



# Formation « Devenir délégué à la protection des données (DPD/DPO) », en 3 jours, par DMOuvrard

Version décembre 2025



Mickaël OUVRARD EI – DMOuvrard  
5 rue du Stade, 78300 Poissy – FRANCE  
mickaelouvrard@dmouvrard.com - +336 79 71 28 28  
Entrepreneur Individuel - SIRET : 918 689 720 00012  
N° TVA Intracommunautaire : FR24918689720

# Sommaire

<b>Introduction</b>	<b>3</b>
<b>1. Édito</b>	<b>3</b>
<b>2. La formation</b>	<b>3</b>
Durée :	3
Lieu	3
Profil des stagiaires	3
Objectifs professionnels	4
Méthodes pédagogiques	4
<i>En amont de la formation</i>	4
<i>Modèle ajustable et adapté en fonction des stagiaires</i>	4
<i>Méthodes pédagogiques générales</i>	4
<i>Distinction selon format</i>	4
<i>Documents fournis :</i>	5
<i>En aval de la formation</i>	5
Programme de la formation	5
<b>Jour 1 :</b>	<b>5</b>
<i>Module 1 - Introduction à la protection des données et au RGPD</i>	5
<i>Module 2 - Les grands principes du RGPD et de la protection des données personnelles</i>	5
<i>Module 3 - Les grandes étapes d'une mise en conformité au RGPD</i>	6
<i>Module 4 - Documentation de la conformité RGPD</i>	6
<i>Module 5 - Désignation d'un pilote RGPD</i>	6
<i>Module 6 - Cartographie et registre des traitements</i>	6
<i>Synthèse de la journée</i>	6
<b>Jour 2 :</b>	<b>7</b>
<i>Module 7 - La sous-traitance et le RGPD</i>	7
<i>Module 8 - Transfert de données hors UE</i>	7
<i>Module 9 - Contrôle CNIL</i>	7
<i>Module 10 - Sécurité et confidentialité des données</i>	7
<i>Synthèse de la journée</i>	8
<b>Jour 3 :</b>	<b>8</b>
<i>Module 11 - Violations de données</i>	8
<i>Module 12 - Gestion et analyse des risques, AIPD/PIA</i>	8
<i>Module 13 - La montée en compétence</i>	9
<i>Module 14 - PCA (Plan de Continuité d'Activité) et PRA (Plan de Reprise d'Activité)</i>	9
<i>Module 15 - Conclusion + questionnaires</i>	9

# Introduction

## 1. Édito

Dans un monde où les données sont au cœur des activités, disposer d'un **Délégué à la protection des données (DPO)** n'est plus une option mais devient une nécessité pour tout organisme soucieux de sa conformité et de sa réputation. Devenir ou être le DPO de son organisme, c'est être le pivot opérationnel et stratégique de son organisation et c'est accepter d'en être le garant de la confiance numérique.

D'ailleurs, le Règlement Général sur la Protection des Données (RGPD) n'est pas seulement une obligation légale : c'est aussi un cadre indispensable pour instaurer la confiance, sécuriser les pratiques et garantir le respect des droits de chacun.

Fort de 8 années d'expertise en protection des données et de plus de 20 ans d'expérience auprès de TPE et PME, Mickaël Ouvrard, activateur France Num, accompagne les organismes avec des formations conçues pour être stimulantes, concrètes, utiles et engageantes. Chaque module est pensé sur mesure, afin de répondre aux spécificités des stagiaires et de leur établissement, afin que cette contrainte réglementaire soit abordée avec sérénité et devienne un véritable levier de confiance.

## 2. La formation

Durée :

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

Les trois jours peuvent être consécutifs mais nous recommandons, afin d'améliorer l'assimilation des notions et la mise en pratique réelle, de les séparer.

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

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

Profil de poste concerné :

- DPO désigné ou en cours de désignation, relais ou référents protection des données.
- Toute personne dont la mission est d'assurer le respect de la protection des données personnelles au sein de son organisation, publique ou privée.

## Objectifs professionnels

- **Acquérir les connaissances indispensables** à l'accomplissement de la mission de DPO
- Connaitre **les bonnes pratiques** pour mettre en place un processus de mise en conformité RGPD
- Acquérir les connaissances et la pratique **pour jouer un rôle de conseil** sur tout nouveau projet de traitement
- **Savoir mettre en place les outils** de communication et de sensibilisation
- Connaitre **les points essentiels de contrôle**

## 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 et de sécurité des données.

**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.

### *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 en matière de protection des données personnelles, leurs besoins et attendus sur la formation) **et celui de leur organisme** (secteur spécifique, traitements particuliers).

