Démonstration de conformité de Productiv[IA] et plan de mise en conformité (Québec 2025)

Introduction

Productiv[IA] est une plateforme d'**intelligence artificielle** conçue pour répondre aux exigences réglementaires et aux meilleures pratiques numériques du secteur public québécois en **2025**. Ce document présente comment Productiv[IA] **démontre sa conformité** aux obligations applicables – en matière de protection des données, de cybersécurité, d'accessibilité, etc. – et décrit le **plan de mise en conformité** final pour assurer un respect total de l'ensemble des normes d'ici son déploiement généralisé. L'objectif est de montrer que Productiv[IA] est **apte à être adoptée par les institutions publiques et parapubliques du Québec**, en offrant dès maintenant un cadre sécuritaire et conforme pour un déploiement pilote, tout en prévoyant les actions restantes pour une conformité complète avant l'implantation officielle.

Ce document s'aligne sur les orientations gouvernementales récentes, dont la **Stratégie gouvernementale de cybersécurité et du numérique 2024–2028**, qui vise des services numériques *« accessibles, complets, conviviaux et sécuritaires »* pour la population. Il tient compte des nouvelles **exigences légales** (telles que la **Loi 25** au Québec, le **RGPD** européen et la **LPRPDE** canadienne) et des **directives spécifiques** encadrant l'utilisation de l'IA dans le secteur public (par exemple l'arrêté ministériel 2024-01 du MCN sur les projets en IA). Productiv[IA] adhère également aux **principes d'IA responsable** promus par le gouvernement – notamment l'importance pour l'utilisateur de garder le contrôle, la transparence des algorithmes et la gestion diligente des risques – afin de renforcer la confiance des parties prenantes.

(Note : Ce document est de nature générale et ne comporte aucune information confidentielle sur le développement interne de Productiv[IA]. Il se concentre uniquement sur la conformité réglementaire et la gouvernance, sans référence au plan de développement technique interne.)

Structure corporative et pérennité du projet

Productiv[IA] est portée par une structure corporative solide garantissant la **pérennité du service**. Productiv[IA] est une entreprise 100% québécoise et est en partie détenue par PVP Média (entreprise établie depuis 1987), ce qui lui confère une base financière et une expertise de longue date. Contrairement à une startup isolée, Productiv[IA] bénéficie du soutien d'un groupe bien établi, assurant ainsi stabilité et ressources sur le long terme. Une **équipe de développement dédiée** travaille exclusivement sur Productiv[IA].

Par ailleurs, Productiv[IA] s'appuie sur des **partenariats fiables** pour l'exploitation et la sécurité. Le support technique aux utilisateurs finaux est assuré en collaboration avec *Informidata*, une firme TI d'expérience, tandis que la **cybersécurité** de la plateforme est supervisée par *Ninpo Cybersécurité*, qui opère un centre opérationnel de sécurité (**SOC**) fonctionnant 24/7. Cette organisation robuste – incluant des garanties telles que le dépôt du code source chez notaire et une assurance responsabilité professionnelle de 2 M$ – offre aux institutions clientes la certitude que Productiv[IA] est un service **viable à long terme**, doté de moyens suffisants pour assurer la continuité même en cas d'imprévus. En somme, la gouvernance du projet et la solidité du fournisseur sont gages de **confiance** pour toute organisation publique souhaitant adopter la solution.

Surveillance cybersécurité continue et support 24/7

La sécurité étant un enjeu prioritaire, Productiv[IA] bénéficie d'une **surveillance proactive en continu (24/7/365)** grâce à son partenariat avec Ninpo Cybersécurité. Dès son déploiement en phase pilote, l'ensemble de l'infrastructure et des applications est monitoré en temps réel par ce SOC externe. La moindre menace ou activité anormale déclenche une alerte immédiate et une réponse rapide, y compris en dehors des heures ouvrables traditionnelles. Ce haut niveau de vigilance garantit qu'aucun incident critique ne passe inaperçu et qu'une expertise est disponible à toute heure pour y remédier.

En complément, des **rapports de sécurité réguliers** (hebdomadaires) sont fournis, synthétisant les événements notables et les mesures prises. Cette couche d'audit externe vient renforcer les mécanismes internes de sécurité de Productiv[IA]. De plus, dès le lancement des projets pilotes, Productiv[IA] s'engage dans une démarche de **certification de sécurité** reconnue (par exemple, l'attestation **SOC 2** Type I visée d'ici 2026, suivie de la certification SOC 2 Type II), afin de faire valider par des experts indépendants l'efficacité de l'ensemble des contrôles de sécurité en place. Ces initiatives démontrent la volonté de Productiv[IA] de se conformer aux **meilleures pratiques de l'industrie** et d'offrir aux organismes publics un niveau de sécurité conforme à leurs exigences.

