

**Consultation publique de l'ARCEP sur le Projet de Recommandation
relative à l'interopérabilité et à la portabilité des services d'informatique
en nuage (cloud)
Juillet 2025**

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 ?

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

Question 1 :

Avant tout, IBM recommande de se référer autant que possible aux normes internationales et européennes en matière d'interopérabilité et de portabilité. ISO, CEN-CENELEC JTC 25 et ETSI sont des processus de normalisation ouverts qui reposent sur une large participation de tous les acteurs pertinents. Les codes CISPE ou SWIPO sont issus de travaux n'ayant bénéficié que d'un soutien partiel du secteur.

Compte tenu de l'état actuel des normes en matière d'interopérabilité et de portabilité dans le Cloud, IBM recommande à l'ARCEP de s'appuyer autant que possible sur la norme "ISO/IEC 19941:2017 Technologies de l'information - Informatique en nuage - Interopérabilité et portabilité" (actuellement en cours de révision) pour l'élaboration de ces lignes directrices. Les sections 5 et 10 de la norme ISO/IEC 19941 en particulier contiennent des dispositions utiles pour permettre aux clients de mieux comprendre les caractéristiques d'interopérabilité et de portabilité des services Cloud.

À l'avenir, il sera également pertinent, le cas échéant, de prendre en compte les normes européennes susceptibles d'être développées dans le cadre du CEN-CENELEC JTC 25 et de l'ETSI.

Cela étant, compte tenu du fait que l'ARCEP sollicite un avis sur les 14 points issus des codes de conduite SWIPO, veuillez trouver ci-dessous nos observations pour chacun d'eux :

1. Données (brutes ou dérivées) et actifs numériques qui peuvent être transférés dans le cadre d'une migration ou d'une utilisation simultanée des services de différents fournisseurs ;

Ces informations doivent être documentées dans le processus de migration propre à chaque produit ou service (voir point 2). Par exemple, la documentation relative à la migration d'une base de données explique comment extraire les données et sous quel format elles seront obtenues. Ces informations sont fournies sans garantie que les formats seront compatibles avec des services équivalents proposés par un autre fournisseur de Cloud.

Dit autrement, les Cloud providers sont en mesure d'expliquer comment extraire les données de leurs services et sous quel format elles seront disponibles, mais ne peuvent garantir que ces formats fonctionneront comme attendu sur les services d'un autre fournisseur Cloud. Compte-tenu de la diversité des services et des fournisseurs vers lesquels les données pourraient être transférées, tester la compatibilité des formats de données avec l'ensemble des fournisseurs et services de Cloud serait excessivement complexe.

Notre politique est que le client est propriétaire de ses données et n'est pas empêché de les transférer hors du Cloud en raison d'une obligation contractuelle ou de licence avec IBM. Il peut arriver que les éditeurs de logiciels tiers opérant sur le Cloud aient leurs propres accords de licence avec les clients, qui peuvent restreindre ou interdire un tel transfert de données, ce que le fournisseur Cloud ne peut pas contrôler.

2. Procédures pour initier une migration depuis le service cloud ;

Il est possible pour le fournisseur d'inclure, dans la documentation officielle du produit, des informations indiquant les procédures à suivre pour initier des options de migration dans le cadre de scénarios de migration courants. Cependant, les fournisseurs ne devraient pas avoir à fournir de plan de migration personnalisé, la stratégie de migration restant de la responsabilité du client ou d'un partenaire de migration.

Ces informations sont fournies en l'état et n'altèrent en rien le modèle de responsabilité partagée.

3. Procédures pour initier une migration vers le service cloud ;

La réponse est la même qu'au point n°2.

4. Méthodes (téléversement, API, expédition de disques) disponibles pour la migration et l'utilisation simultanée des services de différents fournisseurs, y compris les protections disponibles (chiffrement) et les restrictions et limitations techniques connues ;

La plupart des méthodes de migration reposent sur des outils. Le fournisseur Cloud peut, dans certains cas, suggérer un outil utile pour un scénario de migration, en se basant sur les tendances générales observées dans le secteur. Il s'agit souvent d'outils open source ou de produits tiers.