**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 (cybersécurité, transfert de données hors UE, préparation à un contrôle CNIL, etc.), liens utiles (organismes, textes réglementaires, etc.), grille d'évaluation de maturité RGPD ou cybersécurité, modèles de cartographies et de registres, plan d'action opérationnel, 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

### Jour 1 :

#### Module 1 – Introduction à la protection des données et au RGPD

- **Durée** : 30 min
- **Contenu** : historique de la protection des données et principaux textes français et européens, présentation générale du RGPD (qui, quoi, etc.), de ses principaux concepts (donnée personnelle, traitement de données personnelles, Responsable de traitement / Sous-traitant / Co-responsable de traitement, des risques de non-conformité et des avantages de sa mise en place)
- **Méthode** : exposé interactif, avec alternance théorie/exemples pratiques, étude de mini-cas de jurisprudence, quiz illustratif et corrigé
- **Documentation** : textes législatifs (lien et/ou document)

#### Module 2 – Les grands principes du RGPD et de la protection des données personnelles

- **Durée** : 2h30
- **Contenu** : les grands principes (licéité, loyauté et transparence, limitation, minimisation et exactitude des données, limitation de la conservation, intégrité et confidentialité), fondement juridique (les 6 bases légales), focus sur le consentement, cas spécifiques et autres principes du RGPD, transparence (mentions d'information, cookies) et droits des personnes (présentation des droits, focus sur le droit d'accès)
- **Méthode** : étude de cas simple, mise en situation réelle, mini-quiz
- **Documentation** : modèles de mentions d'information, tableau récapitulatif des droits des personnes, diagrammes d'interprétation et de réponse à une demande de droit d'accès, fiches pratiques, exemple de demande de consentement

### *Module 3 – Les grandes étapes d'une mise en conformité au RGPD*

- **Durée** : 0h20
- **Contenu** : présentation des grandes étapes de la mise en conformité RGPD selon la méthode proposée par la CNIL (désignation d'un pilote, cartographie des traitements, priorisation des actions, gestion des risques, organisation des processus internes), en détaillant les principales actions à mener et les documents de conformité associés
- **Méthode** : exposé interactif, déroulé de la méthode

### *Module 4 – Documentation de la conformité RGPD*

- **Durée** : 0h20
- **Contenu** : présentation de la documentation de conformité RGPD : l'ensemble des documents présents dans le dossier conformité RGPD selon la CNIL, et les autres documents possibles
- **Documentation** : registres, document de suivi des demandes d'exercice de droits, modèles de documents, de contrats, etc.

### *Module 5 – Désignation d'un pilote RGPD*

- **Durée** : 0h50
- **Contenu** : le pilote RGPD (qui, pourquoi, responsabilités) et le DPO (statut, profil et compétences, désignation, publication, missions et responsabilités, moyens)
- **Méthode** : jeu de rôle, étude de cas (conflit d'intérêt ?), échange en groupe, quiz
- **Documentation** : fiche de poste et lettre de mission du DPO, checklist pour désignation d'un DPO

### *Module 6 – Cartographie et registre des traitements*

- **Durée** : 2h
- **Contenu** : présentation de la cartographie des données et des traitements de données (méthode de travail, flux de données, etc.) + atelier, présentation des registres de traitements (comme responsable de traitements et comme sous-traitant) + atelier
- **Méthode** : atelier participatif de cartographie collective des flux puis atelier d'élaboration d'une fiche de traitement
- **Documentation** : modèle et exemple de cartographie des données, modèles de registre des traitements

### *Synthèse de la journée*

- **Durée** : 10 min
- **Format** : synthèse rapide, discussion ouverte, Q/R.

## **Jour 2 :**

### *Module 7 - La sous-traitance et le RGPD*

- **Durée** : 1h
- **Contenu** : les obligations du sous-traitant (transparence et traçabilité, sécurité des données traitées, assistance et conseil, appel à sous-traitant ultérieur, etc.), contrats et clauses obligatoires, partage des responsabilités, cartographie des sous-traitants et co-traitants
- **Méthode** : analyse de contrat type, atelier de rédaction de clauses, simulation d'audit de sous-traitant
- **Documentation** : contrats/clauses type, questionnaire d'audit de cybersécurité et de conformité RGPD des sous-traitants

### *Module 8 - Transfert de données hors UE*

- **Durée** : 1h30
- **Contenu** : les principes en matière de transfert de données hors UE et d'encadrement des transferts de données, décisions d'adéquation avec focus sur certains pays (G-B, Etats-Unis, etc.), clauses contractuelles types, cas particuliers (Cloud, USA, prestataires tiers), présentation de l'AITD (Analyse d'Impact sur les Transferts de Données) et méthode d'élaboration de l'AITD.
- **Méthode** : étude de cas pratiques (transfert vers un prestataire américain), prise en main du modèle d'AITD, mini-quiz
- **Documentation** : fiches pratiques, modèle d'AITD.

