CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Charte des contrôles

Charte des contrôles de la CNIL

CETTE CHARTE NE SE SUBSTITUE PAS AUX DISPOSITIONS LÉGALES APPLICABLES AUX CONTRÔLES EFFECTUÉS PAR LA CNIL.

Version du 23 novembre 2026

Table des matières

Résumé du document 3
Introduction – Les missions de la CNIL 4
Informer, protéger les droits 4
Accompagner la conformité et conseiller 4
Anticiper et innover 4
Contrôler et sanctionner 4
Objectif du présent document 5
Quelques définitions utiles 5
Qu'est-ce qu'une donnée personnelle ? 5
Qu'est-ce qu'un traitement de données personnelles ? 5
Qu'est-ce qu'un responsable de traitement ? 6
Qu'est-ce qu'un sous-traitant ? 6
1. Le contrôle de la mise en œuvre des traitements par la CNIL 6
Quel est l'objectif d'un contrôle de la CNIL ? 6
Qui peut être contrôlé par la CNIL ? 7
Comment la CNIL décide-t-elle de faire un contrôle ? 7
Quelles sont les différentes formes de contrôles ? 8
2. Les pouvoirs et obligations des agents de contrôle 8
Comment les agents de contrôle de la CNIL sont-ils désignés ? 8
L'habilitation délivrée par la CNIL aux agents de ses services 9
Les habilitations délivrées par le Premier ministre aux agents de la CNIL 9
Quels sont les pouvoirs des agents de contrôle de la CNIL ? 9
Le pouvoir d'accès aux locaux 9
Le pouvoir de se faire communiquer tous renseignements ou documents utiles 10
Quelles sont les obligations des agents de contrôle de la CNIL ? 10
3. Les droits et obligations des organismes contrôlés 11
Identité des contrôleurs et information sur l'objet du contrôle 11
Peut-on refuser le contrôle de la CNIL ? 11
Peut-on opposer le secret professionnel ? 12
Peut-on se faire assister d'un conseil ? 12
4. Le déroulement des contrôles de la CNIL 13
Comment se déroule un contrôle sur place ? 13
Avant le début de la mission de contrôle 13
Le déroulement de la mission de contrôle 14
Les contrôles sur ordonnance du juge des libertés et de la détention 15
Comment se déroule un contrôle en ligne ? 15
Comment se déroule un contrôle sur audition ? 16

Comment se déroule un contrôle sur pièces ? 17
Le questionnaire de la CNIL 17
Modalités de réponse de l'organisme 18
5. Les suites d'un contrôle 18
Que se passe-t-il après le contrôle ? 18
La notification du procès-verbal de contrôle 18
L'instruction du dossier par la CNIL 18
Que peut faire l'organisme concerné après le contrôle ? 19
Quelles sont les suites possibles d'une procédure de contrôle ? 19
La clôture de la procédure, avec ou sans observations 19
L'avertissement et le rappel aux obligations légales par la présidente de la CNIL 19
La mise en demeure 20
Les décisions prononcées par la formation restreinte 20
6. Les principes de bonne conduite 22
Principes applicables aux contrôleurs de la CNIL 22
Respecter un principe de proportionnalité et de minimisation des données demandées 22
Expliquer le contexte et le déroulé de la mission de contrôle 22
Se comporter de manière professionnelle, neutre et courtoise 23
Agir avec diligence 23
Comportement attendu des personnes sollicitées durant les missions de contrôle 23
Répondre aux questions posées par les contrôleurs avec loyauté et coopérer avec les contrôleurs 23
Communiquer les pièces et explications demandées dans des délais raisonnables 24
Conserver une attitude neutre, professionnelle et courtoise pendant la durée du contrôle 24
7. Protection des données personnelles 24

Résumé du document

La Commission nationale de l'informatique et des libertés (CNIL) dispose de pouvoirs de contrôle auprès de tout organisme public ou privé mettant en œuvre des traitements de données personnelles[1]. Afin d'assurer le bon déroulement de ces missions, la CNIL a décidé de diffuser une charte des contrôles.

Les missions de contrôle sont un moyen d'action indispensable pour vérifier l'application concrète de la législation sur la protection des données personnelles[2] et d'en apprécier les enjeux émergents.

Les missions de contrôle sont déclenchées sur décision de la présidente de la CNIL à la suite d'une réclamation ou d'un signalement, d'une alerte parue dans la presse, ou de sa propre initiative (notamment sur la base de thématiques prioritaires annuelles[3] arrêtées par la CNIL).

Ces contrôles peuvent être réalisés sur place, sur pièces, sur convocation ou en ligne[4].

La CNIL peut demander communication de tous documents ou renseignements utiles et nécessaires à l'accomplissement de sa mission, à l'exception des informations protégées par l'un des secrets cités à l'article 19(III) de la loi Informatique et Libertés. Les agents en charge des contrôles peuvent également accéder aux programmes informatiques et aux données ainsi qu'en demander la transcription.

Les agents de la CNIL font l'objet d'une habilitation et sont soumis au secret professionnel.

Pour l'exercice de leurs missions, les agents peuvent accéder à tous locaux de 6 heures à 21 heures, sans informer au préalable l'organisme contrôlé. L'accès à des locaux affectés au domicile privé ne peut se faire que sur autorisation du juge des libertés et de la détention[5].

Avant de débuter la mission, la délégation notifie à l'organisme la décision de la présidente de la CNIL d'effectuer un contrôle et l'ordre de mission identifiant les agents chargés des vérifications[6]. Lors des contrôles sur place, le responsable des lieux bénéficie d'un droit d'opposition à la visite, sauf si la visite a été autorisée par le juge des libertés et de la détention.

Le déroulement des opérations de contrôle est retranscrit dans un procès-verbal dressé à l'issue de la mission. Ce procès-verbal est signé par les agents de la CNIL et, dans le cas de contrôles sur place et sur convocation, par le représentant de l'organisme contrôlé qui peut formuler toutes observations qu'il juge utiles. Ces observations peuvent également être adressées après le contrôle. Ce procès-verbal, dont une copie est remise au responsable des lieux à l'issue d'un contrôle sur place ou sur audition, est ensuite notifié par lettre recommandée avec demande d'avis de réception au responsable du traitement.

L'organisme contrôlé doit coopérer avec la CNIL et prendre toutes mesures utiles afin de faciliter le déroulement des opérations. Le délit d'entrave à l'action de la CNIL est passible d'une peine d'emprisonnement d'un an et d'une amende de 15 000 €[7].

Pour de plus amples informations sur l'action de la CNIL, nous vous invitons à consulter le site web www.cnil.fr. Il vous sera notamment possible de poser des questions en ligne sur l'application du RGPD et de la loi Informatique et Libertés.

[1] Articles 8-2° g) de la loi du 6 janvier 1978 modifiée, dite loi Informatique et Libertés.
[2] Principalement la loi Informatique et Libertés et le règlement général sur la protection des données ou RGPD, entré en application le 25 mai 2018.
[3] Le programme annuel des contrôles est un ensemble de thématiques qui ont été retenues par la CNIL en raison du grand nombre de personnes concernées par les traitements mis en œuvre et de leur impact sur la vie quotidienne. Ce programme annuel est publié sur le site de la CNIL.
[4] Article 19 de la loi Informatique et Libertés.
[5] Article 19(III) de la loi Informatique et Libertés.
[6] Dans les cas des contrôles en ligne, ces documents sont adressés après les contrôles.
[7] Article 226-22-2 du Code pénal.

