Microsoft Sovereign Cloud pour l'Europe

Mars 2026

Microsoft

Notifications

Ce livre blanc fournit une présentation détaillée du Microsoft Sovereign Cloud, l'approche globale de Microsoft en matière de souveraineté numérique pour les gouvernements, les organisations du secteur public et les entreprises opérant dans des secteurs hautement réglementés ou critiques. Il explique comment Microsoft assure la souveraineté grâce à l'architecture technique, à la gouvernance opérationnelle et aux engagements juridiques, sans fragmenter la plateforme cloud ni limiter l'accès à l'innovation.

Ce document s'adresse à des publics externes, notamment des clients, des organismes de réglementation et des parties prenantes. Il est fourni à titre informatif uniquement et ne crée pas d'engagements contractuels.

Table des matières

Introduction

Chez Microsoft, nous pensons que les clients ne devraient jamais avoir à choisir entre souveraineté, sécurité et innovation. Le Microsoft Sovereign Cloud est conçu comme un portefeuille complet offrant des contrôles souverains de classe mondiale sur les clouds publics, privés et partenaires nationaux, là où les réglementations propres à chaque pays exigent une propriété et un contrôle indépendants.

À mesure que le cloud computing, les données et l'intelligence artificielle deviennent des éléments fondamentaux de la compétitivité économique, des services publics et de la sécurité nationale, les gouvernements et les entreprises accordent une attention croissante à la maîtrise du contrôle et de l'accès à leur infrastructure numérique, à leurs données et à leurs systèmes critiques. Ce changement a placé la souveraineté numérique au premier plan de la prise de décisions stratégiques. À travers l'Europe, ces technologies sous-tendent désormais tout, de l'administration publique et des soins de santé aux marchés financiers, en passant par la production industrielle et les chaînes d'approvisionnement. C'est pourquoi les questions de contrôle, de gouvernance et de cadres juridiques applicables sont désormais traitées au plus haut niveau, tant dans les conseils d'administration que dans les gouvernements.

Microsoft fournit une infrastructure mondiale sécurisée, résiliente et complète, couvrant plus de 70 régions de datacenters et opérant dans plus de 400 datacenters à travers le monde. Cette infrastructure prend en charge les clients avec un continuum de contrôles souverains. Elle intègre des contrôles qui permettent aux organisations d'appliquer le niveau de souveraineté approprié pour chaque charge de travail, dans des environnements publics, hybrides, entièrement déconnectés ou gouvernés localement si nécessaire. En intégrant une protection à chaque couche du cloud, Microsoft permet aux clients d'exécuter leurs charges de travail critiques en toute confiance, en les aidant à garder le contrôle sur les données, les accès et les opérations afin de répondre aux exigences de sécurité et de conformité les plus strictes.

Forte de plus de 40 ans d'expérience en tant qu'entreprise en Europe, Microsoft réalise des investissements soutenus et à long terme afin de veiller à ce que cette infrastructure mondiale soit construite, exploitée et régie conformément aux valeurs, aux lois et aux attentes européennes. Ces investissements comprennent l'expansion continue des infrastructures cloud et d'IA dans les États membres de l'Union européenne et de l'AELE, renforçant ainsi la résilience, la capacité et la redondance régionales tout en soutenant la croissance numérique et économique de l'Europe.

Parallèlement, l'Europe est confrontée à un paysage réglementaire en évolution rapide, à la montée des cybermenaces et à une incertitude géopolitique accrue. Les organisations subissent une pression croissante pour innover de manière responsable en adoptant les technologies de cloud et d'IA, tout en veillant à ce que leurs données, leurs opérations et leur propriété intellectuelle restent protégées par le droit européen. Ces pressions s'étendent au-delà du secteur public aux opérateurs d'infrastructures critiques et aux secteurs hautement réglementés, notamment les services financiers, la santé, l'énergie, les télécommunications et la production industrielle. Pour de nombreuses organisations, la souveraineté numérique n'est plus un concept abstrait, c'est une exigence concrète à laquelle les fournisseurs du cloud doivent répondre sur les plans de la technologie, des opérations et de la gouvernance.