Ces suggestions peuvent être utiles, mais les fournisseurs Cloud ne contrôlent généralement pas les feuilles de route de ces outils et ne peuvent garantir ni leur disponibilité continue, ni l'exactitude des informations contenues dans leur documentation, notamment en ce qui concerne les fonctionnalités, les protections, les limitations ou les restrictions. Ces informations relèvent de la responsabilité du tiers concerné. Les clients doivent donc se référer à la documentation propre à chaque outil, l'examiner attentivement et choisir la méthode ou l'outil le plus adapté à leurs besoins.

Compte tenu de l'émergence de technologies comme l'informatique quantique, qui posent des défis importants aux technologies de chiffrement actuelles, il est également important que chaque client adopte une approche personnalisée, adaptée à ses objectifs métier et à son appétence au risque.

5. Méthodes de migration recommandées en fonction du volume de données à transférer ;

La principale distinction entre les méthodes de migration de données en fonction du volume de données à transférer a toujours été le choix entre une migration en ligne et une migration physique (utilisant des disques ou bandes magnétiques transportés physiquement entre sites), cette dernière étant parfois privilégiée pour les volumes de données très importants.

Étant donné que les frais de sortie de données Cloud dans le cadre d'un changement de fournisseur (*switching*) sont encadrés - et bientôt supprimés - dans l'UE en vertu du Data Act, la méthode de migration en ligne devrait devenir l'option de sortie par défaut, quel que soit le volume de données. Les fournisseurs devraient publier des instructions claires pour guider les clients européens sur la

procédure à suivre afin d'initier cette migration de données (*switching, extraction*) sans encourir de frais.

Certains fournisseurs continueront à proposer d'autres méthodes de migration, optimisées pour des volumes de données très élevés, comme le transfert physique, mais ces méthodes restent spécifiques à leur organisation, à leurs capacités logistiques, à leur profil client et à la demande. Ces capacités ne sont rentables que dans des cas exceptionnels et ne peuvent pas être reproduites facilement par tous les fournisseurs sans investissements préalables considérables.

D'autres aspects influencent également le choix de la méthode de migration en lien avec les volumes de données (par exemple : réplication, sauvegarde/restauration, etc.). Ces choix dépendent toujours de la situation spécifique du client (format des données, fréquence d'accès, comportement et fonctionnalités des services source et destination, etc.). Des recommandations générales sur ces sujets seraient d'une utilité limitée pour les clients.

Les fournisseurs peuvent donc partager des méthodes de migration recommandées en fonction du volume de données, mais il convient de noter que cela se limite souvent à une seule méthode (c'est à dire la migration en ligne), car, comme expliqué ci-dessus, tous les fournisseurs ne proposent pas de migration physique, et il est peu pertinent pour le client de recevoir des recommandations générales sur d'autres aspects (format des données, service source, etc.).

6. Méthodes pour garantir la sécurité des données lors du transfert (contrôle d'accès, authentification des utilisateurs, confidentialité et intégrité) ;

Ces informations dépendent de la méthode de migration et de l'outil choisi par le client. Le client devrait se référer à la documentation du fournisseur tiers pour connaître les fonctionnalités disponibles et la manière de les utiliser.

7. Procédures pour tester les différents mécanismes de migration, notamment ceux de sauvegarde (snapshot), de restauration (rollback) et de vérification de l'intégrité des données ;

Tous les fournisseurs Cloud doivent fournir une documentation sur la création de sauvegardes, ainsi que sur les procédures de restauration (rollback), et sur d'autres méthodes de migration telles que la réplication. Ces procédures sont essentielles pour permettre au client de garantir la sécurité et la résilience de ses données au quotidien.

Cependant, cette documentation ne couvre pas nécessairement en détail l'utilisation de la méthode de sauvegarde/restauration dans le cadre d'une migration, ni la manière de tester les sauvegardes dans le contexte d'un transfert de données vers un autre service ou fournisseur Cloud. Pour pouvoir proposer des procédures fiables pour de tels tests, il est nécessaire de connaître à l'avance le service de destination ainsi que ses limitations ou contraintes techniques. Exiger cela de tous les fournisseurs Cloud serait lourd pour les fournisseurs et disproportionné par rapport à l'objectif du régulateur.