Introduction – Les missions de la CNIL

La Commission nationale de l'informatique et des libertés (CNIL) est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité, aide les particuliers à maîtriser leurs données personnelles et à exercer leurs droits[8] et contrôle et le cas échéant sanctionne le respect des règles relatives à la protection des données.

Informer, protéger les droits

La CNIL répond aux demandes des particuliers et des professionnels. Toute personne peut lui adresser une plainte en cas de difficulté dans l'exercice de ses droits.

La CNIL est investie d'une mission générale d'information des personnes de leurs droits et répond aux demandes des particuliers et des professionnels. Elle mène des actions de communication grand public que ce soit à travers la presse, son site web, sa présence sur les réseaux sociaux ou en mettant à disposition des outils pédagogiques.

Accompagner la conformité et conseiller

La mise en conformité constitue l'objectif prioritaire de l'autorité indépendante qu'est la CNIL.

L'activité d'accompagnement de la CNIL est variée : avis sur des projets de texte gouvernementaux concernant la protection des données personnelles ou créant de nouveaux fichiers, conseils, participation à des auditions parlementaires. Dans le cadre de cette activité, la CNIL recherche des solutions permettant aux organismes publics et privés de poursuivre leurs objectifs légitimes dans le strict respect des droits et libertés des citoyens.

Anticiper et innover

Dans le cadre de son activité d'innovation et de prospective, la CNIL s'intéresse aux nouvelles tendances et sujets émergents.

Elle participe ainsi à la mise en place d'un débat de société sur les enjeux éthiques des données. Elle constitue un point de contact et de dialogue avec les écosystèmes d'innovation du numérique (chercheurs, *start-ups*, *labs*).

Contrôler et sanctionner

Le contrôle constitue un moyen privilégié d'intervention auprès des responsables de traitement de données personnelles et de leurs sous-traitants. Il permet à la CNIL de vérifier la mise en œuvre concrète de la réglementation relative à la protection des données. Il peut aboutir à l'adoption de différentes mesures, y compris répressives.

Cette mission est plus particulièrement l'objet de ce document.

[8] Pour en savoir plus, consulter « Les missions de la CNIL » sur cnil.fr.

Objectif du présent document

Cette charte ne se substitue pas aux dispositions légales applicables aux contrôles effectués par la CNIL. Elle n'a pas vocation à décrire en détail l'ensemble du déroulé d'un contrôle. Elle en explique uniquement le processus. Elle n'a pour objectif que d'informer sur ses pratiques et renvoie, pour plus de détails, aux textes applicables en vigueur.

Cette charte sert à assurer le bon déroulement des missions de contrôle en les faisant mieux connaître et en précisant un certain nombre de principes de bonne conduite que les contrôleurs de la CNIL s'engagent à appliquer, mais également les comportements qui sont attendus des personnes sollicitées au cours des investigations.

Enfin, cette charte est publiée sur le site web www.cnil.fr.

Quelques définitions utiles

La loi Informatique et Libertés et le RGPD s'appliquent à tout traitement de données personnelles mis en œuvre par un responsable de traitement ou un sous-traitant[9].

Une brève définition[10] de chacun de ces termes est proposée ci-après afin de faciliter la compréhension des droits et obligations des personnes et des organismes dans le cadre d'un contrôle effectué par la CNIL.

Qu'est-ce qu'une donnée personnelle ?

Il s'agit de toute information concernant une personne physique qui peut être identifiée de manière directe (exemple : un nom et un prénom) ou indirecte (exemple : un numéro de sécurité sociale, une adresse de domicile, une image renvoyée par un dispositif de vidéosurveillance, etc.)[11].

Qu'est-ce qu'un traitement de données personnelles ?

Un traitement de données personnelles correspond à toute opération ou tout ensemble d'opérations portant sur de telles données, que le procédé utilisé soit automatisé ou non, et indépendamment du nombre de données traitées.

Le traitement est ainsi constitué, par exemple, par la collecte, l'enregistrement, l'organisation, la conservation, la modification, l'extraction, la consultation, l'utilisation, la communication, le rapprochement ou bien encore l'effacement de données[12].

[9] Sous réserve de respecter les critères des champs d'application matériels et territoriaux de ces textes.
[10] Des définitions plus détaillées figurent à l'article 4 du RGPD ainsi que dans la partie « Glossaire » sur cnil.fr.
[11] Article 4(1) du RGPD.
[12] Article 4(2) du RGPD.

Qu'est-ce qu'un responsable de traitement ?

Le responsable d'un traitement de données personnelles est la personne, l'autorité publique, le service ou encore l'organisme qui, seul ou avec d'autres, détermine les finalités et les moyens du traitement[13].

Par exemple, une société ou un organisme public est responsable du traitement de gestion de ses ressources humaines, dès lors qu'il en définit la finalité (gestion du personnel, de la carrière, de la formation, etc.) et les moyens (mise en œuvre d'outils dédiés à ces finalités, par exemple).

Qu'est-ce qu'un sous-traitant ?

C'est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles pour le compte du responsable du traitement[14].

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

Quel est l'objectif d'un contrôle de la CNIL ?

L'objectif des missions de contrôle est de vérifier que les données sont traitées par l'organisme en conformité avec la règlementation des données personnelles, en particulier le RGPD et la loi Informatique et Libertés, notamment :

- de s'assurer que le traitement mis en œuvre ne porte pas atteinte aux droits et libertés des personnes dont les données sont traitées ;
- de s'assurer que les organismes répondent au principe de responsabilisation (« *accountability* »), par exemple en ayant établi un registre recensant les traitements mis en œuvre ou en ayant effectué, lorsque c'est nécessaire, une analyse d'impact relative à la protection des données.

Lors d'un contrôle, la CNIL s'intéresse **notamment** :

- à la finalité du traitement et à sa base légale[15] ;
- à la nature des données collectées ;
- aux modalités d'information des personnes concernées, en particulier s'agissant de leurs droits ;
- aux durées de conservation et aux mises à jour des données personnelles traitées ;
- aux destinataires de ces données;
- aux moyens mis en œuvre afin de préserver la sécurité des données ;
- aux transferts des données personnelles, le cas échéant.

[13] Article 4(7) du RGPD.
[14] Article 4(8) du RGPD.
[15] Voir « Les bases légales » sur cnil.fr.

Qui peut être contrôlé par la CNIL ?

La CNIL peut contrôler tout organisme traitant des données personnelles (responsable de traitement ou sous-traitant) dans le cadre des activités de l'un de ses établissements sur le territoire français, que le traitement ait lieu ou non en France. La CNIL peut également procéder à des contrôles dans le cadre du RGPD lorsque le traitement mis en œuvre concerne des personnes résidant en France, que l'organisme soit ou non situé en France.

Ces missions peuvent être effectuées dans le cadre d'une coopération avec d'autres autorités de protection des données si l'organisme dispose de plusieurs établissements dans l'Union européenne (UE) et/ou traite les données personnelles de plusieurs personnes concernées dans l'UE.

Le RGPD permet par ailleurs à la CNIL d'effectuer des vérifications auprès des prestataires sous-traitants, en charge de la mise en œuvre d'un traitement pour le compte d'un organisme responsable de traitement (ex. : hébergement, maintenance).

Comment la CNIL décide-t-elle de faire un contrôle ?

