Lefebvre Dalloz
Compétences.

Tél.: 01 83 10 10 10
src-formation@lefebvre-dalloz.fr
formation.lefebvre-dalloz.fr

Parcours Délégué à la protection des données personnelles (DPO/DPD)

Certification Lefebvre Dalloz enregistré auprès de France Compétences (RS5524)

Code	Durée	Tarif Inter*
600579	5 jours	4 193 € HT

Repas inclus (en présentiel)

PROCHAINES SESSIONS

- **A DISTANCE, PARIS :**
  7 oct. au 20 déc. 2024

Voir toutes les sessions

PUBLIC

Délégués à la protection des données (DPO/DPD) - Directeurs de services informatiques (DSI) - Avocats - Juristes - Toute personne s'intéressant à l'économie de la data et/ou en charge de la conformité de traitements de données personnelles

PRÉ-REQUIS

Aucun prérequis nécessaire

LES POINTS FORTS

Approche métier sur les différents aspects du DPO et suivant les critères requis par l'autorité de contrôle (CNIL) - Présentation d'outils d'aide à la gestion du traitement des données personnelles

MOYENS PÉDAGOGIQUES

- Dispositif de formation structuré autour du transfert des compétences
- Acquisition des compétences opérationnelles par la pratique et l'expérimentation
- Apprentissage collaboratif lors des moments synchrones
- Parcours d'apprentissage en plusieurs temps pour permettre engagement, apprentissage et transfert
- Formation favorisant l'engagement du participant pour un meilleur ancrage des enseignements

SATISFACTION ET EVALUATION

Le parcours fera l'objet d'une évaluation des compétences donnant lieu à la délivrance d'un certificat Lefebvre-Dalloz - évaluation facultative (sauf pour les participants bénéficiant d'un financement CPF) - suivant les modalités ci-

Objectifs pédagogiques

- Déterminer les règles du pilotage de la protection des données personnelles de l'entreprise
- Monter et suivre un programme de conformité en matière de données personnelles
- Évaluer les risques numériques et repérer les failles de sécurité
- Gérer les contrôles de la CNIL

Programme de la formation

Protection des données personnelles : mise en conformité (1 jour)
Voir le moduleRéduire

Déterminer les obligations techniques et organisationnelles des entités concernées par le RGPD

Rappeler le champ d'application, les objectifs et les enjeux du RGPD

- Origine de la directive 95-46 et de la loi Informatique et Libertés et philosophie du RGPD
- Critères d'application territoriale et personnelle
- Acteurs et responsabilités : coresponsabilité des clients et prestataires
- Débat : quel impact de la suppression des formalités et autorisations par la création du "Guichet unique"

Définir les concepts et principes du RGPD

- Notion de donnée, traitement, finalité, base légale, responsable de traitement, sous-traitant, destinataire, profilage, etc.)
- Principes de licéité/loyauté de la collecte, limitation des finalités, minimisation/exactitude et conservation limitée des données, confidentialité, proportionnalité, responsabilité, transparence, et sécurité des traitements...
- Cas particulier du profilage (eprivacy) et de la prise de décision algorithmique
- Eprivacy : spécificités des données de communications électroniques, cookie consent
- Exercice pratique : identifier les données personnelles directes et indirectes

Identifier les contraintes techniques et organisationnelles

après : présentation d'un projet professionnel démontrant l'acquisition des compétences attendues d'un délégué à la protection des données (Durée de l'épreuve : 30 minutes de soutenance orale)

- Cartographie des traitements, durées de conservation, finalités aux bases légales
- Implémentation et documentation des exigences « Privacy by Design » et mesures de sécurité logistique/physique (pseudonymisation, certifications, plan d'assurance sécurité)
- Gestion d'une violation de données personnelles
- Adoption d'une gouvernance interne et sensibilisation des équipes
- Procédures de conformité : gestion des demandes des droits, des violations de données et des AIDP et communiquer auprès des personnes concernées

- Cas pratique : constituer sa documentation d'accontability

Définir le rôle pour le délégué à la protection des données (DPD/DPO)

Repérer les raisons de nommer un DPO

- Prévenir les risques et sanctions : amendes/CA, actions des personnes concernées, condamnation et préjudices
- Fonction quasi-obligatoire dans l'entreprise

- Débat : quel intérêt de nommer un DPO ?

