

Piloter la mise en conformité des modalités de traitement et de protection des données personnelles en TPE/PME

Prérequis : L'accès à la certification ne requiert pas d'expertise particulière. En revanche, l'importance et les enjeux attachés à la fonction, ainsi que l'objet de celle-ci, imposent que chaque candidat justifie d'un titre ou diplôme de niveau 5.

A titre dérogatoire, les candidatures des professionnels ne pouvant se prévaloir d'un titre ou diplôme de niveau 5 mais justifiant d'une expérience professionnelle de 3 années minimales pourront être examinées et se voir réserver une issue positive.

Toutes les candidatures font l'objet d'une évaluation, sous la forme d'un entretien téléphonique, visant à vérifier l'aptitude du candidat et l'adéquation de son projet de certification avec ses attentes professionnelles.

Durée : 5 jours, 35 heures , évaluation comprise

Objectifs : Intégrer les enjeux et outils de la mise en conformité au Règlement Général sur la Protection des Données (RGPD) et en assurer le pilotage dans son entreprise

Compétences visées :

- Identifier les obligations évolutives de l'entreprise en matière de traitement et de protection des données personnelles
- Analyser la problématique spécifique à l'entreprise en matière de traitement et de protection des données personnelles
- Exposer la démarche de mise en conformité de la gouvernance des données à l'ensemble du personnel de l'entreprise,
- Etablir la cartographie des traitements des données personnelles opérés par l'entreprise et ses sous-traitants
- Définir les actions de mise en conformité des traitements de données personnelles à mettre en œuvre au sein de l'entreprise
- Déterminer l'opportunité ou le besoin de réaliser des études d'impact relatives à la protection des données personnelles
- Mettre en application les procédures de traitement des données personnelles au sein de l'entreprise
- Construire un programme de maintien du dispositif de protection des données personnelles
- Constituer la documentation technique et organisationnelle relative aux traitements des données personnelles au sein de l'entreprise

Programme :

Analyser la problématique spécifique à l'entreprise en matière de traitement et de protection des données personnelles en lien avec l'environnement juridique

Identifier et interpréter les lois qui régissent les obligations en matière de traitement et de protection des données personnelles

Identifier les enjeux liés à la protection de données dans son entreprise

Analyser la problématique

Préparer le projet de mise en conformité des activités de traitement des données personnelles de la TPE/PME

Déterminer la démarche à initier pour mettre

Choisir une méthodologie de projet adaptée

Préparer la mise en conformité

Communiquer sur le projet de mise en conformité auprès du personnel

Cartographier les traitements de données

Réaliser le registre des traitements

Collecter l'information nécessaire à la cartographie auprès des sous-traitants

Mettre en conformité les activités de traitement de données personnelles de la TPE/PME

Définir les actions de mise en conformité à réaliser

Les procédures de traitement des données à appliquer

Le choix de la documentation technique et organisationnelle du dispositif de traitement des données à destination de la CNIL et des collaborateurs internes

Assurer le maintien du dispositif de protection des données personnelles de l'entreprise

Le programme de maintien du dispositif de protection des données

Evaluer les procédures et modalités de traitement particulières des données à caractère sensible

Appliquer le plan de communication défini dans le projet

Référentiel des compétences attendu CCI France	Programme de la Formation	Contenu développé	Durée	Méthode d'apprentissage	Méthode d'évaluation formative
Analyser la problématique spécifique à l'entreprise en matière de traitement et de protection des données personnelles					
C.1 Identifier les obligations évolutives de l'entreprise en matière de traitement et de protection des données personnelles	Identifier et interpréter les lois qui régissent les obligations en matière de traitement et de protection des données personnelles	<p>Présentation du RGPD : obligations règlementaires et périmètre d'application Enjeux et philosophies du législateur européen Loi informatique et liberté Définitions clés Principes juridiques Textes règlementaires Traitement des informations Rôles et missions des acteurs institutionnels</p> <p>Ressources et outils pour assurer la veille règlementaire (dans boîte à outil du DPO)</p> <p>Identifier les rôles et missions des acteurs institutionnels (CNIL, CEPD, Commission Européenne, ANSSI, ...) participant à l'application de la réglementation en matière de protection des données personnelles</p>	½ journée		

Préparer le projet de mise en conformité des activités de traitement des données personnelles de la TPE/PME

