DATA ACT & contrat SaaS

Cadre contractuel

&

recommandations de l'ARCEP (épisode 1)

Eléonore SCARAMOZZINO, Avocate,

CONSTELLATION AVOCATS

SOMMAIRE

DATA ACT & contrat SaaS : Cadre contractuel et recommandations de l'ARCEP (épisode 1)

Depuis le **12 septembre 2025**, le **Data Act européen** (Règlement UE 2023/2854) est entré en vigueur. Il vise à fixer des règles harmonisées à l'échelle de l'Union Européenne pour l'équité et l'accès aux données. Il se lit au regard du règlement sur la gouvernance des données (règlement 2022/868 « Data Governance Act »), entré en application en septembre 2023, et qui a pour finalité de faciliter le partage des données.

Le réglement est transversal. Il est dès lors applicable à l'ensemble des domaines de l'économie numérique dans laquelle des données numériques sont collectées, analysées, stockées ou échangées entre acteurs, entreprise/entreprise (B2B) ou entreprise/ consommateur (B2C).

Avec le Data ACT / les données générées par l'utilisation d'un objet connecté ou d'un service appartiennent à l'utilisateur et non au fournisseur de services/fabricant. Le Data Act vise ainsi à permettre un accès et une valorisation des données générées notamment par les produits connectés à l'occasion de leur utilisation, dans un contexte où ces dernières sont exclusivement captées par le fabricant de ces produits.

I LES OBLIGATIONS DE LA LOI SREN : ANTICIPATION DU DATA ACT

Certaines mesures issues du Data Act 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. SREN vise notamment à 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).

1.1 Obligations tarifaires

- a**fin de traiter les barrières tarifaires au changement de fournisseur ou à l'utilisation simultanée de services cloud,** l'article 27 de la loi SREN impose des obligations tarifaires à la charge des fournisseurs de services cloud. En particulier, il interdit à tout fournisseur de cloud de facturer des frais de transfert de données dans le cadre d'un changement de fournisseur qui soient supérieurs aux coûts supportés par le fournisseur. Ces frais doivent être facturés dans le respect d'un montant maximal de tarification fixé par le ministre chargé du numérique, sur proposition de l'Arcep. De plus, l'article 27 de la loi SREN interdit à tout fournisseur de facturer des frais de transfert de données dans le cadre du multi-cloud, ou des frais de changement de fournisseur (autres que ceux liés au transfert de données), qui soient supérieurs aux coûts supportés par le fournisseur. Pour la mise en œuvre de ces obligations, l'Arcep doit publier des lignes directrices sur les coûts susceptibles d'être pris en compte dans la détermination de ces deux types de frais.

1.2 Interopérabilité-Portabilité-API

- **afin de traiter les barrières techniques au changement de fournisseur ou à l'utilisation simultanée de services cloud,** l'article 28 de la loi SREN impose aux fournisseurs de services cloud d'assurer la conformité de leurs services avec des exigences essentielles en matière d'interopérabilité, de portabilité et d'ouverture des interfaces de programmation d'applications.

L'article 29 indique que l'Arcep a pour mission de préciser les règles et les modalités de mise en œuvre de ces exigences.

> « 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 oeuvre 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. »

- ***édiction de spécifications d'interopérabilité et de portabilité***
  « *[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*** (art 29-I)».
- **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,

En outre, il précise que les fournisseurs de services cloud doivent publier et mettre à jour régulièrement une offre de référence technique d'interopérabilité précisant les conditions de mise en conformité de leurs services avec ces exigences. Enfin, certains fournisseurs de services cloud ont l'obligation de prendre les mesures raisonnables en leur pouvoir afin de faciliter une équivalence fonctionnelle dans l'utilisation du service de destination, lorsqu'il couvre le même type de fonctionnalités

II-CADRE CONTRACTUEL DU DATA ACT

2.1Quels sont les acteurs concernés par le Data Act ?

- **Entreprises** (fabricant d'objets connectés/fournisseurs de services) dès lors qu'il existe la création/collecte/traitement/partage de données et que les objets connectés et les services sont proposés à des clients/utilisateurs situés dans l'UE

  - **fabricants d'objets connectés** (Montres, voitures, appareils ménagers, machines industrielles, capteurs…, tout produit physique qui collecte ou génère des données numériques est concerné.

  - ***fournisseurs de services numériques*** liés à ces objets : Applications, plateformes, Cloud, les éditeurs de logiciels, de plateformes SaaS, ou de services cloud qui collectent, hébergent ou analysent les données issues de ces objets connectés sont aussi directement concernés.

- **Utilisateurs** : les entreprises qui utilisent ces objets connectés dans leur fonctionnement sont également concernées, en tant que bénéficiaires de droits nouveaux.

2.2.Quels sont les services concernés ?

des services de traitement de données, définis à l'article 2 du Data Act et l'article 26 de la loi SREN, et dont font partie les services cloud[1],, mais également d'autres services comme les services d'edge computing [2]..

Considérant 81

> Le concept générique de "services de traitement de données" couvre un nombre important de services ayant un très large éventail de finalités, de fonctionnalités et de configurations techniques différentes. Comme généralement compris par les fournisseurs et les utilisateurs et conformément aux normes largement utilisées, les services de traitement de données relèvent d'un ou de plusieurs des trois modèles de fourniture de services de traitement de données suivants:
>
> - l'infrastructure à la demande (IaaS),
> - la plateforme à la demande (PaaS)
> - **et le logiciel à la demande (SaaS).**
>
> Ces modèles de fourniture de services représentent une combinaison spécifique de ressources TIC proposées par un fournisseur de services de traitement de données. Ces trois modèles de base de fourniture de services de traitement de données sont complétés par de nouvelles variantes, chacune comprenant une combinaison distincte de ressources TIC, telles que le "stockage à la demande" et la "base de données à la demande".
>
> Les services de traitement de données peuvent être classés de manière plus fine et répartis dans une liste non exhaustive d'ensembles de services de traitement de données qui partagent le même objectif principal et les mêmes fonctionnalités principales ainsi que le même type de modèles de traitement de données, qui ne sont pas liés aux caractéristiques opérationnelles du service (même type de services).

[1] *Le 1° du I de l'article L. 442-12 du code de commerce auquel renvoie l'article 27 de la loi n° 2024-449 visant à sécuriser et réguler l'espace numérique (dite « loi SREN ») définit un service cloud comme étant « un service numérique fourni à un client qui permet un accès par réseau en tout lieu et à la demande à un ensemble partagé de ressources informatiques configurables, modulables et variables de nature centralisée, distribuée ou fortement distribuée, qui peuvent être rapidement mobilisées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services. »*

[2] L'edge computing (ou informatique en périphérie de réseau) est un modèle de traitement des données qui déplace le calcul et le stockage près des sources de données, comme des appareils ou des capteurs, afin de réduire la latence et d'améliorer la réactivité des systèmes.

> Les services relevant du même type de service peuvent partager le même modèle de service de traitement de données, toutefois, deux bases de données pourraient sembler partager le même objectif principal, mais après examen de leur modèle de fourniture de traitement de données, de leur modèle de distribution et des cas d'utilisation qu'ils ciblent, ces bases de données pourraient relever d'une sous-catégorie plus fine de services similaires.
>
> Des services du même type de service peuvent présenter des caractéristiques différentes et concurrentes, telles que la performance, la sécurité, la résilience et la qualité du service.

La loi SREN définit **un service d'informatique un nuage** comme un « *service numérique fourni à un client qui permet un accès par réseau en tout lieu et à la demande à un ensemble partagé de ressources informatiques configurables, modulables et variables de nature centralisée, distribuée ou fortement distribuée, qui peuvent être rapidement mobilisées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services*[3] ». Une telle définition couvre un nombre important de finalités, de fonctionnalités et de configurations techniques différentes.

Les services de traitement de données / service d'informatique cloud

L'article 29 de la loi SREN, comme l'article 30 sur le Data Act opèrent une distinction entre,

- les services d'informatique en nuage [article 29.1 ou de traitement de données (art 2.8 du Data ACT] correspondant « *à 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, traités ou déployés sur ces éléments d'infrastructure » et,*
- *« les autres services de traitement de données » ou « services d'informatique en nuage* »

Les trois catégories différentes de services cloud.

Le Data Act fait référence à trois catégories différentes de services cloud.

Considérant 81

> Le concept générique de "services de traitement de données" couvre un nombre important de services ayant un très large éventail de finalités, de fonctionnalités et de configurations techniques différentes. Comme généralement compris par les fournisseurs et les utilisateurs et conformément aux normes largement utilisées, les services de traitement de données relèvent d'un ou de plusieurs des trois modèles de fourniture de services de traitement de données suivants: l'infrastructure à la demande (IaaS), la plateforme à la demande (PaaS) et le logiciel à la demande (SaaS). Ces modèles de fourniture de services représentent une combinaison spécifique de ressources TIC proposées par un fournisseur de services de traitement de données. Ces trois modèles de base de fourniture de services de traitement de données sont complétés par de nouvelles variantes, chacune comprenant une combinaison distincte de ressources TIC, telles que le "stockage à la demande" et la "base de données à la demande". Les services de traitement de données peuvent être classés de manière plus fine et répartis dans une liste non exhaustive d'ensembles de services de traitement de données qui partagent le même objectif principal et les mêmes fonctionnalités principales ainsi que le même type de modèles de traitement de données, qui ne sont pas liés aux caractéristiques opérationnelles du service (même type de services). Les services relevant du même type de service peuvent partager le même modèle de service de traitement de données, toutefois, deux bases de données pourraient sembler partager le même objectif principal, mais après examen de leur modèle de fourniture de traitement de données, de leur modèle de distribution et des cas d'utilisation qu'ils ciblent, ces bases de données pourraient relever d'une sous-catégorie plus fine de services

[3] 1° du I de l'article L. 442-12 du code de commerce depuis l'article 27 de la loi SREN.

similaires. Des services du même type de service peuvent présenter des caractéristiques différentes et concurrentes, telles que la performance, la sécurité, la résilience et la qualité du service.

Il indique à cet égard que « comme généralement compris par les fournisseurs et les utilisateurs et conformément aux normes largement utilisées, les services de traitement de données relèvent d'un ou de plusieurs des trois modèles de fourniture de services de traitement de données suivants :

- l'infrastructure à la demande (IaaS), Infrastructure-as-a-Service
- la plateforme à la demande (PaaS), Platform-as-a-Service
- le logiciel à la demande (SaaS) Software-as-a-Service ;

Certains fournisseurs et utilisateurs peuvent aussi directement classifier les services en fonction des besoins informatiques auxquels ils répondent :

- storage-as-a-service,
- database as-a-service,
- container-as-a-service,
- AI-as-a-service, etc.

Lorsqu'il s'agira de distinguer les problématiques de portabilité et d'interopérabilité qui s'appliquent spécifiquement aux différents types de services cloud, l'ARCEP a utilisé la nomenclature **IaaS/PaaS/SaaS**. (article 29-I de la loi SREN)

IaaS	Les services IaaS sont ceux répondant à la définition s de l'article 29, I de la loi SREN. Il s'agit en particulier de services fournissant de la puissance de calcul, de la mémoire, du stockage de données et de la connectivité réseaux pour permettre à l'utilisateur d'exécuter des machines virtuelles sur lesquelles installer le système d'exploitation et les applications correspondant à ses besoins métiers
PaaS	Les services PaaS recouvrent les services intermédiaires qui permettent de développer et de déployer des applications en déléguant au fournisseur la gestion des ressources d'infrastructure sous-jacentes, et dans certains cas la gestion des mises à jour et des dépendances logicielles des applications. Leur valeur ajoutée réside dans la simplification du développement et du déploiement des applications. Parmi les services PaaS, on trouve par exemple - les bases de données hébergées, - les plateformes d'application ou - les environnements prêts à l'usage pour l'intelligence artificielle : l'utilisateur ne gère pas directement les ressources matérielles, mais il peut utiliser ces services pour construire ses propres applications.
SaaS	Les services SaaS constituent un mode de mise à disposition de solutions logicielles applicatives auprès d'utilisateurs, dont l'installation, l'hébergement et la gestion des mises à jour sont intégralement déléguées au fournisseur. Lorsqu'il utilise un logiciel SaaS, l'utilisateur dépend à la fois de l'application et des ressources informatiques allouées à son exécution par le fournisseur. Ces logiciels peuvent être très divers et couvrir de nombreux domaines tels que la gestion des ressources humaines, la gestion de la relation client (CRM), les progiciels de gestion intégrés (ERP), les suites bureautiques, etc. Les fonctionnalités varient souvent en fonction du fournisseur
« Services auxiliaires »	les fournisseurs proposent des services dits « auxiliaires », qui ne correspondent formellement ni au IaaS, au PaaS ou au SaaS. Ils concourent à la gestion et au fonctionnement d'une architecture cloud. Ceux-ci permettent par exemple de - gérer les accès des utilisateurs au sein d'une même organisation (identity & access management ou IAM), - planifier les coûts des services (billing ou facturation), ou

	- de proposer des données et des indicateurs utiles au pilotage de l'architecture (on peut parler d'observabilité des services et des applications).

En règle générale, les fournisseurs de services cloud proposent une offre de services large susceptible de couvrir l'ensemble des besoins de leurs clients dans une logique d'écosystème, c'est-à-dire qui vise à inciter les clients à confier l'ensemble de leurs besoins de services cloud actuels et futurs au même fournisseur.

Cette offre de services est constituée :

- **de services dits « standards** », que l'on retrouve chez la plupart des fournisseurs de cloud : il s'agit par exemple de certains services d'infrastructure, de services de stockage d'objets, de services d'orchestration de conteneurs[4] ou de certains systèmes de gestion de bases de données ;
- **de services dits « spécifiques »,** qui n'admettent pas d'équivalent chez les fournisseurs concurrents en termes de fonctionnalités : ces services spécifiques constituent généralement un facteur de différenciation important que ce soit en termes de valeur ajoutée (meilleure qualité de service, sécurité renforcée, intégration améliorée avec les autres services du fournisseur, etc.) ou d'innovation dans le catalogue de fonctionnalités qu'il propose.

Un outil « cloud-agnostique » est une solution capable de fonctionner sur plusieurs plateformes de cloud sans être dépendant d'un fournisseur spécifique. Il offre une couche d'abstraction qui s'adapte aux différences entre leurs environnements.

2.3-Quelles sont les obligations des fournisseurs fabricants ?

Obligations des fabricants

- concevoir leurs produits pour que les données puissent être partagées (avec l'utilisateur ou un tiers autorisé),
- garantir un accès clair, documenté et sécurisé à ces données,
- ne pas restreindre l'usage des données par l'utilisateur (sauf raisons légales de confidentialité ou de sécurité

Obligations des fournisseurs de services numériques

- respecter le droit à la portabilité des données,
- permettre le changement de fournisseur sans blocage technique ni frais abusifs,

[4] **Un conteneur** est un élément de virtualisation unique qui regroupe le code d'une application accompagné de tous les éléments nécessaires à son exécution, dont les fichiers de configuration, les bibliothèques ou les dépendances. Cette technologie permet aux développeurs de déployer leurs applications quel que soit l'environnement (machines physiques, virtuelles, hébergées sur site ou sur le cloud).

- assurer la sécurité, la confidentialité et la transparence des données traitées,
- préciser dans leurs contrats les conditions d'accès, d'usage, d'export ou de suppression des données.

La portabilité des données et des applications est au cœur des enjeux de changement de fournisseur de services cloud

Lorsqu'un client veut changer de fournisseur de services cloud, il doit migrer ses systèmes d'information depuis un environnement source vers un environnement cible. D'un point de vue technique, l'opération de migration consiste

- (i) à extraire de l'écosystème du fournisseur d'origine, les données, les applications et plus généralement tous les éléments nécessaires à leur fonctionnement,
- (ii) à les transformer si nécessaire, et
- (iii) à les intégrer dans les services de destination.

La loi SREN, ainsi que le DATA ACT, font référence à la notion de portabilité, définie notamment par la norme ISO/IEC 19941:2017 :

- **La portabilité des données** désigne « la capacité à transférer facilement des données d'un système à l'autre sans avoir à les saisir à nouveau » ;
- **La portabilité des applications** désigne « la capacité à migrer une application d'un système source vers un système cible ».

La portabilité s'apparente ainsi à la notion de réversibilité d'un service cloud, utilisée par les utilisateurs rencontrés par l'Autorité pour désigner la capacité à récupérer les données et autres actifs liés à un service cloud avant de les déployer dans un nouvel environnement.

Dans le cadre d'un changement de fournisseur, le périmètre des éléments susceptibles d'être portés par les utilisateurs est défini par la loi SREN, grâce aux notions de données exportables et d'actifs numériques.

- les **données exportables** désignent l'ensemble des données que les utilisateurs sont en droit de récupérer, et la loi SREN exclut de ce périmètre les données protégées au titre de la propriété intellectuelle ou du secret des affaires d'un tiers.
- la **notion d'actifs numériques** permet de prendre en compte la diversité des éléments qui participent au fonctionnement des services cloud et que les utilisateurs ont besoin de conserver lors d'un changement de fournisseur de services cloud. Plus précisément, ils désignent « *tous les éléments au format numérique, y compris les applications, sur lesquels le client d'un service d'informatique en nuage a un droit d'utilisation, indépendamment de la relation contractuelle que le client a avec le service d'informatique en nuage qu'il a l'intention de quitter.* »(art 28 de la loi SREN)

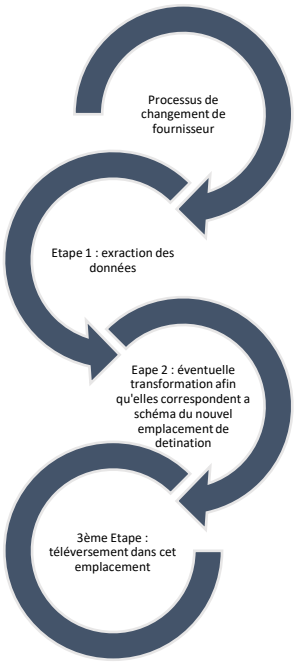
Actifs numeriques

- les applications ;
- les métadonnées décrivant les paramètres de configuration, les règles de sécurité et de gestion des droits d'accès et de contrôle ;
- «les réalisations des technologies de virtualisation, y compris les machines virtuelles et la conteneurisation [i.e. les conteneurs] »

Le processus de changement de fournisseur, selon le Data Act.

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. […]* »



L'article 30 « « Aspects techniques du changement de fournisseur » et l'article 35 « Interopérabilité des services de traitement de données » prévoient une meilleure circulation des données via

- la portabilité,
- l'interopérabilité,
- l'ouverture d'interfaces de programmation d'application (API), « 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 : « API RESTful »).

Selon l'article 35, « *35.5. 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* ». Ces normes couvrent des exigences essentielles en matière notamment d'interopérabilité et de portabilité.

Problématique de portabilité de données spécifique pour logiciel SaaS

Contrairement aux autres modèles de services cloud, un logiciel SaaS permet aux utilisateurs de disposer d'applications « clef en main », développées, maintenues et hébergées par le fournisseur. Cela signifie en pratique que les ressources matérielles (stockage et puissance de calcul) et logicielles (système d'exploitation, bases de données, etc.) nécessaires au fonctionnement de l'application SaaS sont intégralement gérées par le fournisseur. Ainsi, l'utilisateur n'a pas à se soucier des enjeux liés à l'infrastructure ou à l'environnement logiciel de l'application lors d'une migration entre des logiciels SaaS du même type.

En revanche, cette migration soulève des enjeux de portabilité des données. L'utilisateur ne disposant pas d'un accès direct aux serveurs sur lesquels ses données sont stockées par les logiciels SaaS, il doit passer par le logiciel SaaS ou son fournisseur pour les récupérer, métadonnées incluses, puis les adapter au format requis par le logiciel SaaS destinataire avant de les y injecter.

La portabilité des données et des éventuels autres actifs numériques est alors assurée soit par des interfaces graphiques, soit par des interfaces de programmation d'application (application programming interface, ou API), qui permettent de réaliser des exports. Bien qu'en général ces interfaces soient disponibles pour la plupart des services cloud de type SaaS, certains utilisateurs rencontrés constatent que des API ne sont pas toujours disponibles lorsqu'il s'agit de récupérer des données depuis un logiciel SaaS.

Par ailleurs, certains utilisateurs interrogés ont fait part de difficultés sur le périmètre des données qu'ils sont en mesure de récupérer. Il s'agirait en particulier de données qu'ils auraient utilisées ou

produites grâce à des logiciels SaaS. Ces difficultés peuvent concerner aussi bien les données qu'ils ont téléversées dans le logiciel, les données générées par son utilisation, ou encore les métadonnées liées à l'utilisation de ce service. Selon les utilisateurs, cette problématique de périmètre sur les données récupérables serait spécifique à la migration des services SaaS et ne concernerait pas les autres types de service cloud (IaaS ou PaaS).

2.4-Architecture Multi-Cloud : recours à plusieurs fournisseurs

Si la loi SREN ne définit pas spécifiquement ce qui est entendu par le recours simultané d'un client à plusieurs fournisseurs de services cloud, le considérant 99 du Règlement sur les données apporte des précisions sur l'utilisation simultanée de services de traitement de données multiples dotés de fonctionnalités complémentaires : « *[…] Sont visées les situations dans lesquelles les clients ne résilient pas un contrat pour changer de fournisseur de services de traitement de données, mais utilisent simultanément plusieurs services de différents fournisseurs, de manière interopérable, afin de bénéficier des fonctionnalités complémentaires des différents services dans la mise en place du système du client* ».

Lorsqu'un utilisateur choisit de recourir en parallèle aux services de différents fournisseurs de services cloud, c'est-à-dire de mettre en place une architecture multi-cloud, il peut avoir besoin que ces différents services puissent interagir et communiquer entre eux. La réponse à ce besoin d'interaction et de communication entre services différents est désignée sous le terme « interopérabilité », que le règlement sur les données définit comme « la capacité d'au moins deux espaces de données ou réseaux de communication, systèmes, produits connectés, applications, services de traitement de données ou composants d'échanger et d'utiliser des données afin de remplir leurs fonctions »72. Les architectures multi-cloud sont tributaires de l'interopérabilité des différents fournisseurs de services cloud. Toutefois, les besoins varient en fonction du type d'architecture multi-cloud utilisée, que l'on peut rapprocher de l'un des trois modèles suivants

Différents modèles d'architectures multi-cloud et des besoins d'interopérabilité correspondants ?

Différents modèles d'architectures multi-cloud et des besoins d'interopérabilité correspondants	Multi-cloud « siloté » : l'utilisateur a recours à plusieurs fournisseurs pour des besoins métiers différents dont les applications n'ont que peu, voire aucune, interaction ; dans cette situation, les besoins d'interopérabilité seraient limités ;
	Multi-cloud sous forme de « déploiement agnostique » : l'utilisateur fait appel à des ressources d'infrastructure de plusieurs fournisseurs, en particulier des services IaaS, et parfois à ses ressources propres afin de répartir les charges de travail entre ces ressources. Pour ce faire, il peut recourir à une plateforme de déploiement multi-cloud proposée par un fournisseur de services cloud (par exemple Azure Arc ou GCP Anthos), ou bien construire une telle plateforme en interne afin d'harmoniser les différences techniques entre les infrastructures des différents fournisseurs ; ce modèle nécessite une interopérabilité des services IaaS et des plateformes de déploiement ;
	Multi-cloud « intégré » : l'utilisateur a recours aux services de différents fournisseurs pour répondre à un même besoin métier. Par exemple, utiliser un service d'analyse de données d'un fournisseur A pour traiter les données stockées dans un service de stockage d'un fournisseur B. Cette situation présente un fort besoin en interopérabilité. Une telle situation peut se produire pour les applications souhaitant s'appuyer sur les services spécifiques proposés par des différents fournisseurs de services cloud que ce soit pour bénéficier de leurs spécificités ou limiter les évolutions du code des applications en cas de migration de celles-ci vers un autre fournisseur. Le modèle multi-cloud intégré peut également correspondre à une situation où des utilisateurs font appel à des logiciels tiers, souvent proposés en tant que SaaS, en complément d'une architecture cloud primaire (IaaS/PaaS) pour surveiller et analyser le fonctionnement de ces services primaires ou pour renforcer la cybersécurité de l'architecture. Dans ce cas de figure, des échanges de données ont lieu entre le fournisseur de services cloud primaire et les solutions tierces.

Complexité technique du changement de fournisseur et du multi-cloud : principalement due à la différenciation entre des services du même type

La consultation publique menée de l'ARCEP 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)* » a identifié la différenciation technique entre les services de même type proposés par des fournisseurs différents, comme 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. Selon les utilisateurs interrogés, les services spécifiques à un fournisseur sont techniquement difficiles à migrer. En effet, l'absence d'équivalent immédiat chez les fournisseurs concurrents nécessite une réécriture de code voire une réadaptation de l'architecture, ainsi que l'adaptation des données et des différents actifs numériques. D'après certains utilisateurs rencontrés, il serait toutefois possible de limiter la dépendance aux fournisseurs de cloud et de garantir la portabilité des applications en privilégiant des services « standards », à savoir les services dont tous les fournisseurs proposent une déclinaison, souvent compatibles entre elles, en raison de l'importance et de l'ampleur de leurs usages.

Obligations du Data Act dans le multicloud

Concernant le changement de fournisseur ou le multi-cloud, le Data Act prévoit 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 ;
- la suppression progressive des frais de changement de fournisseur, y compris les frais de transfert de données appliqués dans ce cadre, ainsi que l'interdiction, dans le cadre du multi cloud, de la facturation de frais de transfert des données supérieurs aux coûts supportés par le fournisseur ;
- une meilleure circulation des données via la portabilité, l'interopérabilité, et l'ouverture d'interfaces de programmation d'application (API).

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 Data Act prévoient 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.**

Exigences essentielles d'interopérabilité et de portabilité de la loi SREN

Pour faciliter le changement de fournisseur et le recours au multi-cloud, la loi SREN prévoit pour les fournisseurs de services cloud, une obligation de conformité de leurs services avec les exigences essentielles suivantes :

- « 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 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.

la loi SREN prévoit notamment une **obligation d'équivalence fonctionnelle imposant aux fournisseurs de services IaaS** de « pren[dre] les mesures raisonnables en leur pouvoir afin de faciliter une équivalence fonctionnelle dans l'utilisation du service de destination, lorsqu'il couvre le même type de fonctionnalités ». À ce titre, le règlement sur les données mentionne également que « *[l]e fournisseur de services de traitement de données d'origine devrait, en revanche, prendre toutes les mesures raisonnables en son pouvoir pour faciliter le processus de réalisation de l'équivalence fonctionnelle en fournissant des capacités, des informations, une documentation, une assistance technique adéquates et, le cas échéant, les outils nécessaires* »

L'ARCEP doit préciser les règles et modalités de mise en œuvre de ces exigences essentielles, notamment par l'édiction de spécifications d'interopérabilité et de portabilité (voir ci-après)

Interopérabilité : documentation des API

L'interopérabilité implique que les informations soient renseignées selon des formats interprétables, à l'aide de protocoles partagés et que les systèmes soient interconnectés par des réseaux pour pouvoir les échanger. En pratique, la mise en œuvre de l'interopérabilité entre services cloud passe par l'utilisation des API. La documentation des API permet d'informer les utilisateurs quant aux formats attendus en entrée et renvoyés en sortie. Elle serait donc essentielle pour permettre aux utilisateurs de construire des architectures où l'interopérabilité entre les services cloud est effective. Au-delà de la documentation, la disponibilité et la stabilité des API sont également essentielles pour assurer une interopérabilité effective entre différents services cloud. D'après certains utilisateurs, des changements soudains et trop fréquents de certaines API clés pourraient limiter la capacité de l'utilisateur à maintenir et adapter son architecture.

L'interopérabilité des services cloud nécessaire au développement d'architecture multi-cloud repose sur la mise à disposition par chaque fournisseur de services cloud d'API stables, documentées et accessibles depuis l'extérieur de son écosystème.

2.5-Cloud vs on Premisse : solution hybride

Pour les solutions dans le Cloud :

Les nouvelles règles du Data Act sont applicables aux éditeurs de logiciels, les clients peuvent

- **résilier leur contrat** SaaS à tout moment,
- **récupérer (portabilité et partage)** l'ensemble de leurs données,
- **changer (switching & exit)** de fournisseur sans blocage technique ni frais abusifs Plus de loock-in sur 2/3 ans comme prévus dans certains contrats

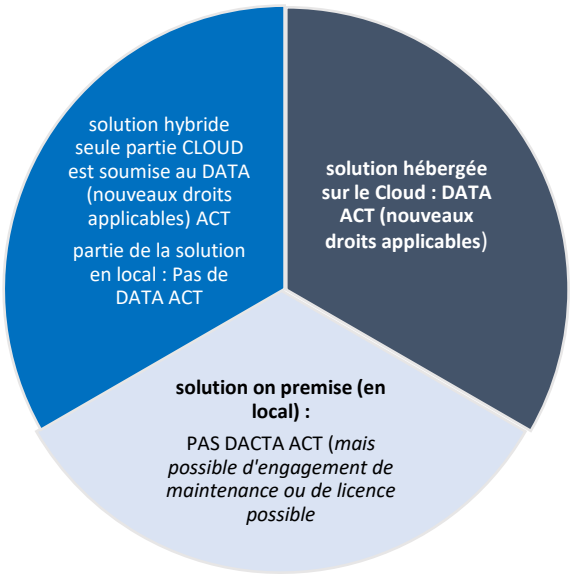
Pour des logiciels uniquement on-premise ?

- Si licence logicielle installée localement (on-premise) : Pas application du Data Act.
  - La licence logicielle locale ne relève pas du champ des "services de traitement de données".
  - Pas application des nouveaux droits du Data Act (portabilité, résiliation ou interdiction des frais).

Pour les solutions hybrides

- Si une partie du service repose sur le cloud (synchronisation, sauvegarde, support distant…) alors le Data Act s'applique uniquement à la partie cloud
  - fournisseur ne peut ni restreindre l'accès aux données, ni conditionner leur transfert à des frais abusifs, dès lors qu'elles sont hébergées à distance.
- **pour la partie purement locale (installée sur vos serveurs),** un engagement de maintenance ou de licence possible, mais *le fournisseur ne peut plus l'utiliser pour verrouiller la donnée elle-même.*

-Accès permanent
-Portabilité ; Droit à l'export complet dans un format standard (CSV, JSON, XML, etc.)
-Interopérabilité : Obligation de proposer des formats interopérables et documentés
-Résiliation anticipée (délai de préavis)
-Switching & Exit : maintien du service pendant la migration + tarification limitée aux coûts techniques réels jusqu'en 2027, puis suppression totale



2.6-Quels sont les droits des utilisateurs ?

Les utilisateurs ont le droit de :

- accéder aux données produites par leurs propres machines ou appareils,
- exploiter les données pour améliorer leur performance,
- partager les données avec d'autres partenaires ou prestataires,
- changer de fournisseur sans perdre les données.

Le Data Act vise à établir un équilibre contractuel plus juste et plus transparent entre Utilisateur / fournisseur :

- **interdiction des clauses abusives** imposées par des acteurs puissants (grands fournisseurs de cloud, éditeurs dominants, plateformes incontournables, etc.) ;
- **Accès permanent aux données de l'utilisation d'un IoT/SaaS** à tout moment par l'utilisateur : le fabricant ou le fournisseur de service ne peut plus se fonder sur le droit sui generis sur les bases de données (directive 96/9/CE) pour refuser l'accès ;
- **portabilité SaaS , cloud** à tout moment: proposer des formats d'export standardisés, assurer la continuité du service pendant la transition, et limiter ou supprimer les frais de sortie ;
- **résiliation** (« Le client peut à tout moment mettre fin à son contrat de service de traitement de données, **moyennant un préavis raisonnable**, sans frais disproportionnés ni obstacle technique. » (Article 23 du Règlement UE 2023/2854)) ;
- **changement de fournisseur à tout moment**, sans frais abusifs (tarification), pas de blocage technique (interopérailité entre les services, documentation pour importer les données, transparence sur les délais et modalités du transfert et maintien de l'accès au service jusqu'à la fin de la période de préavis ou jusqu'à la fin de la migration des données) ;
- **Les autorités publiques (collectivités, organismes de santé, autorités de sécurité civile, etc.) pourront accéder à certaines données détenues par le secteur privé, dans des situations**

d'intérêt général ou d'urgence publique (catastrophes naturelles, crises sanitaires, etc.). Cet accès doit rester proportionné et respecter la confidentialité commerciale et la protection des données personnelles. Concerne les entreprises qui détiennent des données d'intérêt public (santé, énergie, transport…)

2.7-Informations pour se conformer aux exigences de transparence du Data Act

Certaines informations revêtent un intérêt particulier pour les clients et clients potentiels de services cloud, pour renforcer leur capacité de choix. Il s'agit en particulier de celles correspondant aux informations identifiées 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 :

Considérant 95

« *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,*
- *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 influer sur le processus de changement de fournisseur;*
- *le temps considéré comme nécessaire pour achever ledit processus de changement* ».

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 ;
- 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,
- méthodes pour garantir la sécurité des données lors du transfert.

2.8-Tarification : frais de changement

Pour des mesures qui concernent les frais de changement de fournisseur, l'article 29 du Data Act prévoit

- dès **le 11 janvier 2024 et jusqu'au 12 janvier 2027**, qu'un fournisseur ne peut imposer à ses clients des frais de changement de fournisseur qui soient supérieurs aux coûts supportés par ce fournisseur et directement liés au processus de changement de fournisseur.
- **À compter du 12 janvier 2027**, les fournisseurs ne peuvent imposer aucun frais de changement de fournisseur au client pour le processus de changement de fournisseur.

La figure 1 ci-dessous présente l'articulation chronologique entre les obligations relatives aux frais de transfert de données et de changement de fournisseur introduites par la loi SREN d'une part et le règlement sur les données d'autre part.

2.8.Clauses abusives ou présumés abusives

En vue de garantir les principes d'équité et de transparence dans les relations B2B consacrés par le règlement,

.

Encadrement des clauses contractuelles imposées unilatéralement : article 13

« toute clause relative à l'accès aux données, à leur utilisation, ainsi qu'à la responsabilité ou aux recours en cas de violation ou de résiliation d'obligations liées aux données » imposée unilatéralement sans possibilité possibilité d'influencer le contenu malgré une tentative de négociation

Une clause « abusive » au sens du règlement est « d'une nature telle que son utilisation s'écarte manifestement des bonnes pratiques commerciales en matière d'accès aux données et d'utilisation des données et de responsabilité».

clause noire : clause abusive

- **visant à exclure ou à limiter la responsabilitéo de la partie qui a unilatéralement imposé la clause en cas d'actes intentionnels ou de négligence grave ;**
- **visant à exclure les voies de recours en cas d'inexécution d'obligations contractuelles** ou la responsabilité de la partie qui a unilatéralement imposé la clause en cas de manquement à ces obligations
- **de donner un droit exclusif de déterminer si les données fournies sont conformes au contrat ou d'interpréter toute clause contractuelle à la partie qui a unilatéralement imposé la clause.**

clause grise : clause présumée abusive

- **(i) de limiter les voies de recours de la partie à qui elle a été imposée unilatéralement,**
- **(ii) de permettre à la partie qui a imposé unilatéralement la clause d'avoir accès aux données de l'autre partie contractante et de les utiliser de manière qui porte gravement atteinte aux intérêts légitimes de cette autre partie, en particulier lorsque ces données contiennent des informations commercialement sensibles ou sont protégées par des secrets d'affaires ou des droits de propriété intellectuelle, ou encore**
- **(iii) de permettre à la partie qui a imposé unilatéralement la clause de modifier substantiellement le prix indiqué dans le contrat ou toute autre condition de fond liée à la nature, au format, à la qualité ou à la quantité des données à partager sans motif valable**

Application différée au 12 septembre 2027 pour les contrats longs et les contrats à durée indéterminée

Il convient d'ajouter que les dispositions relatives aux clauses contractuelles en question s'appliquent **aux contrats conclus après le 12 septembre 2025.**

Cependant, pour ne pas risquer de perturber l'équilibre des engagements les plus importants, certains contrats tels que les contrats à durée indéterminée et les contrats longs (dont l'échéance est au moins de 10 ans à compter du 11 janvier 2024, soit prenant fin au 11 janvier 2034 ou après) disposent d'un régime dérogatoire en vertu duquel le Data Act ne leur sera applicable qu'à compter du 12 septembre 2027.

III-RECOMMANDATION de l'ARCEP sur Interopérabilité et portabilité des services d'informatique en nuage 25 septembre 2025

Cette recommandation de l'ARCEP fait suite à la consultation publique du 17 juin 2025 au 18 juillet 2025, intitulée « projet de recommandation relative à l'interopérabilité et à la portabilité des services d'informatique en nuage (cloud) ;

La recommandation est dépourvue de toute portée normative.

Elle

- définit 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) ;
- 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 DATA ACT ;
- est sans préjudice des obligations de transparence, d'interopérabilité, de portabilité et d'ouverture des API issues DATA ACT et de la loi SREN.

Dans cette recommandation, l'ARCEP a souhaité des préconisations concernant,

- **les informations utiles de porter à la connaissance des clients** et clients potentiels relatives à la portabilité et l'interopérabilité des services cloud utilisés, afin de favoriser leur libre choix et pour inciter à réduire les éventuelles barrières techniques existantes.

- **les modalités pratiques de mise en oeuvre de la portabilité et de l'interopérabilité, en proposant des API stables et documentées**.

Codes de conduite SWIPO

Les codes de conduite SWIPO (Switching Cloud Providers and Porting Data), élaborés en application de l'article 6 du Data Act établissent 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 prévoyait que soit fournie, ***antérieurement à la signature d'un contrat***, *une déclaration de transparence détaillant entre autres :*

- *les données exportables ;*
- *les procédures à suivre lors d'un changement de fournisseur*.

L'initiative a pris fin, mais de nombreux acteurs de l'écosystème reconnaissent encore la pertinence du contenu de ces codes de conduite.

3.1-Publication des informations par les fournisseurs de services cloud

L'ARCEP 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,

- dans un format libre (par exemple via une page web ou un document PDF), et
- dans un format lisible par ordinateur (par exemple un fichier JSON) :

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 ;	SWIPO IaaS SCR01 et SCR02, SWIPO SaaS 3.2.7, 3.2.8 et 3.2.17
2	Procédures pour initier une migration depuis le service cloud ;	SWIPO IaaS PR01, SWIPO SaaS 3.2.1
3	Procédures pour initier une migration vers le service cloud ;	SWIPO IaaS PR02 PR05, SWIPO SaaS 3.3.1
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 ;	SWIPO IaaS PR03, SWIPO SaaS 3.2.11 et 3.2.16 SWIPO IaaS PLR04,

	• Méthodes pour garantir la sécurité des données lors du transfert (contrôle d'accès, authentification des utilisateurs, confidentialité et intégrité) ;	SWIPO SaaS 3.2.12
5	Procédures pour tester les différents mécanismes de migration, notamment ceux de sauvegarde (snapshot), de restauration (rollback) et de vérification de l'intégrité des données ;	SWIPO IaaS PLR01, SWIPO SaaS 3.2.1 et 3.2.15
6	Processus disponibles pour garantir l'intégrité des données, la continuité de service et prévenir la perte de données pendant la migration ;	SWIPO IaaS DP09, SWIPO SaaS 3.2.15
7	Processus de résiliation d'un service cloud existant, lorsque le client souhaite mettre fin à son utilisation du service après la migration ;	SWIPO IaaS PR06
8	Outils de supervision disponibles pour la migration et coûts associés à leur usage ;	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 formats ;	SWIPO IaaS PR03, SWIPO SaaS 3.2.9 et 3.2.10
10	Référence de la documentation des API permettant la mise en œuvre de la portabilité et de l'interopérabilité ;	SWIPO IaaS DP04
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.	SWIPO IaaS DP04 DP07, SCR02, SWIPO SaaS 3.2.3, 3.2.4, 3.2.5, 3.2.10, 3.2.17 et 3.2.18

Certaines de ces informations doivent déjà être contractuellement fournies aux utilisateurs dans le cadre de la loi SREN et du DATA ACT, **les articles 25 et 26 du règlement sur les données, et l'article 28 de la loi SREN.**

3.2-Mise à disposition d'API stables et documentées

Le DATA ACT 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.

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*. »

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.

Quels sont les critères pour qualifier les API de stables et documentées.

En ce qui concerne la description et la documentation,

OpenAPI est largement employé par une large majorité de fournisseurs, notamment dans le domaine du Cloud. Elle apparaît 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).

En ce qui concerne la stabilité des API

Les mises à jour soudaines et trop fréquentes de certaines API clés, lorsque ces mises à jour ne sont pas rétrocompatibles[5], peuvent limiter la capacité des fournisseurs tiers à garantir la compatibilité de leurs services, et *in fine* leur interopérabilité. Un délai de 12 mois semble accepté par l'écosystème, sauf dans les cas où les mises à jour sont nécessaires (faille de sécurité). Dans ces cas exceptionnels, les clients doivent être avertis le plus rapidement possible.

L'ARCEP ne recommande 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.**

To be continued ….

[5] 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

Pour toute information sur le sujet vous pouvez contacter *

Eléonore Scaramozzino, escaramozzino@constellation.law

constellation • law