

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Délégué à la protection des données (DPO)

RNCP41460 · Certification RNCP · Niveau 7

Ce parcours de 440 heures prépare au titre RNCP41460 « Délégué à la protection des données (DPO) » de niveau 7 et couvre ses quatre blocs de compétences : conformité et gouvernance, sécurité des systèmes d'information, gestion des risques et des crises, formation et sensibilisation. Le fil rouge suit une DPO nouvellement nommée dans une entreprise de santé numérique, et chaque compétence du référentiel France Compétences est ainsi mobilisée dans des situations professionnelles réalistes.

VOLUME HORAIRE	COURS	BLOCS
440 h	20	4

01 · PRÉSENTATION

La formation en bref

Intitulé	Délégué à la protection des données (DPO)
Code	RNCP41460
Type	Certification RNCP
Niveau	Niveau 7
Certificateur	DORANCO ESPACE MULTIMEDIA
Durée	440 h, 20 cours
Modalité	Formation à distance (e-learning), tutorat assuré par l'organisme de formation
Formats	SCORM 1.2 / 2004, xAPI, sources éditables
Mise à jour	Novembre 2026
Fin d'enregistrement de la certification	27/10/2028

Le métier et les compétences visées

Le délégué à la protection des données (DPO) veille à la conformité de son organisation au RGPD, à la loi Informatique et Libertés et aux exigences sectorielles. Il cartographie les traitements, tient le registre et audite les pratiques. Il encadre les contrats avec les sous-traitants et les transferts hors Union européenne. Il conçoit la politique de gouvernance des données et organise la gestion des consentements et des droits des personnes. Avec le RSSI, il supervise la sécurité des systèmes d'information, conduit les analyses d'impact et pilote la gestion des crises. Interlocuteur de la CNIL, il conseille la direction, présente des indicateurs au COMEX et diffuse une culture de la protection des données par la communication, la sensibilisation et la formation des équipes.

Public visé

- Juristes souhaitant se spécialiser dans la protection des données personnelles
- Professionnels de l'informatique (chefs de projet, administrateurs, consultants SI) évoluant vers une fonction conformité
- Correspondants RGPD, référents conformité ou DPO désignés souhaitant faire certifier leurs compétences
- Responsables qualité, compliance officers ou auditeurs internes intégrant la dimension données personnelles
- Consultants indépendants souhaitant proposer une offre de DPO externalisé

Prérequis

- Être titulaire d'une certification professionnelle ou d'un diplôme de niveau 6
- Ou être titulaire d'une certification ou d'un diplôme de niveau 5 et justifier d'au moins un an d'expérience dans l'informatique ou le droit
- Disposer d'un poste informatique avec connexion internet et maîtriser les outils bureautiques courants

Objectifs pédagogiques

À l'issue du parcours, l'apprenant est capable de :

- Cartographier les traitements de données personnelles d'une organisation et établir un diagnostic de conformité hiérarchisé
- Créer et maintenir un registre des traitements complet, intégrant les spécificités technologiques et métiers
- Auditer les contrats de sous-traitance et sécuriser les transferts de données hors Union européenne
- Concevoir une politique de gouvernance des données, des protocoles de consentement et un processus de gestion des droits des personnes accessibles à tous les publics
- Gérer les échanges avec la CNIL lors d'un contrôle ou d'une demande d'information
- Intégrer les principes de Privacy by Design et Privacy by Default dans les projets et piloter la conformité par des indicateurs
- Superviser, en collaboration avec le RSSI, les audits de sécurité, les mesures techniques de protection et la réponse aux incidents
- Conduire une analyse d'impact relative à la protection des données (AIPD) et prioriser les risques selon une méthodologie reconnue
- Concevoir et coordonner un protocole de gestion de crise et en tirer les enseignements
- Élaborer et déployer une stratégie de communication, de sensibilisation et de formation RGPD inclusive

02 · FIL ROUGE PÉDAGOGIQUE

Medelys Services

CV

Claire Vasseur

Juriste d'entreprise nommée Déléguée à la protection des données

Santé numérique et e-commerce de dispositifs médicaux connectés

Medelys Services est une entreprise française de taille intermédiaire qui exploite une plateforme de prise de rendez-vous médicaux, un service de téléconsultation et une boutique en ligne de dispositifs de santé connectés (tensiomètres, balances, capteurs de sommeil). Elle traite des données de santé de patients, des données de praticiens, des données clients issues du e-commerce et les données RH de ses collaborateurs répartis sur trois sites. Son hébergement repose en partie sur un prestataire dont le support technique est situé hors de l'Union européenne, et un projet d'outil d'aide au tri des demandes de téléconsultation fondé sur un algorithme d'apprentissage automatique est en cours. À la suite d'un audit externe pointant des lacunes, la direction générale nomme Claire Vasseur, juriste de l'entreprise, DPO avec pour mission de structurer toute la démarche de conformité.

