

# Projet co réseau Nexem et partenaires – Occuper la fonction de Délégué à la Protection des Données (Dpd) en ESMS

## Fiche technique

### Secteurs

Tous secteurs

### Public

Délégué à la protection des Données ou futur DPD identifié dans le "Club DPD Régional NEXEM ET SES PARTENAIRES"

### Durée

9 jours

### Organisme de formation

☞ FORMAT différence

### Date limite d'inscription

31/03/2020

### Lieux & dates

#### ☞ Groupe 1

#### Nice - 2020

Les 29 & 30 avr. 2020

+ Le 12 mai 2020

+ Le 9 juin 2020

+ Le 25 mai 2020

+ Le 16 juin 2020

+ Le 23 juin 2020

+ Les 29 & 30 juin 2020

+ Les 19 & 20 oct. 2020

### Interlocuteur Opcos Santé

**Afida MEYSTRE**

[afida.meystre@unifaf.fr](mailto:afida.meystre@unifaf.fr)

04 91 14 05 42

### Interlocuteur OF

**Madié DIAKITE**

[madie.diakite@formatdifference.org](mailto:madie.diakite@formatdifference.org)

[e.org](http://e.org)

05 61 00 71 78

## Contexte

La donnée est désormais devenue critique et sa protection est un impératif absolu. Le RGPD (Règlement Général de la Protection des Données) est entré en vigueur le 25 mai dernier sur tout le territoire de l'Union Européenne.

Un peu plus de 4 mois après la mise en application du RGPD, la CNIL recensait déjà à plus de 740 violations de données déclarées dont 65% étaient liées à des causes externes et actes de malveillances (piratages).

En s'emparant de la question, les professionnels des ESSMS prennent de plus en plus conscience de l'enjeu qu'il y a à mettre en place une gestion sécurisée leurs données :

- ☞ inter-dépendance qui existe entre les systèmes d'information des traitements de données,
- ☞ renforcement de la garantie de l'effectivité du respect des droits fondamentaux des usagers,
- ☞ respect du droit à l'information,
- ☞ respect du consentement préalable de la personne accompagnée,
- ☞ protection de la vie privée, etc.

Cela est d'autant plus critique que le RGPD s'applique à tous les supports de données personnelles... Papiers comme numériques : toutes les formes de stockage de l'information sont concernés.

Chaque jour, les ESSMS collectent, traitent, partagent et stockent de nombreuses données à caractère personnel (nom, prénom, date de naissance, adresse, données électroniques, numéro d'identification, origine culturelle, sociale ou économique, données judiciaires, données de santé.) sous formats papier et numérique.

Nous sommes à l'heure de la généralisation du dossier patient informatisé (DPI) et du dossier médical partagé (DMP), du Projet Personnalisé d'Accompagnement (PPA) Informatisé et chacun se doit d'être extrêmement vigilant.

Avec le RGPD, protéger les données personnelles des résidents, des mineurs, des salariés devient un enjeu majeur.

## Objectifs

À l'issue de la formation les participants seront à même de :

- ☞ Valider les compétences et connaissances nécessaires à la conduite de leur mission de DPD/DPO
- ☞ Positionner sa mission dans la gouvernance de l'information de l'établissement

- ⇒ Assister la direction dans la mise en oeuvre, le maintien et les bonnes pratiques qui mènent à la conformité au RGPD
- ⇒ Analyser l'organisation de l'établissement et en ressortir la cartographie des données personnelles
- ⇒ Bâti ou mettre en conformité le plan de gestion de l'archivage
- ⇒ Réaliser les registres (registre d'activités de traitement, du registre des catégories d'activités de traitement et du registre des violations de données) et toute la documentation de mise en conformité.
- ⇒ Faire appliquer par l'établissement les nouveaux droits acquis des citoyens Européens en matière de protection des données.
- ⇒ Auditer ou faire auditer les bonnes pratiques informatiques
- ⇒ Se présenter à la certification CNIL
- ⇒ Procéder à des REX du DPO en ESMS

### Prérequis

- ⇒ Avoir suivi une formation de sensibilisation d'au moins 14 heures
- ⇒ Etre en capacité de se repérer dans des textes juridiques ciblés métiers.
- ⇒ Avoir une culture informatique fonctionnelle, et connaître les grands principes d'un réseau, de l'internet
- ⇒ Avoir des capacités ou qualités en matière de diplomatie et d'ouverture sur la co-traitance et sous-traitance.
- ⇒ Savoir travailler en mode projet

### Contenu

#### JOUR 1 – Présentiel

- ⇒ Etude du règlement no 2016/679 et des règlements liés.
- ⇒ Présentation des associations et groupements de DPD/DPO
- ⇒ Les rôles, les missions du DPO. Organisation, en mode projet et diplomatie.
- ⇒ Référentiel de certification du DPD, enjeux, établissements de certification.

