Mars 2019

Que faire quand la Cnil frappe à votre porte ?

Fiches pratiques pour anticiper et gérer un contrôle

Mathias Avocats

SOMMAIRE

INTRODUCTION

Le contrôle figure parmi les missions dévolues à la Commission Nationale de l'Informatique et des Libertés (Cnil) et lui permet de s'assurer de la bonne application de la réglementation relative à la protection des données à caractère personnel. Il peut être mis en œuvre à la suite d'une plainte, à la demande d'une autorité de protection des données établie dans un autre Etat membre de l'Union européenne ou encore sur initiative de la Cnil.

Les conséquences qui peuvent en résulter pour l'organisme contrôlé, notamment son image de marque, conduisent généralement les responsables de traitement et les sous-traitants à redouter ces contrôles.

Dans ce contexte, deux stratégies peuvent être adoptées : l'une peut consister à réagir une fois que la Cnil est à votre porte, l'autre peut consister à agir et anticiper le contrôle en élaborant une procédure adaptée à la taille et l'activité de votre organisme.

Mathias Avocats accompagne ses clients dans les deux cas, mais ce Livre blanc a pour objectif d'encourager les responsables de traitements et les sous-traitants à opter pour la seconde solution. En effet, grâce au cadre juridique en vigueur, des outils de conformité et de gouvernance sont d'ores et déjà mis à disposition des acteurs afin de leur permettre de gérer le risque (registre, analyse d'impact, désignation d'un délégué à la protection des données, etc.).

En diffusant ce Libre Blanc, nous avons souhaité vous faire bénéficier de notre expérience de la pratique précontentieuse et contentieuse relative à la protection des données à caractère personnel.

Nous vous souhaitons une bonne lecture, en espérant sincèrement que les lignes qui suivent pourront vous être utiles dans l'hypothèse où vous seriez confronté(e) à un tel contrôle.

Restant à votre écoute,

Garance Mathias

Avocat Associé
Mathias Avocats

Fiche 1 - Rappel du contexte

Les visites de contrôle de la Cnil sont en pleine expansion et cette tendance va sans nul doute continuer. Ainsi, en 2017, les agents de la Cnil ont procédé à 341 contrôles, dont 65 contrôles en ligne et 47 contrôles de vidéoprotection. Par ailleurs, la Présidente de la Cnil a mis en demeure 79 organismes. Enfin, la formation restreinte de la Cnil a prononcé 14 sanctions dont 9 sanctions financières et 5 avertissements (2018 - La CNIL en bref).

Nous attendons désormais le bilan de l'année passée qui devrait être publié en avril prochain. Cela nous permettra d'évaluer si l'entrée en application du Règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) le 25 mai 2018 a impacté fortement ou non l'activité de la Cnil.

En effet, ce nouveau cadre européen, bien qu'il s'agisse d'un règlement d'application directe, a nécessité une adaptation de la loi n° 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (la loi Informatique et Libertés). Ainsi, la loi n° 2018/493 relative à la protection des données personnelles du 20 juin 2018 (la Loi sur la protection des données) a été adoptée définitivement après de nombreux débats entre les deux Chambres du Parlement le 14 mai 2018. Sa promulgation a été retardée du fait de la saisine du Conseil Constitutionnel qui a rendu sa décision le 12 juin 2018. Le décret n° 2005-1309 du 20 octobre 2005 pris en application de la loi Informatique et Libertés a également été modifié par décret n° 2018-687 du 1er août 2018.

Cependant, les praticiens de la protection des données avaient déjà mis en exergue de nombreuses incohérences et imprécisions dans la Loi relative à la protection des données lors des débats parlementaires. C'est pourquoi la possibilité pour le Gouvernement de recourir à une ordonnance de réécriture avait été intégrée dans cette loi, afin de la rendre intelligible et cohérente. L'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la Loi relative à la protection des données et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel a ainsi pour objectif d'améliorer la lisibilité du cadre juridique en la matière.

Dans ce cadre législatif en mouvement, de nouveaux pouvoirs ont été dévolus à la Cnil.

Fiche 2 - Pourquoi mon organisme est-il contrôlé ?

Les agents de la Cnil peuvent contrôler tout organisme traitant des données à caractère personnel disposant d'un établissement en France, ou concernant des personnes résidant en France.

Bien souvent, les organismes sont sélectionnés pour des contrôles portant sur la conformité au cadre réglementaire de la protection des données à caractère personnel pour l'une (ou plusieurs) des raisons suivantes :

⇒ Lorsque l'organisme procède à des traitements inscrits dans le programme annuel de la Cnil.

En effet, en France, 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. Par exemple, dans le programme pour l'année 2018, la Cnil avait planifié des contrôles sur trois grandes thématiques : les traitements liés au recrutement, les pièces justificatives demandées par les agences immobilières et les traitements relatifs à la gestion des services de stationnement.

⇒ Lorsqu'une personne concernée a déposé une plainte auprès de la Cnil (ou bien une association).

Les plaintes sont en forte hausse ces dernières années. Cette recrudescence peut être liée à une prise de conscience par le public de l'importance d'une protection accrue de ses données personnelles.

À noter que, si la Cnil estime fondés les griefs avancés relatifs à la protection des droits et libertés d'une personne, elle peut saisir le Conseil d'État afin que celui-ci ordonne la suspension d'un transfert de données vers un Etat non membre de l'Union européenne et transmette une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de la décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du RGPD (article 43 quinquies, Loi Informatique et Libertés).

⇒ Si une autre autorité publique suspecte ou constate une non-conformité à la réglementation relative à la protection des données personnelles et qu'elle en a alerté la Cnil.

La Commission peut opérer un contrôle notamment à la suite d'informations transmises par la Cnil d'un autre État membre de l'Union européenne. Dans ce cas, le responsable de traitement ou le sous-traitant doit en être

informé. Il sera également informé du fait que les informations collectées au cours des vérifications pourront être transmises à la Cnil « étrangère » (article 63 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

La Cnil peut également diligenter un contrôle après avoir obtenu des informations de la part d'une association de protection des consommateurs ou de tout autre autorité publique avec laquelle un partenariat serait mené concernant la protection des données. A titre d'illustration, en vertu d'un protocole de coopération conclu en 2011, mis à jour depuis le 31 janvier 2019, 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 - ont renforcé leur collaboration. Il s'agira notamment de réaliser des contrôles communs.

⇒ Si l'attention des médias s'est portée sur l'organisme.

C'est le cas par exemple lorsqu'une importante violation des données a été rendue publique.

A titre d'illustration, la Cnil avait été informée par l'éditeur d'un site internet spécialisé dans la sécurité des systèmes d'information d'une violation de données à caractère personnel à partir de l'URL d'un site de la société Etablissements Darty et fils. Par la suite, les agents de la Cnil avaient réalisé un contrôle en ligne, puis un contrôle sur place permettant de démontrer qu'une défaillance de sécurité rendait plusieurs centaines de milliers de demandes ou réclamations concernant le traitement des demandes de service après-vente librement accessibles. Une sanction d'un montant de 100.000 euros a été prononcée par la formation restreinte.

⇒ Si un contrôle a eu lieu dans la filiale d'une entreprise.

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. Ce sera par exemple le cas lorsque l'entité initialement contrôlée n'est pas le responsable de traitement de l'activité visée par la Cnil. A titre d'illustration, le groupe peut avoir réparti les activités BtoC et BtoB dans deux entités différentes. Si le contrôle est réalisé dans les locaux de la société en charge du BtoB alors que les agents souhaitent auditer l'activité BtoC, il sera pertinent d'anticiper un contrôle dans les locaux de la société en charge de l'activité BtoC.

Si 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.

⇒ Si un contrôle a eu lieu chez un prestataire ou un client.

Si un contrôle a lieu chez un prestataire auquel a été confié tout ou partie des activités de traitement de données personnelles, les agents de la Cnil sont susceptibles de procéder à un contrôle complémentaire chez le responsable de traitement ou le responsable conjoint de traitement. Inversement, si un contrôle est diligenté chez un responsable de traitement, la présidente de la Cnil peut décider de faire procéder à un contrôle chez le sous-traitant ou le responsable conjoint de traitement.

L'application du RGPD a une influence forte sur les relations entre responsable de traitement et sous-traitant. Jusque-là, seul le responsable de traitement assumait les manquements à la réglementation auprès de l'autorité de contrôle de protection des données à caractère personnel. Le sous-traitant était, de ce point de vue, à l'abri des sanctions prononcées par la Cnil.

⇒ Les dispositifs de vidéoprotection

En application de l'article L.253-2 du Code de la sécurité intérieure, la Cnil est compétente pour contrôler les conditions de fonctionnement des systèmes de vidéoprotection de la voie publique.

Fiche 3 - Quels types de contrôle ?

Quel que soit le contrôle, deux agents du service des contrôles (ou plus) seront désignés par la Présidente de la Cnil pour mener la mission, un juriste et un auditeur des systèmes d'information.

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 de données à caractère personnel avec la réglementation en vigueur.

A noter que l'article 44 de la Loi Informatique et Libertés a été modifié par l'article 5 de la Loi sur la protection des données. Auparavant, les agents de la Cnil ne pouvaient se rendre que dans des locaux à usage professionnel. Cette limitation a été supprimée, seule la protection du domicile privé demeure dans la nouvelle version.

Préalablement au contrôle sur place, le procureur de la République compétent en est informé au plus tard 24 heures auparavant la date de la visite (article 61 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Quant à l'organisme contrôlé, il est informé au plus tard lors de son arrivée sur place de l'objet du contrôle, de l'identité des agents de la Cnil et du droit d'opposition à la visite (article 62 du décret précité).

Dans l'hypothèse où il exerce son droit d'opposition, le contrôle ne pourra avoir lieu qu'après autorisation du juge des libertés et de la détention du tribunal de grande instance compétent. Ce même juge peut également autoriser préalablement une visite à laquelle le responsable des lieux ne pourra s'opposer, « lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie ». Le droit d'opposition peut être exercé après avoir permis aux agents de la Cnil d'entrer dans les locaux (article 56 du Règlement intérieur de la Cnil). Un procès-verbal sera établi en ce sens.

Lors du contrôle sur place et conformément à l'article 55 du Règlement intérieur de la Cnil, les agents peuvent être assistés d'experts à la demande de la Présidente de la Cnil. Ces experts sont « désignés par l'autorité dont ils dépendent ». Toutefois, cette faculté soulève des questions. Par exemple, ces experts relèvent-ils du régime des experts judiciaires ?

Contrôle sur pièces

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 (article 44, III, de la loi Informatique et

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

L'organisme reçoit une lettre recommandée de la part du service des contrôles de la Cnil qui l'informe du contrôle sur pièces. Ce contrôle porte généralement sur un sujet précis, indiqué dans la lettre, comme le recueil et la transmission de données à caractère personnel à des organismes partenaires par exemple. Les éléments demandés par la Cnil doivent être communiqués avant l'expiration d'un délai indiqué dans la lettre.

La décision de procéder à une mission de contrôle auprès de l'organisme et l'ordre de mission, ainsi que le questionnaire destiné à évaluer les pratiques au regard de la réglementation en vigueur le cas échéant, sont annexés à cette lettre. En outre, toute pièce justificative ou illustrative peut être adressée, notamment quant à la présentation générale de l'organisme ou le cadre contractuel formalisant le traitement de données à caractère personnel mis en place (organigramme, contrats, politiques et procédures, dessins d'enregistrement, matérialisation en base de données, etc.).

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

Contrôle sur audition

Les agents de la Cnil peuvent également convoquer toute personne qu'ils souhaitent interroger dans le cadre d'une mission de contrôle (article 44, III, de la loi Informatique et Libertés). La convocation est adressée « par lettre remise contre signature, ou remise en main propre contre récépissé ou acte d'huissier », réceptionnée au moins 8 jours avant la date de l'audition.

Lors de l'audition, la personne interrogée peut être assistée du conseil de son choix.

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 connecté à Internet, et sans la présence du responsable du traitement ou du sous-traitant. Ce type de contrôle a été créé par la loi « Hamon » relative à la consommation du 17 mars 2014 (article 44, III, de la loi Informatique et Libertés).

La Cnil a ainsi un pouvoir d'investigation adapté au développement numérique et peut notamment constater des violations de données. Cela per-

met à la Cnil de vérifier plus spécifiquement certains aspects de la Loi Informatique et Libertés, notamment :

⇒ la pertinence des données collectées (article 6 de la loi) ;

⇒ les mentions d'information à destination du public (article 32 de la loi) ;

⇒ la sécurité des données collectées et traitées (article 34 de la loi).

Ce contrôle en ligne permet également de vérifier la conformité des pratiques des organismes à la réglementation relative aux cookies et autres traceurs adoptée. Ainsi la Cnil vérifiera :

⇒ le nombre et la nature des cookies déposés sur le poste informatique de l'utilisateur ;

⇒ les modalités d'information à destination du public en matière de cookies ;

⇒ la qualité et la pertinence de l'information ;

⇒ les modalités de recueil du consentement de l'utilisateur.

Ce pouvoir s'applique aux données librement accessibles ou rendues accessibles en ligne, y compris par imprudence, par négligence ou par le fait d'un tiers. Il ne donne pas, évidemment, la possibilité à la Cnil de forcer les mesures de sécurité mises en place pour pénétrer dans un système d'information.

En pratique, le contrôle en ligne peut être indépendant ou complémentaire d'un contrôle sur place, sur pièce ou sur audition. Il se déroule de façon similaire au contrôle sur place : une décision de contrôle est prise par la Présidente de la Cnil, un ordre de mission désigne les agents chargés de réaliser le contrôle et un procès-verbal de constatation est rédigé. Cependant, le contrôle et le procès-verbal ne sont pas effectués de manière contradictoire. Le procès-verbal de constatation et les vérifications de l'environnement de contrôle sont adressés à l'entité concernée dans les 8 jours qui suivent le contrôle. Au terme de la procédure, la Cnil décide si les constations doivent donner lieu à une mise en demeure ou à une procédure de sanction.

Par ailleurs, la loi relative à la protection des données personnelles a modifié l'article 44 de la loi Informatique et libertés. Désormais, les agents de la Cnil peuvent effectuer des contrôles en ligne sous une identité d'emprunt, sans incidence sur la régularité de la procédure. A 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. À la suite de ce contrôle, un procès-verbal sera rédigé dans lequel seront décrites les modalités de consultation et d'utilisation des services de communication au public

en ligne, des réponses obtenues et de leurs constatations. A priori, les « réponses obtenues » rapportées dans le procès-verbal pourront également être celles de *chatbots*. Il conviendra donc de veiller au paramétrage de ces agents conversationnels.

Fiche 4 - Comment anticiper un contrôle ?

Afin de faire face à un contrôle mené par la Cnil, les administrations, les entreprises et les associations se doivent d'être proactives. En effet, outre les éventuelles sanctions financières qui pourraient être prononcées, tout contrôle emporte des risques pour la réputation de l'entité. A noter que, parfois, la non-conformité est identifiée une fois l'inspection menée. Ainsi, la continuité des activités peut être remise en cause, même pour des entités qui semblent, au premier abord, en totale conformité avec le cadre réglementaire.

Les politiques de protection des données personnelles déjà mises en place au sein de l'entité sont des facteurs importants dans la gestion des contrôles. Les organismes conscientes des risques et qui y sont préparés seront en mesure de gérer plus efficacement les contrôles.

Effectuer un audit de conformité

La première étape pour un responsable de traitement ou un sous-traitant est de se pencher sur la conformité à la réglementation en vigueur et mettre en place les changements nécessaires. La conformité minimale implique notamment :

⇒ l'information des personnes concernées sur la collecte et le traitement de leurs données personnelles,

⇒ la tenue d'un registre des traitements,

⇒ la mise en place de procédures et de politiques écrites (par exemple sur la sécurité des données, la conservation des données),

⇒ la désignation d'un délégué à la protection des données personnelles (DPO).

Préparer les documents généralement demandés par la Cnil

La mission de contrôle vise prioritairement à obtenir copie du maximum d'informations, techniques et juridiques, pour apprécier les conditions dans lesquelles sont mis en œuvre des traitements de données à caractère personnel.

Ces documents pourront par exemple permettre à la Cnil de prendre connaissance de la politique de sécurité mise en place. Aussi, mieux vaut avoir ces documents sous la main lorsque les agents les demandent. Ils devront refléter la réalité car les agents ne se contenteront pas de les lire mais également de vérifier leur application effective.

Il est par ailleurs pertinent de réfléchir en amont aux éventuels documents que l'organisme souhaiterait ne pas communiquer aux agents de la Cnil en cas de contrôle. Il est possible d'invoquer le secret applicable aux relations entre un avocat et son client, le secret

des sources des traitements journalistiques ou le secret médical (article 44, III, de la Loi Informatique et Libertés). L'organisme doit indiquer les dispositions législatives ou réglementaires sur lesquelles il s'appuie et la nature des données couvertes. La mention de l'opposition, son fondement textuel et la nature des données figureront sur le procès-verbal rédigé par les agents de la Cnil à l'issue du contrôle.

Rédiger une procédure de gestion de contrôle

Il apparaît judicieux d'élaborer une procédure qui énonce comment réagir à la visite de la Cnil. Le plan de gestion de crise permet notamment de déterminer qui est le responsable des lieux ou encore quels sont les bureaux et les ressources mises à disposition des agents de la Cnil. Il sera également important de préciser que le DPO doit être immédiatement prévenu (même si cela conduit à interrompre une réunion).

