Les contrôles inopinés de la CNIL

Comment y faire face et à quoi s'attendre ?

18/04/2019

syntec numérique

Quels types de contrôle?

- Un contrôle en ligne
- Une audition sur convocation
- Un contrôle sur pièces
- Un contrôle sur place

Le contrôle sur place étant celui des 4 auxquels vous serez le moins préparé, nous concentrerons notre attention, lors de cette conférence, tout particulièrement sur lui.

Le contrôle en ligne :

Il est de plus en plus répandu à mesure que les entreprises développent des solutions de type Application et/ou site de e-commerce.

L’issue de ce contrôle dépendra essentiellement de la configuration de votre système d’information et des informations que vous mettrez à disposition (CGU/CGV/Politique de confidentialité, mentions légales).

Il peut donner lieu, seul, au prononcé d’une sanction définitive.

L’audition sur convocation :

La CNIL est autorisée à convoquer les responsables de votre société dans ses locaux afin de les inviter à répondre à une série de questions liées à vos traitements de données à caractère personnel.

Le plus souvent ce contrôle aura lieu postérieurement à un contrôle en ligne.

Il peut être utile de faire intervenir lors de cette audition, le responsable technique de votre entreprise et le responsable juridique (ou DPO) s’il y en a.

Le contrôle sur pièces :

Les agents de la CNIL adressent aux responsables de l'entreprise un courrier recommandé 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 Commission ses réponses en y joignant tout document utile permettant de les justifier.

Il est important de répondre de façon sincère et exacte à tous les points objets des questions pour la bonne et simple raison pour la bonne et simple raison que la CNIL aura pu et pourra, par la suite, vérifier l'exactitude de tout ou partie d'entre eux lors d'un contrôle sur place.

Le contrôle sur pièces (2):

De manière générale, la CNIL peut solliciter, pour un contrôle sur pièces, la communication de tous documents nécessaires à l'accomplissement de sa mission.

La CNIL demandera à l'organisme contrôlé de préciser la nature des opérations réalisées, les conditions de sécurité des traitements visés, etc.

En pratique les demandes de précisions figurant dans ledit contrôle vont dépendre étroitement du niveau de maturité de l'entreprise sur la question du traitement des données à caractère personnel.

La CNIL n'a, en effet, vocation à interroger l'organisme que sur ce sur quoi elle n'a pas obtenu de réponse en précédant au préalable à une analyse de ce qui figure notamment déjà sur le site institutionnel de l'entreprise.

Le contrôle sur place : il s’agit du contrôle objet principal de cette conférence.

Les contrôles sur place :

Un contrôle par qui?

La CNIL a des agents habilités à assurer ces contrôles. La liste de ces agents est disponible sur le site de la CNIL et fait l'objet d'une délibération annuelle en ce sens.

La plupart du temps, elle enverra quatre personnes : trois juristes et un auditeur des services d'information.

Les agents habilités de la CNIL

La liste des agents habilités à effectuer des contrôles est disponible sur le site de la CNIL

Un agent ne peut pas contrôler un organisme dans lequel au cours des 3 années précédant le contrôle il détenait un intérêt direct ou indirect ou s'il y a exercé des fonctions ou une activité professionnelle ou encore détenu un mandat

La CNIL peut se faire assister d'experts à ses frais

Les contrôles sur place :

Un contrôle quand?

Les contrôles peuvent avoir lieu dans vos locaux de six heures du matin à vingt-une heures.

Dans les faits, la CNIL tentera de provoquer un effet de surprise et n’arrivera jamais à six heures, faute de pouvoir prétendre vous y surprendre.

Les contrôles sur place :

Un contrôle où?

Les contrôles de la CNIL peuvent avoir lieu partout où a lieu un traitement de données à caractère personnel.

Ainsi, la CNIL a un champ de possibilités large même si la plupart du temps elle ira au siège social de votre entreprise.

Elle a néanmoins la possibilité d'envoyer quatre agents au siège ainsi que d'autres dans des locaux annexes où sont traitées des données à caractère personnel (effet de surprise oblige).

Premier contact avec la CNIL

Conformément à l'article 44 de la loi du 6 janvier 1978 :

le responsable des lieux est informé de **son droit d'opposition** à la visite.

Un droit à utiliser seulement dans les cas extrêmes car très mal perçu (tentative de dissimulation de preuve).

L'utilisation de ce droit ne signifie pas la clôture définitive du contrôle (bien au contraire).

