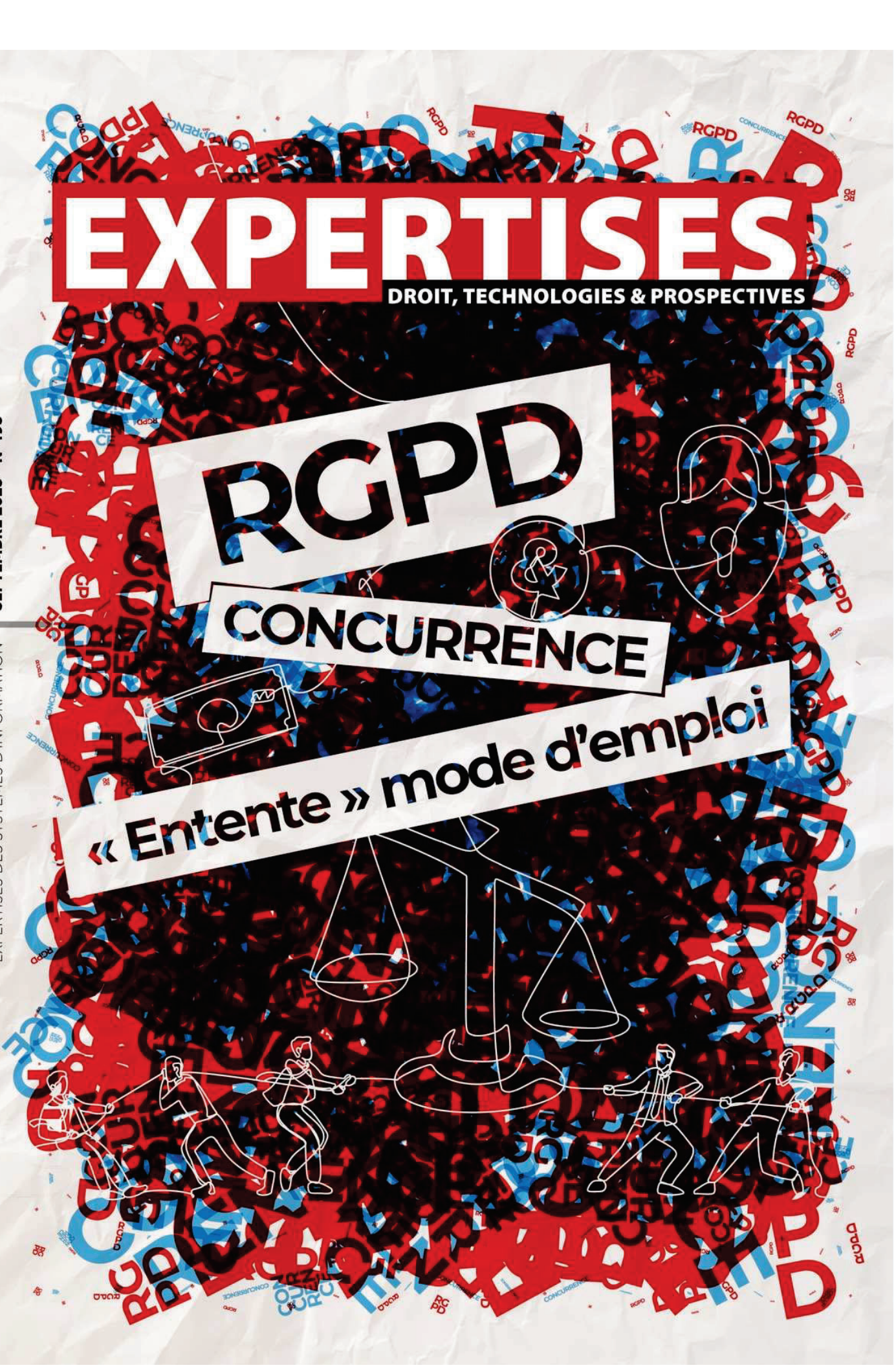
EXPERTISES DES SYSTÈMES D'INFORMATION
SEPTEMBRE 2023 - N°493

EXPERTISES

DROIT, TECHNOLOGIES & PROSPECTIVES

RGPD & CONCURRENCE

« Entente » mode d'emploi



RGPD

Contrôle sur audition par la CNIL, mode d'emploi

Retour d'expérience de conseils intervenus dans l'exercice du contrôle sur audition de la CNIL, moins fréquent que le contrôle sur place mais en augmentation, et qui peut avoir une influence majeure sur la décision qui en résultera.