Il revient donc au client de tester ces méthodes, y compris de commander et de mettre en place les moyens nécessaires à ces tests, comme une plateforme de préproduction ou un banc d'essai. Le client reste responsable de la mise en œuvre de la méthode choisie, ce qui inclut la protection et la vérification de ses sauvegardes, ainsi que la vérification de l'intégrité des données.

8. Processus disponibles pour garantir l'intégrité des données, la continuité de service et prévenir la perte de données pendant la migration ;

Les fournisseurs Cloud peuvent fournir des recommandations générales sur les bonnes pratiques en la matière, mais les procédures spécifiques varient selon chaque scénario de migration, en fonction du choix de l'approche et des outils par le client.

En particulier, en raison de la complexité de certaines applications, il n'est pas possible de tester de manière fiable tous les scénarios de défaillance permettant de garantir la continuité de service après la migration. Les clients doivent se référer à la documentation des outils spécifiques qu'ils ont choisis.

9. Processus de résiliation d'un service cloud existant, lorsque le client souhaite mettre fin à son utilisation du service après la migration ;

Le processus de résiliation et les politiques de conservation des données doivent être clairement définis dans les contrats, les accords de licence et les conditions générales. Ces éléments peuvent varier en fonction de l'accord commercial spécifique entre le fournisseur et le client, ainsi que des politiques internes du fournisseur.

Bien qu'une partie de ces informations puisse être adaptée à chaque contrat et ne soit pas rendue publique, les conditions générales standard, y compris les politiques générales en matière de résiliation et de conservation des données, devraient être accessibles sur le site web public du fournisseur, afin de garantir transparence et accessibilité.

10. Outils de supervision disponibles pour la migration et coûts associés à leur usage ;

Certains fournisseurs Cloud disposent d'outils de migration natifs, tandis que d'autres n'en proposent pas.

Néanmoins, comme mentionné précédemment, la plupart des outils de migration sont open source et/ou développés par des tiers. Le fournisseur Cloud peut, dans certains cas, suggérer un outil utile pour un scénario de migration. Certains de ces outils peuvent inclure des fonctionnalités de supervision, et dans ce cas, ces fonctionnalités doivent être documentées par la partie qui développe, possède, gère ou commercialise l'outil.

Les fournisseurs Cloud mettent à disposition des moyens permettant à chaque client de suivre et d'estimer le coût de leur consommation des services Cloud au quotidien. La facturation peut être filtrée par étiquette (tag) ou par groupe de ressources. Il appartient au client d'exploiter ces fonctionnalités et de créer ces regroupements logiques de consommation s'il souhaite suivre les coûts liés à la migration.

11. Formats disponibles, recommandés ou utilisés dans le cadre d'une migration ou d'une utilisation simultanée des services de différents fournisseurs, ainsi que les spécifications et la documentation relatives à ces formats ;

Les fournisseurs Cloud ne peuvent pas fournir ces informations de manière exhaustive et systématique : les formats disponibles pour l'importation et l'exportation de données et d'actifs numériques dépendent du service concerné, du service de destination, ainsi que de l'outil de migration utilisé.

12. Référence de la documentation des API permettant la mise en œuvre de la portabilité et de l'interopérabilité ;

Oui, les fournisseurs Cloud documentent et doivent continuer à documenter l'ensemble de leurs API afin de permettre aux clients de déterminer par eux-mêmes comment adopter un service équivalent chez un autre fournisseur Cloud. Cependant, un fournisseur Cloud ne devrait pas être contraint de maintenir la liste actuelle des API pendant toute la durée du contrat, car cette liste (ainsi que les options de migration associées) est susceptible d'évoluer dans le temps.

