

Fiche conseil. 12

Que faire en cas de contrôle CNIL ?

La CNIL a le pouvoir d'effectuer des contrôles auprès de l'ensemble des organismes qui traitent des données personnelles. Les entreprises privées, les associations ou encore les organismes publics peuvent ainsi faire l'objet d'un contrôle de la CNIL.

Risques

1. **Mise en demeure de l'organisme** d'adopter des mesures pour se mettre en conformité (cette mise en demeure peut être rendue publique)
2. Le Président de la CNIL peut engager une **procédure de sanctions** contre l'organisme
3. **Risques réputationnels** pour l'organisme

Que dit le RGPD ?

La CNIL peut effectuer des contrôles auprès de tout organisme traitant des données personnelles disposant d'un établissement en France, ou concernant des personnes résidant en France.

Ces contrôles peuvent se dérouler sur place, sur pièces, sur audition ou en ligne. Ces missions d'investigation sont un moyen d'action indispensable pour vérifier le respect de la loi Informatique et Libertés modifiée et du règlement européen sur la protection des données (RGPD) du 27 avril 2016 par les responsables de traitement et les sous-traitants. Elles permettent aussi d'apprécier concrètement les enjeux émergents en matière de protection des données personnelles.

La CNIL peut effectuer des contrôles auprès de tout organisme traitant des données personnelles disposant d'un établissement en France, ou concernant des personnes résidant en France.

Ces contrôles peuvent se dérouler sur place, sur pièces, sur audition ou en ligne. Ces missions d'investigation sont un moyen d'action indispensable pour vérifier le respect de la loi Informatique et Libertés modifiée et du règlement européen sur la protection des données (RGPD) du 27 avril 2016 par les responsables de traitement et les sous-traitants. Elles permettent aussi d'apprécier concrètement les enjeux émergents en matière de protection des données personnelles.

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).

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'UE et/ou traite les données personnelles de plusieurs personnes concernées dans l'UE.



Fiche conseil. 12

Que faire en cas de contrôle CNIL ? (suite)

Comment se déroule le contrôle ?

1. L'objet d'un contrôle est de vérifier que les traitements mis en œuvre par l'organisme sont conformes aux dispositions de la loi Informatique et Libertés modifiée et du RGPD.
2. À l'occasion d'une mission de contrôle, les agents ont vocation à prendre copie de toute information dans lesquelles sont mis en œuvre les traitements de données personnelles.
3. Les agents de la CNIL peuvent s'entretenir avec tout personnel susceptible de détenir des informations utiles pour apprécier la conformité des traitements de données personnelles.
4. Les contrôleurs peuvent accéder aux programmes informatiques et aux données, et en demander la transcription pour les besoins du contrôle.
5. La délégation peut demander copie de contrats (par exemple : contrats de location de fichiers, contrats de sous-traitance informatique), de formulaires, de dossiers papiers, de bases de données, etc.
6. Un procès-verbal est établi à l'issue du contrôle et fait état de toutes les informations recueillies par la délégation et des constatations qu'elle a réalisées. Il répertorie en annexe tous les documents qui ont été copiés dans le cadre du contrôle.



Ce document a été conçu par 15:MA à des fins d'information et de sensibilisation. Il ne peut être reproduit ou diffusé, même partiellement, sans mention de la source.

Bonnes pratiques

- Écrire une procédure à suivre en cas de violation de données et la diffuser auprès des personnes susceptibles d'accueillir les inspecteurs de la CNIL (accueil...);
- Tenir à jour l'ensemble de la documentation RGPD (accountability, registre procédures, audits,
- AIPD, durée de conservation et sensibilisation des collaborateurs);
- Garantir des mesures de sécurité suffisantes afin de maintenir la confidentialité des données.