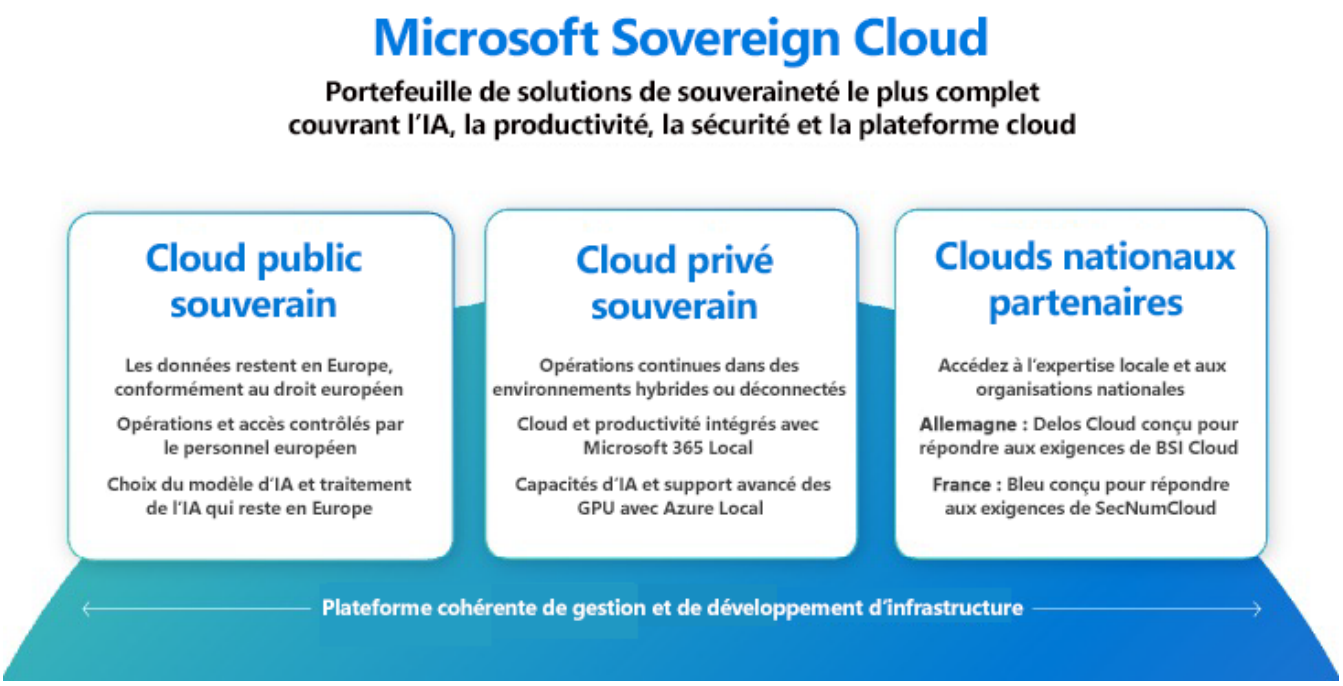
En avril 2025, nous avons réaffirmé et approfondi notre engagement à long terme envers l'Europe en annonçant nos engagements européens en matière de numérique, renforçant et élargissant un ensemble d'assurances juridiques, techniques et opérationnelles contraignantes conçues spécifiquement pour répondre à ces préoccupations. Ces engagements s'appuient sur plus d'une décennie d'investissements dans la confidentialité, la sécurité, la conformité et la résilience, notamment la préparation au RGPD, des pratiques de transparence de longue date, et la limite des données de l'UE pour le Microsoft Cloud. Ensemble, ils reflètent le rôle de Microsoft en tant qu'infrastructure critique pour l'Europe et la responsabilité qui l'accompagne d'opérer de manière à soutenir les cadres juridiques, les attentes réglementaires et les valeurs européennes.

Le Microsoft Sovereign Cloud s'appuie sur cette base en convertissant l'échelle mondiale de Microsoft, ses investissements en Europe et ses engagements numériques européens en capacités de souveraineté pratiques et configurables pour les clients. Plutôt que d'isoler nos clients dans des environnements séparés ou à fonctionnalités réduites, nous fournissons la souveraineté directement dans le Microsoft Cloud grâce à des contrôles intégrés, des modèles de déploiement flexibles et des engagements juridiquement contraignants. Cette approche permet aux organisations de répondre aux exigences de souveraineté en constante évolution, tout en continuant de bénéficier de la puissance, de la sécurité et de l'innovation du Microsoft Cloud, tout en préservant la conformité, le contrôle et la confiance.

