



Guide relatif aux données, aux outils et aux conditions d'usage des systèmes d'IA

Guide relatif aux données, aux outils et aux conditions d'usage des systèmes d'IA

I. Introduction

L'utilisation de systèmes d'intelligence artificielle dans les services support et les activités administratives de l'Université implique des enjeux importants en matière de protection des données, de sécurité des systèmes d'information, de conformité réglementaire et de maîtrise des environnements numériques mobilisés. Les outils d'intelligence artificielle peuvent en effet traiter, analyser, conserver ou réutiliser des informations présentant des niveaux variables de sensibilité, dans des contextes impliquant des obligations particulières de confidentialité, de sécurité et de responsabilité.

Dans ce contexte, les conditions d'usage des systèmes d'intelligence artificielle doivent être adaptées à la nature des données manipulées, aux garanties offertes par les outils mobilisés ainsi qu'aux exigences réglementaires et institutionnelles applicables aux activités administratives et aux missions de service public de l'établissement.

La présente section vise à préciser les principes encadrant l'utilisation des systèmes d'intelligence artificielle dans les services administratifs, à rappeler les exigences relatives à la protection des données et à proposer un cadre d'aide à la décision permettant d'orienter le choix des solutions pouvant être mobilisées selon la nature et le niveau de sensibilité des données traitées.

II. Protection des données et encadrement des usages de l'intelligence artificielle

Les usages de l'intelligence artificielle dans les services support et les activités administratives impliquent des niveaux variables de sensibilité des données et des exigences particulières en matière de protection, de confidentialité, de sécurité et de conformité réglementaire.

Les données manipulées dans ce cadre peuvent notamment concerner :

- des données publiques ;
- des données internes non sensibles ;
- des données administratives internes sensibles ;
- des données à caractère personnel au sens du RGPD ;
- des données pédagogiques ;
- des données de recherche ;
- des données contractuelles ou partenariales ;
- des données protégées par la propriété intellectuelle.

L'utilisation de systèmes d'intelligence artificielle nécessite une vigilance renforcée concernant la circulation des données, les modalités de conservation et de traitement des informations, les risques de réutilisation des contenus transmis ainsi que la maîtrise des environnements techniques mobilisés.

Les informations saisies dans un système d'intelligence artificielle peuvent être transmises au fournisseur du service, conservées, analysées, utilisées pour l'entraînement des modèles, réutilisées ou exploitées dans les conditions prévues par les politiques d'utilisation des plateformes concernées. Elles peuvent également être hébergées sur des infrastructures situées hors de l'Union européenne, dans des conditions ne permettant pas toujours de garantir un niveau suffisant de maîtrise, de traçabilité ou de protection des traitements réalisés.

Tous les outils d'intelligence artificielle ne présentent pas les mêmes garanties en matière :

- de sécurité des données ;
- de confidentialité des traitements ;
- de gouvernance des informations ;
- de conformité réglementaire ;
- de maîtrise des conditions d'utilisation ;
- de souveraineté numérique ;
- de contrôle institutionnel des traitements.

Les conditions d'usage des outils d'intelligence artificielle doivent donc être adaptées à la nature et au niveau de sensibilité des données traitées afin de garantir la protection des activités administratives et la maîtrise des risques associés.

Les utilisateurs demeurent responsables des données, documents et contenus introduits dans les systèmes d'intelligence artificielle mobilisés dans le cadre de leurs activités professionnelles.

En conséquence, toute manipulation de données sensibles, personnelles, administratives, contractuelles, stratégiques, confidentielles ou non publiques doit être réalisée exclusivement au moyen d'outils ou d'infrastructures explicitement validés par l'Université Paris 8.

À titre d'exemple, ne doivent pas être introduits dans des outils ne présentant pas les garanties suffisantes de sécurité, de confidentialité et de conformité :

- des données personnelles non anonymisées ;
- des contenus soumis à des obligations de confidentialité ;
- des données de recherche non publiques ;
- des documents contractuels ou partenariaux ;

- des contenus protégés par la propriété intellectuelle ;
- des informations permettant d'identifier directement ou indirectement des étudiants, personnels, partenaires ou usagers de l'établissement.
- de solutions d'intelligence artificielle déployées sur les infrastructures de l'université et gérées par la DSI ;
- de solutions d'intelligence artificielle installées localement sur des postes institutionnels gérés par la DSI (solutions locales ou isolées sur postes institutionnels gérés par la DSI).

Les données ne pouvant être rendues publiques sans restriction ne doivent pas être saisies dans un système d'intelligence artificielle ne présentant pas les garanties nécessaires en matière de sécurité, de conformité réglementaire, de protection des données, de localisation des traitements et de maîtrise institutionnelle des usages.

La transmission d'un document administratif à un système d'intelligence artificielle externe peut juridiquement être analysée comme une communication à un tiers.

En application notamment :

- du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des données à caractère personnel (RGPD) ;
- du règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act) ;
- du Code des relations entre le public et l'administration ;
- du Code du patrimoine ;
- du Code de la propriété intellectuelle ;

Les documents transmis ou générés dans le cadre d'une mission de service public peuvent être soumis à des obligations particulières de protection, de conservation, de communicabilité et de confidentialité.

Ces environnements présentent des niveaux variables de maîtrise, de sécurité, de confidentialité, de gouvernance des données et de conformité réglementaire.

Le choix des solutions mobilisées doit être apprécié au regard :

- de la nature des données traitées ;
- de leur niveau de sensibilité ;
- des contraintes réglementaires et contractuelles applicables ;
- des besoins de sécurité et de confidentialité ;
- des capacités de maîtrise technique des environnements utilisés.

Une attention particulière doit être portée :

- aux conditions d'utilisation des services mobilisés ;
- à la localisation des infrastructures et des serveurs ;
- aux modalités de traitement et de conservation des données ;
- aux garanties proposées en matière de sécurité et de protection des données ;
- aux risques de transfert, de captation ou de réutilisation non maîtrisée des informations transmises.

L'Université encourage, lorsque cela est possible, le recours à des environnements maîtrisés, à des infrastructures sécurisées ainsi qu'à des solutions institutionnelles ou académiques permettant de renforcer la maîtrise des données, la sécurité des traitements et la souveraineté numérique de l'établissement.

Les modalités d'usage des outils d'intelligence artificielle doivent demeurer cohérentes avec les politiques institutionnelles relatives à la protection des données, à la sécurité des systèmes d'information, aux référentiels de gestion des données et aux règles applicables au sein de l'Université Paris 8.

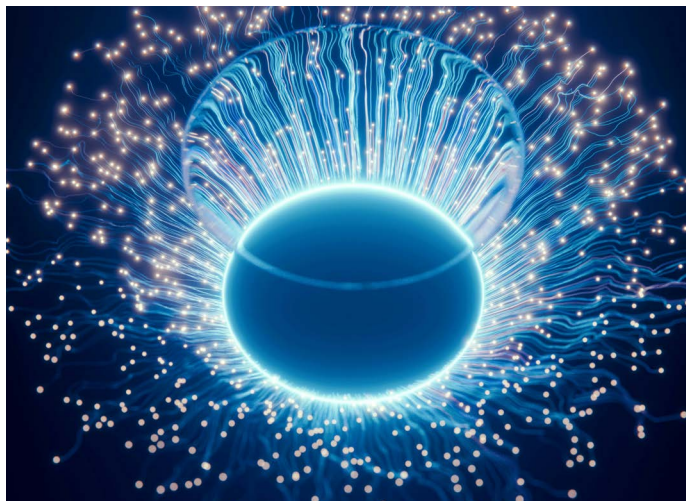
III. Conditions de recours aux solutions d'intelligence artificielle

Le choix d'une solution d'intelligence artificielle ne peut être dissocié de la nature des données manipulées et du niveau de maîtrise des environnements techniques mobilisés.

Selon leur mode de déploiement, d'hébergement et de gouvernance des données, les solutions d'intelligence artificielle peuvent relever :

de services d'intelligence artificielle grand public, accessibles directement par les utilisateurs via des plateformes ouvertes (services grand public) (ex. ChatGPT, Gemini, Le Chat de Mistral AI) ;

- de services d'intelligence artificielle professionnels ou institutionnels, bénéficiant de garanties contractuelles spécifiques en matière de sécurité, de confidentialité ou de protection des données (services professionnels ou institutionnels) (ex. ChatGPT Enterprise, Microsoft Copilot for Microsoft 365, Mistral Le Chat Enterprise) ;
- de solutions d'intelligence artificielle académiques ou mutualisées, proposées par des établissements publics, organismes de recherche ou infrastructures de l'enseignement supérieur et validées par la DSI (ex. RAG Rennes, supercalculateur Jean Zay) ;



IV. Matrice d'aide à la décision pour l'usage des solutions d'intelligence artificielle selon la nature des données

Afin d'accompagner les services dans l'application des principes précédemment exposés, la matrice suivante propose une aide à la décision permettant d'orienter l'usage des différentes solutions d'intelligence artificielle en fonction de la nature et du niveau de sensibilité des données traitées.

Cette matrice vise à garantir la protection des données, la conformité réglementaire, la sécurité des usages et une utilisation responsable des outils d'intelligence artificielle au sein de l'établissement. Elle constitue

un outil d'appui destiné à faciliter l'identification des environnements pouvant être mobilisés selon les catégories de données concernées. Elle ne se substitue ni aux obligations légales applicables, ni aux procédures internes de validation et de sécurisation mises en œuvre par l'Université.

 Catégories de données	 Service grand public	 Services professionnels ou institutionnels	 Solutions académiques ou mutualisées validées par la DSI	 Infrastructures de l'Université gérées par la DSI	 Solutions locales ou isolées sur postes gérés par la DSI
Données publiques 	Sous conditions 	Sous conditions 	Autorisé 	Autorisé 	Autorisé 
Données internes non sensibles 	Interdit 	Sous conditions 	Autorisé 	Autorisé 	Autorisé 
Données administratives internes sensibles 	Interdit 	Interdit 	Interdit 	Sous conditions 	Sous conditions 
Données à caractère personnel (RGPD) 	Interdit 	Sous conditions 	Sous conditions 	Sous conditions 	Sous conditions 
Données de recherche (hors RGPD) 	Interdit 	Sous conditions 	Autorisé 	Autorisé 	Autorisé 
Ressources pédagogiques (hors données étudiantes et évaluations) 	Interdit 	Sous conditions 	Autorisé 	Autorisé 	Autorisé 
Données contractuelles et partenariales 	Interdit 	Sous conditions 	Sous conditions 	Autorisé 	Autorisé 
Données protégées par la propriété intellectuelle 	Interdit 	Interdit 	Autorisé 	Autorisé 	Autorisé 