



Consultation publique de l'Arcep

17 juin 2025 au 18 juillet 2025

Projet de recommandation relative à l'interopérabilité et à la portabilité des services d'informatique en nuage (*cloud*)

Réponse d'Orange

Contact : affaires.reglementaires@orange.com

Lien vers les documents en consultation :

[Projet de recommandation relative à l'interopérabilité et à la portabilité des services d'informatique en nuage \(cloud\) - CONSULTATION PUBLIQUE - Du 17 juin 2025 au 18 juillet 2025](#)

Synthèse générale

La consultation publique de juin 2025 sur l'interopérabilité et la portabilité des services d'informatique en nuage s'inscrit dans le prolongement des travaux de l'Arcep pour mettre en œuvre la loi SREN et le Data Act européen.

Notre contribution s'articule autour de deux axes principaux : le renforcement de la transparence sur le degré de portabilité et d'interopérabilité des services *cloud*, et la mise à disposition d'API stables et documentées. Ces deux dimensions sont essentielles pour permettre aux entreprises de faire des choix éclairés et de mettre en œuvre des stratégies *multi-cloud* efficaces.

Concernant la transparence, nous soutenons la proposition de l'Arcep visant à standardiser les informations mises à disposition des utilisateurs. La liste des informations proposée constitue une base solide, couvrant les aspects essentiels de la portabilité et de l'interopérabilité. Nous suggérons toutefois de l'enrichir pour mieux refléter la complexité des architectures *cloud* actuelles, notamment en détaillant davantage les interdépendances entre services et les impacts potentiels lors des migrations. Cette approche permettrait aux entreprises d'évaluer plus précisément les implications techniques et économiques de leurs choix.

Sur la question des API, nous appuyons l'adoption de la spécification OpenAPI comme standard, tout en recommandant de compléter cette approche par la fourniture de providers Terraform, outil de référence pour l'Infrastructure-as-Code. Le délai proposé de préavis de douze mois pour les modifications « non-rétrocompatibles » nous paraît approprié pour permettre aux entreprises d'adapter leurs systèmes, tout en prévoyant un cadre d'exception pour les situations liées à la sécurité nécessitant des interventions plus rapides.

Notre vision repose sur un équilibre entre standardisation et innovation. Si la standardisation est nécessaire pour garantir l'interopérabilité et la portabilité, elle ne doit pas freiner la capacité des fournisseurs à développer des services différenciants. Cette approche pragmatique, tenant compte des réalités techniques et économiques du marché, nous semble la plus à même de favoriser l'émergence d'un écosystème *cloud* européen dynamique, sécurisé et interopérable.

Enfin, Orange souligne à nouveau l'importance d'une approche pragmatique dans la mise en œuvre des obligations réglementaires. Les futures lignes directrices de l'ARCEP devraient établir un cadre, qui facilite la portabilité et l'interopérabilité tout en tenant compte des contraintes techniques et en préservant la capacité d'innovation du marché.

*** **

Observations d'Orange sur le renforcement de la transparence sur le degré de portabilité et d'interopérabilité des services *cloud*

Question 1 : Les informations proposées couvrent-elles selon vous les besoins des clients pour comprendre les modalités de portabilité et d'interopérabilité d'un service *cloud* ? Sinon, comment cette liste devrait-elle être modifiée selon vous ?

La liste des informations proposée par l'Arcep représente une avancée significative vers une meilleure transparence du marché des services *cloud*. Cependant, notre expérience opérationnelle, notamment dans l'accompagnement des migrations complexes, démontre la nécessité d'enrichir cette documentation pour répondre aux enjeux réels des entreprises.

L'environnement *cloud* moderne se caractérise par une imbrication croissante des services et des architectures. Par exemple, une application critique typique peut combiner des services IaaS pour l'infrastructure de base, des services PaaS pour la gestion des données, et des services auxiliaires pour la sécurité et le monitoring. Cette complexité nécessite une documentation plus approfondie des interdépendances et des impacts potentiels lors des migrations.

Un défi majeur que nous identifions concerne les difficultés dans le cadre de migration simple de transfert de données sortant, particulièrement liées à la définition du périmètre. En effet, une migration peut impliquer plusieurs flux entrants et sortants successifs, rendant difficile l'identification précise des données concernées. Il est donc essentiel de clarifier l'information fournie aux clients sur ces flux multiples et d'établir des mécanismes permettant de distinguer clairement les flux de données liés à la migration des flux de données d'usage courant tel que l'accès à internet. Cette distinction est cruciale tant pour la planification de la migration que pour la tarification appropriée des transferts de données.

Les aspects de performance constituent un enjeu majeur insuffisamment couvert par la proposition actuelle. Notre expérience montre qu'une migration apparemment identique en termes de spécifications techniques peut conduire à des performances significativement différentes dans le nouvel environnement. Par exemple, une base de données relationnelle migrée vers un service équivalent peut nécessiter une optimisation importante pour maintenir les mêmes temps de réponse.

