
# Les RDV Experts

## RISQUES CYBER - RGPD | DORA | NIS2

# La CNIL rappelle que le responsable de traitement doit auditer son sous-traitant

La CNIL vient de prononcer une nouvelle sanction https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000049231950 à hauteur de 310 000€ pour un double manquement :

- un manquement à l'obligation de traiter les données de manière licite ;
- un manquement à l'obligation d'assurer la sécurité des données.

**Mais cette décision remet sur le devant de la scène l'impérieuse nécessité pour un responsable de traitement de s'assurer que son sous-traitant respecte le RGPD.**

## Le responsable de traitement, primo responsable

En l'espèce, le responsable de traitement réalisait des campagnes de prospection commerciale par téléphone à partir de fichiers de prospects achetés auprès de plusieurs fournisseurs de données, ces derniers procédant à la collecte desdites données par l'intermédiaire de formulaires de participation à des jeux-concours en ligne.

La CNIL reproche en particulier l'absence d'identification du responsable de traitement lors de la collecte des données.

En défense, le responsable de traitement a indiqué qu'il était lié par un contrat avec le sous-traitant, contrat dans lequel figurait bien l'obligation pour le sous-traitant de fournir la liste de ses partenaires.

La réponse de la CNIL est sans appel, elle rappelle que le responsable de traitement est tenu de vérifier les conditions d'exécution de ses obligations par le sous-traitant :

*« Il résulte de ces dispositions qu'en sa qualité de responsable de traitement, la société F. **est tenue de vérifier elle-même** que les conditions lui permettant de réaliser des opérations de prospection commerciale sont réunies ».*

La CNIL précise que les obligations contractuelles pouvant être imposées aux sous-traitants ne sauraient exonérer le responsable de traitement de sa responsabilité malgré l'existence éventuelle d'une responsabilité des fournisseurs.

La CNIL enfonce le clou en indiquant que le responsable de traitement n'est pas en mesure d'attester des contrôles qu'il prétendait avoir réalisés.

## Règles à respecter pour le responsable de traitement

Ainsi, il apparaît clairement que la seule signature d'un contrat, fût-elle assortie d'obligations précises voir de sanctions contre le sous-traitant, ne dégage pas le responsable de traitement de sa propre responsabilité.

L'obligation de procéder à des audits apparait d'autant plus nécessaire que le DPA (data processing agreement), qui lie le sous-traitant au responsable de traitement, est supposé comporter un article dédié

*« Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique (…)*

*Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :*
*(…)*
*met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article **et pour permettre la réalisation d'audits, y compris des inspections**, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits. »*

Le responsable de traitement doit donc :

- vérifier avant le contrat, que le sous-traitant présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Cette obligation ne peut être remplie sans adresser au sous-traitant un questionnaire approprié ;
- rédiger un DPA ou accepter (après vérification) un DPA conforme aux exigences de l'article 28 ;
- procéder à des audits des agissements de son ou ses sous-traitants si nécessaire par des contrôles sur place.

De fait, les conditions matérielles d'un audit devraient être précisées dans le DPA :

- quand déclencher un audit ?
- sous quelle forme (documentaire / inspection) ?
- qui peut être l'auditeur (interne / externe) ?
- que fait-on si le rapport d'audit révèle des non-conformités ?
- ...

## Le sous-traitant n'est pas un irresponsable

Cette décision n'est pas de nature à remettre en cause la possibilité pour la CNIL de sanctionner un sous-traitant es qualité.

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000045614368?init=true&page=1&query=san-2022-009&searchField=ALL&tab_selection=all

## Votre cybersécurité repose sur vos sous-traitants : êtes-vous prêts ?

Pour explorer le sujet plus en détail et répondre à toutes les questions que vous devriez vous poser :

- À quels textes suis-je soumis ?
- Quel est le niveau de maturité attendu ?
- Quelles sont les sanctions encourues ?
- Quel référentiel appliquer ?
- Comment vérifier la conformité de mes prestataires IT ?
- Quelles sont les clauses contractuelles imposées ou impactées ?
- Quelles sont mes obligations en termes d'audit et leurs conséquences ?

**Nous vous donnons rendez-vous le 19 mars à 10h pour un webinar inédit, animé par nos experts !**

👉 **https://webikeo.fr/webinar/cybersecurite-impact-des-nouvelles-regles-europeennes-sur-vos-relations-avec-vos-prestataires-it**


Eric Barbry
Avocat Associé spécialisé IP/ IT
ebarbry@racine.eu

Marc-Antoine Ledieu
Avocat à la Cour et RSSI legal
marc-antoine@ledieu-avocats.fr

Jean-Philippe G
CEO de Cyberze
jpg@cyberzen.