



Membres en exercice	20
Membres présents	
Pouvoirs	0
Votes :	
Pour	15
Contre	0
Abstentions	0

DELIBERATION N° 14/2026

OBJET : CHARTE INFORMATIQUE ET ANNEXE RELATIVE AUX USAGES DE
L'INTELLIGENCE ARTIFICIELLE (IA)Réunion du 1^{er} juillet 2026

Envoyé en préfecture le 07/07/2026

Reçu en préfecture le 07/07/2026

Publié le



ID : 025-200066264-20260701-D14_2026-DE

Le Conseil d'administration de l'Agence départementale d'appui aux territoires, convoqué le 18 juin 2026, s'est réuni le 1^{er} juillet 2026 à 14h30, sous la présidence de Madame Christine BOUQUIN, Présidente de l'ADAT.

Etaient présents les membres de l'Agence suivants :

Olivier BILLOT, Christian BRAND, Damien CHARLET, Serge DELFILS, André-Marie DEPOUTOT, Gérard DEQUE, Philippe FRANCHINI, Ida JEANGIRARD, Raphaël KRUCIEN, Géraldine LEROY, Pierre LIEVREMONT, Thierry MAIRE DU POSET, Patricia PAQUIEZ, Pascal ROUTHIER

Etaient excusés les membres de l'Agence suivants :

Marie-France BOTTARLINI, Valérie MAILLARD, Catherine RACINE, Florence ROGEBOSZ, Géraldine TISSOT-TRULLARD, Martine VOIDEY, Michel VIENET

VU le Code général des collectivités territoriales

L'ADAT accompagne quotidiennement les collectivités dans leurs usages numériques et traite, dans ce cadre, des données parfois sensibles. Par ailleurs, les outils d'intelligence artificielle se développent rapidement et sont désormais utilisés dans de nombreuses activités professionnelles.

Afin de garantir un usage sécurisé, responsable et conforme à la réglementation, l'ADAT a élaboré :

- une **charte informatique**, qui définit les règles d'utilisation des équipements et systèmes d'information, les bonnes pratiques en matière de cybersécurité et de protection des données ;
- une **charte des usages de l'intelligence artificielle (IA)**, qui encadre l'utilisation des outils d'IA par les agents, tout en favorisant l'innovation et l'amélioration des pratiques professionnelles.

Ces documents ont pour objectif :

- de protéger les données de l'agence et de ses adhérents
- de prévenir les risques numériques
- d'accompagner les agents une utilisation éthique des outils numériques

Leur rédaction s'est largement appuyée sur les travaux engagés par le Département du Doubs, dont les chartes ont servi de référence, tout en étant adaptées aux spécificités de l'ADAT.

Cette démarche s'inscrit dans la volonté de l'ADAT d'être exemplaire dans ses propres pratiques numériques et cohérente avec les recommandations qu'elle formule auprès des collectivités qu'elle accompagne.

Les outils d'IA générative (ChatGPT, Copilot, Claude ...) se développent rapidement et sont utilisés dans de nombreux contextes professionnels : aide à la rédaction, synthèse d'informations, assistance technique, recherche documentaire, développement informatique ...

L'objectif de la charte des usages de l'IA n'est pas d'interdire ces usages, mais de les encadrer afin de garantir un usage responsable et sécurisé. Elle vise à concilier innovation et protection des données.

Après en avoir délibéré, les membres du Conseil d'administration

APPROUVENT à l'unanimité la charte informatique et son annexe relative aux usages de l'intelligence artificielle.

La Présidente de l'ADAT,

Christine BOUQUIN

Envoyé en préfecture le 07/07/2026

Reçu en préfecture le 07/07/2026

Publié le

ID : 025-200066264-20260701-D14_2026-DE



CHARTRE INFORMATIQUE

Mise à jour le 25 juin 2026

Préambule

En tant qu'opérateur public de services numériques (OPSN), l'Agence départementale d'appui aux territoires (ADAT) accompagne les collectivités locales du département du Doubs dans leurs usages numériques. À ce titre, elle traite des données sensibles (financières, RH, sociales) et doit garantir un haut niveau de sécurité.

La présente charte a pour objet de définir les règles d'utilisation du système d'information et des équipements numériques (matériels et logiciels) mis à disposition des agents. Elle vise également à :

- garantir un usage conforme aux finalités professionnelles
- préserver la confidentialité, l'intégrité et la disponibilité du système d'information
- assurer la protection des données personnelles et institutionnelles
- responsabiliser les utilisateurs dans leurs pratiques numériques pour prévenir les usages abusifs et les risques liés à la cybersécurité
- garantir le respect des obligations légales , notamment issues du règlement général de la protection des données (RGPD)

1. Champ d'application

La charte s'applique à tous les utilisateurs des ressources numériques de l'agence :

- agents permanents et contractuels
- stagiaires, apprentis
- prestataires et partenaires disposant d'un accès au système d'information
- élus disposant d'un accès aux systèmes d'information

Elle concerne toutes les ressources informatiques et numériques mises à disposition :

- les équipements (ordinateurs, téléphones, tablettes, serveur, copieurs...)

- les logiciels et applications : suite bureautique, logiciels métiers, applications collaboratives, plateformes professionnelles ...
- les réseaux et services numériques : accès internet, VPN, wifi interne, outils de communication
- les données : fichiers, courriels, base de données, documents partagés

2. Principes d'utilisation

Toute utilisation des outils numériques doit s'inscrire dans le respect des principes établis par la présente charte.

Les outils informatiques sont mis à disposition pour un usage professionnel. Un usage personnel limité peut être toléré s'il reste occasionnel, n'affecte pas le fonctionnement du service, n'entrave pas les missions professionnelles, ne compromet pas la sécurité ou la réputation de l'ADAT. Les répertoires ou messages à caractère personnel doivent être clairement identifiés par la mention « privé » ou « personnel ».

Chaque utilisateur est responsable des actions réalisées avec ses accès.

3. Accès aux systèmes et sécurité

Identifiants et mots de passe

- Les identifiants sont strictement personnels et ne doivent jamais être partagés
- Les mots de passe doivent être robustes (12 caractères minimum)
- L'utilisation d'un gestionnaire de mots de passe validé est **obligatoire**
- Une authentification renforcée peut être mise en place (MFA)

Postes et logiciels

- Toute installation de logiciel non validée par le service informatique est interdite
- Les configurations ne doivent pas être modifiées sans autorisation.

Suspension ou restriction d'accès au système d'information

L'accès au système d'information pourra être suspendu temporairement ou non, sans préavis, pour l'un des motifs suivants :

- menace sur la sécurité informatique (virus, intrusion fuite de données ...)
- non-respect manifeste de la présente charte
- fin de contrat
- tout autre raison pour nécessité de service (maintenance, obligation légale ...)

4. Utilisation des équipements

Les équipements professionnels doivent être utilisés dans des conditions garantissant leur sécurité et ne doivent pas être prêtés à des tiers non autorisés. Il est impératif de :

- Ne pas laisser un équipement sans surveillance
- Éviter les connexions à des réseaux Wi-Fi publics ou non sécurisés
- Signaler immédiatement toute perte, vol ou dysfonctionnement

L'usage **de supports externes personnels** (clé USB...) est interdit sans validation préalable.

5. Utilisation d'internet et des outils numériques

- La navigation internet doit être en lien avec les missions professionnelles.
- L'accès à certains sites peut être restreint pour des raisons de sécurité.
- L'utilisation de services en ligne (cloud, outils externes) doit être validée.

6. Données et confidentialité

- Les données professionnelles doivent être traitées avec confidentialité.
- Il est interdit de divulguer des informations sensibles ou confidentielles sans autorisation.
- Les documents contenant des données sensibles ne doivent pas sortir des locaux sans accord.
- Les principes du RGPD doivent être respectés en toutes circonstances. Un engagement de confidentialité est joint à la présente charte en *annexe 1* et s'applique même après la cessation des fonctions de l'agent

7. Authentification multi facteur (MFA) et accès à distance

- Pour garantir un niveau de sécurité optimal des accès au système d'information de l'ADAT, et tout particulièrement pour sécuriser les connexions distantes, l'usage d'une authentification multi facteur (MFA) sera déployé progressivement.
- Sécurisation des accès à distance : Toute connexion depuis l'extérieur au réseau interne de l'ADAT (notamment via un réseau privé virtuel ou VPN) est conditionnée à la validation de cette authentification forte. Cette mesure technique empêche toute intrusion sur le réseau de l'agence en cas de compromission ou de vol du mot de passe de l'utilisateur.
- Pour valider cette authentification, l'agent peut choisir d'installer une application approuvée par l'ADAT sur son smartphone personnel. Cet usage repose sur la base du volontariat. En cas de refus, de non-équipement ou d'impossibilité technique, l'ADAT fournira un dispositif matériel alternatif dédié à cette validation.