Exigences de conformité applicables

Dans le contexte des organismes publics québécois, l'adoption d'une plateforme numérique telle que Productiv[IA] doit satisfaire à de nombreuses **exigences réglementaires et normatives**. Les principales exigences considérées sont :

- **Accessibilité numérique** – Conformité aux standards d'accessibilité Web (par exemple *RGAA 4.1* aligné sur WCAG 2.1) pour garantir l'accès aux personnes en situation de handicap.

- **Protection des renseignements personnels (Québec)** – Respect de la **Loi 25** (issue de l'ex-projet de loi 64) et des lois provinciales en vigueur, impliquant notamment le consentement des usagers, la limitation des finalités d'utilisation des données et la tenue d'un registre des informations collectées.
- **Protection des données – Canada (LPRPDE)** – Alignement sur la loi fédérale **LPRPDE** (*PIPEDA*) pour les organismes de juridiction fédérale ou les partenaires privés, ce qui recouvre des principes de transparence, de consentement et de sécurité appropriée des données.
- **Protection des données – Europe (RGPD)** – Adhérence aux grands principes du **RGPD** (Règlement général sur la protection des données) en prévision d'utilisateurs internationaux éventuels, incluant transparence, minimisation des données, droit à l'oubli, etc.
- **Hébergement sécurisé et souveraineté des données** – Hébergement des informations sur une infrastructure canadienne certifiée, idéalement localisée au Québec, afin d'assurer la **souveraineté des données** et la conformité avec les directives gouvernementales en matière d'infonuage (cloud).
- **Sécurité de l'information** – Mise en place de contrôles de sécurité techniques et organisationnels conformes aux politiques gouvernementales (p. ex. Politique gouvernementale de cybersécurité et Directive sur la sécurité de l'information) : gestion des accès, chiffrement, pare-feux, détection d'intrusions, etc.
- **Auditabilité et traçabilité** – Capacité de journaliser et tracer les actions des utilisateurs et de l'IA, afin de vérifier l'usage approprié, détecter les abus et prouver la conformité en cas d'audit.
- **Architecture ouverte et intégration aux systèmes** – Architecture logicielle favorisant l'**interopérabilité** (standards ouverts, API documentées) et intégration à l'écosystème numérique existant des organisations (p. ex. authentification unique **SSO** via le fournisseur d'identité de l'organisme). Cela inclut également la transparence sur le fonctionnement des algorithmes utilisés et l'absence de verrouillage propriétaire, conformément aux orientations gouvernementales encourageant l'usage de solutions ouvertes (« *logiciels libres* ») lorsque pertinent.

En plus de ces obligations, Productiv[IA] s'aligne sur les **orientations éthiques et stratégiques** entourant l'IA au Québec. Notamment, le ministère de la Cybersécurité et du Numérique (MCN) a émis en 2024 un **Guide des bonnes pratiques d'utilisation de l'IA générative** invitant les organismes publics à faire preuve de prudence et de responsabilité dans l'adoption de ces outils. De même, l'**arrêté ministériel 2024-01** du MCN

(28 février 2024) impose aux organismes publics de **déclarer tout projet impliquant de l'IA** et d'en respecter les cadres gouvernementaux applicables, tandis que l'**arrêté 2024-02** (27 juin 2024) énonce des *principes pour une utilisation responsable de l'IA* dans l'administration publique. Enfin, le **Conseil de l'innovation du Québec** recommande de **renforcer rapidement le cadre de gouvernance de l'IA** au sein de l'État, par exemple via la création d'un registre public des systèmes d'IA déployés ou la mise en place d'évaluations d'impact algorithmiques. Productiv[IA] anticipe ces orientations dans sa conception même, comme détaillé ci-dessous pour chaque volet de conformité.

Accessibilité numérique (RGAA 4.1)

Statut : *En cours de conformité.* Productiv[IA] a été conçu en intégrant dès le départ les bonnes pratiques d'**accessibilité Web**. L'interface utilise une structure HTML sémantique appropriée, des contrastes de couleurs adéquats, des textes alternatifs sur les images et permet la navigation au clavier – de sorte qu'aucun obstacle bloquant n'a été identifié à ce stade pour les personnes en situation de handicap. Un premier audit interne d'accessibilité a permis de couvrir environ **50 % des critères RGAA 4.1**, couvrant les aspects majeurs. Cela assure qu'aucun utilisateur ne soit empêché d'utiliser la plateforme durant les pilotes actuels. Néanmoins, certains détails doivent encore être améliorés pour atteindre une conformité totale.

Plan d'action : Productiv[IA] vise une **conformité à 100 % avec le RGAA 4.1** d'ici le déploiement officiel (cible : septembre 2026). Pour ce faire, une démarche d'amélioration continue de l'accessibilité est en place : chaque nouvelle fonctionnalité développée fait l'objet d'une vérification systématique au regard des critères d'accessibilité avant sa mise en production. Un audit externe par des spécialistes indépendants sera mené en 2026 afin de valider officiellement que tous les critères applicables sont satisfaits. En parallèle, l'équipe de développement continue de se former aux standards *WCAG/RGAA* afin de pérenniser une **culture de l'accessibilité** au sein du projet. Enfin, des fonctionnalités additionnelles pourront être ajoutées pour améliorer encore l'expérience des utilisateurs en situation de handicap (par ex. synthèse vocale des réponses, compatibilité accrue avec les lecteurs d'écran, sous-titrage automatique du contenu généré). Ces mesures assureront qu'au moment du déploiement à grande échelle, Productiv[IA] sera **entièrement accessible** et conforme aux obligations réglementaires du gouvernement en la matière.

Protection des données et confidentialité

Statut : *En cours, principes appliqués dès la conception.* La **protection des renseignements personnels** des usagers est un pilier central de Productiv[IA]. Dès l'origine, l'architecture du système a suivi les principes de "confidentialité par conception" afin de

respecter ou dépasser les exigences de la Loi 25 (Québec) et de la LPRPDE (Canada). Concrètement :

- **Souveraineté et sécurité de l'hébergement :** Toutes les données de Productiv^{IA} (profils utilisateurs, contenu des interactions, documents importés, etc.) sont hébergées au **Canada**, plus précisément sur l'infrastructure d'OVHcloud Canada. Les serveurs étant localisés au Québec, cela assure une *souveraineté des données* conforme aux politiques du secteur public québécois (aucune donnée n'est stockée à l'étranger sans autorisation). OVHcloud est par ailleurs un hébergeur certifié (ISO 27001, SOC 1/2/3, etc.), apportant des garanties élevées en matière de sécurité physique et logique des centres de données. Ce choix d'hébergement souverain répond directement aux attentes gouvernementales de localisation des données et de contrôle sur celles-ci.
- **Confidentialité par conception :** Productiv^{IA} n'exploite **aucune donnée personnelle** de l'utilisateur à des fins autres que le service rendu à cet utilisateur lui-même. En particulier, les contenus fournis par les usagers (questions posées à l'IA, documents analysés, etc.) restent *strictement confidentiels*. Ils ne sont jamais réutilisés pour entraîner des modèles publics ni partagés avec des tiers non autorisés. L'utilisateur conserve en tout temps le contrôle de ses informations, avec la possibilité de **supprimer son historique** d'interactions à la demande. Ces principes fondamentaux – transparence, limitation des finalités, contrôle par l'usager – placent déjà Productiv^{IA} en conformité avec les objectifs de la Loi 25 et de la LPRPDE, qui exigent le consentement éclairé et la minimisation de la collecte des renseignements personnels.
- **Contrôles de consentement explicite :** Là où des fonctionnalités de Productiv^{IA} impliquent le traitement de données potentiellement sensibles, des mécanismes de **consentement éclairé** sont prévus. Par exemple, si un utilisateur souhaite analyser via l'IA un document contenant des informations personnelles, la plateforme lui demandera explicitement confirmation et consentement avant de procéder. Chaque organisation cliente peut en outre configurer des politiques internes via les paramètres d'administration de Productiv^{IA}: il est possible de désactiver certaines fonctionnalités ou d'appliquer des filtres et restrictions adaptés à son contexte (p. ex. filtrage de certains types de contenus). Cette flexibilité garantit que l'utilisation de Productiv^{IA} reste conforme aux règles de gouvernance propres à chaque entité.

En l'état actuel (fin 2025), Productiv^{IA} est donc **largement conforme aux exigences de la Loi 25** au Québec et de la LPRPDE fédérale, du point de vue des pratiques opérationnelles.

Aucune lacune majeure n'a été identifiée relativement à ces lois pour le déploiement pilote. Bien que le RGPD de l'UE ne s'applique pas d'office aux organismes québécois, la plateforme incorpore d'ores et déjà les grands principes du RGPD (transparence, minimisation, droits des utilisateurs, etc.) et serait prête à s'y conformer formellement en cas d'utilisation par des partenaires européens. Par exemple, aucune création de profil à l'insu de l'usager n'est réalisée, et un mécanisme de suppression/droit à l'oubli pourrait être activé au besoin.

Mesures de protection renforcée (phase pilote) : Afin d'aller encore plus loin dans la sécurisation des renseignements sensibles durant la phase pilote, Productiv[IA] intègre des fonctions innovantes :

- *Option « Données sensibles – Canada seulement »* : Une option dédiée permet de restreindre certains traitements d'IA aux **seuls serveurs situés au Canada**. Concrètement, si cette option est activée (par l'administrateur ou l'utilisateur lui-même selon les droits), les requêtes concernées seront redirigées vers un modèle d'IA hébergé localement ou via une API dans des centres de données canadiens (par ex. un LLM de Cohere opéré au Canada), de sorte qu'aucune donnée sensible ne transite hors du pays. Ces requêtes sont marquées et journalisées spécifiquement pour pouvoir en auditer le traitement a posteriori. Cette fonction répond directement aux préoccupations de **juridiction des données** : elle permet d'éviter l'envoi de renseignements confidentiels sur des infrastructures cloud étrangères, ce qui est un enjeu crucial pour de nombreux organismes publics.
- *Filtrage automatique des informations personnelles* : La plateforme comporte un filtre intelligent capable de **détecter et masquer automatiquement les données personnelles identifiables** dans les entrées utilisateur (ex. numéros d'assurance sociale, numéros d'étudiant, adresses, numéros de téléphone). Si un utilisateur tente involontairement de soumettre de telles données à l'IA, le système bloque ou anonymise ces informations avant tout envoi à un modèle externe. Chaque occurrence de blocage est consignée, et un rapport périodique des éléments filtrés peut être transmis à l'administrateur de l'institution utilisatrice pour transparence. Techniquement, ce filtrage préventif s'appuie sur un micro-modèle d'IA dédié déployé en amont, chargé d'analyser les messages en temps réel et d'empêcher toute fuite de **renseignements personnels** vers des services externes. Ce mécanisme de sauvegarde s'aligne sur les recommandations gouvernementales invitant à la plus grande prudence quant au partage de données sensibles avec des outils d'IA générative : *« Il ne faut jamais soumettre des informations personnelles,*

confidentielles ou sensibles […] à des systèmes d'IA générative » rappelle notamment le guide du MCN.

- *Surveillance externe et rapports de conformité :* En plus des contrôles internes, Productiv[IA] bénéficie du regard d'un tiers de confiance (Ninpo) qui surveille toute tentative d'accès ou d'exfiltration anormale de données en continu (voir section cybersécurité). Des **rapports de sécurité et de confidentialité** peuvent être fournis régulièrement aux clients institutionnels, résumant les incidents bloqués et les mesures prises. Cela offre un niveau supplémentaire d'**audit externe** sur la protection des données, venant corroborer les efforts internes et rassurer les équipes de gouvernance de l'organisme client.

Plan d'action : D'ici le déploiement final, Productiv[IA] finalisera l'ensemble des documents et processus requis pour une conformité formelle impeccable. Un **registre détaillé des renseignements personnels** traités par la plateforme est en cours d'élaboration, conformément aux exigences de la Loi 25 (chaque catégorie de données y est documentée avec sa finalité, sa durée de conservation, les personnes y ayant accès, etc.). Ce registre sera achevé et validé durant les projets pilotes, de sorte qu'il pourra être mis à disposition en cas de vérification par la Commission d'accès à l'information (CAI) ou le Commissariat à la vie privée du Canada.

Parallèlement, chaque nouvelle fonctionnalité impliquant des données personnelles fera l'objet d'une **évaluation de conformité** dédiée (incluant, si nécessaire, une analyse de risques ou une PIA – *Évaluation des facteurs relatifs à la vie privée* – selon les critères de la CAI). Les flux de consentement utilisateur seront ajustés au besoin pour maintenir un haut niveau de conformité légale en toute circonstance (par ex. ajout d'une double confirmation avant l'utilisation d'un document hautement sensible, afin de respecter le principe de consentement explicite).

Enfin, bien que Productiv[IA] ne vise dans l'immédiat qu'une clientèle québécoise et canadienne, l'équipe se tient prête à **étendre la conformité au RGPD** européen en cas d'ouverture vers l'international. Avant toute entrée d'utilisateurs européens, une analyse d'écart complète serait menée pour s'assurer que les droits des personnes concernées (droit à l'oubli, portabilité des données, etc.) peuvent être exercés sans heurts via la plateforme. Les mécanismes techniques nécessaires (export des données personnelles sur demande, suppression définitive d'un compte, etc.) sont déjà prévus ou facilement activables dans l'architecture, ce qui place Productiv[IA] dans une posture favorable pour une **mise en conformité rapide au RGPD** le cas échéant.

Sécurité de l'information

Statut : *En cours, dispositifs de base en place.* La **cybersécurité** a été intégrée au cœur du développement de Productiv[IA] dès le début, suivant une approche de "sécurité par conception". À ce jour, l'**infrastructure technique** et l'application mettent en œuvre plusieurs contrôles de sécurité conformes aux politiques gouvernementales en vigueur (ex. Politique et Directive gouvernementales en sécurité de l'information). En particulier : les serveurs et conteneurs applicatifs sont isolés et maintenus à jour régulièrement, toutes les communications sont chiffrées (HTTPS/TLS obligatoire), l'**authentification** des utilisateurs est requise en tout temps et gérée via un contrôle strict des accès (rôles et permissions définis pour chaque profil), et une surveillance initiale des journaux système est effectuée.

Le choix d'**OVHcloud Canada** comme hébergeur renforce également la sécurité : outre la localisation des données mentionnée précédemment, OVHcloud offre des garanties de haut niveau en termes de protection des centres de données (contrôles d'accès physiques, redondance de l'alimentation électrique et des liens réseau, dispositifs anti-DDoS, etc.). L'application Productiv[IA] est déployée dans des conteneurs **Docker/Kubernetes**, ce qui améliore son isolation, facilite l'application rapide de correctifs de sécurité et assure une scalabilité maîtrisée.

À l'heure actuelle, aucune brèche de sécurité n'a été constatée dans le cadre des pilotes. Toutefois, certains mécanismes avancés restaient partiellement implémentés en phase initiale (ex. journalisation exhaustive des actions de l'IA, détection automatique d'anomalies sophistiquée). La priorité a été mise sur la sécurisation des éléments essentiels, avec l'intention d'étoffer progressivement le dispositif.

Plan d'action : Plusieurs initiatives sont en cours pour **renforcer continuellement la sécurité** de Productiv[IA] d'ici son déploiement officiel en 2026 :

- **Journalisation et SIEM :** Un module complet de journalisation des événements sera déployé (voir section Auditabilité) et un outil de type **SIEM** (*Security Information and Event Management*) sera intégré. Cela permettra de **corréler les événements de sécurité** sur l'ensemble du système et de repérer proactivement les comportements suspects ou à risque. Par exemple, si un compte utilisateur ou un agent logiciel générait un volume anormal de requêtes ou accédait à des données de façon inhabituelle, une alerte serait automatiquement levée.
- **Détection d'intrusion et réponse automatisée :** Des mécanismes d'**IDS/IPS** (systèmes de détection/prévention d'intrusion) seront activés en environnement de production. Par exemple, en cas de comportement anormal (un compte qui effectuerait des milliers de requêtes en très peu de temps, signe potentiel d'un

script malveillant ou d'une clé compromise), la plateforme pourra bloquer temporairement le compte ou la requête incriminée et notifier immédiatement un administrateur humain. Ce type de protection automatique assure une **réaction en temps réel** aux incidents, limitant les dommages éventuels.

- **Tests d'intrusion et revues de code :** Avant la mise en production finale, des **pentests externes** (tests de pénétration réalisés par des experts indépendants) seront conduits pour éprouver la résistance de Productiv[IA] face à des attaques. Les résultats de ces tests guideront d'éventuels ajustements de sécurité. En interne, l'équipe de développement a institué des **revues de code** systématiques axées sur la sécurité pour chaque mise à jour majeure, et suit des formations continues en sécurité applicative afin de demeurer à jour sur les menaces émergentes.
- **Certification de sécurité :** Comme mentionné, une démarche de certification **SOC 2** a été initiée. L'attestation *Type I* (conception des contrôles) est visée d'ici mars 2026, et la certification *Type II* (efficacité continue des contrôles sur la durée) d'ici septembre 2026. Obtenir cette certification reconnue démontrera aux organismes publics que Productiv[IA] respecte un **standard élevé de contrôle interne** en sécurité de l'information, audité par un tiers de confiance.

Grâce à l'ensemble de ces mesures, Productiv[IA] entend dépasser les exigences minimales et se placer parmi les solutions les plus sûres pour l'administration publique. La stratégie suivie est pleinement en phase avec la volonté gouvernementale de protéger rigoureusement les données confiées et de mériter la confiance des citoyens et employés publics en matière de numérique.

Auditabilité et traçabilité

Statut : *En cours, base établie.* La **traçabilité** des actions et décisions est un aspect crucial dans l'utilisation d'une IA en contexte public, tant pour des raisons de **redevabilité** (accountability) que pour répondre aux enjeux éthiques. Actuellement, Productiv[IA] conserve des **journaux d'activité** pour les opérations principales : connexions des utilisateurs, actions d'administration, et erreurs systèmes critiques sont journalisées avec horodatage. Toutefois, la journalisation détaillée des interactions avec l'IA elle-même n'était que partiellement implémentée lors des premiers pilotes. Cela signifie qu'à ce stade, on enregistre les éléments nécessaires pour un suivi minimal, sans encore tracer *chaque* question posée et *chaque* réponse générée de manière exhaustive.

Plan d'action : Un **module d'auditabilité avancé** est en cours de développement et sera déployé durant les phases pilote. Ce module visera à **journaliser finement chaque interaction** avec l'IA et chaque action significative sur la plateforme. Concrètement, pour

chaque question posée à Productiv[IA], la plateforme enregistrera de manière non-répudiable : l'utilisateur ou le système qui l'a initiée, l'heure exacte, le contexte (document utilisé, agent IA concerné…), ainsi que la réponse fournie par l'IA. De même, toute modification de configuration par un administrateur, ajout ou suppression de contenu, ou intégration d'une nouvelle source de données seront tracés. Ces journaux détaillés, conservés de façon sécurisée, permettront aux administrateurs de l'organisme utilisateur d'accéder à des **rapports d'utilisation complets**.

L'objectif est double : d'une part **prouver la conformité** en pouvant démontrer a posteriori que les règles établies sont respectées (par exemple, prouver qu'aucun usage non autorisé n'a été fait d'un module de Productiv[IA]), et d'autre part **détecter les abus ou dérives éventuelles**. En milieu éducatif, cela pourrait servir à enquêter sur une utilisation inappropriée par un étudiant; de façon plus générale, dans un ministère ou une municipalité, cela permet d'assurer que l'IA n'est pas utilisée à des fins hors cadre. Cette traçabilité répond aux recommandations gouvernementales encourageant la documentation du fonctionnement des IA pour plus de **transparence** dans les décisions automatisées.

D'ici septembre 2026, l'implémentation de ce module d'audit complet sera finalisée et testée. Les journaux seront exportables ou consultables via une interface dédiée, avec des fonctions de recherche et de filtrage pour faciliter les audits internes ou externes. Des **politiques de rétention** seront appliquées à ces journaux conformément aux lois applicables (p. ex. conservation suffisante pour permettre des enquêtes, mais pas plus longtemps que nécessaire afin de respecter la vie privée).

En somme, au moment du déploiement officiel, Productiv[IA] fournira une **traçabilité fine de bout en bout** de l'ensemble des activités liées à l'IA. Cette capacité d'auditabilité renforcée apportera aux directions de la gouvernance TI et aux services juridiques des institutions clientes une assurance supplémentaire quant à la maîtrise de l'outil et au respect des cadres établis.

Architecture ouverte et intégration aux systèmes internes

Statut : *En cours d'intégration.* Productiv[IA] a été conçu comme une solution **ouverte et interopérable**, apte à s'intégrer facilement dans l'environnement technologique des organismes publics. En particulier, l'authentification unique **SSO** (Single Sign-On) via le fournisseur d'identité de l'institution cliente est prévue afin d'harmoniser la gestion des utilisateurs. Durant les toutes premières phases pilotes, si l'intégration SSO n'était pas encore finalisée, des mécanismes temporaires ont été utilisés (comptes locaux provisoires, importation manuelle d'utilisateurs, etc.) pour permettre aux usagers

d'accéder au service. Ces mesures transitoires assurent la continuité du service sans compromettre la sécurité, en attendant l'interconnexion complète avec le système de l'organisation.