La réalisation de contrôles, conséquence logique de la nouvelle responsabilité mise en place par le Règlement général sur la protection des données (RGPD), constitue la pierre angulaire du pouvoir de sanction de la Commission nationale informatique et libertés (CNIL).

Ce pouvoir lui est conféré par l'article 8-2° g) de la loi du 6 janvier 1978 modifiée, dite « *informatique et libertés* », qui l'autorise à « *procéder ou faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions* ».

Le régime des contrôles est quant à lui détaillé à l'article 19 de cette même loi. Les prérogatives de la Commission ainsi que les modalités des différents types de contrôle sont également reprises dans la charte publiée à cet effet[1]. Le contrôle dit « *sur audition* » est la méthode la moins utilisée par la CNIL, représentant seulement 9% des contrôles réalisés en 2022[2]. La CNIL lui préfère généralement le contrôle sur place (dans les locaux de l'entité contrôlée) ou en ligne (audit des sites webs de l'entité contrôlée), qui regroupés constituent la grande majorité des contrôles. Toutefois, le contrôle sur audition gagne chaque année en popularité : alors que 4 contrôles sur audition sur 310 ont été effectués en 2018, 31 des 345 enquêtes de la CNIL ont été réalisées sur ce modèle en 2022. La pandémie et les confinements, en réduisant la possibilité de contrôles sur place, ont contribué à cette hausse. Si de nombreux guides et retours d'expérience existent ainsi, concernant les contrôles sur place, les modalités du contrôle sur audition restent moins connues.
La préparation de cette audition et la connaissance de son déroulement peuvent cependant avoir une influence majeure sur la décision qui en résulte. Le cabinet revient donc sur ses expériences de contrôles sur audition et vous en décrit, chronologiquement, les différentes étapes.

Etape 1 – la convocation

La convocation est le point de départ du contrôle. Elle est reçue par l'entité contrôlée au plus tard 8 jours avant l'audition par lettre remise contre signature, ou remise en main propre contre récépissé ou acte d'huissier[3]. Elle contient l'ensemble des informations nécessaires à sa préparation ; il est donc essentiel pour l'organisation contrôlée, passée la mauvaise surprise de l'annonce d'un contrôle, d'en faire une lecture approfondie.

En premier lieu, cette convocation précise la date, l'heure et le lieu du contrôle. En ce qui concerne le lieu, les auditions ont en principe lieu au siège de la CNIL, place de Fontenoy à Paris. Compte tenu de la réalisation des différentes étapes de cette audition, il vaut mieux prévoir d'y consacrer la journée complète ! Surtout, la convocation précise le périmètre du contrôle réalisé par la CNIL

Cette information est notamment située dans la délibération de la Commission ayant ordonné la réalisation du contrôle, et jointe en annexe à la convocation. Cette information est primordiale car elle conditionne les informations que peuvent requérir les contrôleurs et sur la base desquelles d'éventuelles non-conformités pourront être identifiées. L'audition peut tout aussi bien concerner un traitement précis, qui aurait par exemple été affecté par une violation de données, que « *la conformité des traitements mis en œuvre par la société X* » de manière générale.
La convocation demande également au contrôlé, par le biais des coordonnées fournies, d'informer la Commission sur l'identité des personnes qui prendront part à l'audition. Il convient donc de s'assurer que l'ensemble des personnes en charge des traitements de données

audités sont présentes, afin de pouvoir répondre à l'ensemble des questions de la CNIL.

Sans déplacer toute l'entreprise, il peut donc être pertinent d'évoquer la présence des personnes suivantes :

- Un dirigeant ou directeur, au fait de l'histoire de l'entité, son activité, sa clientèle, ses objectifs, etc.
- Le DPO (data protection officer), spécialiste des questions RGPD et chapeautant l'ensemble des traitements réalisés par l'entreprise ;
- Le chef du service concerné, qui dirige la mise en place et la réalisation des traitements audités ;
- Le RSSI (responsable de la sécurité des systèmes informatiques) si le contrôle concerne la sécurité des données traitées par l'entreprise – notamment si le contrôle fait suite à une violation de données à caractère personnel ;
- Le développeur ou le collaborateur expert quant à la conception ou la manipulation des outils informatiques nécessaires aux traitements audités.