Trois cas de figure relatifs au droit d'opposition

1. Vous ne vous opposez pas au contrôle: alors celui-ci se déroulera de **manière classique** en présence des quatre agents habilités par la CNIL

2. Vous vous opposez au contrôle: dans ce cas ce refus aura des conséquences administratives puisque la CNIL ne se privera pas de la faculté qui lui est donnée de demander une autorisation au juge des libertés et de la détention. Si ce dernier autorise le contrôle, la visite aura lieu sous son autorité et son contrôle.
Vous ne pourrez plus vous opposer au contrôle.

3. Dans certains cas, parce que « *l'urgence, la gravité des faits ou le risque de destruction ou de dissimulation de documents le justifie* », la CNIL peut directement demander l'autorisation préventive au juge des libertés et de la détention de procéder au contrôle sur place.
Dans ce cas de figure, vous n'aurez donc pas la possibilité de vous opposer au contrôle (et ce dès l'origine).

Un contrôle en présence de qui?

En plus des quatre agents habilités de la CNIL, le contrôle se fait en présence du responsable des lieux, c'est-à-dire: le représentant social de la société ou toute personne désignée par l'entreprise en ce sens.

Il est préférable de faire intervenir un sachant tel que le directeur de la technique, le CTO, le RSSI ou le DSI pour répondre aux questions de la CNIL.

L'idéal serait qu'ils soient assistés du responsable juridique ou du DPO, notamment lorsque vous êtes tenu, par le RGPD, d'en avoir un.

Prérogatives des agents habilités une fois sur place

L'article 44. III de la loi du 6 janv. 1978 prévoit que les agents habilités peuvent demander :

- la communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie.

-tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission.

Ils peuvent également accéder:

-**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.**

Ce pouvoir doit s'exercer dans des conditions préservant la confidentialité à l'égard des tiers.

La CNIL ne pourra pas demander la communication et/ou la copie des informations couvertes par:

Le secret professionnel régissant la relation entre un avocat et son client.

Il s'agit essentiellement des échanges entre l'avocat et son client. L'Avocat ne peut prétendre valablement faire jouer le secret professionnel quant il s'agit de rendre compte, à la CNIL, de son travail d'accompagnement en tant que DPO auprès de la société objet du contrôle.

Le secret médical

Le secret des sources des traitements journalistiques

Toujours au titre des prérogatives de la CNIL, l'article 44 prévoit que :

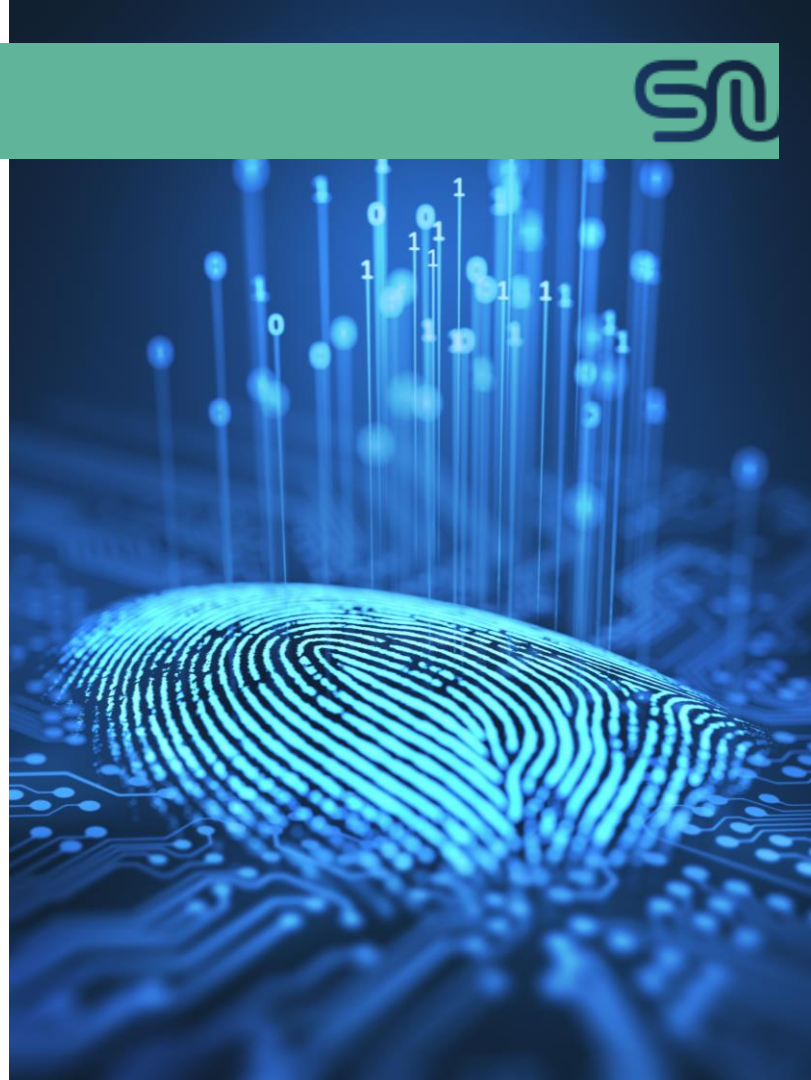
La CNIL a l'autorisation de se maintenir dans votre STAD (système de traitement automatisé de données) sans risquer de poursuites sur le fondement de L.323-1 du code pénal pour maintien frauduleux.