La décision de procéder à un contrôle relève de la compétence de la présidente ou de la vice-présidente déléguée de la CNIL. Les missions de contrôle effectuées durant l'année par la CNIL peuvent avoir différentes origines :

- **Les thématiques prioritaires annuelles de contrôle :** chaque année, la CNIL décide de porter son attention sur de grandes thématiques identifiées notamment en raison de leurs effets sur la vie privée de nombreuses personnes. Ces thématiques sont publiées sur le site web de la CNIL. À l'issue du programme annuel, la CNIL communique également sur les pratiques qui ont pu être constatées et sur les suites apportées à ces procédures.
- **Les réclamations et les plaintes :** la CNIL reçoit des réclamations et des plaintes concernant des défauts de conformité aux règles relatives à la protection des données personnelles. Des contrôles sont ainsi réalisés pour vérifier ces pratiques et s'assurer du respect des droits des personnes. Cela représente plus de 40 % des contrôles.
- **Les initiatives :** la CNIL peut s'autosaisir pour mener des investigations sur des sujets variés, notamment au regard de l'actualité, susceptibles de présenter des risques pour les droits et libertés des personnes. Ces contrôles peuvent notamment concerner des traitements potentiellement intrusifs, des secteurs d'activités à enjeux, ou faire suite à une violation de données.
- **Les dispositifs de vidéoprotection :** la CNIL est compétente pour contrôler les caméras filmant des lieux ouverts au public (p. ex. un centre commercial, un musée, etc.) et réserve chaque année une partie de son activité de contrôle à la vérification de ces dispositifs.
- **Les procédures de contrôle closes, les mises en demeure et les sanctions :** des investigations peuvent être menées à la suite d'une procédure de contrôle close, d'une mise en demeure ou d'une sanction, notamment pour vérifier les mesures de mise en conformité adoptées par les organismes.

Quelles sont les différentes formes de contrôles ?

Sur décision de sa présidente, la CNIL peut effectuer des contrôles pouvant prendre 4 formes différentes :

- **Le contrôle sur place :** une délégation de la CNIL se rend directement au sein des locaux d'un responsable de traitement ou d'un sous-traitant afin de mener des investigations portant sur des traitements de données personnelles.
- **L'audition sur convocation :** un courrier est adressé au responsable de traitement ou au sous-traitant afin que des représentants de l'organisme se présentent, à une date donnée, dans les locaux de la CNIL. Ces représentants devront répondre à des questions portant sur le(s) traitement(s) faisant l'objet des vérifications et, le cas échéant, rendre possible un accès aux ressources informatiques de l'organisme.
- **Le contrôle en ligne :** la CNIL effectue des vérifications depuis ses locaux, en consultant notamment des données librement accessibles ou rendues accessibles directement en ligne, y compris par imprudence, négligence ou du fait d'un tiers. Ces vérifications sont effectuées à partir d'un service de communication au public en ligne (par exemple sur un site internet, une application mobile ou un produit connecté) et peuvent également être réalisées sous une identité d'emprunt.
- **Le contrôle sur pièces :** la CNIL adresse un courrier accompagné d'un questionnaire destiné à évaluer la conformité des traitements mis en œuvre par un responsable de traitement ou un sous-traitant. L'organisme visé par le contrôle doit communiquer à la CNIL ses réponses dans un délai déterminé en y joignant tout document utile permettant de les justifier.

Ces modalités de contrôle peuvent être utilisées de manière complémentaire. Ainsi, la CNIL pourra par exemple initier ses vérifications en ligne et les poursuivre sur place. Un contrôle sur pièces pourra également être opéré préalablement à un contrôle sur place.

Tout contrôle, à l'exception du contrôle sur pièces, nécessite la rédaction d'un procès-verbal au sein duquel les agents de la CNIL consignent factuellement l'ensemble des informations qui ont été portées à leur connaissance pendant le contrôle ainsi que les constatations qu'ils ont effectuées.

2. Les pouvoirs et obligations des agents de contrôle

Comment les agents de contrôle de la CNIL sont-ils désignés ?

Tous les agents de la CNIL amenés à réaliser des missions de contrôle sont habilités.

L'habilitation est délivrée par la CNIL et, pour certains traitements, par le Premier ministre.

La liste des agents habilités à procéder à des missions de contrôles est disponible sur le site de la CNIL[16] et au *Journal officiel* de la République française.

[16] Voir « Comment se passe un contrôle de la CNIL ? » sur cnil.fr.

L'habilitation délivrée par la CNIL aux agents de ses services

- L'article 19 de la loi Informatique et Libertés prévoit que les agents des services de la CNIL qui sont appelés à participer à la mise en œuvre des missions de contrôle sont habilités par la CNIL. Les membres du Collège de la CNIL peuvent également être désignés pour procéder à ces missions de contrôle.
- L'habilitation est accordée pour une durée de cinq ans renouvelables, à condition que l'agent concerné n'ait pas fait l'objet d'une condamnation à une peine correctionnelle ou criminelle inscrite au bulletin n° 2 du casier judiciaire[17].
- La désignation d'un agent habilité des services de la CNIL pour procéder à une vérification auprès d'un organisme ne peut avoir lieu que si l'agent ne détient pas, ou n'a pas détenu au cours des trois années précédant cette vérification, un intérêt direct ou indirect avec cet organisme[18].

Les habilitations délivrées par le Premier ministre aux agents de la CNIL

- Les agents qui procèdent à des vérifications portant sur des traitements de données personnelles qui concernent la sûreté de l'État, la défense, la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales, l'exécution des condamnations pénales ou des mesures de sûreté[19], doivent bénéficier d'une habilitation spécifique délivrée par le Premier ministre[20].
- Par ailleurs, les agents qui sont appelés à prendre connaissance d'informations classifiées au titre de la protection du secret de défense nationale, dans le cadre des missions de contrôle, doivent y être habilités par le Premier ministre[21].

Quels sont les pouvoirs des agents de contrôle de la CNIL ?

Le pouvoir d'accès aux locaux

Pour l'exercice de leur mission de contrôle, les agents de contrôle ont accès à tous lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données personnelles[22].

Lorsqu'un traitement de données personnelles est mis en œuvre dans des lieux affectés en tout ou partie à un domicile privé, la visite ne peut se dérouler qu'après l'autorisation du juge des libertés et de la détention territorialement compétent.

---

[17] Articles 16 et 17 du décret n°2019-536 du 29 mai 2019 (décret d'application de la loi Informatique et Libertés).
[18] Article 18 du décret d'application de la loi Informatique et Libertés.
[19] Traitements relevant de l'article 31 de la loi Informatique et Libertés
[20] Article 23 du décret d'application de la loi Informatique et Libertés.
[21] *Ibid.*
[22] Article 19(I) de la loi Informatique et Libertés et article 58(1.f) du RGPD.

Cet accès peut s'opérer entre 6 heures et 21 heures. Dès lors qu'il a débuté dans cet intervalle de temps, le contrôle peut se prolonger si nécessaire au-delà de 21 heures.

Le pouvoir de se faire communiquer tous renseignements ou documents utiles

Les agents de contrôle de la CNIL peuvent à l'occasion d'un contrôle et après celui-ci[23] :

- demander communication de tous documents nécessaires à l'accomplissement de leur mission à l'exception des informations protégées par l'un des secrets professionnels listés dans la loi Informatique et Libertés[24] (cf. point 3.3 de la présente charte), quel qu'en soit le support, et en prendre copie ;
- recueillir tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission.

