



Retrouvez nous sur
www.99-advisory.com

► Comment le DPO évalue-t-il les risques associés à un nouveau traitement de données ?

1/ Lancer un **nouveau traitement de données** personnelles

Qualification du traitement

- Nature
- Portée
- Contexte
- Finalités
- Enjeux

Contributions des parties prenantes

- DPO
- RSSI
- MOA
- CNIL

2/ Identifier les **caractéristiques du traitement**

Identification du type de données

- Données sensibles
- Données personnelles

Identification du traitement de données

- Innovant
- À grande échelle
- Méthode de scoring
- Etc.

3/ Estimer les **risques d'atteinte à la vie privée (DPIA)** 

Estimation des critères de risques

- *Vraisemblance* : estimation de la probabilité d'occurrence de l'évènement
- *Gravité* : conséquences pour la personne concernée

Estimation des impacts potentiels

- Impact sur la vie privée
- Impact sur les droits fondamentaux

4/ Déterminer les **mesures préventives** pour minimiser le risque

Mesures préconisées

- Information des personnes concernées
- Facilitation de l'exercice des droits d'accès pour les personnes concernées (rectification, effacement, etc.)

Précautions de traitement préconisées

- Anonymisation
- Chiffrement / contrôles d'accès



Qu'est-ce que le DPIA* ?

- **Outil** : Analyse d'impact fournie par la CNIL et disponible sur son site web
- **Responsable** : Responsable du traitement de données
- **Objectif** : évaluer l'impact sur la vie privée d'une collecte de données personnelles
- **Parties prenantes** : DPO, RSSI, MOA, la CNIL

Quelle est sa valeur ajoutée ?

- **Maitrise des risques** : estimer le risque d'atteinte à la vie privée et mettre en œuvre des actions préventives réduisant ce risque
- **Optimisation des coûts** : anticiper les contraintes et possibilités d'ajustements ex-ante
- **Traçabilité** : documenter les efforts réalisés pour se conformer à la réglementation

* *Data Privacy Impact Assessment*