



**Consultation de l'Autorité de régulation des communications électroniques, des postes
et de la distribution de la presse (Arcep)**

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

1. Transparence sur le degré de portabilité et d'interopérabilité des services cloud

Première question : 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 ?

Hexatrust, association des acteurs de la confiance cloud et cybersécurité en France, salue l'initiative de l'Arcep de porter à consultation son projet de recommandation relative à l'interopérabilité et à la portabilité des services d'informatique en nuage, qui intervient à un moment charnière pour la filière avec l'entrée en vigueur prochaine du Data Act. Nous nous inscrivons pleinement dans la démarche de l'Arcep, qui traduit la volonté du législateur posée dans la loi SREN, de renforcer l'interopérabilité et la portabilité dans le cloud, sous réserve toutefois d'une approche pragmatique et proportionnée.

Avant d'analyser la liste proposée, il convient de distinguer plusieurs niveaux de complexité dans l'interopérabilité et la portabilité qu'il paraît nécessaire d'explicitier.

Tout d'abord, l'interopérabilité totale entre services cloud reste aujourd'hui globalement difficile, du fait de l'hétérogénéité des structures, API, et autres services. De ce fait, l'exercice de transparence doit avoir pour objectif d'indiquer clairement pour l'utilisateur ce qui est effectivement possible, et ce qui ne l'est pas, afin de permettre à l'utilisateur de faire un choix éclairé lors de la sélection d'un fournisseur de services cloud.

La clarification du processus d'interopérabilité, et notamment la description de ses limites, est à ce titre essentielle. Par exemple, la portabilité de microservices ou d'applications complexes implique quasi systématiquement des étapes de migration ou d'adaptation, qui ne peuvent pas être totalement automatisées ni garanties par le seul fournisseur.

Toutefois, un tel niveau de détail pourrait transformer ces lignes directrices en une structure excessivement complexe à mettre en œuvre, d'autant que les modalités d'une migration dépendent non seulement du fournisseur de cloud d'origine, mais aussi de celui de destination, ainsi que des besoins et préférences de migration exprimées par le client concerné (ex : garanties de sécurité d'une migration, garanties de continuité pendant la migration).



Par ailleurs, nous pensons qu'il serait inadapté de faire porter aux fournisseurs d'origine de cloud seuls la responsabilité de toutes les difficultés liées à la migration. En effet, le fournisseur de cloud est uniquement tenu de garantir à son client la possibilité de récupérer ses actifs tels quels en amont d'une migration et de résilier les services associés. Il doit à ce titre être tenu de documenter la demi-interface mise à disposition du client. La gestion des données pendant et après la migration relève quant à elle de la responsabilité du client. Il incombe donc à ce dernier de mettre en place, chez son fournisseur d'origine, les procédures nécessaires à une préparation adéquate de sa migration. C'est également au client de définir les modalités selon lesquelles il souhaite mener cette opération et les mesures qu'il entend mettre en œuvre à cet effet.

Enfin, il nous semble nécessaire de noter que la migration d'une infrastructure cloud est un chantier qui se complexifie avec le nombre et le volume de services consommés, mais dépend aussi d'une multitude d'autres facteurs tels que la bande passante ou encore le niveau d'intégration. La portabilité ne peut alors se résumer à l'existence d'une API compatible : c'est un projet qui se planifie, s'évalue, se cadre, se pilote, et s'étale sur des mois/années, principalement au gré des accords contractuels pré-existants. Il existe une multitude de manières de réaliser une migration, qui complexifient donc la documentation des données relatives (ex : procédures pour initier une migration, méthodes de migration). Comme précisé ci-dessus, il revient ainsi au client lui-même de s'assurer de la bonne préparation de sa migration selon les conditions qu'il envisage.

Concernant, la liste de 14 informations proposée pour améliorer la transparence sur le degré de portabilité et d'interopérabilité des services cloud, nous recommandons de ne pas aller au-delà du code SWIPO. La transparence doit avant tout signifier d'indiquer clairement ce qui est faisable et ce qui ne l'est pas en matière de portabilité et d'interopérabilité, plutôt que de prétendre à une exhaustivité technique parfois irréalisable ou incompréhensible pour l'utilisateur final. De plus, il est crucial de considérer la propriété intellectuelle des fournisseurs. Les informations à publier ne devraient pas porter atteinte aux actifs stratégiques des entreprises, un point de vigilance déjà identifié lors des discussions sur la transposition du Data Act.



2. Favoriser la mise à disposition d'API stables et documentées

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

Un délai de 12 mois de préavis avant toute évolution importante non rétrocompatible des API nous paraît être un équilibre satisfaisant : il offre aux utilisateurs le temps nécessaire pour tester, adapter et déployer les nouvelles versions sans rupture de service, tout en laissant aux fournisseurs la marge de manœuvre pour planifier leurs évolutions.

Toutefois, en cas de mise à jour urgente motivée par une vulnérabilité critique ou un impératif de performance, le fournisseur doit maintenir l'ancienne version de l'API en mode "déprécié" pendant au moins 12 mois supplémentaires, informer les clients des risques encourus et préciser, le cas échéant, la date de fin de vie de la version dépréciée. Cette modalité garantit à la fois la sécurité des environnements et la continuité opérationnelle des services.

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

La recommandation de l'Arcep d'exiger un méta-modèle de documentation d'API lisible par machine et harmonisé nous paraît parfaitement justifiée, puisqu'elle répond au besoin de transparence et de compréhensibilité pour les utilisateurs. Nos membres utilisent déjà des méta-modèles largement éprouvés, tels qu'OpenAPI, pour décrire et documenter toutes les interfaces, ce qui garantit cohérence, automatisation des tests et intégration fluide dans la chaîne DevOps, OpenAPI étant reconnu à ce jour pour sa capacité à structurer la documentation des interfaces et à faciliter la compréhension technique.

Nous recommandons cependant de ne pas nommer un standard unique dans le texte de la recommandation. L'exigence doit porter sur la publication d'un méta-modèle ouvert et versionné, sans verrouillage sur un format particulier, afin de laisser les fournisseurs libres d'adopter la solution la plus adaptée à leurs architectures et à l'évolution des pratiques industrielles. Plusieurs acteurs, notamment en Europe, pourraient s'appuyer sur d'autres spécifications et il serait risqué d'isoler les fournisseurs français si le Data Act ou d'autres textes européens venaient à privilégier une alternative.

→ En somme, l'Arcep pourrait formuler l'exigence en ces termes : *'Les fournisseurs publient une documentation d'API publique, versionnée et lisible par machine selon un méta-modèle ouvert, type OpenAPI ou spécifications équivalentes'*. Cette approche



combinera interopérabilité immédiate et agilité pour intégrer de nouveaux formats à l'avenir.

Cinquième question : Avez-vous d'autres commentaires sur cette recommandation ?

La transparence sur le degré de portabilité et d'interopérabilité des services cloud est essentielle pour renforcer la confiance des utilisateurs européens.

Afin d'évaluer clairement ce degré de documentation des APIs, il serait intéressant de prendre en compte, en plus d'une documentation standardisée et de la clarté sur les limitations techniques, un critère d'indicateurs de performance des APIs associés à la documentation, pour évaluer le taux d'appels d'API réussis. Des indicateurs clairs permettraient non seulement d'évaluer la performance des APIs, mais aussi de suivre leur évolution dans le temps.

Par ailleurs, au-delà d'une harmonisation de la documentation des API, une plus grande standardisation des services cloud semble pertinente pour lever les freins à l'interopérabilité et à la portabilité. C'est pourquoi les travaux engagés par l'Arcep doivent venir nourrir les discussions engagées à l'échelle européenne dans le cadre de l'application du Data Act, y compris concernant les enjeux de normalisation.

Hexatrust salue le projet de recommandation de l'Arcep tout en recommandant une approche proportionnée et alignée sur le Data Act, en veillant notamment à ne pas créer de surcouche qui pourrait s'avérer contre-productive. L'objectif doit rester le renfort de l'interopérabilité et la portabilité au bénéfice des utilisateurs, en s'assurant de la préservation de la compétitivité des acteurs français et européens du cloud.