Webinaire - Élaborer et déployer une charte d'utilisation de l'intelligence artificielle

Webinaire | Jeudi 3 septembre 2026 | Belgique, Luxembourg | Jeoffrey Vigneron

Description

L'intégration rapide de systèmes d'intelligence artificielle dans les outils bureautiques, les processus décisionnels, la gestion des ressources humaines, la relation avec les clients ou les usagers et les activités de contrôle oblige les organisations à définir un cadre d'utilisation clair, juridiquement fondé et opérationnel.

Une charte IA ne peut toutefois se limiter à l'énoncé de quelques principes éthiques. Elle doit **déterminer les usages autorisés ou interdits, organiser les responsabilités internes, encadrer les données utilisées, assurer la supervision humaine, prévenir les discriminations, sécuriser les systèmes et prévoir les mécanismes de contrôle** applicables pendant tout leur cycle de vie.

Cette formation propose une **méthodologie complète pour élaborer, adopter et déployer une charte d'utilisation de l'intelligence artificielle au sein d'une entreprise, d'une association, d'une institution ou d'un organisme public.**

Elle s'appuie notamment sur le règlement européen sur l'intelligence artificielle — le règlement (UE) 2024/1689 ou « AI Act » —, le RGPD, les règles de cybersécurité issues de NIS2 lorsqu'elles sont applicables, ainsi que sur le Data Act et les principaux standards de gouvernance de l'IA.
Les participants apprennent à transformer ces exigences juridiques en règles internes directement applicables aux principaux usages de l'IA : assistants rédactionnels et copilotes, outils intégrés à des solutions SaaS, chatbots, systèmes de classification ou de priorisation, outils RH, modèles entraînés ou affinés sur des données propres et systèmes d'aide à la décision.
Une attention particulière est également accordée aux obligations spécifiques susceptibles de s'appliquer selon le secteur, la nature de l'organisation ou les personnes affectées, notamment en matière de droits fondamentaux, de décisions individuelles, de services publics, de marchés publics et d'accessibilité.

OBJECTIFS

À l'issue de la formation, les participants seront en mesure de :

- comprendre la fonction juridique et organisationnelle d'une charte IA ;
- identifier les systèmes et fonctionnalités d'IA utilisés au sein de leur organisation, y compris l'IA intégrée à des logiciels ou services SaaS ;

- distinguer les pratiques interdites, les systèmes soumis à des obligations de transparence, les systèmes à haut risque et les autres usages de l'IA ;
- déterminer les obligations de l'organisation selon son rôle de fournisseur, déployeur, importateur, distributeur ou utilisateur d'un modèle d'IA à usage général ;
- encadrer l'utilisation de données à caractère personnel, confidentielles, protégées ou couvertes par des droits de tiers ;
- articuler, lorsqu'elles sont requises, l'analyse d'impact relative à la protection des données — DPIA — et l'évaluation d'impact sur les droits fondamentaux — FRIA ;
- organiser une supervision humaine effective et prévenir la validation purement automatique des résultats produits par un système d'IA ;
- définir les règles de transparence applicables aux interactions avec une IA et aux contenus synthétiques ou manipulés ;
- intégrer les exigences de robustesse, de cybersécurité, de journalisation, d'auditabilité et de gestion des incidents ;
- encadrer contractuellement l'acquisition ou l'utilisation de solutions d'IA ;
- structurer une charte IA autour de règles, responsabilités et procédures directement applicables ;
- organiser le suivi, la révision et l'amélioration continue de la gouvernance de l'IA.

Aucune compétence technique avancée en intelligence artificielle n'est requise !

Programme

1. Comprendre la fonction et le périmètre d'une charte IA
– Définition et finalités de la charte IA.
– Distinction entre charte éthique, politique interne, procédure de conformité et gouvernance de l'IA.
– Usages internes et externes concernés.
– Développement, acquisition, intégration et utilisation de systèmes d'IA.
– IA visible et fonctionnalités d'IA intégrées à des solutions SaaS.
– Articulation entre la charte, les politiques de sécurité, les règles de protection des données, les procédures RH et les contrats conclus avec les fournisseurs.
2. Identifier le cadre juridique applicable
– Architecture générale et calendrier d'application de l'AI Act.
– Classification des systèmes selon leur niveau de risque.
– Pratiques interdites.

– Obligations de transparence.
– Systèmes d'IA à haut risque.
– Modèles d'IA à usage général et solutions d'IA générative.
– Obligations respectives des fournisseurs et des déployeurs.
– Surveillance humaine, journalisation, suivi du fonctionnement et gestion des incidents.
– Obligations particulières applicables à certaines organisations ou à certains secteurs.

3. Encadrer les données et protéger la vie privée

– Application des principes du RGPD aux projets d'IA.
– Détermination des finalités et des bases juridiques.
– Minimisation, transparence, exactitude et limitation de la conservation.
– Données anonymes et données pseudonymisées.
– Données utilisées pour l'entraînement, l'affinage ou l'évaluation des modèles.
– Exercice des droits dans les environnements d'IA.
– Identification des risques de régurgitation ou de mémorisation de données.
– Réalisation d'une DPIA et articulation avec la FRIA.
– Accès aux données, partage, portabilité et réversibilité au regard du Data Act et, lorsque cela est pertinent, du Data Governance Act et des règles relatives à la réutilisation des informations publiques.

4. Organiser la gouvernance, la sécurité et la supervision humaine

– Mise en place d'un comité ou d'une fonction de gouvernance de l'IA.
– Répartition des rôles entre direction, métiers, juristes, DPO, responsables informatiques et responsables de la sécurité.
– Désignation d'un responsable pour chaque cas d'usage.
– Processus d'autorisation des nouveaux usages.
– Formation et compétences des utilisateurs.
– Exigences de robustesse, d'exactitude et de cybersécurité.
– Risques propres aux systèmes d'IA : empoisonnement de données, attaques adversariales, manipulation des entrées, exfiltration d'informations ou compromission des modèles.
– Gestion des accès, sécurité des données, des modèles et des infrastructures.
– Journalisation, audits, mécanismes d'arrêt et procédures de repli.
– Coordination entre les incidents liés à l'IA, les violations de données et les incidents de cybersécurité.

5. Garantir la transparence, l'explicabilité et la non-discrimination

– Information des personnes lorsqu'elles interagissent avec un système d'IA.
– Marquage des contenus synthétiques et des deepfakes.
– Information des personnes affectées par un système d'IA à haut risque.
– Explication du rôle de l'IA dans un processus ou une décision.
– Prévention du « rubber-stamping » et organisation d'une intervention humaine effective.

– Documentation des données, critères, variables et corrections.
– Identification des biais et des variables de substitution susceptibles de produire des discriminations.
– Mise en place de tests d'équité et d'indicateurs de suivi.
– Garanties procédurales, voies de recours et réexamen humain.
– Exigences particulières de motivation et de transparence applicables aux organismes publics et aux décisions administratives.

6. Encadrer les fournisseurs et l'acquisition de solutions d'IA

– Due diligence préalable au choix d'un système ou d'un fournisseur.
– Documentation et preuves de conformité à demander.
– Répartition contractuelle des rôles et responsabilités.
– Accès aux journaux et à la documentation technique.
– Droits d'audit.
– Sécurité de la chaîne de sous-traitance.
– Localisation et transferts de données.
– Réversibilité et portabilité des données et artefacts.
– Gestion des mises à jour, changements de modèle et modifications substantielles.
– Clauses relatives au RGPD, à l'AI Act, à la cybersécurité et au Data Act.
– Adaptation de ces exigences aux contrats privés et, pour les organismes concernés, aux marchés publics et cahiers des charges.

7. Construire la charte IA en dix étapes

La formation présente une démarche opérationnelle permettant :

1. de cartographier les systèmes et cas d'usage ;
2. de qualifier les rôles de l'organisation et des fournisseurs ;
3. de classer les usages selon les catégories de l'AI Act ;
4. de définir la gouvernance et les responsabilités ;
5. d'identifier les évaluations d'impact requises ;
6. d'organiser la gouvernance des données ;
7. de définir les exigences de transparence et de supervision humaine ;
8. d'intégrer les exigences dans les contrats et procédures d'achat ;
9. de préparer la mise en production, les tests et la journalisation ;
10. d'organiser la surveillance continue, la gestion des incidents et les révisions périodiques.

8. Définir les douze rubriques essentielles de la charte

Les participants étudient une structure de charte comprenant notamment :
– les finalités et le périmètre des usages autorisés ;
– les usages interdits ou soumis à autorisation préalable ;
– les principes de nécessité, de proportionnalité, d'équité et de transparence ;
– la gouvernance et les responsabilités ;
– les règles relatives aux données et à la confidentialité ;
– les évaluations d'impact ;

– la supervision humaine ;
– la sécurité et la robustesse ;
– l'information des personnes et le marquage des contenus ;
– les règles d'acquisition et de gestion des fournisseurs ;
– la traçabilité, les audits et la gestion des incidents ;
– le contrôle, les sanctions internes et la révision périodique de la charte.

9. Mettre la charte en œuvre dans l'organisation

– Adoption et validation de la charte.
– Communication auprès du personnel et des parties prenantes.
– Formation à la maîtrise de l'IA prévue par l'AI Act.
– Procédure de déclaration ou d'autorisation d'un nouvel usage.
– Registre des systèmes et cas d'usage.
– Mise en place de notices d'information.
– Contrôles périodiques et indicateurs de performance.
– Gestion des changements de version et tests de non-régression.
– Révision de la charte en fonction des évolutions techniques, réglementaires et organisationnelles.

10. Outils, modèles et cas pratiques

La formation s'appuie sur des cas concrets, notamment :
– l'utilisation d'un assistant rédactionnel ou d'un copilote interne ;
– le déploiement d'un chatbot destiné à des clients, collaborateurs ou usagers ;
– l'utilisation d'un système de tri, de classement ou de priorisation ;
– l'utilisation de l'IA dans les processus de recrutement et de gestion des ressources humaines ;
– l'entraînement ou l'affinage d'un modèle sur des données propres ou issues du web ;
– l'utilisation de données provenant d'objets connectés ;
– l'intégration d'une fonctionnalité d'IA dans une solution SaaS.

Orateurs

Orateur

- **Jeoffrey Vigneron** : Avocat au barreau de Bruxelles, coding lawyer, co-fondateur du cabinet Lawgitech et spécialiste en intelligence artificielle

Informations pratiques

Date et horaire

Jeudi 3 septembre 2026, webinaire de 14h00 à 17h00
Vous pourrez suivre la formation en direct sur le Web. Vous recevrez les détails de connexion à l'avance par e-mail.
Attention ! L'adresse e-mail par laquelle vous procédez à l'inscription sera l'adresse à laquelle le lien vers le webinaire sera envoyé. Si vous vous inscrivez par l'intermédiaire

d'une autre personne (secrétaire, collègue…), cette personne devra vous faire suivre le lien en question pour que vous puissiez vous connecter et suivre la formation. Les inscriptions qui arrivent moins d'une heure avant le début du webinaire ne seront malheureusement pas prises en compte.

Prix
230,00 € TTC : inscription au webinaire

Documentation
Support préparé par l'orateur.

Publics visés
Cette formation s'adresse notamment :
– aux juristes et avocats ;
– aux délégués à la protection des données et responsables de la conformité ;
– aux responsables de la sécurité de l'information et de la cybersécurité ;
– aux directions informatiques, responsables de l'innovation et chefs de projets numériques ;
– aux responsables des ressources humaines, des achats et de la gestion des fournisseurs ;
– aux dirigeants et membres des organes de gouvernance ;
– aux administrations, organismes publics et entités chargées d'une mission de service public ;
– à toute personne chargée de préparer ou de mettre en œuvre une politique interne d'utilisation de l'intelligence artificielle.

Formation permanente
Une demande d'agrément a été introduite auprès d'AVOCATS.BE, avocats.lu et l'IJE.
Ce webinaire peut faire l'objet d'une prime Liberform si vous remplissez les conditions.

Renseignements complémentaires
Larcier-Intersentia
formations@larcier-intersentia.com
Numéro gratuit : 0800 39 067