La procédure peut prévoir la mise en œuvre d'une « équipe de gestion de crise » qui inclut les principaux responsables pour gérer le contrôle. Il peut ainsi s'agir du DPO, du directeur juridique, du DSI, du RSSI et des responsables des départements les plus importants (comme les DRH ou le directeur marketing par exemple) selon l'objet du contrôle. Il est intéressant de prévoir d'ores et déjà la composition de l'équipe (par métier et non de manière nominative), la manière d'accueillir et d'accompagner les agents le temps de leur contrôle, la manière de répondre à leurs questions, la coordination avec les autres membres du personnel, la présence aux entretiens, etc. Les membres de l'équipe devront alors être informés directement d'une visite de la Cnil. Ainsi, leurs numéros de téléphones devront-ils être disponibles dans les bureaux et surtout à l'accueil, afin de pouvoir les contacter au plus vite s'ils ne sont pas présents et que l'organisme fait face à un contrôle. À noter que les agents de la Cnil peuvent s'entretenir avec les personnes de leur choix.

Il conviendra également de préciser si l'avocat conseil spécialisé en la matière doit être contacté.

Dans tous les cas, anticiper un éventuel contrôle de la Cnil relève de l'application du fameux principe d'*accountability*.

Sensibiliser et former le personnel

Un bon niveau de conformité permet de préparer l'organisme et son personnel aux contrôles. Une formation régulière ainsi qu'une connaissance des obligations générales de l'entité et de ses salariés permettra notamment de minimiser les risques de non-conformité.

Les membres du personnel devront également être sensibilisés sur le rôle qu'ils pourront avoir à jouer lors de

l'inspection. Il est nécessaire qu'ils sachent à quoi s'attendre lors du contrôle et de son impact éventuel. Si les employés sont préparés, ils seront alors mieux à même de répondre aux questions de la Cnil et d'identifier les documents demandés.

La formation devra inclure des sujets comme :

⇒ la manière de répondre aux questions,

⇒ la manière de communiquer les documents,

⇒ les risques d'une obstruction à l'enquête, lorsque des informations fausses ou trompeuses sont communiquées,

⇒ etc.

Les réceptionnistes et les gardiens devront plus particulièrement 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 5 - Comment gérer un contrôle sur place ?

Les agents de la Cnil ne procèdent aux investigations que sur décision de la Présidente de la Cnil. Pour les contrôles en ligne, sur audition et sur pièces, plusieurs recommandations exposées ci-dessus seront applicables. Dans tous les cas, il est conseillé d'être diligent dans les échanges avec la Cnil et de répondre aux interrogations de ses agents.

A leur arrivée sur place, les agents de la Cnil notifient au responsable des lieux la décision de la Présidente de la Cnil autorisant le contrôle. En outre, d'autres documents peuvent être demandés et analysés par le responsable de traitement ou le sous-traitant avant la tenue du contrôle (ordre de mission et habilitations).

Vérifier les habilitations des agents de la Cnil

Les auditeurs pouvant réaliser des missions de contrôle sont habilités à cet effet par une délibération du Bureau de la Cnil, disponible sur le site de la Cnil. Cette habilitation vaut pour une durée de 5 ans.

À noter qu'une décision du Premier ministre habilite certains agents de la Cnil à procéder à des contrôles portant sur les traitements relevant de l'article 26 de la loi Informatique et Libertés (mis en œuvre pour le compte de l'Etat et ayant notamment pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales). 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 pour la mise en œuvre du contrôle.

Analyser l'ordre de mission

L'ordre de mission présenté par les agents de la Cnil à la demande de l'organisme contrôlé spécifie l'objet du contrôle (article 62 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Il est donc conseillé de solliciter la communication de l'ordre de mission dès le début des investigations. L'équipe de gestion de crise de l'organisme devra alors déterminer la portée du contrôle, notamment afin de savoir si celui-ci se concentre sur un secteur en particulier (le service client, les ressources humaines, etc.) ou bien encore si le contrôle est dû à une visite prévue dans le cadre du programme annuel de la Cnil.

Il est important de discuter du déroulement du contrôle puisque cela permet à l'organisme de mieux organiser les ressources nécessaires pour rassembler les informations et pour planifier les éventuels entretiens avec les membres du personnel. De plus, cela permettra de limiter les perturbations dans les activités de l'entité, tout en permettant aux collaborateurs interrogés de se rendre disponibles.

Prévoir la logistique

Une fois que les agents sont arrivés, ils doivent 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 (téléphone, papiers, fournitures, etc.).

Par ailleurs, en plus de cette pièce, un lieu pour leur permettre de faire des photocopies doit leur être attribué. Il est par ailleurs important 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.

L'équipe de gestion de crise doit identifier tout problème de logistique quand elle répond à la requête 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). L'agent ne comprend pas toujours l'organisation de l'entité et le procédé de gestion des documents. Cependant, les représentants de l'organisme devront s'abstenir de questionner sur la pertinence du document demandé. Ils devront plutôt expliquer aux agents leurs difficultés et demander ainsi un report du délai imposé par la Cnil pour la remise des documents.

Transmettre des documents

Les agents de la Cnil doivent notamment pouvoir compter sur la pleine collaboration des organismes contrôlés, en vertu de l'article 21 de la Loi Informatique et Libertés, de « prendre toutes mesures utiles afin de faciliter [la] tâche » de l'autorité de contrôle. Le DPO peut avoir à fournir des documents en tant que point de contact de la Cnil et en vertu de son obligation de coopération. D'autres membres du personnel peuvent toutefois être également concernés.

Les agents sont par ailleurs autorisés à consulter et à demander des copies de documents, à s'entretenir avec le personnel, à examiner et imprimer les données électroniques. Ils peuvent également effectuer des contrôles sur des outils, des supports de données ou un système d'information utilisé pour le traitement des données mais aussi demander des explications écrites ou orales.

Les documents fournis aux agents doivent répondre à leur demande mais pas au-delà. Sans demande expresse de document, il est recommandé de se limiter à répondre aux questions.

Dans tous les cas, les documents sensibles devront être marqués comme étant « confidentiels » avant toute copie.