Par ailleurs, la convocation peut contenir une mention de la nécessité d'apporter à l'audition les moyens techniques (comme un ordinateur) permettant à la CNIL d'auditer directement les systèmes nécessaires aux traitements contrôlés. Les documents relatifs à la gouvernance des données et la conformité RGPD (tel que le registre des traitements) sont également à fournir.
La convocation précise également l'identité des membres de son personnel chargés du contrôle. Ces contrôleurs sont soumis à un strict processus d'habilitation, et ne peuvent participer à une procédure à l'encontre d'une organisation dans laquelle ils auraient exercé des fonctions ou détenu un intérêt les 3 dernières années[4]. Enfin, la CNIL rappelle que l'entité contrôlée est en droit de se faire assister par un avocat lors de l'audition.

Etape 2 – la préparation de l'audition

Une chose ressort clairement de la convocation : pas question d'arriver sans préparation le jour de l'audition. La CNIL attend des sociétés contrôlées une maîtrise de leurs traitements, de leurs outils informatiques, et surtout de la documentation liée à la conformité RGPD.
Les jours ou semaines précédant l'audition doivent donc être consacrés à la préparation active de cette dernière, suivant plusieurs étapes. D'abord, le rassemblement des différentes pièces nécessaires, ainsi que la recherche et compilation de toutes les informations qui pourraient être demandées par la CNIL. C'est ici que l'analyse du périmètre du contrôle prend tout son sens. Registres, politiques d'informations, contrats avec les sous-traitants, rapports d'incidents... doivent être réunis.
Il convient par ailleurs d'anticiper les points qui pourraient faire sourciller les contrôleurs et d'en préparer la justification. Pourquoi telle catégorie de données était-elle conservée pour une durée aussi longue ? Ce traitement de données sensibles entre-t-il bien dans le cadre des exceptions qui pourraient le rendre licite ? Un audit de conformité du ou des traitements concernés, afin de détecter les éventuelles aspérités et d'être prêt à les justifier, est fortement recommandé. Les traitements de chaque société sont réalisés en fonction de finalités, de moyens, de contraintes pratiques ou légales qui lui sont propres, et qu'il convient d'expliquer aux contrôleurs.

Ces auditions de la CNIL n'obéissent en outre pas au formalisme rigoriste qui caractérise les procédures judiciaires. Le but sera ici pour l'auditionné de décrire ses traitements, d'en démontrer la conformité ; sa proactivité ne pourra que jouer en sa faveur. Pour ce faire, l'organisme contrôlé pourra recourir à tous les mémoires explicatifs, tableaux, ou schémas de fonctionnement qu'il souhaite.
Une précision est ici nécessaire : les contrôleurs ne recueilleront aucune pièce au format papier durant l'audition. Si ce support peut être utile afin d'échanger directement sur les documents que vous avez préparé en amont, il ne faut donc pas oublier d'en préparer une copie numérique qui pourra être transmise via l'espace sécurisé de la CNIL.

Enfin, une fois les personnes se rendant à l'audition choisie, il convient de les entraîner avant leur entrée dans l'arène.
Elles doivent toutes maîtriser les moindres détails du traitement concerné, mais également l'ensemble du vocabulaire et des notions de la conformité RGPD. Pas question de faire état de lacunes devant la CNIL.

Ce travail de préparation accompli, l'auditionné est désormais prêt à être reçu par les contrôleurs.

Etape 3 – le jour J

Comme précédemment indiqué, le contrôle a généralement lieu dans les locaux de la CNIL. Les auditionnés peuvent donc s'attendre à être reçus dans une salle de réunion de taille où ils feront face durant la journée aux questions des contrôleurs.

L'audition commence généralement par une description générale de l'organisation auditionnée : son activité, sa clientèle, son chiffre d'affaires. Puis, la CNIL conduira la discussion spécifiquement sur les traitements qui l'intéressent. Ces interrogations concernent en premier lieu la responsabilité des traitements audités ; la CNIL s'assure que l'organisation contrôlée est bien responsable des traitements concernés, en ayant fixé les moyens et les finalités. La conformité documentaire de la société est également examinée, notamment via le registre des traitements.

Enfin, ce sont les modalités des traitements contrôlés qui seront examinées en détail : moyens utilisés, durées de conservation choisies, mesures de sécurité mises en place... Si le contrôle fait suite à une violation de données, ses circonstances et son instruction par le responsable de traitement feront également l'objet de questions détaillées.

