



Les 7 erreurs courantes dans la gouvernance des données

et comment les éviter !

www.keyrus.com

Les 7 erreurs courantes dans la gouvernance des données

et comment les éviter !

La gouvernance des données constitue un enjeu majeur pour les organisations confrontées à une explosion des volumes d'information, à la diversité croissante des sources, et à des exigences réglementaires de plus en plus strictes. Une gestion optimale des données s'avère essentielle pour garantir leur qualité, leur sécurité, et leur utilisation efficace au service de la stratégie de l'entreprise. Cependant, de nombreuses erreurs récurrentes, allant de l'absence de rôles clairement définis à un désalignement avec les objectifs métiers, viennent entraver les efforts en matière de gouvernance. Comprendre ces écueils et les moyens de les éviter est essentiel pour tirer pleinement parti de l'immense potentiel des données tout en minimisant les risques qu'elles impliquent.



Images générées par **Midjourney** avec la consigne :
« Hyper-realistic portrait of a happy marketing team, capturing the essence with bright eyes, lit by overhead lighting, framed in a centered manner --chaos 10 --ar 3:4 --style raw --v 6 »

Comprendre les enjeux et les fondamentaux

La gouvernance des données repose sur des principes clés visant à encadrer l'accès, l'utilisation, et la protection des informations au sein d'une organisation. Elle vise notamment à garantir la qualité des données, leur conformité aux réglementations en vigueur, et leur exploitation optimale pour créer de la valeur.

Cependant, plusieurs défis viennent compliquer la mise en place de cette gouvernance :

- **des volumes de données toujours plus importants**, issus de sources variées.
- **une évolution rapide des technologies et des besoins métiers.**
- **des exigences croissantes en matière de conformité et de sécurité.**

Dans ce contexte, l'adoption d'une stratégie claire et structurée devient un impératif. Mais c'est souvent à cette étape précisément que des erreurs majeures sont commises.



Les 7 erreurs communes dans la gouvernance des données

Chaque organisation est susceptible de rencontrer des obstacles lorsqu'elle entreprend de structurer la gouvernance de ses données. Ces erreurs, bien que fréquentes, peuvent être évitées en les identifiant et en adoptant les bonnes pratiques. Voici les sept écueils principaux auxquels il convient de prêter attention.

1. Absence de rôles et de responsabilités clairement définis

La première étape d'une gouvernance efficace consiste à attribuer des rôles clairs aux différents intervenants : data owner(s), data steward(s), utilisateurs, etc. En l'absence de cette structuration, les responsabilités se diluent, ce qui conduit à des incohérences, des erreurs, voire à des conflits.

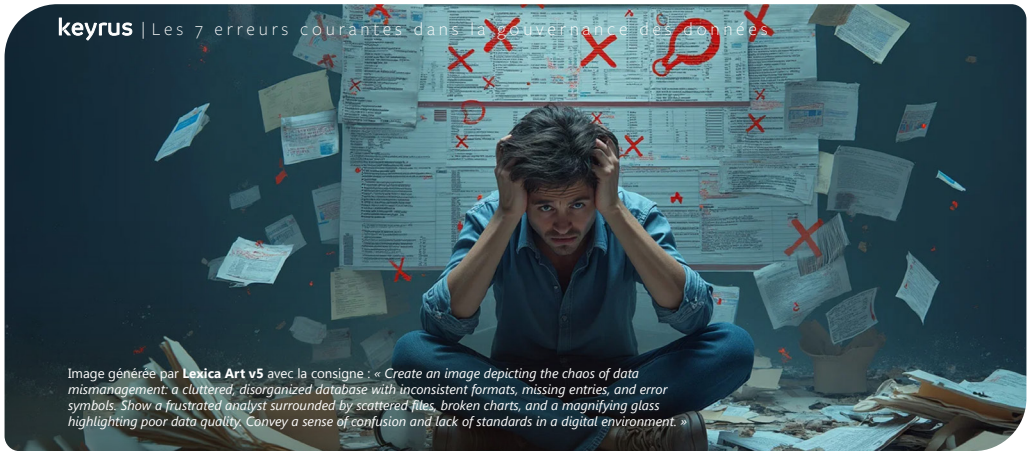


Image générée par **Lexica Art v5** avec la consigne : « Create an image depicting the chaos of data mismanagement: a cluttered, disorganized database with inconsistent formats, missing entries, and error symbols. Show a frustrated analyst surrounded by scattered files, broken charts, and a magnifying glass highlighting poor data quality. Convey a sense of confusion and lack of standards in a digital environment. »

Une entreprise bancaire, par exemple, pourrait rencontrer des conflits internes si elle ne désigne pas de propriétaires clairs pour ses bases de données clients. Dans un tel cas, différents départements pourraient modifier les données sans coordination, créant ainsi des incohérences dans la conformité réglementaire.

