



autorité de régulation  
des communications électroniques,  
des postes et de la distribution de la presse

RÉPUBLIQUE FRANÇAISE

# CONSULTATION PUBLIQUE

Du 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*)**

## Modalités pratiques de la consultation publique

L'avis de tous les acteurs intéressés est sollicité sur l'ensemble du présent document. Il est néanmoins possible de ne répondre qu'à une partie des questions.

La présente consultation publique est ouverte jusqu'au 18 juillet 2025 à 18h00, heure de Paris. Seules les contributions arrivées avant l'échéance seront prises en compte.

Les réponses doivent être transmises à l'Arcep de préférence en utilisant le formulaire disponible sur le site internet de l'Arcep :

<https://www.arcep.fr/actualites/les-consultations-publiques/p/gp/detail/consultation-recommandation-interoperabilite-portabilite-cloud-juin2025.html>

L'Arcep, dans un souci de transparence, publiera le résultat de la consultation, à l'exclusion des éléments d'information couverts par le secret des affaires. Au cas où leur réponse contiendrait de tels éléments, les contributeurs sont invités à transmettre leur réponse en deux versions :

- une version confidentielle, dans laquelle les passages qui peuvent faire l'objet d'une protection au titre du secret des affaires sont identifiés entre crochets et surlignés en gris, par exemple : « une part de marché de [SDA : 25]% » ;
- une version publique, dans laquelle les passages qui peuvent faire l'objet d'une protection au titre du secret des affaires auront été remplacés par [SDA], par exemple : « une part de marché de [SDA]% ».

Les contributeurs sont invités à limiter autant que possible les passages qui peuvent faire l'objet d'une protection au titre du secret des affaires. L'Arcep se réserve le droit de déclasser d'office des éléments d'information qui, par leur nature, ne relèvent pas du secret des affaires.

En complément des questions posées ci-après, les acteurs sont libres de faire part de tout commentaire en lien avec l'objet de la consultation. Des renseignements complémentaires peuvent être obtenus en adressant vos questions à : [CPcloud@arcep.fr](mailto:CPcloud@arcep.fr).

Ce document est disponible en téléchargement sur le site : [www.arcep.fr](http://www.arcep.fr).

# Recommandation de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du X 2025 relative à l'interopérabilité et à la portabilité des services d'informatique en nuage (*cloud*)

## 1 Contexte

Le règlement européen sur les données<sup>1</sup>, publié le 22 décembre 2023, vise notamment à éliminer les obstacles au bon fonctionnement du marché intérieur des données. Par ses chapitres VI et VIII, il met en place à la charge des fournisseurs des services de traitement de données<sup>2</sup> la mise en œuvre de mesures techniques, organisationnelles et contractuelles destinées à faciliter le changement de fournisseur de service par les utilisateurs. Pour ce faire, le règlement européen sur les données prévoit concernant le changement de fournisseur ou le multi-cloud, notamment :

- un encadrement de la relation contractuelle et précontractuelle entre l'utilisateur et le fournisseur de service de traitement de données dans le cadre d'un changement de fournisseur<sup>3</sup> ;
- une meilleure circulation des données via la portabilité, l'interopérabilité, et l'ouverture d'interfaces de programmation d'application<sup>4</sup>.

Le règlement prévoit par ailleurs que la Commission européenne pourra édicter des normes harmonisées ou des spécifications d'interopérabilité ouvertes opposables à ces acteurs<sup>5</sup> qui couvrent des exigences essentielles en matière notamment d'interopérabilité et de portabilité.

Ce règlement est applicable à partir du 12 septembre 2025.

Certaines mesures issues du règlement sur les données ont été introduites, par anticipation, en droit français par la loi n° 2024-449 visant à sécuriser et réguler l'espace numérique (ci-après « loi SREN »), promulguée le 21 mai 2024, qui vise également la levée de barrières techniques et tarifaires au changement de fournisseur d'informatique en nuage (fournisseurs de services cloud) ou à l'utilisation simultanée des services cloud de plusieurs fournisseurs (multi-cloud). Ainsi, elle prévoit à son titre III, relatif à la confiance et la concurrence dans l'économie de la donnée, plusieurs obligations pour les

---

<sup>1</sup> Règlement (UE) 2023/2854 du Parlement européen et du Conseil en date du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données).

<sup>2</sup> La définition de service d'informatique en nuage telle qu'introduite dans le code de commerce par le I. de l'article 26 de la loi SREN est identique à la définition des services de traitement de données du paragraphe 8) de l'article 2 du règlement sur les données.

<sup>3</sup> Voir les articles 25 « *Clauses contractuelles concernant le changement de fournisseur* » et 26 « *Obligation d'information incombant aux fournisseurs de services de traitement de données* » du règlement sur les données.

<sup>4</sup> Voir les articles 30 « *Aspects techniques du changement de fournisseur* » et 35 « *Interopérabilité des services de traitement de données* » du règlement sur les données.

Les interfaces de programmation d'application (*Application Programming Interface*, ou API) sont les façades des systèmes informatiques qui leur permettent d'échanger des données à l'aide de requêtes prédéfinies. L'architecture la plus répandue est REST (Representational State Transfer) : on parle des API RESTful.

<sup>5</sup> Voir en particulier l'article 35 du règlement sur les données : « 5. La Commission peut, par voie d'actes d'exécution, adopter des spécifications communes fondées sur des spécifications d'interopérabilité ouvertes couvrant toutes les exigences essentielles prévues aux paragraphes 1 et 2 ».

fournisseurs de services d'informatique en nuage et confie dans ce cadre de nouvelles missions à l'Arcep.

Le II de l'article 28 de la loi SREN prévoit que les fournisseurs de services cloud garantissent la conformité de leurs services aux exigences essentielles d'interopérabilité, de portabilité et de mise à disposition des API<sup>6</sup>, et le I de l'article 29 dispose notamment que « [L'Arcep] *précise les règles et les modalités de mise en œuvre des exigences mentionnées au II de l'article 28, notamment par l'édiction de spécifications d'interopérabilité et de portabilité* ».

L'article 64 de la loi SREN prévoit que les dispositions relatives à l'interopérabilité des services d'informatique en nuage ne s'appliquent que jusqu'au 12 janvier 2027.

Dans ce contexte, l'Arcep a mis en consultation publique du 14 octobre au 16 décembre 2024 un document décrivant notamment sa compréhension des pratiques et outils existants en matière de portabilité et d'interopérabilité des services cloud, et les besoins de transparence et d'harmonisation identifiés lors des rencontres avec les utilisateurs.

L'Autorité a reçu 22 contributions à sa consultation publique<sup>7</sup>, dont 19 qui ont abordé les enjeux liés aux exigences techniques d'interopérabilité, de portabilité et d'ouverture des interfaces de programmation d'applications. Ces contributions émanaient d'acteurs français, d'acteurs issus des autres États membres de l'Union européenne, et d'acteurs extra-européens, dont les principaux fournisseurs mondiaux de services cloud ainsi que des fournisseurs alternatifs.

Dans ce cadre, au vu de ces contributions, du calendrier d'application de la loi SREN et des délais de mise en conformité des acteurs à d'éventuelles règles contraignantes lesquelles pourraient se superposer à d'éventuels actes d'exécution de la Commission européenne, l'Arcep estime plus approprié de définir, par la présente recommandation dépourvue de toute portée normative, des bonnes pratiques à destination de l'ensemble des fournisseurs de services cloud dans le but de faciliter le changement de fournisseur de services cloud et le recours simultané à plusieurs fournisseurs (multi-cloud). Ce document est susceptible de nourrir les réflexions futures de la Commission européenne quant à l'édiction de spécifications communes d'interopérabilité dans le cadre de la mise en œuvre du règlement sur les données.

Il est sans préjudice des obligations de transparence, d'interopérabilité, de portabilité et d'ouverture des API issues du règlement sur les données et de la loi SREN.

---

<sup>6</sup> « Les fournisseurs de services d'informatique en nuage assurent la conformité de leurs services aux exigences essentielles : 1° D'interopérabilité, dans des conditions sécurisées, avec les services du client ou avec ceux fournis par d'autres fournisseurs de services d'informatique en nuage pour le même type de service ; 2° De portabilité des actifs numériques et des données exportables, dans des conditions sécurisées, vers les services du client ou vers ceux fournis par d'autres fournisseurs de services d'informatique en nuage couvrant le même type de service ; 3° De mise à disposition gratuite aux clients et aux fournisseurs de services tiers désignés par ces utilisateurs à la fois d'interfaces de programmation d'applications nécessaires à la mise en œuvre de l'interopérabilité et de la portabilité mentionnées aux 1° et 2° du présent II et d'informations suffisamment détaillées sur le service d'informatique en nuage concerné pour permettre aux clients ou aux services de fournisseurs tiers de communiquer avec ce service, à l'exception des services qui relèvent des services mentionnés au III de l'article 29. »

<sup>7</sup> Les contributions sont disponibles à l'adresse suivante : <https://www.arcep.fr/actualites/les-consultations-publiques/p/gp/detail/consultation-cloud-changement-fournisseur-services-architectures-tarifs-oct2024.html>

## 2 Les contributions à la consultation publique soulignent que la transparence sur les modalités de portabilité et d'interopérabilité et des API stables et documentées pourraient favoriser le libre choix des utilisateurs

Dans la consultation publique de fin 2024, l'Arcep a partagé sa compréhension des modalités techniques du changement de fournisseur de cloud et de développement d'architectures multi-cloud, ainsi que des freins à leur mise en œuvre. Elle y a également présenté des leviers d'action potentiels permettant de contribuer à lever ces freins.

Premièrement, le document soumis à consultation publique décrivait le processus de changement de fournisseur, en se référant au règlement sur les données. Il le présentait comme une opération en plusieurs étapes consistant, notamment en une extraction de données, leur éventuelle transformation afin qu'elles correspondent au schéma du nouvel emplacement de destination, et enfin leur téléversement dans cet emplacement.<sup>8</sup>

Ce document soulignait aussi que la complexité de la migration dépendait de la nature et de l'architecture des actifs numériques à transférer, et *in fine* des types de services cloud qui utilisent ces actifs. Ainsi, il était relevé l'absence d'obstacle majeur pour la migration des applications reposant uniquement sur les services IaaS<sup>9</sup>. Pour les applications reposant sur des services PaaS<sup>10</sup>, la difficulté principale de migration identifiée était liée à la nécessité de s'adapter aux fonctionnalités spécifiques offertes par les différents fournisseurs. Pour les services SaaS<sup>11</sup>, dont la migration nécessite d'exporter les données des utilisateurs, l'enjeu réside dans la disponibilité d'une API ou d'interfaces graphiques pour réaliser ces exports.

Les contributeurs ont généralement adhéré à cette description, tout en apportant certains détails techniques quant aux processus de migration déployés (par exemple l'importance des phases de test dans l'environnement de destination a pu être soulignée) et en mentionnant d'autres causes aux difficultés pouvant être rencontrées par l'utilisateur. En particulier, certaines contributions ont suggéré que les choix et besoins des utilisateurs pouvaient également complexifier la migration : ce serait notamment le cas lorsque l'utilisateur a des besoins spécifiques en matière de sécurité ou de continuité de service, lorsque son architecture contient des dépendances complexes, ou encore lorsqu'il a une dette technique<sup>12</sup> importante.

Deuxièmement, l'Autorité indiquait également dans son document soumis à consultation publique que les architectures multi-cloud sont tributaires de l'interopérabilité des différents fournisseurs de

---

<sup>8</sup> Règlement sur les données, considérant (85) : « Le changement de fournisseur est une opération orientée vers le client, qui consiste en plusieurs étapes, notamment l'extraction de données, qui correspond au téléchargement de données à partir de l'écosystème du fournisseur d'origine de services de traitement de données; la transformation, lorsque les données sont structurées d'une manière qui ne correspond pas au schéma de l'emplacement cible; et le téléversement des données dans un nouvel emplacement de destination. [...] »

<sup>9</sup> L'acronyme IaaS fait référence à « Infrastructure-as-a-Service ».

<sup>10</sup> L'acronyme PaaS fait référence à « Platform-as-a-Service ».

<sup>11</sup> L'acronyme SaaS fait référence à « Software-as-a-Service ».

<sup>12</sup> La dette technique désigne les compromis fait lors du développement logiciel (comme utiliser des solutions rapides pour répondre à un besoin immédiat) qui facilitent le travail à court terme, mais entraînent des coûts accrus et des difficultés de maintenance à long terme.

services cloud. Elle faisait le constat que les besoins d'interopérabilité variaient en fonction du type d'architecture multi-cloud utilisé et décrivait à cet égard trois modèles de multi-cloud<sup>13</sup>.

Elle estimait que l'utilisation des API permettait en pratique de répondre à ces besoins d'interopérabilité afin d'échanger, entre différents services cloud, des informations renseignées selon des formats documentés et interprétables, à l'aide de protocoles partagés et au travers de systèmes interconnectés par des réseaux. Elle concluait que l'interopérabilité des services cloud nécessaire au développement d'architecture multi-cloud reposait ainsi sur la mise à disposition par chaque fournisseur de services cloud d'API stables, documentées et accessibles depuis l'extérieur de son écosystème.

Dans leurs réponses à la consultation publique, une majorité de contributions a adhéré aux descriptions des architectures multi-cloud, de leurs besoins en matière d'interopérabilité, et reconnu l'importance d'API stables et documentées. Toutefois, certaines contributions ont souligné les limites des architectures multi-cloud notamment en matière de latence et de coûts.

Troisièmement, dans le document soumis à consultation publique, la différenciation entre les services *cloud* du même type proposés par différents fournisseurs était présentée comme le facteur principal à l'origine de difficultés techniques limitant la capacité de l'utilisateur à changer de fournisseur et à construire des architectures multi-cloud. En effet, tout en soulignant le potentiel d'innovation des services spécifiques destinés à répondre à des besoins particuliers des utilisateurs, l'Arcep indiquait que ces derniers pouvaient être techniquement plus difficiles à migrer en l'absence d'équivalent immédiat chez les fournisseurs concurrents, nécessitant des opérations techniques importantes telles qu'une réadaptation de l'architecture des applications.

Dans ce cadre, l'Autorité estimait que pour que l'utilisateur soit en capacité d'arbitrer entre, d'une part, la performance ou la disponibilité de certaines fonctionnalités et, d'autre part, la portabilité et l'interopérabilité des services, une plus grande transparence sur le caractère spécifique des services fournis et le degré de portabilité des services pouvait apparaître nécessaire.

Une majorité de contributeurs a partagé le constat de l'Autorité et reconnu que l'information des utilisateurs est essentielle afin de favoriser leur libre choix et pour inciter à réduire les éventuelles barrières techniques existantes.

**Ainsi, au regard de l'ensemble des éléments qui précèdent, l'Autorité souhaite formuler des préconisations concernant, d'une part, les informations qu'il serait utile de porter à la connaissance des clients et clients potentiels relatives à la portabilité et l'interopérabilité des services *cloud* utilisés et, d'autre part, les modalités pratiques de mise en œuvre de la portabilité et de l'interopérabilité, en proposant des API stables et documentées.**

### **3 Renforcer la transparence sur le degré de portabilité et d'interopérabilité des services *cloud***

Les contributeurs à la consultation publique reconnaissent qu'une plus grande transparence sur le degré d'interopérabilité et de portabilité des services cloud serait bénéfique.

---

<sup>13</sup> Par ordre croissant de besoin d'interopérabilité, il s'agissait d'un modèle « siloté », lorsque les services fournis par différents fournisseurs poursuivent des objectifs différents et que les applications qui reposent sur ces services n'interagissent pas ; d'un modèle « déploiement agnostique », lorsque l'utilisateur a recours à des ressources d'infrastructure fournies par différents fournisseurs grâce à une plateforme de déploiement ; et d'un modèle « intégré », lorsqu'une application a recours aux services de différents fournisseurs afin de répondre à un même besoin métier.

Les acteurs ont majoritairement reconnu l'intérêt de rendre disponibles des informations comparables permettant aux clients potentiels d'effectuer un choix éclairé de leur fournisseur de service cloud, tout en émettant des réserves quant à une harmonisation trop stricte du format de diffusion de ces informations, susceptible de générer des lourdeurs excessives en particulier pour des fournisseurs de petite taille.

Une majorité de contributions a suggéré la prise en compte des travaux déjà menés au sein du secteur, en s'appuyant sur les codes de conduite tels que SWIPO ou CISPE Cloud Switching Framework<sup>14</sup>. Les codes de conduite SWIPO (Switching Cloud Providers and Porting Data), élaborés en application de l'article 6 du règlement établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (« Free flow of non personal data »), fournissent un ensemble de préconisations en matière de transparence destinées à faciliter la portabilité des données et le changement de fournisseur. Cette initiative, à laquelle avaient adhéré certains fournisseurs de services cloud, prévoyait que soit fournie, antérieurement à la signature d'un contrat, une déclaration de transparence détaillant entre autres les données exportables et les procédures à suivre lors d'un changement de fournisseur. Bien que l'initiative ait pris fin, de nombreux acteurs de l'écosystème reconnaissent encore la pertinence du contenu de ces codes de conduite.

L'Autorité considère que le contenu de ce code de conduite pourrait être une référence pertinente pour déterminer quelles informations devraient être rendues disponibles aux clients et clients potentiels, afin de leur permettre d'exercer leur liberté de choix.

A cet égard, certaines informations revêtent un intérêt particulier pour les clients et clients potentiels de services cloud, dans l'objectif de fluidifier le marché des services cloud et de renforcer la capacité de choix des utilisateurs. Il s'agit en particulier de celles correspondant aux informations identifiées dans le règlement sur les données dans le cadre des exigences de transparence incombant aux fournisseurs de services cloud, et susceptibles d'appuyer la stratégie de sortie des clients, à savoir : *« les procédures à suivre pour entamer le changement de services de traitement de données; les formats de données lisibles par machine vers lesquels les données de l'utilisateur peuvent être exportées; les outils destinés à exporter les données, dont des interfaces ouvertes, ainsi que les informations sur la compatibilité avec les normes harmonisées ou les spécifications communes fondées sur des spécifications d'interopérabilité ouvertes; des informations sur les restrictions et les limites techniques connues qui pourraient influencer sur le processus de changement de fournisseur; et le temps considéré comme nécessaire pour achever ledit processus de changement »*<sup>15</sup>.

En outre, d'autres informations sont susceptibles de contribuer à lever les barrières techniques au changement de fournisseur et au multi-cloud : outils de supervision disponibles pour la migration, processus disponibles pour garantir l'intégrité des données et la continuité des services, référence de documentation des API utilisées et des dépendances dans le cadre d'une migration, procédures de test disponibles, durée de transfert des données et méthodes pour garantir la sécurité des données lors du transfert.

Afin de faciliter la comparaison entre les services cloud, l'Autorité estime pertinent que ces informations soient aisément accessibles et présentées selon un ordonnancement uniforme.

Au regard de ce qui précède, l'Autorité estime souhaitable, en reprenant les principales informations requises par les codes de conduite SWIPO, notamment le code relatif aux services IaaS, que les fournisseurs de services cloud publient les informations suivantes assorties de leur index, de manière

---

<sup>14</sup> CISPE Cloud Switching Framework est un code de conduite élaboré par l'association de fournisseurs CISPE Cloud et qui vise à faciliter la conformité au règlement sur les données.