Chaque cours se termine par une mise en situation dans cette entreprise : l'apprenant accompagne Claire dans des situations professionnelles réalistes, de plus en plus complexes, jusqu'à la préparation des épreuves.

La progression

1. Bloc 1 : Claire cartographie les traitements de Medelys, réalise le diagnostic de conformité, reconstruit le registre, renégocie les contrats des sous-traitants, encadre les transferts hors UE et prépare l'entreprise à une demande d'information de la CNIL.
2. Bloc 2 : Claire installe, avec le RSSI Karim Benali, un cadre de gouvernance Privacy by Design pour le projet d'algorithme de tri, construit un tableau de bord présenté au COMEX, supervise un audit ISO 27001 et traite ses premiers incidents de sécurité.
3. Bloc 3 : Claire conduit l'AIPD de la téléconsultation et des objets connectés, priorise les risques avec EBIOS Risk Manager, pilote un plan d'actions correctives puis coordonne la gestion d'une crise réelle de rançongiciel touchant un site.
4. Bloc 4 : Claire mobilise un réseau de relais RGPD, déploie une campagne de communication et de sensibilisation accessible, puis conçoit et anime un programme de formation adapté à chaque métier de Medelys.

03 · ARCHITECTURE

Organisation du parcours

Le parcours est construit sur les blocs de compétences du référentiel officiel : chaque bloc regroupe les cours qui préparent à son évaluation.

N°	Bloc et cours	Durée
RNCP41460BC01 · Auditer et élaborer la politique de conformité et de gouvernance des données		**132 h**
1	Cadre réglementaire, posture du DPO et cartographie des traitements	22 h
2	Évaluer la conformité et produire un rapport de diagnostic	22 h
3	Créer et maintenir le registre des traitements	22 h
4	Encadrer les contrats avec les sous-traitants et les transferts hors UE	22 h
5	Concevoir la politique de gouvernance et la gestion des consentements	22 h
6	Gérer les droits des personnes et les relations avec la CNIL	22 h
RNCP41460BC02 · Superviser la sécurité des données et des systèmes d'information		**110 h**
7	Cartographier les acteurs et intégrer la Privacy by Design	22 h
8	Piloter la conformité et la sécurité par les indicateurs	22 h
9	Superviser un audit de sécurité et de conformité et en exploiter les résultats	22 h
10	Superviser les mesures techniques de sécurité avec le RSSI	22 h
11	Surveiller les cybermenaces et évaluer les incidents de sécurité	22 h
RNCP41460BC03 · Gérer les risques et les crises liés aux traitements de données		**110 h**
12	Conduire une analyse d'impact relative à la protection des données	22 h
13	Cartographier les risques et évaluer les vulnérabilités technologiques	22 h
14	Prioriser les risques avec une méthodologie reconnue	22 h
15	Définir et superviser un plan d'actions correctives	22 h
16	Concevoir, coordonner et évaluer la gestion de crise	22 h
RNCP41460BC04 · Former et sensibiliser les parties prenantes aux enjeux de protection des données		**88 h**
17	Coordonner les parties prenantes et capitaliser sur les retours d'expérience	22 h
18	Élaborer et piloter la stratégie de communication RGPD	22 h
19	Concevoir et déployer des campagnes de sensibilisation	22 h
20	Concevoir et animer des formations à la protection des données	22 h
Total du parcours		**440 h**

Répartition des modalités pédagogiques

Chaque sous-chapitre s'ouvre sur une vidéo de 3 à 5 minutes. La vidéo représente 30 % du volume horaire, complétée par du cours texte enrichi, des infographies, des études de cas, des mises en situation et des QCM.



- Vidéos : 132 h
- Cours texte et infographies : 138 h 30
- Études de cas et mises en situation : 108 h
- QCM et évaluations : 61 h 30

Contenu des cours

RNCP41460BC01 · 132 h

Auditer et élaborer la politique de conformité et de gouvernance des données

Cours 1 · Cadre réglementaire, posture du DPO et cartographie des traitements

22 h

OBJECTIFS

- Maîtriser le cadre juridique applicable (RGPD, loi Informatique et Libertés, loi du 20 juin 2018) et les missions du DPO
- Cartographier les traitements, les flux et les acteurs en classifiant les données selon leur sensibilité
- Identifier les enjeux de conformité sectoriels (santé, finance, e-commerce)

ÉVALUATION FORMATIVE

QCM de validation des notions juridiques et exercice de cartographie des flux corrigé

CONTENUS

- Le RGPD et la loi Informatique et Libertés : architecture, notions clés et champ d'application
- Missions, positionnement, indépendance et responsabilités du DPO
- Les principes fondamentaux : licéité, loyauté, transparence, minimisation, limitation de la conservation
- Méthodes de recensement des traitements et entretiens avec les métiers
- Classification des données : données courantes, sensibles, de santé, relatives aux infractions
- Modélisation des flux de données et identification des acteurs (responsable de traitement, sous-traitant, responsable conjoint)
- Exigences sectorielles : hébergement de données de santé, secteur financier, e-commerce

Fil rouge · Claire prend ses fonctions chez Medelys Services et rencontre les directions métiers pour dresser la première cartographie des traitements, en distinguant les données de santé de la téléconsultation des données clients de la boutique en ligne.