Citons aussi pour exemple une start-up technologique travaillant sur des données sensibles peut risquer des fuites si les droits d'accès ne sont pas révoqués pour les anciens employés. Ce manque de clarté peut fragiliser la sécurité globale et affecter les opérations quotidiennes.

2. Manque de standards et de contrôles sur la qualité des données

Les données de mauvaise qualité sont une source majeure de décisions erronées. Sans validation, nettoyage et surveillance systématique, les organisations s'exposent à des incohérences et des duplications. Cependant, toutes les données ne nécessitent pas le même niveau de contrôle. Une approche efficace consiste à prioriser le monitoring en fonction des usages clés et stratégiques. Par exemple, un indicateur critique comme le chiffre d'affaires mérite une attention particulière : il est pertinent de concentrer les efforts sur la validation et la qualité des sources qui l'alimentent, plutôt que d'imposer un contrôle uniforme sur l'ensemble des données.

Dans cette logique, la **Data Governance** et la **Data Observability** sont étroitement liées : sans une surveillance active de la qualité et de la fiabilité des données, la gouvernance des données risque de rester un cadre théorique sans réel impact opérationnel. La Data Observability permet d'ancrer la Data Governance dans le concret en identifiant en temps réel les problèmes de qualité, en facilitant leur correction et en garantissant que les règles établies sont effectivement respectées dans les usages métiers.

Pour illustrer le propos, nous pouvons imaginer dans le secteur de la grande distribution, une entreprise qui ferait face à des surstocks si les doublons dans les bases de produits ne sont pas éliminés par des contrôles rigoureux. Cela entraînerait des pertes financières considérables.

De même, un hôpital utilisant des bases de données pour ses dossiers médicaux pourrait rencontrer des retards critiques dans les soins aux patients si les informations sont mal saisies ou incomplètes, ce qui affecterait directement la qualité des soins.

3. Documentation et accessibilité des métadonnées insuffisantes

Les métadonnées jouent un rôle fondamental dans la compréhension et l'exploitation des données. Lorsqu'elles sont mal documentées ou inaccessibles, leur portée est limitée et les silos d'information se renforcent, freinant ainsi l'interopérabilité et la confiance dans les données.

« La **Data Governance** et la **Data Observability** sont étroitement liées : sans une surveillance active de la qualité et de la fiabilité des données, la gouvernance des données risque de rester un cadre théorique sans réel impact opérationnel. »

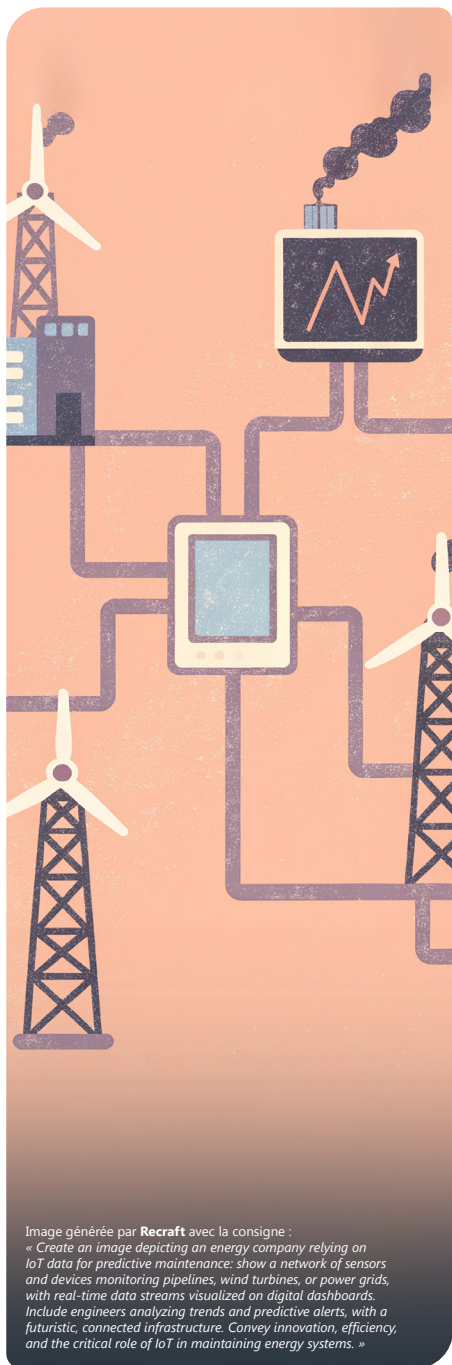


Image générée par **Recraft** avec la consigne :
« Create an image depicting an energy company relying on IoT data for predictive maintenance: show a network of sensors and devices monitoring pipelines, wind turbines, or power grids, with real-time data streams visualized on digital dashboards. Include engineers analyzing trends and predictive alerts, with a futuristic, connected infrastructure. Convey innovation, efficiency, and the critical role of IoT in maintaining energy systems. »

Au-delà des métadonnées, la **traçabilité des données** (*data lineage*) est un élément clé pour assurer une gouvernance efficace. Elle permet de suivre le cycle de vie des données, de leurs origines à leurs transformations successives, jusqu'à leur utilisation finale. Cette visibilité est essentielle pour garantir la fiabilité des analyses, faciliter l'audit des processus et assurer la conformité réglementaire. Sans un suivi clair du data lineage, les décisions basées sur les données restent vulnérables aux erreurs et aux biais induits par des manipulations non maîtrisées.

Ainsi une entreprise de logistique qui gère des livraisons complexes pourrait échouer dans sa transformation digitale si les métadonnées concernant les points de livraison ne sont pas à jour. Cela compliquerait la planification et engendrerait des retards.

De la même manière, une société énergétique dépendant de données IoT pour la maintenance prédictive de ses infrastructures peut se heurter à des coûts élevés si les métadonnées des capteurs ne sont ni centralisées ni documentées. CQFD !

4. Insuffisance des dispositifs de sécurité et de protection de la vie privée

Un manque d'outils pour protéger les données expose l'organisation à des cyberattaques, à des fuites de données sensibles, et à des amendes réglementaires.

Imaginons une plateforme e-commerce qui pourrait être exposée à un ransomware si les mots de passe utilisés ne sont ni cryptés ni suffisamment robustes. Cette faille compromettrait l'intégrité des données clients et la confiance des utilisateurs.

Ou évoquons une mutuelle gérant des données sensibles. Elle risque des sanctions réglementaires sévères si des fichiers confidentiels sont partagés par inadvertance en dehors de l'organisation, exposant ainsi les données personnelles des adhérents. Sans parler du problème moral ou éthique envers ses adhérents...



Image générée par Midjourney avec la consigne :
« Humans are the weak link. »

Cependant, au-delà de l'outillage, c'est avant tout une question de **maturité en matière de sécurité des données**. Les principales failles ne proviennent pas uniquement d'un déficit technologique, mais souvent d'un manque de processus adaptés et de sensibilisation des équipes.

La dimension humaine reste le maillon faible : rares sont les employés qui ont connaissance de l'existence d'une **PSSI (Politique de Sécurité des Systèmes d'Information)** et encore moins nombreux sont ceux qui l'appliquent rigoureusement. Une approche efficace de la sécurité repose donc autant sur la mise en place de contrôles techniques robustes que sur une **culture de la cybersécurité**, incluant formation, sensibilisation et responsabilisation des collaborateurs.

5. Désalignement avec les objectifs stratégiques

La gouvernance des données doit être en phase avec les priorités de l'entreprise. Lorsqu'elle est perçue comme une contrainte technique déconnectée des enjeux métiers, elle perd de son impact.

Ainsi, une entreprise industrielle investissant dans une solution de gouvernance sans impliquer les responsables métiers constatera vraisemblablement que l'outil est sous-utilisé, faute d'adhésion ou de formation adaptée.

De même, une administration locale qui centralise ses archives numériques sans définir de métriques claires pour évaluer le succès du projet risque de dilapider ses ressources (enfin, celles des contribuables) sans résultats concrets.

Précisons qu'un des écueils fréquents réside dans l'approche *hors-sol* (on a les noms !), où un framework de gouvernance est bâti sur des standards théoriques sans réelle adaptation au contexte et aux besoins spécifiques de l'entreprise. Une gouvernance efficace ne peut être figée dès le départ : c'est un projet qui s'éprouve dans la pratique, en acceptant d'ajuster et d'itérer. Essuyer les plâtres au début permet d'identifier les véritables leviers d'adhésion et d'efficacité, et ainsi de construire progressivement une gouvernance opérationnelle et alignée avec les usages métiers.

