



**DATA
LEGAL
DRIVE**

x



CONFÉRENCE RGPD

Recours à la sous-traitance : comment lier respect du RGPD
et business opérationnel ?

PRÉSENTATION DE L'INTERVENANT



Thomas Vini Pires

Consultant RGPD



AU PROGRAMME DE LA CONFÉRENCE

1
Qualifier préalablement les
responsabilités avec
l'équipe projet

2
Sensibiliser et déléguer aux
équipes concernées

3
Adapter le Data Processing
Agreement à la réalité
opérationnelle

4
Anticiper les actions à
réaliser par les
opérationnels

1

QUALIFIER PRÉALABLEMENT

LES RESPONSABILITÉS AVEC L'ÉQUIPE PROJET

QUALIFIER PRÉALABLEMENT LES RESPONSABILITÉS DES PARTIES



Responsable du traitement

...**détermine** les finalités et les moyens du traitement...
Art. 4 (7) RGPD

« Exerce une influence déterminante sur le traitement de données »
guidelines EDPB 8/2022

Qui entreprend de réaliser le traitement ? A qui bénéficie le traitement ? Qui a fait appel à qui ?

Qui détermine pourquoi et comment ?
Qui détermine les moyens essentiels ?

Qui maîtrise les modalités du traitement ?
Qui a un degré d'instruction supérieur à l'autre ?

Qui a l'air d'être responsable aux yeux des personnes concernées ?



Sous-traitant

... traite des données **pour le compte** du responsable de traitement
Art. 4 (8) RGPD

N'effectue pas « le traitement pour sa ou ses propres finalités »
guidelines EDPB 8/2022

2

SENSIBILISER ET DÉLEGUER
AUX ÉQUIPES CONCERNÉES

RECOURS À LA SOUS-TRAITANCE

SENSIBILISER ET DÉLÉGUER AUX ÉQUIPES CONCERNÉES

Phase projet (*Privacy by Design*)

Phase contractuelle

ÉTAPE 1

Qualification des responsabilités des (futures) parties



Chef de Projet

ÉTAPE 2

Evaluation préalable du futur ST par RT



Acheteur ou Sales

ÉTAPE 3

Documentation des éléments d'évaluation préalable

ÉTAPE 4

Contractualisation incluant un *DPA* (*Data Processing Agreement*)



Acheteur ou Sales

ÉTAPE 5

Documentation (notamment dans le registre des traitements)



Chef de Projet

BONUS

Coopération dans l'exécution des traitements (et de la clause)

DPOs en support

3

ADAPTER LE DATA PROCESSING AGREEMENT À LA RÉALITÉ OPÉRATIONNELLE

ADAPTER LE DATA PROCESSING AGREEMENT À LA RÉALITÉ OPÉRATIONNELLE

Obligations des parties

- Respect des **instructions** du RT
- Aider le RT à démontrer sa **conformité** (fournir documentation, répondre à audit)
- Assister le RT (PIA, droits, violations de données, etc...)
- **Sensibiliser** / Former les équipes
- Prendre les mesures de **sécurité** nécessaires
- Assurer conformité des **sous-traitants ultérieurs** (STU)

Etc.

+

Description des traitements

- Décrire les rôles des parties
- Décrire des modalités du traitement (nature, objectifs, personnes concernées, données, durées, lieux de stockage, etc...)
- Lister les STU et destinataires éventuels, les éventuels transferts, ...
- **Documenter les instructions du Responsable de traitement** (ou définir de leur format)



Report des instructions aux équipes opérationnelles

Acheteurs ou Sales
Juristes

4

**ANTICIPER LES ACTIONS
OPÉRATIONNELLES À RÉALISER**

ANTICIPER LES ACTIONS OPÉRATIONNELLES À RÉALISER

Le ST doit **se préparer** à accompagner son RT en fonction de ses instructions



Alerte / Conseil

Si les instructions ne sont pas conformes aux exigences du RGPD



Accountability

Accompagner dans la démonstration de sa conformité (PIA, documentation, etc.)



Violations

Anticiper sa collaboration (délais et canaux d'avertissement, accompagnement, responsabilité de la notification, etc...)



Droits

Anticiper sa collaboration (délais et canaux d'avertissement du RT, processus de gestion de la demande, etc...)



Sécurité

Compléter les mesures de sécurité minimales avec les instructions du RT



STU

Avertir / obtenir l'autorisation de recours à des STU, et reporter les mêmes obligations



Conservation

Appliquer les mesures de **conservation** des données



Réversibilité

Retourner, supprimer, ou anonymiser les données à échéance



VOUS AVEZ DES QUESTIONS ?
ÉCHANGEONS !



Merci pour votre attention !



*Partagez ce moment
sur LinkedIn !*

