

Réponse du CNLL à la consultation de l'ARCEP

Version: 1.1

Auteur: Stefane Fermigier (sf@fermigier.com (mailto:sf@fermigier.com)), pour le CNLL <https://cnll.fr/> (<https://cnll.fr/>)

Contexte: <https://www.arcep.fr/actualites/les-consultations-publiques/p/gp/detail/consultation-cloud-changement-fournisseur-services-architectures-tarifs-oct2024.html> (<https://www.arcep.fr/actualites/les-consultations-publiques/p/gp/detail/consultation-cloud-changement-fournisseur-services-architectures-tarifs-oct2024.html>)

Résumé exécutif

Contexte et enjeux de la consultation ARCEP

Dans le cadre de l'évolution rapide des services cloud et de l'émergence d'un oligopole d'acteurs non-européens (AWS, GCP, Google), qui plus est soumis à des lois extra-territoriales à l'étendue extrêmement large qui compromettent la confidentialité des données des individus, des entreprises et des administrations européennes, la régulation devient un enjeu stratégique pour garantir la souveraineté numérique, encourager l'innovation et protéger les droits des utilisateurs.

La consultation publique de l'ARCEP sur le **changement de fournisseur, l'interopérabilité et les pratiques tarifaires dans le cloud** intervient à un moment clé, où l'adoption massive des solutions cloud a révélé des pratiques potentiellement restrictives. Ces pratiques, telles que le verrouillage fournisseur (*vendor lock-in*) ou la facturation punitive des transferts de données, menacent la compétitivité et la résilience des écosystèmes numériques, en particulier pour les PME et les administrations publiques.

Le **Conseil National du Logiciel Libre (CNLL)**, représentant la filière française des entreprises du numérique ouvert, fort de son expertise dans le domaine des technologies libres et ouvertes, salue cette initiative et souhaite apporter une contribution détaillée, alignée sur ses valeurs fondamentales : la promotion des standards ouverts, la défense des droits des utilisateurs et le développement d'une infrastructure numérique souveraine et interopérable.

Objectifs de la contribution du CNLL

La réponse du CNLL se concentre sur plusieurs axes clés :

1. Garantir l'interopérabilité et la portabilité des services :

- Promouvoir des **standards ouverts** conformément à la définition stricte de l'EIFv1 (European Interoperability Framework) pour éviter toute dépendance propriétaire.
- Définir et encourager la notion d'**interopérabilité opposable**.
- Assurer la transparence et la fluidité des **migrations entre fournisseurs**.

2. Encourager une régulation centrée sur l'utilisateur :

- Protéger **les droits des utilisateurs** à travers des contrats clairs, des pratiques tarifaires équitables et une sécurisation des données.
- Renforcer **la cybersécurité et la résilience** des architectures cloud.

3. Soutenir les acteurs européens :

- Développer un **écosystème compétitif et souverain**, en particulier pour les PME et startups européennes, afin de réduire la domination des hyperscalers non européens.
- Mettre en avant des **solutions locales** fondées sur des technologies ouvertes, innovantes et interopérables.

4. Repenser les services cloud à travers une approche systémique :

- Articuler les problématiques de souveraineté, de cybersécurité et d'efficacité économique, dans une approche systémique plutôt que en silos.
- Créer des cadres de régulation qui favorisent l'innovation tout en encadrant les abus tarifaires et les entraves juridiques et techniques à la concurrence.

Positionnement général

Le CNLL considère que cette consultation est une opportunité de poser les bases d'un cloud **ouvert, loyal et résilient**, aligné avec les priorités européennes en matière de souveraineté numérique. En mettant l'accent sur la normalisation, la transparence et la promotion des technologies libres, cette régulation peut devenir un levier stratégique pour bâtir un écosystème cloud européen fort, concurrentiel et respectueux des utilisateurs.

Le document qui suit apporte des réponses détaillées aux différentes questions soulevées par l'ARCEP, tout en inscrivant ces propositions dans une vision globale et systémique de la régulation des services cloud.