Mesurer les fonctions du DPO dans l'entreprise

- Tenir le registre
- Limiter les mises en cause de responsabilité
- Expliquer ses missions

- Partage d'expériences : le rôle du DPO

Cerner les oblications juridiques

Repérer les obligations juridiques

- Constitution et suivi du registre des traitements
- Conception et déploiement des mentions d'information et modalités de recueil des consentements des personnes

- Cas pratique : comment instruire des demandes d'exercice des droits des personnes concernées ?

Gérer la conformité RGPD sur le plan contractuel

- Qualification des protagonistes et vérification des responsabilités
- « Roadmap » de mise en conformité des contrats
- Clauses et annexes du RGPD

- Exercice pratique : qualifier les protagonistes des relations complexes et en cerner les conséquences

Caractériser les spécificités du traitement des données

Analyser les flux transfrontaliers de données

- « BCR », clauses contractuelles types
- Conventions de flux complémentaires

- Débat : Privacy Shield et conséquences du nouvel accord pour le transfert de données entre l'Union européenne et les États-Unis

Utiliser les fichiers Marketing

- Respect du RGPD dans le cadre des prospections commerciales
- Respect du RGPD dans le cadre des locations ou cessions de fichiers

- Check-list : procédure d'utilisation du fichier Marketing

DPO (DPD) : désignation, rôle et missions du délégué à la protection des données personnelles (1 jour)
Voir le moduleRéduire

Définir le rôle du DPO dans l'entreprise

Déceler l'origine du DPO : accountability et fin des déclarations préalables

- Accountability : philosophie de la conformité dynamique et responsabilisation des acteurs (responsable du traitement et sous-traitant)
- Conséquence immédiate : fin des déclarations préalables à la CNIL
- Principaux outils de la conformité dynamique : analyse d'impact à la protection des données (AIPD)

- Quiz : les principes de mise en conformité de la protection des données personnelles

Expliquer le rôle du DPO

- Pilotage de la mise en conformité : DPO chef d'orchestre de la mise en conformité, DPO et comité de pilotage
- Conseil de l'organisme pour son maintien en conformité/bilan annuel

- Débat : positionnement du DPO par rapport à la direction de l'entreprise, indépendance et/ou lien hiérarchique ?

- Cas pratique : différences entre un DPO désigné auprès de la CNIL et un référent RGPD non désigné auprès de la CNIL

Examiner son mode de désignation et ses responsabilités

Désigner un DPO interne, externe ou mutualisé

- Cas dans lesquels la désignation du DPO est obligatoire (UE et États membres)
- Conditions et modalités de la désignation (qualifications et compétences requises)
- Choix entre la désignation d'un DPO interne, externe ou mutualisé, désignation dans un groupe

- Mise en situation : désignation du DPO auprès de la CNIL et en interne

Analyser le statut et les responsabilités des DPO

- Statut du DPO interne/du DPO externe ou mutualisé
- Responsabilités

- Jeu de rôle : deviner qui est qui ?

- Étude de cas : quelle responsabilité du DPO en cas de mise en cause de l'entreprise et de violation de données ?

Exercer les missions de DPO

Lister les missions du DPO

- Information et conseil du RT ou du ST
- Contrôle du respect du RGPD et des autres dispositions en matière de protection des données
- Conseil sur l'analyse d'impact/coopération et point de contact avec l'autorité de contrôle
- Identification, évaluation et préconisations avec le RSSI des mesures organisationnelles et techniques de sécurité
- Point de contact des personnes concernées pour l'exercice des droits
- Sensibilisation et formation, communication interne et externe (missions complémentaires)

- Quiz interactif : les missions du DPO

Déployer la fonction de DPO dans l'entreprise

- Participation à toutes les questions de protection des données

- Ressources pour exercer ses missions/accès aux données à caractère personnel, formation continue
- Mise en situation : le positionnement du DPO dans l'entreprise

Encadrer la fin de mission du DPO

- Circonstances de la fin de mission : à l'initiative du DPO ou de l'organisme
- Cadre juridique
- Droits du DPO

- Cas pratique : dans quelles circonstances mettre fin à la mission du DPO ?

