Répertoire spécifique

Intégrer les enjeux éthiques et juridiques de l’intelligence artificielle dans les activités professionnelles

RS7806 · RS · Publiée

L'essentiel

Code(s) NSF	315n, 315p, 326p
Formacode(s)	14231, 31028, 31025
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/10/2026
Date d'échéance	30/10/2029

Certificateur(s)

AIVANCITY · SIRET : 88343992900067

Résumé de la certification

OBJECTIFS ET CONTEXTE

Dans un contexte de déploiement accéléré des systèmes d’intelligence artificielle au sein des organisations, les entreprises sont confrontées à un besoin croissant de sécurisation juridique, éthique et technique de leurs usages. L’entrée en vigueur de cadres réglementaires structurants, notamment le règlement européen sur l’intelligence artificielle (AI Act), le RGPD ainsi que les réglementations en matière de cybersécurité (directive NIS2, Cyber Resilience Act), renforce les obligations de conformité, de transparence et de responsabilité des acteurs économiques.

Parallèlement, les usages de l’IA, en particulier générative, se diffusent dans l’ensemble des fonctions métiers sans toujours faire l’objet d’un encadrement formalisé, exposant les organisations à des risques juridiques, éthiques, opérationnels et réputationnels.

Dans ce contexte, la certification vise à répondre à un besoin du marché et atteste de compétences professionnelles pour permettre à des professionnels d’intégrer ces exigences dans les projets d’intelligence artificielle, en articulation avec les fonctions métiers, techniques et de gouvernance.

Elle s’adresse ainsi à des professionnels impliqués dans la mise en œuvre concrète de projets IA (managers, profils techniques, consultants), et non uniquement dans leur cadrage stratégique.

COMPÉTENCES ATTESTÉES

S’assurer de la conformité de la mise en œuvre d’un système d’IA au cadre juridique en vigueur, en réalisant une évaluation de la conformité par rapport au cadre réglementaire français et européen, en évaluant les implications juridiques et les responsabilités associées pour les acteurs impliqués, en assurant une veille continue sur les cadres réglementaires applicables, et en intégrant les évolutions relatives à l’accessibilité numérique, à la responsabilité environnementale et aux conditions de travail liées aux usages de l’IA, afin d’anticiper les risques juridiques liés à l’IA et de sécuriser juridiquement son intégration dans un cadre professionnel.

Analyser les enjeux éthiques des systèmes d’intelligence artificielle mis en œuvre dans un cadre professionnel, en structurant une démarche d’audit et d’analyse d’impact éthique, en identifiant les enjeux éthiques potentiels (loyauté, vie privée et gouvernance des données, transparence, équité, fiabilité, contrôle humain, bien-être social et environnemental, sécurité, accessibilité des systèmes et inclusion des publics, impacts sur les conditions de travail et sur l’environnement), en proposant des recommandations à déployer à chaque étape de la mise en œuvre système IA, et en intégrant des principes d’inclusion, de sobriété numérique et de prévention des risques professionnels, afin de renforcer la confiance des parties prenantes dans l'utilisation des technologies d’intelligence artificielle.

Établir des mesures relatives à la confidentialité et à la protection des données dans les systèmes d’IA en identifiant les traitements de données personnelles dans les flux IA, en prenant en compte les données pouvant révéler des

situations de vulnérabilité ou de handicap et les risques d'exclusion associés, en mettant en œuvre des mesures techniques appropriées, en intégrant des principes de minimisation, de sécurité renforcée et de limitation des impacts environnementaux liés aux traitements de données, et en définissant des mesures organisationnelles de gouvernance des données, incluant des dispositifs de sensibilisation, d'accessibilité des politiques de données et de prévention des usages à risque, afin d'assurer la conformité au RGPD et aux principes de minimisation, de finalité, et de sécurité des données.
Contribuer à l'élaboration d'une politique de sécurité adaptée aux systèmes d'IA en identifiant les menaces spécifiques aux systèmes IA, y compris celles liées aux usages inadaptés, à la surcharge cognitive ou à la dépendance aux systèmes, en évaluant les vulnérabilités des modèles et des environnements de déploiement, en intégrant les enjeux d'accessibilité des systèmes, d'inclusion des utilisateurs et de continuité d'usage pour des publics diversifiés, et en recommandant ou déployant des mesures de prévention adaptées, incluant des dispositifs favorisant la sécurité, la résilience, la sobriété des systèmes et la protection des conditions de travail, afin de garantir la résilience des systèmes IA et leur conformité aux exigences du Cyber Resilience Act et de la directive NIS2.

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Expérience professionnelle en lien avec l'utilisation ou le déploiement de systèmes numériques, de données ou de projets en entreprise.

COMPOSITION DU JURY — FORMATION CONTINUE

2 représentants de l'école (le directeur Académique d'aivancity et le responsable pédagogique de la certification)
3 professionnels du secteur de l'IA/Data dont un(e) désigné(e) comme président(e) du jury. Parmi ces 3 professionnels, il doit y avoir au moins un salarié en activité, un employeur et une femme.

Base légale

Date de décision	30/10/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	30/10/2029
Date de dernière délivrance possible	29/04/2030

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2026	32	—	—	—

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

https://story.aivancity.com/integrer-les-enjeux-ethiques-et-juridiques-de-lintelligence-artificielle-dans-les-activites-professionnelles/

Fiche officielle (France Compétences)
https://www.francecompetences.fr/recherche/rs/7806/

Où se former

Formations référencées	1
Organismes	1
Régions couvertes	0

Prix indicatif	1 800 €

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.