La sécurité et la conformité réglementaire représentent également des préoccupations majeures pour nos clients entreprise. La documentation doit détailler précisément les mécanismes de sécurité disponibles, les certifications applicables et les processus de maintien de la conformité pendant et après la migration.

Les aspects économiques, notamment la structure détaillée des coûts d'interconnexion et les frais associés aux différentes options de connectivité, doivent être explicitement documentés pour permettre une évaluation complète des projets de migration ou de déploiement *multi-cloud*.

Question 2. Avez-vous d'autres commentaires sur cette recommandation ?

La recommandation proposée par l'Arcep mérite d'être enrichie pour refléter plus fidèlement la réalité opérationnelle du marché du *cloud*. Notre expérience démontre que l'approche de la documentation doit être adaptée selon la nature des services concernés.

Pour les services IaaS, la standardisation est relativement mature et les processus de migration sont bien établis. En revanche, les services PaaS et SaaS présentent des spécificités qui nécessitent une documentation plus nuancée. Par exemple, la migration d'une base de données managée implique non



seulement le transfert des données mais aussi l'adaptation des paramètres de configuration et des processus de maintenance.

L'innovation constitue un moteur essentiel du marché du *cloud*. La standardisation de la documentation ne doit pas freiner la capacité des fournisseurs à développer des services différenciants. Notre expérience dans le développement de services *cloud* innovants montre qu'une documentation trop rigide peut constituer un frein à l'innovation.

Observations d'Orange sur le fait de favoriser la mise à disposition d'API stables et documentées

Question 2 : Le délai de préavis proposé vous semble-t-il approprié ? Dans le cas contraire, quel délai préconisez-vous ? Pourquoi ?

Le délai de préavis de 12 mois pour les modifications "non-rétrocompatibles" correspond à une réalité opérationnelle que nous observons quotidiennement dans la gestion des environnements *cloud* complexes. Notre expérience dans l'accompagnement des grandes entreprises démontre qu'un tel délai est nécessaire pour plusieurs raisons fondamentales.

Prenons l'exemple concret d'une migration majeure d'un système d'information bancaire : la planification débute généralement 6 à 8 mois avant l'opération, suivie d'une phase de tests et de validation de 3 à 4 mois, puis d'une période de stabilisation post-migration. Un délai de 12 mois permet d'intégrer sereinement ces différentes phases tout en maintenant la continuité des services critiques.

Cependant, nous constatons que certaines situations, notamment liées à la sécurité, peuvent nécessiter des modifications plus rapides. Par exemple, la correction d'une vulnérabilité critique ne peut pas toujours attendre 12 mois. Il est donc essentiel de prévoir un cadre d'exception clairement défini pour ces cas particuliers.

Notre expérience montre également que la notion de "non-rétrocompatibilité" mérite d'être précisée. Dans les architectures *cloud* modernes, une modification apparemment mineure d'une API peut avoir des répercussions en cascade sur de nombreux services interconnectés. La documentation devrait donc inclure une évaluation détaillée des impacts potentiels de chaque modification majeure.

Question 3 : L'adoption généralisée de la spécification OpenAPI vous semble-t-elle souhaitable, notamment afin de permettre une documentation des API harmonisée ?

La standardisation via OpenAPI constitue une approche pertinente et utile pour améliorer l'interopérabilité des services *cloud*. Notre expérience dans le développement et l'exploitation de services *cloud* démontre les avantages concrets d'une telle standardisation, notamment en termes de simplification des intégrations et de réduction des délais de mise en œuvre.

Dans notre pratique quotidienne, nous constatons que l'utilisation d'OpenAPI facilite significativement l'intégration de nouveaux services et la maintenance des interfaces existantes. Par exemple, lors de l'intégration de services de monitoring *multi-cloud*, la disponibilité d'une documentation standardisée permet de réduire de 30 à 40 % le temps de développement et d'intégration. Cela illustre l'impact positif d'une documentation harmonisée sur l'efficacité opérationnelle.

Cependant, il est important de souligner que l'adoption d'OpenAPI ne doit pas devenir un cadre rigide qui limiterait l'innovation. Dans des domaines tels que l'Intelligence Artificielle ou le Edge Computing, où les services évoluent rapidement, il est crucial de maintenir une certaine flexibilité dans la définition des interfaces. De plus, la spécification OpenAPI devrait intégrer des mécanismes permettant de répondre aux enjeux de sécurité spécifiques à certains secteurs, comme les services financiers ou les données de santé, tout en restant conforme aux standards.