Notre approche de conception

Notre approche est simple : la souveraineté numérique est fondamentale pour notre cloud et nos services, délivrée par une combinaison bien gouvernée de contrôles techniques, contractuels et opérationnels. Dans la mesure où chaque charge de travail et chaque organisation présente des niveaux différents de sensibilité et de criticité, les exigences de souveraineté sont adaptables aux besoins de chaque client.

Le Microsoft Sovereign Cloud regroupe l'IA, la productivité, la sécurité et les charges de travail cloud afin de s'adapter aux environnements publics, hybrides et déconnectés, pour que les clients puissent appliquer le niveau de contrôle, de capacité et de conformité approprié en fonction de la sensibilité et de la criticité de chaque charge de travail, au lieu de s'appuyer sur un seul modèle de déploiement.



Cloud public souverain

Fort de notre expérience dans la fourniture de solutions de souveraineté répondant aux besoins du secteur public et des clients les plus réglementés, notre cloud public souverain est le seul fournisseur de cloud à proposer des capacités sur toute la pile technologique en matière d'IA, de productivité, de sécurité et de plateforme cloud à tous les clients européens dans l'ensemble des régions de datacenters européennes existantes.

Avec le cloud public souverain, les données client (y compris les données traitées par les services d'IA, qu'elles soient au repos ou en transit) restent en Europe, conformément au droit européen, avec des opérations et des accès contrôlés par du personnel européen, et un chiffrement sous le contrôle total des clients. Cela s'applique à toutes les charges de travail client exécutées dans nos régions de datacenters européennes, sans nécessité de migration. Les organisations n'ont pas à migrer vers un cloud distinct, à repenser leurs environnements ou à modifier leurs architectures pour répondre à leurs exigences de souveraineté. Elles peuvent appliquer des contrôles de souveraineté dans l'environnement qu'elles exploitent déjà.

Limite des données de l'UE pour les environnements de cloud public

Depuis 2023, Microsoft exploite une Limite des données de l'UE complète pour stocker et traiter les données des clients des pays de l'Union européenne (UE) et de l'Association européenne de libre-échange (AELE) au sein de l'Europe, sauf si les clients configurent explicitement les services autrement. Cet engagement vise à donner aux clients un contrôle clair sur l'emplacement des données, tout en respectant les exigences de protection des données de l'UE et des États membres.

Dans le cadre de la Limite des données de l'UE, Microsoft conserve le contenu des clients (fichiers, courriels, documents et données d'application) dans des datacenters situés au sein de l'UE/AELE pour les services couverts, y compris Microsoft 365, Azure, Dynamics 365 et Power Platform. Les clients conservent la possibilité de configurer le déplacement des données ou d'activer des scénarios interrégionaux lorsque cela est requis par leurs opérations commerciales.

Outre le contenu des clients, la Limite des données de l'UE de Microsoft s'étend aux données générées par le service, y compris les données personnelles pseudonymisées, les journaux système, la télémétrie et les données des services professionnels générées lors des interactions de support. Avec l'achèvement de la phase finale de la Limite des données de l'UE, cette catégorie de données, souvent négligée dans les discussions sur la résidence des données, est également stockée au sein de l'UE/AELE pour les services concernés (cela n'inclut pas les données de facturation). Cela réduit les flux de données transfrontaliers et favorise une position de résidence plus complète que les modèles qui se concentrent uniquement sur les données créées par les clients.

Les engagements de Microsoft concernant la limite des données incluent également le traitement des données par l'IA. Pour les services éligibles tels que Microsoft 365 Copilot, les requêtes et les réponses sont traitées au sein de la Limite des données de l'UE pour les clients résidant dans l'UE/AELE et Microsoft développe des options de traitement local des données d'IA afin de localiser davantage le traitement lorsque cela est nécessaire.

Microsoft collabore étroitement avec ses clients, les régulateurs et les autorités de protection des données afin de fournir une documentation claire, des rapports de transparence et des engagements contractuels décrivant les pratiques de gestion des données et les contrôles utilisés pour garantir le respect de la Limite des données de l'UE. Cette approche permet aux clients d'évaluer et de démontrer leur conformité tout en continuant à bénéficier de l'échelle, de la sécurité et de l'innovation du Microsoft Sovereign Cloud.

