RÉFÉRENTIELS D'ACTIVITÉS, DE COMPÉTENCES ET D'ÉVALUATION

RÉPERTOIRE SPÉCIFIQUE

CERTIFICATION EXERCER LES FONCTIONS DE DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au Règlement européen sur la protection des données au sein de l'organisme qui l'a désigné. Il peut occuper cette fonction à plein temps, ou à temps, partiel. Les organismes peuvent désigner un DPO interne ou externe à leur structure. Si ce rôle est rempli par un employé interne à l'organisation, ses missions de DPO ne doivent pas présenter de conflits d'intérêt avec ses autres missions.

Notre certification s'adresse à toute personne évoluant dans le secteur informatique, juridique, administratif, financier, de la conformité, de l'audit, …, souhaitant acquérir de nouvelles compétences qui lui permettront d'endosser le rôle de DPO au sein de la structure dans laquelle elle évolue professionnellement.

RÉFÉRENTIEL D'ACTIVITES	RÉFÉRENTIEL DE COMPETENCES	RÉFÉRENTIEL D'EVALUATION	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
		I- Questionnaire Le candidat répond individuellement à une série de 25 questions ouvertes et de cas à résoudre, portant sur ses connaissances juridiques. Durée de l'épreuve : 3 heures **II – Mise en situation professionnelle individuelle, réelle ou reconstituée, plaçant le candidat en position de DPO** Le/la candidate réalisera cette mise en situation : -à partir d'un cas réel rencontré dans le cadre de sa pratique professionnelle, en cas de mise en situation professionnelle réelle ou -à partir d'un cahier des charges établi par l'organisme certificateur, en cas de mise en situation professionnelle reconstituée Le candidat devra produire un rapport détaillant à minima les thèmes 1 à 5 décrits ci-dessous.	

		Ce rapport devra être remis au centre certificateur, au plus tard 15 jours avant le passage devant le jury. Durée : 20 minutes de présentation orale individuelle par le/la candidat(e), suivies de 20 minutes de questions du jury	
1-Cartographie des traitements de données personnelles	C1 - Recenser les différents traitements de données personnelles en respectant la réglementation, pour les enregistrer dans le registre de traitements des données C2 - Lister les catégories de données personnelles traitées pour les identifier dans le registre de traitements des données C3 - Définir les objectifs poursuivis par les opérations de traitements de données en s'appuyant sur la réglementation en vigueur C4 - Lister les acteurs (internes ou externes) qui traitent ces données, notamment en identifiant clairement les prestataires sous-traitants, afin d'actualiser les clauses de confidentialité C5 - Recenser les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne C6 - Mettre en place le registre de traitements des données personnelles en réponse à l'obligation prévue par le RGPD	*1/5* Réalisation d'une cartographie de traitement des données. Un registre des traitements de données doit être produit.	Le registre donne une vue d'ensemble du traitement des données de l'organisation. Il répond à l'obligation du RGPD de tenu du registre. Il permet d'identifier précisément : - les parties prenantes (représentant, sous-traitants, co-responsables...) qui interviennent dans le traitement des données - les catégories de données traitées - à quoi servent ces données, qui accède aux données et à qui elles sont communiquées, - combien de temps elles sont conservées - comment elles sont sécurisées Il est régulièrement mis à jour ou sa mise à jour est planifiée

2-Gestion des risques des traitements de données	C7 - Identifier les risques de sécurité et de conformité associés aux opérations de traitement de données, dans un cadre national ou international afin d'en contrôler les impacts C8 - Évaluer la pertinence d'effectuer une AIPD (analyse d'impact relative à la protection des données) en s'appuyant sur les outils mis à disposition par la CNIL, pour construire un traitement conforme au RGPD et respectueux de la vie privée en cas de détection de traitements de données personnelles susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées C9 - Mettre en place les mesures de sécurité adaptées pour limiter les risques de violation de données C10 - Rédiger les procédures de gestion de crise pour prévenir les situations contentieuses, instruire les réclamations, identifier les violations de données et réaliser les signalements à la CNIL C11 - Rédiger la procédure interne en cas de contrôle de la CNIL (modalités d'accueil, personnes à prévenir, informations à obtenir) C12 - Identifier et gérer un incident de sécurité et/ou de conformité à la réglementation en matière de protection des données, afin de déterminer la nature de la faille et de mettre en place des solutions de résolution	*2/5* Identification des risques sur l'ensemble du cycle de vie des données, et identification de ceux pour lesquels une AIDP est nécessaire	- L'identification des risques est complète. - La responsabilité juridique de l'organisation et les risques encourus sont connus et identifiés. - Les violations de données personnelles nécessitant une notification à l'autorité de contrôle et celles nécessitant une communication aux personnes concernées sont identifiées. - Des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement sont présentées. - La méthode de l'analyse d'impact (description, évaluation de la nécessité et de la proportionnalité, l'évaluation des risques, les mesures envisagées) est respectée Le candidat détermine s'il est nécessaire ou non d'effectuer une analyse d'impact relative à la protection des données (AIPD), et en vérifie l'exécution.