C'est le III de l'article 19 de la loi Informatique et libertés qui encadre le pouvoir d'investigation de la CNIL à l'occasion de l'audition. Les prérogatives des contrôleurs sont vastes : ils « *peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie* », mais également « *tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission* ».

Le caractère secret des informations demandées par la CNIL ne peut généralement pas être opposé aux contrôleurs. Seuls pourront être valablement invoqués le secret des relations entre avocat et client, ainsi que le secret des sources journalistiques. Quant au secret médical, il n'est opposable que dans le cas de traitements relatifs à la recherche ou la santé – et il est prévu que des données médicales individuelles puissent être communiquées sous l'autorité et en présence d'un médecin[5].

Lorsqu'un tel secret est opposé au contrôleur, la mention de cette opposition est portée au procès-verbal établi à l'issue du contrôle[6].

L'attitude des contrôleurs de la CNIL, durant ces interrogatoires, peut être déconcertante. Il faut ici rappeler que ces auditeurs ne sont pas là pour porter un jugement, ou décider d'une sanction, mais pour constater une situation. Plus huissier que juge, le contrôleur adopte une attitude neutre que pourraient lui envier les plus grands joueurs de poker, et ne réagit pas aux faits qui lui sont rapportés. Il reporte scrupuleusement sur son ordinateur les propos des personnes auditionnées, en préparation du procès-verbal qui sera rédigé en fin de journée. Il ne faut pas non plus s'attendre à obtenir, de la part de ces contrôleurs, des conseils sur la marche à suivre ou une manière d'améliorer le traitement.

Cette attitude leur est imposée par la charte des contrôles de la CNIL, qui stipule : « *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.* »[7]

La loi informatique et libertés prévoit également la possibilité pour les contrôleurs d'« *accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.* »[8].

Si la convocation prévoit un tel examen de systèmes d'informations, le matériel apporté par les personnes auditionnées sera connecté à un projecteur. Les contrôleurs ne manipulent pas eux-mêmes ce matériel, mais demandent aux participants de leur faire la démonstration de leurs bases de données ou logiciels. Des extractions de ces bases pourront être réalisées, et chaque étape de la visite est immortalisée par une capture d'écran.

À l'issue de ces deux étapes, généralement en fin de journée, les contrôleurs se retirent pour rédiger le procès-verbal de l'audition. Ce temps est l'occasion d'un peu de repos et de réflexion pour les auditionnés ; il peut aussi leur permettre, afin de les communiquer immédiatement à la CNIL, de réunir les pièces supplémentaires dont la nécessité est ressortie pendant les discussions.

Suite à la rédaction du procès-verbal, une relecture contradictoire est réalisée par les agents de la CNIL ainsi que les personnes auditionnées. Il s'agit pour ces dernières d'un moment crucial, qui ne doit pas être sous-estimé : le procès-verbal constituera la base de la décision de la Commission quant aux suites à donner au contrôle. L'organisation contrôlée doit se montrer vigilante et s'assurer que les informations qui y figurent reflètent bien la réalité des traitements, telle qu'elle a été relatée durant les échanges de la journée. Il ne faut donc pas hésiter à demander à ce que certaines modifications ou nuances soient opérées avant la signature de la version finale.

Un espace permet également aux personnes auditionnées de librement fournir leurs commentaires sur le procès-verbal et le sujet du contrôle en général. Une fois le Procès-verbal finalisé et signé, l'audition prend fin.

Etape 4 – les suites de l'audition

La fin de la journée d'audition ne signifie cependant pas la fin des efforts de l'organisation contrôlée.

En effet, il sera dans la majorité des cas ressorti des débats la nécessité de produire certaines informations et pièces supplémentaires ; elles doivent alors être réunies et fournies à la CNIL dans un délai de 8 jours ouvrés. L'efficacité est donc de mise. De la même manière, si la CNIL a demandé la réalisation de certaines actions en urgence (comme la purge de certaines données), il conviendra d'en justifier.

En outre, il convient de préciser à l'attention des organisations internationales que, comme le prévoit l'article 12 du décret n° 2019-536 du 29 mai 2019 pris en application de la loi informatique et libertés, la CNIL est en droit d'exiger du responsable de traitement qu'il joigne, le cas échéant, une traduction en français des documents demandés.

