AFINUM wis®

REFERENTIELS D'ACTIVITES, DE COMPETENCES ET D'EVALUATION

« Délégué à la protection des Données – Data Protection Officer (DPD/DPO) »

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. »

Articulation en blocs de compétences :

Bloc 1 : Auditer les politiques, les pratiques de gestion (des données) et la conformité des processus de traitement des données (*Compétences C1 à C9)*
Bloc 2 : Piloter la conformité des traitements de données mis en œuvre par l'organisation (*Compétences C10 à C16)*
Bloc 3 : Conseiller et accompagner l'organisation pour garantir la conformité réglementaire en matière de protection des données (*Compétences C17 à C23)*
Bloc 4 : Déployer les actions préventives et correctives en cas de violations liées à la protection des données (*Compétences C24 à C31)*

Intitulé : Délégué à la Protection des Données – Data Protection Officer (DPD/DPO)

REFERENTIEL D'ACTIVITES *Décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *Identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *Définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
Activité 1 - Analyse et audit des politiques de l'organisation, des pratiques de gestion des données - Analyse de la structure de l'organisation en lien avec la politique de protection des données ; - Analyse des besoins de l'organisation en termes de sécurité et de conformité ; - Veille technique, légale et juridique ; - Audit régulier de conformité des traitements de données de l'organisation ; - Vérification de la bonne application des mesures de protection ;	C1 Analyser les spécificités de l'organisation en identifiant les rôles et responsabilités des parties prenantes, les activités, l'écosystème, les besoins afin de déterminer le cadre réglementaire et légal applicable en matière de protection des données (RGPD) et les sources (personnes, services) de traitements de données au sein de l'organisation.	**Mise en situation professionnelle reconstituée** A partir d'un cahier des charges précisant les besoins d'une organisation fictive, le candidat élabore un dossier comprenant : - Un organigramme fonctionnel dans lequel est présenté le rôle de chaque ressource dans la mise en place d'une politique de protection de données ; - Une analyse diagnostique de la sécurité du système d'information par la production d'une cartographie ; - Tout ou partie d'un rapport d'audit de conformité en fonction du périmètre du cahier des charges ; - Le périmètre de l'audit et les critères d'évaluation ; - Une présentation des dispositifs de surveillance mis en place ;	- L'organigramme fonctionnel des différents services de la structure comprend de manière exhaustive les ressources humaines en lien avec la gestion des données personnelles ; - Les rôles et responsabilités de chacun dans la mise en place de la politique de protection des données, de manière directe ou indirecte, sont précisés ; - Les besoins sont déterminés en fonction de l'écosystème ; - L'organigramme permet de déterminer le cadre règlementaire et légal applicable et les sources (personnes, services...) des traitements des données personnelles.
	C2 Analyser le système d'information (SI) existant au sein de la structure dans son intégralité, selon une méthode d'analyse adaptée et en établissant une cartographie, afin d'établir un diagnostic sur le système étudié.		- La méthode d'analyse (Merise, ou autre) est décrite et adaptée au SI de l'organisation ; - La cartographie présente de manière exhaustive les processus métier de la structure et précise les couches fonctionnelle, applicative et technologique du SI ; - Un outil de cartographie est mobilisé qui permet de mettre en valeur les imbrications et les interdépendances entre les multiples composantes du système d'information (SI) et ses différentes couches.
	C3 Effectuer une veille continue sectorielle, technologique, légale et réglementaire sur la protection des données en s'appuyant sur un processus organisé et en mobilisant des outils de veille et des sources d'informations fiables et diversifiées afin de pouvoir mesurer la conformité des processus de traitement des données de l'organisation et réaliser un audit de conformité.		Le candidat présente une proposition de processus de veille sectorielle, technologique, légale et réglementaire : - Des sources d'information fiables concernant le RGPD et le Data Act sont identifiées ; - Une méthodologie de veille est préconisée (méthode push, méthode pull d'information) ; - Un outil de veille (Feedly, Netvibes, Google alert…) est mobilisé ; - Les informations recueillies sont analysées et synthétisées ; - Un plan de diffusion de la veille est établi, qui permet de diffuser l'information à toutes les cibles identifiées ;

