Maîtrise des sous-traitant : le projet de certification de la CNIL

3 juillet 2025

> Agir en acteur de confiance pour un monde plus sûr, durable, et porteur de progrès partagés

Notre intervenant

Salomé THIBAUT
Manager Pôle Protection des Données

1

L’ENJEU DU CONTRÔLE DE SES SOUS-TRAITANTS : LA RESPONSABILITÉ

Impact sur la gestion des relations contractuelles

2

LA CERTIFICATION DES SOUS-TRAITANTS

Décryptage du projet de la CNIL

3

NOTRE ACCOMPAGNEMENT

Et si vous déléguiez cette évaluation à APAVE ?

Diagnostics, audit, formations…

4

QUESTIONS / RÉPONSES

Nos experts répondent à toutes vos questions !

1. L’enjeu du contrôle de ses sous-traitants : la responsabilité

Impact sur la gestion des relations contractuelles

Fournisseurs : quel statut au sens du RGPD ?

- **Fournisseurs** = définition opérationnelle pour indiquer un prestataire/entité qui fournit un service et avec qui une relation contractuelle existe.

- Au sens du RGPD, le statut de « fournisseur » n'existe pas. Un fournisseur peut donc être un **Responsable de traitement** ou un **Sous-traitant**. Cette différence de statut s'analyse sous l'angle des données personnelles éventuellement traitées par le fournisseur.

L’identification du sous-traitant

Responsable de Traitement

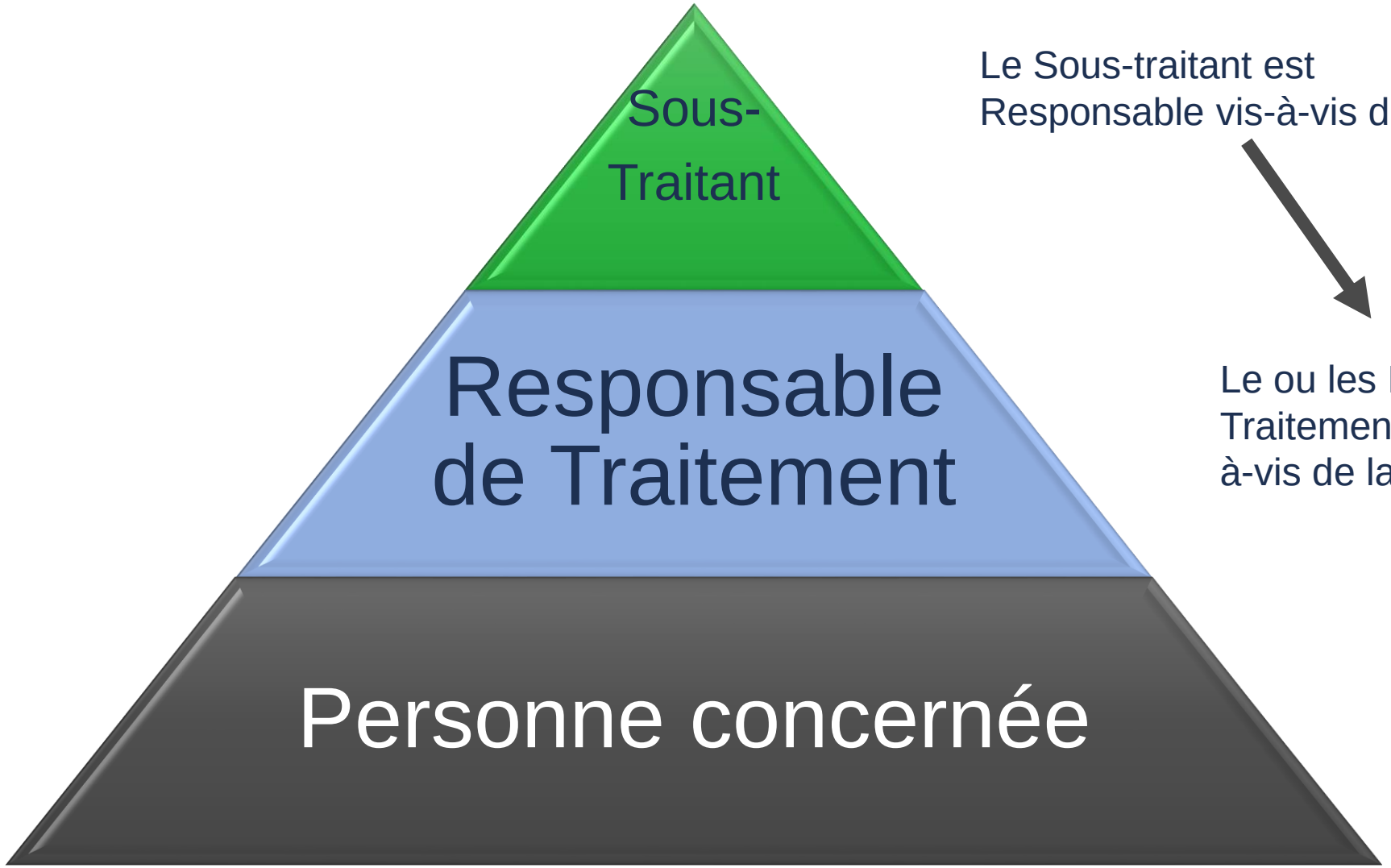
Traite les données pour son propre compte, à la maitrise des finalités et moyens