<sup>15</sup> Règlement sur les données, considérant 95.

accessible sur leur site internet, d'une part dans un format libre (par exemple via une page web ou un document PDF), et d'autre part dans un format lisible par ordinateur (par exemple un fichier JSON)<sup>16</sup> :

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 ;
2. Procédures pour initier une migration depuis le service cloud ;
3. Procédures pour initier une migration vers le service cloud ;
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 ;
5. Méthodes de migration recommandées en fonction du volume de données à transférer ;
6. Méthodes pour garantir la sécurité des données lors du transfert (contrôle d'accès, authentification des utilisateurs, confidentialité et intégrité) ;
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 ;
8. Processus disponibles pour garantir l'intégrité des données, la continuité de service et prévenir la perte de données pendant la migration ;
9. Processus de résiliation d'un service cloud existant, lorsque le client souhaite mettre fin à son utilisation du service après la migration ;
10. Outils de supervision disponibles pour la migration et coûts associés à leur usage ;
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 ;
12. Référence de la documentation des API permettant la mise en œuvre de la portabilité et de l'interopérabilité ;
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 ;
14. Délais de migration et durée de transfert des données.



**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 ?

Les informations proposées nous semblent tout à fait pertinentes pour les services IaaS. En effet, en s'appuyant sur les exigences issues des travaux menés par SWIPO et CISPE, cette approche s'aligne avec les pratiques déjà en place chez les acteurs du IaaS comme OUTSCALE, marque de Dassault Systèmes.

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

En revanche, nous émettons de fortes réserves quant à l'applicabilité de l'ensemble de ces éléments aux services PaaS, et plus encore aux services SaaS. La diversité, la spécialisation et l'ancrage métier des offres SaaS rendent toute tentative d'harmonisation largement illusoire. Les logiques fonctionnelles et les modèles de données varient très sensiblement d'un fournisseur à l'autre, faisant ainsi obstacle à une approche standardisée en termes d'interopérabilité.

Plusieurs des exigences proposées relèvent davantage de l'ingénierie d'échange ou de prestations de service spécifiques comme la migration différenciée selon les volumes, les tests de restauration ou la continuité de service, qui doivent rester du ressort des acteurs industriels, selon une approche au cas par cas. Comme déjà signalé à l'autorité, il ne serait pas forcément souhaitable de vouloir encadrer ces aspects par la loi car ils relèvent de logiques contractuelles et dépendent de contraintes opérationnelles.

D'une manière générale, ces exigences appliquées au PaaS/SaaS reposent sur une vision figée du logiciel, inspirée du modèle IaaS, avec une hypothèse implicite de transfert complet (données + environnement d'exécution) qui ne s'applique pas aux services PaaS/SaaS. Pour ces derniers, les données n'ont bien souvent de valeur que dans leur environnement applicatif propre ; envisager un export complet, intégrant cette logique applicative, n'est ni réaliste ni souhaitable.

Les codes de conduite SWIPO et CISPE ont d'ailleurs été élaborés spécifiquement pour les services IaaS, dont la structure et les cas d'usage se prêtent davantage à une telle démarche. À l'inverse, la nature même des services SaaS ne permet pas de transposer ces référentiels.

Par conséquent, comme déjà mentionné, nous recommandons à l'ARCEP, s'agissant des services PaaS/SaaS, de concentrer ses efforts sur la promotion de pratiques communes en matière de conception, d'utilisation et de documentation des API. Une telle approche favoriserait une meilleure interopérabilité et un échange de données plus fluide entre services hétérogènes, sans imposer une normalisation qui, à ce stade, ne serait ni réaliste ni souhaitable.

Nous suggérons donc à l'ARCEP de préciser que cette recommandation, ainsi que la liste des informations à partager, s'applique exclusivement aux services IaaS.