Une fois l'ensemble des pièces remises, la CNIL procède à l'instruction du dossier. Cette période peut durer plusieurs mois, et résulter en de nouvelles questions ou demandes de la part de la Commission. Durant cette période, l'organisation peut communiquer de manière spontanée à la CNIL sa progression en matière de conformité RGPD. Si de nouvelles politiques sont mises en place ou des traitements modifiés afin d'assurer la conformité, communiquer ces informations à la CNIL ne pourra que démontrer de l'attitude proactive et de la volonté d'amélioration de la société.

L'auditionné ne doit pas s'inquiéter du sort réservé aux informations et documents dont les contrôleurs prennent copie au cours du contrôle : le règlement intérieur de la CNIL oblige cette dernière à les conserver dans des conditions garantissant leur authenticité, leur intégrité et leur confidentialité, quel qu'en soit le support. Ils sont détruits « *un an après la clôture du contrôle, sous réserve d'éventuels contentieux.* »[9]

Par ailleurs, à tout moment et en particulier durant cette période, l'auditionné doit également veiller à ce que ses sites web et autres ressources accessibles via Internet laissent entrevoir de sa conformité. En effet, l'article 19 de la loi Informatique et Libertés autorise également les contrôleurs, « *en dehors des contrôles sur place et sur convocation* »,

à « *consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations.* ».

Suite à cette instruction, la présidence de la CNIL décide de l'orientation à donner. Les possibilités sont diverses :

- La réalisation de contrôles supplémentaires, par exemple dans les locaux de l'organisation ;
- La clôture de la procédure, avec ou sans observations : en cas d'absence de manquements au RGPD, ou de manquements peu graves ne nécessitant qu'une recommandation de la CNIL.
- L'avertissement ou le rappel à l'ordre par la CNIL : Le rappel à l'ordre, prévu par l'article 20, II, 1er alinéa de la loi informatique et libertés constitue une alternative à la mise en demeure en cas de suspicion de manquements au RGPD ou pour les manquements les moins graves.
- La mise en demeure : en cas de manquements significatifs, l'organisme peut être mis en demeure d'y remédier dans un délai fixé, qui peut, dans les cas les plus extrêmes, être de vingt-quatre heures. Le mis en demeure devra justifier de sa mise en conformité. La mise en demeure caractérise les manquements du responsable auditionné, fixe un délai de mise en conformité, et prévient des conséquences en cas de non-respect[10]. La mise en demeure peut être publiée par la CNIL, ce qui peut déjà, même en l'absence de toute sanction, causer un dommage réputationnel important à l'organisation visée.
- La saisine de la formation restreinte : la formation restreinte est l'organisme de sanction de la CNIL. Sa saisine signifie un réexamen du dossier, dans le cadre d'une procédure contradictoire, suite à la détection de violations de la réglementation applicable en matière de données personnelles. A l'issue de la procédure, la formation restreinte pourra décider de mettre fin aux poursuites, de soumettre l'auditionné à une injonction, de lui retirer une certification, ou encore d'imposer une amende administrative d'un montant pouvant, dans les cas les plus graves, atteindre 20 millions d'euros ou 4% du chiffre d'affaires du groupe dont fait partie l'auditionné[11].

En résumé, outre la longue journée d'audition dans les locaux de la CNIL qui en constitue le point d'orgue, la procédure de contrôle sur audition représente pour l'organisation auditionnée un travail important en amont et en aval.

Prendre au sérieux ce travail et s'assurer d'une bonne préparation, avec l'accompagnement d'un conseil rompu à l'exercice, permet d'améliorer les chances de l'auditionné d'éviter une transition vers la procédure de sanction.

Sylvain JOYEUX
Avocat associé

Corentin POUSSET-BOUGERE
Avocat

Cloix Mendès Gil

Notes

(1) CNIL, charte des contrôles

(2) CNIL, rapport d'activité 2022

(3) Art. 34, Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

(4) Art. 18, décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

(5) Art. 19-III, loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

(6) Art.37, décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

(7) « Principes applicables aux contrôleurs de la CNIL », 6-Les principes de bonne conduite, Charte des contrôles de la CNIL

(8) Art. 19-III, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

(9) Art. 57, règlement Intérieur de la CNIL

(10) Art.20, loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; art. 38, décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; Art. 59 et 60, règlement intérieur de la CNIL

(11) Art. 20-III, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés