



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

RÉPUBLIQUE FRANÇAISE

RECOMMANDATION

Interopérabilité et portabilité des services d'informatique en nuage

25 septembre 2025

A decorative graphic in the bottom right corner consisting of a dense, overlapping pattern of thin, light grey lines that form a fan-like or cloud-like shape.

ISSN n°2258-3106

Recommandation de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du 25 septembre 2025 relative à l'interopérabilité et à la portabilité des services d'informatique en nuage

1 Contexte

Le règlement européen sur les données¹, 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 données² 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 l'utilisation simultanée de services de plusieurs fournisseurs (*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 fournisseur³ ;
- une meilleure circulation des données via la portabilité, l'interopérabilité, et l'ouverture d'interfaces de programmation d'application (API)⁴.

Le règlement prévoit par ailleurs que la Commission européenne pourra édicter des normes harmonisées ou des spécifications d'interopérabilité ouvertes opposables à ces acteurs⁵ 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

¹ 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).

² 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.

³ 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.

⁴ 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.

⁵ 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* ».

changement de fournisseur de services d'informatique en nuage (services *cloud*) ou à l'utilisation simultanée des services d'informatique en nuage 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 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 API⁶, 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 publique⁷, 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 *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.

La présente recommandation a fait l'objet d'une consultation publique du 17 juin au 25 juillet 2025 et a été amendée en tenant compte des 14 contributions reçues⁸.

⁶ « 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. »

⁷ 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>

⁸ Les contributions sont disponibles à l'adresse suivante : https://www.arcep.fr/uploads/tx_gspublication/contributions-cp-recommandation-interoperabilite-portabilite-cloud_sept2025.zip

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.⁹

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 IaaS¹⁰. Pour les applications reposant sur des services PaaS¹¹, 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 SaaS¹², 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 technique¹³ 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

⁹ 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. [...] »

¹⁰ L'acronyme IaaS fait référence à « Infrastructure-as-a-Service » ou « infrastructure en tant que service ».

¹¹ L'acronyme PaaS fait référence à « Platform-as-a-Service » ou « plateforme en tant que service ».

¹² L'acronyme SaaS fait référence à « Software-as-a-Service » ou « logiciel en tant que service ».

¹³ 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*¹⁴.

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.

¹⁴ 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.

3 Renforcer la transparence sur le degré de portabilité et d'interopérabilité des services d'informatique en nuage

3.1 Analyse de l'Autorité

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.

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 Framework¹⁵. 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 »*¹⁶.

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

¹⁵ 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.

¹⁶ Règlement sur les données, considérant 95.

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.

3.2 Recommandation

Au regard de ce qui précède, et notamment au vu des réponses à la consultation publique, 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 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 dont un modèle figure en annexe)¹⁷ :

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 fournisseurs¹⁸ ;
2. Procédures pour initier une migration depuis le service *cloud*¹⁹ ;
3. Procédures pour initier une migration vers le service *cloud*²⁰ ;
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 connues²¹ ; Méthodes pour garantir la sécurité des données lors du transfert (contrôle d'accès, authentification des utilisateurs, confidentialité et intégrité)²² ;
5. Procédures pour tester les différents mécanismes de migration, notamment ceux de sauvegarde (*snapshot*), de restauration (*rollback*) et de vérification de l'intégrité des données²³ ;
6. Processus disponibles pour garantir l'intégrité des données, la continuité de service et prévenir la perte de données pendant la migration²⁴ ;
7. Processus de résiliation d'un service *cloud* existant, lorsque le client souhaite mettre fin à son utilisation du service après la migration²⁵ ;
8. Outils de supervision disponibles pour la migration et coûts associés à leur usage²⁶ ;

¹⁷ Sauf, bien évidemment, lorsque le service concerné ne présente pas les caractéristiques sur lesquelles portent les informations listées dans la présente recommandation.

¹⁸ Cf. SWIPO IaaS SCR01 et SCR02, SWIPO SaaS 3.2.7, 3.2.8 et 3.2.17

¹⁹ Cf. SWIPO IaaS PR01, SWIPO SaaS 3.2.1

²⁰ Cf. SWIPO IaaS PR02 et PR05, SWIPO SaaS 3.3.1

²¹ Cf. SWIPO IaaS PR03, SWIPO SaaS 3.2.11 et 3.2.16

²² Cf. SWIPO IaaS PLR04, SWIPO SaaS 3.2.12

²³ Cf. SWIPO IaaS PLR01, SWIPO SaaS 3.2.1 et 3.2.15

²⁴ Cf. SWIPO IaaS DP09, SWIPO SaaS 3.2.15

²⁵ Cf. SWIPO IaaS PR06

²⁶ Cf. SWIPO IaaS PR07, SWIPO SaaS 3.2.4 et 3.2.5

9. 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 formats²⁷ ;
10. Référence de la documentation des API permettant la mise en œuvre de la portabilité et de l'interopérabilité²⁸ ;
11. 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*²⁹.