Ils peuvent également accéder aux programmes informatiques, aux données, et en demander la transcription, par tout traitement approprié, dans des documents directement utilisables pour les besoins du contrôle[25].

Lorsqu'ils y accèdent depuis un poste de travail depuis le lieu du contrôle, les contrôleurs peuvent copier des données hébergées localement ou chez un prestataire.

Quelles sont les obligations des agents de contrôle de la CNIL ?

Les agents de la CNIL sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, sous peine de poursuites pénales[26].

Les agents de la CNIL ne peuvent participer au contrôle d'un organisme au sein duquel :

- ils détiennent ou ont détenu, au cours des trois années précédant le contrôle, un intérêt direct ou indirect ;
- ils exercent ou ont exercé, au cours de ces trois années, des fonctions ou une activité professionnelle ;
- ils détiennent ou ont détenu, dans la même période, un mandat.

Ils ont en outre l'obligation de signaler à leur hiérarchie cette éventuelle incompatibilité[27].

Les agents sont en tout état de cause tenus de respecter des principes de bonne conduite lorsqu'ils procèdent à des vérifications auprès d'un organisme. Ces principes sont développés au point 6 de la présente charte.

Les données et documents recueillis lors d'un contrôle et leur conservation ultérieure font l'objet de procédures garantissant leur authenticité, leur intégrité et leur confidentialité, quel qu'en soit le

---

[23] Article 19(III) de la loi Informatique et Libertés et article 58(1) du RGPD.
[24] Voir « Peut-on opposer le secret professionnel ? » page 10
[25] Article 19(III) de la loi Informatique et Libertés.
[26] Article 54(2) du RGPD.
[27] Article 54 du règlement intérieur de la CNIL.

support.[28] Ces données et documents sont stockés de manière sécurisée. Seuls les agents de la CNIL ayant besoin d'en connaître[29] dans l'exercice de leurs missions peuvent accéder aux dossiers de contrôle.

Les dossiers de contrôles, comprenant notamment toutes les pièces ayant été collectées auprès de l'organisme à l'occasion du contrôle, sont conservés pendant toute la durée de la procédure et sont détruits cinq ans après la clôture de la procédure de contrôle, sous réserve de l'exercice de voies de recours et des délais y afférents.

3. Les droits et obligations des organismes contrôlés

Identité des contrôleurs et information sur l'objet du contrôle

L'organisme contrôlé dispose du droit de s'assurer de l'identité des contrôleurs en charge des investigations le concernant. Il peut s'appuyer sur les documents qui lui sont remis par la délégation au début du contrôle. L'identité des agents en charge du contrôle est précisée dans l'ordre de mission signé par le secrétaire général de la CNIL.

Les contrôleurs doivent être en mesure de prouver leur identité, à l'aide de leur carte professionnelle ou d'un document d'identité valable. L'organisme peut vérifier que les contrôleurs figurent bien parmi les agents habilités (cf. « Comment les agents de contrôle de la CNIL sont-ils désignés ? »).

L'objet de la mission de contrôle est indiqué sur la décision signée par la présidente de la CNIL et remise à l'organisme contrôlé en début de contrôle.

Peut-on refuser le contrôle de la CNIL ?

Il n'est pas possible de refuser un contrôle de la CNIL.

En effet, les détenteurs ou utilisateurs de traitements de données personnelles ne peuvent s'opposer à l'action de la CNIL et doivent, au contraire, prendre toutes les mesures utiles afin de faciliter cette action[30]. Les responsables de traitement et les sous-traitants sont tenus à une obligation de coopération envers la CNIL[31].

Dans le cadre d'un contrôle sur place, le responsable des lieux peut s'opposer à la visite de ses locaux par la CNIL, sauf si cette visite a été autorisée par un juge des libertés et de la détention.[32] Par exception, les organismes étatiques ne peuvent jamais s'opposer à la tenue d'un contrôle.

Enfin, l'article 226-22-2 du Code pénal punit d'un an d'emprisonnement et de 15 000 € d'amende le fait d'entraver l'action de la CNIL :

---

[28] Article 57 du règlement intérieur de la CNIL.
[29] L'expression « besoin d'en connaître » signifie que l'information n'est traitée que par les agents de la CNIL habilités pour qui l'information est pertinente et nécessaire.
[30] Article 18 de la loi Informatique et Libertés.
[31] Article 31 du RGPD.
[32] Article 19 de la loi Informatique et Libertés.

- soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 10 de la loi Informatique et Libertés lorsque la visite a été autorisée par le juge ;
- soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 10 de la même loi, ou aux agents d'une autorité de contrôle d'un État membre de l'Union européenne en application de l'article 62 du RGPD, les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;
- soit en communiquant des informations qui ne sont pas 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.

Peut-on opposer le secret professionnel ?

Dans le cadre d'une mission de contrôle opérée par la CNIL, le secret ne peut lui être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, dans certaines conditions, par le secret médical.[33]

S'agissant du secret médical, celui-ci ne pourra être opposé en présence d'un médecin, accompagnant la délégation de la CNIL, qui sera à même de se faire communiquer, sous son autorité, les données médicales individuelles nécessaires à l'accomplissement de la mission de contrôle.[34]

Lorsqu'une personne interrogée dans le cadre des vérifications faites par la CNIL oppose un de ces trois secrets, la mention de cette opposition est portée au procès-verbal établi par les agents de la CNIL chargés du contrôle. Les dispositions législatives ou réglementaires auxquelles peut se référer la personne interrogée sont alors mentionnées, ainsi que la nature des données qu'elle estime couvertes par ces dispositions[35].

Peut-on se faire assister d'un conseil ?

À l'occasion des missions de contrôle sur place[36] et des auditions sur convocation, le responsable des lieux ou la personne auditionnée peut se faire assister par tout conseil de son choix.

Lorsque le contrôle s'effectue sur le fondement d'une ordonnance du juge des libertés et de la détention autorisant la visite des agents de contrôle de la CNIL, le responsable des lieux est informé qu'il peut, s'il l'estime utile, se faire assister du conseil de son choix ou à défaut, de deux témoins n'étant pas sous l'autorité de la délégation de la CNIL[37].

---

[33] Articles 18(2) et 19(III.1) de la loi Informatique et Libertés et article 90 du RGPD.
[34] Art. 19(III.2) de la loi Informatique et Libertés.
[35] Article 37 du décret d'application de la loi Informatique et Libertés.
[36] Article 19(II) de la loi Informatique et Libertés.
[37] Article 19(II.2) de la loi Informatique et Libertés.

Si le responsable des lieux souhaite faire appel à son avocat, ce choix ne peut avoir pour effet d'empêcher la tenue du contrôle.

4. Le déroulement des contrôles de la CNIL

Comment se déroule un contrôle sur place ?

Avant le début de la mission de contrôle

Avant chaque contrôle sur place, le procureur de la République territorialement compétent est informé de la mission de contrôle. Le nom de l'organisme contrôlé ainsi que la date, le lieu et l'objet du contrôle lui sont communiqués[38].

Les agents qui effectuent la mission de contrôle sont désignés dans l'ordre de mission du secrétaire général de la CNIL. Une délégation est généralement composée d'au moins deux agents, un juriste et un auditeur des systèmes d'information ayant respectivement un profil juridique et technique. Selon les besoins, la délégation peut être renforcée.