L'équipe de gestion de crise devra garder une liste des documents qui auront été communiqués aux agents, en faisant, par exemple, référence à la

date ou à la version du document. Il lui faudra également garder les copies de tous les documents ou extraits de documents photocopiés par les agents. Il ne faudra pas oublier non plus de dresser la liste des éléments demandés par les agents mais qui ne leur ont pas encore été délivrés.

Echanger avec les agents de la Cnil

Les agents demandent toujours des entretiens avec le personnel de l'entité et il peut leur arriver de demander à voir une personne en particulier. Il est recommandé de répondre positivement à cette demande. A noter que, parfois, les auditeurs peuvent s'entretenir avec une autre personne suggérée par l'équipe de gestion de crise. Il faut cependant garder à l'esprit que la non-présentation de l'employé convoqué pour un entretien peut être interprétée comme une entrave à l'inspection.

Sous réserve de l'accord exprès du supérieur hiérarchique, de l'équipe juridique ou de l'équipe de gestion de crise, 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 établi en fin de contrôle.

Lorsque l'organisme est prévenu du contrôle avant le jour de son déroulement, l'équipe de gestion de crise doit s'interroger sur les personnes qui seront probablement appelées à s'entretenir avec les agents. Des réunions devront donc 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. A noter que l'équipe de gestion de crise de la société devra être présente pendant l'entretien.

Si les agents sont d'accord, il serait bon de commencer et de finir chaque journée par une réunion entre l'équipe de gestion de crise et les agents.

Eviter le délit d'entrave

S'opposer aux demandes des agents, leur refuser le droit d'accéder aux locaux et à des documents ou tout autre refus pourra être perçu comme une entrave au contrôle. Empêcher les agents de mener à bien leurs tâches est punissable d'une peine d'un an d'emprisonnement et d'une amende de 15 000€ d'amende. Conformément à l'article 51 de la loi Informatique et Libertés, le délit d'entrave à l'action de la Cnil est constitué par :

⇒ l'opposition à l'exercice des missions confiées aux agents de la Cnil lorsque la visite a été autorisée par le juge ;

⇒ le refus de communiquer aux agents de la Cnil les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les détruisant ;

⇒ la communication d'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.

La Cnil a déjà prononcé un avertissement public pour défaut de coopération notamment contre une société qui avait ignoré une trentaine de courriers qu'elle avait envoyés et deux convocations suite à l'impossibilité à procéder un contrôle sur place.

Lorsqu'elle constate un délit d'entrave, la Cnil peut également dénoncer les faits au Procureur de la République. Le Tribunal de grande instance de Paris a, par exemple, prononcé une amende de 5 000€ dont 4 000€ avec sursis sur le fondement de l'article 51 de la loi Informatique et Libertés suite au refus du Directeur général de l'entreprise contrôlée de permettre aux agents de la Cnil de poursuivre leur investigations alors que le Président directeur général, désigné responsable des lieux, ne s'était pas opposé au contrôle.

Communiquer en interne sur le contrôle

Il peut également être intéressant de rappeler aux employés qu'ils ne doivent pas écrire de mail, de mémos ou tout autre document sur le contrôle. Exception faite si leurs managers, l'équipe juridique ou l'équipe de gestion de crise le demande.

En outre, il est parfois opportun de ne pas avertir le personnel d'un contrôle. Dans ce cas, il arrive même que des accords de confidentialités soient signés par les membres de l'équipe de gestion de crise.

Organiser la fin du contrôle

Un procès-verbal de fin de mission est établi contradictoirement à l'issue du contrôle dont le contenu est prévu par le décret d'application de la loi.

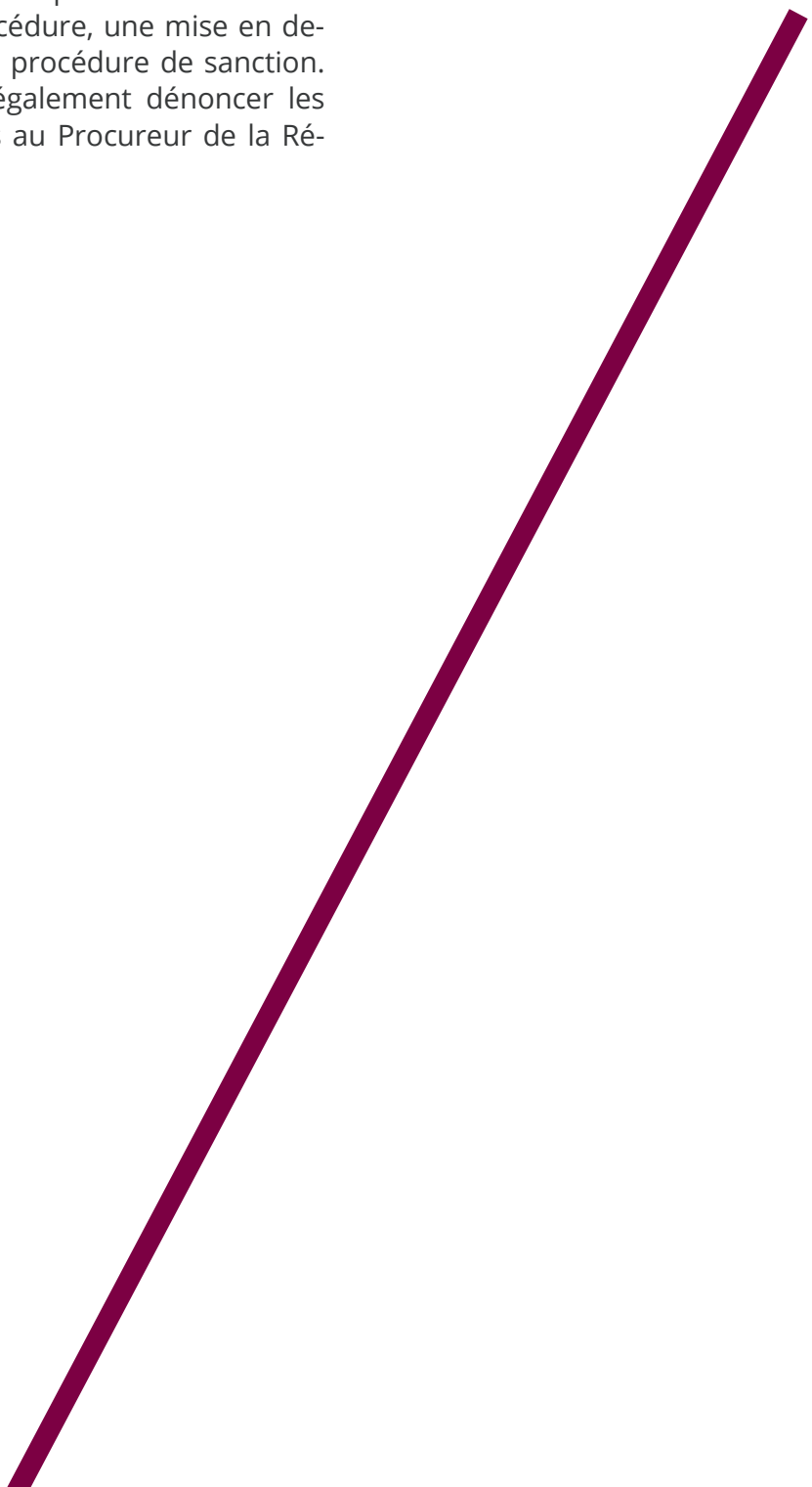
Il est important de garder une trace écrite des étapes du contrôle et de toutes les communications avec les agents. Le procès-verbal doit inclure toutes les questions ou demandes de la Cnil, toutes les réponses à celles-ci, le nom de la personne qui y a répondu, etc..

