utiles.

Peut-on opposer le secret professionnel aux agents de la Cnil ?

Le secret professionnel n'est pas opposable à la Cnil sauf certaines exceptions prévues par la loi. Il s'agit du secret applicable aux relations entre un avocat et son client, du secret des sources des traitements journalistiques ou du secret médical (Article 19, III de la Loi n° 78-17 du 6 janvier 1978).

Si l'organisme l'invoque, il doit indiquer le fondement législatif ou réglementaire du secret professionnel ainsi que la nature des données couvertes par celui-ci. Ces informations figureront sur le procès-verbal à l'issue du contrôle.

CONTRÔLE SUR PLACE

Ce contrôle consiste pour la Cnil à désigner des agents qui se rendent dans les locaux du responsable de traitement ou du sous-traitant afin de vérifier la conformité de leurs traitements avec la réglementation en vigueur (Article 19, I de la Loi n° 78-17 du 6 janvier 1978).

Les agents de la Cnil peuvent se rendre à la fois dans des locaux à usage professionnel et dans des lieux affectés en tout ou partie à un domicile privé. Toutefois, l'accès au domicile privé est soumis à une autorisation préalable du juge des libertés et de la détention territorialement compétent.

Le procureur de la République compétent est informé au plus tard 24 heures avant la date de la visite. Quant à l'organisme contrôlé, il est informé au plus tard lors de l'arrivée des agents de la Cnil sur place.

A leur arrivée, les agents de la Cnil fournissent à l'organisme notamment les informations suivantes :

- L'identité et la qualité des agents,
- L'objet du contrôle,
- Le droit d'opposition à la visite,
- La copie de la décision de contrôle,
- La copie de l'ordre de mission qui désigne les agents chargés du contrôle.

Peut-on s'opposer à la visite des agents ?

Dans l'hypothèse où l'organisme exerce son droit d'opposition, le contrôle ne pourra avoir lieu qu'après autorisation du juge des libertés et de la détention territorialement compétent. Ce même juge peut également autoriser préalablement une visite « *lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie* », auquel cas l'organisme ne pourra pas s'y opposer.

Le droit d'opposition peut être également exercé après avoir permis aux agents d'entrer dans les locaux (Article 56 du Règlement intérieur de la Cnil). Un procès-verbal est alors établi en ce sens.

CONTRÔLE SUR PIECES

Un contrôle ne nécessite pas forcément un déplacement des agents de la Cnil dans les locaux de l'organisme concerné. Ils peuvent demander la communication de certains documents à des fins de vérifications (Article 19, III de la Loi n° 78-17 du 6 janvier 1978).

Le contrôle sur pièces se déroule en général de manière suivante :

⇒ L'organisme reçoit une lettre recommandée de la part du service des contrôles de la Cnil qui l'informe du contrôle sur pièces et de son objet.

La décision de procéder à un contrôle auprès de l'organisme l'ordre de mission, ainsi que le questionnaire destiné à évaluer les pratiques au regard de la réglementation en vigueur sont annexés à cette lettre.

⇒ Les éléments demandés par la Cnil, ainsi que toute pièce justificative ou illustrative, doivent être communiqués avant l'expiration du délai indiqué dans la lettre.

⇒ A la suite de la transmission de ces documents par l'organisme concerné, les agents en charge du contrôle sont susceptibles de demander des informations et des précisions complémentaires.

Le fait de procéder à un contrôle sur pièces n'empêche pas la Cnil de mener ensuite des **vérifications sur place**. Ainsi, il ne faut pas considérer le contrôle sur pièces comme étant moins risqué qu'un contrôle sur place.

Délibération SAN-2021-003 du 12 janvier 2021

Dans le cadre des contrôles portant sur l'utilisation de drones équipés de caméras pour surveiller le respect du confinement, la Présidente de la Cnil a adressé des questionnaires à plusieurs organismes dont le ministère de l'intérieur et la préfecture de police de Paris.

A la suite des réponses apportées, les agents de la Cnil ont réalisé un contrôle sur place dans les locaux de la préfecture de police de Paris.

CONTRÔLE SUR AUDITION

Les agents de la Cnil peuvent convoquer toute personne qu'ils souhaitent interroger dans le cadre d'une mission de contrôle. En général, ce type de contrôle a lieu dans les locaux de la Cnil.

La convocation est adressée « *par lettre remise contre signature, ou remise en main propre contre récépissé ou acte d'huissier* », réceptionnée au moins huit jours avant la date de l'audition (Article 34 du Décret n°2019-536 du 29 mai 2019).

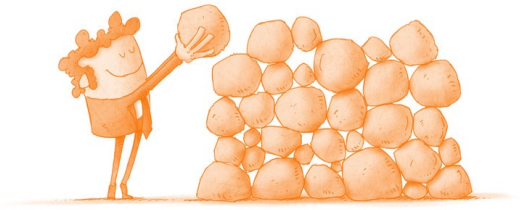
Cette convocation mentionne l'objet du contrôle, la date, l'heure, le lieu de l'audition et le droit de l'organisme de se faire assister par un conseil de son choix (Cnil, Charte des contrôles, 5 août 2020, p. 13).

CONTRÔLE EN LIGNE

La Cnil dispose d'un moyen de contrôle qui permet de procéder à des **constatations en ligne**, depuis ses propres locaux, à partir d'un ordinateur ou d'un terminal mobile connecté à Internet, et sans la présence du responsable du traitement ou du sous-traitant.

La Cnil a ainsi un pouvoir d'investigation adapté au développement numérique. Les agents de la Cnil peuvent consulter les **données librement accessibles ou rendues accessibles** en ligne, y compris par imprudence, par négligence ou par le fait d'un tiers.

