UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Recommandation des Correspondantes à la protection des données (DPOs)
Usage des données avec les outils IA dans l'exercice de son activité à l'Université de Fribourg

Version 1 du 21 octobre 2026
Cette Recommandation peut être mise à jour régulièrement pour suivre l'évolution rapide de l'intelligence artificielle.

I. Champ d'application

La présente recommandation s'applique à l'usage de données dans des systèmes faisant appel à des technologies d'intelligence artificielle, quelle qu'en soit la forme ou la finalité, notamment IA générative, analytique, conversationnelle, décisionnelle ou agentique (ci-après « outils IA »), dans le cadre de l'activité professionnelle à l'Université.

1. Par usage de données, on entend toute opération réalisée à l'aide d'un outil IA portant sur des données, qu'il s'agisse de leur introduction dans le système (prompts, fichiers, bases de données, flux automatisés), de leur traitement par le système ou de l'utilisation des contenus générés en sortie.

2. La présente recommandation couvre :
   - les outils IA mis à disposition par des fournisseurs tiers, à titre gratuit ou payant ; et
   - les outils IA développés, adaptés ou déployés par le personnel de l'Université.

3. La présente recommandation couvre :
   - les utilisations ponctuelles d'outils IA (ex. la rédaction de textes ou d'emails, le brainstorming sur un thème ; l'aide à la formulation pour les textes déjà existants, les traductions, …) ; et
   - les projets particuliers ou utilisations spécifiques d'outils IA, y compris les projets pilotes et proof-of-concept.

Cette recommandation se fonde sur la Loi du 12 octobre 2023 sur la protection des données du canton de Fribourg.

II. Principe

Les données personnelles – y inclus les données personnelles sensibles – et les informations confidentielles ou soumises au secret de fonction, ainsi que tout document contenant de telles données, ne doivent pas être utilisées avec des outils IA, sauf dans le cadre des usages encadrés.

Se référer à l'Annexe 1 pour les définitions des données personnelles, données personnelles sensibles, et informations confidentielles ou soumises au secret de fonction. Les usages encadrés sont décrits dans la section III.

Les données personnelles anonymisées ne sont pas soumises à l'interdiction de principe d'utilisation avec des outils IA, si la réidentification des personnes n'est plus possible sans efforts disproportionnés.
Se référer à l'Annexe 1 pour des explications détaillées.

III. Usages encadrés

Usage encadré n. 1 – Utilisation de Microsoft Copilot Chat Basic

Microsoft Copilot Chat Basic[1] peut être utilisé avec des données personnelles et des informations confidentielles ou soumises au secret de fonction. **En revanche, les données personnelles sensibles ne doivent pas être utilisées dans Microsoft Copilot Chat Basic.**

> Microsoft Copilot Chat Basic est un outil institutionnel mis à disposition de tous les collaborateurs et collaboratrices de l'Université par la DIT. Son usage est encadré par un contrat avec Microsoft qui offre des garanties en termes de protection des données personnelles et de confidentialité, notamment la non-réutilisation des données pour le renforcement de l'algorithme commercial (données d'entraînement).

Important

- Les garanties de protection associées à Microsoft Copilot Chat Basic s'appliquent uniquement lorsque l'utilisateur ou l'utilisatrice est connecté-e avec son compte institutionnel Unifr. Un bouclier vert apparaît en haut à droite de la fenêtre.
- Pour renforcer la confidentialité de l'utilisation de Microsoft Copilot Chat Basic, il est possible de désactiver la fonction « Web Search »[2].

Usage encadré n. 2 – Usage présentant un risque élevé

Pour les projets présentant un risque élevé, le traitement de données personnelles ou d'informations confidentielles ou soumises au secret de fonction avec un outil IA n'est autorisé que si :

- le traitement a fait l'objet d'une **analyse d'impact sur la protection des données** (AIPD) ; et
- **le niveau de risques identifié par l'AIPD est accepté** par l'organe compétent conformément à la procédure AIPD applicable[3].

Sont notamment considérés comme présentant un risque élevé les traitements avec un outil IA impliquant :

- l'usage de données personnelles **sensibles** ;
- l'usage d'informations **hautement confidentielles** ;
- l'évaluation, la classification, la notation, la prévision ou le profilage de personnes portant sur des aspects personnels ou le comportement ;
- la surveillance ou le suivi systématique du comportement de personnes ;

[1] Cet usage encadré ne s'applique pas à Microsoft 365 Copilot, qui constitue un service distinct nécessitant un abonnement supplémentaire.

[2] Lors de l'utilisation standard de Copilot Chat Basic, Microsoft analyse la requête (prompt) et identifie les termes pour lesquels des informations provenant du web permettraient d'améliorer la qualité de la réponse. À partir de ces termes, Copilot génère une requête de recherche qu'il envoie au service de recherche Bing afin d'obtenir davantage d'informations.
Pour désactiver la fonction websearch : ouvrir le menu Chat settings>Personalisation>Advanced.

[3] La procédure AIPD est actuellement en cours d'élaboration. Pour toute question, vous pouvez contacter les DPOs à l'adresse suivante : dpo@unifr.ch.

- un traitement de données à grande échelle compte tenu notamment du nombre de personnes concernées, du volume des données traitées, de la durée du traitement ou de sa portée géographique ;
- une décision individuelle automatisée ou semi-automatisée, produisant des effets juridiques ou d'autres effets significatifs pour les personnes concernées ;
- un traitement susceptible de priver une personne de l'accès à un service, de l'empêcher de conclure un contrat, ou de limiter l'exercice ou l'obtention d'un droit.

Important : L'usage de Microsoft Copilot Chat Basic n'est pas autorisé en l'absence d'une AIPD approuvée pour les projets présentant un risque élevé.

Une AIPD est une analyse approfondie et structurée du traitement de données projeté, des risques associés et des mesures de protection à mettre en œuvre.

Il s'agit d'un outil standard prévu par la législation sur la protection des données en cas de traitement de données personnelles qui présente des risques élevés pour les personnes concernés.

La réalisation d'une AIPD représente un travail conséquent. Cet investissement est néanmoins indispensable afin de s'assurer que les risques sont identifiés, évalués et maîtrisés de manière appropriée avant la mise en œuvre du projet.

Les DPOs mettent à votre disposition un guide pour la réalisation d'une AIPD et vous soutiennent dans cette démarche, en collaboration avec d'autres services (notamment la DIT et le ou la Responsable sécurité informatique).

Usage encadré n. 3 – Usage ayant fait l'objet d'une analyse des risques

Pour les projets ne présentant pas de risque élevé, le traitement des données personnelles ou d'informations confidentielles ou soumises au secret de fonction avec un outil IA est autorisé si :

- **une analyse de risques a été réalisée au préalable ; et**
- **le niveau de risques identifié par cette analyse est accepté par le collaborateur ou la collaboratrice qui est responsable de ce traitement.**

Les DPOs mettent à votre disposition un guide pour la réalisation de l'analyse de risques et vous soutiennent dans cette démarche, en collaboration avec d'autres services (notamment la DIT et le ou la Responsable sécurité informatique).

Dans l'hypothèse où les DPOs estiment que le niveau de risques accepté n'est pas approprié au regard des enjeux identifiés, ils ou elles peuvent en référer au supérieur administratif ou à la supérieure administrative de la personne responsable du traitement.

Usage encadré n. 4 – Usage sur des infrastructures locales

L'utilisation de données personnelles, y compris de données personnelles sensibles, ainsi que d'informations confidentielles ou soumises au secret de fonction, au moyen d'outils d'IA déployés exclusivement sur des infrastructures ou sur des serveurs de l'Université, est autorisée, pour autant que ces outils ne permettent aucun échange de données avec des systèmes externes à l'infrastructure universitaire.

> Le caractère fermé de l'outil d'IA doit être validé préalablement par le ou la Responsable de la sécurité informatique.

Annexe 1 – Définitions

1. Données personnelles

Définition **:** informations qui se rapportent, directement ou indirectement à une personne, qu'importe leur forme, leur contenu ou leur support.

Certaines données sont directement identifiantes (nom, prénom, email, n. AVS, …). D'autres données sont indirectement identifiantes (date de naissance, lieu d'habitation précis, …).

Les données qui pourraient permettre d'identifier des personnes selon le contexte ou en corrélation avec d'autres informations sont aussi des données personnelles.

Forme : Les données personnelles peuvent prendre toute forme : donnée textuelle, donnée audio, image, enregistrement vidéo, … La voix et l'image d'une personne sont des données personnelles.

2. Données personnelles sensibles

Les données personnelles sensibles sont une sous-catégorie des données personnelles. Sont des données personnelles sensibles :

- les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales;
- les données sur la santé, la sphère intime ou l'origine raciale ou ethnique;
- les données génétiques;
- les données biométriques identifiant une personne physique de manière univoque;
- les données sur des mesures d'aide sociale;
- les données sur des poursuites ou des sanctions pénales et administratives.

3. Données anonymisées

Les données anonymisées ne sont plus considérées comme des données personnelles.

L'anonymisation est un procédé technique qui consiste à **modifier de façon irréversible** les données personnelles afin qu'elles **ne puissent plus être liées à une personne spécifique**, sans efforts disproportionnés.

Pour déterminer si une réidentification est possible sans efforts disproportionnés, il faut tenir compte de l'ensemble des moyens raisonnablement susceptibles d'être utilisés et de l'ensemble des circonstances. Il faut apprécier concrètement le risque de réidentification et les moyens raisonnablement susceptibles d'être mobilisés pour permettre la réidentification d'une personne. Le coût et le temps nécessaires à la réidentification, ainsi que les technologies disponibles et leur évolution prévisible, sont des critères à prendre en considération.

En raison des capacités particulièrement puissantes des outils d'IA en matière d'analyse, de corrélation et d'inférence, le risque de réidentification ne doit pas être sous-estimé. L'évaluation de ce risque doit tenir compte de la possibilité que des données apparemment anonymisées puissent être associées à d'autres informations et conduire à l'identification directe ou indirecte de personnes.

Le seul remplacement des données directement identifiantes par un code **(données codées ou pseudonymisées**) n'équivaut pas à une anonymisation des données. Il s'agit souvent uniquement d'une étape du procédé d'anonymisation, qui n'est pas forcément suffisante pour retenir que les données personnelles ne peuvent plus être liées à une personne spécifique sans efforts disproportionnés.

4. Informations confidentielles ou soumises au secret de fonction

Les informations confidentielles ou soumises au secret de fonction sont les informations dont vous avez connaissance dans l'exercice de vos tâches et qui ne sont pas publiques.

Exemples : procès-verbaux de commissions ou de séances non publiques, dossiers d'étudiant-e-s, dossiers de candidatures, examens d'étudiant-e-s, correspondance interne, données qui sont couvertes par une obligation contractuelle de confidentialité.

Sont comprises toutes les informations dont la divulgation à des tiers non autorisés serait susceptible de porter atteinte aux intérêts, aux activités, au patrimoine, à la sécurité, à la réputation ou au bon fonctionnement de l'Université ou de ses partenaires.

Les **informations hautement confidentielles** sont informations dont la divulgation à des tiers non autorisés serait susceptible de porter une **atteinte grave** aux intérêts, aux activités, au patrimoine, à la sécurité, à la réputation ou au bon fonctionnement de l'Université ou de ses partenaires.

Dans la recherche, il est conseillé de qualifier de confidentielles :

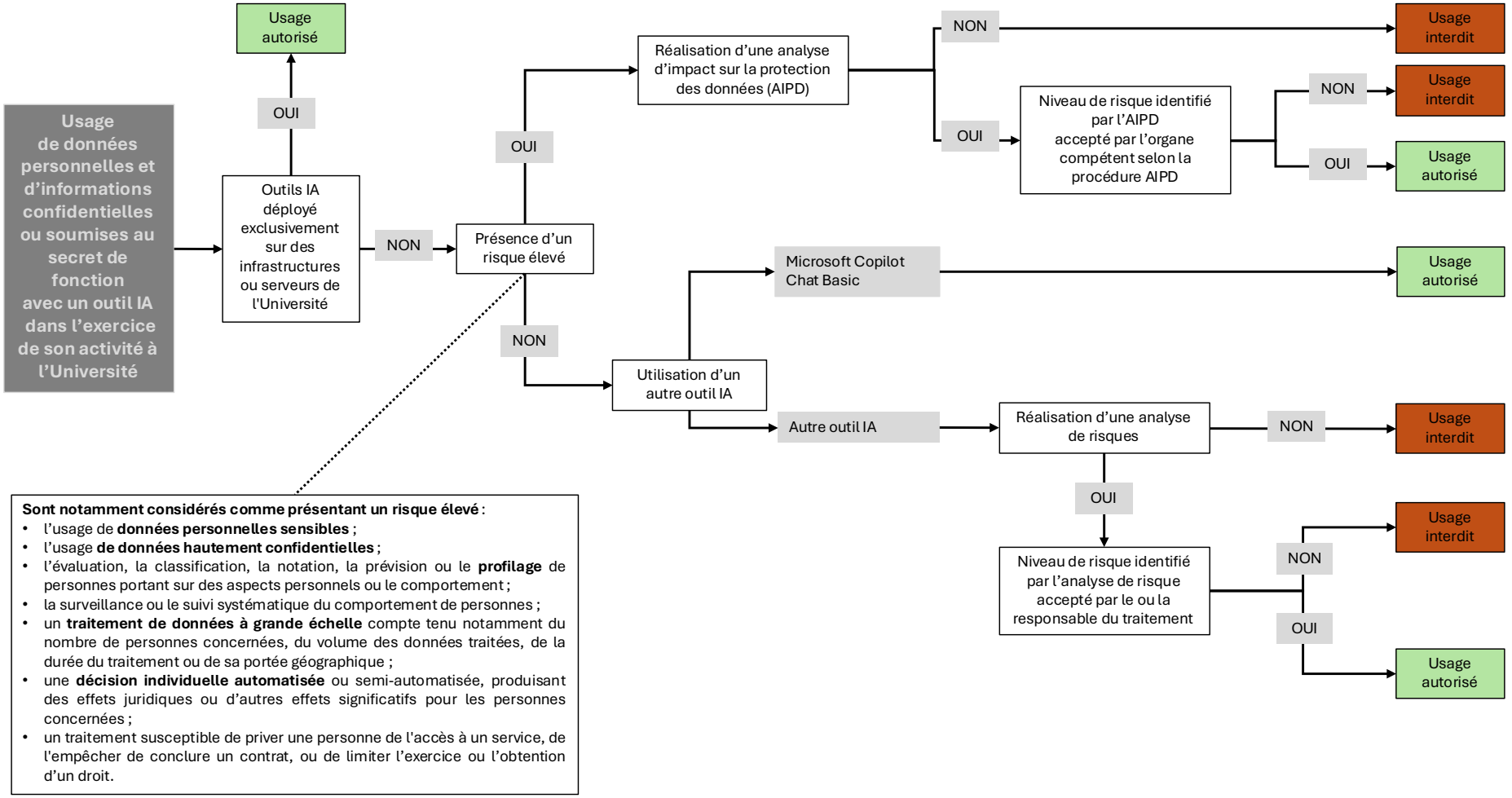
- les données et résultats de recherche qui n'ont pas encore fait l'objet d'une publication scientifique ;
- les données et résultats qui pourraient avoir une valeur commerciale et/ou mener au dépôt d'un brevet ;
- les donnée pour lesquelles l'Université ou vous ne détenez pas les droits de propriété intellectuelle ;
- toute autre donnée ou résultat que vous considérez comme confidentiel dans le cadre de la recherche (par exemple dual use case).

Les informations confidentielles ou soumises au secret de fonction contiennent souvent des données personnelles, raison pour laquelle il est cohérent de les traiter dans la même recommandation.

Besoin d'aide

En cas de doute si une donnée, une information ou un document concret doit être considéré comme une donnée personnelle, une donnée personnelle sensible, une information confidentielle ou soumise au secret de fonction, ou si des données peuvent être considérée comme anonymisées, vous pouvez vous renseigner auprès des DPOs (dpo@unifr.ch).

Annexe 2 – Diagramme représentatif des usages autorisés ou interdits



Ce schéma est fourni à titre illustratif et vise à faciliter la compréhension de la Recommandation des DPOs du 21 octobre 2026. Il ne remplace pas le texte de la Recommandation, qui seul fait foi.

Annexe 3 - Pourquoi encadrer l'usage des données avec des outils IA

Malgré les efforts déployés par les fournisseurs d'outils IA en proposant des options de protection des données, aucun outil IA en ligne ne peut garantir à 100% la confidentialité des données qui y sont introduites. Bien que les algorithmes des outils IA offrent des capacités d'analyse et de synthèse puissantes, leur utilisation doit rester conforme au droit. Assurer la protection des données personnelles et la confidentialité des informations est non seulement une exigence éthique mais aussi une obligation légale.

Les risques légaux majeurs de l'utilisation de données personnelles ou confidentielles ou soumises au secret de fonction dans des outils IA sont :

- la fuite de données entraînant une violation de l'obligation de confidentialité, du secret de fonction ou du secret professionnel
- la fuite de données stratégiques entraînant une atteinte aux intérêts, aux activités, au patrimoine, à la sécurité, à la réputation ou au bon fonctionnement de l'Unifr ou de ses partenaires
- la réutilisation illicite de données personnelles pour l'entraînement des solutions
- le risque de profilage
- un transfert international illicite de données personnelles
- une externalisation illégale d'un traitement de données personnelles

S'y ajoutent les risques généraux de l'usage de l'IA, dont les conséquences peuvent être d'autant plus critiques en cas d'usage avec des données personnelles ou confidentielles :

- Manque de transparence des systèmes : difficulté à comprendre la manière dont la solution IA fonctionne et à expliquer pourquoi elle a donné tel résultat (boîte noire).
- Hallucinations ou contenus inventés
- Informations erronées ou inexactes
- Absence de vérification des sources utilisées par l'IA
- Biais et discrimination dans les résultats produits
- Dépendance excessive à l'IA entraînant une perte de savoir interne et d'esprit critique