- Mesure de l'efficacité des actions mise en œuvre.		- Un processus de veille sectorielle, technique et juridique dans le domaine de la protection des données personnelles adapté au cas de l'organisation, le plan de diffusion de la veille et la synthèse d'une veille ; - Le plan d'un rapport d'évaluation des risques et quelques éléments l'illustrant ; - Une liste des anomalies constatées et une synthèse concernant les tests réalisés ; - Une matrice de conformité ; - Un rapport de tests techniques ; - Une partie d'un plan d'actions correctives. Le dossier sera présenté à l'oral.	- La synthèse rédigée présente les informations à forte valeur ajoutée et vulgarise les termes juridiques.
	C4 Réaliser un audit des mesures de sécurité des données existantes en réalisant des enquêtes et interviews et en analysant la base documentaire disponible afin de mettre en évidence les dysfonctionnement éventuels ou anomalies du SI existant.		- Les méthodes de contrôle d'accès au SI et de sauvegarde de données existantes sont listées de manière exhaustive et analysées ; - Le processus de traçabilité et les méthodes de chiffrement existants sont présentés et une analyse en est faite ; - Le plan d'audit de sécurité des données présenté est conforme à la méthode MEHARI (MEthode HArmonisée d'Analyse des Risques) ; - L'audit présente des indicateurs d'évaluation mesurables et représentatifs qui permettent une analyse objective.
Activité 2 – Évaluation des politiques de gestion des données de l'organisation - Mesure de l'efficacité des actions mises en œuvre - Analyse des résultats d'audit - Rédaction des livrables de l'audit de conformité - Plan d'actions de mise en conformité	C5 Rédiger un rapport d'audit de conformité comprenant les objectifs de l'audit, le périmètre, la méthodologie, les résultats et les constats effectués afin d'identifier des écarts mineurs ou majeurs en vue d'apporter des corrections et d'assurer une mise en conformité.		**Critères sur la forme :** - Le rapport d'audit est structuré et détaillé ; - Il est rédigé dans un langage simple et accessible (les termes techniques sont définis). **Critères sur le fond :** - Le périmètre de l'audit est défini ; - Les objectifs de l'audit sont précisés ; - La méthodologie d'audit est expliquée et argumentée ; - Les constats effectués sont indiqués de manière exhaustive, factuelle et détaillée ; - Des recommandations pratiques et actionnables sont formulées en fonction des résultats de l'audit ; - Un plan de mise en œuvre des recommandations est proposé.
	C6 Rédiger un rapport d'évaluation des risques en les classifiant en fonction de leur degré gravité et de leur impact, en décrivant les scénarios potentiels en cas d'incident de sécurité et en proposant des mesures pour réduire ou éliminer ces risques afin de détailler les risques identifiés lors de l'audit et permettre de déterminer les impacts des non-conformités relevés.		Le plan de rapport d'évaluation des risques proposé : **Critères sur la forme :** - Est structuré et rédigé dans un langage simple et accessible (les termes techniques sont définis) ; - Respecte le formalisme demandé dans le cahier des charges. **Critères sur le fond :** - Est à même d'être mis en place dans l'organisation présentée dans le cahier des charges ;

			- Présente de manière détaillée jusqu'a 3 risques majeurs pour l'organisation en indiquant leurs causes, en tenant compte des différents domaines concernés, et en identifiant les impacts des non-conformités ; - Les raisons pour lesquelles chaque risque a été identifié sont expliquées ; - Une méthodologie d'évaluation des risques adaptée au cas de l'organisation et qui pourra être utilisée par l'organisation est présentée.
	C7 Réaliser la matrice de conformité en listant les exigences légales et réglementaires, en évaluant le niveau de conformité et en indiquant les écarts identifiés afin de cartographier la conformité de l'organisation par rapport aux exigences réglementaires.		La matrice de conformité élaborée par le candidat : - Couvre tous les articles clefs du RGPD qui s'appliquent à l'organisation ; - Précise chaque exigence pour une vérification complexe ; - Indique la mise à jour et la version du document ; - Précise les points de conformité associés aux articles du RGPD de façon explicite ; - Comprend des termes techniques vulgarisés ; - Détermine le statut de chaque exigence de manière standardisée ; - Indique pour chaque exigence conforme, la matrice des preuves ou documents justificatifs ; - Propose pour chaque exigence non conforme, des recommandations concrètes, pratiques et adaptées au contexte de l'organisation.
	C8 Réaliser un rapport de tests techniques en résumant les tests mis en œuvre en collaboration avec le Responsable de la Sécurité du Système d'Information (RSSI) (tests d'intrusions, test de vulnérabilité, audit des systèmes de sécurité) et le résultat des tests afin de permettre d'établir des recommandations techniques et de définir le calendrier de remédiation associé.		Le rapport de tests techniques : - Détaille les types de tests effectués ; - Explicite et argumente la fiabilité des tests choisis au regard des objectifs de l'audit et de la réglementation ; - Mentionne les résultats de tous les tests effectués, y compris les tests réussis et échoués, afin de fournir une vision complète ; - Décrit les outils et techniques de tests utilisés ; - Mentionne les contraintes rencontrées pendant les tests.
	C9 Proposer un plan d'actions correctives en décrivant les actions à entreprendre, les responsables des actions, le calendrier de mise en œuvre et les indicateurs de succès afin de		- Le plan d'actions correctives permet la mise en œuvre des recommandations de l'audit ; - Les actions sont définies et reliées à un objectif clair et mesurable ;