Par ailleurs, les agents de la Cnil ont la possibilité d'utiliser une **identité d'emprunt.** Ainsi, à l'instar de leurs collègues de l'Autorité des marchés financiers ou de la DGCCRF, ils pourront utiliser un pseudonyme ainsi que des coordonnées (adresse électronique, etc.) différentes de celles qui leur ont été attribuées par la Cnil pour l'exercice de leurs missions. Toutefois, cela ne signifie pas que les agents de la Cnil utilisent toujours une identité d'emprunt.



Délibération SAN-2020-018 du 8 décembre 2020

Les agents de la Cnil ont diligenté un contrôle en ligne afin de vérifier la conformité du parcours d'inscription des personnes aux services d'une société spécialisée dans la préparation et la livraison de repas. A ce titre, les agents ont créé un compte au nom de la Cnil.

En pratique, ce contrôle permet aux agents de la Cnil de vérifier l'application de la réglementation relative à la protection des données. Ainsi, ils peuvent tester les liens de désinscription intégrés dans les courriels de prospection commerciale ou simuler l'exercice des droits reconnus aux personnes concernées. Ils peuvent également vérifier la sécurité des données, sans possibilité de forcer les mesures de sécurité mises en place pour pénétrer dans un système d'information.

Délibération SAN-2019-005 du 28 mai 2019

La Cnil a reçu une plainte de la part du client d'une société du secteur de l'immobilier qui met à la disposition des candidats à la location un espace pour qu'ils puissent constituer leur dossier en ligne. Le plaignant faisait valoir qu'en changeant les caractères des adresses URL, il pouvait accéder aux données d'autres candidats. Au cours d'un contrôle en ligne, la délégation de la Cnil a saisi les adresses URL fournies par le plaignant à des fins de vérification et a pu accéder à plusieurs documents. Elle a également constaté qu'il était possible de télécharger ces documents.

Le contrôle en ligne permet également de vérifier la conformité des pratiques des organismes à la réglementation relative aux cookies et autres traceurs. Ainsi, les agents de la Cnil peuvent vérifier :

- le nombre et la nature des cookies déposés et lus sur le terminal de l'internaute,
- les modalités et le contenu de l'information relative aux cookies,
- les modalités de recueil et de retrait du consentement,
- les modalités d'exercice du droit d'opposition.

Délibération SAN-2020-013 du 7 décembre 2020

La délégation de la Cnil a diligenté un contrôle en ligne du site Internet d'une société spécialisée dans la vente en ligne pour vérifier la conformité des opérations du dépôt et de la lecture des cookies sur le terminal des internautes. A cette occasion, les agents ont notamment constaté que 40 cookies publicitaires étaient déposés sans recueil du consentement préalable des internautes. Ils ont également constaté que l'information relative aux cookies n'était pas complète, ni aisément accessible.

Le contrôle en ligne peut être indépendant ou complémentaire d'un contrôle sur place, sur pièces ou sur audition.

Délibération SAN-2019-001 du 21 janvier 2019

Dans le cadre de l'investigation des traitements mis en œuvre par un éditeur de système d'exploitation, les agents de la Cnil ont diligenté un contrôle en ligne, sans procéder à des contrôles supplémentaires.

Délibération SAN-2019-005 du 28 mai 2019

A la suite d'une plainte de la part du client d'une société du secteur de l'immobilier, la délégation de la Cnil a diligenté un contrôle en ligne, suivi par un contrôle sur place dans les locaux de ladite société.

Fiche 3 - Comment anticiper un contrôle ?

Tout contrôle emporte des risques pour l'organisme contrôlé, que ce soient des risques financiers, juridiques, opérationnels ou encore de réputation. Ces risques existent également pour les entités qui semblent, au premier abord, en conformité avec le cadre réglementaire. En effet, la non-conformité peut parfois être identifiée à la fin de la procédure de contrôle et ainsi remettre en cause la continuité des activités de l'entité.

Anticiper un contrôle participe plus généralement d'une gestion des risques. Les organismes devraient être proactifs afin d'être en mesure de gérer les contrôles avec efficacité.

A ce titre, les entités peuvent mettre en place les actions suivantes.

Cartographier les actions de conformité et suivre leur mise en œuvre

Nombreuses sont les entités qui ont défini un plan d'action dans le cadre de leur mise en conformité. Lorsqu'il est désigné, le Délégué à la protection des données (DPO) de l'organisme peut effectuer à ce titre un audit de conformité. Ainsi, l'organisme pourra, par anticipation, connaitre la maturité de sa conformité, enrichir son plan d'action et gérer les risques en amont.

Il s'agira de vérifier, par exemple :

- la mise en œuvre de la procédure de gestion des droits des personnes,
- l'application de la politique relative à la conservation des données par les collaborateurs et dans les systèmes d'information,
- la mise à jour du registre des activités de traitement,
- les clauses relatives à la protection des données stipulées dans les contrats de sous-traitance ou de responsabilité conjointe, etc.

« GDPR Compliance Support Tool », outil de conformité de l'autorité de contrôle luxembourgeoise

L'autorité de contrôle luxembourgeoise, la Commission nationale pour la protection des données (CNPD), a développé un outil gratuit permettant à toute entité notamment de gérer et d'évaluer le niveau de conformité de divers documents tels que le registre des activités de traitement et les clauses contractuelles relatives à la protection des données.

Quels outils pour auditer les pratiques relatives aux cookies ?

- **Outil « Website Evidence Collector » du CEPD**

Le Contrôleur européen de la protection des données (CEPD), ou *European Data Protection Supervisor* (EDPS), a développé un outil disponible en open source. Il permet d'identifier les traitements de données mis en œuvre lors de la consultation d'un site Internet, tels que les traitements réalisés grâce au dépôt et à la lecture de cookies (transmission, stockage de données, etc.).

