A la croisée des Arts

AI Act : encadrement juridique et technique des systèmes d'IA

Note d'accompagnement pédagogique

Ce projet a pour objectif de mettre en relation deux groupes d'étudiants MSc DPO et DATA/IA, afin de collaborer sur la conception d'un produit IA qui touche aux données personnelles et constitue un risque élevé dans l'IA act en tant que système d'IA prenant des décisions de manière autonome ou supervisée ayant des conséquences potentielles sur des personnes physiques.

Chaque étudiant rejoint un groupe hybride DPO + DATA/IA et sera évalué selon la grille de compétences de sa formation.

Introduction du sujet

L'essor de l'intelligence artificielle générative marque une rupture technologique majeure.
Ces systèmes sont capables de produire du texte, des images, des sons ou des recommandations à partir d'ensembles de données massifs.
Leur usage soulève cependant de nouveaux défis juridiques et éthiques.

Du côté technique, les entreprises font face à un afflux de demandes d'idéation et d'innovation, pour rester concurrentielles et adopter de nouveaux usages, qui touchent de plus en plus intimement la vie privée et les données personnelles des

personnes physiques. Dans cet élan, de nombreuses solutions sont industrialisées sans que la conformité aux impératifs RGPD et IA act soit pleinement prise en compte. Il est d'autant plus important de former et mettre en place des habitudes liées à ce besoin de conformité, que les systèmes sont amenés à prendre des décisions automatisées. Expliciter, rendre lisible, permettre l'interaction avec un superviseur. Voici autant d'exigences de gestion de produits à intégrer dans la roadmap des architectures utilisant l'IA.

Le RGPD encadre déjà le traitement des données personnelles, en imposant transparence, sécurité et respect des droits fondamentaux. Désormais, l'AI Act (ou R.IA) , premier règlement européen dédié spécifiquement à l'intelligence artificielle, vient compléter ce dispositif en classant les usages de l'IA selon leur niveau de risque et en imposant des obligations de gouvernance et de contrôle.

Le projet proposé met les étudiants face à un cas pratique qui croise ces deux dimensions :

- *M2 DPO : analyser et encadrer les traitements impliquant données personnelles et décisions automatisées.*

- *M2 Data/IA : concevoir et développer les spécifications d'une architecture logicielle respectueuse des exigences de conformité.*

Réglementation	Type violation	Montant max	Exemples	Entreprises	Particularités
RGPD	Violations graves (art. 83.5)	20M€ ou 4% CA mondial	Traitement sans base légale, violations principes fondamentaux, non-respect droits des personnes	Toutes entreprises	CA du groupe pour filiales (CJUE 2025)
RGPD	Violations moins graves (art. 83.4)	10M€ ou 2% CA mondial	Défaut de coopération avec autorité, non-respect obligations responsable/sous-traitant	Toutes entreprises	Sanctions progressives possibles
IA Act	Pratiques interdites (art. 5)	35M€ ou 7% CA mondial	Manipulation cognitive, notation sociale, surveillance biométrique non autorisée	Toutes entreprises IA	PME/start-ups: montant le plus bas
IA Act	Obligations systèmes haut risque	15M€ ou 3% CA mondial	Défaut transparence, absence analyse impact, non-respect supervision humaine	Fournisseurs/déployeurs IA	Sanctions depuis août 2025
IA Act	Informations trompeuses	7,5M€ ou 1% CA mondial	Informations incorrectes aux autorités, documentation incomplète	Tous opérateurs IA	Sanctions procédurales

Les risques et obligations avec le RGPD et le RIA

Sujet

Conception et audit d'une IA générative pour recommandations personnalisées dans la fashion tech : enjeux RGPD et IA Act

Fournir une **étude avec mise en œuvre des principes du RGPD et de l'IA Act dans le contexte de l'IA générative**. Les étudiants devront évaluer les implications éthiques et juridiques de l'utilisation de modèles génératifs et proposer des solutions pour assurer la conformité.

Le projet plonge les étudiants dans le contexte d'une *start-up* qui souhaite développer une solution innovante d'IA, permettant à chaque utilisateur de recevoir des **recommandations personnalisées de vêtements et accessoires, à partir de photographies et autres données personnelles**.