“ La gouvernance des données doit être en phase avec **les priorités de l'entreprise**. Lorsqu'elle est perçue comme une contrainte technique déconnectée des enjeux métiers, elle perd de son **impact**. ”

6. Résistance au changement et manque d'adaptabilité

Les organisations qui n'anticipent pas l'évolution des volumes, variétés, et réglementations des données se privent d'un atout majeur pour leur croissance et leur innovation.

On se souviendrait tous d'une société automobile qui pourrait mal évaluer l'évolution des volumes de données générés par ses véhicules connectés, ce qui entraînerait des interruptions dans les services clients...

Autre exemple, une institution financière, en refusant d'adopter des outils modernes pour intégrer ses données, peut obliger ses équipes d'analystes à travailler avec des systèmes fragmentés et obsolètes, freinant ainsi son agilité face aux évolutions du marché. Et donc, consécutivement, limiter sa performance.

7. Absence d'outils collaboratifs pour favoriser une approche agile

Une gouvernance des données cloisonnée freine la collaboration entre équipes, ce qui complique l'adoption de bonnes pratiques communes.

Évoquons enfin, dans l'industrie pharmaceutique, un projet d'essais cliniques qui pourrait subir des retards importants si les laboratoires impliqués ne disposent pas d'un espace collaboratif pour partager et valider les données...

...ou une société de conseil, qui pour sa part, peut échouer à livrer une mission critique si ses équipes n'ont pas accès à des outils collaboratifs permettant une gestion fluide et interactive des analyses.



Comment éviter ces erreurs ?

Pour transformer ces erreurs en opportunités d'amélioration, il est essentiel d'adopter une approche méthodique et proactive. Les recommandations qui suivent offrent des solutions concrètes pour bâtir une gouvernance des données robuste et efficace.

Clarifier les rôles et responsabilités : la définition claire des rôles est un pilier essentiel de la gouvernance des données. Chaque intervenant doit connaître précisément ses missions et ses responsabilités : propriétaires des données, gestionnaires, ou utilisateurs. Cette clarté permet d'éviter les conflits et garantit une gestion fluide et coordonnée.



Image générée par Midjourney avec la consigne : « Create an image depicting the establishment of data quality standards and systematic controls: a structured, modern data center with clear labels, organized workflows, and validation tools in action. Show a team of professionals monitoring dashboards, with symbols like checkmarks, magnifying glasses, and flowcharts representing rigorous checks and lifecycle management. Convey precision, efficiency, and the importance of high-quality data for effective use. --chaos 10 --style raw --weird 300 »

Mettre en place des standards de qualité et des contrôles systématiques : la qualité des données est au cœur de leur exploitation efficace. En établissant des standards rigoureux, accompagnés d'outils performants pour valider et surveiller les données tout au long de leur cycle de vie, les organisations peuvent prévenir les erreurs et les incohérences.

Renforcer la documentation et l'accessibilité des métadonnées. On n'insistera jamais assez sur la valeur d'une bonne documentation des métadonnées. Complète et accessible, elle favorise la collaboration et améliore l'exploitation des données. Investir dans des outils de gestion adaptés et garantir leur mise à jour régulière permettent d'éliminer les silos d'information et d'accroître la transparence.

« En toutes choses sachons raison garder » répétaient inlassablement nos profs de lycées, vous en souvenez-vous ? Et bien en *datagouv*, c'est pareil ! Il faut savoir **prioriser la sécurité et la conformité sans tomber dans l'excès de complexité**.

Protéger les données sensibles et garantir la conformité réglementaire sont des impératifs majeurs pour toute organisation. Mettre en œuvre des dispositifs de sécurité robustes et réaliser des audits réguliers permet d'assurer cette protection tout en limitant les risques de sanctions.

Cependant, une erreur courante consiste à traiter ces sujets de manière trop stricte et déconnectée de la réalité opérationnelle. Une **surcomplexité dans la gestion des permissions**, par exemple, peut générer des contraintes inutiles sans véritable gain en sécurité ou en conformité. Dans la pratique, une approche plus pragmatique permet souvent d'optimiser ces mécanismes en simplifiant les règles d'accès tout en garantissant un niveau de protection adéquat. Il s'agit de trouver un **équilibre entre rigueur et pragmatisme**, en adaptant les exigences aux vrais risques et aux besoins métiers, plutôt que de suivre une approche purement théorique.

Une gouvernance efficace doit s'inscrire dans les priorités stratégiques de l'entreprise. En impliquant les parties prenantes dès le départ et en répondant aux besoins métiers identifiés, les organisations transforment la gouvernance en levier de performance.

Last but not least, la gouvernance des données est un processus évolutif. Pour réussir, les entreprises doivent **sensibiliser leurs équipes aux enjeux, encourager une approche agile, et promouvoir l'adoption d'outils collaboratifs**. Des formations régulières et des ateliers pratiques peuvent accélérer cette transition vers une culture de l'amélioration continue.

Le principe think big, start small s'applique plus que jamais : il est essentiel de penser la gouvernance à l'échelle de l'entreprise, mais de commencer par **un ou deux projets pilotes** permettant de capitaliser sur un retour d'expérience (ReX) concret et d'obtenir des résultats tangibles avant toute généralisation. Sans cette approche itérative, on risque de s'engager dans des chantiers lourds, interminables et démobilisants pour les équipes.

Un bon point de départ consiste à **tester des règles de qualité de données simples mais structurantes**, comme la validation des **clés uniques** (*unique key*), des contraintes de **non-nullité** (*not null*), ou encore des vérifications élémentaires au plus proche des transformations de données, notamment via des approches comme **dbt** (*data build tool*, qui permet aux spécialistes data de transformer leurs données au sein-même de leur *data warehouse*). Ces premières étapes apportent rapidement de la valeur tout en préparant une montée en maturité progressive et maîtrisée.

Les bénéfiques d'une gouvernance maîtrisée pour une transformation durable

Une gouvernance des données bien conçue et exécutée offre de nombreux avantages :

- **Amélioration de la prise de décision** grâce à des données fiables et pertinentes.
- **Optimisation des coûts** par une meilleure gestion des ressources et une réduction des duplications.
- **Renforcement de la sécurité** et de la conformité, évitant ainsi des amendes et des litiges.
- **Accélération de l'innovation** grâce à des données mieux exploitées.

Keyrus accompagne les entreprises dans cette démarche, en proposant des solutions sur mesure pour mettre en place une gouvernance des données efficace et pérenne. Grâce à son expertise, Keyrus aide les organisations à transformer leurs défis en occasions et à exploiter pleinement le potentiel de leurs données.

Pour exploiter pleinement ce potentiel, les organisations peuvent bénéficier d'un accompagnement spécialisé, capable de transformer une contrainte en véritable levier de performance.

En évitant les erreurs classiques et en adoptant des pratiques solides, votre organisation peut transformer sa gouvernance des données en un atout stratégique durable.

Article co-écrit par Keyrus, ChatGPT4o et Mistral, Claude, Copilot, Perplexity, deepseek et Gemini

Les unes auxquelles vous avez échappé...

Lors de la création de nos ebooks, chaque image naît d'un processus itératif avec le moteur d'IA. Des allers-retours répétés permettent d'affiner chaque visuel, jusqu'à atteindre l'expression la plus fidèle de l'idée souhaitée. Mais le travail ne s'arrête pas là : parmi les images générées, il faut ensuite opérer des choix. Ce processus de sélection repose sur un effort d'objectivation, où il s'agit de mettre de côté sa propre subjectivité pour respecter au mieux le « cahier des charges ». Une démarche délicate, tant les images peuvent inspirer, surprendre, voire fasciner, mais essentielle pour rester fidèle à l'intention initiale.

L'atelier du prompteur...

Images générées par **MidJourney** avec la

consigne : « *Hyper-realistic portrait of a happy marketing team, capturing the essence with bright eyes, lit by overhead lighting , framed in a centered manner*

--chaos 10 --ar 3:4 --style raw --v 6 »



Vous avez trouvé cette lecture utile ?