- **Outil « Cookieviz » de la Cnil**

En septembre 2020, la Cnil a publié la nouvelle version de l'outil Cookieviz qui permet de visualiser les cookies déposés et lus lors de la visite d'un site Internet, les interactions entre les différents acteurs ainsi que les flux de données. Tout organisme peut télécharger cet outil à partir du compte GitHub de la Cnil.

Préparer les documents généralement demandés par la Cnil

Une mission de contrôle vise prioritairement à obtenir toute information utile, de nature technique ou juridique, pour apprécier les conditions dans lesquelles sont mis en œuvre des traitements de données à caractère personnel.

Par exemple, dans le cadre d'un contrôle sur place, les agents de la Cnil peuvent demander la communication d'un certain nombre de documents, l'accès à des systèmes et outils informatiques ou encore la réalisation de certaines actions par les collaborateurs de l'organisme.

Exemples de demandes des agents de la Cnil lors d'un contrôle

- Registre des activités de traitement
- Présentation générale de l'organisme
- Schéma de responsabilité intra-groupe
- Liste des cookies et des finalités correspondantes
- Nombre de clients et de prospects présents dans une base de données
- Liste des situations particulières prises en compte pour l'exercice du droit d'opposition

Ainsi, l'élaboration et la mise à jour de ces documents doivent être assurées afin de pouvoir répondre aux demandes de la délégation de la Cnil. Cette démarche s'inscrit également dans le respect du principe d'*accountability.*

A noter que ces documents devraient refléter la réalité opérationnelle puisque les agents de la Cnil vérifient leur application effective dans le cadre du contrôle mené.

Mettre en place une procédure de gestion du contrôle

Il apparaît judicieux d'élaborer une procédure de gestion du contrôle. Si le contenu d'une telle procédure dépend de l'organisation interne et des moyens de chaque organisme, elle peut notamment préciser :

- qui est le responsable des lieux ou encore quels sont les bureaux et les ressources mises à disposition des agents de la Cnil en cas d'un contrôle sur place,
- les personnes à prévenir dès lors que l'organisme a connaissance d'un contrôle,
- la manière d'accueillir et d'accompagner les agents de la Cnil au jour d'un contrôle sur place,
- la manière de répondre aux questions et demandes des agents de la Cnil et ce quelle que soit la nature du contrôle, etc.

Mise en place d'une équipe de gestion du contrôle

La procédure de gestion du contrôle peut également prévoir la mise en place d'une équipe qui inclut les principales parties prenantes de la gestion du contrôle. Il peut ainsi s'agir du DPO, du directeur juridique, du DSI, du RSSI et des responsables des départements, services ou directions métier (comme les DRH ou le directeur marketing par exemple) selon l'objet du contrôle. Ainsi, il serait intéressant d'anticiper la composition de l'équipe (par métier et non de manière nominative).

Information de l'équipe de gestion du contrôle

Les membres de l'équipe devront alors être informés directement du contrôle diligenté par la Cnil qu'il ait lieu sur place ou qu'il prenne une autre forme. A titre d'exemple, pour un éventuel contrôle sur place, leurs numéros de téléphones devront être disponibles dans les bureaux et surtout à l'accueil, afin de pouvoir les contacter au plus vite.

Sensibiliser et former l'ensemble des acteurs de l'organisme

Un bon niveau de conformité permet de préparer l'organisme aux contrôles. Une formation régulière et une connaissance des obligations de l'entité permettront notamment de minimiser les risques de non-conformité. Cette formation devrait viser tout collaborateur, y compris les organes décisionnels et stratégiques de l'organisme.

Les membres du personnel devront également être sensibilisés sur le rôle qu'ils pourront avoir à jouer pendant le contrôle. Il est nécessaire qu'ils sachent à quoi s'attendre lors du contrôle et de son impact éventuel. Si les collaborateurs sont préparés, ils seront alors mieux à même de répondre aux questions de la Cnil, notamment lors d'un contrôle sur place ou sur audition, et d'identifier les documents demandés.

La formation pourrait inclure des sujets comme :

- la manière de répondre aux questions,
- la manière de communiquer les documents,
- les risques d'une obstruction au contrôle lorsque des informations erronées sont communiquées, etc.

Concernant les contrôles sur place, les réceptionnistes et les gardiens pourraient également être formés sur la manière dont il faut accueillir les agents de la Cnil et les personnes qu'ils devront informer de leur arrivée. Il convient de leur rappeler de demander aux agents d'attendre dans une salle de réception ou de conférence jusqu'à ce que le responsable des lieux et le DPO se présentent.

A noter que cette formation peut être étendue à des contrôles menés par d'autres autorités, comme la DGCCRF.