13. Description et documentation des dépendances, dont les bibliothèques de code, les données connectées à d'autres services cloud du fournisseur, et les services et outils tiers nécessaires à l'export des données dans le cadre d'une migration ou d'une utilisation multi-cloud ;

Un fournisseur Cloud documente les dépendances de ses services afin d'aider les clients à comprendre leur posture de fiabilité (ces informations sont par exemple nécessaires pour répondre aux besoins de conformité des clients au règlement DORA). Ces dépendances sont propres à la manière dont chaque fournisseur Cloud délivre ses services. Cependant, chaque charge de travail (workload) des clients utilise des combinaisons différentes de services. Les dépendances entre la charge de travail et les services Cloud, ou entre les différentes charges de travail du client, ne sont connues que du client. Le modèle de responsabilité partagée décrit ce qui relève du fournisseur cloud et ce qui relève des clients.

14. Délais de migration et durée de transfert des données.

Les délais de migration sont propres à chaque scénario de migration et varient d'un client à l'autre. Elles dépendent de multiples variables, telles que la bande passante réseau utilisée par le client, la quantité de données à transférer, la distance entre la source et la destination de la migration, etc.

Des recommandations générales ne seraient pas utiles aux clients individuellement et pourraient même s'avérer trompeuses dans de nombreux cas.

Question 2 :

Depuis plusieurs décennies, IBM est un acteur de premier plan de la normalisation en France et en Europe. Grâce à l'expertise de ses laboratoires de R&D et de ses équipes techniques en France et dans toute l'Europe, IBM contribue à l'élaboration de normes de qualité, fondées sur le consensus, répondant aux besoins du marché ainsi qu'aux exigences réglementaires de l'Union européenne. Les standards ouverts sont au cœur de la stratégie d'IBM en matière de technologies ouvertes. Dans l'accompagnement de nos clients français dans leur transformation vers plus de compétitivité et résilience, nous sommes convaincus que des infrastructures ouvertes fondées sur des normes de haute qualité sont essentielles.

IBM est également un soutien actif du système réglementaire européen, régi par le Nouveau Cadre Législatif de l'UE (NLF). Nous reconnaissons la grande pertinence du NLF pour le bon fonctionnement du marché unique européen harmonisé. Le principe fondamental consistant à définir les objectifs via des exigences essentielles dans les actes juridiques, tout en déléguant l'élaboration des normes au secteur privé, constitue un atout majeur pour l'efficacité de la réglementation technique dans l'UE. En

confiant à des experts techniques de référence la définition des modalités techniques permettant de répondre aux exigences réglementaires, les normes européennes bénéficient d'une forte acceptation sur le marché, permettent une disponibilité rapide des innovations, et facilitent l'introduction de technologies sur le marché unique européen, en cohérence avec l'état de l'art technologique.

Dans ce contexte, IBM se félicite que le Data Act européen ainsi que les travaux de l'ARCEP s'inscrivent dans les principes du NLF, en faisant des normes une voie privilégiée pour démontrer la conformité. Avec les organismes européens de normalisation en première ligne, et en s'appuyant sur les bons exemples de partenariats public-privé, l'Union européenne est bien positionnée pour produire des normes de premier plan en soutien au Data Act.

Bien que cela puisse permettre un plus fort partage d'informations et un niveau de transparence accru, il convient de souligner que de nombreux aspects fondamentaux et concepts liés à la fourniture de services Cloud sont déjà documentés. Il existe de nombreuses normes internationales déjà publiées qui fournissent des briques de base, des détails et des lignes directrices à destination des fournisseurs de services Cloud, des utilisateurs, des clients et des partenaires. Ces standards décrivent également de manière claire les relations d'interopérabilité et de portabilité, sans oublier les capacités des plateformes, les catégories de services, les architectures, les approches de développement et les cycles de vie, notamment lorsqu'il s'agit de services de type IaaS, PaaS ou SaaS.