---

<sup>16</sup> Certaines de ces informations doivent déjà être contractuellement fournies aux utilisateurs dans le cadre de la loi SREN et du règlement sur les données, voir en particulier les articles 25 et 26 du règlement sur les données, et l'article 28 de la loi SREN.

## 4 Favoriser la mise à disposition d'API stables et documentées

Le règlement sur les données prévoit que les fournisseurs de services cloud mettent des interfaces ouvertes à disposition de leurs clients afin de faciliter le changement de fournisseur et l'interopérabilité<sup>17</sup>.

Ces interfaces permettent de garantir que les informations utilisées entre deux systèmes cloud sont renseignées selon des formats interprétables, à l'aide de protocoles partagés et que les systèmes soient interconnectés par des réseaux pour pouvoir les échanger.

Dans le document mis en consultation publique, les contributeurs étaient invités à réagir au constat selon lequel, d'une part, la disponibilité des API serait essentielle pour assurer l'interopérabilité entre les services cloud, et, d'autre part, leur documentation permettrait d'informer les utilisateurs quant aux formats attendus en entrée et renvoyés en sortie dans le cadre d'un export de données résultant d'une migration ou d'une utilisation du multcloud. Les acteurs étaient par ailleurs invités à donner leur avis sur les critères selon lesquels les API pourraient être qualifiées de stables et documentées.

En réponse, les contributeurs à la consultation publique reconnaissent unanimement l'importance d'API disponibles, stables et documentées.

S'agissant, d'une part, de la documentation des API, certaines contributions ont mis en avant la spécification OpenAPI<sup>18</sup> comme pertinente pour faciliter des documentations exhaustives et comparables. La spécification OpenAPI définit une interface standard afin de simplifier l'interaction des utilisateurs et des applications avec les API. Elle repose sur des standards et des spécifications de l'Internet Engineering Task Force (IETF).

L'Arcep considère que promouvoir cette spécification, qui constitue une bonne pratique déjà employée par une large majorité de fournisseurs, notamment dans le domaine du cloud, permettrait de maximiser l'interopérabilité sans pour autant nécessiter des adaptations majeures de la part des acteurs et d'assurer une certaine flexibilité quant à la description des API et de leur fonctionnement.

S'agissant, d'autre part de la stabilité des API, les retours à la consultation ont confirmé que des mises à jour soudaines et trop fréquentes de certaines API clés, lorsque ces mises à jour ne sont pas rétrocompatibles<sup>19</sup>, peuvent limiter la capacité des fournisseurs tiers à garantir la compatibilité de leurs services, et *in fine* leur interopérabilité. À cet égard, pour répondre à de telles difficultés, les contributeurs proposent différents délais de préavis en cas de mise à jour non-rétrocompatibles, comprise entre trois et douze mois. L'Autorité comprend ainsi qu'un délai minimal est déjà appliqué par une partie de l'écosystème en cas de mise à jour sans garantie de rétrocompatibilité, et que les fournisseurs mettent en place des avertissements dans ces cas de figure.

---

<sup>17</sup> Article 30, paragraphe 2 : « Les fournisseurs de traitement de données, autres que ceux qui concernent des ressources informatiques modulables et variables limitées à des éléments d'infrastructure tels que les serveurs, les réseaux et les ressources virtuelles nécessaires à l'exploitation de l'infrastructure, sans donner accès aux services, logiciels et applications d'exploitation qui sont stockés, autrement traités ou déployés sur ces éléments d'infrastructure mettent gratuitement et dans la même mesure à la disposition de tous leurs clients et des fournisseurs de destination de services de traitement de données concernés des interfaces ouvertes afin de faciliter le processus de changement de fournisseur. Ces interfaces contiennent des informations suffisantes sur le service concerné pour permettre le développement de logiciels capables de communiquer avec les services, aux fins de la portabilité et de l'interopérabilité des données. »

Article 34, paragraphe 1 : « Les exigences prévues [...] à l'article 30, [paragraphe 2] s'appliquent également mutatis mutandis aux fournisseurs de services de traitement de données pour faciliter l'interopérabilité aux fins de l'utilisation simultanée de services de traitement de données. »

<sup>18</sup> <https://www.openapis.org/>

<sup>19</sup> La rétrocompatibilité est ici comprise comme la capacité d'une API, après une mise à jour, à répondre aux requêtes rédigées pour une version antérieure.