- *Il décide pourquoi et comment les données sont traitées*

Sous-traitant

Traite les données pour le compte et uniquement sur instructions du Responsable de Traitement

Une Responsabilité différente du fournisseur selon son statut



Le Sous-traitant est Responsable vis-à-vis du RT

Le ou les Responsables de Traitement sont Responsables vis-à-vis de la personne concernée

Sanctions CNIL

Conséquences

Le RT assume les conséquences d'une plainte des personnes concernées auprès de la CNIL

Le RT assume les conséquences juridiques éventuelles d'une violation de données, même lorsque celle-ci est causée par un ST : contrôle CNIL par exemple

Le RT peut se retourner contre son Sous-traitant pour non-respect de ses obligations

LE RT est responsable du choix de ses Sous-traitants vis-à-vis de la personne concernée

2. La certification des sous-traitants

Décryptage du projet de la CNIL

Faciliter l’obligation de vérification des sous-traitants du Responsable de traitement

La CNIL a mis en place un projet de référentiel qui liste les critères auxquels le sous-traitant doit démontrer sa conformité pour obtenir la certification

La certification permettra d’orienter les responsables de traitement dans le choix de leurs sous-traitants : elle assure que les traitements réalisés par le sous-traitant ont été évalués comme étant conformes aux critères du référentiel CNIL :
https://www.cnil.fr/sites/cnil/files/2024-12/projet_de_referentiel_certification_des_sous-traitants.pdf

Conditions de la certification

Tout sous-traitant situé en Europe

Par un organisme certificateur agréé

90 points de contrôles

CNIL.

Les points clés du référentiel

01

Contractualisation : contrat écrit, description du traitement, durée du contrat, clauses de sous-traitance, transparence sur les transferts hors UE, sur la sous-traitance ultérieure et les mesures de sécurité. Audits à intervalle réguliers et raisonnables, assistance du RT.

02

Préparation de l'environnement du traitement incluant les mesures de sécurité requises en annexe du référentiel : Registre, désignation d'un DPO, encadrement des transferts et de la sous-traitance ultérieure, référent certification, description des mesures de sécurité, procédures.

03

Mise en œuvre du traitement : instructions du RT, sensibilisation, formation, engagement de confidentialité, demandes de droits, notification des violations, audit technique de sécurité, registre des incidents.

04

Fin du traitement : choix du sort des données, confirmation de suppression.