Les missions de vérification s'effectuent généralement de façon inopinée, c'est-à-dire que **les organismes ne sont pas prévenus à l'avance de la tenue d'un contrôle**.

À leur arrivée sur les lieux, les agents de contrôle de la CNIL se présentent et demandent à être mis en relation avec le représentant légal de l'organisme ou, en cas d'indisponibilité, avec tout autre responsable en lien avec le traitement ou, à défaut, avec toute personne exerçant une activité professionnelle au sein de l'organisme.

Après cette prise de contact et l'identification d'un responsable des lieux, qui peut être désigné par le responsable des traitements, la délégation demande à être mise en relation avec une personne en capacité de présenter les traitements visés par le contrôle et/ou, lorsqu'il a été désigné, avec le délégué à la protection des données (DPD/DPO).

Le responsable des lieux (ou son représentant) est, en pratique, l'interlocuteur privilégié, mais pas exclusif, de la délégation. Il doit se rendre disponible pour suivre les agents tout au long de la mission de contrôle. En fin de journée, il procède à la relecture et à la signature du procès-verbal de contrôle sur place. Le responsable des lieux sera ainsi en mesure de s'assurer que le contenu du procès-verbal correspond aux informations délivrées à la délégation et aux constatations faites au cours de la journée. Tout refus ou absence de signature est inscrit dans le procès-verbal[39].

Au début de la mission et avant toute constatation, les agents chargés du contrôle délivrent au responsable des lieux les informations suivantes :

- l'identité et la qualité des agents de la délégation ;
- la copie de la décision de contrôle de la présidente de la CNIL ;

[38] Article 19(I.2) de la loi Informatique et Libertés.
[39] Article 19-III alinéa 6 de la loi Informatique et Libertés et article 31 du décret n°2019-536 du 29 mai 2019 (décret d'application de la loi Informatique et Libertés).

- la copie de l'ordre de mission général désignant les agents de la CNIL qui effectuent le contrôle ;
- l'objet du contrôle ;
- des éléments d'information issus des articles 19 de la loi Informatique et Libertés et L253-3 du Code de la sécurité intérieure ;
- la notification à l'organisme de son droit d'opposition à la visite (à l'exception des organismes de l'État[40]) sauf lorsque la visite a été autorisée par une ordonnance du juge des libertés et de la détention. Dans ce cas, une copie certifiée conforme à l'original de l'ordonnance du juge des libertés et de la détention est transmise à l'organisme.

Le déroulement de la mission de contrôle

Un contrôle sur place se déroule généralement en 4 étapes :

- d'abord des entretiens sont menés afin de recueillir des éléments d'information relatifs à l'organisme contrôlé et aux traitements mis en œuvre (activités, structure juridique de l'organisme, fonctionnement, traitements, architecture des systèmes d'informations, etc.) ;
- ensuite, la délégation procède à des **constatations et recueille des pièces** permettant d'apprécier la conformité à la réglementation relative à la protection des données des traitements de données mis en œuvre ; elle peut, en tant que de besoin, se déplacer au sein des locaux pour effectuer toute constatation utile et interroger toute personne ;
- enfin, à l'issue des constats, un procès-verbal est dressé. Celui-ci rend compte, de manière factuelle, de l'ensemble des informations qui ont été communiquées à la délégation de contrôle et des constatations qu'elle a opérées. Il y est également précisé l'identité et la qualité des personnes avec lesquelles la délégation s'est entretenue. Il peut également faire mention de demandes de communication de pièces complémentaires (contrats, extractions de bases de données, etc.) dans un délai imparti. Le procès-verbal précise que les pièces complémentaires doivent être adressées à la CNIL de manière à en assurer la sécurité et la confidentialité. La Commission dispose de sa propre plateforme de dépôt de fichiers sécurisée qu'elle peut, au besoin, mettre à disposition de l'organisme pour cette transmission. Une annexe au procès-verbal contient l'inventaire des pièces recueillies durant la mission de contrôle.
- Le procès-verbal est soumis à la relecture et à la signature du responsable des lieux et des agents de contrôle de la CNIL. Le responsable des lieux ou le représentant de l'organisme peut formuler des observations écrites dans un espace prévu à cet effet. Une copie du procès-verbal lui est remise en mains propres à la fin de la mission de contrôle[41].

Ces quatre étapes ne sont pas nécessairement successives. Elles peuvent se dérouler simultanément, par exemple si des pièces sont communiquées lors de la phase d'entretien.

---

[40] Ministères ou administrations déconcentrées relevant d'un ministère et ne disposant pas de la personnalité juridique (p. ex. : préfecture, commissariat, tribunal, prison, rectorat, etc.).

[32] Article 31 du décret n°2019-536 du 29 mai 2019 (décret d'application de la loi Informatique et Libertés).

Une mission de contrôle sur place peut se dérouler sur plusieurs jours. Dans ce cas, il est dressé un procès-verbal par jour de contrôle.

Les contrôles sur ordonnance du juge des libertés et de la détention

La présidente de la CNIL peut décider de saisir le juge des libertés et de la détention afin qu'il délivre une ordonnance autorisant la visite des agents de la CNIL.

Cela concerne les cas suivants :

- lorsque le traitement de données personnelles est mis en œuvre dans un lieu affecté au domicile privé d'une personne ;
- lorsque le responsable des lieux a exercé son droit d'opposition à la visite.

En outre, la présidente de la CNIL peut saisir le juge des libertés et de la détention afin qu'il autorise préalablement la visite des agents de contrôle de la CNIL lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite.

Lorsque la visite a été autorisée par le juge des libertés et de la détention, les vérifications s'effectuent sous son autorité, en présence du responsable des lieux qui peut se faire assister par le conseil de son choix ou, à défaut, de deux témoins qui ne sont pas placés sous l'autorité de la CNIL. Le juge n'a pas à être présent lors du contrôle, mais peut se rendre dans les locaux contrôlés s'il l'estime utile. Il peut autoriser la CNIL à se faire assister de la force publique[42]. En pratique, cela signifie que les contrôleurs de la CNIL peuvent être accompagnés d'agents de la police ou de la gendarmerie afin de constater, le cas échéant, une entrave au bon déroulement de la mission de contrôle telle qu'autorisée par le juge.

Un recours peut être exercé contre l'ordonnance du juge devant le premier président de la cour d'appel. Ce recours n'est pas suspensif, c'est-à-dire qu'il n'empêche pas l'exécution du contrôle.

Comment se déroule un contrôle en ligne ?

Les contrôles en ligne sont réalisés depuis les locaux de la CNIL. Pour permettre aux agents de réaliser les opérations de contrôle dans des conditions garantissant l'authenticité et l'intégrité des éléments constatés et des données et documents recueillis, un poste informatique et une connexion internet dédiés aux seules opérations de contrôle en ligne sont mis à leur disposition. Les opérations de contrôle se déroulent depuis un environnement dont la configuration et les données stockées sont réinitialisées avant chaque contrôle.

Les contrôles en ligne peuvent également se faire à partir d'un terminal mobile, notamment pour contrôler des applications mobiles.

Le contrôle en ligne vise prioritairement à obtenir copie d'informations (éléments techniques et juridiques) permettant d'évaluer les conditions dans lesquelles sont mis en œuvre les traitements.

---

[42] Article 19(II.2) de la loi Informatique et Libertés.

Dans le cas d'un contrôle en ligne réalisé à la suite d'un signalement d'une violation de données[43], celui-ci a également pour objet de constater l'existence et l'étendue de la violation de données.

Toute donnée librement accessible depuis le nom de domaine ou le site web visé par la décision de contrôle peut être recueillie (p. ex. copie d'écran, extraits de base de données, code source de la page, etc.).

Les agents peuvent consulter les données librement accessibles ou rendues accessibles. Ils se comportent comme tout internaute, qui, bien que pouvant être expérimenté, ne pourrait être assimilé à un « attaquant ». Comme tout internaute, les agents de la CNIL peuvent compléter des formulaires en ligne, tester des liens de désinscription ou des procédures permettant l'exercice des droits. Les agents de contrôle peuvent faire usage d'une identité d'emprunt pour les opérations de contrôle en ligne.

Enfin, au cours des opérations de contrôle en ligne, un procès-verbal est dressé. Celui-ci rend compte, de manière factuelle, de l'ensemble des constatations des agents de contrôle et liste les pièces placées en annexe. Le procès-verbal peut également faire mention de demandes de communication de pièces complémentaires (contrats, extractions de bases de données, etc.) dans un délai imparti. Le procès-verbal précise que les pièces complémentaires doivent être adressées à la CNIL de manière à en assurer la sécurité et la confidentialité. Il est signé par les contrôleurs de la CNIL. La Commission dispose de sa propre plateforme de dépôt de fichiers sécurisée qu'elle peut, au besoin, mettre à disposition de l'organisme pour cette transmission.

Comment se déroule un contrôle sur audition ?

Les contrôles sur convocation se déroulent, en principe, dans les locaux de la CNIL à Paris (3, place de Fontenoy, 75007 Paris).

Les agents qui effectuent la mission de contrôle auprès de l'organisme sont désignés dans l'ordre de mission du secrétaire général de la CNIL.

Un courrier de convocation est adressé à l'organisme au moins huit jours avant la date de l'audition. Ce courrier indique l'objet du contrôle, la date, l'heure et le lieu de l'audition ainsi que le droit de l'organisme de se faire assister d'un conseil de son choix. Ce courrier peut également préciser le matériel et la documentation nécessaires au déroulement de l'audition. La décision de contrôle et l'ordre de mission sont joints à ce courrier.

Au début de la mission et avant toute constatation, les agents chargés du contrôle délivrent au responsable des lieux les informations suivantes :

- l'identité et la qualité des agents de la délégation ;
- la copie de la décision de contrôle de la présidente de la CNIL ;
- la copie de l'ordre de mission général désignant les agents de la CNIL qui effectuent le contrôle ;
- l'objet du contrôle ;

[43] Voir « Les violations de données à caractère personnel » sur cnil.fr.

- des éléments d'information issus de l'article 19 de la loi Informatique et Libertés, l'article 56 du règlement intérieur de la CNIL et l'article L253-3 du Code de la sécurité intérieure.

Comme les contrôles sur place, les contrôles sur audition se déroulent généralement en 3 étapes :

- d'abord, des entretiens sont menés afin de recueillir des éléments d'information relatifs à l'organisme contrôlé et aux traitements mis en œuvre (activités, structure juridique de l'organisme, fonctionnement, traitements, architecture des systèmes d'information, etc.) ;
- ensuite, la délégation procède à des constatations et recueille des pièces permettant d'évaluer la conformité à la loi et au RGPD des traitements de données ;
- enfin, à l'issue des constats, un procès-verbal est dressé. Celui-ci rend compte, de manière factuelle, de l'ensemble des informations qui ont été communiquées à la délégation de contrôle et des constatations qu'elle a opérées. L'identité et la qualité des personnes avec lesquelles la délégation s'est entretenue sont précisées. Il peut également faire mention de demandes de communication de pièces complémentaires (contrats, extractions de bases de données, etc.) dans un délai imparti. Le procès-verbal précise que les pièces complémentaires doivent être adressées à la CNIL de manière à en assurer la sécurité et la confidentialité. La Commission dispose de sa propre plateforme de dépôt de fichiers sécurisée qu'elle peut, au besoin, mettre à disposition de l'organisme pour cette transmission. Le procès-verbal est soumis à la relecture et à la signature du représentant de l'organisme. Il est également signé par les agents de contrôle de la CNIL. Le responsable des lieux ou le représentant de l'organisme peut formuler des observations écrites dans un espace prévu à cet effet. Une copie du procès-verbal lui est remise en mains propres à la fin de la mission de contrôle[44].

Ces trois étapes ne sont pas nécessairement successives. Elles peuvent se dérouler simultanément, par exemple si des pièces sont communiquées lors de la phase d'entretien.

Comment se déroule un contrôle sur pièces ?

Le questionnaire de la CNIL

Les contrôles sur pièces consistent en l'envoi d'un questionnaire à l'organisme visé, par courrier recommandé avec avis de réception.

Ce questionnaire est destiné à recueillir des éléments d'information ainsi que des pièces et documents justificatifs. Un même questionnaire peut être adressé à une série d'organismes similaires afin d'avoir une vue générale des traitements mis en œuvre dans un secteur particulier.

Le questionnaire est adressé à l'organisme avec un courrier qui indique l'objet du contrôle, le délai imparti pour répondre au questionnaire et transmettre les documents demandés, au format demandé, ainsi que la possibilité pour l'organisme d'envoyer toute autre documentation utile. La copie de la décision de contrôle et l'ordre de mission sont joints au courrier.

[34] Article 31 du décret 2019-536 du 29 mai 2019 (décret d'application de la loi Informatique et Libertés).

Modalités de réponse de l'organisme

L'organisme contrôlé peut adresser sa réponse :

- par courrier postal, soit par courrier recommandé avec avis de réception, soit par porteur ;
- de manière dématérialisée soit par l'utilisation de la plateforme d'échange sécurisée de la Commission soit par courrier électronique.

En cas d'envoi de la réponse par courrier électronique, il est indispensable de sécuriser cet envoi en chiffrant les documents adressés (par exemple en rassemblant l'ensemble des documents au sein d'une archive chiffrée[45]).

Le mot de passe permettant le déchiffrement devra être communiqué par un autre moyen que celui par lequel l'archive a été envoyée.

Les réponses au questionnaire et les pièces justificatives feront l'objet d'une instruction par la CNIL. À l'issue de celle-ci, la présidente de la CNIL pourra décider des suites de la procédure ou faire réaliser un nouveau contrôle de l'organisme selon d'autres modalités.

5. Les suites d'un contrôle

Que se passe-t-il après le contrôle ?

La notification du procès-verbal de contrôle

Pour les contrôles sur place, le procès-verbal est notifié au responsable de traitement dans un délai de 15 jours à compter du contrôle par courrier recommandé avec accusé de réception.

Pour les contrôles en ligne, le courrier de notification envoyé à l'organisme comprend une clef de chiffrement ainsi que des coordonnées auxquelles l'organisme peut prendre contact avec l'agent en charge du dossier, qui lui transmettra un lien vers une plateforme d'échange sécurisée où il pourra obtenir une copie numérique des pièces numériques issues du contrôle (captures d'écran, archives, etc.).