Cours 2 · Évaluer la conformité et produire un rapport de diagnostic

22 h

OBJECTIFS

- Analyser les écarts entre les pratiques existantes et les obligations légales et sectorielles
- Qualifier les non-conformités et prioriser leur gravité, y compris pour les technologies émergentes
- Rédiger un rapport de diagnostic hiérarchisé assorti de recommandations

ÉVALUATION FORMATIVE

Étude de cas écrite : rédaction d'un extrait de rapport de diagnostic hiérarchisé

CONTENUS

- Méthodologie d'audit de conformité RGPD : référentiels, grilles et preuves
- Analyse des bases légales et des finalités des traitements
- Traitements liés aux technologies émergentes : IA, objets connectés, biométrie
- Qualification des non-conformités et échelles de gravité
- Hiérarchisation des risques juridiques, opérationnels et réputationnels
- Structure et rédaction d'un rapport de diagnostic
- Formulation de recommandations et feuille de route de mise en conformité

Fil rouge · À partir de la cartographie, Claire audite les traitements de Medelys, constate notamment l'absence de base légale documentée pour le suivi des objets connectés et présente son rapport de diagnostic à la direction générale.

Cours 3 · Créer et maintenir le registre des traitements

22 h

OBJECTIFS

- Élaborer des fiches de traitement détaillées en collaboration avec les responsables métiers
- Consolider les informations exigées par l'article 30 du RGPD et intégrer les spécificités technologiques

ÉVALUATION FORMATIVE

Exercice pratique : rédaction de trois fiches de registre à partir d'un dossier métier

CONTENUS

- Obligations relatives au registre : responsable de traitement et sous-traitant
- Contenu d'une fiche de traitement : finalités, catégories de données et de personnes, destinataires, durées, mesures de sécurité
- Conduite des entretiens de collecte avec les métiers
- Intégration des spécificités technologiques : algorithmes d'IA, protocoles IoT, API
- Outils de gestion du registre et choix d'un format exploitable
- Gouvernance du registre : mise à jour, versioning et traçabilité
- Articulation du registre avec les autres éléments de documentation de la conformité

Fil rouge · Claire reconstruit le registre de Medelys avec la directrice produit et le responsable RH, en documentant précisément les traitements liés aux capteurs de sommeil connectés et au futur algorithme de tri.

Cours 4 · Encadrer les contrats avec les sous-traitants et les transferts hors UE

22 h

OBJECTIFS

- Auditer les contrats avec les sous-traitants et partenaires au regard de l'article 28 du RGPD
- Mettre en œuvre les mécanismes juridiques d'encadrement des transferts hors Union européenne et en assurer le suivi

ÉVALUATION FORMATIVE

Analyse critique d'un contrat de sous-traitance et quiz sur les mécanismes de transfert

CONTENUS

- Qualification des relations : sous-traitance, responsabilité conjointe, partenariat
- Clauses obligatoires et clauses de protection des données : traitement, stockage, partage, sous-traitance ultérieure
- Processus d'audit contractuel et questionnaires d'évaluation des prestataires
- Cadre juridique des transferts : décisions d'adéquation, garanties appropriées, dérogations
- Clauses contractuelles types et Binding Corporate Rules
- Évaluation de l'impact des transferts et mesures supplémentaires
- Suivi des obligations et revue périodique des transferts

Fil rouge · Claire découvre que le support technique de l'hébergeur de Medelys accède aux données depuis un pays tiers : elle audite le contrat, négocie un avenant et met en place les clauses contractuelles types accompagnées d'une évaluation du transfert.

Cours 5 · Concevoir la politique de gouvernance et la gestion des consentements

22 h

OBJECTIFS

- Concevoir une politique de gouvernance et ses documents opérationnels avec les départements métiers
- Concevoir des protocoles de gestion des consentements intégrant preuve, révocation et accessibilité

ÉVALUATION FORMATIVE

Production commentée d'un extrait de politique de conservation et d'un parcours de consentement

CONTENUS

- Architecture d'une politique de gouvernance des données personnelles
- Politique de conservation des données et référentiels de durées
- Politique de confidentialité et information des personnes
- Charte RGPD et règles internes à destination des collaborateurs
- Le consentement : conditions de validité et articulation avec les autres bases légales
- Mécanismes de preuve (horodatage, journalisation) et de révocation (interface dédiée, suppression automatisée)
- Accessibilité et compréhension des parcours de consentement pour tous les publics, y compris les personnes en situation de handicap

Fil rouge · Claire coordonne avec le juridique, l'IT et le marketing la rédaction de la politique de conservation de Medelys et refond le recueil du consentement de la boutique en ligne pour le rendre traçable et compatible avec les lecteurs d'écran.

Cours 6 · Gérer les droits des personnes et les relations avec la CNIL

22 h

OBJECTIFS

- Mettre en place un processus structuré et accessible de gestion des demandes d'exercice des droits
- Définir les indicateurs de suivi des demandes
- Gérer les échanges avec la CNIL lors d'un contrôle ou d'une demande d'information

ÉVALUATION FORMATIVE

Jeu de rôle d'entretien avec un contrôleur CNIL et QCM sur les droits des personnes

CONTENUS

- Panorama des droits des personnes : accès, rectification, effacement, opposition, limitation, portabilité
- Conception d'un processus de traitement des demandes et délais réglementaires
- Workflows automatisés et système de ticketing
- Accessibilité des démarches pour tous les publics, notamment les personnes en situation de handicap
- Indicateurs de suivi : délais de réponse, taux de résolution, motifs de refus
- Pouvoirs de la CNIL, procédures de contrôle et de sanction
- Préparation d'un contrôle : constitution du dossier de preuves et coordination interne

Fil rouge · Une patiente saisit la CNIL après une demande d'accès restée sans réponse : Claire organise la réponse à la demande d'information de l'autorité, puis déploie un processus de ticketing pour toutes les demandes de droits.

RNCP41460BC02 · 110 h

Superviser la sécurité des données et des systèmes d'information

Cours 7 · Cartographier les acteurs et intégrer la Privacy by Design

22 h

OBJECTIFS

- Cartographier les acteurs internes et externes et leurs responsabilités dans la gestion des données
- Définir avec les équipes IT et juridiques un cadre de gouvernance intégrant Privacy by Design et Privacy by Default

ÉVALUATION FORMATIVE

Exercice de construction d'une matrice RACI et étude de cas Privacy by Design

CONTENUS

- Identification des parties prenantes : direction, RSSI, DSI, métiers, sous-traitants, partenaires
- Matrices de responsabilités (RACI) appliquées à la protection des données
- Principes de Privacy by Design et Privacy by Default (article 25 du RGPD)
- Intégration de la protection des données dans la gestion de projet
- Cas d'application : déploiement d'un SIRH, application métier, solution d'IA
- Jalons de revue de conformité et critères de validation projet

Fil rouge · Claire construit la matrice des responsabilités de Medelys et impose, avec le RSSI Karim Benali, des revues de conformité à chaque étape du projet d'algorithme de tri des téléconsultations.

Cours 8 · Piloter la conformité et la sécurité par les indicateurs

22 h

OBJECTIFS

- Définir et suivre des KPI de gouvernance et de sécurité au moyen de tableaux de bord
- Présenter les résultats aux parties prenantes internes et externes en formulant des analyses stratégiques

ÉVALUATION FORMATIVE

Conception d'un tableau de bord et présentation enregistrée de cinq minutes

CONTENUS

- Choix des indicateurs : résilience aux cybermenaces, conformité des sous-traitants, délais de traitement des droits
- Collecte, fiabilité et fréquence de mise à jour des données d'indicateurs
- Conception d'un tableau de bord de conformité
- Analyse des écarts et actions d'optimisation
- Restitution au COMEX, aux directions métiers et aux partenaires
- Argumentation pour prioriser les investissements en sécurité

Fil rouge · Claire conçoit le tableau de bord trimestriel de Medelys et présente au COMEX une analyse qui justifie le financement d'un renforcement de la gestion des accès.

Cours 9 · Superviser un audit de sécurité et de conformité et en exploiter les résultats

22 h

OBJECTIFS

- Définir le périmètre et les exigences réglementaires d'un audit des systèmes d'information
- Analyser les écarts identifiés et veiller à la mise en œuvre des mesures correctives

ÉVALUATION FORMATIVE

Étude de cas écrite : analyse d'un rapport d'audit et priorisation des écarts

CONTENUS

- Typologie des audits : organisationnel, technique, test d'intrusion, audit de configuration
- Référentiels mobilisables : RGPD, ISO 27001, ISO 27002
- Rédaction d'un cahier des charges et définition du périmètre
- Pilotage d'un auditeur externe et suivi des travaux
- Lecture et analyse d'un rapport d'audit
- Transformation des constats en plan de remédiation suivi

Fil rouge · Claire cadre avec Karim un audit ISO 27001 de la plateforme de téléconsultation, puis analyse le rapport et s'assure que chaque écart impactant les données de patients reçoit une mesure corrective datée.

Cours 10 · Superviser les mesures techniques de sécurité avec le RSSI

22 h

OBJECTIFS

- Comprendre et superviser l'application des mesures techniques de protection des données
- S'appuyer sur les standards ISO 27001, ANSSI et NIST pour garantir une conformité continue

ÉVALUATION FORMATIVE

Quiz technique et grille d'évaluation des mesures de sécurité à compléter

CONTENUS

- Panorama des standards : ISO 27001, guide d'hygiène informatique de l'ANSSI, cadre NIST
- Chiffrement des données au repos et en transit
- Gestion des identités, segmentation et revue des accès
- Tests de vulnérabilité et gestion des correctifs
- Sauvegardes, journalisation et traçabilité
- Répartition des rôles entre DPO et RSSI et modalités de collaboration

Fil rouge · Claire et Karim vérifient ensemble que les données des objets connectés sont chiffrées et que les accès des prestataires de maintenance sont segmentés et revus régulièrement.

Cours 11 · Surveiller les cybermenaces et évaluer les incidents de sécurité

22 h

OBJECTIFS

- Organiser avec le RSSI une veille sur les menaces émergentes et exploiter les outils de détection
- Évaluer les incidents signalés et superviser les plans de réponse

ÉVALUATION FORMATIVE

Étude de cas : qualification de trois incidents et décision argumentée de notification

CONTENUS

- Panorama des cybermenaces : rançongiciels, hameçonnage, fuites de données, attaques sur la chaîne d'approvisionnement
- Outils de détection : SIEM, EDR et centres opérationnels de sécurité
- Organisation d'une veille active et sources institutionnelles
- Qualification d'un incident et notion de violation de données personnelles
- Registre des violations et critères de notification à l'autorité et aux personnes
- Supervision des plans de réponse et mesures de prévention des récidives

Fil rouge · Une alerte de l'EDR signale un accès anormal à une base de rendez-vous : Claire qualifie l'incident avec Karim, décide de son inscription au registre des violations et suit les mesures correctives.

RNCP41460BC03 · 110 h

Gérer les risques et les crises liés aux traitements de données

Cours 12 · Conduire une analyse d'impact relative à la protection des données

22 h

OBJECTIFS

- Évaluer au préalable les impacts des traitements sensibles ou à risque sur les droits et libertés et les classer par gravité
- Définir des mesures adaptées : pseudonymisation, anonymisation, contrôle des accès

ÉVALUATION FORMATIVE

Exercice pratique : réalisation d'une AIPD simplifiée sur un cas fourni

CONTENUS

- Critères rendant l'AIPD obligatoire et listes publiées par la CNIL
- Méthodologie d'AIPD : description, nécessité, proportionnalité, risques
- Évaluation de la gravité et de la vraisemblance des risques pour les personnes
- Pseudonymisation et anonymisation : différences et techniques
- Renforcement des contrôles d'accès et autres mesures de réduction
- Consultation préalable de l'autorité et suivi de l'AIPD dans le temps

Fil rouge · Claire conduit l'AIPD du service de téléconsultation et propose la pseudonymisation des données transmises à l'algorithme de tri pour réduire le risque résiduel.

Cours 13 · Cartographier les risques et évaluer les vulnérabilités technologiques

22 h

OBJECTIFS

- Cartographier les risques selon leur typologie et leur origine interne ou externe
- Évaluer les vulnérabilités des technologies utilisées (IA, IoT, API) et leurs impacts sur les droits des personnes

ÉVALUATION FORMATIVE

Élaboration d'une cartographie des risques et QCM sur les vulnérabilités technologiques

CONTENUS

- Typologie des risques : financiers, juridiques, réputationnels, opérationnels
- Origines internes : erreurs humaines, falsification, pratiques non conformes
- Origines externes : extorsion de données, hameçonnage, intrusion
- Vulnérabilités des systèmes d'IA : biais, fuite de données d'entraînement, opacité
- Vulnérabilités des objets connectés et des API
- Construction d'une cartographie des risques exploitable

Fil rouge · Claire cartographie les risques des tensiomètres connectés vendus par Medelys et identifie une API mal protégée exposant potentiellement les mesures des clients.