Contrôles techniques

Microsoft met en œuvre des contrôles techniques de défense en profondeur qui réduisent la dépendance envers la confiance de l'opérateur et offrent aux clients un contrôle vérifiable fondé sur le chiffrement de leurs données. Cela inclut :

- **Zone d'atterrissage souveraine (SLZ) pour une gouvernance et un déploiement pilotés par les politiques :** Fondée sur la zone d'atterrissage Azure (ALZ), la zone d'atterrissage souveraine fournit une architecture de référence prescriptive et évolutive ainsi que des outils pour opérationnaliser la souveraineté numérique dans Azure. La SLZ applique les exigences de gouvernance et de conformité dès le départ, avec les dernières mises à jour, notamment une hiérarchie améliorée des groupes d'administration et des définitions, initiatives et affectations d'Azure Policy intégrées, alignées sur les niveaux de contrôle du cloud public souverain. La SLZ inclut des conseils pour le déploiement de services clés, tels qu'Azure Key Vault Managed HSM le cas échéant, afin de prendre en charge des niveaux plus élevés de contrôle souverain. Le déploiement est rationalisé grâce aux accélérateurs de zone d'atterrissage Azure, à l'Infrastructure en tant que code (IaC) et aux bibliothèques réutilisables, ce qui permet aux organisations d'appliquer des contrôles souverains de manière cohérente dans tous les environnements.

- **Isolation matérielle et protection des données en cours d'utilisation :** Au niveau de l'infrastructure, Microsoft propose Azure Confidential Computing, qui protège les données lorsqu'elles sont en cours de traitement en exécutant les charges de travail à l'intérieur d'environnements d'exécution de confiance (TEE) basés sur le matériel. Ces environnements sont conçus de sorte que les données restent chiffrées en mémoire et inaccessibles aux opérateurs du cloud, aux administrateurs ou à tout autre processus logiciel en dehors de l'enclave. Les clients peuvent utiliser l'attestation à distance pour valider l'intégrité de la pile matérielle et logicielle avant que les charges de travail ne soient autorisées à être exécutées, ce qui permet de s'assurer que seuls des environnements de confiance peuvent traiter des données sensibles.

- **Contrôle client basé sur des clés pour l'accès aux données :** Microsoft restreint davantage l'accès via un chiffrement sous contrôle du client. Grâce à Customer Managed Keys, Azure Key Vault Managed HSM et External Key Management, les clients conservent le contrôle des clés de chiffrement utilisées pour protéger leurs données. Dans la mesure où Microsoft ne possède pas ces clés, nous ne pouvons pas déchiffrer les données client de manière indépendante. Dans le cas d'une demande d'accès gouvernemental légal, toutes les données fournies restent chiffrées et la possibilité de les déverrouiller appartient au client.

- **Accès restreint et auditable des opérateurs :** Pour les scénarios opérationnels impliquant un accès limité afin de garantir la fiabilité du service, Microsoft impose des contrôles d'accès stricts avec visibilité pour le client. Customer Lockbox exige l'approbation explicite du client avant que le personnel de Microsoft ne puisse accéder au contenu du client lors des incidents de support. Pour les opérations souveraines européennes, Data Guardian ajoute l'approbation du personnel européen et enregistre toutes les actions d'accès privilégié dans des journaux infalsifiables, permettant ainsi une revue a posteriori et un audit réglementaire. Les chemins d'accès sont authentifiés, autorisés et consignés, et l'outillage est conçu pour rendre les accès privilégiés à la fois exceptionnels et traçables, plutôt qu'implicites.

- **Transparence et journalisation :** Microsoft fournit des fonctionnalités complètes de journalisation et d'audit sur ses services cloud, permettant aux clients d'assurer le pilotage des actions administratives, des tentatives d'accès et des opérations relatives aux données. Les enregistrements d'audit sont protégés pour empêcher toute modification non autorisée et sont disponibles pour soutenir la gouvernance interne et l'examen réglementaire externe. Les engagements contractuels de Microsoft renforcent encore ces mesures techniques en exigeant la journalisation, la justification de l'accès et la notification au client dans le cadre de ses contrôles opérationnels, ce qui permet de s'assurer que les garanties techniques sont complétées par des obligations exécutoires.

Feuille de route du cloud public

- **Data Guardian (fonctionnalité à venir)** pour les opérations sous contrôle européen dans nos régions de datacenters européennes. Data Guardian offrira une garantie supplémentaire que le personnel européen contrôle l'accès à ces régions de datacenters européennes. L'accès des ingénieurs Microsoft aux systèmes qui stockent et traitent des données en Europe est approuvé et surveillé en temps réel par le personnel européen, et sera consigné dans un registre infalsifiable.
- **Gestion de clés externes (fonctionnalité à venir)** pour le chiffrement contrôlé par le client. En utilisant des clés externes ou détenues par le client, les clients peuvent empêcher les tiers et les fournisseurs de cloud de déchiffrer leur contenu afin de pouvoir contrôler les décisions d'autorisation et de réduire l'exposition aux demandes d'accès extraterritoriales.
- **La gestion de l'environnement réglementé (fonctionnalité à venir)** fournira une configuration simplifiée de ces contrôles souverains.