L'instruction du dossier par la CNIL

À l'issue du contrôle, la phase d'instruction du dossier est initiée par les services de la CNIL. Il est procédé à une analyse des éléments et des pièces recueillis lors du contrôle afin de déterminer le niveau de conformité de l'organisme aux dispositions du RGPD et de la loi Informatique et Libertés. Des demandes complémentaires peuvent être adressées à l'organisme contrôlé pour obtenir des précisions ou des documents supplémentaires. De nouveaux contrôles peuvent alors être décidés par la présidente de la CNIL.

L'instruction d'une procédure de contrôle est réalisée dans les meilleurs délais. Cette instruction se déroule toutefois sur une période de plusieurs mois. En cas de circonstances exceptionnelles

[45] Voir « Comment chiffrer ses documents et ses répertoires ? » sur cnil.fr

allongeant le temps d'instruction du dossier, un courrier est adressé à l'organisme contrôlé pour lui indiquer que l'instruction du dossier est toujours en cours.

Lorsque le traitement est transfrontalier et concerne d'autres pays de l'espace économique européen, la CNIL est tenue de communiquer, à différentes étapes, les résultats de ses investigations avec les autorités de protection des données personnelles des autres pays concernés.

Que peut faire l'organisme concerné après le contrôle ?

Les organismes contrôlés peuvent adresser à la CNIL, postérieurement au contrôle et pendant la durée de l'instruction du dossier, des observations complémentaires et la tenir informée d'éventuelles modifications de leur traitement. Par exemple, un organisme peut adresser à la CNIL la nouvelle version de la politique de confidentialité mise en ligne sur son site web.

Les coordonnées des agents de contrôle de la CNIL sont systématiquement communiquées aux organismes contrôlés. Ils peuvent être contactés pour toute question en lien avec la procédure de contrôle.

Quelles sont les suites possibles d'une procédure de contrôle ?

La présidente de la CNIL décide de l'orientation et des suites des procédures de contrôle. Ces suites peuvent être de deux ordres : la clôture de la procédure et les mesures correctrices et sanctions[46].

Quelle que soit l'issue de la procédure, celle-ci n'exclut pas la possibilité de vérifications ultérieures. En effet, la présidente de la CNIL peut décider de faire procéder à de nouveaux contrôles de l'organisme afin de s'assurer de sa mise en conformité.

Par ailleurs, un contrôle porte toujours sur un périmètre limité et n'emporte pas, quelle qu'en soit l'issue, validation de l'ensemble des traitements de l'organisme contrôlé.

La clôture de la procédure, avec ou sans observations

En l'absence de manquements aux dispositions du RGPD et de la loi Informatique et Libertés, ou en l'absence de mise en œuvre d'un traitement de données personnelles, la présidente de la CNIL adresse un courrier à l'organisme contrôlé pour l'informer de la clôture de la procédure.

Dans le cas où des manquements peu graves à la réglementation relative à la protection des données ont été relevés, la présidente de la CNIL peut décider de clore la procédure et d'indiquer dans le courrier de clôture des recommandations à l'égard des manquements relevés afin que l'organisme prenne des mesures pour y mettre un terme.

L'avertissement et le rappel aux obligations légales par la présidente de la CNIL

La présidente peut avertir un responsable de traitement ou un sous-traitant que les opérations de traitement qu'il envisage de mettre en œuvre sont susceptibles de violer les dispositions du RGPD.

[46] Voir « La chaîne répressive de la CNIL » sur cnil.fr.

La présidente peut également, en application de l'article 58(2) du RGPD, rappeler à ses obligations un responsable de traitement ou un sous-traitant ayant mis en œuvre des traitements qui ne respectaient pas la réglementation en vigueur.

La mise en demeure

En cas de manquements significatifs, l'organisme contrôlé peut être mis en demeure de se conformer aux dispositions du RGPD et de la loi Informatique et Libertés[47].

La mise en demeure est une décision de la présidente de la CNIL qui énumère les manquements reprochés à l'organisme ainsi que les mesures qu'il doit prendre pour se mettre en conformité.

La présidente de la CNIL peut fixer un délai de mise en conformité de l'organisme. Ce délai peut être fixé à vingt-quatre heures en cas d'urgence.

La présidente de la CNIL peut, en outre, demander qu'il soit justifié de la mise en conformité. Dans ce cas, l'organisme mis en demeure devra apporter une réponse étayée et fournir les justificatifs appuyant ses propos pour démontrer l'effectivité de sa mise en conformité dans le délai fixé par la présidente qui prononcera alors, si les réponses apportées sont satisfaisantes, la clôture de la procédure de mise en demeure.

Le cas échéant, cette mise en demeure peut être rendue publique par décision du bureau de la CNIL[48].

Enfin, la présidente de la CNIL peut décider de faire procéder à des vérifications après la mise en demeure afin de s'assurer de la mise en conformité de l'organisme.

Les décisions prononcées par la formation restreinte

- *La procédure ordinaire*

La présidente de la CNIL peut désigner un rapporteur qui saisira la formation restreinte de la CNIL. Celle-ci peut, à l'issue d'une procédure contradictoire, prononcer des sanctions[49] (pécuniaires ou non) ou une relaxe.

Une procédure de sanction peut être engagée à l'encontre d'un organisme notamment pour les motifs suivants :

- absence de réponse à la mise en demeure ;
- absence de mise en conformité dans le délai imparti par la mise en demeure ;
- manquements significatifs constatés.

Une procédure de sanction peut être engagée sans mise en demeure préalable en cas de manquements significatifs.

---

[47] Voir « La procédure de mise en demeure » sur cnil.fr.
[48] Article 20(II.5) de la loi Informatique et Libertés et article 43 du décret 2019-536 du 29 mai 2019 (décret d'application de la loi Informatique et Libertés). Le bureau de la CNIL est constitué de sa présidente et de ses deux Vice-Présidents.
[49] Voir « La procédure de sanction » sur cnil.fr.

Dans le cadre d'une procédure ordinaire (hors urgence), les mesures pouvant être prononcées par la formation restreinte[50] de la CNIL sont les suivantes (plusieurs mesures peuvent être prononcées pour une même procédure) :

- un rappel à l'ordre ;
- une injonction de mettre en conformité le traitement avec les dispositions de la loi Informatique et Libertés et du RGPD, ou une injonction de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits. Cette injonction peut-être assortie, sauf dans les cas où le traitement est mis en œuvre par l'État, d'une astreinte[51] dont le montant ne peut excéder 100 000 euros par jour de retard ;
- dans certains cas, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du RGPD ou de la loi Informatique et Libertés ;
- le retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée ;
- la suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;
- la suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes ;
- dans certains cas, une amende administrative, dont le montant peut s'élever **jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial** en cas de non-respect des principes fondamentaux du RGPD, des droits des personnes, des dispositions sur les transferts ou de non-respect d'une injonction d'une autorité. Cette amende peut atteindre jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial en cas de non-respect des obligations du responsable de traitement ou du sous-traitant (en matière de sécurité, d'analyse d'impact, de tenue du registre des activités, de désignation d'un DPO, etc.) ou de non-respect des obligations incombant à l'organisme de certification ou en charge des codes de conduite.

❖ *La procédure simplifiée*

Dans le cadre d'une procédure de sanction dite simplifiée[50], la présidente de la CNIL peut désigner un rapporteur qui saisira le président de la formation restreinte de la CNIL. Celui-ci peut déléguer la procédure de sanction dite simplifiée à un membre de la formation restreinte qu'il désigne. Le président de la formation restreinte ou le membre qu'il a désigné peut, à l'issue d'une procédure contradictoire, prononcer des sanctions[52] (pécuniaires ou non) ou une relaxe.