Plan d'action : L'intégration SSO complète fait partie des livrables avant le déploiement généralisé. D'ici 2026, Productiv[IA] sera relié aux annuaires d'entreprise des clients (ex. Active Directory/Office 365 Azure AD, ou fédération SAML/OAuth selon le standard utilisé). Chaque utilisateur pourra se connecter avec ses **identifiants institutionnels existants**, éliminant le besoin de gérer un mot de passe supplémentaire. Cette intégration permettra aussi une **synchronisation automatique des rôles et droits** : ainsi, si un employé quitte l'organisation ou change de poste, ses accès à Productiv[IA] seront mis à jour ou révoqués automatiquement via le SSO, en cohérence avec les pratiques RH et TI de l'organisme. Cela garantit une **gestion centralisée des accès** conforme aux politiques de sécurité en vigueur (par exemple, retrait immédiat des accès lors du départ d'un employé).

Au-delà du SSO, Productiv[IA] offre une **architecture modulaire ouverte**. Ses interfaces de programmation (**API**) sont documentées et peuvent permettre des intégrations sur mesure avec d'autres systèmes d'information (par ex. export des résultats de l'IA vers un portail intranet, connexion avec une base de connaissances locale, etc.). Le choix de technologies standard (protocoles web, formats d'échange courants comme JSON) facilite l'interopérabilité. De plus, Productiv[IA] n'enferme pas les données dans un format propriétaire : les contenus générés ou importés peuvent être extraits au besoin, assurant à l'organisation cliente une **maîtrise sur ses données** et évitant toute dépendance forcée.

Cette philosophie d'**architecture ouverte** rejoint les orientations gouvernementales encourageant l'utilisation de solutions souples et non exclusives, y compris le recours aux logiciels libres lorsque cela est pertinent. Si nécessaire, Productiv[IA] pourrait être déployée dans un environnement cloud privé ou sur des infrastructures détenues par un ministère (solution *on-premise*), grâce à sa modularité. En résumé, l'intégration de Productiv[IA] dans le SI des institutions publiques se fait **dans le respect des standards de l'industrie**, sans friction, tout en laissant aux organisations le contrôle de leurs utilisateurs et de leurs données.

Transparence algorithmique et IA responsable

Statut : *Alignement volontariste en place.* Bien qu'aucune loi n'oblige formellement les fournisseurs à dévoiler leurs algorithmes, Productiv[IA] embrasse le principe de **transparence algorithmique** pour renforcer la confiance de ses utilisateurs institutionnels. Concrètement, cela signifie que Productiv[IA] documente et communique aux administrateurs des clients : la nature des modèles d'IA utilisés (par ex. utilisation de

GPT-5 d'OpenAI, ou de modèles maison selon les cas d'usage), les sources d'entraînement de ces modèles dans la mesure du possible, ainsi que les **limitations connues** (biais potentiels, taux d'erreur estimés, filtres de sécurité appliqués, etc.). Cette démarche de transparence permet aux responsables TI et juridiques de bien comprendre le fonctionnement de l'outil et d'anticiper ses impacts. Elle s'inscrit dans le principe de *« l'utilisateur aux commandes »* promu par le gouvernement : l'humain doit garder le contrôle de l'IA, ce qui passe par une compréhension de ce que fait l'algorithme.

Par ailleurs, Productiv[IA] suit de près les **lignes directrices éthiques** en matière d'IA. Par exemple, le **biais** dans les réponses générées est un risque connu de l'IA : la plateforme encourage les utilisateurs à faire preuve d'esprit critique et offre des options pour **valider les sources** des informations fournies. Les modèles intégrés sont régulièrement évalués quant à la neutralité de leurs résultats. En cas de contenu inapproprié ou discriminatoire produit par l'IA, des mécanismes de filtrage et de correction sont en place (le système de feedback interne permet aux utilisateurs de signaler une réponse problématique, qui est alors examinée et peut mener à ajuster les réglages ou entraînements futurs).

Au niveau organisationnel, Productiv[IA] peut fournir aux clients une **charte d'utilisation responsable** de l'IA, reprenant les bonnes pratiques recommandées par le MCN. On y rappelle notamment que l'IA peut comporter des erreurs et ne doit pas être utilisée pour des décisions critiques sans validation humaine, conformément au guide du MCN qui souligne que *« les réponses générées ne doivent pas être considérées comme des informations définitives »* et qu'il incombe à l'utilisateur de les vérifier. Productiv[IA] facilite cette vérification en affichant, lorsque c'est pertinent, les références documentaires ou sources ayant servi à formuler la réponse de l'IA (pour les modules qui s'y prêtent, comme la recherche de réponses dans une base de documents institutionnels).

