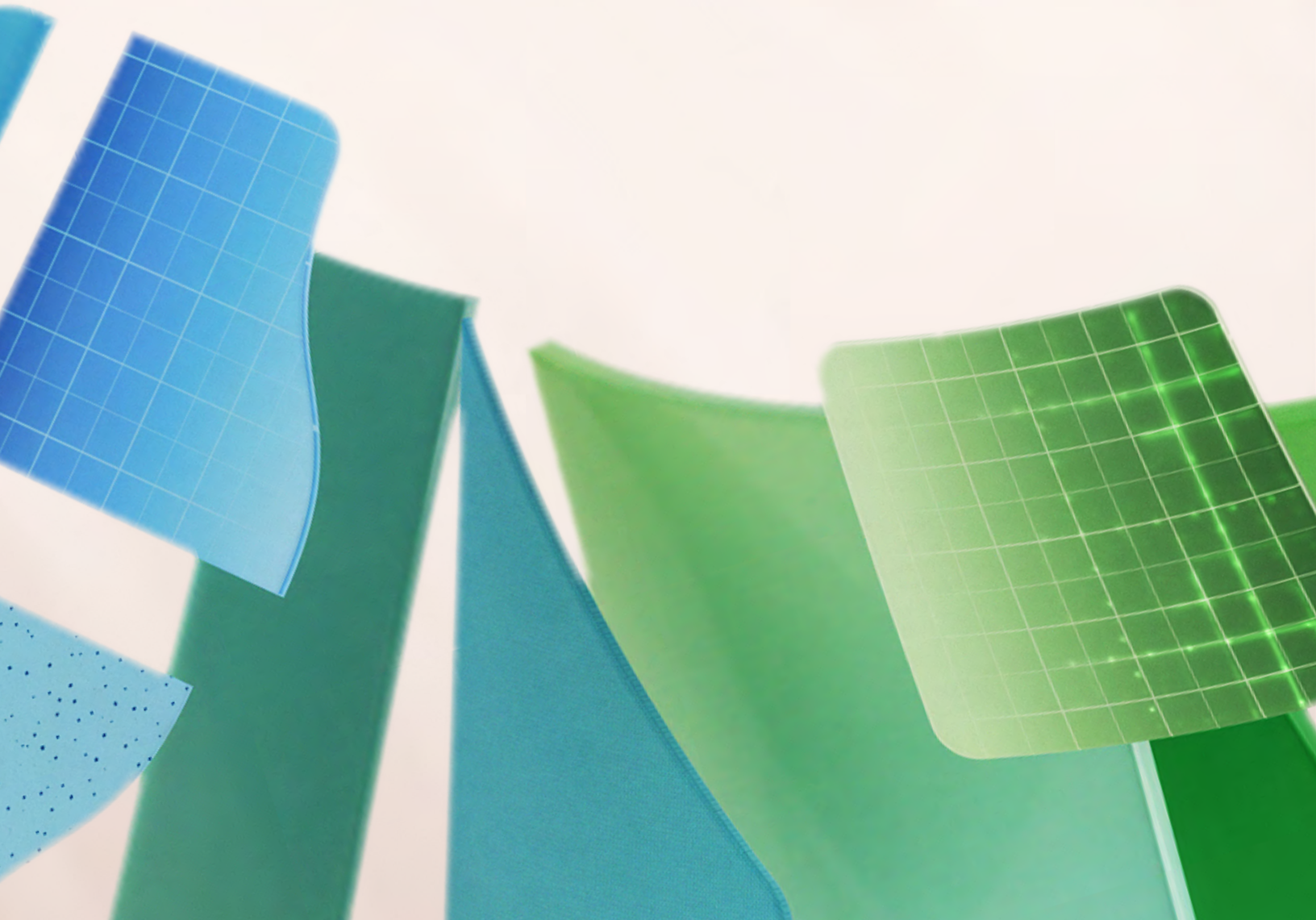
Microsoft 365

Données à contrôler

Maîtriser la gouvernance des données pour asseoir votre réussite grâce à l'IA



Sommaire

Présentation

La gouvernance des données constitue la pierre angulaire d'une adoption de l'IA sécurisée

Conclusion :

Présentation

La gouvernance des données constitue la pierre angulaire d'une adoption de l'IA sécurisée

L'IA générative promet une transformation de l'entreprise, mais pour concrétiser ce potentiel il est nécessaire de disposer de données commerciales de qualité.

Les organisations qui misent sur une gouvernance des données solide seront bien positionnées pour tirer un avantage concurrentiel de l'IA. La gouvernance des données permet de s'assurer que les données interrogées et générées par l'IA sont exactes, sûres, contrôlées et conformes.

Qualité et disponibilité des données : Les systèmes d'IA s'appuient sur de vastes ensembles de données de haute qualité afin de fournir la meilleure réponse possible en tenant compte du contexte des flux de travail spécifiques à votre organisation. Avec des données de qualité, l'IA sera plus à même de tirer des informations stratégiques ou de faire des prévisions tangibles.

Conformité : Une solide gouvernance des données garantit le respect des exigences réglementaires, ce qui minimise l'exposition aux risques d'ordre juridique ou de se voir infliger des amendes.

Sécurité : L'étiquetage et la gestion appropriées des données protègent les informations sensibles contre les accès non autorisés, les partages à mauvais escient et les infractions.

Confiance : Une gouvernance des données fiable renforce la confiance que les parties prenantes accordent aux résultats générés par l'IA, ce qui favorise l'adoption et le soutien des initiatives d'IA.

Cet Ebook présente les pratiques essentielles en matière de gouvernance des données, grâce auxquelles une organisation sera prête à mettre en œuvre l'IA. Il explique comment instaurer des normes rigoureuses en matière de qualité des données, assurer la conformité aux exigences réglementaires et implémenter des mesures de protection et de sécurité des données. Qu'il s'agisse d'empêcher le partage des contenus de réunions sensibles avec des parties externes à l'entreprise ou de se prémunir contre toute éventuelle violation de données, vous découvrirez des stratégies permettant d'instaurer la confiance dans les systèmes d'IA et de rendre les données aisément accessibles afin d'en tirer des informations stratégiques. Grâce à ces pratiques, votre organisation pourra tirer le plein potentiel de l'IA pour favoriser une innovation continue et dégager un avantage concurrentiel.

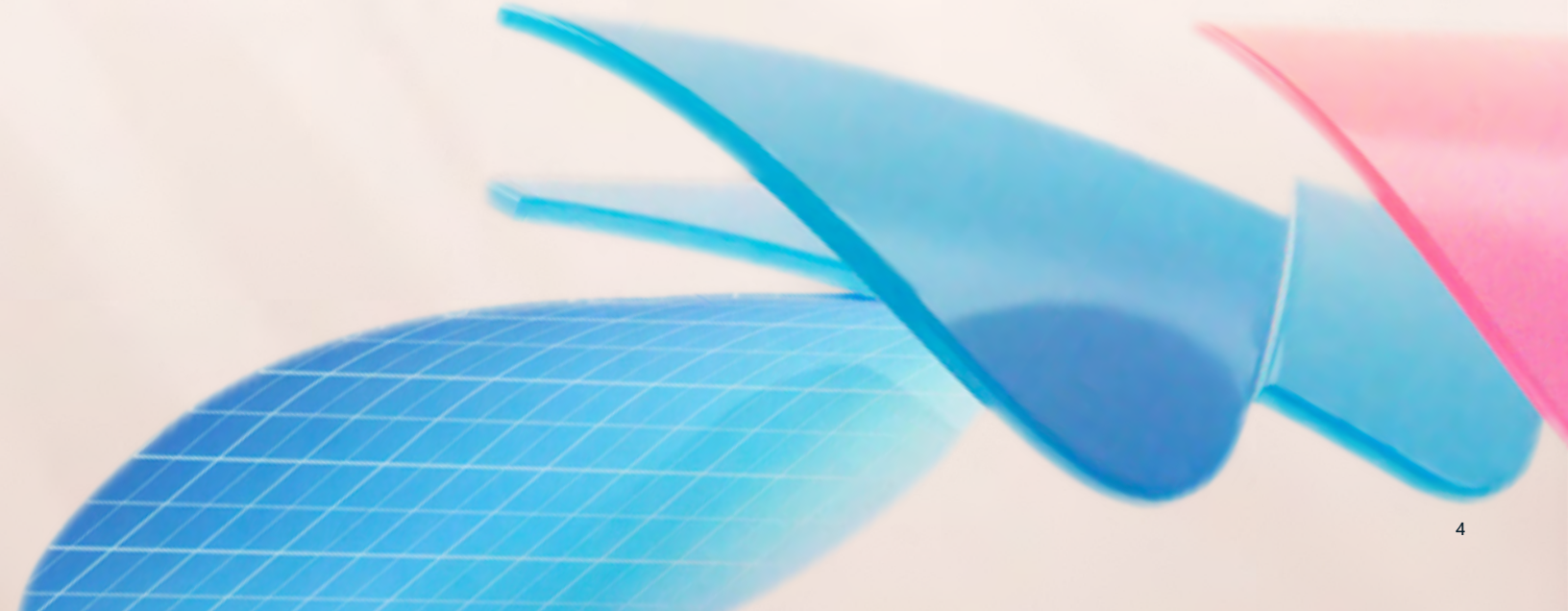
Cas d'utilisation de l'IA générative

Accélérer les communications : Rédiger des contenus personnalisés plus rapidement, pour ainsi consacrer plus de temps à l'établissement de relations et à la collaboration.

Renforcer l'efficacité : Consacrer moins de temps aux tâches routinières, booster la productivité et réduire les coûts.

Favoriser l'innovation : Exprimer des idées et contribuer aux propositions afin de concevoir de nouveaux produits et services.

Personnaliser les expériences client : Adapter le contenu et les recommandations pour favoriser la fidélisation et l'engagement.



1

Renforcer la gouvernance des données pour mener à bien la transformation grâce à l'IA

Chaque entreprise dispose de politiques et de processus qui régissent l'utilisation des données. Les cadres de gouvernance des données varient en termes de maturité et d'exhaustivité, mais peu d'entre eux ont été entièrement optimisés pour l'IA. Si de nombreuses bonnes pratiques en matière de gouvernance des données restent inchangées, comme la garantie de l'exactitude et de la cohérence des données, d'autres aspects doivent être actualisés pour pouvoir maximiser les investissements dans l'IA. Examinons quelques domaines clés.

Visibilité des données

Une connaissance détaillée des flux de données au sein des systèmes d'IA permet de détecter et d'atténuer les utilisations non autorisées ou inappropriées. Cette visibilité contribue à assurer la sécurité et la conformité, en protégeant les données sensibles afin de maximiser la valeur de l'IA.

La gouvernance des données traditionnelle se focalise sur l'identification des emplacements où résident les données et sur le contrôle de l'accès. Cependant, à mesure que l'IA s'intègre davantage dans les activités de l'entreprise, la gouvernance des données doit suivre l'évolution des besoins en matière de sécurité. Par exemple, dans le cas d'un lancement de produit hautement sensible, la gouvernance doit désormais s'étendre à la gestion du contenu généré par l'IA, en veillant à ce que les documents liés au projet, les communications et les idées produites par l'IA soient sécurisés. Cela signifie qu'il faut mettre en place des mesures de protection afin que seuls les membres autorisés de l'équipe puissent accéder à l'IA et l'utiliser pour analyser ou résumer des informations relatives au projet.

En outre, en gérant les volumes de traitement et de stockage des données, les organisations peuvent mieux contrôler les coûts opérationnels associés à l'IA.

Qualité des données

L'IA exacerbe l'importance de la qualité des données, car celle-ci a un impact direct sur les résultats produits par l'IA. Lorsque vous utilisez des outils d'IA pour interroger les données de votre entreprise, vous devez vous assurer que ces données sont actuelles et fiables. Il est tout aussi important de connaître la provenance et la qualité des données que vos équipes utilisent lorsqu'elles conçoivent leurs propres modèles et applications d'IA. Des audits de données réguliers, des processus de validation rigoureux et une gestion proactive permettent de garantir l'intégrité des données. En se concentrant sur ces domaines, les organisations peuvent obtenir des résultats d'IA fiables qui favorisent la prise de décision et l'innovation.

Gestion des utilisateurs

Avec l'IA, les utilisateurs interagissent avec les données de manière sophistiquée. Ils communiquent avec des systèmes d'IA tels que Microsoft 365 Copilot par le biais d'invites en langage naturel. Avec les autorisations et les protections en place, l'IA peut accéder au contexte pertinent des données (fichiers, chats et e-mails) ainsi qu'à des sources externes via des plugins pour générer une réponse.

Il est essentiel de contrôler les données utilisées dans ces processus pour s'assurer que l'IA fournit des réponses correctes et pertinentes. La transparence, par le biais de notes de bas de page ou de liens vers les sources originales, aide les utilisateurs à vérifier la véracité des informations, ce qui réduit le risque d'utilisation abusive des données et garantit la bonne conformité aux réglementations.

Conformité et eDiscovery

L'essor de l'IA vient poser de nouveaux défis en matière de conformité et d'eDiscovery (à savoir la manipulation des données ayant trait à des affaires juridiques), notamment en ce qui concerne la gestion des données générées par l'IA et l'adaptation à l'évolution de l'appareil législatif. L'actualisation des cadres de gouvernance des données pour relever ces défis implique l'élaboration de politiques qui couvrent le contenu généré par l'IA, par exemple en veillant à ce que les documents ou les communications produits par l'IA soient suivis, classés et stockés de manière sécurisée. Par exemple, il peut être nécessaire de mettre à jour les politiques pour s'assurer que les e-mails ou les rapports générés par l'IA sont étiquetés et archivés correctement en vue d'une récupération ultérieure.

L'amélioration des capacités d'eDiscovery passe par l'intégration d'outils d'IA capables de rechercher et d'identifier le contenu généré par l'IA à travers différentes plateformes. Par exemple, lors d'une enquête juridique, les outils d'eDiscovery doivent être capables de trouver et d'extraire des documents spécifiques générés par l'IA, de résumer les communications pertinentes et de fournir des pistes d'audit claires pour prouver la conformité. En mettant à jour ces capacités, les organisations peuvent mieux gérer les données lors d'audits ou d'enquêtes juridiques, en veillant à ce que toutes les informations pertinentes générées par l'IA soient accessibles et défendables devant les tribunaux.

Sécurité des données

La sécurisation des opérations pilotées par l'IA doit impliquer l'application des principes Zero Trust au niveau de la gestion des identités, afin de minimiser le risque d'accès non autorisé. Des mises à jour régulières des terminaux, y compris des appareils et des applications, réduisent les vulnérabilités susceptibles d'être exploitées. Une bonne connaissance des outils d'IA générative utilisés au sein de l'organisation permet de bloquer les applications non autorisées ou non sécurisées, ce qui permet d'éviter les failles de sécurité potentielles.
En limitant l'accès aux outils et aux données d'IA au seul personnel de confiance, les organisations peuvent atteindre une plus grande intégrité des données et protéger leurs opérations d'IA contre les menaces potentielles.

En quoi consiste le Zero Trust ?

Le Zero Trust est un modèle de sécurité qui consiste à vérifier chaque demande comme si elle provenait d'un réseau non fiable. Plutôt que de supposer que tout ce qui se trouve à l'intérieur du pare-feu de l'entreprise est sans danger, cette approche repose sur le principe « ne jamais faire confiance, toujours vérifier ».

Principes Zero Trust

Vérifier de manière explicite : toujours authentifier et autoriser sur la base de tous les points de données disponibles.

Utiliser l'accès basé sur le principe du moindre privilège : limiter l'accès des utilisateurs avec un accès juste à temps et juste suffisant, des politiques adaptatives basées sur le risque et la protection des données.

Anticiper les violations : limiter les dégâts, contrôler l'accès, assurer le chiffrement et utiliser les données pour détecter les menaces et renforcer les défenses.

2

Le rôle de la gouvernance des données dans la transformation pilotée par l'IA : origines, qualité et fiabilité des données

Lorsque les organisations adoptent l'IA pour éclairer leurs prises de décision, elles doivent s'assurer que ces systèmes peuvent fournir des résultats corrects et fiables. Les données sur lesquelles reposent les réponses de l'IA doivent être disponibles, cohérentes et bien documentées.

La gestion des données favorise une IA digne de confiance en mettant en œuvre des politiques de gouvernance qui permettent de suivre l'origine des données, de vérifier leur qualité et de garantir leur fiabilité et leur exactitude. Ces pratiques jettent les bases de systèmes d'IA qui fournissent des informations fiables, permettant une prise de décision éclairée et confiante.

Lignage des données : Comprendre les origines et les modifications des informations

Le lignage des données suit le parcours des données au sein d'une organisation. Il documente les origines, les transformations et les destinations des données. Pour les entreprises optimisées par l'IA, il est essentiel de comprendre le lignage des données, et ce pour plusieurs raisons :

- **Transparence :** Savoir d'où viennent les données et comment elles évoluent permet de confirmer l'exactitude des résultats générés par l'IA et de garantir la conformité réglementaire grâce à une compréhension claire de l'historique des données.
- **Traçabilité :** Le lignage des données permet aux organisations de remonter à la source des erreurs ou des incohérences, ce qui simplifie la résolution des problèmes et la correction des données.
- **Analyse de l'impact :** Comprendre comment les données sont utilisées par les outils d'IA générative permet d'évaluer l'impact potentiel des changements dans les sources de données ou les méthodes de traitement sur la précision des résultats et les résultats commerciaux.

Qualité des données : La qualité des données a une incidence sur la pertinence des réponses fournies par l'IA

La qualité des données a une influence directe sur la fiabilité des résultats fournis par l'IA. Des données de haute qualité fournissent le contexte nécessaire pour que les modèles d'IA soient en mesure de retourner des réponses correctes et véritablement pertinentes compte tenu de la requête de l'utilisateur. Les principaux aspects de la qualité des données sont les suivants :

- **Précision :** Les données doivent représenter fidèlement les conditions réelles.
- **Exhaustivité :** Toutes les données requises doivent être présentes et comptabilisées.
- **Cohérence :** Les données doivent être cohérentes entre les différents systèmes et dans le temps.
- **Rapidité :** Les données doivent être à jour et disponibles en cas de besoin.

Fiabilité des données : Garantir la fiabilité des données

La fiabilité des données signifie que les données répondent systématiquement aux normes de qualité et qu'elles sont disponibles en cas de besoin. Pour les entreprises optimisées par l'IA, la fiabilité des données est un point crucial pour instaurer la confiance dans les outils d'IA et dans les décisions qui en découlent. Voici les points nécessaires pour garantir la fiabilité des données :

- **Redondance des données :** Mettre en place des systèmes de sauvegarde qui évitent les pertes et augmentent la disponibilité.
- **Sauvegardes régulières :** Effectuer des sauvegardes fréquentes pour se protéger contre la corruption ou les pertes de données.
- **Surveillance et alertes :** Mettre en place des systèmes de surveillance pour détecter et alerter les parties prenantes sur les problèmes liés aux données en temps réel.
- **Plans de reprise après sinistre :** Élaborer et tester des plans pour récupérer les données et reprendre les opérations rapidement après des perturbations.

3

La relation entre la gouvernance, la sécurité et une IA responsable

Ensemble, la gouvernance et la sécurité des données constituent l'épine dorsale d'une utilisation responsable de l'IA. Des données sécurisées de haute qualité garantissent une IA à la fois éthique et efficace. Les domaines clés à évaluer comprennent la classification des données, les contrôles d'accès, le chiffrement, la réponse aux incidents et la conformité réglementaire.

Classification des données

La classification des données est un élément essentiel pour contrôler la manière dont les outils d'IA traitent les informations sensibles. En règle générale, les données et les réunions sont classées dans les catégories suivantes : générales, confidentielles ou hautement confidentielles. Une classification appropriée garantit que l'IA n'accède qu'aux informations appropriées, réduisant ainsi le risque d'exposer des données sensibles à des utilisateurs non autorisés.

Une classification inappropriée, en revanche, peut conduire l'IA à traiter des données dont l'utilisation doit être restreinte, ce qui est susceptible de donner lieu à des failles de sécurité ou à des problèmes de conformité. Une gouvernance efficace des données, que ce soit par le biais d'outils automatisés ou de politiques à l'attention des utilisateurs finaux, garantit que les données sont classées correctement, afin de protéger les données sensibles et de permettre à l'IA de fournir des résultats fiables et conformes.

Contrôles d'accès

Ces contrôles déterminent qui peut accéder aux données pertinentes pour l'IA et quelles applications ou identités sont autorisées à interagir avec ces données. Des contrôles d'accès vulnérables peuvent entraîner une exposition non autorisée d'informations sensibles, ce qui accroît le risque d'infraction ou d'utilisation abusive.

La gouvernance des données joue un rôle clé dans l'application de ces contrôles car elle limite l'accès aux données au personnel autorisé et à des applications spécifiques, et veille à ce que les données sensibles soient traitées comme telles. Cela permet non seulement de préserver l'intégrité des données, mais aussi de s'assurer que les systèmes d'IA fonctionnent sur des ensembles de données sécurisés et fiables, ce qui renforce leur fiabilité et leur conformité.

Chiffrement

La sécurisation des données contre toute interception et falsification à l'aide du chiffrement permet de s'assurer que les outils d'IA générative peuvent ancrer leurs réponses dans le contexte adéquat, comme les données liées au travail, les fichiers, les chats et les e-mails, sans risquer une fuite des données.

Les politiques de gouvernance des données peuvent imposer des pratiques de chiffrement robustes, afin de protéger ces dernières sur l'ensemble de leur cycle de vie. Cette approche garantit des réponses fiables de la part des outils d'IA, tout en sécurisant vos données et en préservant la confiance.

Réponse aux incidents

Les données organisationnelles sensibles peuvent être exposées lors d'incidents impliquant des outils d'IA générative qui accordent un accès non autorisé à des fichiers, des e-mails ou d'autres données d'entreprise que les systèmes utilisent pour générer des réponses.

Un plan d'intervention proactif en cas d'incident est crucial dans ces scénarios. Sans un tel plan, l'organisation risque non seulement d'exposer des données sensibles, mais aussi de s'appuyer sur des résultats que l'IA aura produits sur une base erronée. La gouvernance des données inclut des protocoles de réponse détaillés pour traiter rapidement toute infraction, minimiser son impact et préserver la fiabilité des systèmes d'IA.

Conformité aux réglementations

Les applications d'IA doivent adhérer à des réglementations telles que le RGPD ou le CCPA, qui régissent la protection et la confidentialité des données. Tout manquement à de telles réglementations peut entraîner des pénalités conséquentes et éroder la confiance. Il est également crucial de comprendre où les outils d'IA traitent les données, car de nombreux outils gratuits peuvent traiter des données à l'échelle mondiale ou en dehors des lieux de stockage habituels de votre entreprise. La gouvernance des données garantit que les applications d'IA respectent non seulement des cadres légaux, mais qu'elles conservent également les données dans les bonnes limites de service, conformément aux normes de votre organisation. Cette approche sous-tend l'utilisation éthique de l'IA et contribue à renforcer la confiance dans la technologie de l'IA.

4

Mettre à jour votre cadre de gouvernance des données pour favoriser l'adoption de l'IA

Compte tenu de l'évolution rapide de l'IA, il est important d'identifier les domaines spécifiques de votre cadre de gouvernance des données existant qui pourraient nécessiter une attention particulière. Plutôt que de revoir l'ensemble du cadre, vous pouvez vous concentrer sur les domaines les plus susceptibles d'évoluer, en orientant vos efforts là où ils augmenteront le plus la valeur de l'IA tout en garantissant que vos données restent protégées et sécurisées. Voici quelques éléments clés à prendre en compte :

Adapter les politiques et les procédures

L'IA implique de nouveaux types de collecte, de traitement et d'utilisation des données. La mise à jour des politiques de données peut aider à répondre aux besoins pertinents en matière de confidentialité des données, de conformité réglementaire et d'utilisation éthique. Par exemple, exiger l'anonymisation des données dans des cas spécifiques peut protéger les informations personnelles et rendre leur utilisation plus sûre tout au long du cycle de vie de l'IA.

Rôles et responsabilités

Il est essentiel d'intégrer la préparation à l'IA dans tous les rôles impliqués dans la gouvernance des données. Les employés qui connaissent les exigences de l'IA en matière de données peuvent endosser le rôle de garant de la qualité et de la conformité des données. La collaboration interfonctionnelle entre les équipes juridiques, informatiques et de science des données peut permettre de relever plus efficacement les défis spécifiques à l'IA.

Adapter les normes et les définitions des données

La normalisation des formats de données, des définitions et des mesures de qualité simplifie la mise en œuvre des politiques régissant l'utilisation des outils d'IA au sein d'une organisation. Des normes de données claires facilitent le choix des ensembles de données sur lesquels les outils d'IA peuvent raisonner pour fournir un contexte commercial et des données que les utilisateurs peuvent télécharger à des fins d'analyse. Cela garantit que les applications d'IA utilisent les données les plus pertinentes et les plus fiables, ce qui renforce leur efficacité tout en assurant leur conformité avec les politiques de l'organisation.

Amélioration continue

La gouvernance des données est un processus continu, en particulier en ce qui concerne l'IA. Des audits réguliers et des mises à jour de votre cadre de gouvernance peuvent permettre de l'adapter plus rapidement aux évolutions de l'IA et à celles de l'appareil réglementaire. L'IA elle-même peut être utilisée pour vérifier et améliorer les pratiques de gouvernance, en identifiant toute lacune potentielle et en suggérant des améliorations. Cette approche proactive renforce la conformité et l'efficacité au fil de l'évolution des technologies de l'IA.