Au-delà de l'adoption d'OpenAPI, nous souhaitons également mettre en avant l'importance de fournir des providers Terraform. Terraform est aujourd'hui l'outil de référence pour l'Infrastructure-as-Code (IaC), utilisé par la majorité des entreprises pour déployer et gérer leurs environnements *cloud*. La disponibilité de providers Terraform standardisés et bien documentés représenterait un bénéfice majeur pour les utilisateurs, en leur permettant de gérer leurs infrastructures de manière automatisée et cohérente, tout en réduisant les efforts de développement et de maintenance.

Nous soutenons donc une approche équilibrée et progressive de l'adoption d'OpenAPI, complétée par la fourniture de providers Terraform, afin de maximiser les bénéfices pour les utilisateurs tout en préservant la capacité d'innovation des fournisseurs de services *cloud*.

Cette approche devrait inclure :

1. la standardisation des interfaces fondamentales via OpenAPI pour garantir une interopérabilité de base entre les services.
2. la fourniture de providers Terraform pour répondre aux besoins opérationnels des utilisateurs en matière d'Infrastructure-as-Code.
3. l'intégration des exigences de sécurité spécifiques à chaque secteur, notamment pour les données sensibles.
4. la préservation de la performance des services, en veillant à ce que les standards adoptés n'introduisent pas de contraintes techniques inutiles.

En conclusion, cette approche combinée permettrait de tirer parti des avantages de la standardisation tout en répondant aux besoins opérationnels des utilisateurs et en soutenant la dynamique d'innovation du marché du *cloud*.

Question 4 : Avez-vous d'autres commentaires sur cette recommandation ?

Cette recommandation concernant les API pourrait prendre compte de la complexité des environnements *cloud* et des besoins spécifiques en matière de services complémentaires, qui ne sont pas standards même s'il existe des normes, particulièrement dans les domaines de la fédération des identités et de l'observabilité.

Par exemple, bien que des normes comme SAML existent pour le Single Sign-On, leur simple existence ne garantit pas une fédération d'identité effective entre différents environnements cloud ; de même, si OpenAPI offre un langage commun pour documenter les interfaces, ce qui est un prérequis, cela n'implique pas automatiquement que les API soient compatibles, ou que les applications fonctionnent ensemble, ce qui souligne la nécessité d'aller au-delà de la simple adoption de standards pour assurer une véritable interopérabilité fonctionnelle.

À titre d'exemple, l'API Factory au sein d'Orange Business vise à développer un référentiel commun pour l'ensemble des APIs proposées, une initiative déjà très ambitieuse à l'échelle d'un seul opérateur, ce qui illustre la complexité que représenterait une telle harmonisation à l'échelle du secteur tout entier. Dans cette optique, Orange propose d'ailleurs un catalogue d'API documentées avec l'ambition de le rendre accessible en open source à terme, démontrant ainsi notre engagement concret en faveur de l'interopérabilité.

Notre expérience opérationnelle démontre que la stabilité des API ne peut pas être traitée de manière uniforme pour tous les services. Un cas concret récent chez l'un de nos clients du secteur bancaire illustre cette problématique : une mise à jour mineure d'une API d'authentification a nécessité la révision de plus de 200 points d'intégration dans leur système d'information.

En matière d'observabilité, la documentation des API doit être particulièrement détaillée pour permettre une supervision efficace des environnements *multi-cloud*. Notre expérience montre que les entreprises utilisant plusieurs *clouds* ont besoin d'une vision unifiée de leurs métriques de performance et de leurs journaux d'événements.

Par exemple, un client du secteur e-commerce gérant des charges de travail réparties entre trois fournisseurs *cloud* différents a dû développer des adaptateurs spécifiques pour normaliser la collecte des métriques, faute de standardisation suffisante des API de monitoring.

Il nous semble donc important de développer afin de répondre plus efficacement aux enjeux de sécurité et de résilience des architectures *cloud* modernes, tout en facilitant l'adoption de pratiques *multi-cloud*:

1. Une attention particulière aux services additionnels critiques : La normalisation des API pour les services IAM et d'observabilité devrait être considérée comme prioritaire, car ces services sont essentiels pour la sécurité et la résilience des environnements *cloud*. Notre expérience montre qu'une standardisation dans ces domaines permettrait de réduire significativement les coûts d'intégration et de maintenance.
2. Une approche différenciée selon la criticité des services : Les exigences de stabilité et de documentation devraient être adaptées en fonction de l'impact potentiel des modifications. Par exemple, les changements affectant les services de sécurité devraient faire l'objet d'un processus de validation et de communication renforcé.
3. Un cadre de gouvernance des API : Au-delà de la documentation technique, nous recommandons la mise en place d'un cadre de gouvernance définissant clairement les processus de gestion du cycle de vie des API, incluant les procédures de test, de validation et de déploiement des modifications.

*** **

*** **