Il peut permettre de contredire les conclusions des agents ou le rapport du rapporteur désigné par la Présidente de la Cnil si une procédure de sanction est engagée. Il sert aussi à préparer au mieux les éventuels contrôles ultérieurs.

L'équipe de gestion de crise peut demander l'ajout de certaines précisions dans le procès-verbal. Par exemple, si une remarque des agents de la Cnil paraît déplacée, il est possible de le faire noter dans le procès-verbal. Il est

par ailleurs pertinent de faire inscrire le fait que, selon l'organisme contrôlé, une réparation du manquement constaté par les agents de la Cnil - lorsque celui-ci est manifeste et évident - est envisageable à bref délai.

Trois issues sont possibles : une clôture de la procédure, une mise en demeure ou une procédure de sanction. La Cnil peut également dénoncer les faits constatés au Procureur de la République.



Fiche 6 - Quelles actions mettre en place à la suite d'un contrôle ?

A la suite du contrôle, les membres de l'équipe d'inspection de la société devront notamment :

⇒ savoir si les documents communiqués et les explications donnés étaient suffisants ;

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

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

⇒ se demander s'il est nécessaire de corriger une mauvaise impression. Selon le résultat du contrôle (notamment si des sanctions sont à prévoir), l'équipe d'inspection va devoir déterminer quelles actions doivent être prises afin de remédier aux manquements constatés. A noter qu'il est nécessaire que les actions correctrices envisagées soient documentées.

Echanger avec les agents de la Cnil

A la suite du contrôle, les agents 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 rédigé à l'issue du contrôle. Un délai de transmission de ces documents est indiqué. Il convient de garder à l'esprit qu'ils doivent être transmis de manière sécurisée, aussi est-il conseillé de contacter un agent de la Cnil dont les coordonnées sont fournies afin de lui demander les modalités pratiques de communication. De même, il ne faut pas hésiter à demander un report du délai si certains documents sont compliqués à obtenir (détenus par une filiale à l'étranger par exemple).

Rester vigilant même si la procédure est clôturée

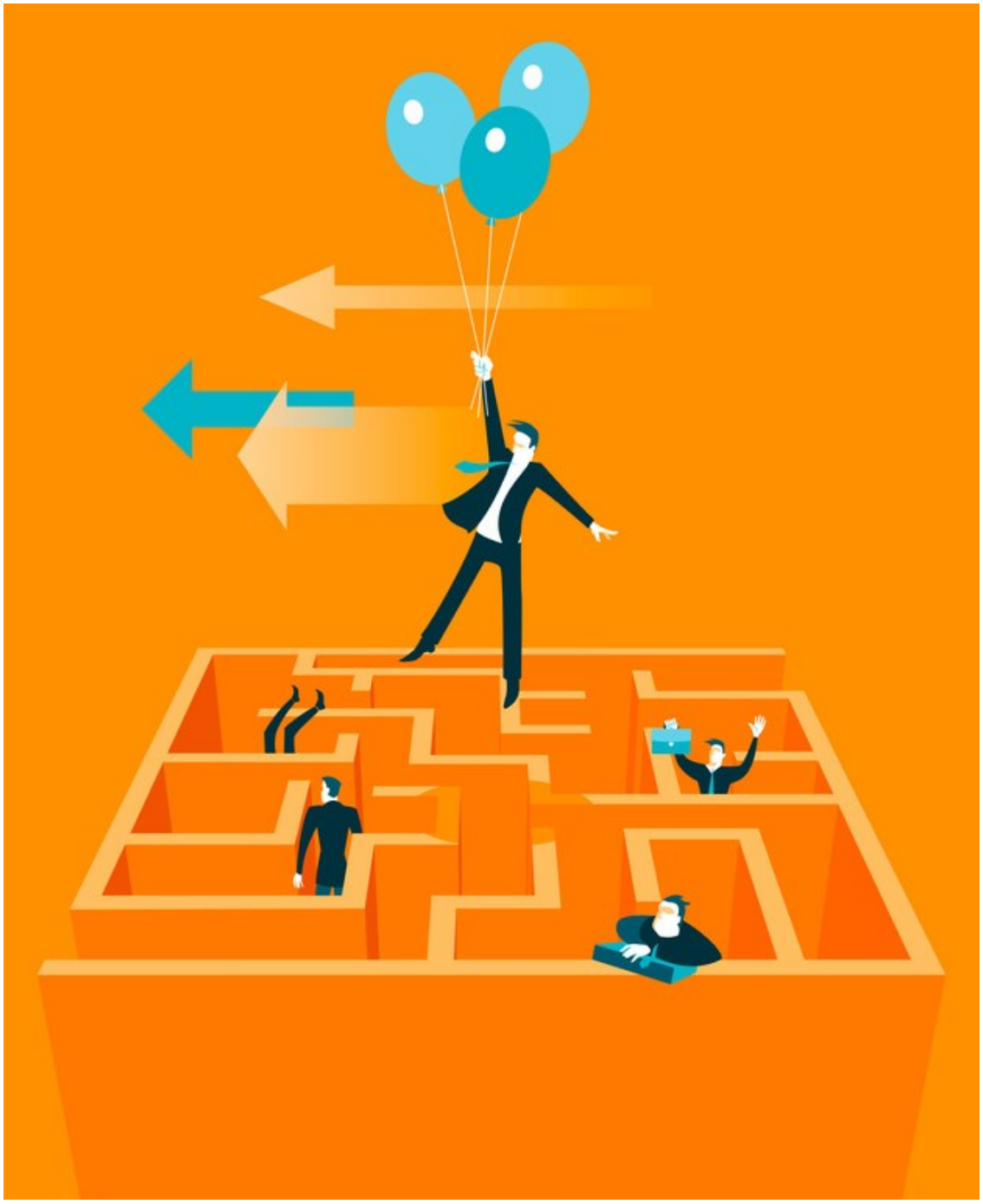
La Cnil statue ensuite sur la conformité ou non de l'entité à la loi. Si c'est le cas, la procédure de contrôle sera clôturée par une lettre de la Présidente de la Cnil dans laquelle elle peut formuler des recommandations si nécessaire.