Ainsi, au regard de ce qui précède, l'Autorité estime qu'il serait pertinent que les fournisseurs :

- informent leurs utilisateurs par l'intermédiaire de message d'avertissement douze mois au minimum avant l'exécution de mises à jour importantes de leurs API en cas de non-rétrocompatibilité ;
- adoptent la version la plus récente de la spécification OpenAPI pour la description et la documentation de leurs API.

**Question 3 :** Le délai de préavis proposé vous semble-t-il approprié ? Dans le cas contraire, quel délai préconisez-vous ? Pourquoi ?

Nous considérons qu'un préavis de douze mois pour toute évolution non-rétrocompatible des API constitue un équilibre satisfaisant entre la nécessité pour les utilisateurs d'anticiper et de planifier leurs adaptations et l'impératif des fournisseurs de garantir la sécurité et la performance de leurs services. Ce délai permet aux équipes techniques de tester en conditions réelles les impacts des changements, de mettre à jour les environnements de production sans rupture de service, et de coordonner les mises à niveau avec leurs fournisseurs de solutions tierces.

En cas de mise à jour urgente motivée par une vulnérabilité critique ou un besoin impérieux d'optimisation des performances, il est toutefois essentiel que le fournisseur maintienne l'ancienne version de l'API en mode « deprecated » (« déprécié ») pendant une période complémentaire d'au moins douze mois. Il devra informer les clients des risques encourus et préciser la date de fin de vie de la version « dépréciée » le cas échéant. Cette approche garantit à la fois la sécurité des environnements et la continuité opérationnelle des services des utilisateurs.

**Question 4 :** L'adoption généralisée de la spécification OpenAPI vous semble-t-elle souhaitable, notamment afin de permettre une documentation des API harmonisée ?

Nous utilisons déjà des méta-modèles largement éprouvés et standardisés, tels qu'OpenAPI, pour la description et la documentation de nos interfaces. La généralisation d'OpenAPI ne serait ainsi *a priori* pas être problématique.

Nous recommandons toutefois de formuler cette exigence sans faire référence à un nom de spécification particulier, afin de laisser aux fournisseurs la liberté de recourir à la solution la mieux adaptée à leurs architectures et à l'évolution des standards industriels. Cette flexibilité favorisera l'émergence de nouveaux méta-modèles plus efficaces à l'avenir, tout en assurant dès aujourd'hui une base commune minimale pour la description des API, sans verrouillage technologique.

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

Comme nous l'avons déjà noté, nous souhaitons attirer l'attention sur une distinction essentielle concernant la disponibilité des API dans le cadre des services SaaS.

Il est en effet important de distinguer clairement deux catégories d'API :

- Les API publiques ou exposées en continu, qui sont conçues pour être utilisées de manière récurrente ou dans des cas d'usage tiers, par exemple pour l'intégration à des services ou plateformes externes. Ces API doivent généralement répondre à des exigences strictes en matière de disponibilité, de performance, de sécurité et de rétrocompatibilité.
- Les API dédiées exclusivement au switching (par exemple de services SaaS), c'est-à-dire mises à disposition dans le cadre d'une procédure ponctuelle de changement de fournisseur. Ces API sont utilisées dans un contexte donné et délimité, souvent en mode « one shot », pour permettre l'extraction et la transmission de données vers un nouveau prestataire. Dans ce cas, les exigences de disponibilité sont différentes : il s'agit moins d'une exposition continue que d'une accessibilité garantie à la demande, avec des mécanismes d'activation encadrés.