Initiative Data Compétences
Un réseau CCI FRANCE

Référentiels de compétences et d'évaluation

Intitulé de la certification		
Piloter un projet de mise en conformité des modalités de traitement et de protection des données en TPE/PME		
Description de la situation professionnelle et de l'activité		
Information, conseil et accompagnement du chef d'entreprise et des salariés de la TPE/PME dans l'évaluation des pratiques actuelles en matière de traitement des données personnelles et mise en place des actions, procédures et outils associés afin d'assurer la mise en conformité de l'entreprise au regard des obligations découlant du contexte règlementaire. Tâches exercées : • Préparation du projet de mise en conformité des activités de traitement des données personnelles de la TPE/PME • Diagnostic du degré de conformité de la TPE/PME au regard des activités de traitement des données personnelles • Mise en conformité des activités de traitement des données personnelles de la TPE/PME • Etablissement des conditions de maintien de la conformité des activités de traitement des données personnelles de la TPE/PME		
COMPÉTENCES	**MODALITÉS D'ÉVALUATION**	**CRITÈRES D'ÉVALUATION**
C.1 Identifier les obligations évolutives de l'entreprise en matière de traitement et de protection des données personnelles, en analysant les textes règlementaires concernés (RGPD, loi informatique et liberté…) et en opérant une veille sur les sujets en lien avec les données personnelles et la sécurité des systèmes d'information, afin de déterminer la démarche à initier pour mettre et maintenir l'entreprise en conformité.	Les candidats se présentent aux deux modalités suivantes : **1/** *En relation avec les compétences C.1 à C.9 :* **Une mise en situation simulée à partir d'une étude de cas fictif**, consistant pour chaque candidat en la **réalisation d'un projet de mise en conformité de traitement des données** sur un périmètre limité à une activité, une fonction ou un	- L'analyse et l'interprétation des textes légaux et règlementaires sont exactes et permettent une identification correcte des obligations incombant à l'entreprise en matière de traitement et de protection des données personnelles, selon son contexte. - Les rôles et missions des acteurs institutionnels (ANSSI, CNIL…) participant à l'application de la règlementation en matière de protection des données personnelles sont identifiés, ainsi que l'utilité des ressources et outils qu'ils proposent.
C.2 Analyser la problématique spécifique à l'entreprise en matière de traitement et de protection des données personnelles, en évaluant – en concertation avec le chef d'entreprise – le périmètre et l'importance de la démarche de mise en conformité à mener, afin de proposer une méthode, une organisation, une planification et un plan d'action adaptés à l'entreprise et à ses enjeux en la matière.		- L'analyse de la problématique de l'entreprise permet de qualifier et de quantifier ses enjeux liés à la protection des données, au regard de la nature de son activité, de son modèle économique, de son organisation interne et de ses moyens techniques. - La méthodologie de projet choisie (approche agile ou prédictive, phasage, étapes…) est adaptée au contexte de l'entreprise (moyens techniques et humains, culture…) et optimise ses conditions d'aboutissement.

	service d'une entreprise. Chaque candidat devra notamment produire les éléments suivants : - L'analyse et la prise en compte des exigences et obligations règlementaires issues du RGPD et de la loi informatique et liberté (C.1). - Le plan projet résultant de l'analyse de la problématique spécifique de l'entreprise et présentant la méthode de conduite de projet retenue, le plan d'action, le calendrier des actions, la composition de l'équipe projet (C.2). - La présentation du projet (C.3). - Le registre de traitement des données personnelles de l'entreprise sur un périmètre limité à une fonction ou un service (C.4). - L'évaluation de l'opportunité de mener une AIPD (C.5). - La liste des actions de mise en conformité à réaliser (C.6). - Les procédures renouvelées de traitement des données à appliquer (C.7). - Le choix de la	- La planification des actions constitutives du projet est réaliste, adaptée aux objectifs visés concernant les échéances fixées et cohérente avec la méthodologie de projet retenue. - L'équipe projet est correctement dimensionnée au regard des moyens de l'entreprise et des objectifs visés, sa constitution est justifiée au regard de la position fonctionnelle et hiérarchique que ses membres occupent au sein de l'entreprise. - Les spécificités des collaborateurs impliqués sont prises en compte et des adaptations sont identifiées pour garantir l'inclusivité de la démarche, notamment concernant le personnel en situation de handicap. - Le plan projet est globalement correctement dimensionné au regard des objectifs visés et des moyens de l'entreprise.
C.3 Exposer la démarche de mise en conformité de la gouvernance des données à l'ensemble du personnel de l'entreprise, en présentant le RGPD et les obligations qui en résultent et en spécifiant la structure du projet à mener, afin de les sensibiliser à l'importance et au sens de la démarche et de favoriser leur compréhension, leur adhésion et en définitive leur implication.		- Le sens et l'importance de la démarche à conduire sont exposés de façon convaincante, et ses enjeux associés sont explicités par une présentation à la fois claire, synthétique et précise du contexte règlementaire. - Le rôle assuré en tant que meneur du projet, ainsi que la périmètre de sa fonction et son champ de responsabilité, sont présentés. - La présentation est dynamique et le soin apporté à privilégier une approche pédagogique favorise la compréhension et l'adhésion de l'auditoire.
C.4 Etablir la cartographie des traitements des données personnelles opérés par l'entreprise et ses sous-traitants, en mobilisant les services internes/externes concernés et en recensant pour chaque activité de traitement : - les catégories de données et leur degré de sensibilité, - les finalités de collecte, de traitement et d'utilisation des données, - les opérateurs internes ou externes des traitements opérés (sous-traitants compris), - les conditions d'hébergement, de conservation et de sécurisation des données, - les destinataires internes et externes des données,		- L'identification des activités de traitement des données personnelles opérées sur le périmètre de la fonction ou du service est exhaustive et intègre, le cas échéant, celles d'éventuels sous-traitants. - La qualité et la précision des informations portées dans le registre satisfont les exigences règlementaires. Sont notamment spécifiés pour chaque activité de traitement : l'identité et les coordonnées du responsable du traitement ; les objectifs poursuivis ; la liste exhaustive des données collectées et l'identification de celles présentant un degré de criticité

afin de réaliser le registre de traitement des données et d'identifier les éventuels écarts avec les obligations découlant du contexte légal (loi informatique et liberté & RGPD).	documentation technique et organisationnelle du dispositif de traitement des données à destination de la CNIL et des collaborateurs internes (C.8). - Le programme de maintien du dispositif de protection des données (C.9). *La modalité est réalisée individuellement par chaque candidat en centre de formation et conjugue une partie écrite et une partie orale.*	particulier ; les mesures de conservation et de sécurisation des données ; les services et personnels destinataires des données en interne ; les destinataires externes des données en cas de transfert hors de l'UE. - La qualité du registre et de son niveau d'information permet l'évaluation du degré de conformité de l'entreprise en matière de traitement des données personnelles et d'identifier les actions à conduire pour optimiser et régulariser les pratiques usuelles.
C.5 Définir les actions de mise en conformité des traitements de données personnelles à mettre en œuvre au sein de l'entreprise, en s'appuyant sur l'analyse des pratiques ressortant du registre de traitement des données et en priorisant les mesures identifiées au regard des caractéristiques des données et de leur criticité, afin de prévenir tout risque de non-conformité et d'entorses aux libertés individuelles des personnes.		- Les points de non-conformité sont identifiés de façon exhaustive et leur degré d'importance est qualifié. - Les actions identifiées satisfont les obligations règlementaires concernant la mise en œuvre de traitements licites, le respect des droits des personnes, les éventuels transferts vers un pays tiers, les destinataires des données collectées, la durée de conservation des données collectées. - Les dispositions d'information des personnes concernant le traitement de leurs données sont prévues et appliquent les principes de concision, de transparence, d'intelligibilité et d'accessibilité. - La collecte et le traitement des données sont justifiés par leur utilité au regard de la finalité du traitement ; les données et fichiers inutiles sont supprimés. - Les données sont sécurisées en croisant différents moyens correctement dimensionnés au regard des capacités de l'entreprise : infrastructure informatique, outils de protection (antivirus), limitation d'accès aux données par des mesures de protection (mots de passe…). - L'accès aux données est règlementé et restreint aux seuls opérateurs ayant un intérêt avéré à les consulter ou traiter. - La durée de conservation des données est justifiée et limitée. - Les transferts de données hors de l'UE sont encadrés. - Le recours à des sous-traitants pour le traitement des données est encadré et contractualisé (objet, durée du traitement, nature

		et finalité du traitement, type de données à caractère personnel et catégories de personnes concernées, obligations et droits). La suffisance des mesures techniques et organisationnelles mises en œuvre est garantie au regard des exigences du RGPD.
C.6 Déterminer l'opportunité ou le besoin de réaliser des études d'impact relatives à la protection des données personnelles (AIPD[1]), en évaluant la criticité des données traitées et en qualifiant les risques sur les droits et libertés des personnes associés, afin d'identifier les mesures correctement proportionnées et dimensionnées pour les prévenir et éliminer toute possibilité d'usage menaçant la vie privée des personnes.		- Les données à caractère sensible (santé, opinion politique, conviction religieuse…) sont identifiées et leur degré de criticité est correctement évalué. - Les traitements porteurs de risques élevés pour les droits et libertés des personnes concernées sont identifiés. - Le choix de conduire ou non une AIPD est justifié par l'analyse de la nature des données personnelles et de leurs traitements ; il traduit une compréhension et une application correcte du RGPD.
C.7 Mettre en application les procédures de traitement des données personnelles au sein de l'entreprise, en veillant à la bonne observation des règles édictées et à la satisfaction des multiples exigences légales (licéité des données collectées, durée de conservation, sécurité et confidentialité des données, information et consentement des personnes concernées...), afin de protéger l'intégrité des données en dépit de la survenue d'événements internes ou externes.		- Les risques identifiés sont traités de façon suffisante pour minorer leurs menaces. - Les mesures techniques et organisationnelles adaptées aux risques identifiés sont définies et déterminent les éléments à protéger et les principes supplémentaires à appliquer (sauvegarde, traçage de l'activité, gestion des violations de données…). - Les différentes procédures stipulent clairement et précisément les acteurs internes concernés. - La gestion des réclamations et l'exercice des droits des personnes sont garantis par une procédure leur permettant notamment d'accéder à leurs données, d'en demander la rectification ou l'effacement et d'en limiter la durée de traitement. - Une procédure est mise en place en cas de violation des données, prévoyant notamment l'alerte de l'autorité compétente et l'information des personnes concernées.

[1] Ce type d'étude est couramment désigné par l'acronyme AIPD, pour « Analyse d'impact de la protection des données » ; on peut également rencontrer l'acronyme anglais PIA pour « *Privacy Impact Assessment* ».

		- Les procédures mises en place garantissent l'application des réflexes de la protection des données par les différents opérateurs concernés au sein de l'entreprise.
C.8 Constituer la documentation technique et organisationnelle relative aux traitements des données personnelles au sein de l'entreprise, en rassemblant les éléments obligatoires (registre de traitement, AIPD…) et en formalisant les outils à usage interne (catalogue de mesures techniques et organisationnelles, procédures, guide…), afin de prouver sa conformité aux obligations légales et de mettre à disposition des acteurs internes les moyens favorisant son maintien.		- La documentation obligatoire est, sur la forme et le fond, conforme et suffisante au regard des attentes et exigences de l'autorité administrative. - Le choix de la documentation non obligatoire est adapté aux besoins de l'entreprise et à ses salariés.
C.9 Construire un programme de maintien du dispositif de protection des données personnelles de l'entreprise, en prévoyant ses modalités de gouvernance, ainsi que celles de contrôle et de mise à jour périodique du registre de traitement et en déterminant les actions d'information et de sensibilisation à mettre en œuvre auprès des collaborateurs au sujet du RGPD, afin de pérenniser des usages et pratiques respectant les obligations règlementaires et garantissant la protection des personnes concernées.		- L'analyse justifiant le choix de désigner ou non un DPO est correcte et s'appuie sur la prise en compte de paramètres externes (les dispositions du RGPD en la matière) et internes (taille et organisation de la TPE/PME, compétences, enjeux concernant ses données…). - Le programme prévoit une vérification et une évaluation régulières des procédures mises en place, ainsi que des modalités de traitement particulières des données à caractère sensible. - Les conditions de maintien de la conformité sont assurées par l'entretien de l'information et de la sensibilisation des collaborateurs, sous la forme d'un plan de communication concis et synthétisant le type d'actions à mettre en œuvre et leur périodicité.