#### Jour 2 – Présentiel

- ⇒ La boîte à outils du DPO, Organisation du quotidien, la GED, les outils d'analyses, les méthodes.
- ⇒ Les registres de traitements – Outil libre PIA de la CNIL pour l'analyse d'impact (AIPD). méthodologie, l'éventuelle sous-traitance, les mesures techniques et organisationnelles à adopter

#### JOUR 3 – 1er demi-journée WEBINAR

- ⇒ JURIDIQUE : principes de licéité du traitement, identifier la base juridique d'un traitement, réglementation sectorielle qui fixe des conditions spécifiques au traitement de données (Code de santé), cadre juridique relatif à la sous-traitance.

#### JOUR 3 – 2eme demi-journée WEBINAR

- ⇒ Gestion des relations fournisseurs et sous-traitants évaluation et contractualisation.

#### JOUR 4 – Présentiel

- ⇒ PILOTER LES ACTEURS DE LA MAINTENANCE ET DU DEVELOPPEMENT INFORMATIQUE : identifier des mesures de protection des données dès la conception et par défaut

adaptées aux risques et à la nature des opérations de traitement

⇒ SENSIBILISER ADHESION : formation et de sensibilisation du personnel et des instances dirigeantes en matière de protection des données, communication et plan d'actions

#### **JOUR 5 – 1er demi-journée WEBINAR**

⇒ ARCHIVAGE : La gouvernance, les délais, la procédure, la destruction maîtrisée, les nouveaux modes d'archives numériques sécurisées

#### **JOUR 5 – 2eme demi-journée WEBINAR**

⇒ JURIDIQUE Information requise et procédures d'exercice des droits des personnes concernées. Transfert de données hors UE et instruments juridiques

#### **JOURS 6 et 7 – Présentiel**

⇒ AGIR – REAGIR : Procédure de gestion de la violation des données – ACCOUNTABILITY : registre d'activités de traitement, du registre des catégories d'activités de traitement et du registre des violations de données ainsi que de la documentation nécessaire pour prouver la conformité à la réglementation en matière de protection des données

⇒ Tableau de bord et audits en matière de protection des données

⇒ Recommandations pour le passage de la certification CNIL

#### **INTERSESSION**

#### **JOURS 8 et 9 – Présentiel**

⇒ Réalité de terrain : Confrontation de la représentation à l'aune de l'application. Les principaux questionnements issus des premières applications des acquis sur le terrain  
Le positionnement de la missions et les activités au regard de la hiérarchie / au regard des équipes

⇒ Travail en sous-groupe : Retour d'expérience sur la place du DPO en ESMS. Débriefing et débat, apports conceptuels, réajustements

⇒ Le positionnement d'une nouvelle fonction en ESMS ; intégration au secteur

⇒ Cartographie des missions, de la fonction, repérage des pratiques les plus efficaces au regard des situations rencontrées sur le terrain

⇒ Modéliser la fonction de DPD en ESMS : quels outils ? quelles techniques ? quels points de vigilance ?

⇒ Cartographie des outils associés aux missions du DPO

#### **PLANIFICATION =**

#### **NICE**

#### **Présentiel**

jour 1 = 29/04/2020

jour 2 = 30/04/2020

#### **web 1 (juridique)**

0.5 j (9h30-13h) = 12/05/2020

#### **web 2 (fournisseurs)**

0.5 j (9h30-13h) = 09/06/2020

#### **Présentiel**

jour 3 = 25/05/2020

**web 3 (archivage)**

0.5 j (9h30-13h) = 16/06/2020

**web 4 (juridique)**

0.5 j (9h30-13h) = 23/06/2020

**Présentiel**

jour 4 = 29/06/2020

jour 5 = 30/06/2020

**intersession 2/3 mois**

**Présentiel**

jour 6 = 19/10/2020

jour 7 = 20/10/2020