Les organismes qui ont été contrôlés peuvent s'attendre à être contactés par la Cnil pour faire savoir quelles actions ont été prises pour mettre en œuvre les recommandations énoncées dans la lettre de clôture adressée par la Présidente de la Cnil. 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.

En revanche, lorsque les manquements constatés appellent des sanc-

tions, il appartient à la formation contentieuse de se prononcer.

Cependant, avant d'engager une procédure de sanction, la Présidente de la Cnil peut décider d'adresser une mise en demeure. Il s'agira alors de tout mettre en œuvre pour obtenir la clôture de cette mise en demeure.



Fiche 7 - Comment gérer la phase contentieuse ?

Si une procédure de sanction est engagée, un rapporteur est désigné par la Présidente de la Commission hors de la formation restreinte.

Le rapporteur n'appartient pas à la formation restreinte et ne doit pas avoir de conflit d'intérêt à l'égard de l'organisme contrôlé. Il peut procéder à toute diligence utile avec le concours des services de la Cnil si besoin. Il peut également auditionner le responsable de traitement et/ou le sous-traitant et, de manière générale, toute personne dont le témoignage est jugé utile.

Son rapport est notifié à l'organisme contrôlé par tout moyen permettant à la Cnil d'apporter la preuve de la date de cette notification, généralement signifié par huissier. Il est d'ailleurs conseillé de vérifier les modalités de la signification du rapport.

Le responsable du traitement ou le sous-traitant dispose d'un délai d'un mois pour transmettre ses observations écrites au rapporteur et à la formation restreinte (deux mois s'il est établi hors du territoire métropolitain).

Il est fortement conseillé de prendre connaissance et copie des pièces du dossier auprès des services de la Commission, comme précisé au début de tout rapport.

Demander un huis-clos

L'article 65 du Règlement intérieur de la Cnil prévoit les modalités d'assistance aux séances de la formation restreinte. Il est possible de demander au président de séance de « restreindre la publicité de l'audience dans l'intérêt de l'ordre public, ou lorsque la protection de secrets protégés par la loi l'exige ». A noter que la version du Règlement intérieur de la Cnil date du 22 janvier 2015 et qu'elle n'a pas été mise à jour pour ajouter la mention de « sous-traitant ». Cependant, un sous-traitant contrôlé devrait pouvoir demander un huis clos.

Il convient de toujours demander à ce que l'audience se tienne à huis clos, même si l'on doute de pouvoir obtenir la publicité restreinte de l'audience. D'expérience, il y a toujours au moins un argument à exploiter; qu'il s'agisse du secret ou de l'ordre public.

Par ailleurs, la décision de la formation restreinte doit comporter les raisons pour lesquelles la séance s'est tenue à huis clos. En d'autres termes, la formation restreinte doit expliquer pourquoi elle a accepté d'accorder le huis clos au responsable de traitement ou au sous-traitant. Nous pouvons toutefois nous étonner du fait que cette exigence de motivation ne soit pas également exigée lorsque la formation restreinte refuse d'accéder à la demande de l'organisme contrôlé. En effet, comment contester ce refus en l'absence de justification de la part de la formation restreinte ? À ce sujet, à la lecture des délibérations faisant état d'une

demande de huis clos refusée par le président de la formation restreinte, nous pouvons effectivement constater qu'aucune motivation n'est exposée.

Dans l'hypothèse où la demande de huis clos n'est pas acceptée, il ne faut pas hésiter à contester ce refus dans les observations écrites adressées au rapporteur et à la formation restreinte et à insister sur l'absence de motivation, notamment en invoquant le principe du contradictoire. En effet, le Conseil d'État a reconnu à la formation restreinte de la Cnil la qualité de tribunal, au sens de l'article 6§1 de la CESDH relatif au droit au procès équitable, dans l'exercice de son pouvoir de sanction (CE référé, 19 février 2008, n° 311974, Société Profil France). C'est notamment la raison pour laquelle les responsables de traitement et sous-traitants mis en cause peuvent être assistés d'un avocat, accéder à leur dossier et être entendus lors de la formation contentieuse.

Enfin, pour information, même si l'audience est censée être publique, il faut tout de même s'annoncer préalablement et recevoir confirmation de la possibilité d'assister à la séance.

