

Contrôle CNIL : comment ça se passe, comment s'y préparer

Qui est contrôlé, sur quoi, avec quelles suites : démystifier le contrôle — et la courte liste qui vous met en position de force.

8 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/contrôle-cnil

Le contrôle CNIL évoque l'inspection surprise et l'amende à six chiffres — la réalité est plus prosaïque : des contrôles souvent écrits, déclenchés par des plaintes ou des thématiques annuelles, et des suites graduées où la sanction lourde punit surtout la négligence persistante et la mauvaise foi. Pour une PME au socle RGPD en place, le contrôle est un exercice de démonstration — à condition d'avoir les pièces prêtes.

1. Pourquoi et comment on est contrôlé

- Les déclencheurs : les plaintes (client mécontent, salarié en litige — la source n° 1 pour les PME), les violations de données notifiées ou médiatisées, les thématiques annuelles annoncées par la CNIL, et le signalement en chaîne (un sous-traitant contrôlé mène à ses clients)
- Les formes : le contrôle sur pièces (courrier avec questionnaire et demande de documents — le plus courant), l'audition, le contrôle en ligne (vos sites et applis, testés à distance), et le contrôle sur place (délégation dans les locaux, plutôt pour les cas sérieux)
- Les agents ont des pouvoirs réels : accès aux locaux professionnels, aux traitements, copies de documents — l'obstruction est elle-même une infraction lourdement sanctionnée

2. Ce qui est demandé en pratique

- Le registre des traitements : LA pièce maîtresse, demandée systématiquement — son absence est un très mauvais départ
- Les mentions d'information et politiques (site, formulaires, contrats de travail) et les preuves de consentement quand il est requis
- Les contrats de sous-traitance (article 28 / DPA) des prestataires qui touchent aux données
- Les mesures de sécurité : c'est là que MFA, gestion des accès, sauvegardes et chiffrement deviennent des pièces de conformité
- Le registre des violations et les preuves de traitement des demandes de droits — même vides, leur existence démontre le processus
- Sur les thèmes sensibles : vidéosurveillance, géolocalisation, prospection, cookies — les classiques du contrôle PME

BON À SAVOIR

Le « classeur CNIL » (physique ou numérique) : registre des traitements, politiques et mentions, liste des sous-traitants avec DPA, description des mesures de sécurité, registres violations et droits, charte informatique. Six pièces tenues à jour = un contrôle sur pièces qui se répond en jours sereins au lieu de semaines de panique. C'est aussi, mot pour mot, ce que demandent les grands donneurs d'ordres et les assureurs.

3. Pendant le contrôle : la bonne attitude

- Coopérer pleinement et dans les délais — demander une prolongation motivée vaut mieux qu'un retard silencieux
- Répondre juste : ni minimiser ni broder ; « ce point est en cours de mise en conformité, voici le plan et l'échéance » est une réponse recevable et appréciée
- Centraliser la parole : un interlocuteur unique (dirigeant, référent ou conseil) — les réponses dispersées se contredisent
- Se faire accompagner pour un contrôle sur place ou un dossier sensible : un avocat ou un DPO externe connaît la partition
- Tout tracer : ce qui est remis, dit, demandé — le dossier du contrôle se gère comme un dossier contentieux

4. Les suites possibles — et la vraie leçon

- L'éventail gradué : clôture simple, rappel aux obligations, mise en demeure (publique ou non) avec délai de mise en conformité, et sanctions (amendes — jusqu'à 4 % du CA mondial en théorie, procédure simplifiée à 20 000 € max pour les dossiers simples — injonctions sous astreinte, publicité)
- Ce qui aggrave : la durée et l'ampleur du manquement, le nombre de personnes touchées, la mauvaise coopération, la récidive ; ce qui atténue : la bonne foi, les corrections engagées, la coopération
- La mise en demeure se traite comme un projet prioritaire : plan d'action, preuves, réponse dans les délais — bien menée, elle se clôt sans sanction
- La leçon générale : la conformité démontrable en amont coûte quelques jours de travail ; le contrôle subi sans préparation coûte des semaines — et parfois bien plus

L'essentiel à retenir

- 01 Constituer et tenir le « classeur CNIL » (6 pièces)
 - 02 Vérifier les classiques PME : cookies, vidéosurveillance, prospection
 - 03 Désigner l'interlocuteur unique en cas de contrôle
 - 04 Répondre dans les délais, avec exactitude et plan d'action
 - 05 Se faire accompagner dès que le dossier est sensible
 - 06 Traiter toute mise en demeure comme un projet prioritaire
-

Questions fréquentes

Une TPE de 5 personnes est-elle vraiment contrôlable ?

Oui — la CNIL contrôle et sanctionne des très petites structures chaque année, presque toujours sur plainte : le salarié licencié qui signale la vidéosurveillance abusive, le prospect harcelé qui n'obtient pas sa désinscription. La taille module les attentes (nul n'exige d'une TPE le dispositif d'un groupe), pas le principe. Et le socle proportionné se construit en quelques jours (voir notre guide RGPD).

Le contrôle en ligne peut-il nous « tester » sans prévenir ?

Oui : la CNIL peut constater à distance, sous procès-verbal, ce que votre site fait réellement — cookies déposés avant consentement, formulaires sans mention, absence de politique. C'est le contrôle le moins coûteux pour elle, donc fréquent. Un audit de votre propre site (dix minutes avec les outils du navigateur, ou via votre prestataire) vous montre exactement ce qu'elle verrait.

Faut-il prévenir notre assureur ou notre avocat dès le courrier reçu ?

Réflexe sain : certains contrats (protection juridique, volet cyber) couvrent l'assistance en cas de contrôle — autant l'activer tôt. Et un conseil qui relit vos réponses avant envoi évite les formulations qui engagent inutilement. Le coût d'une relecture est sans commune mesure avec celui d'une réponse maladroite devenue pièce du dossier.

Pour aller plus loin

CNIL — comment se déroule un contrôle — www.cnil.fr/fr/les-controles-de-la-cnil

CNIL — les sanctions prononcées — www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr