POLYNESIE FRANÇAISE

Le Président

N° 000444 /PR

Papeete, le 27 JAN 2026

à

SECRÉTARIAT GÉNÉRAL
Arrivée le : 28 JAN. 2026
N°: 678

Madame la Vice-Présidente,
Mesdames et Messieurs les ministres,
Mesdames et Messieurs les chefs de services

Objet : Circulaire fixant la charte relative à l'usage de l'intelligence artificielle par le Gouvernement et les services de la Polynésie française.

Réf. : Loi n° 78-17 du 17 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (règlement général sur la protection des données)
Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle)
Délibération n° 95-215 AT du 14 décembre 1995 portant statut général de la fonction publique de la Polynésie française
Code pénal ; articles 226-16 à 226-24 et 323-1 à 323 -7

Mesdames, Messieurs,

La présente circulaire fixe la charte relative à l'utilisation de l'intelligence artificielle par le Gouvernement et les services de la Polynésie française. La présente charte s'applique immédiatement.

PREAMBULE

L'Intelligence Artificielle (IA) évolue rapidement et transforme en profondeur de nombreux secteurs, dont les services publics. L'administration du Pays commence à intégrer des outils d'IA pour gagner en efficacité, automatiser certaines tâches ou faciliter l'analyse de l'information.

L'IA ouvre de nouvelles perspectives pour notre administration : automatisation et gain de temps pour les missions à forte valeur ajoutée, modernisation et simplification des processus, amélioration

B.P. 2551 , 98713 Papeete – TAHITI, Polynésie française – Quartier Broche, – Avenue Pouvanaa a OOPA
Tél. : (689) 40 47 20 00 - Fax. : (689) 40 47 21 10 - Email : capr@presidence.pf - http://www.presidence.pf

des interactions avec les usagers et de la qualité des prises en charge, analyse et optimisation des politiques publiques. Les bénéfices peuvent être nombreux.

Pour en tirer pleinement avantage, l'administration doit encourager l'innovation, dans le respect des réglementations et de l'intérêt des usagers. Pour cela, elle doit établir un cadre clair, garantissant la sécurité des données, la conformité au droit, les valeurs du service public et la maitrise des impacts environnementaux.

Cette transformation soulève en effet des enjeux majeurs en matière de protection des données, éthique, fiabilité et responsabilité. Un usage inadapté ou non encadré de l'IA peut exposer les usagers ou les services à des risques.

OBJET ET PERIMETRE DE LA CHARTE

La présente charte établit des principes clairs et accessibles afin d'encadrer les usages de l'IA dans les services de l'administration pour :

- garantir un usage responsable, éthique et maîtrisé des systèmes d'IA ;
- s'assurer que l'ensemble des agents dispose d'une compréhension suffisante des risques liés à leur utilisation.

Elle encadre les usages de l'IA dans les activités professionnelles des agents, y compris lorsqu'elles sont réalisées en dehors du lieu de travail, dès lors qu'elles sont effectuées pour les besoins du service.

La charte a pour objet de protéger les usagers, sécuriser les pratiques professionnelles et permettre aux agents d'utiliser ces technologies de manière efficace, sans compromettre la légalité, la confidentialité des données ou la sécurité du service.

Elle s'applique à l'ensemble des outils d'IA utilisés dans un cadre professionnel, qu'ils soient mobilisés pour la rédaction de contenus, la synthèse d'informations, la recherche documentaire, l'automatisation de tâches ou intégrés à un logiciel métier.

Elle s'applique à compter de sa signature à l'ensemble du Gouvernement de la Polynésie française et ses services administratifs.

TERMINOLOGIE ET RISQUES IDENTIFIES

L'intelligence artificielle repose sur des procédés automatisés fondés sur des algorithmes permettant d'exécuter des tâches déterminées et, dans certains cas, de reproduire des comportements associés au raisonnement ou à la création. Lorsqu'elle est intégrée dans une application complète incluant des données, une interface et des règles de gestion, elle constitue un système d'IA susceptible d'influencer des décisions, des recommandations ou des contenus.

À ce titre, son usage soulève des risques majeurs qu'il convient d'identifier, de prévenir et d'encadrer.

Risque de biais et de discriminations : Les modèles d'IA, et notamment les modèles de langage de grande taille, fonctionnent de manière probabiliste et peuvent reproduire ou amplifier les biais présents dans leurs données d'entraînement ou issus de choix de conception et d'optimisation.

Ces biais correspondent à des distorsions dans les résultats pouvant conduire à des traitements inéquitables ou discriminatoires fondés notamment sur l'âge, le genre ou l'origine.
Il est donc nécessaire d'encadrer strictement les cas d'usage, de tester régulièrement les effets de biais, de documenter les limites connues des systèmes et de maintenir une responsabilité humaine dans l'interprétation et l'utilisation des résultats produits.

Manque de transparence et perte d'explicabilité : Certains systèmes d'IA présentent un fonctionnement complexe rendant difficile la compréhension des mécanismes ayant conduit à un

résultat donné. Ce manque de transparence peut empêcher de justifier une décision, d'en contester le fondement ou d'en expliquer les effets aux personnes concernées.

Cette opacité accroît le risque de perte de contrôle humain et impose que tout usage d'un système d'IA soit assorti d'un contrôle humain effectif, ainsi que d'une documentation permettant d'expliquer son fonctionnement général et de justifier les résultats obtenus.

Erreurs, contenus inexacts ou inventés (« hallucinations ») : Les systèmes d'intelligence artificielle générative, capables de produire des contenus textuels, graphiques ou audiovisuels, présentent des risques spécifiques. Ils peuvent générer des contenus erronés, incomplets ou entièrement inventés, tout en leur donnant une apparence crédible.

Ces phénomènes, appelés « hallucinations », rendent ces outils impropres à un usage non contrôlé, en particulier lorsque les contenus produits ont une portée juridique, réglementaire ou décisionnelle.

Les productions issues de l'IA générative doivent impérativement être relues, confrontées à des sources fiables et validées par un agent avant toute utilisation ou diffusion.

Atteinte à la vie privée et protection des données personnelles : L'usage d'un outil d'IA non maîtrisé peut entraîner la collecte, le traitement ou la divulgation de données à caractère personnel sans base légale, en méconnaissance des principes du RGPD, notamment ceux de licéité, de minimisation, de transparence et de sécurité.

L'introduction de données personnelles, sensibles ou confidentielles (par exemple : identité, situation sociale, dossier administratif…) dans des outils non validés est susceptible de constituer une violation de la vie privée. Par ailleurs, certains dispositifs peuvent impliquer des transferts de données vers des serveurs situés hors de l'Union européenne, sans garanties appropriées, exposant ainsi les informations à des usages non contrôlés.

Les données sensibles ne peuvent être traitées que dans les cas strictement autorisés par le cadre juridique applicable et avec des mesures de protection renforcées.

Risques liés aux instructions (« prompts ») : L'interaction avec les systèmes d'IA repose largement sur des instructions formulées en langage naturel, appelées prompts. Ces instructions constituent un point d'entrée de données et peuvent, si elles sont mal maîtrisées, conduire à une divulgation d'informations, à des contournements de garde-fous ou à des usages non conformes.

Il est par conséquent indispensable d'interdire la saisie de données personnelles ou confidentielles dans des outils non validés et de promouvoir des pratiques encadrées de rédaction des instructions, claires, sobres et conformes aux règles de sécurité de l'information.

Vulnérabilités techniques et détournement des systèmes : Les systèmes d'IA peuvent être exposés à des vulnérabilités techniques, susceptibles d'être exploitées à des fins malveillantes, telles que la manipulation des résultats, l'extraction de données ou le détournement de leur fonctionnement. Ces risques imposent des mesures de sécurité adaptées et une surveillance continue des usages.

Perte de contrôle humain et responsabilité : L'automatisation excessive de certaines tâches peut conduire à ce que des décisions soient prises exclusivement par l'outil, sans validation ou arbitrage humain. Une telle situation n'est pas acceptable dans un cadre administratif, l'IA devant demeurer un outil d'aide à la décision et non de substitution.

En cas de mauvaise utilisation d'un outil d'IA, la responsabilité de l'agent, celle de son service et, plus largement, celle du Gouvernement de la Polynésie française peuvent être engagées. Il est donc essentiel d'assurer une supervision humaine constante.

RECOMMANDATIONS GENERALES : RESPONSABILITES ET VIGILANCES ATTENDUES

o Primauté humaine

L'usage des systèmes d'intelligence artificielle dans l'administration est régi par le principe de primauté humaine.

Les systèmes d'IA ont vocation à assister les agents dans l'exécution de leurs missions, sans jamais se substituer à leur jugement professionnel, à leur appréciation de la situation ou à leur capacité de décision.

Toute production, analyse, recommandation ou résultat généré par un système d'IA doit faire l'objet d'une validation humaine préalable avant d'être utilisé, communiqué ou intégré dans une décision administrative.

Chaque agent doit être en mesure d'expliquer, de justifier et d'assumer les résultats issus de l'usage d'un système d'IA, en particulier lorsque ceux-ci sont utilisés dans le cadre d'une procédure administrative ou d'un acte préparatoire à la décision.

Il demeure pleinement responsable des contenus qu'il produit, même lorsqu'ils sont assistés par une IA ; il engage également la responsabilité de l'administration.

Il est donc attendu qu'il fasse preuve d'esprit critique vis-à-vis des réponses fournies : il doit vérifier la fiabilité et l'exactitude des informations, et s'assurer qu'aucun contenu inapproprié ou biaisé n'a été généré.

Consignes : Relire, vérifier et corriger systématiquement les informations produites par l'IA, certains éléments pouvant être faux ou biaisés.

o Neutralité et respect des valeurs du service public

Les systèmes d'IA utilisés par les agents doivent respecter le principe de neutralité du service public ainsi que les valeurs d'égalité et de non-discrimination. Il convient d'être vigilant quant aux biais qu'une IA peut contenir ou générer, afin d'éviter toute décision ou tout contenu inéquitable, discriminatoire ou contraire aux valeurs de l'administration.

Consignes : Privilégier les systèmes d'IA qui indiquent leurs sources afin de faciliter la vérification des informations produites - vérifier le résultat pour s'assurer de son adéquation aux valeurs et principes du service public

o Respect des droits de propriété intellectuelle

L'utilisation des outils d'IA doit s'effectuer dans le strict respect des droits de propriété intellectuelle, notamment les droits d'auteur, les marques, les brevets... Il est interdit d'utiliser l'IA pour reproduire, diffuser ou exploiter des contenus protégés sans autorisation préalable des titulaires de droits.

Consignes : Vérifier l'origine des données utilisées. Ne pas utiliser, notamment pour une diffusion externe, un contenu que l'on pourrait légitimement suspecter de réutiliser du contenu protégé.

o Protection des données et confidentialité

Par principe, seules des informations publiques peuvent être utilisées dans les outils d'intelligence artificielle.

Les outils d'IA ne doivent pas être utilisés pour traiter ou transmettre :

- ***des données personnelles***[1] a fortiori si elles sont sensibles. Elles sont protégées au titre du Règlement général sur la protection des données (RGPD) et couvertes par le secret professionnel. Elles sont, par défaut, confidentielles.

- ***des données détenues par l'administration et couvertes par le secret professionnel.*** L'administration détient de nombreuses autres informations, qui sans être des données personnelles, sont couvertes par le secret professionnel car elles sont non publiques, peuvent être sensibles ou stratégiques : leur périmètre est large et peut inclure des informations administratives, financières, économiques, techniques, des documents non communicables pouvant prendre diverses formes ....

La plus grande vigilance s'impose donc quant à la nature des informations communiquées dans un outil d'IA.

> ***Consignes :*** *Des données personnelles ou d'autres données détenues par l'administration et couvertes par le secret professionnel ne doivent pas être communiquées dans un outil d'IA. Seules des informations non confidentielles et non sensibles peuvent être utilisées. En cas de doute sur le caractère personnel, confidentiel ou sensible d'une donnée, l'agent doit s'abstenir de l'utiliser ou solliciter l'avis de sa hiérarchie.*

Toute dérogation à ces interdictions doit être formalisée et sécurisée.

L'utilisation d'une IA sur des données personnelles ou des données détenues par l'administration et couvertes par le secret professionnel ne peut être envisagée que par le service et ne peut pas être à l'initiative du seul agent.

À ce titre, le service concerné associe obligatoirement son référent informatique et libertés et, le cas échéant, le délégué à la protection des données.

Le besoin du recours à une IA pour de tels cas d'usage doit être signalé préalablement à la DSI et faire l'objet d'une procédure de visa technique.

L'utilisation d'une IA sur des données personnelles doit également être documentée dans le registre des activités de traitement.

> ***Consignes (applicable au service) :*** *Tout recours à une IA sur des données personnelles ou d'autres données détenues par l'administration et couvertes par le secret professionnel doit être préalablement signalé à la DSI et fait l'objet d'une procédure de visa technique.*

> ***Consignes (applicable au service) :*** *L'utilisation d'une IA sur des données personnelles doit être documentée dans le registre des activités de traitement.*

o Transparence

La transparence est le socle de la confiance. Les agents doivent utiliser l'IA de manière ouverte et transparente, tant en interne qu'à l'égard du public. En interne, cela implique d'informer sa hiérarchie de l'utilisation d'un outil d'IA dans le cadre de ses missions.

Vis-à-vis des usagers, toute personne interagissant avec un système d'IA ou recevant un contenu substantiellement généré par une IA doit en être clairement informée. Cette transparence permet de préserver la confiance.

---

[1] Données personnelles : informations permettant l'identification directe ou indirecte d'une personne physique :

Données directement identifiantes : Information qui permet d'identifier une personne sans avoir besoin d'autres données. Exemples : Nom, Prénom, date et lieu de naissance, Adresse postale, adresse e-mail (pro/perso), numéro de téléphone, Identifiants professionnels (n° RH, matricule...)

Données indirectement identifiantes : Information qui ne permet pas seule d'identifier une personne, mais qui peut le faire si elle est combinée avec d'autres informations par recoupement, déduction, corrélation.

Données personnelles sensibles : Information dont la divulgation a un impact fort sur la vie privée (État de santé, Données génétiques ou biométriques, Origine raciale ou ethnique, Opinions politiques, Convictions religieuses ou philosophiques, Appartenance syndicale, Orientation sexuelle ou données liées à la vie sexuelle)

Avant d'utiliser un nouvel outil IA, l'agent et/ou son service doit effectuer une vérification préalable : identification de l'éditeur, lecture de la documentation technique, connaissance du mode de fonctionnement et des garanties offertes en matière de sécurité et de conformité.

Consignes : Informer sa hiérarchie de tout usage d'un outil d'IA. Se documenter et vérifier le fonctionnement de l'outil que l'on souhaite utiliser. Vérifier qu'il n'est pas soumis au visa de la DSI conformément au point 4.4, 6 ou 7 de la présente charte. S'assurer de l'Information des personnes concernées lorsque l'IA a contribué à la production d'un contenu ou à une décision.

Consignes (applicable au service) : Documenter et vérifier le fonctionnement de l'outil. Vérifier qu'il n'est pas soumis au visa de la DSI conformément au point 4.4, 6 ou 7 de la présente charte. Organiser l'information des personnes concernées lorsque l'IA a contribué à la production d'un contenu ou à une décision.

- **Sécurité**

L'introduction de l'IA ne doit en aucun cas affaiblir la sécurité des systèmes d'information de l'administration. Les agents doivent veiller à respecter les politiques internes de sécurité définies par la DSI Pf lors de l'utilisation d'outils d'IA. Il convient d'avoir conscience que les systèmes d'IA peuvent présenter des vulnérabilités spécifiques susceptibles d'être exploitées par des acteurs malveillants.

Consignes : Signaler sans délai au RSSI et à la DSI Pf toute anomalie, incident ou comportement suspect d'un système d'IA.

- **Limitation de l'impact environnemental**

L'utilisation de l'IA a un impact important sur l'environnement. Son usage doit donc être mesuré en termes de valeur ajoutée c'est à dire réservé aux cas où elle apporte une réelle plus-value.

Consignes : Réserver l'usage de l'IA aux cas où cela est pertinent et apporte une réelle plus-value

5. INTERDICTIONS

Dans la continuité des recommandations générales, les pratiques suivantes sont interdites :

- Utiliser un contenu généré par une IA sans relecture ni vérification ;
- Déléguer entièrement une tâche de réflexion, d'analyse ou de production intellectuelle à une IA ;
- Déléguer à une IA des tâches ou décision engageant juridiquement l'administration ;
- Confier à une IA la prise de décisions automatisées sans intervention ou supervision humaine ;
- transmettre à une IA non validée, des données protégées, personnelles, stratégiques ou d'autres données couvertes par le secret professionnel ;
- reproduire des contenus protégés par le droit d'auteur.

6. USAGES AUTORISES

Les usages listés ci-après sont regardés comme des usages à faible risque lorsqu'ils respectent strictement les recommandations de la présente charte :

- Faciliter la recherche ;
- Effectuer une prise de notes, élaborer des comptes rendus de réunions ;
- Rédiger, corriger, traduire et faire la synthèse de documents ;
- Produire des images et contenus visuels ;
- Analyser et modéliser des données publiques.

Tout usage n'entrant pas dans la liste figurant ci-dessus doit être préalablement autorisé par le chef de service. Il doit être signalé à la DSI et faire l'objet d'une procédure de visa technique.

***Consignes** : Dans le cadre des usages autorisés l'ensemble des recommandations générales détaillées au point 4 ci-dessus s'appliquent - Les usages non prévus au présent point 6 doivent être préalablement signalés à la DSI et font l'objet d'une procédure de visa technique.*

7. SOLUTIONS A PRIVILEGIER

Les solutions utilisées doivent être prioritairement sélectionnées dans le *Panorama des solutions "sur étagère" pour les administrations publiques*, de la DINUM[2].

Ce panorama ne constitue pas une validation officielle ni un label ou agrément des solutions. En particulier il n'évalue pas la qualité fonctionnelle, ni la maturité de la solution d'IA. Néanmoins ces solutions ont été évaluées sur des critères réglementaires (respect des législations sur la protection des données, l'IA, le droit d'auteur), de sécurité et de souveraineté.

Le recours aux solutions de ce panorama doit donc être privilégié. Néanmoins, cela n'exonère pas l'agent ou le service de procéder aux vérifications nécessaires (juridiques, techniques, opérationnelles) dans le cadre de ses démarches d'achat et de projet, ni de respecter les règles de la commande publique ainsi que les autres exigences applicables à leur secteur d'activité et aux cas d'usages.

Le recours à une solution ne figurant pas dans le panorama doit être préalablement signalé à la DSI et faire l'objet d'une procédure de visa technique.

L'utilisation d'un abonnement personnel ou d'un profil personnel n'est pas autorisé dans le cadre professionnel.

***Consignes** : Dans le respect des règles de la commande publique, privilégier les solutions figurant dans le panorama des solutions « sur étagère » de la DINUM tout en effectuant les vérifications nécessaires avant de faire son choix. Le recours à une solution ne figurant pas dans ce panorama doit être préalablement signalé à la DSI et fait l'objet d'une procédure de visa technique.*

***Consignes** : L'utilisation d'un abonnement personnel ou d'un profil personnel n'est pas autorisé dans le cadre professionnel.*

[2] Consulter la liste des solutions d'IA recommandées : Découvrez le panorama solutions IA issues de l'appel à manifestation d'intérêt 2025 — ALLiaNCE

8. SOLUTION COPILOT MISE A DISPOSITION PAR L'ADMINISTRATION

Microsoft 365 Copilot constitue aujourd'hui un outil d'IA proposé à l'ensemble des agents, dans la mesure où il est directement intégré à la suite Microsoft 365 professionnelle mise à disposition par l'administration.

Son utilisation s'inscrit dans le cadre du contrat d'entreprise conclu entre l'administration et Microsoft qui garantit le respect de nos réglementations.

Copilot figure à ce jour dans le panorama des solutions d'IA recommandées par la DINUM ; cet outil peut être considéré comme une solution pour les usages administratifs.

Tout agent disposant d'un compte en *@administration.gov.pf* ou en *@gouvernement.pf*, a la possibilité d'utiliser Copilot via son compte.

Néanmoins son utilisation doit respecter les mêmes principes que tout autre outil d'IA. Il convient donc de ne pas inclure de données personnelles ou confidentielles dans l'instruction (prompt) ou dans des documents joints, vérifier la fiabilité des contenus produits, et conserver une validation humaine sur tout document ou analyse générée.

Selon les cas d'usage, une autre mesure de sécurité peut s'appliquer en désactivant la recherche web lors de l'instruction (prompt) ou en précisant qu'elle doit être effectuée « sans recherche sur internet ».

9. APPLICATION ET MISE A JOUR DE LA CHARTE

Les agents sont tenus au respect de la présente charte. Leur responsabilité peut être engagée en cas de mauvaise utilisation d'un outil d'intelligence artificielle.

Les chefs de service peuvent édicter des règles plus restrictives que celles prévues par la présente charte, afin de tenir compte des spécificités de leurs missions et des risques propres à leurs activités.

Compte tenu de l'évolution rapide des technologies, la présente charte sera modifiée autant que nécessaire. Cette revue régulière sera portée à la connaissance des personnels.

Pour le Président absent
La Vice-présidente
Moetai BROTHERSON

Minarii Chantal GALENON TAUPUA