

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

5 - RÉFÉRENTIELS

Article L6113-1 [En savoir plus sur cet article...](#) Créé par [LOI n°2018-771 du 5 septembre 2018 - art. 31 \(V\)](#)

« Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un **référentiel d'activités** qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un **référentiel de compétences** qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un **référentiel d'évaluation** qui définit les critères et les modalités d'évaluation des acquis. »

BLOC 1 : Définir les besoins de l'entreprise en termes de sécurité et de conformité

REFERENTIEL D'ACTIVITES <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	REFERENTIEL DE COMPETENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	REFERENTIEL D'ÉVALUATION <i>définit les critères et les modalités d'évaluation des acquis</i>	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>A1. Analyse du secteur d'activité de l'entreprise et des impacts potentiels sur la protection des données personnelles</p> <ul style="list-style-type: none"> ● Analyse du secteur d'activité et identification des spécificités de l'entreprise ● Réalisation d'une veille ● Analyse des traitements de données ● Réalisation une analyse d'impact 	<p>C1. Analyser le contexte de l'entreprise en menant une étude de ses activités et de son secteur, afin de déterminer le cadre juridique dans lequel elle s'inscrit</p>	<p>Une soutenance orale qui permet d'évaluer les compétences 1, 2, 3, 4 et 5.</p> <p>Le candidat présente oralement sa production liée aux cas étudiés devant le jury d'évaluation. Le ou les cas devront porter sur l'analyse du secteur d'activité et l'identification des risques et de conformité de l'entreprise. Le choix de présenter une ou plusieurs situations professionnelles et / ou pédagogique est laissé à la discrétion du candidat.</p>	<p>Le contexte et le cadre juridique de l'entreprise sont identifiés et compris :</p> <ul style="list-style-type: none"> ● Une analyse sectorielle de l'entreprise est réalisée ● Une analyse de l'écosystème de l'entreprise est établie ● Le cadre juridique de l'entreprise vis-à-vis de la protection des données personnelles est identifié ● Les sources utilisées pour la veille sont fiables (CNIL, DALLOZ, ...)

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

	<p>C2. Réaliser une analyse d'impact relative à la protection des données personnelles en recensant les traitements effectués et leur importance, afin de sécuriser les données traitées de façon optimale</p>	<p>La présentation est suivie d'un temps d'échanges et de questions où le jury peut approfondir des détails relatifs aux cas présentés pour s'assurer de la maîtrise des compétences par le candidat.</p> <p>La soutenance dure une heure et trente minutes, décomposée en quarante-cinq minutes de présentation par le candidat de ses productions et quarante-cinq minutes d'échanges et de questions avec le jury d'évaluation.</p>	<p>L'analyse d'impact est menée et qualifiée :</p> <ul style="list-style-type: none"> ● L'analyse de l'entreprise permet de recenser l'ensemble des données personnelles traitées ● Les données traitées sont qualifiées (ordinaires, sensibles...) ● Les mesures de sécurité proposées sont adaptées aux types de données traitées et aux types de personnes concernés
<p>A2. Identification des risques de sécurité et de conformité de l'entreprise</p> <ul style="list-style-type: none"> ● Détermination d'une matrice de risque en lien avec la réglementation en vigueur (RGPD, loi informatique et libertés, ...) ● Etablissement du plan de traitement des risques ● Définition de la politique de protection des données 	<p>C3. Identifier les risques de sécurité et de conformité de l'entreprise en s'appuyant sur une méthode d'analyse de risque, afin d'avoir une vision exhaustive des risques potentiels encourus par l'organisation</p>		<p>Les risques de sécurités sont identifiés, qualifiés et priorisés :</p> <ul style="list-style-type: none"> ● L'identification des risques est complète ● La matrice de risques est construite en prenant en compte la réglementation en vigueur (RGPD, loi informatique et libertés, ...) ● Les risques majeurs pour l'organisation sont déterminés et argumentés

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

	<p>C4. Établir un plan de traitement de risques en élaborant une matrice en lien avec la réglementation en vigueur, afin de prioriser les risques majeurs pour l'organisation</p> <p>C5. Définir la politique de protection des données personnelles en déterminant les objectifs et les moyens et en s'appuyant sur la réglementation en vigueur, afin de l'adapter aux risques et à la nature des opérations de traitement</p>		<p>Le plan de traitement des risques est établi :</p> <ul style="list-style-type: none">● Un document détaillant les mesures prises est réalisé● L'ensemble des risques sont identifiés et classifiés● Des mesures de mitigation sont proposées et permettent de réduire les risques <p>La politique de protection des données est définie :</p> <ul style="list-style-type: none">● Les objectifs de la politique de protection des données sont déterminés et argumentés en regard des risques de sécurité et de non-conformité encourus● Les exigences établies prennent en compte les nouveautés légales et doctrinales● Les moyens à allouer sont déterminés
--	--	--	---

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

BLOC 2 : Implémentation d'une politique de sécurité et de conformité des données personnelles

REFERENTIEL D'ACTIVITES <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	REFERENTIEL DE COMPETENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	REFERENTIEL D'ÉVALUATION <i>définit les critères et les modalités d'évaluation des acquis</i>	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>A1. Mise en place d'un registre de traitement des données personnelles</p> <ul style="list-style-type: none"> ● Création et maintien à jour du registre de traitements des données personnelles ● Recensement de l'ensemble des données personnelles traitées par l'organisation ainsi que leurs responsables ● Intégration d'une politique de sécurité ● Tenue des registres dès la conception au titre de l'accountability 	<p>C1. Mettre en place et maintenir à jour un registre de traitement des données en recensant les données personnelles traitées par l'entreprise et en identifiant les responsables de traitement, afin d'assurer la traçabilité des données et d'être en conformité avec la réglementation en vigueur</p> <p>C2. Intégrer la politique de sécurité et la conformité dans le Système d'Information en définissant et en appliquant un plan d'actions, afin de permettre la mise en conformité de l'existant</p>	<p>Une soutenance orale qui permet d'évaluer les compétences 1, 2, 3, 4, 5, 6, 7 et 8.</p> <p>Le candidat présente oralement sa production liée aux cas étudiés devant le jury d'évaluation. Le ou les cas devront porter sur la mise en place d'un registre de traitement, le suivi et l'ajustement du plan d'action et de la politique de protection des données personnelles, la cartographie du flux de données et la gestion de contrat avec des tiers. Le choix de présenter une ou plusieurs situations professionnelles et / ou pédagogique est laissé à la discrétion du candidat.</p>	<p>Le registre de traitement des données est mis en place :</p> <ul style="list-style-type: none"> ● Les différents outils de gestion de la conformité sont étudiés ● Le choix de l'outil choisi est explicite ● L'ensemble des traitements de données personnelles opérés par l'organisation sont recensés ● Les responsables des traitements sont identifiés <p>Le système d'information intègre la politique de sécurité et la conformité :</p> <ul style="list-style-type: none"> ● Les procédures de sécurité / de mise en conformité sont déterminées dans le respect de la politique de protection des données ● Les personnes impliquées sont déterminées

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

	<p>C3. Formaliser les mesures de protection des données dès la conception, en les adaptant aux risques et à la nature des opérations de traitement et en tenant les registres à jour, afin d'éviter les incidents de sécurité et de conformité</p>	<p>La présentation est suivie d'un temps d'échanges et de questions où le jury peut approfondir des détails relatifs aux cas présentés pour s'assurer de la maîtrise des compétences par le candidat.</p> <p>La soutenance dure une heure et trente minutes, décomposée en quarante-cinq minutes de présentation par le candidat de ses productions et quarante-cinq minutes d'échanges et de questions avec le jury d'évaluation.</p>	<ul style="list-style-type: none"> ● La période de réalisation est fixée ● Les critères de réussite du plan d'action sont définis <p>Les mesures de protection des données sont formalisées :</p> <ul style="list-style-type: none"> ● Les mesures de protection des données sont adaptées à la nature des opérations de traitement créées. ● Les mesures de protection sont systématisées dès la conception (Security by Design) ● Un registre documentant l'ensemble des mesures et opérations de traitement est établi.
<p>A2. Suivi et ajustement du plan d'action et de la politique de protection des données personnelles</p> <ul style="list-style-type: none"> ● Détermination d'indicateurs de suivi ● Révision des procédures de sécurité et de conformité ● Mise en place d'actions correctives 	<p>C4. Assurer le suivi de l'application de la politique de protection des données personnelles à l'aide d'outils de traçabilité de la sécurité et de la conformité de l'entreprise, afin d'identifier et de mesurer les éventuels écarts</p>		<p>La mise en place de la politique de protection des données est monitorée :</p> <ul style="list-style-type: none"> ● Des outils de suivi sont mis en place, leur choix est justifié ● Les éventuels écarts sont identifiés, leurs caractéristiques sont explicitées

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

	<p>C5. Réviser les procédures de sécurité, de conformité et la politique de protection des données en identifiant l'évolution de la réglementation et des facteurs de risques de l'organisation, afin de les réduire</p>		<p>Des mises à jour sont proposées pour assurer la conformité de la politique de protection des données :</p> <ul style="list-style-type: none"> ● Des modifications sont formulées et permettent d'assurer la poursuite du plan d'action ● Les modifications formulées prennent en compte l'évolution éventuelle de la réglementation et des facteurs de risques de l'organisation
<p>A3. Cartographie des flux de données de l'entreprise</p> <ul style="list-style-type: none"> ● Détermination de l'origine des données ● Vérification de la destination des données ● Définition des actions à entreprendre ● Analyse du type de données 	<p>C6. Cartographier les flux de données en indiquant leur origine et leur destination, afin de tracer l'ensemble des données traitées et d'identifier les éventuels transferts de données hors de l'Union européenne</p> <p>C7. Définir des actions à mener en analysant la nature des données traitées, afin d'assurer une protection optimale des données</p>		<p>Les différents flux de données sont cartographiés :</p> <ul style="list-style-type: none"> ● Une matrice permet de visualiser les flux de données ● L'ensemble des flux sont répertoriés ● Les transferts de données en dehors de l'UE sont identifiés <p>La nature des données est analysée et permet une protection optimale des données :</p> <ul style="list-style-type: none"> ● L'ensemble des données sont analysées ● Les actions définies sont différentes en fonction du type

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

			<p>de données analysées (données sensibles, données de santé, handicap...)</p> <ul style="list-style-type: none"> ● Des outils juridiques de transfert de données ont été mis en place (BCR, CCT, Décisions d’approbation...) ● Le choix des outils de transfert mis en place est justifié
<p>A4. Gestion des contrats avec les tiers</p> <ul style="list-style-type: none"> ● Identification du cadre juridique applicable (UE, hors UE...) ● Etablissement des clauses de sécurité du contrat 	<p>C8. Gérer les contrats avec les sous-traitants et les clients du point de vue de la protection des données personnelles, en s’appuyant sur une identification du cadre juridique applicable, afin de sécuriser la contractualisation</p>		<p>Les contrats sont établis et posent le cadre juridique de la protection des données personnelles applicable :</p> <ul style="list-style-type: none"> ● Le cadre juridique applicable est identifié (UE, hors UE, ...) ● Le respect du droit des propriétaires des données est évalué ● Les préconisations de corrections ou amendements sont argumentés en regard de la mise en conformité du contrat.

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

BLOC 3 : Gérer un incident de sécurité et/ou de conformité de protection des données personnelles

REFERENTIEL D'ACTIVITES <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	REFERENTIEL DE COMPETENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	REFERENTIEL D'ÉVALUATION <i>définit les critères et les modalités d'évaluation des acquis</i>	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>A1. Assurer le suivi de l'incident</p> <ul style="list-style-type: none"> ● Suivi et documentation des actions entreprises ● Interaction et réponse aux sollicitations avec la CNIL 	<p>C1. Assurer le suivi de la résolution de l'incident, en déterminant les personnes concernées en fonction de la nature de la faille en documentant et en suivant l'ensemble des actions entreprises à l'aide d'outils de traçabilité, afin d'être en capacité de rendre compte des démarches de résolution mises en oeuvre pour éviter qu'un incident similaire se reproduise</p> <p>C2. Assurer le lien avec la CNIL en répondant à ses sollicitations et en collaborant lors de l'instruction des plaintes et des missions de contrôle, afin de se conformer à la législation en vigueur</p>	<p>Une soutenance orale qui permet d'évaluer les compétences 1, 2, 3, et 4.</p> <p>Le candidat présente oralement sa production liée aux cas étudiés devant le jury d'évaluation. Le ou les cas doivent porter sur la gestion d'incident de sécurité et / ou de conformité, de protection des données personnelles (suivi de l'incident, création et maintien du registre de violation des données personnelles). Le choix de présenter une ou plusieurs situations professionnelles et / ou pédagogique est laissé à la discrétion du candidat.</p> <p>La présentation est suivie d'un temps d'échanges et de questions où le jury peut approfondir des détails relatifs aux cas présentés afin</p>	<p>Les différentes actions de suivi d'incident sont menées :</p> <ul style="list-style-type: none"> ● Les personnes concernées par l'incident de sécurité et/ou de conformité sont identifiées et informées ● L'ensemble des actions entreprises sont documentées à l'aide d'outils de traçabilité ● Le choix des outils de traçabilité est argumenté en fonction de la nature de l'incident ● Des préconisations argumentées sont formulées afin d'éviter qu'un incident similaire se reproduise <p>Les procédures de suivi d'incident en lien avec la CNIL sont mises en place et respectées :</p> <ul style="list-style-type: none"> ● La nature de l'incident est présentée dans un courrier à la CNIL ● La résolution de la faille de sécurité est justifiée à l'aide de la

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

		<p>de s'assurer de la maîtrise des compétences par le candidat.</p> <p>La soutenance dure une heure et trente minutes, décomposée en quarante-cinq minutes de présentation par le candidat de ses productions et quarante-cinq minutes d'échanges et de questions avec le jury d'évaluation.</p>	<p>documentation des actions entreprises</p> <ul style="list-style-type: none"> ● Le respect du RGPD est démontré à l'aide des outils et des processus de l'organisation
<p>A2. Création et maintien à jour du registre de violation de données personnelles</p> <ul style="list-style-type: none"> ● Identification des personnes concernées dans la chaîne de la gestion de crise ● Mise en place d'un registre de violation des données ● Réponse aux sollicitation de l'autorité de contrôle en cas de besoin ● Communication de l'incident auprès de la victime ● Mise en place de mesures de résolution 	<p>C3. Identifier les données personnelles violées en récoltant les informations liées à l'incident auprès des différents services métier, afin de maintenir à jour le registre de violation des données</p>		<p>Le registre de violation des données est tenu :</p> <ul style="list-style-type: none"> ● Les données personnelles violées sont identifiées ● Le choix de l'outil de gestion du registre de violation est justifié ● Le maintien en conformité est prouvé

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

	<p>C4. Communiquer l'incident auprès de la personne concernée par la faille en l'informant du préjudice et des mesures de résolution mises en place, afin qu'elle puisse exercer ses droits</p>		<p>La personne concernée par la faille est informée du préjudice :</p> <ul style="list-style-type: none">● Le préjudice causé est explicité auprès de la personne concernée par la faille● Les mesures de résolution entreprises sont communiquées● Les demandes d'exercices de droits sont prises en compte
--	---	--	---

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

	<p>rester informé et d'anticiper les changements à mettre en œuvre dans l'entreprise</p>	<p>aux cas présentés afin de s'assurer de la maîtrise des compétences par le candidat.</p> <p>La soutenance dure une heure et trente minutes,</p>	<ul style="list-style-type: none"> ● Les plateformes de textes juridiques francophones et anglophones sont connues ● Les nouveaux textes de lois sont étudiés de façon approfondie
<p>A2. Information des droits des personnes concernées par le traitement de données personnelles</p> <ul style="list-style-type: none"> ● Intégration des mentions légales ● Intégration de formulaires d'autorisation (explicite ou implicite) ● Mise en place de moyen de demande d'exercice de droits des personnes ● Etablissement de procédures permettant d'exécuter les demandes d'exercice de droits 	<p>C3. Informer les propriétaires de l'utilisation de leurs données personnelles en intégrant les modalités d'usage dans les mentions légales, afin de respecter le principe de transparence</p> <p>C4. Établir des procédures de demande d'exercice de droits des personnes en mettant en place des moyens de communication, afin de permettre aux usagers de pouvoir exercer leurs droits</p>	<p>La soutenance dure une heure et trente minutes, décomposée en quarante-cinq minutes de présentation par le candidat de ses productions et quarante-cinq minutes d'échanges et de questions avec le jury d'évaluation.</p>	<p>Les utilisateurs sont informés de leurs droits concernant l'utilisation de leurs données personnelles :</p> <ul style="list-style-type: none"> ● Les mentions légales rédigées respectent le cadre réglementaire applicable ● Les mentions légales sont visibles et accessibles pour tous (format adapté aux personnes en situation de handicap) ● Le formulaire d'autorisation explicite ou implicite est établi. Le type de formulaire retenu est justifié au regard de la jurisprudence <p>Des moyens sont mis en place pour permettre aux propriétaires des données d'exercer leurs droits :</p> <ul style="list-style-type: none"> ● Les propriétaires sont clairement informés de la façon dont ils peuvent exercer leurs droits ● Les moyens mis en oeuvre sont explicités

ÉLÉMENTS COMPLÉMENTAIRES RELATIFS A LA DEMANDE

			<ul style="list-style-type: none"> ● Des procédures de traitements des demandes d'exercice de droits sont établies
<p>A3. Accompagnement de la sous-traitance</p> <ul style="list-style-type: none"> ● Audit des moyens mis en œuvre par le sous-traitant permettant d'assurer sécurité et conformité ● Conseil sécurité et conformité et alerte aux sous-traitants 	<p>C5. Auditer les sous-traitants en vérifiant les moyens mis en œuvre, afin de s'assurer de la sécurisation et de la conformité des données personnelles traitées</p>		<p>Les sous-traitants sont audités et conseillés dans le but de rester en conformité :</p> <ul style="list-style-type: none"> ● Les points clés de l'audit sont explicités ● Les moyens mis en œuvre par le sous-traitant sont évalués ● Les manquements éventuels de la part du sous-traitant sont identifiés ● Des conseils et alertes sont promulgués et permettent de tendre vers plus de sécurité et de conformité des DCP