	définir les mesures à mettre en œuvre pour remédier aux non-conformités.		- Les actions sont classées par criticité ; - L'impact des actions est évalué ; - Les échéances des actions sont adaptées aux priorités ; - Les délais de mises en œuvre sont réalistes ; - Les responsables des actions sont désignés ; - Les ressources nécessaires sont identifiées.
Activité 3 - Pilotage du projet de conformité règlementaire liée à la protection de données (*accountability* RGPD et/ou de conformité RIA) - Constitution de l'équipe projet ; - Décomposition du projet de mise en conformité en séquences ; - Elaboration d'une cartographie des traitements et les flux de données ; - Mise en place du registre obligatoire de traitement des données ; - Supervision de la mise en œuvre de mesures préventives ; - Réalisation d'une analyse d'impacts sur la protection des données.	C10 Piloter le projet de mise en conformité règlementaire (*accountability,* RGPD et conformité RIA) en ayant au préalable constitué une équipe projet adaptée, et ce en tenant compte des spécificités de son équipe, notamment des personnes en situation de handicap, afin de s'assurer de la bonne mise en œuvre du projet et du respect du cadre organisationnel.	**Mise en situation professionnelle reconstituée** A partir d'un cahier des charges, précisant les besoins en matière de traitements de données et d'IA d'une organisation fictive, le candidat élabore un dossier dans lequel il : - Présente les objectifs de la protection de données personnelles ; - Présente un plan d'actions du projet (tâches, livrables, ressources humaines, échéance de livraison…) ; - Décrit la méthodologie de gestion de projet choisie ; - Décrit les différentes étapes du projet ; - Décrit l'équipe projet constituée (compétences et organisation) ; - Rédige une analyse des risques du projet ; - Présente un document présentant les risques identifiés et leurs impacts ;	- Une fiche mission reprenant les tâches et activités attendues dans le cadre du projet est rédigée ; - Les profils des équipiers projet sont présentés ; - L'organisation mise en place pour animer l'équipe projet est détaillée ; - Les besoins spécifiques des personnes en situation de handicap sont identifiés ; - Un ensemble de règles de bonnes pratiques et des outils permettant l'inclusion des personnes en situation de handicap est proposé ; - La méthode de gestion de projet choisie est adaptée à la politique de protection des données de l'organisation.
	C11 Allotir le projet en déterminant les actions spécifiques en décomposant le projet en grandes séquences et en tenant compte des contraintes de délais, de coûts et de moyens afin de pouvoir ordonner les activités, les prioriser et formaliser une feuille de route (roadmap) ou un planning objectivé.		- Les grandes étapes du projet de mise en conformité sont établies de manière à mesurer l'avancement du projet ; - Un découpage abouti des sous- projets (ou tâches, missions, phases, composants, lots de travail...), organisés sous forme d'arborescence et représentant des livrables permet d'organiser le travail de l'équipe projet ; - Les indicateurs de performance objectifs, mesurables et représentatifs sont définis.
	C12 Cartographier les traitements et les flux de données en indiquant leur origine et la destination des données, en établissant le registre obligatoire de traitement des données, afin d'identifier les données traitées et les bases légales et réglementaires.		Les flux de données sont cartographiés en indiquant l'ensemble des éléments suivants pour chaque traitement de données : - Acteurs concernés ; - Emplacement du stockage des données ; - Temps de conservation des données ; - Liste des traitements classés par finalité principale (et non par outil ou applicatif utilisé) ; - Types de données traitées ; - Sous-traitants qui interviennent sur chaque traitement.