DPO (DPD) : piloter la protection des données personnelles de l'entreprise (1 jour)
Voir le moduleRéduire

Identifier les mesures de conformité à mettre en place dans l'entreprise

Auditer la protection des données

- Méthodologie, identification des interlocuteurs, interviews, collecte des documents et informations
- Distinction entre les opérateurs (responsables de traitement, responsables conjoints, sous-traitants)
- Identification des bases juridiques des traitements

- Quiz : points clés de l'audit

Mettre en œuvre la cartographie des traitements

- Cartographie des traitements et des données
- Rôle du DPO lors de la cartographie des traitements : aide lors de l'enregistrement des traitements ou seul contrôle des registres ?
- DPO et registres de l'art. 30 (RT et ST)

- Construction d'outil (check-list) : méthodologie pour réaliser l'audit

Mettre en conformité la documentation contractuelle et d'information

- Rôles respectifs de la direction juridique et du DPO
- Identification des réglementations sectorielles
- Focus sur les transferts de données personnelles vers des pays tiers (décisions d'adéquation et garanties appropriées)

- Construction d'outils : bâtir sa documentation de mise en conformité

- Plan d'action : construire sa politique de protection des données personnelles (RT et ST, BtoC et BtoB)

- Cas pratique : rédiger les clauses relatives à la protection des données personnelles dans les contrats

Déterminer l'opportunité d'une AIPD (ou DPIA)

- Rappels sur l'AIPD (accountability, finalité, caractère obligatoire)
- Critères sur l'opportunité d'une AIPD
- Notion de risque sur la vie privée
- Réalisation d'un AIPD : méthode et outils à la disposition du RT et du DPO, conseils sur la sous-traitance et sur les mesures organisationnelles et techniques de sécurité

- Mise en situation : dans plusieurs situations données, de l'opportunité ou non de réaliser une PIA

Réagir face aux exigences liées à la protection de données des personnes concernées

Répondre aux demandes d'exercice des droits des personnes interessées

Attributions du DPO
- Mise en place des procédures d'exercice des droits
- Exercice des droits en pratique

- Cas pratique : demande d'accès, quel rôle et quelles diligences du DPO ?

Répliquer à une violation de données
- Procédures de détection/de notification : mise en place
- Rôle du DPO en cas de violation de données

- Mise en situation : réagir à une violation de données

Utiliser les ressources pertinentes pour piloter la conformité

Sensibiliser les différentes parties de l'entreprise
- Communication dans l'entreprise
- Élaboration des programmes de formation

- Mise en situation : alerter les acteurs de l'entreprise des enjeux de la protection des données

Mettre à disposition des outils méthodologiques et logiciels pour l'exercice des fonctions de DPO
- Nécessité de s'appuyer sur des outils de gouvernance des données
- Outils à disposition : CNIL et éditeurs
- Outils et traçabilité des activités de traitement

- Partage d'expérience : les outils adaptés au contexte de son entreprise

CNIL : gérer les contrôles liés à la protection des données personnelles (1 jour)
Voir le moduleRéduire

Préparer un contrôle CNIL

Intégrer le renforcement des contrôles de la CNIL depuis le RGPD
- Renforcement du cadre
- Origine des contrôles
- Typologie des contrôles

- Autodiagnostic : identifier les actions préventives à mener depuis le RGPD

Lister les points d'attention lors du déroulement d'un contrôle sur place (au sein de l'entité)
- Vérification de l'identité des contrôleurs habilités
- Informations et droits dans le cadre d'une procédure de contrôle
- Etendue des pouvoirs des agents de contrôle

- Jeu de rôle : quelle posture adopter face à un contrôle de la CNIL ? comment accompagner les agents ?

Critère d'évaluation de la compétence : Check-list - Les vérifications à opérer avant et pendant le contrôle CNIL

Adopter les mesures adéquates à la suite d'un contrôle CNIL

Traiter les suites d'un contrôle
- Procès-verbal du contrôle
- Actions à prendre par l'entité contrôlée à la suite du contrôle
- Décision de l'autorité de contrôle
- Point sur la nouvelle procédure simplifiée de sanction CNIL (loi du 24/01/2022 et Décret 8/04/2022)

- Débat : comparer la procédure simplifiée et la procédure ordinaire

Examiner les sanctions en cas de manquement et les voies de recours offertes

- Typologie des sanctions et exemples de décisions
- Publicité
- Voies de recours et exemples de décisions
- Point sur les mesures correctrices dans la nouvelle procédure simplifiée de sanction CNIL
- Coopération renforcée avec le RGPD entre la CNIL et ses homologues européens, exemples de décisions

- Check-list : points d'attention pour répondre à une mise en demeure de la CNIL

Critère d'évaluation de la compétence : Exercice de synthèse - Récapituler les éléments recueillis lors du contrôle