Cours 14 · Prioriser les risques avec une méthodologie reconnue

22 h

OBJECTIFS

- Appliquer EBIOS Risk Manager et ISO 27005 pour évaluer la criticité des risques
- Orienter les actions de remédiation selon la criticité et les enjeux de conformité

ÉVALUATION FORMATIVE

Étude de cas écrite : priorisation de scénarios de risque argumentée

CONTENUS

- Principes de la gestion des risques et vocabulaire commun
- La méthode EBIOS Risk Manager : ateliers et livrables
- La norme ISO 27005 et son articulation avec ISO 27001
- Matrices de criticité et seuils d'acceptation
- Articulation entre risques pour l'organisation et risques pour les personnes
- Restitution de la priorisation aux décideurs

Fil rouge · Claire anime avec Karim et la direction produit les ateliers EBIOS Risk Manager consacrés à la plateforme de rendez-vous et fait valider la priorisation des scénarios par la direction.

Cours 15 · Définir et superviser un plan d'actions correctives

22 h

OBJECTIFS

- Définir des mesures organisationnelles et techniques adaptées aux risques identifiés
- Coordonner leur mise en œuvre avec jalons et échéanciers, évaluer leur efficacité et ajuster

ÉVALUATION FORMATIVE

Rédaction d'un plan d'actions correctives et analyse d'un tableau de suivi

CONTENUS

- Construction d'un plan d'actions : mesures, responsables, ressources, échéances
- Équilibre entre mesures organisationnelles et techniques
- Coordination avec les équipes IT et métiers
- Jalons, échéanciers et outils de suivi
- Évaluation de l'efficacité des mesures et indicateurs de résultat
- Ajustement du plan et gestion des écarts

Fil rouge · Claire formalise le plan d'actions issu des ateliers, puis suit son avancement en comité mensuel et réoriente les priorités lorsque la sécurisation de l'API prend du retard.

Cours 16 · Concevoir, coordonner et évaluer la gestion de crise

22 h

OBJECTIFS

- Concevoir un protocole de crise avec niveaux d'alerte et modalités de signalement accessibles
- Coordonner les actions en crise et la communication avec la CNIL et les personnes concernées
- Évaluer les réponses apportées et améliorer les protocoles

ÉVALUATION FORMATIVE

Simulation de crise en jeu de rôle et rédaction d'une notification de violation

CONTENUS

- Architecture d'un protocole de gestion de crise et définition des niveaux d'alerte
- Cellule de crise : rôles, circuits de décision et de signalement
- Notification à la CNIL dans les 72 heures et communication aux personnes concernées
- Communication accessible : langage simplifié, supports adaptés, personnes en difficulté numérique
- Coordination des actions correctives avec l'IT, le juridique et les métiers
- Retour d'expérience post-crise et mise à jour des protocoles
- Exercices de crise : conception et animation

Fil rouge · Un rançongiciel paralyse le site logistique de Medelys : Claire active la cellule de crise, notifie la CNIL, informe les clients en langage simplifié et conduit ensuite le retour d'expérience.

RNCP41460BC04 · 88 h

Former et sensibiliser les parties prenantes aux enjeux de protection des données

Cours 17 · Coordonner les parties prenantes et capitaliser sur les retours d'expérience

22 h

OBJECTIFS

- Mobiliser les parties prenantes internes et assurer le suivi des actions RGPD
- Analyser les retours d'expérience avec les métiers pour adapter les politiques de conformité

ÉVALUATION FORMATIVE

Étude de cas : plan d'animation d'un réseau de relais et synthèse de retour d'expérience

CONTENUS

- Constitution et animation d'un réseau de relais RGPD
- Organisation des échanges interservices et des comités de conformité
- Outils de suivi collaboratif des actions
- Leviers d'engagement et gestion des résistances
- Méthodes de retour d'expérience et identification des bonnes pratiques
- Adaptation des politiques et procédures aux réalités opérationnelles

Fil rouge · Claire crée un réseau de relais RGPD dans chaque direction de Medelys et organise un retour d'expérience sur la gestion des demandes de droits avec le service client.

Cours 18 · Élaborer et piloter la stratégie de communication RGPD

22 h

OBJECTIFS

- Définir objectifs et messages clés pour les publics internes et externes
- Superviser une diffusion multicanale accessible et évaluer son efficacité

ÉVALUATION FORMATIVE

Production d'un plan de communication et d'une grille d'indicateurs

CONTENUS

- Diagnostic de communication et définition des publics : collaborateurs, clients, partenaires
- Objectifs, messages clés et plan de communication
- Choix des canaux : intranet, newsletters, plateformes collaboratives, webinars
- Accessibilité numérique : sous-titrage, langage simplifié, compatibilité lecteurs d'écran
- Indicateurs quantitatifs et qualitatifs : participation, retours, engagement
- Ajustement des campagnes et capitalisation

Fil rouge · Claire bâtit le plan de communication annuel de Medelys, publie une page de transparence destinée aux patients et analyse les retours des collaborateurs pour ajuster les messages.

