



Le 3 octobre 2023

Formation en  
présentiel  
7 heures

Tarif : 60 000 XPF

## La gestion des violations de données personnelles

Un responsable de traitement ne peut plus détourner les yeux en cas d'incident de sécurité impactant les données personnelles qu'il traite et doit – dans certaines circonstances – notifier la violation de données à la CNIL, voire la communiquer aux « victimes ». Le rôle du DPO est ici crucial.

Quelles mesures prendre en amont pour éviter d'avoir à notifier une violation de données ? Comment détecter tous les incidents susceptibles d'être qualifiés de « violation » ? Et qui réalise cette qualification ? À partir de quand démarrent les « 72 heures » attendues par la CNIL pour réaliser la notification auprès d'elle ? Au final, qui prend la décision de notifier ? Comment décider s'il faut en plus communiquer la violation aux personnes concernées ? Et que leur dire ? Faut-il leur donner des précisions sur l'incident lui-même ? Faut-il s'excuser ? Et qui signe le courrier ? Que faut-il imposer aux sous-traitants à ce sujet ? Combien de temps maximum doit-on laisser à ses sous-traitants pour nous signaler un incident ? Comment tirer des enseignements utiles des violations pour en faire un levier de progrès ? Autant de questions cruciales auxquelles Bruno RASLE, expert reconnu et ancien DPO mutualisé de l'une des branches de la Sécurité sociale, répond lors de cette journée durant laquelle les aspects opérationnels sont privilégiés.

À l'issue d'une session très interactive, avec l'intense participation des apprenants, les participants repartent forts de toutes les connaissances leur permettant de maîtriser le sujet. De plus, l'intervenant partage des documents opérationnels qu'il a forgé dans le cadre de sa pratique professionnelle.

## Objectifs pédagogiques

- Mettre son organisme en situation de gérer des violations de données
- Être en mesure de formaliser une procédure de gestion des violations de données qui soit adaptée à son contexte
- Faire le lien entre la notification des violations de données, le Privacy by Design et les analyses d'impact
- Faire de la gestion des violations de données un levier en faveur de la mise en conformité de son organisme

## Organisation de la formation

### Public

- DPO et futurs DPO (internes, externes) ou équivalent
- Personnes accompagnant le DPO dans ses missions (adjoint, collaborateurs, relais...)
- Personnes amenées à piloter ou participer à une AIPD.

### Prérequis

- Cette formation convient à tout secteur et à toute taille d'entreprise / organisation, aucun prérequis n'est exigé.

### Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation

- Feuilles de présence.
- Questionnaires digitaux et études de cas concrets
- Formulaires d'évaluation de la formation.
- Certificat de réalisation de l'action de formation.

### Moyens pédagogiques et techniques

- Accueil des apprenants dans une salle dédiée à la formation.
- Documents supports de formation projetés.
- Exposés théoriques et étude de cas concrets et animation digital
- Mise à disposition en ligne de documents supports à la suite de la formation.



## Contenu de la formation

- **Ouverture de la formation par un tour de table**
  - Présentation de chacun des participants et de leurs entreprises
- **Module 1 : une violation de données, c'est quoi ?**
  - Définition
  - Genèse
  - Ce que prévoient les textes
  - Risque de sanctions
  - Mise en application : qualification de plusieurs exemples concrets d'incidents (violation ou pas ?)
- **Module 2 : comment gérer les violations de données**
  - Rôle et apports du DPD
  - Prévention
  - Signalement interne
  - Signalement externe
  - Détection

- Lien avec la procédure de gestion des incidents de sécurité
- Lien avec la procédure de gestion de crise
- Qualification pour notification à la CNIL
- Qualification pour communication aux personnes concernées
- En présence de sous-traitant, optimisation des clauses de sous-traitance
- Mise en application : rédaction d'une note de synthèse destinée au responsable de traitement à la suite d'une violation de données

- **Module 3 : notification et communication de la violation de données**

- Notification à la CNIL
- Pouvoirs et réactions de la CNIL
- Communication aux personnes concernées
- Maîtrise de la communication
- Gestion du temps
- Mises en application : rédaction d'une communication aux personnes concernées

- **Module 4 : Le plan d'action du DPO**

- Boucles de rétroaction
- Documentation des violations et indicateurs
- Retex
- Procédure de gestion des violations de données.
- Mise en application : débat concernant la procédure de gestion des violations de données « idéale »

## Notre intervenant

Bruno RASLE DPO, membre de l'AFCDP et