La CNIL peut exercer sa mission sous un nom d'emprunt lorsqu'elle contrôle en ligne sans risquer de poursuites La CNIL peut exercer sa mission sous un nom d'emprunt lorsqu'elle contrôle en ligne sans risquer de poursuites pour usurpation d'identité (226-4-1 du code pénal)

Les issues du contrôle :

Un contrôle peut se terminer par :

- -Une clôture (ex: Affaires Malakoff Médéric, Teemo, Singlespot, etc…)
- -Une mise en demeure de réaliser des corrections et de prendre des mesures
- -Un projet de sanctions soumis par un rapporteur désigné à l'entreprise contrôlée ainsi qu'à la formation restreinte de la CNIL suivie d'une phase de contestation du projet par l'entreprise contrôlée
- -Une sanction définitive prononcée (ou non) par la formation restreinte de la CNIL
- -Un recours éventuel devant le Conseil d'Etat par l'entreprise contrôlée dans un délai de 2 mois ou alors de 4 mois si l'entreprise est étrangère (ex: JC DECAUX)



La clôture du contrôle

La clôture intervient lorsque le contrôle n’appelle pas d’observations particulières ou lorsque les manquements observés ne justifient pas l’engagement d’une procédure contentieuse

La mise en demeure

Elle contient les manquements qui vous sont reprochés et dans quel délai vous devez vous mettre en conformité.

En pratique, et à la condition que vos excuses soient fondées et démontrées, il est envisageable d'expliquer à la CNIL les difficultés matérielles vous empêchant de tenir les délais qu'elle vous impose. La CNIL n'est pas tenue légalement d'en tenir compte.

La procédure de sanction :

Un rapporteur désigné établi un rapport contenant notamment un projet de sanction

Convocation de la formation restreinte

Possibilité d'avoir accès à votre dossier (Procès verbal, etc…)

Vos observations écrites :

En vertu de l'article 75 du décret numéro 2005-1309 du 20 oct. 2005: vous serez notifié du rapport transmis à la formation restreinte. Vous disposerez alors d'un mois pour transmettre au rapporteur et à la formation restreinte vos observations écrites.

Le rapporteur peut vous répondre dans un délai de 15 jours suivant la réception de vos observations. Dans ce cas, vous disposerez à nouveau d'un délai de 15 jours pour produire des observations écrites.

A tout moment, le rapporteur peut décider de modifier son rapport. Dans ce cas, la procédure permettant de produire des observations écrites reprendra tel que précédemment.

Par ailleurs, vous sera notifiée, la date de la séance de la formation restreinte au cours de laquelle est inscrite votre affaire. Vous aurez alors, la faculté d'y être entendu.

Le prononcé d'une sanction définitive

Sur le plan financier, la CNIL a la possibilité de prononcer des amendes administratives :

2% du chiffre d'affaires annuel mondial ou 10 millions d'euros pour le non-respect de certaines obligations imposées par le RGPD telles que l'obligation de procéder à une analyse d'impact, de nommer un DPO, d'établir des registres de traitement ou d'alerter la CNIL sur les failles de sécurité, etc...

4% du chiffre d'affaires annuel mondial ou 20 millions pour le non-respect de principes fondamentaux tels que le respect de la finalité du traitement de données, la minimisation ou encore le droit d'accès des personnes à leurs données, etc…

Le recours éventuel :

En cas de sanction prononcée par la formation restreinte, il vous est possible d'exercer un recours devant le Conseil d'Etat:

Vous disposerez alors d'un délai de deux mois à compter de la signification de la décision (*quatre mois s'il s'agit d'une entreprise dont le siège social est basé à l'étranger*)

Des questions ?

Merci pour votre attention

syntec numérique

CONTACTS

Sadry PORLON
Avocat au Barreau de Paris
Docteur en Droit

www.porlon-avocats.com
38 Avenue Hoche – Paris 75008
Tel. +33 1 77 62 88 13 – Fax. +33 9 72 16 37 15
Email : cabinet@porlon-avocats.com