Cours 19 · Concevoir et déployer des campagnes de sensibilisation

22 h

OBJECTIFS

- Concevoir des supports de sensibilisation adaptés aux différents publics, y compris les personnes en situation de handicap
- Coordonner le déploiement des campagnes et en mesurer l'impact

ÉVALUATION FORMATIVE

Conception d'un support de sensibilisation accessible et de son plan de déploiement

CONTENUS

- Analyse des publics internes : RH, marketing, IT, service client
- Formats de sensibilisation : affiches, vidéos, guides pratiques, microlearning
- Messages sur les cybermenaces et les bons réflexes
- Conception accessible des supports et respect des référentiels d'accessibilité
- Planification et coordination du déploiement : intranet, newsletters, événements
- Mesure de l'impact : indicateurs de diffusion et d'engagement

Fil rouge · Après la crise de rançongiciel, Claire déploie une campagne contre l'hameçonnage avec des supports adaptés à chaque service et une version audio pour un collaborateur malvoyant.

Cours 20 · Concevoir et animer des formations à la protection des données

22 h

OBJECTIFS

- Analyser les besoins de formation par métier
- Concevoir des modules gradués et inclusifs intégrant des études de cas
- Animer des sessions avec des méthodes pédagogiques actives

ÉVALUATION FORMATIVE

Animation filmée d'une séquence de formation et grille d'auto-évaluation

CONTENUS

- Analyse des besoins de compétences par métier : juridique, technique, opérationnel
- Ingénierie de formation : objectifs, niveaux initiation, perfectionnement et expertise
- Conception d'études de cas et de scénarios métiers
- Adaptation des modules aux personnes en situation de handicap
- Méthodes d'animation : ateliers pratiques, quiz, jeux de rôle
- Évaluation des acquis et amélioration continue des formations
- Préparation du projet professionnel et de la soutenance

Fil rouge · Claire conçoit un parcours de formation à trois niveaux pour Medelys et anime un atelier en jeu de rôle avec les conseillers du service client sur le traitement d'une demande d'effacement.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

Correspondance entre les compétences du référentiel France Compétences et les cours du parcours.

Compétence	Bloc	Cours
Cartographier les traitements, les flux et les acteurs et classifier les données selon leur sensibilité	RNCP41460BC01	1, 3
Évaluer la conformité des traitements existants, y compris liés aux technologies émergentes	RNCP41460BC01	2
Produire un rapport de diagnostic hiérarchisant les risques et formulant des recommandations	RNCP41460BC01	2
Créer ou mettre à jour les registres des traitements	RNCP41460BC01	3
Analyser les contrats avec les sous-traitants et partenaires externes	RNCP41460BC01	4
Gérer les transferts de données hors Union européenne	RNCP41460BC01	4
Concevoir une politique de gouvernance des données personnelles	RNCP41460BC01	5
Concevoir des protocoles de gestion des consentements et des préférences	RNCP41460BC01	5
Mettre en place un processus de gestion des demandes d'exercice des droits	RNCP41460BC01	6
Gérer les échanges avec la CNIL lors d'un contrôle ou d'une demande d'information	RNCP41460BC01	6
Cartographier les acteurs internes et externes et leurs responsabilités	RNCP41460BC02	7
Définir un cadre de gouvernance intégrant Privacy by Design et Privacy by Default	RNCP41460BC02	7
Suivre les politiques de gouvernance et de sécurité par des KPI et tableaux de bord	RNCP41460BC02	8
Présenter les résultats des KPI aux parties prenantes internes et externes	RNCP41460BC02	8
Superviser un audit de sécurité et de conformité des systèmes d'information	RNCP41460BC02	9
Exploiter les résultats d'un audit de sécurité et de conformité	RNCP41460BC02	9
Superviser l'application des mesures techniques de sécurité avec le RSSI	RNCP41460BC02	10
Surveiller l'évolution des cybermenaces avec le RSSI	RNCP41460BC02	11
Évaluer les incidents de sécurité signalés et superviser les plans de réponse	RNCP41460BC02	11
Évaluer au préalable les impacts des traitements sensibles ou à risque	RNCP41460BC03	12
Définir des mesures correctives adaptées aux analyses d'impact	RNCP41460BC03	12
Cartographier les risques selon leur typologie et leur origine	RNCP41460BC03	13
Évaluer les vulnérabilités des technologies utilisées (IA, IoT, API)	RNCP41460BC03	13
Prioriser les risques selon une méthodologie d'évaluation (EBIOS RM, ISO 27005)	RNCP41460BC03	14