Cloud privé souverain

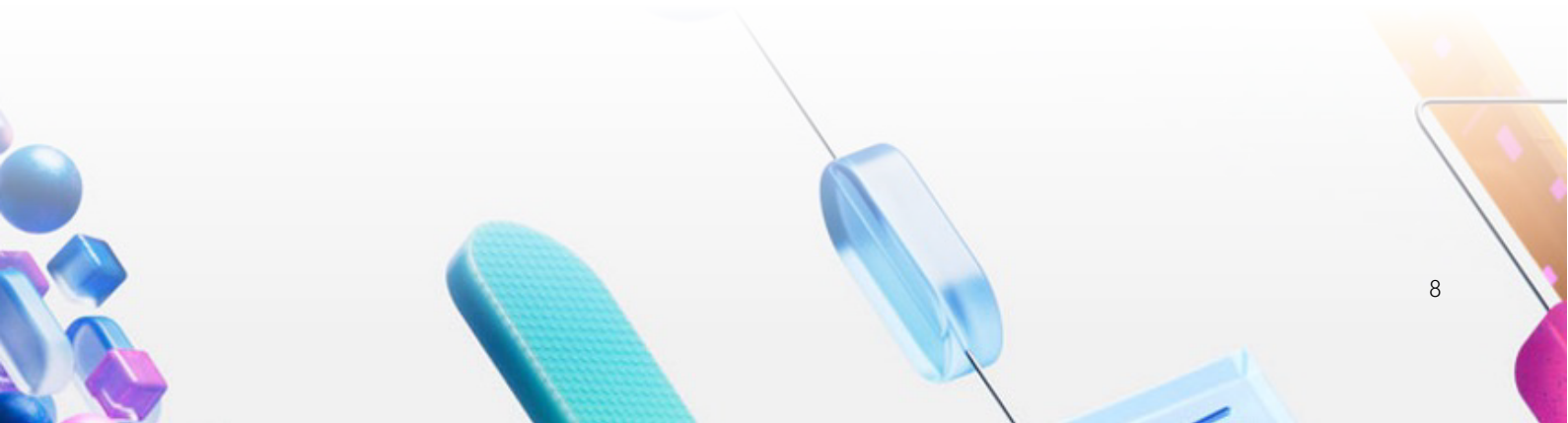
Pour les clients dont les charges de travail ont des besoins spécialisés, le cloud privé souverain prend en charge des services critiques de collaboration, de communication et de virtualisation sur Azure Local (comme Exchange, SharePoint et Skype Entreprise), ainsi que des services Azure tels que les machines virtuelles, les services de données, la sécurité, le développement d'applications et l'IA, dans des opérations connectées ou déconnectées. S'appuyant sur les décennies d'expérience de Microsoft dans la fourniture de technologies sur site et hybrides aux gouvernements et aux secteurs réglementés, les opérations déconnectées fournissent un plan de contrôle entièrement local qui permet aux organisations de fonctionner en toute sécurité et de manière indépendante dans leurs propres environnements dédiés. Tout en garantissant la résidence des données, la conformité réglementaire et des performances à faible latence, Azure Local et Microsoft 365 Local proposent des capacités avancées dans des environnements hybrides ou déconnectés pour répondre aux exigences de résilience des clients et de continuité de service, y compris dans des situations hautement réglementées ou en périphérie.

Environnements hybrides

Le cloud privé souverain prend en charge les environnements hybrides qui permettent aux organisations d'étendre les services de cloud computing Microsoft dans une infrastructure contrôlée par le client, tout en maintenant des capacités de gestion, de sécurité et de conformité cohérentes. Grâce à Azure Local et Microsoft 365 Local activés par Azure Arc, les clients peuvent exploiter des charges de travail dans des environnements sur site et connectés au cloud avec un plan de contrôle unifié, permettant la résidence des données, le traitement à faible latence et l'autonomie opérationnelle si nécessaire. Ce modèle hybride est parfaitement adapté aux secteurs réglementés et aux organismes publics qui doivent concilier innovation et évolutivité avec un contrôle localisé et une conformité réglementaire.