Vous aimerez sûrement aussi :

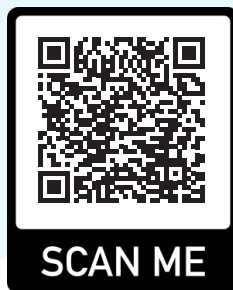
We don't need no limitations

Déconstruire les murs de l'IA

We Don't Need No Limitations explore les barrières qui freinent le développement et l'intégration de l'intelligence artificielle, à travers la métaphore des murs. S'appuyant sur la théorie des cinq murs de l'IA de Bertrand Braunschweig (confiance, consommation énergétique, sécurité des systèmes, interactions homme-machine, inhumanité des machines), il ajoute un sixième obstacle : la limitation des données d'apprentissage. Le document analyse ces barrières sous l'angle actif/passif : certaines sont intentionnellement érigées pour protéger, d'autres émergent des limites techniques. LeBook invite à une réflexion sur la démolition consciente de ces murs pour intégrer l'IA de manière harmonieuse, équilibrée et éthique.

Quelles sont les 3 principales idées ?

1. Les murs de l'IA comme obstacles : les six murs (confiance, consommation énergétique, sécurité, interactions homme-machine, inhumanité, limitation des données) freinent le développement et l'intégration de l'IA.
2. Distinction actif/passif : certains murs sont consciemment érigés pour protéger, tandis que d'autres émergent des limites techniques ou contextuelles.
3. Démolition consciente : surmonter ces barrières nécessite innovation, régulation et éthique pour intégrer l'IA de manière équilibrée et au service de l'humain.





Tech Advisory Board

Tech Advisory Board TAB

Conçu pour éclairer les orientations technologiques de Keyrus en s'appuyant sur des convictions fortes et des offres de pointe, notre TAB incarne une vision ambitieuse et innovante au service de l'excellence technologique.

Le TAB, c'est qui ?

Il est aujourd'hui composé de 9 experts, qui couvrent de concert toute la chaîne de valeur de la donnée : de l'architecture à l'ingénierie, l'analyse, la gouvernance, la gestion, jusqu'à la stratégie des données. Et évidemment notre ancrage dans la data science avec nos experts en Intelligence Artificielle.

Les membres du TAB : **Arnaud Col, Van Tuan Dang, Gilles Dansou, Cao Tri Do, Benoit Domas, Antoine Giraud, Ali Hadji, Mostepha Khouadjia, Jonathan Meklat, Nassim Nalla, et Patricio Touchard.**

Le TAB, c'est quoi ?

C'est LE board réunissant les leaders Tech de Keyrus France ! Il incarne l'expertise collective de nos Tech Leads en France pour positionner Keyrus comme un acteur de référence en termes de technologie et d'innovation.

Le TAB, pourquoi ?

- Participer à la co-construction de nos offres innovantes
- Transformer les technologies disruptives en cas d'usage à valeur
- Développer l'excellence de réalisation de nos équipes
- Challenger nos clients dans leurs orientations et choix technologiques

Le TAB, pour qui ?

Pour nos clients et partenaires dans l'écosystème Keyrus France ! Parce que notre objectif est de toujours vous offrir une expérience technologique unique, le TAB est à vos côtés pour vous aider à naviguer avec succès dans un paysage technologique en constante évolution.

keyrus

make data matter

Du conseil en management à l'intégration des technologies digitales, Keyrus met depuis 28 ans les données au cœur de chaque transformation pour accompagner ses clients dans l'amélioration continue et durable de leur performance au travers de 5 domaines d'expertise :

- **IA & Automatisation** : accompagner les entreprises et organisations publiques dans l'optimisation de leurs processus, l'augmentation de leur productivité et de leur performance opérationnelle pour leur permettre ainsi de se concentrer sur des activités à forte valeur ajoutée.
- **Expérience digitale** : aider les entreprises à imaginer et à créer des expériences digitales multicanales inspirantes et engageantes pour atteindre leurs objectifs commerciaux.
- **Data & Analytics** : permettre aux organisations de développer et de déployer les capacités nécessaires pour donner du sens et de la valeur aux données.
- **Cloud & Sécurité** : offrir des solutions Cloud robustes, flexibles et sécurisées, garantissant la confidentialité et l'intégrité des données dans un environnement en pleine transformation.
- **Transformation & Innovation** : aider les organisations à accélérer leur transformation métier et digitale et renforcer leur agilité, résilience et compétitivité dans un contexte en perpétuelle évolution.

Avec une présence dans 28 pays et comptant plus de 3 300 experts, Keyrus est l'acteur incontournable et inspirant dans les domaines du conseil en management, de la data, du digital et bien sûr de l'IA en France et à l'international.

Pour en savoir plus : www.keyrus.fr

#HumanizingTheFuture

Jean-Philippe CLAIR

Directeur Marketing, Communication & Expérience client

jean-philippe.clair@keyrus.com