L'IA analyse automatiquement des **données biométriques et personnelles** (morphologie, photo, âge, adresse, statut socio-professionnel, habitudes de navigation…) et les croise avec une large base de produits de consommation.

Une contrainte majeure du projet réside dans la gestion des exigences de l'entreprise qui développe la solution, comme (ce n'est qu'un exemple) le **module de filtrage automatisé selon l'âge** : l'admission des utilisateurs dépend exclusivement de l'âge estimé via l'IA à partir de la photo, et non de l'âge déclaré. Cette approche soulève des risques élevés en matière de

décision automatisée et de **traitement de données sensibles**, nécessitant une analyse approfondie des implications éthiques, juridiques et organisationnelles.

Les étudiants devront :

- **Évaluer et cartographier les risques**, en particulier les obligations et impacts liés au RGPD et à l'IA Act (registre, documentation, audit, gouvernance des données),
- Proposer des **solutions techniques et organisationnelles** de **mitigation des risques** permettant la conformité by design et by default,
- Répondre à un challenge en **conditions réalistes, sous pression** des parties prenantes (investisseurs, presse, supervision externe),
- Faire évoluer l'architecture logicielle et documenter tous les traitements et décisions automatisées, pour **présenter un cahier des charges et des spécifications conformes** à la fois aux demandes du client et aux obligations légales.

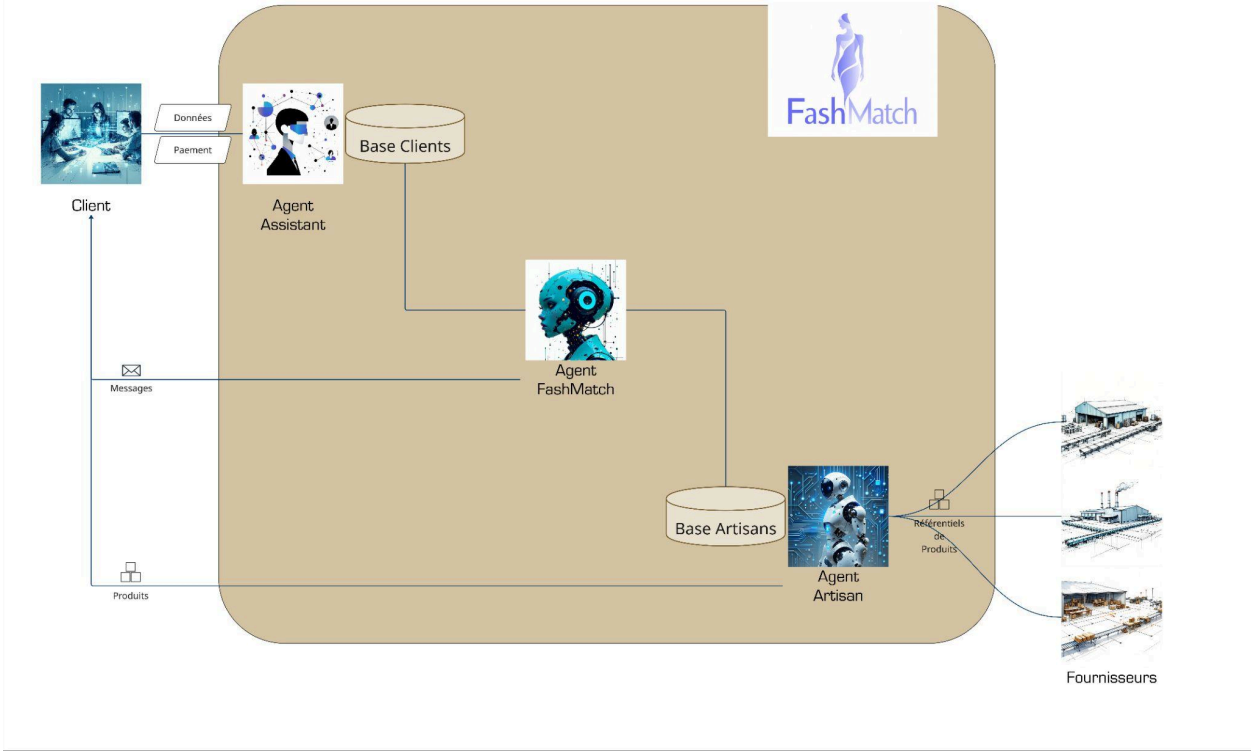
Mise en situation professionnelle

Contexte

*Vous rejoignez **FashMatch**, la startup de la fashion tech, qui vient d'attirer des investisseurs internationaux avec un produit phare : une application e-commerce hyper-personnalisée combinant IA générative, profiling avancé et production "kraftée" à la demande.*

*L'ambition : offrir à chaque client une expérience industrielle de l'artisanat, en exploitant l'ensemble de ses données pour créer des habits et accessoires absolument uniques. Le slogan "**Sortir du prêt-à-porter de masse pour créer l'individualisation industrielle**" guide le développement de l'application.*

*L'équipe dirigeante a imaginé un outil d'IA générative qui doit **permettre à chaque utilisateur de recevoir des recommandations de vêtements et d'accessoires parfaitement adaptés à son style**. Le projet bénéficie d'une forte visibilité : plusieurs médias spécialisés en innovation le présentent déjà comme "la prochaine licorne française de l'intelligence artificielle".*



Un prototype FashMatch V1 a été livré par l'équipe de développeurs et ingénieurs en IA, répondant aux besoins ci-dessous.

L'utilisateur crée un compte et transmet un ou plusieurs éléments multimédia : photos personnelles (tous formats), vidéos, extraits sonores, informations sur la famille (enfants, conjoints…), réseaux sociaux et contacts relationnels. L'IA va ensuite suivre le client et les tiers pour lesquels le client est inscrit, tout au long de leur existence. Le client est incité à partager ses contacts et remplir un formulaire pour mieux connaître ses idées, orientations, styles, préférences…

Le client doit être adulte (avoir plus de 16 ans, et un compte bancaire). L'outil intègre un module de filtrage : si l'IA estime que l'utilisateur a moins de 16 ans, le compte est automatiquement refusé, même si la personne a déclaré 18 ans.

Voici quelques fonctionnalités souhaitées :

- ***Analyse biométrique & physiologique** : suivi évolutif de la morphologie du client à travers ses photos/mois, vidéos d'activité physique et historique de sa santé (imc, poids, mobilité, chirurgie récente, etc.), croisé avec des banques d'images publiques.*
- ***Inscription à vie** pour un suivi intégral et personnalisé dans toutes les dimensions.*
- ***Profilage multidimensionnel** : extraction automatique de données relationnelles, religieuses, idéologiques, professionnelles, sentimentales via le contenu partagé (ex. : scan des réseaux sociaux, posts, "likes", commentaires, tags…).*
- ***Suivi familial** : association automatique de chaque achat à des membres de la famille (enfants, conjoints, parents, etc.). Création d'un historique interconnecté pour tracer l'évolution des besoins du foyer sur plusieurs années.*
- ***Monitoring communautaire** : constitution de graphes relationnels issus du parrainage, interactions sociales, achats entre amis — traçabilité avancée des influences et des "communautés" d'achat. Suggestions de groupes, challenges, tendances et produits co-brandés.*
- ***Système d'envoi automatique de produits de test** : sur la base de l'évolution du client (physique, goûts, communauté), et des changements contextuels (saisons, tendances, influenceurs suivis, étapes de vie), l'IA expédie au client, et à ses proches, des produits de test non demandés (retournables/remboursables après usage), pour maximiser la découverte et l'adoption de nouveautés.*
- ***Recommandation adaptive cross-profil** : suggestions non seulement sur la base du profil individuel mais aussi sur les évolutions comportementales, relationnelles et communautaires. Idem en cas de divorces, déménagement, changement de carrière : l'IA adapte radicalement les recommandations, sans sollicitation.*

- ***Envoi automatique en réseau*** *: partage forcé des recommandations et produits à tester auprès des contacts identifiés (parrainage, membres de communauté, proches), avec traçage des réactions et achats dérivés.*
- ***Scoring psycho-comportemental*** *: association à chaque utilisateur/famille d'un score d'évolution religieuse, idéologique, physique, sentimentale, permettant à FashMatch de prédire et influencer les achats.*
- ***Collecte illimitée de données sensibles et personnelles****, sans consentement explicite ni procédure de purge des données.*
- ***Traitement automatisé des exclusions et filtrages*** *: l'accès au service dépend exclusivement des critères calculés par l'IA : âge estimé, santé apparente, ou autres. Recours non prévu en cas de refus.*
- ***Décisions IA non-supervisées*** *: tout le cycle (de l'inscription à l'achat, SAV, recommendation et exclusions) est supervisé et piloté exclusivement par des algorithmes non explicables.*

Les exigences business associées à ce produit sont les suivantes:

- ***Maximisation du ROI*** *par l'exploitation de réseaux sociaux, profils familiaux, comportements évolutifs et communautés d'achat.*
- ***Automatisation intégrale de la chaîne d'expérience****, y compris la prospection, le scoring, l'envoi de produits non sollicités et la fidélisation.*
- ***Augmentation du panier moyen*** *via une identification proactive des recommandations, des cadeaux en réseau et des produits "imposés".*
- ***Capacités de "marketing préventif"*** *: identifier et influencer des envies encore non formulées à partir des signaux faibles relationnels, communautaires et psychologiques extraits.*
- ***Rétention et fidélisation*** *par constitution d'écosystèmes d'influence, observés et pilotés à partir d'analyses de réseaux sociaux et familiaux.*

Les ***fournisseurs*** *des produits FashMatch sont, partout dans le monde, des usines et des artisans qui automatisent à 100% la conception et la création des produits personnalisés. Le suivi des fournisseurs est intégré dans l'application, afin de fluidifier au maximum la création, l'usinage et la distribution des marchandises.*

Un exemple d'usage:

> *Marie s'inscrit sur FashMatch et envoie une photo selfie. À partir de cette image, l'IA analyse le visage et le corps (morphologie, silhouette, style vestimentaire apparent, couleurs dominantes), extrait automatiquement des proportions, points de repère faciaux, mensurations et associe ces données à un vaste dataset de produits (vêtements et accessoires collectés en ligne et en open source) afin de*

générer des propositions d'assortiments personnalisés. Marie entre alors dans le club FashMatch.

FashMatch propose rapidement quelques produits à Marie, adaptés par l'IA à son profil : vêtements pour le travail et la vie privée, accessoires de bureau et idées de cadeaux pour ses enfants.

***Le prototype FashMatch-V1 a été publié depuis 6 mois en early-access pour des clients sélectionnés et pour la presse**. Ce prototype a ainsi été **entraîné sur les données des premiers clients**.*

Un journaliste spécialisé en numérique vient de contacter la start-up pour obtenir des précisions sur l'utilisation des photographies et sur la conformité RGPD. En parallèle, un parent s'étonne que son enfant de 15 ans ait pu créer un compte en utilisant une photo d'identité retouchée sur la version BETA.

La direction générale vous convoque en urgence :

> ***"Nous avons communiqué partout que nous étions conformes au RGPD et à l'IA Act. Les investisseurs nous demandent des preuves.***
>
> *Nous devons être capables de présenter rapidement un dossier solide, à la fois **sur le plan règlementaire** et des **adaptations du cahier des charges du prototype!***
>
> *Vous avez cinq jours pour préparer un état des lieux et proposer des solutions!"*

En sortant de cette réunion, vos chefs d'équipes DPO et Data/IA vous demandent de travailler en groupe pour établir rapidement les besoins et monter en compétence sur les éléments techniques, juridiques et éthiques du produit. Vous devrez fournir les livrables ci-dessous.

Livrables attendus

En travail de groupe DPO+Data/IA:

- Les DPO doivent sensibiliser les DATA/IA pour le cadrage d'un projet sensible (avec données personnelles, enjeux RGPD et IA Act + risque lié à une décision automatisée)
- L'équipe Data/IA présente une formulation digeste des attentes techniques et fonctionnelles du client, en introduisant le vocabulaire incontournable de l'architecture, des spécifications et de l'expérience utilisateur à fournir.

Côté DPO :

- audit, recommandations, exigences, en classant les catégories de risques
- registre de la donnée pour RGPD
- registre pour IA Act

Côté Data/IA :

- Une étude des risques de la solution actuelle FashMatch-V1, non seulement en termes de conformité règlementaire, mais aussi à tous les niveaux touchant le développement, l'entraînement et l'usage de l'IA pour ce produit.
- Un cahier des charges pour cadrer et spécifier le produit de manière conforme aux exigences de l'équipe DPO, en intégrant toutes les mesures de mitigation des risques nécessaires.

Compétences visées

Compétences du groupe DPO

1. Analyse et gestion des risques juridiques

- Analyser le contexte d'une entreprise et ses activités pour déterminer le cadre juridique applicable.
- Réaliser une analyse d'impact sur la protection des données : recenser les traitements, identifier les risques (méthodes d'analyse de risques), établir une matrice de traitement des risques.

2. Mise en conformité et pilotage RGPD/IA Act

- Concevoir, mettre en place et maintenir un registre des traitements (traçabilité, identification des responsables).
- Formaliser les mesures de protection des données dès la conception (privacy by design & by default), adaptées aux risques et opérations.
- Définir et appliquer les actions nécessaires pour garantir la conformité aux réglementations.

3. Gouvernance et accompagnement

- Sensibiliser et former les utilisateurs/salariés à la protection des données et à la culture RGPD/IA, avec une démarche d'audit, de recommandations et de pédagogie.
- Accompagner l'organisation dans la gestion de ses obligations (tenue des registres, plans d'action, gestion des incidents, suivi des évolutions).

Compétences du groupe Data/IA

1. Pilotage technique et conformité des projets Data/IA

- Comprendre et intégrer les réglementations RGPD/IA Act dans la conception de solutions IA et le cadrage d'architectures logicielles.
- Construire et rédiger un cahier des charges fonctionnel et technique garantissant la conformité (spécifications, architecture, mesures de mitigation).

2. Développement, optimisation et évaluation

- Concevoir, développer, tester et documenter des applications IA/Data (Python, TensorFlow, Jupyter, CI/CD, Docker), en appliquant les règles sur la protection des données.
- Optimiser les solutions pour répondre à la qualité, l'écologie et l'accessibilité.
- Évaluer les implications éthiques et piloter le développement de la gouvernance IA, y compris l'explicabilité, l'audit et la gestion des risques.

3. Soft Skills et conduite de projet

- Organiser, prioriser, collaborer en équipe pluridisciplinaire (gestion de projet, résolution de conflits, leadership).
- Vulgariser les concepts techniques, communiquer clairement à des publics variés et synthétiser les résultats pour la direction ou des parties prenantes externes.

Rendu

Chaque groupe (constitué d'1 ou 2 étudiants DPO et 2 étudiants Data-IA), fournit plusieurs contenus, en plus d'une présentation commune. Le projet fera l'objet d'une soutenance de 45 minutes (30 min présentation, 10 min questions, 5 min retours) .

En commun

- un **espace Git intitulé "Croisée-des-arts"**, contenant l'ensemble des livrables demandés aux DPO et aux experts data/IA ci-dessous. En plus de ces livrables, vous fournissez les transparents d'un document powerpoint intitulé "présentation projet DPO-IA", qui récapitule l'ensemble des travaux pour à une présentation au CEO et au CTO de l'entreprise.

Les DPO

Une étude règlementaire est à rendre sous forme de Google doc, comprenant:

- Un plan et rapport d'audit, recommandations, exigences, en classant les catégories de risques (RGPD et IA Act)
- Un registre d'activités de traitement (RGPD)
- Un registre des SIA

Envoyez ces documents à l'adresse :

Msc-DPO-ResponsablesPedagogiques@laplateforme.io

Les Data-IA

- L'analyse de risques data/IA (pas uniquement RGPD et IA-Act) assortie des recommandations de mitigation que vous aurez préconisées.
- Le cahier des charges, au format doc, incluant
    - un schéma d'architecture proposé pour répondre à l'ensemble des besoins de conformité
    - un ensemble de spécifications conformes aux exigences et aux mitigations préconisées

Base de connaissances

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

https://artificialintelligenceact.eu/fr/

https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/

https://www.cnil.fr/fr/entree-en-vigueur-du-reglement-europeen-sur-lia-les-premieres-questions-reponses-de-la-cnil