Environnements déconnectés

Pour les scénarios où la connectivité au cloud public est limitée ou non autorisée, le cloud privé souverain prend en charge les opérations entièrement déconnectées. Dans ces environnements, les clients peuvent exécuter des services cloud avec un plan de contrôle entièrement local, permettant aux systèmes de fonctionner de manière sécurisée et indépendante sans dépendre d'un accès réseau externe. Les déploiements déconnectés sont conçus pour prendre en charge les charges de travail stratégiques, les scénarios en périphérie et les environnements sensibles où les exigences réglementaires, de sécurité ou de résilience nécessitent un isolement, tout en continuant à bénéficier d'une infrastructure, de mises à jour et de processus de gestion du cycle de vie validés par Microsoft.



Feuille de route du cloud privé

- **Les contrôles des modifications renforcés (capacité future)**
  introduiront des politiques configurables et des workflows d'approbation afin de donner aux organisations une supervision explicite des mises à jour et des modifications de configuration à mesure qu'elles se propagent des environnements connectés au cloud vers l'infrastructure contrôlée par le client, renforçant ainsi la gouvernance et la conformité.

- **La récupération d'urgence de site à site (fonctionnalité future)**
  sera une extension des fonctionnalités d'Azure Site Recovery pour Azure Local afin de prendre en charge la continuité de service en garantissant la disponibilité des applications et des charges de travail lors de défaillances d'infrastructure ou de pannes localisées.

- **La migration d'un environnement hybride à entièrement déconnecté (fonctionnalité future)**
  continuera de soutenir des modèles de déploiement flexibles permettant aux clients de migrer leurs charges de travail d'environnements hybrides vers des opérations totalement déconnectées, offrant ainsi une plus grande autonomie et une résilience accrue à mesure que les exigences opérationnelles ou réglementaires évoluent.

- **Les déploiements à grande échelle (version préliminaire)**
  étendront les capacités d'évolutivité pour prendre en charge des infrastructures de grande taille. Cela signifie que les clients pourront étendre leurs déploiements, passant du nœud unique et du cluster à des environnements multi-racks.

Clouds nationaux partenaires

En France et en Allemagne, nos clouds partenaires nationaux offrent des instances complètes et exploitées de manière indépendante de Microsoft 365 et Microsoft Azure, entièrement sous propriété et contrôle nationaux.

- En France, Bleu, une coentreprise entre Orange et Capgemini, exploite un « cloud de confiance » destiné au secteur public français et aux fournisseurs d'infrastructures critiques. Ce cloud a été conçu pour répondre aux exigences SecNumCloud du gouvernement français (ANSSI).
- En Allemagne, Delos Cloud, filiale de SAP, exploite un cloud souverain destiné au secteur public allemand et conçu pour répondre aux exigences de la plateforme cloud BSI fixées par le gouvernement allemand.

La plupart des organisations utiliseront une combinaison de ces modèles de déploiement, car toutes les charges de travail ne nécessitent pas le même niveau d'indépendance ou d'isolation. Le Microsoft Sovereign Cloud permet aux clients de mettre en place les contrôles nécessaires dès le départ, afin qu'ils soient prêts à opérer conformément aux exigences choisies à tout moment.

Opérations européennes de Microsoft

L'approche de Microsoft en matière de souveraineté en Europe repose sur une gouvernance de droit européen, une responsabilité juridique claire et des contrôles opérationnels transparents. Au lieu de créer une entité juridique isolée pour les charges de travail souveraines, Microsoft assure la souveraineté au moyen d'entités européennes établies, de modèles de gouvernance renforcés et de garanties techniques et contractuelles contraignantes.

Structure des entités

Microsoft fournit des services cloud en Europe par l'intermédiaire d'entités juridiques Microsoft établies et opérant au sein de l'Union européenne (UE), sous réserve du droit européen et conformément aux exigences réglementaires spécifiques à chaque région. Ces entités sont responsables de l'exploitation de l'infrastructure cloud européenne et des services associés, et concluent directement des contrats avec les clients européens. Nos opérations de datacenter européennes sont gouvernées par un conseil d'administration européen qui fonctionne conformément au droit européen, renforçant notre engagement envers la supervision locale. Cette structure assure la continuité de la responsabilité juridique tout en préservant une plateforme cloud cohérente et un portefeuille de services dans les différentes régions.

