RNCP34776 - DELEGUE A LA PROTECTION DES DONNEES (DPO)
REFERENTIELS D'ACTIVITES, DE COMPETENCES ET D'EVALUATION
ASSOCIATION DES FONDATEURS ET PROTECTEURS DE L'INSTITUT CATHOLIQUE DE LYON
FACULTE DE DROIT (UCLY)

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.* »

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**
A1 : Piloter la production et la mise en œuvre des politiques et stratégies de la protection des données en collaboration avec l'ensemble des services de l'organisation	**C1 : élaborer les politiques et stratégies de protection des données**		
> A1.1. Elaboration des politiques et des stratégies de protection des données > A.1.2. Participation à l'identification des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement > A.1.3. Veiller à la bonne application du principe de protection des données dès la	> C.1.1. Articuler les enjeux juridiques, techniques, économiques, éthiques et la stratégie de protection des données de l'organisation en s'appuyant sur les outils de la qualité pour définir une politique de protection des données > C.1.2. Analyser le système d'informations en accord avec les ambitions et la stratégie de l'organisation pour déterminer une politique de protection adaptée	> Rédaction de notes aux différents services de l'organisation portant sur l'analyse du système d'informations >Mise en situation professionnelle avec préparation en groupe : proposition écrite d'une charte de gouvernance, d'une politique et d'une stratégie de protection des données remise à un jury composé d'enseignants et de	- les acteurs internes opérant des flux de données sont identifiés et cités, leur rôle est connu et maîtrisé, - le cahier des charges présente des orientations claires, une progression temporelle et logique de la stratégie, une distinction des

conception et par défaut dans tous les projets comportant un traitement	> C.1.3. Identifier les rôles et responsabilités des collaborateurs de l'organisation en s'appuyant sur un bilan du système d'informations pour mettre en place les bases du système de gestion de la sécurité des données > C.1.4. Intégrer les équipes projet en mobilisant les compétences psychologiques et relationnelles pour construire de manière collaborative des politiques et stratégies de protection des données concertées > C.1.5. Elaborer un cahier des charges des stratégies et actions à mener en s'appuyant sur les normes établies et sur une analyse du système d'informations pour déterminer ses démarches auprès des collaborateurs et dirigeants >C.1.6. Elaborer des chartes informatiques et des chartes de gouvernance en utilisant un langage simple et compréhensible par tous pour appuyer ses démarches auprès des collaborateurs et dirigeants > C.1.7. Promouvoir les valeurs éthiques de la protection des données en favorisant leur intégration dans les chartes de gouvernance pour une compliance des données	professionnels et présidé par un professionnel.	étapes de travail précise, un budget justifié et réaliste, - le cahier des charges intègre les exigences règlementaires à jour et le contexte de l'entreprise, - les échéances de travail de groupe sont respectées, - la contribution du candidat est visible et s'articule avec les contributions des autres membres du groupe de travail, (échange de savoir et savoir-faire pour une montée en compétences de l'ensemble des membres du groupe de travail)
A2 : Informer, sensibiliser, diffuser une culture "informatique et liberté"	**C2: informer, sensibiliser et former les collaborateurs à la protection des données**		
> A.2.1. Pilotage et réalisation des actions de formation et sensibilisation sur les règles à respecter auprès des collaborateurs, de la Direction, des opérationnels participant aux opérations de traitement	> C2.1.Concevoir une politique de sensibilisation et de formation au sujet de la protection des données en tenant compte des métiers et compétences des collaborateurs et des enjeux de leur rôle au sein de l'organisation pour assurer le bon fonctionnement des procédures	> Rédaction de notes à la direction mettant en exergue les enjeux de la protection des données.	- le stress lié à la prise de parole en public est maitrisé - les publics visés sont identifiés, les objectifs de formation et communication sont déterminés clairement et