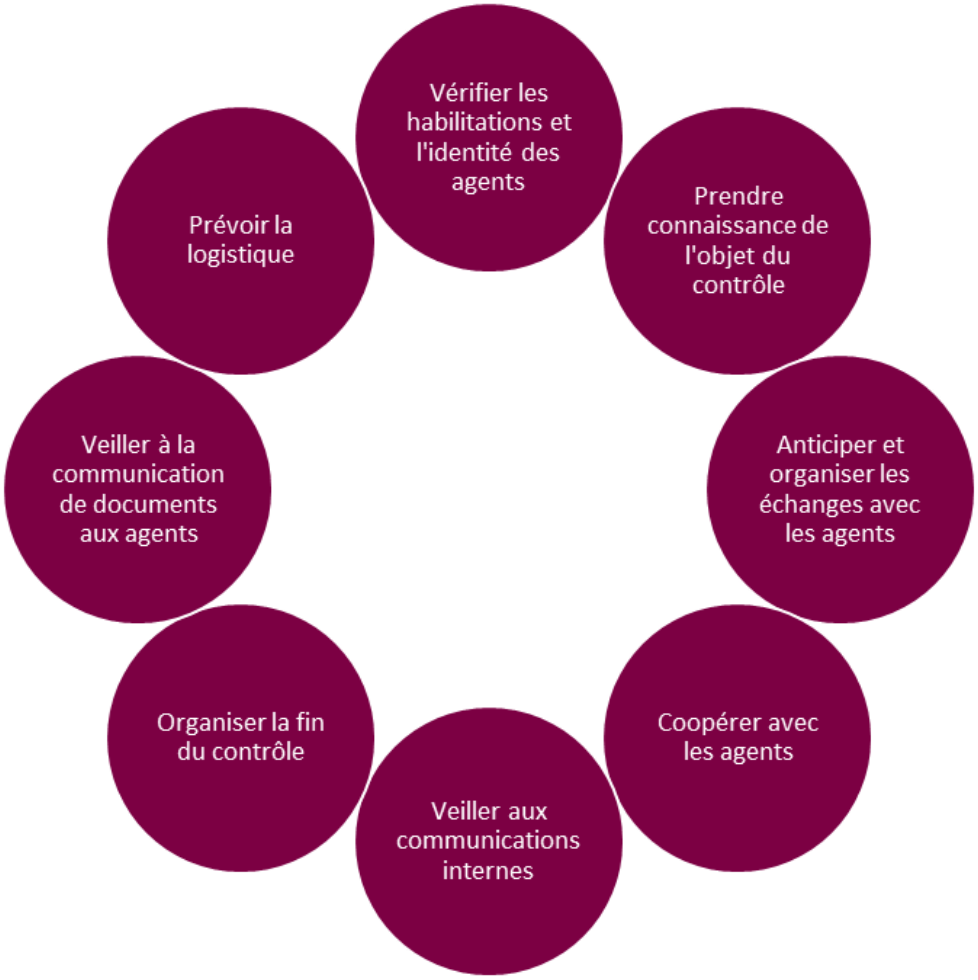
Fiche 4 - Comment gérer un contrôle ?

Qu'il soit responsable de traitement ou sous-traitant, tout organisme a l'obligation de prendre les mesures utiles destinées à faciliter les missions de la Cnil (Article 18 de la Loi n° 78-17 du 6 janvier 1978). Dès lors, la gestion d'un contrôle doit incarner une logique de coopération.

Une telle gestion est également essentielle pour l'organisme contrôlé, afin notamment de limiter les éventuelles perturbations de ses activités, tout en permettant à ses équipes de se mobiliser.

En général, le déroulement d'un contrôle implique le recueil de pièces, la réalisation de constatations par les agents de la Cnil ou l'organisme lui-même pour fournir les éléments demandés et la rédaction d'un procès-verbal de contrôle. Selon la nature du contrôle, les agents de la Cnil peuvent également réaliser des entretiens avec les collaborateurs de l'organisme contrôlé.

Les étapes de la gestion d'un contrôle peuvent être synthétisées de manière suivante.



Vérifier les habilitations et l'identité des agents de la Cnil

Les agents pouvant réaliser des missions de contrôle sont habilités à cet effet par une délibération du bureau de la Cnil. Cette habilitation est valable pendant une durée de cinq ans renouvelable (Article 16 du Décret n°2019-536 du 29 mai 2019).

Toutefois, pour contrôler certains traitements mis en œuvre pour le compte de l'Etat, les agents de la Cnil doivent bénéficier d'une habilitation délivrée par le Premier ministre (Article 23 du Décret n°2019-536 du 29 mai 2019). Par exemple, c'est le cas des traitements concernant la sûreté de l'Etat, la défense, la sécurité publique ou encore la prévention, la recherche ou la poursuite des infractions pénales. Etant précisé que cette habilitation vaut jusqu'à la cessation des fonctions de l'agent.

La première chose à faire est donc de vérifier les habilitations des agents. Plus spécifiquement pour les contrôles sur place, l'identité des agents pourra également être vérifiée en sollicitant la présentation d'une carte professionnelle si les agents ne la présentent pas spontanément.

Prendre connaissance de l'objet du contrôle

En cas d'un contrôle sur place, il est conseillé de solliciter la **communication de l'ordre de mission** dès le début afin de prendre connaissance de l'objet du contrôle. Ainsi, l'équipe de gestion du contrôle pourra déterminer la portée du contrôle, notamment afin de savoir si ce dernier se concentre sur un secteur ou une activité en particulier (le service client, les ressources humaines, etc.). Des questions peuvent également être posées aux agents de la Cnil.

Le **déroulement du contrôle** peut aussi être discuté avec la délégation de la Cnil. Cette échange permettra de **mieux organiser les ressources nécessaires** pour rassembler les informations et pour planifier les éventuels entretiens avec les membres du personnel.

Lorsqu'il s'agit d'un contrôle sur pièces, il conviendrait de **lire attentivement l'ordre de mission, le questionnaire et les demandes formulées** par la délégation de la Cnil. En cas de doute quant au périmètre du contrôle ou d'incompréhension de demandes formulées, il est conseillé de contacter les agents de la Cnil dont les coordonnées figurent en général à la fin de l'ordre de mission.

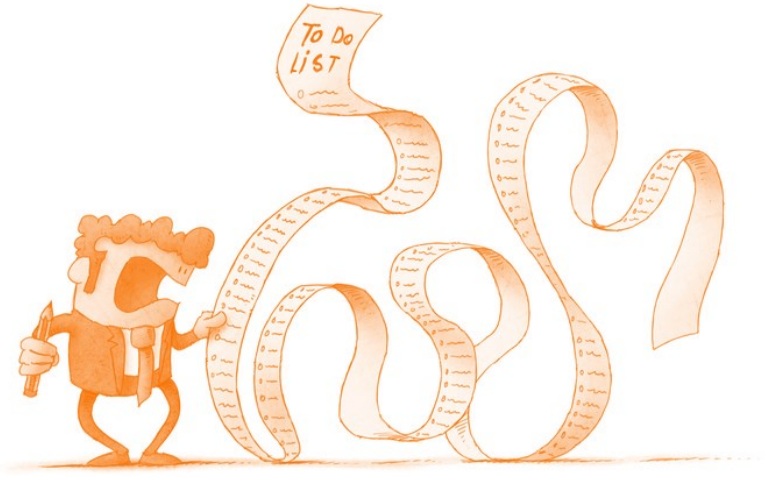
Prévoir la logistique

Au début d'un contrôle sur place, les agents de la Cnil peuvent être accompagnés dans une salle où ils pourront travailler. La pièce qui leur est attribuée doit pouvoir réunir les agents ainsi qu'une équipe de taille similaire de l'organisme contrôlé. En plus de cette pièce, un lieu pour leur permettre de faire des photocopies doit également leur être attribué. Par ailleurs, il est conseillé de faire savoir aux agents que le personnel (qui aura été formé à de tels contrôles) est à leur disposition et qu'ils peuvent leur demander l'assistance dont ils ont besoin.

Dans le cadre d'un contrôle sur pièces, l'organisme devra être en mesure de **mobiliser les bonnes équipes** et **identifier les diligences à réaliser** pour répondre aux demandes de la Cnil.

En tout état de cause, l'équipe de gestion du contrôle doit **identifier tout problème de logistique** quand elle répond aux requêtes des agents. Cela peut être, par exemple, la récupération de documents à partir d'endroits éloignés (notamment lorsque les documents sont détenus par des filiales).

A noter que la délégation de la Cnil n'a pas toujours les informations nécessaires sur l'organisation de l'entité et le procédé de gestion des documents. Ainsi, dans l'hypothèse où l'entité rencontre des difficultés quant à la remise des documents demandés, il conviendrait d'expliquer la situation et demander ainsi un report du délai imparti.



Points de vigilance dans le cadre de la communication de documents

Pour rappel, les agents de la Cnil peuvent demander la communication de tous renseignements ou documents utiles dans le cadre de l'exécution de leurs missions. Ces vérifications peuvent être accompagnées de demandes d'explications ou de justifications écrites ou orales voire d'actions à réaliser par les collaborateurs en fonction de la nature du contrôle (par exemple, connexion à un programme informatique, demande de mise en place de requêtes pour dénombrer les personnes concernées, etc.).

Si un DPO est désigné, il peut avoir à fournir des documents en tant que point de contact de la Cnil. D'autres membres du personnel peuvent toutefois être également concernés.

Les documents fournis aux agents doivent répondre à leur demande. Il est recommandé de se limiter aux demandes et de ne pas fournir de documents sans demande expresse de la Cnil.

En toute hypothèse, les documents sensibles devraient être marqués comme étant « confidentiels » avant toute copie.

Penser à dresser une liste des documents communiqués et de ceux qui n'ont pas encore été adressés aux agents afin d'assurer un suivi.

Anticiper et organiser les échanges avec les agents

En cas d'un contrôle sur place et lorsque l'organisme est prévenu avant le jour de son déroulement, l'équipe de gestion du contrôle devrait s'interroger sur les personnes qui vont s'entretenir avec les agents de la Cnil. Des réunions devront être planifiées avec le personnel identifié afin de discuter des domaines possibles de contrôle, pour déterminer quels documents peuvent être demandés et les préparer à toute question probable.

Néanmoins, les agents de la Cnil peuvent demander des entretiens avec tout membre du personnel de leur choix. Ainsi, ils peuvent s'entretenir avec une autre personne suggérée par l'équipe de gestion du contrôle. Etant précisé que la non-présentation du collaborateur convoqué pour un entretien peut être interprétée comme une entrave au contrôle.

Sous réserve de l'accord exprès du supérieur hiérarchique, de l'équipe juridique ou de l'équipe de gestion du contrôle, les personnes entendues par les agents peuvent tenir un journal de suivi de l'entretien qui pourra éventuellement être utilisé pour enrichir le procès-verbal de contrôle.

Enfin, si les agents sont d'accord, il est recommandé de commencer et de finir chaque journée par une réunion entre l'équipe de gestion du contrôle et les agents.

Dans tous les cas, coopérer avec les agents de la Cnil

S'opposer aux demandes des agents de la Cnil, les empêcher de mener à bien leurs tâches ou refuser de coopérer avec eux peut être perçu comme une entrave au contrôle, punissable d'une peine d'un an d'emprisonnement et d'une amende de 15 000€ d'amende (Article 226-22-2 du Code pénal). Ce délit d'entrave peut être caractérisé lorsque l'organisme :

- s'oppose à l'exercice des missions confiées aux agents de la Cnil lorsque la visite a été autorisée par le juge ;
- refuse de communiquer aux agents les renseignements et documents utiles à leur mission, dissimule lesdits documents ou renseignements, ou les détruit ;
- communique des informations non conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.

Délibération 2012-156 du 1 juin 2012

Dans une délibération du 1 juin 2012, la formation restreinte a constaté, entre autres, un manquement à l'obligation de coopération d'une société pour défaut de réponse à une trentaine de courriers et pour absence à deux convocations adressées par la Cnil.

Délibération SAN-2019-006 du 13 juin 2019

Dans le cadre du calcul du montant de la sanction pécuniaire prononcée à l'encontre d'une société de traduction, la formation restreinte de la Cnil a pris en compte comme critère la réticence de ladite société de se mettre en conformité malgré les échanges effectués avec la Cnil pendant plusieurs années.

Veiller aux communications en interne sur le contrôle

Il serait également intéressant de rappeler aux collaborateurs qu'ils ne devraient pas écrire de courriel, de mémos ou de tout autre document sur le contrôle. Exception faite si leur responsable hiérarchique, l'équipe juridique ou l'équipe de gestion du contrôle le demande.

En outre, il peut être dans certains cas opportun de ne pas avertir le personnel d'un contrôle. Dans ce cas, il arrive même que des accords de confidentialité soient signés par les membres de l'équipe de gestion du contrôle.

Organiser la fin du contrôle

A l'issue de chaque contrôle, un procès-verbal de fin de mission est établi. En fonction du type de contrôle opéré, il doit comporter un certain nombre de mentions, telles que les personnes entendues, les constatations des agents et les difficultés rencontrées lors du contrôle (Article 31 du Décret n°2019-536 du 29 mai 2019).

Lorsqu'il s'agit d'un contrôle sur place ou sur audition, le procès-verbal est établi contradictoirement. A cet effet, un espace est prévu pour que l'organisme contrôlé puisse formuler ses propres observations. Ainsi, il est important de garder une trace écrite des étapes du contrôle et des échanges avec les agents de la Cnil.

L'équipe de gestion du contrôle peut demander l'ajout de certaines précisions dans le procès-verbal qu'elle juge pertinentes et utiles notamment en cas d'une éventuelle procédure de sanction ou de contrôles ultérieurs.

Concernant les contrôles en ligne, le procès-verbal n'est pas établi de manière contradictoire, mais uniquement par les agents de la Cnil.

Dans la Charte des contrôles, la Cnil indique la nécessité de dresser un procès-verbal uniquement pour les contrôles sur place, sur audition et en ligne, à l'exclusion du contrôle sur pièces (Cnil, Charte des contrôles, 5 août 2020, p.7).

Or, l'article 19 de la loi n° 78-17 du 6 janvier 1978 prévoit « [qu'il] *est dressé procès-verbal des vérifications et visites menées en application du présent article* ». Dès lors, il semble que l'établissement du procès-verbal est exigé pour tout type de contrôle, les vérifications opérées grâce à la communication de renseignements et de documents étant également visées par cet article.

Il est ainsi possible de s'interroger sur les raisons qui justifieraient l'absence de procès-verbal pour les contrôles sur pièces. Etant précisé que d'un point de vue procédural, il peut s'avérer essentiel pour l'organisme d'avoir la retranscription de l'ensemble des éléments transmis, des constatations et des demandes de pièces complémentaires.

Fiche 5 - Quelles actions mettre en place à la suite d'un contrôle ?

Réaliser un diagnostic du contrôle qui a eu lieu

A la suite d'un contrôle, le DPO ou l'équipe de gestion du contrôle de l'organisme peut établir un diagnostic qui peut notamment inclure les étapes suivantes :

⇒ Déterminer si les documents communiqués et les explications fournies étaient suffisants ;

⇒ Chercher à savoir si tout facteur favorable à l'organisme a été mis en exergue au cours du contrôle ;

⇒ Evaluer si un contrôle complémentaire est susceptible d'être effectué auprès d'une filiale, de la maison-mère, d'une agence, d'un magasin, etc. ;

⇒ Déterminer s'il y a lieu de mettre en œuvre des mesures correctrices et les documenter.

Ce diagnostic peut être accompagné d'une réunion avec les dirigeants de l'organisme afin de présenter les risques éventuels qui pèsent sur l'organisme.

Echanges ultérieurs avec la Cnil : communication de pièces complémentaires

A l'issue du contrôle, les agents de la Cnil peuvent demander des informations additionnelles. Une liste de documents nécessaires à l'accomplissement de leur mission est souvent insérée à la fin du procès-verbal, avec l'indication d'un délai de transmission.

Il est conseillé de ne pas hésiter à demander un délai supplémentaire en fonction des actions ou démarches à réaliser. Il peut s'agir, par exemple, de demandes à formuler auprès des sous-traitants.

Comment transmettre les documents ?

Quel que soit le type de contrôle, il convient de garder à l'esprit que les documents doivent être transmis de manière sécurisée. A ce titre, la Cnil conseille les moyens de transmission suivants :

- Transmission au format papier par courrier recommandé avec avis de réception ou par porteur ;
- Transmission au format numérique par courrier électronique ou par l'envoi d'un support numérique (par exemple, clé USB) par courrier recommandé avec avis de réception, en veillant à mettre en place une **mesure de chiffrement**. Etant précisé que le mot de passe de déchiffrement doit être transmis à la Cnil par un autre moyen que celui permettant de transmettre les documents.

Source : Cnil, Charte des contrôles, 5 août 2020, p.14

Actions à mettre en place en interne

Il est fortement recommandé aux organismes contrôlés de « tirer les leçons » du contrôle. A ce titre, plusieurs actions peuvent être envisagées en interne :

- **Sensibilisation du personnel**

L'organisme contrôlé et notamment son DPO peuvent se servir de leur expérience de contrôle dans le cadre de la sensibilisation du personnel. Ainsi, le déroulement des entretiens, les questions posées par les agents de la Cnil ainsi que les documents recueillis peuvent être utilisés comme illustration au cours de la formation.