- Respect de la vie privée : l'installation de l'application d'authentification sur un équipement personnel ne confère au service informatique de l'ADAT aucun droit d'accès, de suivi, de gestion ou de contrôle sur l'appareil. Cette application ne collecte aucune donnée personnelle, historique de navigation ou de géolocalisation. L'ADAT ne dispose d'aucun droit d'effacement à distance des données personnelles de l'agent.
- Perte et vol : En cas de perte, de remplacement ou de vol du dispositif servant à l'authentification forte (qu'il s'agisse du smartphone personnel ou du matériel fourni par l'ADAT), l'utilisateur a l'obligation d'en informer immédiatement le service informatique, en vue de révoquer l'équipement perdu, de bloquer les accès distants associés et de garantir l'intégrité du compte utilisateur.

8. Responsabilité des utilisateurs

Tout utilisateur est tenu de :

- respecter la présente charte et adopter un comportement numérique responsable
- signaler immédiatement à sa hiérarchie tout incident ou suspicion de fuite de données ou tentative d'intrusion (virus, intrusion, fuite de données)
- appliquer les consignes de sécurité (ex : déconnexion du réseau en cas de doute)
- participer aux formations et sensibilisations à la cybersécurité proposées par l'ADAT

9. Partage externe et traçabilité

Le partage de fichiers via Onedrive ou SharePoint avec des destinataires externes est autorisé. Tous les partages externes de documents sont journalisés et pourront être analysés en cas d'incidents ou de violation de données.

Les utilisateurs doivent limiter les partages externes aux documents strictement nécessaires et vérifier les autorisations d'accès avant tout envoi.

10. Contrôle et sanctions

Des contrôles peuvent être réalisés, dans le respect de la réglementation, sur les connexions au système d'information, l'utilisation de la messagerie et d'internet ainsi que l'installation et l'usage de logiciels.

Tout manquement, réel ou supposé aux dispositions de la présente charte, fait l'objet d'une analyse préalable afin d'en qualifier la nature, la gravité et les circonstances. Cette qualification est réalisée par les acteurs compétents en matière de sécurité et de protection des données, notamment le responsable du service informatique, l'administrateur informatique et/ou le délégué à la protection des données.

Tout manquement ou usage abusif peut entraîner des évolutions techniques ou organisationnelles, des sanctions disciplinaires, voire des poursuites judiciaires selon la gravité des faits.

11. Intelligence artificielle (IA)

L'utilisation d'outils d'IA est encadrée par une **annexe spécifique** à la présente charte.

12. Évolution de la charte

La présente charte peut être mise à jour pour tenir compte des évolutions réglementaires, techniques, ou organisationnelles. Les utilisateurs seront informés de toute mise à jour.

13. Acceptation de la charte

La présente charte est portée à la connaissance de chaque utilisateur, qui s'engage à la respecter. Cette acceptation conditionne l'accès aux systèmes d'information de l'ADAT.

Nom de l'agent

Signature

Date

Annexe 1 – Charte des usages de l'intelligence artificielle au sein de l'ADAT

Mise à jour le 25 juin 2026

Préambule

L'intelligence artificielle (IA), et plus particulièrement les outils d'IA générative, constituent des outils pouvant faciliter certaines activités professionnelles et améliorer le service rendu aux adhérents.

En tant qu'opérateur public de services numériques (OPSN) accompagnant les collectivités territoriales, l'ADAT considère que ces outils doivent être utilisés dans un cadre responsable, sécurisé et maîtrisé.

Cette charte vise à encadrer les usages de l'IA afin de :

- préserver la confidentialité des données
- sécuriser les informations des collectivités adhérentes
- garantir la qualité des productions réalisées
- maintenir la responsabilité humaine dans les décisions prises
- favoriser un usage raisonné et responsable de ces technologies

L'IA constitue un appui dans l'activité professionnelle. Elle ne se substitue ni à l'expertise métier, ni à la responsabilité des agents. **L'usage responsable de l'IA** garantit la **primauté de l'humain** et vise à maximiser les bénéfices tout en minimisant les risques.

• Cadre général

L'usage de l'IA au sein de l'ADAT s'inscrit notamment dans le respect :

- du règlement européen sur l'intelligence artificielle (IA Act) du 13 juin 2024
- du RGPD du 27 avril 2016
- de la loi Informatique et Libertés du 6 janvier 1978
- des obligations de secret professionnel, discrétion professionnelle et confidentialité applicables aux agents prévues dans la loi du 13 juillet 1983
- de la charte informatique de l'ADAT

La présente annexe complète la charte informatique de l'ADAT et se décline autour de 8 principes à respecter.

I. Les 8 principes à respecter

1. Primauté de l'humain

L'IA assiste les agents mais ne remplace pas leur expertise.

Toute production issue d'un outil d'IA doit être relue et vérifiée. Elle reste sous la responsabilité de l'utilisateur

L'humain conçoit l'usage de l'IA, vérifie les sources, intervient à des étapes choisies et décide de l'utilisation du résultat.

2. Transparence

L'utilisateur de l'IA doit être en capacité d'expliquer les résultats utilisés et vérifier les informations produites. Les résultats générés doivent être considérés comme des propositions et non comme des vérités.

La relation entre l'ADAT et ses adhérents repose sur un principe de transparence. Lorsque l'intelligence artificielle intervient directement dans les échanges avec les adhérents ou joue un rôle significatif dans le traitement de leurs demandes, ceux-ci en sont informés de manière appropriée.)

3. Sécurité

Les outils d'IA utilisés doivent respecter les exigences de sécurité de l'ADAT. Aussi, les agents :

- utilisent prioritairement les outils autorisés par l'ADAT avec un compte professionnel
- refusent la conservation ou la réutilisation des données lorsque l'option existe
- signalent sans délai toute anomalie, incident, suspicion de violations de données ou tentatives d'intrusion

L'utilisation d'un nouvel outil doit faire l'objet d'un accord préalable de la direction ou du référent désigné. En amont, une vérification doit être réalisée afin d'évaluer notamment :

- les conditions de traitement et d'hébergement des données
- les garanties de confidentialité offertes par l'éditeur
- les possibilités de désactiver la réutilisation des données à des fins d'entraînement
- les risques éventuels pour la sécurité des systèmes d'information et des données des adhérents

4. Protection des données et confidentialité

Il est interdit de saisir dans un outil d'IA :

- des données personnelles
- des données sensibles au sens du RGPD
- des informations confidentielles relatives aux adhérents
- des mots de passe, clés techniques ou éléments de sécurité
- des exports de logiciels métiers
- des données issues d'interventions d'assistance informatique

L'utilisation d'un outil d'IA suppose de connaître les règles qui lui sont applicables, notamment les catégories de données pouvant être saisies, les conditions de confidentialité proposées par l'éditeur et les éventuelles limitations définies par l'ADAT.

Lorsque l'usage d'un outil nécessite l'utilisation de données réelles, celles-ci doivent être anonymisées ou pseudonymisées.

5. Vigilance sur les biais et la qualité

Les outils d'IA peuvent produire des résultats inexacts, incomplets ou orientés. Parce qu'ils s'appuient sur des données existantes, ils peuvent parfois générer des biais, c'est-à-dire reproduire certaines idées reçues ou privilégier certains points de vue. Chaque utilisateur doit donc conserver un regard critique sur les contenus générés, vérifier les informations avant de les utiliser et s'assurer qu'elles n'ont pas de caractère erroné ou discriminatoire.

6. Sobriété numérique

Les outils d'IA sont très consommateurs en énergie et ressources informatiques. Cette augmentation de l'empreinte carbone appelle collectivement et individuellement à un usage qui doit rester proportionné au besoin réel.

Une solution plus simple ou moins consommatrice doit être privilégiée lorsqu'elle permet d'atteindre le même résultat.

7. Usage responsable

L'IA peut être utilisée notamment pour :

- préparer des notes ou synthèses;
- assister la rédaction
- produire des supports de communication
- faciliter certaines analyses techniques
- préparer des scripts, requêtes ou procédures techniques
- aider à la veille documentaire ou réglementaire

L'IA ne doit pas être utilisée pour :

- prendre des décisions à la place de l'agent
- produire des avis juridiques sans contrôle humain préalable
- traiter directement des demandes contenant des données confidentielles
- réaliser des actions techniques automatisées sans validation préalable

Les utilisateurs sont responsables de l'utilisation des résultats produits par l'IA. Ils doivent donc s'assurer de la qualité, de la pertinence et de la véracité des contenus, tout en restant transparent sur le recours à l'IA.

8. Formation et acculturation

L'ADAT accompagne les agents dans la compréhension des enjeux liés à l'IA pour leur permettre à chacun de comprendre, maîtriser et évaluer les impacts de l'IA sur ses pratiques professionnelles.

Des actions de sensibilisation seront proposées aux agents.

II – Gouvernance et régulation

1. Expérimentation

L'ADAT encourage l'expérimentation raisonnée des usages de l'IA. Toutefois, tout nouvel usage devra faire l'objet d'une validation préalable pour vérifier son impact sur la sécurité, les données personnelles ou les services proposés aux adhérents.

2. Évolution de la charte

La présente charte pourra être mise à jour pour tenir compte des évolutions réglementaires, techniques, ou organisationnelles. Les utilisateurs seront informés de toute mise à jour.

3. Acceptation de la charte

La présente charte constitue un cadre de référence applicable à l'utilisation de l'IA au sein de l'ADAT. Elle est portée à la connaissance de chaque agent, qui s'engage à la respecter. Cette acceptation conditionne l'accès aux systèmes d'information de l'ADAT.

Nom de l'agent

Signature

Date

Annexe 2 – Engagement de confidentialité pour la protection des données personnelles

Dans le cadre de mes fonctions en tant qu'agent (ou stagiaire) de l'ADAT, je suis amené(e) à accéder, manipuler et traiter des données à caractère personnel (ci-après "données personnelles"). Ces données sont protégées par la législation en vigueur, notamment le Règlement Général sur la Protection des Données (RGPD) et la loi française n° 78-17 du 6 janvier 1978 modifiée, dite "Loi Informatique et Libertés".

Dans le cadre de l'exercice de mes fonctions, je m'engage à :

- Respecter strictement la confidentialité des données personnelles auxquelles j'ai accès dans le cadre de mes fonctions.
- Ne pas divulguer ou communiquer à des tiers non autorisés, sous quelque forme que ce soit, des données personnelles ou toute information confidentielle.
- Utiliser les données personnelles uniquement dans le cadre strictement nécessaire à l'exercice de mes missions professionnelles au sein de l'ADAT.
- Protéger l'intégrité, la disponibilité et la confidentialité des données personnelles en respectant les procédures internes et les mesures de sécurité mises en place par l'ADAT ainsi que toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions.
- Ne pas traiter, stocker ou transférer des données personnelles ou confidentielles via des outils d'intelligence artificielle générative ou toute autre technologie et privilégier des solutions sécurisées et conformes aux réglementations en vigueur.

Je reconnais que les données personnelles doivent être traitées conformément aux principes suivants :

- Licéité, loyauté et transparence : Les données doivent être traitées de manière légitime et dans le respect des droits des personnes concernées.
- Minimisation des données : Seules les données strictement nécessaires à l'accomplissement des finalités prévues peuvent être collectées et utilisées.
- Sécurité et protection : Toutes les mesures raisonnables doivent être prises pour éviter les accès non autorisés, les fuites ou les altérations de données.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

À la cessation de mes fonctions ou à la demande de l'ADAT je m'engage à restituer tous les documents et supports contenant des données personnelles ou informations confidentielles, quel qu'en soit le format, et à ne conserver aucune copie.

Cet engagement de confidentialité demeure valable pendant toute la durée de mes fonctions au sein de l'ADAT ainsi qu'après la cessation de ces fonctions, quelle qu'en soit la raison.

Fait à _____, le _____

Nom et Prénom de l'agent

Fonction au sein de l'ADAT

Signature (Précédée de la mention « Lu et approuvé »)

ADAT – charte informatique – Juin 2026