Pour les charges de travail nécessitant une indépendance juridique accrue ou un alignement sur les régimes de souveraineté nationaux, Microsoft soutient également les clouds partenaires nationaux, tels que ceux se trouvant en France et en Allemagne. Ces environnements sont détenus et exploités indépendamment par des entités locales, soumises à la gouvernance d'entreprise locale, à la législation nationale et à la surveillance réglementaire, tout en fournissant la technologie Microsoft sous des contrôles contractuels et opérationnels stricts. Ce modèle permet aux clients de répondre aux exigences nationales sans fragmenter leur architecture cloud plus large.

Gouvernance d'entreprise et contrôles d'accès

Microsoft fait appliquer les objectifs de souveraineté au moyen d'un modèle de gouvernance de défense en profondeur combinant des contrôles techniques, une supervision opérationnelle et des engagements juridiquement contraignants. Cette approche est conçue pour réduire la dépendance à l'égard de la confiance de l'opérateur et donner aux clients un contrôle vérifiable sur l'accès à leurs données.

Au niveau de l'infrastructure, Microsoft protège les données même lorsqu'elles sont en cours de traitement, ce qui permet de garantir que les opérateurs de cloud n'ont pas accès aux informations sensibles, sauf autorisation explicite. Ces protections sont conçues pour garantir l'isolation et la protection des données des clients tout au long de leur cycle de vie, complétant le chiffrement lorsque les données sont stockées ou transmises et réduisant l'exposition aux accès non autorisés, même dans des scénarios opérationnels hautement privilégiés.

Microsoft limite davantage l'accès par chiffrement contrôlé par le client. Avec des options telles que Customer-Managed Keys et External Key Management, les clients conservent l'autorité sur les clés qui protègent leurs données. Sans ces clés, Microsoft ne peut pas lire ni utiliser le contenu client de manière indépendante, ce qui permet de veiller à ce que les décisions d'accès restent sous le contrôle du client.

Dans les situations où un accès opérationnel limité est nécessaire afin de garantir la fiabilité du service, Microsoft applique des contrôles stricts et auditables. Customer Lockbox exige l'approbation explicite du client avant que le personnel de Microsoft ne puisse accéder au contenu du client lors des incidents de support. Pour les opérations souveraines européennes, Data Guardian ajoute l'autorisation et la supervision du personnel européen, toutes les actions étant enregistrées dans des journaux infalsifiables. Ensemble, ces mesures peuvent garantir que tout accès privilégié est délibéré, transparent et entièrement traçable.

Engagements juridiques et contractuels pour les demandes d'accès

Microsoft ne donne à aucun gouvernement un accès direct ou libre aux données client et gère les demandes d'accès en provenance de l'État ou des forces de l'ordre via des processus juridiques et opérationnels définis, conçus pour garantir l'alignement sur le droit européen et les intérêts des clients. Pour les services cloud européens, Microsoft opère dans le cadre juridique européen et toutes les demandes relatives aux données client sont examinées individuellement par des équipes juridiques, de confidentialité et de conformité disposant d'une expertise régionale. Les demandes sont évaluées en fonction de la compétence, de la légalité et de la portée avant que toute mesure ne soit prise, et celles qui ne répondent pas aux normes juridiques applicables sont contestées ou rejetées.

Conformément à une démarche centrée sur le client, les engagements contractuels et de confidentialité de Microsoft sont conçus pour maximiser le contrôle et la transparence au bénéfice du client. Lorsque la loi l'autorise, Microsoft redirige les demandes vers les clients afin qu'ils puissent y répondre directement ou solliciter un recours judiciaire. Lorsque la notification est autorisée, Microsoft en informe rapidement les clients et fournit suffisamment de détails pour permettre une action appropriée. Si la notification est soumise à des restrictions légales, Microsoft cherche à lever ou à réduire la portée de ces restrictions. Microsoft s'est également engagée publiquement à contester en justice les demandes manifestement invalides ou contraires au droit, y compris les exigences extraterritoriales incompatibles avec les normes juridiques européennes, comme en témoignent ses engagements numériques européens et sa promesse de résilience numérique. Microsoft conteste depuis longtemps avec succès des ordonnances de secret inutiles, à la fois directement dans ses communications avec les forces de l'ordre et officiellement devant les tribunaux.

Ces engagements légaux sont renforcés par les contrôles techniques et contractuels décrits ci-dessus, qui limitent l'accès des opérateurs et réduisent l'exposition aux divulgations non autorisées. Ensemble, la responsabilité juridique régionale, les droits des clients exécutoires et les contrôles vérifiables donnent aux clients l'assurance que les demandes d'accès sont traitées de manière cohérente, transparente et conformément aux exigences légales européennes.

Sous-traitants et transparence

Microsoft garantit la transparence concernant l'utilisation des sous-traitants et applique des garanties contractuelles, techniques et organisationnelles conformes aux exigences de protection et de sécurité des données de l'UE. Les sous-traitants sont soumis à une diligence raisonnable, à des obligations contractuelles et à une surveillance continue afin de répondre aux normes de Microsoft en matière de sécurité, de confidentialité et de conformité.

Les fonctionnalités complètes de journalisation et d'audit à travers les services de cloud computing Microsoft permettent aux clients de surveiller les actions administratives, les tentatives d'accès et les opérations sur les données. Les enregistrements d'audit sont protégés contre toute modification non autorisée et soutiennent à la fois la gouvernance interne et l'examen réglementaire externe. Ces protections techniques sont renforcées par des engagements contractuels exigeant la journalisation, la justification de l'accès et la notification aux clients, garantissant que la transparence et la responsabilité sont à la fois exécutoires et observables.

Ensemble, la structure des entités, le modèle de gouvernance et les contrôles des sous-traitants de Microsoft donnent aux clients l'assurance que les services cloud en Europe fonctionnent sous une responsabilité juridique claire, une surveillance opérationnelle disciplinée et des contrôles d'accès transparents alignés sur les attentes en matière de souveraineté européenne.

Mettre en pratique la souveraineté numérique

Les organisations européennes traversent une période de profonds changements. Les technologies du cloud et de l'IA redéfinissent la manière dont les services publics sont fournis, la compétitivité des secteurs industriels et le fonctionnement des systèmes critiques, tandis que les attentes réglementaires, les menaces qui pèsent contre la sécurité et l'incertitude géopolitique continuent de s'intensifier. Relever ces défis exige plus que la conformité aux normes actuelles, cela nécessite une plateforme cloud conçue pour évoluer en fonction des exigences.

Le Microsoft Sovereign Cloud est conçu pour aider les organisations à franchir l'étape suivante en toute confiance. Au lieu d'exiger un cloud distinct ou isolé, Microsoft permet aux clients d'appliquer des contrôles souverains sur l'ensemble de la Microsoft Stack, sans pour autant sacrifier l'innovation, l'échelle ou les fonctionnalités.

Les organisations peuvent notamment commencer leur parcours de souveraineté numérique dans le cloud public au moyen d'une zone d'atterrissage souveraine (SLZ). Les organisations peuvent commencer par évaluer les exigences de souveraineté par charge de travail et établir une zone d'atterrissage souveraine comme base pour une adoption sécurisée et conforme du cloud et de l'IA. En adoptant la zone d'atterrissage souveraine, les clients peuvent bénéficier d'une architecture pratique qui accélère l'alignement sur les exigences de souveraineté régionale tout en prenant en charge l'évolutivité dans l'ensemble des régions Azure. Au fil du temps, les politiques et contrôles souverains intégrés continueront de s'étendre, aidant les organisations à atteindre des résultats souverains prêts à l'emploi plus rapidement et avec une confiance accrue.

L'engagement de Microsoft est à long terme. Grâce à des investissements continus, une gouvernance transparente et des garanties juridiquement exécutoires, notre objectif est d'être un partenaire stable et fiable pour les gouvernements, les entreprises et les institutions essentielles de l'Europe. Le Microsoft Sovereign Cloud fournit une base pour adopter les technologies de cloud et d'IA en toute confiance, tout en soutenant l'innovation, la résilience et le contrôle dans un environnement numérique de plus en plus complexe.

Microsoft

microsoft.com/sovereignty

Les informations présentées dans ce document représentent les opinions actuelles de Microsoft Corporation sur les sujets évoqués à la date de cette publication. Étant donné que Microsoft doit répondre aux conditions variables du marché, elles ne doivent pas être interprétées comme un engagement de la part de Microsoft, et Microsoft ne peut garantir l'exactitude de toutes les informations présentées après la date de cette publication.

Le présent livre blanc est fourni à titre informatif uniquement. Microsoft n'accorde aucune garantie expresse ou implicite quant aux informations présentées dans ce document.