Implémenter les actions de mise en conformité dans l'entreprise

Organiser l'intégration de la conformité dans l'entreprise

- Sensibilisation des directions opérationnelles aux dispositions du RGPD
- Désignation d'un DPO interne ou externe

- Partage d'expériences : diffuser la culture de la protection des données personnelles dans l'entreprise

Bâtir un process

- Process de gestion d'un contrôle
- Diffusion au sein de l'entité

- Débat : gérer les plaintes

Critère d'évaluation de la compétence : Quiz - Construire un plan d'actions pour gérer les contrôles de la CNIL

Cybersécurité et traitement de données personnelles (1 jour)

Voir le moduleRéduire

Définir une politique de protection des données personnelles

Repérer les données à caractère personnel

- Identification et modélisation des traitements et les flux de données métiers
- Localisation des données à caractère personnel dans le SI et/ou dans le cloud

- Cas pratique : repérer les vulnérabilités pouvant impacter les biens supports

Prévenir les violations de données

- Recensement des mesures de sécurité existantes
- Repérage des vulnérabilités pouvant impacter les biens supports

- Mise en situation : les réflexes pour garantir la violation de données

Évaluer les risques numériques

Analyser les risques numériques

- Listing des scénarios d'attaque convoitant les données sensibles et les données à caractère personnel
- Quantification des risques numériques en termes de probabilité d'occurrence et d'impacts induits

- Mise en situation : élaborer des scénarios d'attaque

Être acteur de la conformité

- Sensibilisation des décideurs sur les risques pour leur donner les moyens d'évaluation des risques

- Comment devenir force de proposition sur la stratégie à élaborer ?
- Jeux de rôle : convaincre les décideurs

Développer des actions de traitement des risques

Échafauder des stratégies

- Prévention des cyberattaques
- Utilisation de l'outil PIA de la CNIL pour protéger les données personnelles
- Mise en situation : détecter une cyberattaque

Agir sur les risques identifiés

- Pilotage des actions : réduction, transfert, acceptation, annulation
- Positionnement des capteurs, des sondes métiers et des techniques pour détecter les signes avant-coureurs ou avérés d'une attaque cyber
- Sélection, implémentation, test et optimisation des mesures de sécurité à même de réduire les risques identifiés
- Plan d'actions : renforcer le système d'information de son entreprise en appliquant les 42 règles du guide d'hygiène de l'ANSSI

Définir une politique de protection des données personnelles

Repérer les données à caractère personnel

- Identification et modélisation des traitements et les flux de données métiers
- Localisation des données à caractère personnel dans le SI et/ou dans le cloud
- Cas pratique : repérer les vulnérabilités pouvant impacter les biens supports

Prévenir les violations de données

- Recensement des mesures de sécurité existantes
- Repérage des vulnérabilités pouvant impacter les biens supports
- Mise en situation : les réflexes pour garantir la violation de données

Évaluer les risques numériques

Analyser les risques numériques

- Listing des scénarios d'attaque convoitant les données sensibles et les données à caractère personnel
- Quantification des risques numériques en termes de probabilité d'occurrence et d'impacts induits
- Mise en situation : élaborer des scénarios d'attaque

Être acteur de la conformité

- Sensibilisation des décideurs sur les risques pour leur donner les moyens d'évaluation des risques
- Comment devenir force de proposition sur la stratégie à élaborer ?
- Jeux de rôle : convaincre les décideurs

Développer des actions de traitement des risques

Échafauder des stratégies

- Prévention des cyberattaques
- Utilisation de l'outil PIA de la CNIL pour protéger les données personnelles
- Mise en situation : détecter une cyberattaque

Agir sur les risques identifiés

- Pilotage des actions : réduction, transfert, acceptation, annulation
- Positionnement des capteurs, des sondes métiers et des techniques pour détecter les signes avant-coureurs ou avérés d'une attaque cyber
- Sélection, implémentation, test et optimisation des mesures de sécurité à même de réduire les risques identifiés

- Plan d'actions : renforcer le système d'information de son entreprise en appliquant les 42 règles du guide d'hygiène de l'ANSSI

Parmi nos formateurs

Pascal Alix

Avocat au barreau de Paris, Délégué à la Protection des Données personnelles externe, EUROPRIVACY Auditor, Chargé d'enseignement en droit de l'intelligence artificielle à l'Université d'Artois.

Hubert De Segonzac

Avocat au barreau de Paris et Délégué à la Protection des Données personnelles externe, membre de l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP)