Référentiel de compétences et d'évaluation

Analyse et pilotage stratégique du projet de mise en conformité de la gestion de données

Analyse du périmètre d'intervention du projet de mise en conformité de la gestion de données.		
Compétences professionnelles	**Modalités d'évaluation**	**Critères d'évaluation**
C1. Analyser les responsabilités et les risques liés à l'exercice de la gestion de données en s'appropriant le cadre réglementaire et juridique de la protection des données personnelles pour le placer dans une perspective historique, européenne et internationale, ainsi que politique et sociétale.	**Me1. Évaluation composante 1** **Mode :** Évaluation orale sur la compréhension des enjeux d'un projet de mise en conformité de la gestion de données. **Durée :** 15 minutes de préparation et 20 minutes de soutenance orale **Modalités d'évaluation :** Il est demandé au candidat de déterminer et de décrire le cadre réglementaire dans lequel s'inscrivent différentes organisations en matière de traitement de gestion des données (RGPD, flux hors Union Européenne…) et les risques encourus par ces organisations en cas de non-conformité. Le candidat est également challengé sur ses responsabilités et son périmètre d'action.	Le candidat identifie le cadre règlementaire, au plan national, et au plan européen, notamment l'attendu du RGPD, et leurs applications dans la pratique. Les enjeux de la protection des données personnelles pour une organisation et les risques encourus en cas de non-conformité sont identifiés. Le candidat priorise et catégorise les risques. Il démontre une capacité à arbitrer entre les différents enjeux. La présentation orale est de qualité : • Le candidat s'exprime avec clarté. • Sa prise de parole et posture sont professionnelles. • Il communique de façon pédagogique et positive
C2. Analyser les spécificités et les champs d'application du Règlement Général de la Protection des Données (RGPD) pour identifier les obligations applicables à une organisation selon son secteur d'activités, la nature de sa structure et son		Le candidat identifie les obligations applicables issues du RGPD applicables aux caractéristiques liées à son organisation et son secteur d'activité.

implantation.		Le candidat démontre une capacité à intégrer les spécificités de son environnement.
C3. Définir le périmètre d'intervention et les enjeux de la mise en conformité de la gestion des données pour avoir la capacité de l'assumer de manière efficace afin d'apporter une stratégie d'accompagnement pérenne dans la mise en conformité des données personnelles.		Le candidat démontre la capacité de décrire le périmètre d'intervention dévolu à la mise en conformité de la gestion de données.
C4. Assurer une veille permanente sur le thème de la protection des données personnelles pour disposer de l'expertise requise sur les plans juridique, technique, opérationnel et sectoriel, dans un cadre national et international.		Le candidat sélectionne des sources multiples (françaises et internationales) et fiables sur la protection des données. Les sources sont suivies de manière assidue et régulière. Elles sont de nature variée, nationales et internationales. Elles permettent une mise à jour continue de l'expertise juridique, technique, opérationnel et sectoriel en matière de protection des données.

Référentiel de compétences et d'évaluation

Analyse et pilotage stratégique du projet de mise en conformité de la gestion de données

Analyse des risques dans l'organisation cible		
C5. Identifier les acteurs, les services et les parties prenantes (internes et externes) traitant les données pour organiser le recueil d'informations auprès des responsables concernés par la gestion des données personnelles de l'organisation.	**Me2. Évaluation Composante 2** **Mode :** Évaluation écrite et orale sur l'analyse de l'existant et l'établissement d'une cartographie des risques à partir d'une étude de cas pratique. **Durée :** 1 heure. **Modalités d'évaluation :** A partir d'un cas pratique, il est demandé au candidat de procéder à une analyse : . Des acteurs, fonctions et services stratégiques impliqués dans le traitement de données. . Des données en fonction de leur sensibilité. . Des traitements depuis la collecte jusqu'au stockage. Il est demandé au candidat d'élaborer une cartographie et une hiérarchisation des risques et de produire une analyse de la situation existante en identifiant les points de non-conformité.	Le candidat identifie les fonctions, acteurs et services impliqués dans le traitement des données (représentant, sous-traitants, co-responsables, etc.). Les données sont catégorisées en fonction de leur nature et de leur sensibilité. Les catégories sont les suivantes : - la finalité - la sensibilité - qui est responsable de traitement - qui accède aux données - qui sont les destinataires - durée de conservation - comment elles sont sécurisées - information sur les droits - auprès de qui et comment exercer les droits des personnes - coordonnées du dpo - éventuels transferts hors UE Les traitements et flux sont repérés de manière exhaustive. Les aspects juridiques et techniques sont traités dans la cartographie des risques. La hiérarchisation des risques est correctement justifiée.

		Les non-conformités sont repérées, traitées et s'appuient sur la réglementation en vigueur.
C6. Recenser les fonctions et les activités de l'organisation nécessitant le traitement de données personnelles pour réaliser l'inventaire des traitements utilisés, depuis la collecte jusqu'à l'archivage.		Le candidat justifie d'une capacité à tracer le flux des données et les activités de traitement au sein de l'organisation. Il organise la collecte des données à l'aide de questionnaires d'audit, d'interviews, ateliers en groupes de travail/brainstorming, d'analyse de documentation pertinente (architecture informatique…) Toutes les activités nécessitant de traiter des données personnelles sont listées de façon exhaustive dans un registre.
C7. Dresser une classification des données personnelles en fonction de leur intérêt, de leur sensibilité, des durées et des modalités de conservation pour évaluer l'existant et établir la cartographie des risques.		Le candidat maîtrise la qualification des données et le régime juridique qui leurs est applicable selon leur utilisation par et/ou pour l'organisation : • Il est en mesure de procéder à une évaluation des risques pour chaque catégorie et usage de données. • Pour chaque traitement, il identifie la base juridique parmi les six bases légales prévues par le RGPD : le consentement, le

		contrat, l'obligation légale, la sauvegarde des intérêts vitaux, l'intérêt public et les intérêts légitimes.
C8. Analyser le niveau de protection et de sécurisation des données pour détecter d'éventuelles non-conformités de leur traitement avec le règlement général des données personnelles.		• Le candidat justifie d'une maîtrise des enjeux et standards sécurité fixés par la CNIL et l'ANSSI • Le candidat sait apprécier le niveau de sécurisation suffisant des données au regard des exigences réglementaires.
C9. Hiérarchiser les risques à partir de la cartographie pour organiser des analyses d'impact (Data Protection Impact Assessment) sur les traitements de données présentant un risque élevé afin de décider de procédures correctives.		Le candidat connaît les critères relatifs à l'exigence de mise en œuvre des analyses d'impacts : • Il suit la méthodologie à appliquer telle que recommandée par la CNIL et notamment le logiciel libre mis à disposition par la CNIL (méthodo EBIOS recommandée par la CNIL) • Il identifie si le traitement envisagé figure dans la liste des types d'opérations de traitement dispensées d'analyse d'impact. L'analyse d'impact est complète : • Elle donne une description du traitement mis en œuvre ;

		• Une évaluation juridique (finalité, données et durées de conservation, information et droits des personnes, etc.), • Une étude technique des risques de sécurité (confidentialité, intégrité et disponibilité). Le candidat définit les mesures correctives fondamentales à mettre en œuvre.
Élaboration et mise en place d'un plan de conformité		
C10. Élaborer un « plan de conformité » en s'appuyant sur des recommandations fonctionnelles, organisationnelles et techniques pour mettre aux normes la gestion des données personnelles d'une organisation.	**Me3. Évaluation composante 3** **Mode :** Évaluation écrite et orale sur l'élaboration et la mise en place d'un plan de conformité à partir d'un cas pratique. **Durée :** 2 heures. **Modalités d'évaluation :** Il est demandé au candidat d'élaborer plusieurs éléments : • un « plan de conformité »	Le « plan de conformité » est de qualité : - Le plan de conformité répond aux exigences réglementaires. - Il intègre la gestion et la hiérarchisation des risques. - Il est réaliste au regard des caractéristiques et spécificités de la structure.

C11. Élaborer un « plan d'actions de conformité » de la gestion des données personnelles et calibrer les moyens nécessaires pour planifier et organiser la mise en place des procédures techniques et organisationnelles de sécurisation et de protection des données personnelles répondant aux exigences de la règlementation.	• un « plan d'actions de conformité » en cohérence avec le cas pratique soumis.	Le « plan d'actions de conformité » rédigés sont complets et répondent aux exigences de la règlementation. Le plan d'action est opérationnel. Il prévoit un rétroplanning raisonnable. Le plan d'actions mentionne les personnes en charge de la mise en œuvre et du contrôle de la bonne réalisation
C12. Concevoir les scenarii de crise, le PCA (plan de continuité d'activité) et le PRA (plan de reprise d'activité) pour mettre en place les mesures adéquates permettant d'assurer la poursuite et la reprise des activités ainsi que l'accès aux données dans des situations critiques.	• Scenarii de crise • Recommandations	Les scenarii d'interruption de service et les moyens d'y remédier pour assurer une continuité de l'activité sont maîtrisés. Le candidat connaît les principaux enjeux et risques qui doivent être couverts
C13. Rédiger les mentions légales et adapter les documents contractuels, y compris ceux concernant les prestataires, pour les mettre en correspondance avec les obligations légales.	• Les situations critiques et les procédures de remédiation en	Le candidat montre sa capacité à rédiger des mentions légales et à mettre en conformité des documents contractuels.