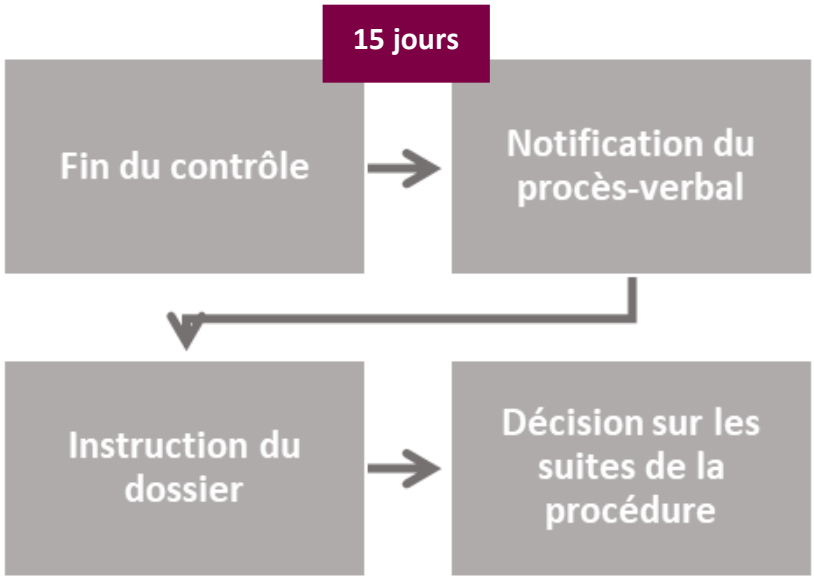
- **Audits internes et/ou externes**

Le contrôle diligenté au sein de l'organisme peut constituer selon les cas une source d'alerte sur la nécessité de réaliser des audits internes ou encore chez les sous-traitants lorsque l'organisme contrôlé est responsable du traitement. En effet, l'organisme contrôlé n'est pas à l'abri de contrôles ultérieurs portant sur des sujets qui ne s'inscrivaient pas dans l'objet du contrôle initial. Ainsi, la réalisation de ces audits peut être intégrée dans le plan d'actions de l'organisme.

Fiche 6 - Quelles sont les suites que la Cnil peut donner à un contrôle ?

A l'issue du contrôle, le **procès-verbal** est notifié à l'organisme contrôlé dans un délai de 15 jours par courrier recommandé avec accusé de réception (Cnil, Charte des contrôles, 5 août 2020, p.15).

La Cnil analyse ensuite le dossier afin d'évaluer le niveau de conformité de l'organisme. En fonction des manquements constatés, cette analyse peut conduire à la clôture de la procédure de contrôle, au prononcé d'une mise en demeure ou encore à l'ouverture d'une procédure de sanction. Notons que cette analyse ne semble enfermée dans aucun délai.



1 Clôture de la procédure

La Présidente de la Cnil peut décider de clore la procédure en **l'absence de manquements** ou encore en cas de constatation de **manquements peu graves** (Cnil, Charte des contrôles, 5 août 2020, p.15). Dans le dernier cas, la lettre de clôture adressée par la Présidente de la Cnil indique le plus souvent des **recommandations sur les actions à mettre en œuvre** par l'organisme afin de se mettre en conformité.

L'organisme contrôlé peut s'attendre à être contacté par la Cnil pour l'informer des actions mises en œuvre afin de répondre aux recommandations énoncées. Ces demandes post-contrôle sont souvent écrites et conduisent à la fourniture de documents additionnels. Le but est en effet de limiter le risque d'une autre procédure de contrôle.

2 Prononcé d'une mise en demeure

Dans l'hypothèse où des **manquements significatifs** ont été constatés, la Présidente de la Cnil peut décider de mettre en demeure l'organisme contrôlé (Article 20, II de la Loi n° 78-17 du 6 janvier 1978— Cnil, Charte des contrôles, 5 août 2020, p.16). A ce titre, un délai est indiqué à l'organisme pour corriger les manquements et se mettre en conformité.

Délibération MED-2020-015 du 15 juillet 2020

Les agents de la Cnil avaient réalisé trois contrôles au mois de juin 2020 pour vérifier la conformité du fonctionnement de l'application anciennement dénommée « StopCovid » (un contrôle en ligne complété par deux contrôles sur place). Par une décision du 15 juillet 2020, la Présidente de la Cnil a prononcé une mise en demeure à l'encontre du ministère des solidarités et de la santé, clôturée un mois plus tard à la suite des réponses apportées par le ministère.

A noter que depuis 2016, la mise en demeure ne constitue plus un préalable à l'ouverture d'une procédure de sanction.