Dans la poursuite de ces travaux, les normes internationales déjà publiées et adoptées devraient être prises en compte comme références ou sources d'inspiration, car elles apportent des réponses et des orientations utiles aux sujets abordés. Parmi celles-ci :

- ISO/IEC 19941:2017 — Technologies de l'information - Informatique en nuage - Interopérabilité et portabilité (*évoquée ci-dessus, actuellement en cours de révision*)
- ISO/IEC 23751:2022 - Technologies de l'information - Informatique en nuage - Data Sharing Agreement (DSA) Framework
- ISO/IEC TR 3445 - Technologies de l'information - Informatique en nuage - Audit des services Cloud
- ISO/IEC 5140:2023 - Technologies de l'information - Informatique en nuage - Concepts pour le multi-nuage et l'utilisation des services en nuages multiples.
- ISO/IEC TR 23188 - Technologies de l'information - Informatique en nuage - Edge computing landscape
- ISO/IEC TS 7339:2025 - Technologies de l'information - Informatique en nuage - Vue d'ensemble des types de ressources et des services de plateformes à la demande

De manière générale, IBM souhaite exprimer son soutien au CEN-CENELEC JTC 25, et, le cas échéant, à l'ETSI, pour l'élaboration des normes européennes pertinentes là où des lacunes existent et en l'absence de normes internationales ou mondiales disponibles. Le CEN-CENELEC JTC 25 se distingue par une large participation de toutes les parties prenantes concernées. Le consensus et le soutien des parties prenantes sont essentiels pour le développement réussi et l'adoption des normes technologiques. Tandis que des cadres comme CISPE ou SWIPO ne bénéficient que d'un soutien partiel du marché et que ces initiatives comportent un risque de fragmenter ce dernier, la décision de la Commission européenne de confier les travaux de normalisation au CEN-CENELEC JTC 25 est bienvenue et mérite un soutien fort à l'échelle européenne. Les bonnes pratiques issues de la réglementation sur le hardware, avec les travaux menés au sein du CENELEC (en lien étroit avec l'IEC),

ainsi que celles issues des télécommunications, avec les travaux de l'ETSI, ont démontré le leadership que l'Europe peut exercer lorsqu'elle suit des processus de normalisation ouverts au service de la réglementation.

Alors qu'IBM soutient pleinement l'utilisation des normes mondiales existantes (spécifications techniques TIC venant d'organisations telles que OASIS, W3C, ou issues de développements open source), et estime qu'il convient d'éviter toute duplication inutile des travaux, l'échange avec les experts techniques du CEN-CENELEC JTC 25 permet de garantir que les normes sélectionnées sont adaptées à leur finalité et que les exigences essentielles définies dans la réglementation sont correctement prises en compte. **Le CEN-CENELEC JTC 25 devrait donc être le principal point de référence pour les travaux liés au Data Act, en tirant parti de l'expertise collective disponible au sein de ce comité.**

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

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

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

Question 2 :

Même si IBM confirme que le délai de préavis de douze mois proposé peut être approprié dans la majorité des cas, il est important que l'ARCEP mentionne que des délais plus courts peuvent être nécessaires dans certaines situations.

Les éléments suivants, précisés dans la description des services Cloud d'IBM, montrent que nous appliquons un préavis de 12 mois sauf si une action plus rapide est requise pour l'une des raisons suivantes :

Modifications des services Cloud : IBM fournira un préavis d'au moins 12 mois en cas d'abandon de fonctionnalités essentielles d'un service Cloud ou de modification d'une API de manière non rétrocompatible, sauf si IBM doit agir plus rapidement pour se conformer aux lois, obligations légales ou réglementations applicables, pour répondre à un problème de sécurité, ou pour éviter une charge économique excessive.

Retrait de services Cloud : Sauf nécessité d'agir plus rapidement pour se conformer aux lois, obligations légales ou réglementations applicables, répondre à un problème de sécurité ou pour éviter une charge économique excessive, IBM fournira un préavis d'au moins 12 mois avant le retrait d'un service, ou, pour certains services Cloud, un retrait pas avant les dates prolongées indiquées ici : https://cloud.ibm.com/docs/overview?topic=overview-services_availability

Cette politique est également alignée avec le cycle de vie de nos services, ainsi qu'avec celui de la plupart des projets open source ou des fournisseurs tiers que nous utilisons. Des événements géopolitiques peuvent conduire à réévaluer l'historique d'un fournisseur tiers et à réexaminer les risques de sécurité associés. Cela peut entraîner une interruption à court terme d'un service, et donc une modification majeure d'API. Il en va de même si un risque de sécurité est détecté sur un outil tiers sans plan de remédiation adéquat. Face à ces situations spécifiques, IBM recommande que le régulateur prévoie une liste de cas raisonnables dans lesquels il serait entendu que les fournisseurs Cloud devraient appliquer un délai de préavis plus court pour mettre en œuvre des mises à jour majeures.