Définir un plan d'actions correctives organisationnelles et techniques	RNCP41460BC03	15
Superviser la mise en œuvre des mesures correctives et en évaluer l'efficacité	RNCP41460BC03	15
Concevoir des protocoles de gestion des crises accessibles	RNCP41460BC03	16
Coordonner les actions correctives en situation de crise	RNCP41460BC03	16
Évaluer les réponses apportées lors d'une crise	RNCP41460BC03	16
Coordonner la mise en œuvre des actions RGPD avec les parties prenantes internes	RNCP41460BC04	17
Analyser les retours d'expérience sur les actions RGPD	RNCP41460BC04	17
Élaborer une stratégie de communication sur les enjeux et actions RGPD	RNCP41460BC04	18
Superviser la diffusion accessible des messages RGPD	RNCP41460BC04	18
Évaluer l'efficacité des actions de communication	RNCP41460BC04	18
Concevoir des supports et outils de sensibilisation adaptés aux publics	RNCP41460BC04	19
Coordonner le déploiement des campagnes de sensibilisation internes	RNCP41460BC04	19
Analyser les besoins de formation en protection des données	RNCP41460BC04	20
Concevoir des modules de formation adaptés aux niveaux des collaborateurs	RNCP41460BC04	20
Animer des sessions de formation inclusives sur la protection des données	RNCP41460BC04	20

Évaluations formatives

Chaque sous-chapitre se conclut par un QCM d'auto-positionnement avec correction commentée, et chaque cours comporte une évaluation formative en lien avec sa mise en situation : étude de cas écrite, production de livrables professionnels (fiches de registre, rapport de diagnostic, AIPD, plan d'actions, plan de communication), jeux de rôle ou présentations enregistrées. Ces activités permettent à l'apprenant de mesurer sa progression, et elles fournissent au formateur de l'organisme de formation des éléments objectifs de suivi des acquis, exploitables dans le cadre de la démarche qualité.

Modalités de certification

Bloc	Modalité d'évaluation
RNCP41460BC01	Études de cas faisant l'objet d'une épreuve écrite
RNCP41460BC02	Études de cas faisant l'objet d'une épreuve écrite
RNCP41460BC03	Études de cas faisant l'objet d'une épreuve écrite et mise en situation professionnelle
RNCP41460BC04	Projet professionnel présenté lors d'une soutenance orale devant un jury

Le parcours reproduit le format des épreuves officielles : les blocs 1 et 2 multiplient les études de cas écrites fondées sur le fil rouge Medelys Services, avec livrables à produire dans un temps contraint. Le bloc 3 combine études de cas et simulations, dont une simulation de crise en jeu de rôle préparant à la mise en situation professionnelle. Le bloc 4 accompagne progressivement la construction du projet professionnel, de l'analyse des besoins à l'animation filmée d'une séquence de formation, et prépare à la

soutenance orale. L'organisme de formation reste seul responsable de l'inscription des candidats et de l'organisation de la certification auprès du certificateur.

06 · MOYENS ET PERSPECTIVES

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche accessible 24 h/24, avec suivi de progression et traçabilité des connexions
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire, sous-titrée pour l'accessibilité
- Cours textes enrichis, infographies et fiches de synthèse téléchargeables représentant 70 % du volume horaire avec les activités
- Études de cas et mises en situation fondées sur le fil rouge Medelys Services
- Modèles professionnels prêts à l'emploi : fiche de registre, grille d'audit, trame d'AIPD, protocole de crise, plan de communication
- QCM interactifs corrigés à chaque sous-chapitre et évaluations formatives par cours
- Contenus conçus selon les principes d'accessibilité numérique (compatibilité lecteurs d'écran, contrastes, transcriptions)

Débouchés et évolutions

- Délégué ou déléguée à la protection des données (Data Protection Officer)
- Chargé de mission protection des données ou chargé de mission RGPD
- Consultant DPO ou consultant RGPD
- Compliance officer spécialisé en protection des données
- Juriste DPO ou juriste protection des données personnelles
- Auditeur ou auditrice en sécurité des systèmes d'information, RSSI avec mission DPO

Accessibilité

Contenus sous-titrés en français, contrastes conformes WCAG AA, navigation au clavier sur les écrans interactifs. L'organisme de formation qui diffuse le parcours adapte les modalités d'accompagnement aux personnes en situation de handicap avec son référent handicap.

Livrables fournis à l'organisme de formation

- Package SCORM 1.2 / 2004 et xAPI, compatible avec les principaux LMS
- Sources éditables des cours, scripts vidéo et banques de QCM
- Livret apprenant et grilles d'évaluation
- Licence marque blanche à vie, stagiaires illimités, maintenance 24 mois

School For Mate
On crée vos formations, vous n'avez plus qu'à les diffuser.

contact@schoolformate.com · catalogue-2026-sfm.netlify.app

Référentiel RNCP41460 consulté sur francecompetences.fr (export officiel du 4 novembre 2026). La délivrance de la certification relève exclusivement du certificateur et de l'organisme de formation habilité. Document non contractuel, susceptible d'évoluer avec le référentiel.