Délibération SAN-2019-001 du 21 janvier 2019

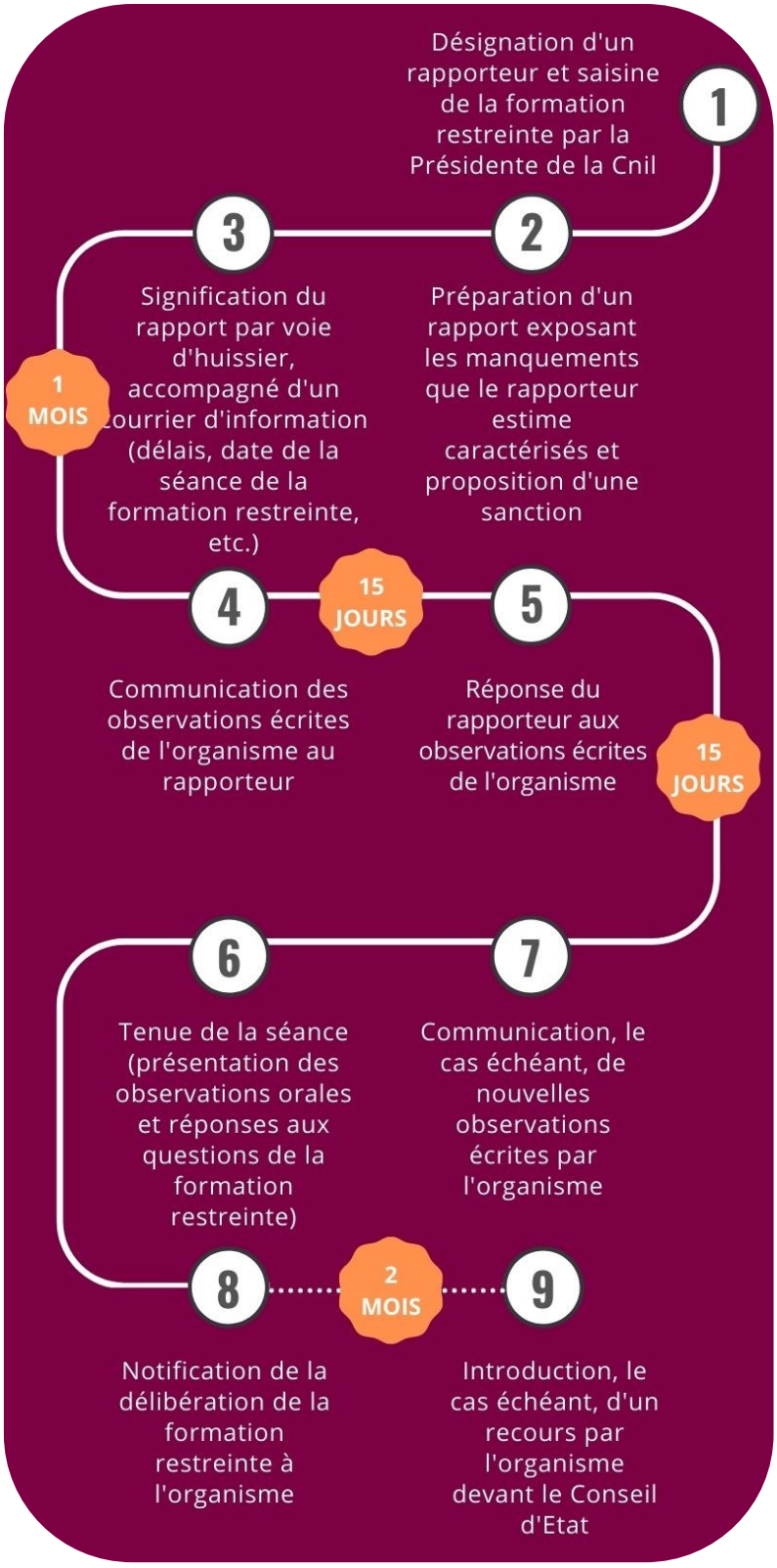
Une procédure de sanction a été engagée à l'encontre d'un éditeur de système d'exploitation à la suite d'un contrôle en ligne diligenté par les agents de la Cnil, sans mise en demeure préalable.

Il est possible qu'un nouveau contrôle soit diligenté à la suite d'une mise en demeure. Cela signifie qu'en pratique, l'organisme contrôlé doit rester vigilant et suivre son plan d'actions de conformité quelle que soit l'issue de la procédure de contrôle.

Délibération SAN-2019-006 du 13 juin 2019

3 Ouverture d'une procédure de sanction et ses suites

En cas de manquements significatifs, d'absence de réponse à une mise en demeure ou de mise en conformité dans le délai imparti, la Présidente de la Cnil peut ouvrir une procédure de sanction (Article 20, III de la Loi n° 78-17 du 6 janvier 1978— Cnil, Charte des contrôlés, 5 août 2020, p.16).



Diligences et vérifications ultérieures par le rapporteur

Le rapporteur a la faculté de procéder « *à toutes diligences utiles avec le concours des services de la commission* » (Article 39 du Décret n° 2019-536 du 29 mai 2019).

A ce titre, il peut notamment auditionner l'organisme concerné lorsqu'il l'estime utile.

Délibération SAN-2020-003 du 28 juillet 2020

A la suite d'un contrôle sur place et après l'ouverture d'une procédure de sanction, le rapporteur a convoqué la société concernée à une audition. Cette dernière a eu lieu avant la rédaction par le rapporteur de son rapport.

Auditions lors de la séance de la formation restreinte

Lors de la séance, la formation restreinte peut entendre toute personne lorsqu'elle l'estime utile (Article 42 du Décret n° 2019-536 du 29 mai 2019).

Il est donc conseillé de préparer l'audience avec l'ensemble des membres du personnel qui seront présents lors de la séance.

Suivez l'actualité juridique sur notre blog

www.avocats-mathias.com/blog

Mathias Avocats

Nous sommes un Cabinet d'avocats indépendant spécialisé dans le droit du numérique (IP/IT/Data).

Nous accompagnons nos clients, de manière pragmatique, au gré des évolutions juridiques et technologiques. Nous les assistons également dans leur contentieux (juridictions judiciaires, autorités de contrôle).

Nous collaborons avec des avocats partenaires exerçant dans le monde entier.

Nos interventions allient la rigueur, la créativité et l'efficacité d'une équipe dédiée et mobilisée aux côtés de ses clients.

Avertissement

Mathias Avocats

Avez-vous des questions ?

Une équipe dédiée répond à vos questions et vous accompagne dans vos actions de conformité.

01 43 80 02 01

contact@avocats-mathias.com

19, rue Vernier – 75017 – Paris

Suivez-nous sur les réseaux sociaux