Il est également important d'avoir à l'esprit les enjeux liés au contexte actuel de course à l'innovation, comme c'est actuellement le cas dans le domaine de l'IA. IBM Cloud met tout en œuvre pour assurer une rétrocompatibilité à long terme de ses API d'IA. Néanmoins, IBM recommande que les lignes directrices soient rédigées de manière à ne pas freiner l'innovation, notamment lorsqu'un changement majeur et disruptif est nécessaire dans un domaine technologique critique ou émergent.

Question 3:

OpenAPI est une spécification largement adoptée, qui peut effectivement être considérée comme un moyen de favoriser une documentation harmonisée des API. Comme de nombreuses autres entreprises, IBM a adopté Open API sur différentes technologies et outils¹. IBM Cloud valide l'ensemble de ses API à l'aide d'un outil de validation OpenAPI.

Comme indiqué sur cette page sur les bonnes pratiques API sur IBM Cloud, « *l'outil OpenAPI Validator valide les documents OpenAPI selon un sous-ensemble des normes définies dans ce guide et identifie les éléments non conformes à la spécification OpenAPI ou aux lignes directrices du guide IBM. Le rapport généré par l'outil identifie les éléments spécifiques de la définition d'API qui ne respectent pas la spécification OpenAPI ou le IBM API Handbook. Toutes les erreurs listées dans le rapport doivent être corrigées avant la publication de l'API, sauf si les corrections entraîneraient des ruptures de compatibilité pour une version existante de l'API.* » (lien: <https://cloud.ibm.com/docs/api-handbook?topic=api-handbook-intro#verifying-compliance>).

L'outil IBM OpenAPI Validator permet de valider les documents OpenAPI 3.0.x et 3.1.x pour vérifier leur conformité à la spécification OpenAPI ainsi qu'aux bonnes pratiques définies par IBM (lien: <https://github.com/IBM/openapi-validator>).

IBM Cloud fournit une documentation pour chaque API, par exemple ici <https://cloud.ibm.com/apidocs/vpc/latest> qui inclut un lien vers la spécification OpenAPI de l'API ici <https://cloud.ibm.com/apidocs/vpc/latest.json>.

IBM Cloud Watson Assistant exploite également OpenAPI pour créer des extensions personnalisées permettant à un agent d'IA d'appeler d'autres applications. « *Pour créer une extension personnalisée, vous devez disposer d'un document OpenAPI décrivant l'API REST à intégrer. De nombreux services tiers publient des documents OpenAPI décrivant leurs API, que vous pouvez télécharger et importer. Pour une API interne à votre entreprise, vous pouvez utiliser des outils standards pour générer un document OpenAPI.* » (lien: <https://cloud.ibm.com/docs/watson-assistant?topic=watson-assistant-build-custom-extension>)

Cependant, afin d'éviter des recommandations trop prescriptives sur ce sujet, il pourrait être pertinent de modifier légèrement la recommandation afin de :

- prendre en compte le fait que certains fournisseurs pourraient avoir besoin de délais pour mettre en œuvre la dernière version de la spécification.
- mentionner OpenAPI "et/ou des certifications équivalentes". Il est toujours délicat d'imposer une technologie spécifique, car cela pourrait avoir un impact sur le marché et favoriser certains acteurs au détriment d'autres. À ce stade, il n'est pas non plus clairement établi s'il est nécessaire de sélectionner ou d'imposer une spécification unique comme OpenAPI, ou s'il est possible d'envisager plusieurs spécifications répondant aux exigences légales, OpenAPI n'étant alors que l'une d'entre elles. Nous recommandons également de porter cette discussion au sein du CEN-CENELEC JTC 25.

¹ <https://www.ibm.com/docs/en/app-connect/13.0.x?topic=apis-openapi-30>