	C13 Repérer les risques liés aux traitements et au transfert de données (UE et Hors UE) en s'appuyant sur le registre de traitements des données et en supervisant ou réalisant les analyses d'impact sur la protection des données (AIPD) afin de garantir la conformité au RGPD et faciliter la prise de décisions éclairées sur la mise en œuvre ou la modification de certains traitements.	- Présente un plan d'actions par suite d'une analyse d'impacts relatifs à la protection de données listant les actions à mettre en œuvre pour assurer la mise en conformité ; - Présente un registre IA : document détaillant pour chaque système d'IA : l'origine, la destination, les acteurs… ; - Présente sur le registre le niveau de risque de chaque système d'IA ; - Un plan d'actions par suite d'une analyse d'impacts et à la classification des systèmes d'IA listant les actions à mettre en œuvre pour assurer la mise en conformité. Le dossier sera présenté à l'oral.	- Les risques pesant sur les traitements de données existants sont identifiés et qualifiés ; - Les impacts des non-conformités sont analysés (AIPD) ; - Les analyses d'impact requises et non requises sont distinguées ; - Une liste d'actions permettant la mise en conformité est dressée et comprend une priorisation ; - Les impacts relatifs à la protection des données (les impacts potentiels, les sources de risques et les menaces réalisables) sont analysés en utilisant une approche AIPD (mise en application de l'approche selon les neuf critères donnés par le CEPD – Comité Européen de la Protection des Données- (Evaluation ou notation d'une personne, prise de décisions automatisées, surveillance systématique, données sensibles ou données à caractère hautement personnel, …) ; - Des recommandations qui permettent de réduire les risques liés aux traitements et au transfert de données (UE et Hors UE) sont formulées en lien avec l'analyse d'impacts.
Activité 4 – Proposition d'un processus de suivi continu lié à l'utilisation de l'IA dans l'entreprise - Inventaire exhaustif des systèmes d'IA utilisés dans l'organisation ; - Hiérarchisation des systèmes d'IA en fonction des risques ; - Etablissement d'un plan d'actions d'atténuation des	C14 Cartographier les systèmes d'IA en établissant une liste exhaustive de tous les systèmes d'IA internes et externes utilisés dans l'organisation (registre IA) afin d'identifier la réglementation applicable et la vigilance à prévoir dans le cadre du traitement des données.		Les systèmes d'IA utilisés sont recensés et les éléments suivants figurent dans le recensement : - Les acteurs concernés ; - L'emplacement du stockage des données ; - Le temps de conservation des données ; - La liste des traitements par finalité principale (et non par outil ou applicatif utilisé) ; - Les types de données traitées.
	C15 Classifier les systèmes d'IA par niveau de risque sur la base des critères définis par la RIA, en identifiant les systèmes d'IA nécessitant une attention particulière pour garantir la sécurité des données personnelles utilisées et le cas échéant, en extraire des bonnes pratiques à transmettre aux équipes.		Le candidat définit une classification des systèmes d'IA utilisés dans l'organisation qui : - Distingue les 4 niveaux de risques et identifie les usages et finalités des systèmes d'IA ; - Evalue les systèmes d'IA en fonction de leurs potentiels impacts et de leur utilisation et du principe de « privacy by design » ; - Propose des recommandations de bonnes pratiques à transmettre aux équipes.

risques de non-conformité RIA (ou IA Act).	C16 Établir la liste des actions prioritaires selon les risques et niveaux de risques associés en s'appuyant sur le registre des systèmes d'IA afin de rendre ses traitements conformes au RIA.		Le plan d'actions liées à l'IA du projet est défini : - La liste des risques qui peuvent peser sur les traitements de données existants est complète ; - Les risques sont classés suivant les niveaux de risques du RIA (risque inacceptable, haut risque, risque spécifique en matière de transparence, risque minimal) ; - L'analyse d'impacts IA (les impacts potentiels, les sources de risques et les menaces possibles) correspond à l'organisation ; - Les actions à mener sont détaillées, réalisables au sein de l'organisation, et sont adaptées aux risques identifiés ; - Le plan d'actions permet à l'organisation d'être en conformité au RIA.
Activité 5 Sensibilisation/formation des collaborateurs de l'organisation sur les meilleures pratiques en matière de protection des données - Identification des enjeux ; - Actions de sensibilisation des collaborateurs à la conformité RGPD, aux usages éthiques des système d'IA ; - Elaboration de contenus thématiques et de documents adaptés	C17 Établir les enjeux techniques, juridiques, financiers et éthiques de l'organisation en faisant le lien avec les différents services, afin d'assurer la cohérence des propositions d'actions avec la stratégie de l'organisation en matière de protection des données.	**Mise en situation professionnelle reconstituée** A partir d'un cahier des charges, précisant les besoins d'une organisation réelle ou fictive, le candidat présente dans un dossier les livrables suivants : - La liste des enjeux techniques, juridiques, financiers et éthiques de l'organisation, et une synthèse de ces enjeux ; - Une campagne de sensibilisation sur la protection des données personnelles (complète ou partielle) ;	**Critère sur la forme :** - La synthèse des enjeux est structurée - Le vocabulaire utilisé est technique et adapté aux enjeux et aux personnes cibles. **Critères sur le fond** - Les enjeux techniques, juridiques, financiers et éthiques de chaque service de la structure sont contextualisés dans une synthèse ; - Les enjeux sont relevés de façon explicite et exhaustive ; - Les enjeux sont catégorisés ;
	C18 Concevoir une campagne de sensibilisation des équipes en réalisant des présentations accessibles, notamment aux personnes en situation de handicap, visuelles et synthétiques afin d'informer l'ensemble des collaborateurs et de partager les principes d'équité, de transparence, de protection des droits notamment dans les systèmes d'IA et d'initier une réflexion globale sur la protection des données à caractère personnel dans la structure.		- Les objectifs de la campagne de sensibilisation sont établis ; - Le public cible de la campagne est identifié ; - Les différentes stratégies de campagne à utiliser sont identifiées et argumentées ; - Les grandes étapes de sa campagne sont explicitées ; - Les points de vigilance à appliquer pour rendre sa documentation accessible à un public en situation de handicap sont précisés et s'appuient sur le référentiel RGAA[1] .

[1] https://accessibilite.numerique.gouv.fr/

aux parties prenantes ; - Formation des parties prenantes.	C19 Animer une action de formation auprès des publics cibles en s'appuyant sur des contenus thématiques adaptés, notamment aux personnes en situation de handicap, afin de les guider dans l'appropriation des procédures et bonnes pratiques en matière de RGPD et de protection des données.	- Un programme de formation sur la règlementation RGPD composé a minima des objectifs et des contenus ; - Une ébauche de présentation générale d'une procédure RGPD ; - Un visuel présentant les éléments illustrant une action de communication ; - Des préconisations en matière de politique de protection des données personnelles adaptées au contexte de l'organisation ; - Une présentation du système de gestion documentaire ; - Des procédures internes pour répondre à un contrôle de la CNIL. Le dossier sera présenté à l'oral	- Un document type pour la formation est formalisé ; - Une fiche programme est établie, qui est composée des objectifs pédagogiques et des contenus envisagés ; - Les contenus proposés sont cohérents avec la mission spécifique du délégué à la protection des données ; - La démarche pédagogique est adaptée aux publics cibles.
	C20 Réaliser des actions de communication internes en élaborant des documents à destination des équipes pour que l'ensemble de collaborateurs l'identifient, comprennent son rôle dans l'organisation et puissent faire appel à lui et pour impliquer les collaborateurs dans la réussite des futurs plans d'actions.		**Critères sur la forme** - Le visuel de type présentation est accessible ; - Le contenu est structuré et lisible ; **Critères sur le fond** - Le vocabulaire est adapté au public cible ; - Le visuel du type présentation comprend la présentation du poste et du rôle du DPO au sein de la structure et l'objectif de la communication ; - L'audience est identifiée et les écrits sont orientés selon le profil des personnes cibles ; - Différents canaux de communication sont proposés qui permettent de toucher les personnes cibles.
Activité 6 : Participation à la gestion documentaire relative à la protection des données - Collaboration avec les parties prenantes ; - Alimentation du système documentaire lié à la gestion des données personnelles ; - Contribution à la formalisation de la documentation	C21 Participer à la création et à la révision des politiques de confidentialité et des procédures de gestion des données en collaborant avec la direction générale, le responsable de la sécurité des systèmes d'information, le responsable juridique et les responsables métiers afin de garantir l'efficacité et la régularité des mesures prises par l'organisation.		- Des préconisations adaptées au contexte sont établies dans le cadre de la refonte de la politique de gestion des données ; - Les éléments nécessaires à une politique de protection des données de l'organisation respectueuse de la règlementation sont précisés ; - La manière dont la politique doit être organisée dans l'organisation est détaillée et argumentée ; - Les éventuels bénéficiaires de transfert de données sont précisés en fonction du contexte de l'organisation ; - Les droits de personnes concernées sont détaillés.
	C22 Gérer le système documentaire de la gestion des données personnelles en collaborant avec le responsable qualité et en utilisant les outils de stockages adaptés (cloud, outils de GED…) afin de disposer des documents et des preuves nécessaires aux audits externes relatifs à la protection des données.		- Le système de gestion documentaire inclut des politiques et procédures spécifiques qui couvrent tous les aspects requis ; - Le registre de traitement des données est complet et conforme aux exigences du RGPD ; - La gestion documentaire inclut des mécanismes pour limiter l'accès aux documents sensibles aux seules personnes habilitées ;

relative à la protection des données.			- La gestion documentaire inclut un système de versioning, d'archivage et de traçabilité des modifications ; - La documentation est inclusive (accès aux personnes en situation de handicap).
	C23 Rédiger une procédure interne en prévision du contrôle de la CNIL en listant les modalités d'accueil, les personnes à prévenir et les informations à obtenir et en la diffusant aux parties prenantes afin de s'assurer que l'organisation est prête à accueillir un audit externe de l'institution.		**Qualité de la procédure interne à suivre en prévision de contrôle de la CNIL :** - Chaque étape du contrôle est détaillée ; - Les points clés à vérifier sont référencés ; - Les étapes de suivi post-contrôle sont prévues, notamment en cas de recommandations ou sanctions de la CNIL.
Activité 7 Déploiement des plans de réduction des écarts constatés - Sélection de la solution adaptée aux traitements sur le SI ; - Rédaction des protocoles de test ; - Suivi des actions de contrôle RGPD régulière ; - Déploiement des mesures de sécurisation.	C24 Déployer les mesures de sécurité applicatives et système en proposant des solutions techniques innovantes pour le système d'information en collaboration avec le responsable de la sécurité du SI (RSSI) de l'organisation afin de traiter chaque risque de façon spécifique et ainsi garantir la conformité règlementaire.	**Mise en situation professionnelle reconstituée** A partir de l'analyse d'un dossier professionnel contenant une situation d'organisation fictive ainsi que des documents annexes présentant les procédures de sécurité du SI, le candidat réalise un ensemble d'activités en atelier et consigne ensuite les informations dans un rapport d'activité présentant les livrables suivants : - Une présentation des solutions de sécurité de SI à mettre en place ; - Une liste des tests techniques réguliers à réaliser ; - Le descriptif du dispositif imaginé pour surveiller en	- Les solutions techniques proposées permettent d'assurer la conformité règlementaire et légale ; - Le fonctionnement des solutions techniques choisies est explicité ; - La solution est détaillée en termes d'intégrité, de confidentialité et de disponibilité des données personnelles.
	C25 Réaliser des tests réguliers de robustesse et d'équité en évaluant les systèmes d'IA utilisés dans l'organisation, en collaboration avec les équipes de développement, afin d'identifier et corriger les biais potentiels et de s'assurer que les modèles d'IA sont équitables et non discriminatoires.		- Les métriques sélectionnées (ex. : précision, recall, F1-score pour la robustesse, disparité de traitement pour l'équité) sont pertinentes par rapport aux objectifs du système d'IA et à son impact potentiel ; - Les métriques sont cohérentes, valides et évaluent la performance et l'équité dans des conditions variées ; - La méthodologie des tests est clairement documentée, avec des étapes détaillées et des justifications des choix de tests ; - Les données utilisées pour les tests sont pertinentes et représentatives des données utilisées dans le contexte de l'organisation.
	C26 Gérer les signalements, les demandes d'accès, de rectification, d'effacement ou de portabilité des données personnelles conformément au RGPD, en proposant un formulaire dédié et en mobilisant des canaux de communication adaptés, notamment aux		- Le formulaire proposé permet de signaler tous les types d'incidents ou de faire parvenir tous les types de demandes ; - Les canaux de communication proposés sont multiples et accessibles ; - Les canaux de communication proposés permettent de garantir une réponse rapide aux utilisateurs ;

	personnes en situation de handicap, afin de s'assurer que les réponses aux demandes sont fournies dans le respect des contraintes réglementaires.	continu des systèmes d'IA proposé ; - Un extrait du registre des traitements de données ; - Une évaluation des incidents constatés et de leurs impacts en termes de violation des données ; - Une note de synthèse des conséquences réputationnelles, juridiques et financières ; - Des préconisations pour maintenir le système de sécurité de SI à mettre en place et contenir les incidents constatés ; - Présenter les actions de communication à réaliser auprès des parties prenantes Les activités seront réalisées en autonomie en ateliers surveillés. Le rapport d'activités sera présenté à l'oral.	- Les canaux de communication sont sécurisés et adaptés ; - Les métriques proposées permettent de garantir le respect des délais de traitement et de quantifier et qualifier les demandes.
	C27 Déployer un registre de traitement de données personnelles, en collaborant avec les services de l'organisation qui traitent des données personnelles, afin de recenser de façon précise et documenter les différents traitements de données personnelles de l'organisation et de le transmettre, le cas échéant, à la CNIL.		- L'extrait de registre de traitement des données est conforme aux préconisations de la CNIL ; - Il permet de répondre aux critères établis par la CNIL ; - Il présente de façon exhaustive les informations des différents services susceptibles de traiter des données personnelles ; - Il fait des focus sur les sites internet, les formulaires en ligne, … etc.
Activité 8 Coordination des actions pour contenir les éventuels incidents - Analyse des incidents et des impacts constatés ; - Enquêtes auprès des équipes techniques ; - Identification des données concernées ; - Estimation des impacts sur l'organisation ;	C28 Déterminer la nature des incidents et l'étendue des violations en recueillant les signalements internes et/ou externes, en identifiant les données concernées et en réalisant des enquêtes préliminaires auprès des équipes techniques afin de documenter l'incident (recueillir des preuves) et d'adapter les actions correctives à mettre en place.		L'évaluation de la nature de l'incident et de son étendue est précise et complète : - L'incident est évalué en profondeur : ampleur, données concernées et systèmes ou services touchés ; - Une évaluation détaillée est réalisée qui permet d'identifier le type de données personnelles exposées ; - La cause de l'incident (erreur humaine, défaillance technique, attaque externe) est précisément identifiée et permet d'évaluer les risques associés
	C29 Évaluer les dommages causés par les incidents en identifiant les données compromises, la durée d'exposition, le type de données, le volume de données afin de déterminer l'impact pour les parties prenantes concernées (fraude, usurpation d'identité, atteinte à la vie privée …) et pour l'organisation.		L'évaluation des dommages causés par l'incident est précise et complète : - Les données exposées sont identifiées et qualifiées selon leur niveau de sensibilité ; - La durée de l'exposition est déterminée ; - L'étendue de l'accès est identifiée (consultation, copie, modification ou suppression) ; - Les résultats de l'évaluation des dommages sont documentés de manière claire et détaillée, permettant une traçabilité complète.

- Mise en place des mesures correctives	C30 Évaluer les conséquences juridiques, financières et réputationnelles des incidents en se référant au cadre réglementaire et légal et en collaboration avec la direction juridique et financière de l'organisation afin d'estimer les risques de sanctions pour l'organisation et de réaliser le cas échéant une communication appropriée avec la direction de la communication de l'organisation.		L'évaluation des conséquences de l'incident est précise et complète : - Une analyse de la portée et de la nature de la couverture médiatique liée à l'incident est présentée ; - Les mentions ou commentaires de l'incident sur les réseaux sociaux sont relevés ; - Les réactions des clients, partenaires et fournisseurs sont recueillies ; - Les sanctions financières et pénales applicables sont estimées en considérant les précédents juridiques similaires ; - Une analyse des probabilités de litiges ou de poursuites judiciaires est présentée.
	C31 Déployer les mesures correctives de sécurité, applicatives et système, en collaboration avec le responsable de la sécurité du SI (RSSI) (isoler les systèmes compromis, suspendre les accès, restaurer des sauvegardes …) afin de contenir les incidents et en tirer parti en termes d'usages à venir.		- Des solutions techniques pour s'assurer de la conformité réglementaire sont proposées et argumentées et respectent le principe de « *privacy by design* » ; - Le fonctionnement de la solution technique choisie est expliqué ; - La solution est détaillée en termes de transparence, intégrité, confidentialité, disponibilité de la donnée personnelle.