	cas d'interruption de service doivent être décrites et analysées par le candidat. • Le candidat est challengé sur la documentation à tenir, les accès aux données personnelles à prévoir et les clauses légales à rédiger.	Les mentions légales mentionnent : - Les caractéristiques du traitement y compris la durée de conservation - Les acteurs (responsable de traitement, catégories de destinataires) - Les droits des personnes - Mention compréhensible, lisible et accessible
C14. Mettre en place les modalités d'accès aux données pour l'exercice des droits sur les données personnelles (droit d'accès, droit de rectification, droit à la portabilité, retrait du consentement, droit d'effacement) imposés par la CNIL (loi Informatique et Libertés) et par le RGPD.		Les modalités d'exercice sont effectives et efficaces. Les modalités d'exercice tiennent compte des caractéristiques du traitement.
C15. Alimenter le registre des traitements et organiser la documentation interne sur les traitements des données personnelles et leurs incidents (violation de données) afin de se mettre en conformité avec le RGPD et assurer la traçabilité des évènements en cas de contrôle.		Le candidat identifie les informations requises devant figurer dans le registre. Il justifie de capacités à collecter les informations pertinentes permettant d'alimenter le registre. Il applique les méthodes d'audit des services et personnes en charge d'activités de traitement de données à caractère personnel. Questionnaires d'audit et interviews + ateliers en petits groupes de travail/brainstorming Il identifie les procédures et politiques encadrant les processus de collecte et

		gestion des données (politique de confidentialité, référentiel de durée de conservation, politique de sécurité des données, procédure de gestion des incidents et violations de données) La nécessité de tenue d'une documentation complète et les contraintes légales d'accès aux données est prise en compte.
Pilotage et suivi du plan de conformité de la gestion des données		
C16. Mettre en place et animer un cadre opérationnel de pilotage et de gouvernance de la conformité pour garantir l'application et la réussite du plan de conformité de l'organisation, à l'aide des techniques et la méthodologie de conduite du changement pour garantir et optimiser la mise en place du « plan de conformité ».	**Me4. Évaluation composante 4** **Mode :** Évaluation orale sur le pilotage et le suivi du « plan de conformité ». **Durée :** 1 heure de préparation et 30 minutes de présentation. **Modalités d'évaluation :** Il est demandé au candidat de proposer une démarche de conduite du changement pour impliquer et fédérer les parties prenantes sur la mise en place et le suivi du « plan de conformité ».	Le candidat montre sa capacité à communiquer de manière pédagogique et positive sur la mise en place et le suivi d'un « plan de conformité ». Les techniques et la méthodologie de conduite du changement sont utilisées. Les conditions à mettre en place pour garantir la fluidité et l'efficacité dans les échanges avec les organismes de contrôle sont acquises. Le candidat montre sa capacité à contrôler le « plan de conformité » et à adapter les actions en fonction du contexte.

SciencesPo EXECUTIVE EDUCATION

Référentiel de compétences et d'évaluation

Analyse et pilotage stratégique du projet de mise en conformité de la gestion de données

C17. Élaborer des programmes de formation et de sensibilisation auprès des parties prenantes (internes et externes) pour les fédérer autour des enjeux du « plan de conformité » afin de l'**i**nscrire efficacement et durablement dans la politique de l'organisation.	Le candidat est challengé sur les conditions à mettre en place pour anticiper les signalements et limiter les risques de contrôle et de sanctions.	Les contenus des formations sont conformes aux exigences réglementaires et aux recommandations de la CNIL et l'ANSSI sur les aspects sécurité. Les formations sont adaptées aux services et personnes concernées. Les formations intègrent un contrôle des connaissances.
C18. Mettre en place des process de signalement et de notification de violation des données personnelles pour instruire les situations contentieuses et les signalements aux autorités de contrôle afin de limiter les risques de sanctions civiles, pénales et administratives.		Le candidat qualifie une violation de données personnelles. Il applique les conditions de notification à l'autorité de contrôle ainsi que de communication aux personnes concernées.
C19. Contrôler, via des audits internes, le respect du « plan de conformité » de gestion des données personnelles afin de mesurer l'efficacité des actions mises en place et les améliorer, le cas échéant.		Le candidat a une vision sur la fréquence des audits de contrôles compatible avec les spécificités et la culture de l'organisation. Le candidat applique les outils et méthodes de contrôle de conformité. Questionnaires d'audit et interviews + ateliers en petits groupes de travail/brainstorming