> A.2.2. Définition et diffusion des bonnes pratiques d'utilisation des données personnelles et veille sur leur application > A.2.3. Information et responsabilisation de son responsable de traitement quant aux risques encourus > A.2.4. Présentation de rapports à son responsable de traitement > A.2.5. Identification des traitements, des données, et des opérateurs dans l'organisation pour définir sa stratégie de sensibilisation /formation/information/accompagnement	> C2.2. Concevoir des actions de communication et de formations adaptées aux différents métiers de l'organisation et aux objectifs définis dans la politique de sensibilisation et de formation en s'appuyant sur l'analyse du système d'informations de l'organisation pour assurer le rôle opérationnel des collaborateurs vis-à-vis de la protection des données > C.2.3.Contrôler l'impact des actions de communication et de formation en les évaluant pour rectifier ou adapter le programme > C.2.4. Dispenser les programmes de formation et de sensibilisation du personnel et des instances dirigeantes en s'appuyant sur les méthodes pédagogiques adéquates pour assurer une collaboration effective de chacun à la protection des données > C.2.5. Adapter sa posture, son discours, le choix des modalités pédagogiques en s'ajustant à son public cible (direction, services informatiques, services juridiques, RH, cœur de métier de l'organisation...) et au contexte pour assurer la transmission des messages > C.2.6. Argumenter son propos en identifiant les réticences et en analysant les freins pour favoriser la coopération > C.2.7. Synthétiser et adapter un propos technique en identifiant les éléments saillants pour calibrer la forme de son propos en fonction de son public (direction, services informatiques, services juridiques, RH, cœur de métier de l'organisation...)	> Mise en situation individuelle orale : jeu de rôle, consistant en une action de sensibilisation et de formation auprès des salariés d'une organisation, observé par un jury d'enseignants et de professionnels présidé par un professionnel.	adaptés à l'organisation de l'entreprise, au besoin de l'entreprise et contextualisés à chaque catégorie d'acteurs, le calendrier est cité et réaliste au regard du contexte de l'entreprise, il contient un planning d'évaluation (d'étude d'impact de la formation), le format et le volume horaire proposé est adapté aux besoins et aux contraintes des publics - les enjeux éthiques de la protection des données sont cités et valorisés - les modalités pédagogiques sont adaptées et choisies en fonction du public et des objectifs - les outils pédagogiques sont choisis en cohérence avec les modalités et les objectifs - le contenu des actions de formation fait référence aux éléments législatifs à jour, adéquats à la situation rencontrée par l'entreprise - les éléments de langage choisis pour exprimer son propos sont adaptés au public

	> C.2.8. Mettre en valeur les actions mises en œuvres et leurs résultats en concevant des rapports écrits à destination du représentant de l'organisation pour informer et responsabiliser le responsable de traitement sur les mesures et risques (bilan annuel) > C.2.9. Maitriser ses émotions et ajuster sa posture en s'appuyant sur une connaissance du lien à l'autre pour assurer la prise de parole en public > C.2.10. Interagir avec l'ensemble des services de l'organisation (juridique, techniques, direction…) en s'appuyant sur une capacité d'adaptation pour faire adhérer l'ensemble des collaborateurs aux processus de protection des données.		- les éléments de présentation (choix des qualificatifs employés pour se présenter, posture physique, les codes vestimentaires, clarté et intelligibilité de la voix) pour exprimer son propos sont adaptés au public - les réactions et langage non verbal du public sont repérés et une adaptation immédiate de la présentation est observée - les données citées sont contextualisées, exploitables, proviennent de sources fiables et sont utilisées pour étayer un propos
A3 : Analyser, investiguer, auditer et contrôler la conformité des traitements de données	**C3 – assurer la conformité des traitements de données**		
> A.3.1. Etablissement et maintien d'une documentation relative aux traitements des données à caractère personnel (registre d'activités de traitement, registre des catégories de traitement, documentation permettant de prouver la conformité). > A.3.2. Identifier les données et traitements de l'organisation	>C.3.1.Cartographier les traitements de données réalisés dans l'entreprises en s'appuyant sur l'analyse du système d'informations pour établir la documentation de conformité. > C.3.2. Etablir le registre d'activités de traitement et le registre des catégories de traitements en s'appuyant sur l'analyse du système d'informations pour assurer la traçabilité des traitements de données > C.3.3.Etablir et faire évoluer les processus et procédures de protection des données en collaborant	> Elaboration de documents de traçabilité de la conformité des traitements, rédaction de clauses liant responsables de traitement et sous-traitant... > Mise en situation individuelle et écrite : présentation d'un projet de mise en conformité d'une organisation. Le rapport est soumis à un jury composé d'enseignants et de	les documents opérationnels, chartes informatiques sont compréhensibles par tous les collaborateurs et le grand public, ils sont complets et synthétiques - le registre des traitements répertorie les opérations faites sur les données personnelles, le type de données, les durées de conservation de

> A.3.3. Mise en place des mesures de protection des données dès la conception des projets et par défaut adaptées aux risques et à la nature des traitements réalisés. > A.3.4. Représentation des normes de conformité dans les processus de l'organisation > A.3.5. Gestion des droits d'accès aux données récoltées > A.3.6. Décision et conseil lors de l'exécution des analyses d'impacts > A.3.7. Intervention auprès des fournisseurs et prestataires pour contrôler la conformité > A.3.8. Assurer la conformité des mesures en place avec la loi > A.3.9. Formulation de conseils, exigences et procédures tendant à assurer la conformité des traitements de données mis en œuvre par l'organisation	avec l'ensemble des services et s'appuyant sur le cadre légal, les techniques de sécurité et les outils de la qualité afin de prévenir les aléas > C.3.4. Piloter l'analyse d'impacts en adéquation avec les attendus légaux pour évaluer les risques des traitements de données > C.3.5.Déterminer les durées de conservation des données en s'appuyant sur les obligations légales en la matière et les techniques d'archivage pour assurer la compliance des données. > C.3.6.Piloter des audits de services internes en s'appuyant sur le cadre légal et les indications des autorités de contrôle pour vérifier l'exécution des analyses d'impact et s'assurer de la conformité avec la loi > C.3.7.Piloter des audits de conformité de protection des données auprès des fournisseurs et prestataires en s'appuyant sur le cadre légal de la sous-traitance en matière de protection des données pour s'assurer de la conformité des sous-traitants. > C.3.8. Contrôler la base juridique des traitements de données et le respect des principes de loyauté, transparence, limitation des finalités, minimisation, exactitude, intégrité et confidentialité des traitements de données en s'appuyant sur l'analyse du système d'informations pour assurer la compliance des traitements de données >C.3.9. Identifier l'existence d'un transfert de données hors Union européenne en s'appuyant sur le cadre légal de la compliance des données et la	professionnels et présidé par un professionnel.	données. Il est conforme aux attentes de l'autorité de contrôle (cnil.fr) - le caractère opérationnel et réaliste des modes d'actions, procédures et mesures est observé - le Bilan des Systèmes d'Information (BSI : outil d'analyse des SI développé par le certificateur) est utilisé de manière conforme - la méthode d'analyse d'impacts est connue - les outils de gestion de projets sont utilisés - les outils d'audits sont utilisés - les propositions techniques sont contextualisées et organisées en mode projet (exemple : identification des ressources internes et externes, budget des propositions, etc.)

	compréhension des infrastructures de stockage des données pour déterminer les instruments juridiques et techniques de transfert adéquats. > C.3.10. Déterminer les précautions à prendre en matière de contenu de zones libres et cookies en s'appuyant sur le cadre légal pour assurer le respect des droits individuels. > C.3.11. Etablir les procédures de réception et de gestion des demandes d'exercices des droits des personnes concernées en s'appuyant sur le cadre légal de la protection des données pour assurer le respect de l'autodétermination des personnes concernées. > C.3.12. Déterminer les moyens appropriés et le contenu de l'information à fournir en s'appuyant sur la méthode facile à lire et à comprendre et le cadre légal de la protection des données pour assurer le respect de l'autodétermination informationnelle des personnes concernées.		
A4 : GERER DE MANIERE OPERATIONNELLE LES RISQUES DES TRAITEMENTS DE DONNEES	**C4 : gérer les risques et fuites de données**		
> A.4.1. Réalisation des opérations nécessaires en cas d'aléa (déclaration CNIL, information des titulaires de données, mesures techniques, mise en place d'une cellule de crise, registre des violations)	> C.4.1. Gérer les relations avec les autorités de contrôle en répondant à leur sollicitation afin de faciliter leur action > C.4.2.Evaluer les risques encourus et suscités par les activités et processus de l'organisation en tenant compte de la nature, la portée, le contexte et la finalité	> Rédaction de notes adressées à la direction relatives à la procédure interne en cas de contrôle par la CNIL et aux évolutions nécessaires des processus de protection des données.	- les enjeux de la e-réputation des organisations sont cités - les obligations légales en cas de violation sont connues

> A.4.2. Participation à la reconstruction de la réputation de l'entreprise > A.4.3. Représentation du responsable de traitement et interaction avec les autorités de contrôle (CNIL) > A.4.4. Analyse des risques > A.4.5. Veille juridique et technique sur le sujet de la protection des données >A.5.6 Analyse des nouvelles données au regard des procédures mises en place dans l'organisation	des traitement de données pour calibrer les plans d'action proposés à la direction de l'organisation > C.4.3.Conduire les actions de rectifications des procédures en mobilisant les services concernés et la veille réalisée pour actualiser la conformité et prévenir les fuites de données > C.4.4.Mettre en œuvre la gestion des risques en intégrant les groupes projets relatifs aux SI et en appliquant les procédures de gestion de risques afin de prévenir les risques de fuite de données > C.4.5. Déterminer la communication nécessaire auprès des autorités de contrôle et des personnes concernées en s'appuyant sur les obligations légales pour assurer l'autodétermination informationnelle des personnes. >C.4.6. Diriger la cellule de crise en sollicitant les outils de la communication et les valeurs éthiques de l'organisation pour participer à la reconstruction de la réputation de l'organisation > C.4.7. Etablir la documentation des violation de données en s'appuyant sur les outils des autorités de contrôle pour assurer la traçabilité des fuites de données > C.4.8. Conseiller les dirigeants quant aux ajustements des mesures à apporter en s'appuyant sur les évolutions juridiques et technologiques pour prévenir une nouvelle fuite de données > C.4.9. Réaliser une veille juridique et technique sur le sujet de la protection des données en consultant de	> Mise en situation individuelle et orale : présentation d'un plan d'action faisant suite à une fuite de données devant un jury composé d'enseignants et de professionnels et présidé par un professionnel.	- les parties prenantes internes de la gestion de crise sont repérées - les risques sont justement évalués - les techniques de sécurité des SI sont connues - les professions clés pour mettre en oeuvre la gestion des risques (exemple : DSI) sont repérées et les périmètres d'action sont connus - les enjeux et contraintes de la sécurité des SI sont cités - les leviers de communication (media, interlocuteurs, etc.) appropriés en cas de gestion de crise sont connus - les sources documentaires sont citées et les propos sont juridiquement et techniquement à jour - les textes de lois sont analysés, les dispositifs existants sont analysés et mis en perspective et les évolutions potentielles sont identifiées

	nombreuses sources pour déterminer les actions de rectifications à réaliser > C.4.10. Anticiper les évolutions en analysant les informations juridiques et techniques relatives à la protection des données pour mettre en œuvre une réflexion prospective		