Rédiger des observations écrites

Il s'agit de contester les manquements reprochés. Si les manquements sont avérés, il conviendra alors de trouver des « circonstances atténuantes » car la formation restreinte de la Cnil les prend en compte pour réduire le montant de la sanction financière, le cas échéant. À ce titre, il importe notamment de faire preuve de coopération avec les agents de la Cnil, lors du contrôle. Par ailleurs, il est indispensable de mettre en exergue tous les actes réalisés depuis le premier jour du contrôle par les membres du personnel de l'organisme contrôlé ainsi que l'implication de ces derniers tout au long du contrôle et au-delà.

Bien entendu, une sanction financière peut toujours être prononcée en cas de manquements avérés, aussi est-il conseillé de remettre en cause la pertinence du montant de la sanction et d'insister sur son caractère disproportionné, ainsi que de contester les modalités de calcul appliquées par le rapporteur lorsqu'elles sont expliquées. Si ces modalités de calcul ne font pas l'objet d'une explication dans le rapport, il peut être opportun de le rappeler dans les observations écrites.

En outre, il convient de ne pas négliger les éventuelles erreurs de procédure commises par les agents de la Cnil et ne pas hésiter à demander à la formation restreinte d'écarter certaines pièces de la procédure.

Si le rapporteur s'appuie sur des normes ou référentiels publiés il y a plusieurs années, l'obsolescence de ces textes peut parfaitement être invoquée, d'autant plus après l'entrée en application du RGPD. Inversement, il peut être intéressant d'utiliser des do-

‘La qualité de tribunal étant reconnue à la formation restreinte, il est particulièrement important de l’amener à expliquer clairement les raisons qui la conduisent à se déterminer.’

cuments publiés sur le site de la Cnil pour contester les propos du rapporteur car il y a parfois des contradictions. Il nous paraît en effet nécessaire de relever les éventuelles incohérences et inexactitudes présentes dans les procès-verbaux et/ou le rapport. En effet, comment sanctionner une entité sur la base de constatations imprécises ?

En l'absence de mise en demeure, il convient d'insister, lorsque c'est possible, sur le fait que le manquement pouvait être réparé et que la Présidente de la Cnil n'a pas motivé sa décision d'engager directement une procédure de sanction. Cet argument a déjà pu être soulevé dans d'autres contentieux devant la Cnil mais il nous paraît que cette dernière y a répondu de manière très laconique. Aussi est-il important de rappeler que la qualité de tribunal lui étant reconnu, ses décisions doivent être motivées.

Si le rapporteur envisage la publicité de la sanction, plusieurs arguments peuvent être soulevés selon le cas d'espèce pour convaincre la formation restreinte de ne pas rendre sa décision publique.

En conclusion, la qualité de tribunal étant reconnue à la formation restreinte de la Cnil, il est particulièrement important de l'amener - par les observations écrites - à expliquer clairement les raisons qui la conduisent à se déterminer. À notre sens, cela participe d'une meilleure compréhension - et donc acceptation - de la « jurisprudence » de la Cnil.

Adresser les observations écrites à la formation restreinte

Avant l'expiration du délai d'un mois (8 jours en cas de procédure d'urgence), des observations écrites et les éléments permettant d'attester du chiffre d'affaires et du résultat si l'organisme contrôlé est une société, doivent être transmises au rapporteur et à la formation restreinte en huit exemplaires.

Nous préconisons de les déposer directement dans les locaux de la Cnil (3 Place de Fontenoy, 75007, Paris). Avant d'arriver sur les lieux, il convient de prévenir les agents de la Cnil afin que l'un d'entre eux se présente à l'accueil. Un reçu sera délivré (à réclamer le cas échéant). Par la suite, les agents de la Cnil demanderont une version dématérialisée des observations écrites.

Préparer l'audience

Le responsable du traitement ou le sous-traitant et, le cas échéant, leur avocat sont invités à présenter des observations orales à l'appui de leurs observations écrites. À ce propos, il convient d'être le plus exhaustif possible dans les observations écrites. Pendant l'audience, aucun élément nouveau ne peut être présenté.

En outre, la formation restreinte peut entendre toute personne dont elle estime l'audition utile. À noter que, lorsque la formation restreinte s'estime insuffisamment éclairée, elle peut demander au rapporteur de poursuivre ses diligences.

Bien entendu, il est fortement conseillé de préparer l'audience avec l'intégralité des membres du personnel qui sera présent lors de la séance. À ce titre, il s'agira probablement de plusieurs membres de l'équipe d'inspection (DPO, juriste, RSSI, etc.)

Et après la décision de la formation restreinte ?

Si une sanction est prononcée, un recours contre la décision de la formation restreinte est toujours possible devant le Conseil d'Etat. De manière générale, il est conseillé de rédiger les observations écrites adressées au rapporteur et à la formation restreinte de sorte à pouvoir réutiliser certains arguments devant le Conseil d'Etat si un appel devait être décidé par le responsable de traitement ou le sous-traitant.

Enfin, nous ne pouvons que recommander aux organismes contrôlés de « tirer les leçons » du contrôle. Il pourra notamment servir de base à une sensibilisation efficace des membres du personnel. En effet, que la formation restreinte prononce une sanction ou non, les services de la Cnil peuvent toujours diligenter un nouveau contrôle auprès de l'organisme.

Abonnez-vous à notre Newsletter :

www.avocats-mathias.com

Mathias Avocats

Nous sommes un cabinet spécialisé dans le droit du digital et accompagnons nos clients au gré des changements que le monde numérique implique.

Nos clients font partie de grands groupes bancaires ou sont des entreprises leaders dans l'innovation digitale. Nous représentons également des startups, au développement desquelles nous avons participé au fil des ans.

Mathias Avocats

Avez-vous des questions ?

Une équipe dédiée vous accompagne dans la réalisation de vos ambitions.

01 43 80 02 01
contact@avocats-mathias.com
19, rue Vernier – 75017 – Paris

Retrouvez les conseils pratiques de Mathias Avocats sur Twitter :
@GaranceMathias