### *Module 9 - Contrôle CNIL*

- **Durée** : 1h
- **Contenu** : focus sur la CNIL (missions, pouvoirs, collège) et sur les contrôles de la CNIL (fonctionnement d'un contrôle, procédure de sanction, etc.), préparation à un contrôle de la CNIL (pourquoi et comment se préparer)
- **Méthode** : atelier de réflexion de préparation d'un contrôle, exercice de mise en situation
- **Documentation** : diagrammes de fonctionnement d'un contrôle et de la procédure de sanction

### *Module 10 - Sécurité et confidentialité des données*

- **Durée** : 3h
- **Contenu** : Sécurité du traitement (article 32), types de menaces, mesures de sécurité techniques, organisationnelles et juridiques, les bonnes pratiques en 12 fiches conseils de sécurisation de son informatique, que faire en cas d'incident, méthodes de chiffrement et d'anonymisation et pseudonymisation des données, audits de sécurité, cartographie du SI
- **Méthode** : sensibilisation par l'expérience, simulation de cyberattaques
- **Documentation** : checklist sécurité, grille d'évaluation du niveau de sécurité des données au sein de son organisme

### *Synthèse de la journée*

- **Durée** : 10 min
- **Format** : synthèse rapide, discussion ouverte, Q/R.

### **Jour 3 :**

#### *Module 11 – Violations de données*

- **Durée** : 1h15
- **Contenu** : définition et typologie de violations, exemples, documentation et procédure de notification, retour d'expérience
- **Méthode** : jeu de rôle « crise RGPD », mise en situation dynamique, exercice d'évaluation de la gravité et du besoin de notification, exercice de rédaction de procédure
- **Documentation** : registre des incidents et violations de données

#### *Module 12 – Gestion et analyse des risques, AIPD/PIA*

- **Durée** : 1h30
- **Contenu** :
  - gestion et analyse des risques, en 4 étapes : recensement, des traitements, appréciation des risques (estimation de la gravité et de la vraisemblance des risques), mise en œuvre des mesures et vérification, audits périodiques
  - AIPD (Analyse d'Impact relative à la Protection des Données) ou DPIA/PIA (Data Protection Impact Assessment) : définition et méthodologie d'une AIPD, critères de réalisation, échelle et règle pour estimer la gravité et la vraisemblance
- **Méthode** : études de cas pour estimer gravité et vraisemblance, mini-quiz sur les critères, atelier de co-construction de parties d'AIPD, prise en main de l'outil « pia »
- **Documentation** : tableaux d'échelle et règle pour estimer la gravité et la vraisemblance, modèle d'AIPD, « outil pia » de la CNIL

### *Module 13 – La montée en compétence*

- **Durée** : 1h
- **Contenu** : montée en compétence du DPO (développement de ses compétences clés) et de l'ensemble de l'organisme en protection des données personnelles, gouvernance RGPD et organisation interne, amélioration des process
- **Méthode** : exercices de mise en situation (organisation RGPD), atelier de co-construction d'un plan de sensibilisation et de formation
- **Documentation** : plan de formation et de sensibilisation, liste d'indicateurs de suivi de la protection des données personnelles au sein de l'organisme

### *Module 14 – PCA (Plan de Continuité d'Activité) et PRA (Plan de Reprise d'Activité)*

- **Durée** : 1h15
- **Contenu** : Différence entre PCA et PRA, présentation du PCA (Plan de Continuité d'Activité) et importance de la continuité des activités, présentation du PRA (Plan de Reprise d'Activité) et importance de la reprise d'activité
- **Méthode** : prise en main d'un modèle de PCA et de PRA
- **Documentation** : modèles de PCA et de PRA

### *Module 15 – Conclusion + questionnaires*

- **Durée** : 1h45
- **Contenu** : retour sur quelques points spécifiques, quelques liens utiles + test de validation des acquis + questionnaire de satisfaction de la formation
- **Méthode** : focus sur quelques points précis, discussion ouverte, Q/R, quiz final et questionnaire sur la formation
- **Documentation** : modèle d'audit RGPD et de plan d'action.