Mise en place d'un Plan d'action pour la sécurité du traitement par le sous-traitant

Etablissement d'un plan d'action sur 3 ans

- **Recensement des mesures de sécurité prévues**
- **Priorisation**
- **Actualisation** tous les ans
- **Conservation du plan**

Etablissement d'un plan d'évaluation de la sous-traitance ultérieure

- Sur **3 ans**
- **Evaluation de l'ensemble des sous-traitants ultérieurs**
- **Priorisation**
- **Evaluation renforcée** pour au moins 1 des sous-traitants ultérieurs chaque année
- **Actualisation** tous les ans

Etablissement d'un plan d'amélioration de la prestation

- **identification et mise en œuvre des actions utiles** à l'amélioration de sa prestation ou de son offre de service en matière de protection des données.
- **Recueil des demandes d'amélioration**
- **Conservation** du plan pendant minimum 1 an
- **Veille juridique et technologique**

3. Notre accompagnement

Et si vous déléguiez cette évaluation à APAVE ?

Evaluation des fournisseurs

Assurez-vous que vos partenaires ne soient pas une porte d'entrée vers vos données !
Un accompagnement à la carte pour évaluer vos fournisseurs :

1

EVALUATION DES FOURNISSEURS

Diagnostic de cybersécurité et de la protection des données réalisé sur l'ensemble de vos fournisseurs, en se basant sur notre référentiel établi par nos experts.

En option :

- **Accompagnement à la sélection des fournisseurs.**
- **Intégration du référentiel spécifique de votre entreprise** dans cette évaluation.

2

RESTITUTION & BILAN

Bilan complet avec classement selon le niveau de sécurité de vos fournisseurs.

En option :

- **Cartographie des fournisseurs grâce à notre plateforme numérique** afin d'appréhender le niveau de risque global et identifier facilement les fournisseurs et prestataires les plus exposés.
- **Enrichissement de cette cartographie en intégrant le positionnement stratégique de chaque fournisseur dans la chaîne de valeur de votre entreprise**, afin d'identifier clairement les actions prioritaires à mener.

Evaluation des fournisseurs

3 niveaux d’analyse suivant la criticité de vos fournisseurs et 2 domaines : Cyber et RGPD

Déclaratif

Diagnostic simple

Analyse des pièces

Preuves de conformité analysées

Avec audit sur place

1 journée d’inspection sur site

Offre Cybersécurité du groupe Apave

OFFRE EVALUATION

- **Diagnostic Cybersécurité** *(1er année)*
- **Inspection de vos dispositifs de protection en Cybersécurité** *(années suivantes)*
- **Scan de vulnérabilité de votre site web** *(identification des principales failles de sécurité)*

OFFRE FORMATION

- **Formation des salariés aux bonnes pratiques en cybersécurité**

Formats disponibles : En présentiel, classe virtuelle ou e-Learning

- **Formation des dirigeants et des managers aux enjeux de la cybersécurité**

Formats disponibles : En présentiel, classe virtuelle ou e-Learning

- **Campagnes de phishing**

OFFRE CONSEIL

- **Accompagnement à la certification cybersécurité ISO 27001**
- **Accompagnement PCA & PRA** (rédaction, mise en œuvre…)
- **Accompagnement à la gestion de crise et communication** (rédaction, mise en œuvre…)

Offre Protection des Données

OFFRE EVALUATION :

- **Diagnostic Protection des données** *(1er année)*
- **Inspection de vos dispositifs de protection des données** *(les années suivantes)*
- **Audit de conformité RGPD site(s) web** *(option complémentaire)*

OFFRE FORMATIONS :

- **Formation des salariés aux bonnes pratiques RGPD**

Formats disponibles : En présentiel, classe virtuelle ou e-Learning

- **Formation des dirigeants et des managers aux enjeux de la protection des données** Formats disponibles : En présentiel, classe virtuelle ou e-Learning

OFFRE CONSEIL & ACCOMPAGNEMENT :

- **Externalisation de la fonction DPO**
- **Accompagnement à la mise conformité RGPD** *(pack de conformité RGPD)*
- **Accompagnement en cas de contrôle CNIL**

OFFRE CERTIFICATION :

- **Certification DPO**

Nous **contacter**

Laurent Zeitoun
Directrice offre Protection des Données
Laurent.zeitoun@apave.com

Pour toutes vos demandes :

www.apave.com