Outils et techniques pour une gouvernance efficace des données

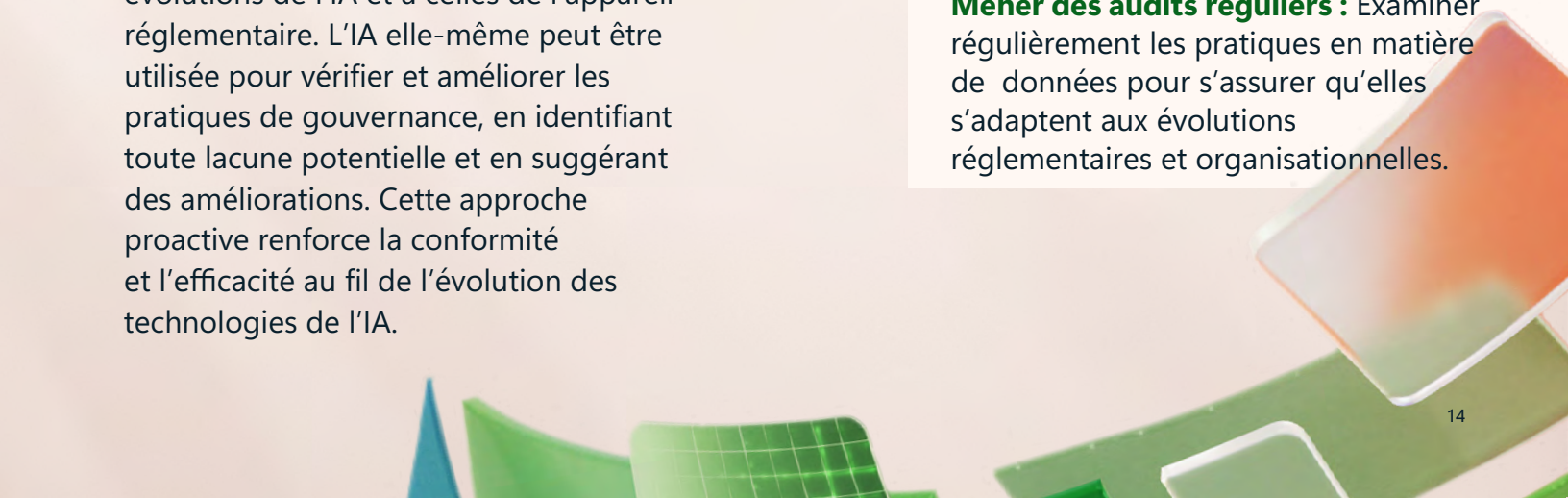
Alignement sur les objectifs de l'entreprise :
Veillez à ce que votre stratégie de gouvernance des données soutienne les objectifs de l'organisation afin d'enrichir la prise de décision et de booster l'efficacité.

Automatiser les tâches de routine :
L'automatisation des tâches répétitives telles que la classification des données et la gestion des accès permet de réduire les erreurs manuelles et de renforcer la sécurité.

Garantir un niveau de précision élevé :
Utiliser des outils de validation et de nettoyage pour garantir l'intégrité des données au fil du temps.

Former les utilisateurs : Proposer une formation aux outils et procédures de gouvernance des données afin d'éviter les erreurs de gestion et de garantir le respect des politiques.

Mener des audits réguliers : Examiner régulièrement les pratiques en matière de données pour s'assurer qu'elles s'adaptent aux évolutions réglementaires et organisationnelles.



Conclusion :

Une gouvernance des données efficace pour la mise en œuvre de l'IA avec Microsoft 365

L'utilisation responsable de l'IA nécessite une solide gouvernance des données. Une gouvernance des données efficace garantit la disponibilité, l'exactitude et la sécurité des données, ce qui permet à l'IA de fournir des informations fiables et de favoriser l'innovation. En misant sur la qualité, la conformité et la sécurité des données, les capacités de l'IA sont optimisées, ce qui permet de prendre de meilleures décisions et de conserver un avantage concurrentiel.

Microsoft 365 : Se préparer efficacement à l'IA

Microsoft 365 offre les meilleures applications de productivité avec des outils intégrés en vue de la classification, du contrôle et de la protection des données. Ces fonctionnalités soutiennent votre cadre de gouvernance des données, et favorisent l'adoption de l'IA en toute confiance lorsque vous êtes prêt. Microsoft 365 vous aide à garantir :

- **Qualité des données :** Soutenir la précision et la fiabilité des résultats de l'IA.
- **Conformité :** Respecter les exigences réglementaires, en réduisant les risques juridiques.
- **Sécurité Zero Trust :** Protéger les informations sensibles contre les accès non autorisés, les violations et les cybermenaces.

Découvrez des outils de productivité complets et améliorés par des options d'IA et une protection robuste pour aider votre organisation à travailler efficacement et en toute sécurité.

Découvrir Microsoft 365