Certaines de ces informations doivent déjà être contractuellement fournies aux clients en application du règlement sur les données (voir notamment les articles 25, 26, 28 et 30 de ce règlement).

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

4.1 Analyse de l'Autorité

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'interopérabilité³⁰.

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 *multi-cloud*. 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.

²⁷ Cf. SWIPO IaaS PR03, SWIPO SaaS 3.2.9 et 3.2.10

²⁸ Cf. SWIPO IaaS DP04

²⁹ Cf. SWIPO IaaS DP04 DP07, et SCR02, SWIPO SaaS 3.2.3, 3.2.4, 3.2.5, 3.2.10, 3.2.17 et 3.2.18

³⁰ 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. »

S'agissant, d'une part, de la documentation des API, certaines contributions ont mis en avant la spécification OpenAPI³¹ 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. Les contributions reçues à la consultation publique du 17 juin au 25 juillet 2025 mentionnent toutefois que lorsque le protocole employé par l'API n'est pas http, la spécification OpenAPI n'est pas applicable.

S'agissant d'autre part de la stabilité des API, les retours aux deux consultations publiques ont confirmé que des mises à jour soudaines et trop fréquentes de certaines API clés peuvent limiter la capacité des fournisseurs tiers et des clients à garantir la compatibilité de leurs services ou de leurs applications, et *in fine* leur interopérabilité, en cas de mise à jour sans rétrocompatibilité. Il est ressorti de la consultation publique menée du 17 juin au 25 juillet 2025 le besoin de préciser davantage les contours de la notion de rétrocompatibilité. Une définition proposée dans le cadre de cette consultation consiste à considérer que les mises à jour sans rétrocompatibilité sont en pratique celles qui provoquent l'échec d'une requête ou d'une opération qui aurait précédemment réussi, obligent les clients ou les fournisseurs tiers à prendre des mesures pour éviter une interruption du service, ou suppriment une caractéristique ou une fonctionnalité du service utilisée par les clients ou les fournisseurs tiers. L'Autorité considère que cette définition recouvre les cas dans lesquels une mise à jour est sans rétrocompatibilité. À cet égard, pour répondre aux difficultés causées par les mises à jour sans rétrocompatibilité, les contributeurs à la première consultation publique précitée ont proposé différents délais de préavis, compris 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 rétrocompatibilité, et que les fournisseurs mettent en place des avertissements dans ces cas de figure.

Le délai de douze mois proposé par l'Arcep a été en majorité accueilli favorablement par les contributeurs à la consultation publique menée du 17 juin au 25 juillet 2025. Néanmoins, ces contributions mentionnent que dans certains cas exceptionnels, des mises à jour sans préavis peuvent être nécessaires. C'est le cas lorsqu'une faille de sécurité est découverte dans une API et doit être corrigée au plus vite, notamment en application d'obligations légales applicables en matière de sécurité. Dans ce cas, il est recommandé d'informer les clients le plus rapidement possible.

4.2 Recommandation

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 sans rétrocompatibilité de leurs API, sauf lorsque les obligations légales applicables, ou les exigences du fournisseur en matière de sécurité et de protection de la propriété intellectuelle, imposent exceptionnellement une mise à jour rapide, auquel cas les clients devraient être informés le plus rapidement possible ;
- adoptent la spécification OpenAPI, ou des spécifications équivalentes notamment dans le cas d'API ne reposant pas sur le protocole http, pour la description et la documentation de leurs API.

³¹ <https://www.openapis.org/>

Annexe 1

Exemple illustratif de fichier au format JSON contenant les informations dont la publication est recommandée³² :

```
{
  "1": "description ou N/A",
  "2": "description ou N/A",
  "3": "description ou N/A",
  "4": "description ou N/A",
  "5": "description ou N/A",
  "6": "description ou N/A",
  "7": "description ou N/A",
  "8": "description ou N/A",
  "9": "description ou N/A",
  "10": "description ou N/A",
  "11": "description ou N/A",
  "12": "description ou N/A"
}
```

³² Ici, les valeurs renseignées sont de type *string*. Les autres types de données pour les valeurs JSON peuvent aussi être employés lorsque c'est pertinent, par exemple le type *null* lorsque l'information n'est pas applicable ou le type *array* pour les listes de plusieurs éléments. Afin de renforcer la comparabilité, il est recommandé de respecter le type *string* pour les noms. Voir la RFC pour une description des objets JSON et des types autorisés : <https://www.rfc-editor.org/rfc/rfc8259>