<p>C.2 Analyser la problématique spécifique à l'entreprise en matière de traitement et de protection des données personnelles</p>	<p>Identifier les enjeux liés à la protection de données dans son entreprise Analyser la problématique</p> <p>Déterminer la démarche à initier pour mettre et maintenir l'entreprise en conformité</p> <p>Choisir une méthodologie de projet adaptée</p> <p>Préparer la mise en conformité</p>	<p>Élaboration du plan d'actions, du planning et des outils de la conformité :</p> <p>Définir des objectifs, des échéances et à planifier des actions à mettre en œuvre</p> <p>Déterminer les finalités de traitement (objectifs poursuivis) Identifier les bases légales (licéité)</p> <p>Appliquer le principe de minimisation des données</p> <p>Limiter les durées de conservation</p> <p>Organiser les processus d'archivage et de destruction</p> <p>Identifier et référencer les durées légales de conservation Identifier les mesures organisationnelles et techniques de protection des données propres à chaque traitement Anticiper les problématiques liées à de nouveaux traitements (<i>privacy by design</i>) Assurer la Veille et maintien à jour des mesures de protection</p> <p>Réaliser d'éventuelles études</p>	<p>1/2 journée</p>		
--	--	--	-------------------------------	--	--

		<p>d'impact, dont l'étude d'impact sur la vie privée</p> <p>Choisir l'équipe projet concernée par la mise en conformité</p> <p>Identifier les rôles et missions de chacun</p> <p>Identifier les moyens techniques à mettre en œuvre</p> <p>Déterminer les secteurs d'activité à risque en fonction notamment des notions de « sensibilité » ou de « large échelle ».</p> <p>Repérer les traitements de données de son organisme et les analyser (cf. définition, cf. cartographie)</p> <p>Mettre en place une méthode d'analyse adapté à l'activité et à la sensibilité de l'organisme (notion de réalisme et de dimensionnement par rapport à son organisme).</p> <p>Prendre en considération les enjeux adjacents (notamment financiers) pouvant influencer ou compromettre les plans d'actions</p>			
--	--	---	--	--	--

<p>C.3 Exposer la démarche de mise en conformité de la gouvernance des données à l'ensemble du personnel de l'entreprise</p>	<p>Communiquer sur le projet de mise en conformité auprès du Personnel</p>	<p>Identifier les rôles et missions de chacun</p> <p>Communiquer sur le RGPD auprès des collaborateurs de l'organisme</p> <p>Boîte à outils du DPO</p> <p>Déterminer un plan de communication périodique des collaborateurs à titre préventif ou sur incident à titre curatif.</p> <p>Organiser les process internes en rédigeant les procédures : nouveau traitement, exercice des droits, notification de faille de sécurité, purge, portabilité, audit, violation de données, réclamations... et définissant la <u>documentation</u> nécessaire pour une communication optimisée à l'égard des parties prenantes.</p> <p>Mettre en œuvre les pédagogies correctives et des contrôles de sécurité</p> <p>Compétence nécessaire du DPO : la pédagogie nécessaire pour convaincre ses collaborateurs.</p> <p>Mettre en place l'outil de</p>	<p>¼ de journée</p>	<p>Mise en situation : Présentation des enjeux, du projet, du rôle du DPO et la démarche</p>	<p>Grille évaluation orale sur la forme : présentation claire, synthétique et précise du contexte réglementaire</p>
---	--	---	----------------------------	--	---

		<p>responsabilisation des acteurs internes (opérationnels des traitements de données)</p> <p>Apprendre à sensibiliser sur les enjeux de la protection des données (notions clés, leviers de réflexions, exemples marquants etc.)</p>			
--	--	--	--	--	--

C.4 Etablir la cartographie des traitements des données personnelles opérés par l'entreprise et ses sous-traitants	<p>Cartographie des traitements de données</p> <p>Réaliser le registre des traitements</p> <p>Collecter l'information nécessaire à la cartographie auprès des sous-traitants</p>	<p>Recenser les traitements de données :</p> <ul style="list-style-type: none"> -les catégories de données et leur degré de criticité les finalités de collecte, de traitement et d'utilisation des données, les opérateurs internes ou externes des traitements opérés (sous-traitants compris), et plus particulièrement l'identité est les coordonnées du responsable du traitement -les conditions d'hébergement, de conservation et de sécurisation des données, -les destinataires internes et externes des données <p>Identifier les « cycles de vie » des données traitées au sein de l'entreprise et en dehors, par les sous-traitants.</p> <ul style="list-style-type: none"> -Les mesures de conservation et de sécurisation des données encadrant la donnée; -Les services et personnels destinataires des données en interne ; -Les destinataires externes des données en cas de transfert hors de l'UE. 	<p>1 journée</p>	

		<p>Qu'est ce que le registre des traitements de données ? Quid du registre des sous-traitants ?</p> <p>Identifier les activités de traitement des données personnelles opérées sur le périmètre de la fonction ou du service et des sous-traitants</p> <p>Evaluer le degré de conformité de l'entreprise</p> <p>Identifier les actions à conduire pour optimiser et régulariser les pratiques usuelles</p> <p>Quelles sont les rôles de chacun dans la tenue du registre des activités de traitement ?</p> <p>Quand et comment mettre à jour le registre ? Par qui ?</p> <p>Sous quel(s) format(s) est-il pertinent de mettre en œuvre le registre ? Qu'est-ce que le <i>versionning</i> et la traçabilité ?</p>			
--	--	--	--	--	--

Mettre en conformité les activités de traitement de données personnelles de la TPE/PME et définir les conditions de maintien de cette conformité					
C5 : Définir les actions de mise en conformité des traitements de données personnelles à mettre en œuvre au sein de l'entreprise	Définir les actions de mise en conformité à réaliser	Identifier et classer les points de non conformités Valider la conformité aux obligations réglementaires des traitements licites Le respect des droits des personnes Les transferts vers un pays tiers Les destinataires des données collectées La durée de conservation des données collectées Les notions de disposition d'information de données Utilité et finalité de traitement des données Les moyens de sécurisation des données Appliquer la réglementation liée à l'accès aux données, la durée de conservation, les transferts hors UE, le recours à des sous-traitants pour le traitement des données	1/2 journée		

		Evaluer l'opportunité de mener une AIPD			
C6 : Déterminer l'opportunité ou le besoin de réaliser des études d'impact relatives à la protection des données personnelles		<p>Comprendre les enjeux de l'AIPD</p> <p>Savoir mener une AIPD</p> <p>Identifier les faisceaux d'indices permettant d'évaluer le caractère « à risque » d'un traitement de données</p> <p>Identifier et évaluer les données à caractère sensible</p> <p>Identifier les traitements porteurs de risques élevés pour les droits et libertés des personnes</p> <p>Analyse de la nature des données personnelles et de leurs traitements dans le respect du RGPD</p>	1/2 journée		

<p>C7 : Mettre en application les procédures de traitement des données personnelles au sein de l'entreprise</p>	<p>Les procédures de traitement des données à appliquer</p>	<p>Identifier les procédures de gestion des risques</p> <p>Analyser les mesures techniques et organisationnelles en présence et savoir déterminer les mesures supplémentaires nécessaires.</p> <p>Identifier les mesures techniques et organisationnelles adaptés aux risques</p> <p>Identifier les acteurs concernés par chaque mesure et/ou procédure.</p> <p>Organiser les process internes en rédigeant les procédures : nouveau traitement, exercice des droits, notification de faille de sécurité, purge, portabilité, audit, violation de données, réclamations... et définissant la documentation nécessaire pour une communication optimisée à l'égard des</p>	<p>1/2 journée</p>		

		parties prenantes			
C8 : Constituer la documentation technique et organisationnelle relative aux traitements des données personnelles au sein de l'entreprise	Le choix de la documentation technique et organisationnelle du dispositif de traitement des données à destination de la CNIL et des collaborateurs internes	<p>Réaliser d'éventuelles études d'impact, dont l'étude d'impact sur la vie privée</p> <p>Organiser et documenter un processus de gestion des incidents de sécurité et des violations de données</p> <p>Tenir le registre des violations</p> <p>Accompagner à la gestion d'un contrôle de la CNIL</p> <p>Assurer la Veille et la mise à jour des mesures de protection</p> <p>Organiser les processus d'archivage et de destruction</p> <p>Mettre en place les contrats conformes aux exigences du RGPD (clauses spécifiques)</p> <p>Mettre en place l'outil de responsabilisation des acteurs internes (opérationnels des traitements de données)</p> <p>Traçer les activités en lien avec la protection des données</p>	½ journée		

		<p>Organiser les procédures de réponses aux demandes d'exercice de droits</p> <p>Journalisation des demandes d'exercice de droits</p> <p>Organiser les process internes en rédigeant les procédures : nouveau traitement, exercice des droits, notification de faille de sécurité, purge, portabilité, audit, violation de données, réclamations... et définissant la documentation nécessaire pour une communication optimisée à l'égard des parties prenantes</p> <p>Concernant la documentation non-obligatoire, savoir adapter les besoins documentaires et de procédures aux activités et risques de l'organisme</p> <p>Mettre en œuvre une procédure de mise à jour de la documentation RGPD (modalités, démarches à suivre, acteurs concernés, facteurs objectifs de mise à jour, etc.)</p>			
--	--	--	--	--	--

Assurer le maintien du dispositif de protection des données personnelles de l'entreprise					
C9 : Construire un programme de maintien du dispositif de protection des données personnelles de l'entreprise	<p>Le programme de maintien du dispositif de protection des données</p> <p>Evaluer les procédures et modalités de traitement particulières des données à caractère sensible</p> <p>Appliquer le plan de communication défini dans le projet</p>	<p>Boîte à outils du DPO</p> <p>Planification des missions du DPO (contrôles réguliers, bilans, interviews internes, etc.)</p> <p>Sensibilisation récurrente du personnel</p>	¼ journée		
Tour de table : évaluation du positionnement en sortie					
Evaluation sommative de certification					