---

[50] La formation restreinte est une formation contentieuse ayant qualité de tribunal au sens de l'article 6(1) de la Convention européenne des droits de l'homme.

[51] Une astreinte est une condamnation à une somme d'argent, à raison de tant par jour, semaine ou mois de retard.

[52] Voir « La procédure de sanction » sur cnil.fr.

[50] Introduite par la loi n°2022-52 du 24 janvier 2022 et le décret n° 2022-517 du 8 avril 2022 modifiant le décret n° 2019-536 du 29 mai 2019

La procédure de sanction dite simplifiée ne peut être engagée que lorsque l'affaire ne présente pas de difficulté particulière, eu égard à l'existence d'une jurisprudence établie, des décisions précédemment rendues par la formation restreinte de la commission ou de la simplicité des questions de fait et de droit qu'elle présente à trancher.

La procédure de sanction simplifiée suit les mêmes étapes que la procédure de sanction ordinaire (pour les délais, la procédure contradictoire, etc.), mais ses modalités de mise en œuvre sont allégées : le président de la formation restreinte (ou le membre qu'il désigne) statue seul, la procédure est écrite et aucune séance publique n'est organisée, sauf si l'organisme demande à être entendu.

Les sanctions susceptibles d'être prononcées dans ce cadre sont limitées au rappel à l'ordre, à une amende administrative d'un montant maximum de 20 000 € et à une injonction avec astreinte plafonnée à 100 € par jour de retard ou, si le chiffre d'affaires annuel mondial de l'exercice précédent du responsable de traitement est supérieur à 50 millions d'euros, 100 000 € d'amende et 500 € par jour de retard. Ces sanctions ne peuvent pas être rendues publiques.

6. Les principes de bonne conduite

Le respect des principes de bonne conduite, par les contrôleurs comme par les personnes physiques et morales concernées par une mission de vérification de la CNIL, contribue à un déroulement satisfaisant des contrôles dans le respect des droits de chacun.

Principes applicables aux contrôleurs de la CNIL

Respecter un principe de proportionnalité et de minimisation des données demandées

Sans nuire aux constatations opérées lors de la mission de contrôle, les contrôleurs veillent à respecter les contraintes opérationnelles, techniques et professionnelles des organismes contrôlés. Les pièces collectées doivent servir strictement aux fins de l'objet de la mission décidé par la présidente de la CNIL et porté dans la décision de contrôle.

Les contrôleurs veillent à minimiser les données collectées en contrôle, que celles-ci soient des données personnelles ou non.

Les contrôleurs peuvent demander des éléments financiers (tels que des bilans comptables récents) à l'organisme afin d'éclairer la délégation sur les moyens dont dispose celui-ci pour mettre en œuvre les mesures nécessaires au respect de la réglementation relative à la protection des données à caractère personnel. Les contrôleurs peuvent également demander, dans le cadre des traitements mis en œuvre par une personne physique, des éléments d'information relatifs à son identité.

Expliquer le contexte et le déroulé de la mission de contrôle

Dans le respect du secret professionnel auquel ils sont astreints, les contrôleurs expliquent le contexte et le cadre de la mission de contrôle ainsi que son déroulé.

En revanche, les contrôleurs ne peuvent communiquer sur l'orientation de la procédure à la fin de la mission de contrôle, laquelle relève de la présidente de la CNIL ou, le cas échéant, de la formation restreinte. Toutefois, en cas de constatation d'un défaut de sécurité manifeste entraînant un risque de violation de données personnelles, les contrôleurs sont autorisés à le signaler sur le champ à l'organisme contrôlé.

Se comporter de manière professionnelle, neutre et courtoise

Les contrôleurs mènent leurs investigations avec diligence et professionnalisme afin de concilier les impératifs de la mission de contrôle, le délai d'investigation et les contraintes de l'organisme contrôlé. Ils sont tenus de signaler sans délai à leur responsable hiérarchique au sein de la CNIL les difficultés de nature à entraver le bon déroulement de la mission, ainsi que tout événement susceptible de la remettre en cause, ou encore toute difficulté qu'ils rencontreraient dans l'exercice de leur activité.

Les contrôleurs exercent leurs prérogatives, notamment en matière d'accès aux informations et aux documents des personnes physiques ou morales sollicitées, en conservant une attitude neutre et courtoise. Ils s'abstiennent d'exprimer tout avis personnel.

Lors des contrôles sur place et sur audition, les contrôleurs s'efforcent de laisser un temps suffisant aux personnes concernées pour prendre connaissance des informations qui leur sont communiquées, en appréhender la portée, répondre aux questions posées de façon pertinente, relire les procès-verbaux rédigés par les contrôleurs avant leur signature.

Les agents de la CNIL ne peuvent bénéficier d'aucune invitation, cadeau ou avantage de la part des personnes en lien avec la mission de contrôle.

Agir avec diligence

En l'absence de délai fixé par les textes, les missions de contrôle ne sont pas limitées dans le temps. La mission dure le temps nécessaire pour mener à terme les investigations, lesquelles peuvent avoir, en fonction de leur complexité et de leur composante internationale, des délais variables.

Comportement attendu des personnes sollicitées durant les missions de contrôle

Répondre aux questions posées par les contrôleurs avec loyauté et coopérer avec les contrôleurs

Les personnes physiques ou les collaborateurs des organismes contrôlés sont invités à répondre avec diligence, loyauté et clairement aux questions qui leur sont posées ou aux demandes de renseignements qui leur sont adressées tout au long de la mission de contrôle.

Les personnes sollicitées dans le cadre d'une mission de contrôle s'efforcent de fournir des réponses complètes et précises. Elles communiquent également les pièces appuyant leurs réponses aux contrôleurs.

Communiquer les pièces et explications demandées dans des délais raisonnables

En application des articles 8(2.g) et 19 de la loi Informatique et Libertés, « *les membres et agents [habilités] peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Ils peuvent recueillir, notamment sur place ou sur convocation, tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission*. » En outre, « *Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, […] par le secret médical.* »

Il est attendu que les demandes de pièces soient satisfaites dans un délai raisonnable qui concilie les contraintes de l'établissement des réponses et la nécessité de ne pas ralentir inutilement le déroulement de la mission de contrôle. Les documents et fichiers de réponse doivent être transmis dans un format facilement exploitable, à déterminer avec les contrôleurs.

Conserver une attitude neutre, professionnelle et courtoise pendant la durée du contrôle

Il est attendu des personnes sollicitées dans le cadre d'une mission de contrôle qu'elles adoptent une attitude professionnelle, neutre et courtoise vis-à-vis des contrôleurs, de la même façon que cette attitude est attendue de ces derniers.

7. Protection des données personnelles

La CNIL met en œuvre des traitements de données personnelles dans le cadre de ses activités de contrôle. Les personnes concernées par ces traitements disposent de droits Informatique et Libertés qu'elles peuvent exercer en s'adressant au délégué à la protection des données de la CNIL, par courrier postal ou via un formulaire en ligne.

Pour en savoir plus sur vos droits, pour consulter le registre des activités de traitement de la CNIL ou pour saisir son délégué à la protection des données, voir la page « Données personnelles » sur le site cnil.fr.