



Formation « Gestion de violation de données », en 1 jour, par DMOuvrard

Version décembre 2025



Sommaire

Introduction	2
1. Édito	2
2. La formation	3
Durée :	3
Lieu	3
Profil des stagiaires	3
Objectifs professionnels	3
Méthodes pédagogiques	3
<i>En amont de la formation</i>	3
<i>Modèle ajustable et adapté en fonction des stagiaires</i>	3
<i>Méthodes pédagogiques générales</i>	4
<i>Distinction selon format</i>	4
<i>Documents fournis :</i>	4
<i>En aval de la formation</i>	4
Programme de la formation	4
Module 1 – Introduction et cadre légal	4
Module 2 – Détection d'une violation et qualification	4
Module 3 – Triage, escalade et registre interne	5
Module 4 – Analyse et remédiation technique	5
Module 5 – Notification et communication externe	5
Module 6 – Retour d'expérience et amélioration continue	5
Synthèse finale et évaluation	5

Introduction

1. Édito

Dans un environnement où les cyberattaques se multiplient, aucune organisation n'est à l'abri. La survenue d'une violation de données n'est plus une hypothèse lointaine mais une réalité opérationnelle : faut-il alerter la CNIL, prévenir les personnes concernées, comment documenter et prouver les actions menées ? Savoir répondre vite et bien n'est pas seulement une exigence réglementaire, c'est un enjeu de confiance vis-à-vis des clients, des partenaires et des autorités.

Ce que vous apporte la formation

Ce parcours vous donne des repères clairs et des outils immédiatement mobilisables pour détecter, qualifier, escalader et remédier à une violation. À l'issue de la formation, vous saurez appliquer les critères de notification, tenir un registre opérationnel, rédiger des notifications conformes et piloter une communication interne et externe maîtrisée. Les contenus sont conçus pour transformer la contrainte réglementaire en processus structuré : procédures, templates, grilles de qualification et scénarios de simulation vous permettront d'agir avec sérénité et d'objectiver vos décisions.

Ce que vous apporte le formateur

Animée par Mickaël Ouvrard, la formation s'appuie sur **8 années d'expertise en protection des données** et plus de **20 ans d'accompagnement des TPE/PME**. Le formateur apporte une pédagogie pragmatique : cas concrets, jeux de rôle, exercices et démonstrations techniques quand nécessaire. Chaque module est adapté aux spécificités des participants et de leur structure, pour garantir transférabilité et appropriation rapide des bonnes pratiques.

Pourquoi suivre ce parcours

Anticiper, c'est réduire l'impact. En vous préparant avant l'incident, vous gagnez en réactivité, en crédibilité et en capacité à limiter les conséquences juridiques et réputationnelles. Cette formation vise à faire de vos équipes des acteurs confiants et opérationnels, capables de transformer une crise potentielle en preuve de professionnalisme.

En conclusion

Aborder la gestion des violations de données avec méthode et outils concrets, c'est protéger vos personnes et préserver la confiance. Ce programme vous donne les moyens d'agir — calmement, efficacement et en conformité, pour que la sécurité des données devienne un avantage compétitif plutôt qu'un risque.

2. La formation

Durée :

1 jours de 7h (6h40 sans les pauses).

Lieu

En présentiel (dans vos locaux pour les formations Intra-entreprises) **ou en distanciel** en mode synchrone (stagiaires en visio). Le mode présentiel est privilégié pour plus d'interactivité et d'efficacité.

Pas de frais de déplacement en Eure et en Ile-de-France.

Profil des stagiaires

Tous profils. Aucune connaissance préalable sur le sujet de la protection des données personnelles n'est requise.

Cette formation cible plutôt les équipes opérationnelles.

Objectifs professionnels

- ✓ **Savoir qualifier une violation** et décider de la notification (autorité et personnes concernées).
- ✓ **Mettre en place un process opérationnel** (triage, escalade, registre, preuves).
- ✓ **Communiquer en interne et en externe** en conformité avec le RGPD.
- ✓ **Améliorer la gouvernance** via retours d'expérience et mesures correctives.

Méthodes pédagogiques

En amont de la formation

Envoi d'un questionnaire à chaque stagiaire pour évaluer ses connaissances, ses lacunes, ses besoins et ses pratiques en matière de RGPD, de sécurité des données et, surtout, en matière de gestion des violations.

Pour les formations Intra, nous prévoyons également **un échange gratuit de 30 minutes avec le représentant** de l'organisme (Direction, DRH ou direction/responsable des stagiaires), afin d'évaluer les pratiques et les besoins spécifiques de l'organisme concernant la gestion des incidents et des violations de données.

Modèle ajustable et adapté en fonction des stagiaires

Ces échanges et questionnaires permettront de **prendre en compte le profil spécifique des stagiaires** (leur niveau de connaissance, leurs pratiques actuelles, leurs besoins et attendus sur la formation) **et celui de leur organisme** (secteur spécifique, traitements particuliers, organisation spécifique).

La formation est adaptée : adaptation et sélection des cas pratiques, des exercices et des exemples les plus pertinents, ajustement de la durée des différents modules, ajout de focus spécifiques sur certains sujets, etc.

Méthodes pédagogiques générales

- ✓ **Une formation adaptée** aux stagiaires et à leur organisme.
- ✓ Une **alternance**, dans chaque module, **d'apports théoriques et d'exercices pratiques**.
- ✓ Des **mini-cours théoriques clairs et compréhensibles**, pour comprendre les enjeux et le contenu de la réglementation.
- ✓ Des cas pratiques réels adaptés aux stagiaires et à leur organisme **pour une mise en œuvre simple, rapide et efficace**.
- ✓ **Des ateliers pratiques** et collectifs, micro-quiz, jeux de rôle, travaux de groupe, mise en situation réelle, etc.
- ✓ **Des outils applicables dès le lendemain**.

Distinction selon format

- **Présentiel** : ce mode privilégie les ateliers pratiques et collectifs (atelier de cartographie des données, élaboration d'un plan d'action, etc.)
- **Distanciel** synchrone : sessions plus rythmées entre théorie et pratique (séquences plus courtes). Ce mode privilégie les exercices pratiques individuels.

Documents fournis :

- **Documents pédagogiques** : support de la formation, documents informatifs complémentaires, fiches pratiques et checklists, liens utiles (organismes, textes réglementaires, etc.), modèles de registre des violations, etc.
- **Documents administratifs** : attestation de formation, quiz d'évaluation des acquis en fin de formation + certificat de validation des acquis, questionnaire de satisfaction sur la formation.

En aval de la formation

Un suivi de la formation avec chaque stagiaire est prévu le mois suivant sa formation (+ un échange de 30 minutes avec le représentant de l'organisme pour les formations Intra) afin de répondre aux éventuelles questions, problématiques ou difficultés de mise en application.

Programme de la formation

Module 1 – Introduction et cadre légal

- **Durée** : 45 min
- **Contenu** : définitions, obligations articles 33–34 RGPD, sanctions.
- **Méthode** : exposé interactif, avec alternance théorie/exemples pratiques + quiz.

Module 2 – Détection d'une violation et qualification

- **Durée** : 1h

- **Contenu** : indicateurs d'incident, critères de violation, seuils de risque.
- **Méthode** : études de cas réels, atelier de qualification
- **Documentation** : template de grille de qualification.

Module 3 – Triage, escalade et registre interne

- **Durée** : 1h30
- **Contenu** : workflow d'escalade, rôles, tenue du registre des violations.
- **Méthode** : jeu de rôle.
- **Documentation** : procédure pas-à-pas + modèle de registre.

Module 4 – Analyse et remédiation technique

- **Durée** : 1h15
- **Contenu** : analyse des causes et origines, mesures techniques et preuves.
- **Méthode** : atelier technique + démonstration (si présentiel).
- **Documentation** : guide d'analyse et plan d'action.

Module 5 – Notification et communication externe

- **Durée** : 1h
- **Contenu** : rédaction notification CNIL, messages aux personnes concernées, médias.
- **Méthode** : rédaction guidée, jeux de rôle.
- **Documentation** : modèles prêts à l'emploi.

Module 6 – Retour d'expérience et amélioration continue

- **Durée** : 1h
- **Contenu** : KPIs, audit post-incident, mise à jour des procédures.
- **Méthode** : atelier de plan d'amélioration.
- **Documentation** : plan d'amélioration et feuille de route.

Synthèse finale et évaluation

- **Durée** : 20 min
- **Contenu** : synthèse rapide, discussion ouverte, Q/R, quiz final, évaluation de la formation à chaud.
- **Outils** : questionnaire de satisfaction, certificat de validation des acquis.