En outre, l'équipe de Productiv[IA] s'engage à **mesurer et suivre les impacts** de l'utilisation de l'outil. Dans un contexte éducatif, cela se traduit par un suivi des usages pédagogiques pour s'assurer que l'IA améliore réellement l'apprentissage sans encourager la tricherie, par exemple. De manière générale, pour chaque institution, Productiv[IA] propose de réaliser périodiquement un **bilan d'usage de l'IA** couvrant les bénéfices observés, les éventuels incidents ou détournements, et les ajustements recommandés. Cette boucle de rétroaction permet de garantir que l'implantation de l'IA demeure alignée avec les valeurs et objectifs de l'organisation.

Enfin, Productiv[IA] se positionne en partenaire de l'administration publique dans son effort global d'**encadrement de l'IA**. Les recommandations du Conseil de l'innovation du Québec (rapport *Prêt pour l'IA*, 2024) invitent l'État à se doter de mécanismes robustes de gouvernance et de contrôle des systèmes d'IA, tels qu'un registre public et des évaluations

d'impact. Productiv[IA] est prête à **collaborer activement** à de telles initiatives : par exemple, fournir aux organismes toute information nécessaire pour alimenter un registre des outils d'IA (description des fonctionnalités, clientèle visée, bénéfices, etc., en accord avec l'article 2 de l'arrêté 2024-01), ou intégrer dans sa feuille de route les exigences qui pourraient découler d'une loi-cadre future sur l'IA. Cette anticipation des enjeux réglementaires à venir démontre la volonté de Productiv[IA] d'être un acteur **proactif et responsable** dans l'écosystème de l'IA québécois.

Conclusion

En résumé, Productiv[IA] présente à ce jour un niveau de conformité **très satisfaisant** vis-à-vis des exigences applicables aux organismes publics du Québec. Les domaines clés – **accessibilité**, **protection des données personnelles**, **sécurité de l'information**, **interopérabilité** et **transparence** – ont été **anticipés et intégrés dès la conception** du projet. Toutes les mesures requises sont soit **déjà en place**, soit en voie de finalisation avec un échéancier clair. Les quelques éléments restant à peaufiner (achèvement de l'audit d'accessibilité, formalisation complète du registre de données personnelles, déploiement du module d'auditabilité avancé, etc.) font l'objet d'un plan d'action rigoureux, avec des échéances d'ici 2026 – en amont de tout déploiement officiel à grande échelle.

Productiv[IA] s'aligne non seulement sur les **obligations légales** (Loi 25, LPRPDE, lois sectorielles, etc.), mais également sur les **orientations gouvernementales stratégiques** en matière de numérique. En ce sens, la plateforme contribue à l'objectif d'une administration publique québécoise moderne, efficace et digne de confiance, tel qu'exprimé dans la Stratégie numérique 2024–2028. Elle intègre les bonnes pratiques d'IA responsable promues par le MCN et se tient prête à s'adapter à toute nouvelle directive ou loi-cadre sur l'IA qui viendrait encadrer encore plus strictement ce domaine en évolution rapide.

Fort de sa **conformité démontrée** et de ses engagements fermes, Productiv[IA] apparaît comme une solution apte à être déployée dans le secteur public québécois **dès maintenant en projet pilote**. Les décideurs – qu'ils soient directeurs TI, responsables de la gouvernance informationnelle, conseillers juridiques ou directeurs généraux – peuvent avoir l'assurance que Productiv[IA] opère *dans le respect des normes* et *des meilleures pratiques*. Le lancement de projets pilotes avec Productiv[IA] permettra de confirmer en conditions réelles l'efficacité de ces mesures de conformité et d'en récolter les bénéfices (optimisation des processus, gain de temps, aide à la décision) sans compromis sur la sécurité ou l'éthique.

En conclusion, Productiv[IA] est prête à **accompagner les institutions publiques du Québec** dans l'ère de l'intelligence artificielle, de manière **innovante mais responsable**. L'ensemble des dispositions décrites dans ce document témoigne d'une approche sérieuse et proactive de la conformité. Productiv[IA] offre ainsi aux organisations publiques une opportunité d'adopter l'IA en toute confiance, en ayant la certitude que leurs obligations réglementaires et leurs valeurs d'intégrité, de transparence et de protection des citoyens seront pleinement respectées.