3-Mise en place d'un système de management des données personnelles	C13 - Identifier la base juridique sur laquelle se fonde le traitement (par exemple, consentement de la personne, intérêt légitime, contrat, obligation légale) pour déterminer le périmètre réglementaire C14 - Vérifier que seules les données strictement nécessaires à la poursuite des objectifs sont collectées et traitées pour être en accord avec la réglementation C15 - Si pertinent, vérifier que les sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, afin qu'ils puissent également se conformer à la réglementation C16 - Établir les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité des données, retrait du consentement...), en respectant le cadre réglementaire, pour recevoir et gérer les demandes d'exercice des droits C17 - Mettre en place des outils de suivi et de contrôle de l'utilisation des traitements (analyse de logs, détection de données interdites, vérification du respect des durées de conservation, ...), afin d'être alerté en cas de non-respect des procédures de sécurité des données C18 - Mettre en place un contrôle de l'effectivité des mesures techniques et organisationnelles de protection des données pour identifier les anomalies et dysfonctionnements C19 - Rédiger la politique générale de traitement des données afin qu'elle soit conforme aux exigences du RGPD, pour informer les personnes concernées par le traitement de leurs données	*3/5* Mise en place d'un système de management des données personnelles, et production de la politique générale de traitement des données	- La base juridique du traitement est identifiée - Le principe de finalité est respecté. - Si pertinent, l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées est prouvée - La traçabilité est assurée à l'aide d'outils de suivi - L'effectivité des mesures techniques et organisationnelles de protection des données mises en place est assurée à l'aide d'outils de contrôle - L'obligation du RGPD d'information et de transparence à l'égard des personnes dont les données sont traitées (clients, collaborateurs, …), est respectée

4-Communication sur les sujets RGPD	C20 - Communiquer avec la CNIL pour faciliter les échanges en cas de contrôle - en étant le point de contact de l'organisme sur les sujets RGPD, - en répondant aux demandes lors d'un contrôle sur place, instruction d'une réclamation, consultation dans le cadre d'une AIPD, notification d'une violation de données, etc C21 - Communiquer avec les personnes dont les données personnelles sont traitées pour faciliter les échanges en cas de demande d'information ou de réclamation, - en étant leur point de contact - en prenant en charge l'organisation du traitement de leurs demandes d'exercice de droits (accès, portabilité, etc.) afin qu'une réponse complète leur soit apportée dans les délais impartis - et en répondant à toutes leurs questions relatives au traitement de leurs données personnelles C22 - Communiquer au sein de l'organisme pour sensibiliser la direction et les collaborateurs aux règles régissant la protection des données personnelles : - en étant l'interlocuteur interne référent pour toute question concernant la protection des données, et si nécessaire au moyen de personnes relais - en procédant à des actions de communication et de sensibilisation sur le sujet de la protection des données (affiches, guides pratiques, …) - en formant en interne, les collaborateurs qui traitent les données au sein de l'organisme sur les grands principes de la protection des données personnelles - en tenant un tableau de bord des activités menées, afin d'alimenter un point régulier (réunion de direction) ainsi qu'un rapport d'activité régulier à destination de la direction de l'organisme	*4/5* Production d'un plan de communication, de sensibilisation et de formation des collaborateurs de l'organisation	- Les modalités de réponse aux demandes extérieures ont été prévues. - Le processus interne permettant de garantir l'identification et le traitement des demandes a un délai court (1 mois au maximum). - Les relations avec les autorités de contrôle sont gérées, en répondant à leurs sollicitations et en facilitant leur action (instruction des plaintes et contrôles en particulier). - Une personne relais a été prévue en cas d'absence ou d'empêchement pour recevoir les demandes et être le point de contact des collaborateurs, des personnes concernées par les données, et de la CNIL. - Des programmes de formation et de sensibilisation du personnel et des instances dirigeantes en matière de protection des données ont été mis en œuvre ou dispensés

5 - Mise en place d'un système de veille	C23 – Effectuer une veille permanente (sur la jurisprudence, les publications des autorités de contrôle, ...) pour entretenir ses connaissances techniques et opérationnelles en lien avec les activités de traitement de l'organisme, et à l'occasion de formations et de partages d'expérience avec son réseau de DPO	*5/5* Établir un système de veille	- Un système de veille a été mis en place. - Le cadre réglementaire relatif à la protection des données est acquis. - Le candidat démontre sa maîtrise du cadre d'intervention du DPO, de son rôle et de ses responsabilités.