Question 1 : Observations sur les pratiques tarifaires

Les pratiques tarifaires qui pénalisent les transferts de données entre fournisseurs cloud vont à l'encontre de la souveraineté numérique et de la lutte contre le verrouillage. Elles freinent la portabilité des données, qui est un droit fondamental des utilisateurs selon les principes de l'open source et des standards ouverts. Le CNLL défend une tarification transparente, avec des coûts alignés sur les véritables dépenses techniques, afin de permettre un accès équitable à des services interopérables.

Question 2 : Description des transferts de données et des éléments d'infrastructure

La description semble correspondre à une vision générique, mais il est essentiel de rappeler que la portabilité des données et l'interopérabilité des infrastructures doivent être garanties par des standards ouverts. En ce sens, toute complexité technique ou infrastructurelle qui limiterait ces principes doit être considérée comme une entrave, surtout si elle favorise des solutions

propriétaires.

Question 3 : Analyse des déterminants des coûts de transfert

Au-delà du transport des données et de l'interconnexion, l'utilisation de formats ou d'outils non standard par certains fournisseurs entraîne des coûts supplémentaires pour les utilisateurs souhaitant migrer leurs données. Ces coûts indirects, imposés par des solutions non interopérables, sont contraires aux principes soutenus par le CNLL, qui prône l'utilisation de standards ouverts pour minimiser ces obstacles.

Question 4 : Estimation et quantification des postes de coûts

Les coûts doivent être évalués sur la base d'une infrastructure standardisée et interopérable. Les données de référence incluent des métriques sur les coûts associés à l'utilisation de bandes passantes dédiées pour des services standards, tout en excluant les charges dues à des restrictions artificielles ou des choix techniques non standard.

Question 5 : Influence de la stratégie du fournisseur sur les coûts

Le degré d'internalisation des éléments d'infrastructure ou les accords d'interconnexion influent effectivement sur les coûts. Cependant, ces choix ne doivent pas être utilisés pour limiter artificiellement la capacité des utilisateurs à changer de fournisseur ou à construire des architectures multi-cloud, en particulier lorsque ces décisions créent des obstacles à la portabilité ou à l'interopérabilité.

Question 6 : Correspondance des coûts au dimensionnement de la bande passante

L'analyse semble valide pour des transferts de données dans des environnements standardisés. Toutefois, le CNLL insiste sur le fait que les fournisseurs ne doivent pas imposer des surcoûts liés à des choix technologiques propriétaires ou des limitations artificielles qui entravent la fluidité des migrations.

Question 7 : Gestion des pics de trafic

Si le dimensionnement du réseau est une contrainte, cela ne doit pas servir de prétexte à des pratiques tarifaires punitives ou dissuasives qui freinent la portabilité. Une infrastructure bien conçue, alignée sur les standards ouverts, doit être capable de gérer ces demandes de manière flexible.

Question 8 : Identification de la finalité des transferts

Le fournisseur peut difficilement identifier la finalité d'un transfert spécifique. Cela renforce l'importance de promouvoir des infrastructures standardisées et interopérables, réduisant la dépendance à des fournisseurs uniques. Les utilisateurs doivent pouvoir réaliser des transferts

sans subir des discriminations ou des restrictions fondées sur des usages présumés.

Question 9 : Transferts de données comme événements non récurrents

La migration liée à un changement de fournisseur est effectivement un événement ponctuel et souvent planifié. Le CNLL soutient que les coûts liés à de tels transferts doivent être transparents et ne pas impliquer de frais cachés, afin de garantir la liberté des utilisateurs de choisir leurs fournisseurs.

Question 10 : Déploiement d'équipements supplémentaires

Un transfert de données dans le cadre d'un changement de fournisseur ne doit généralement pas nécessiter d'équipements supplémentaires. Si des coûts spécifiques sont invoqués, ils doivent être justifiés et établis à partir des critères objectifs, sans pénaliser indûment l'utilisateur.

Question 11 : Coût incrémental nul pour les transferts

Le coût incrémental pour un transfert ponctuel est proche de zéro dans un environnement bien dimensionné. Toute tentative de facturer des coûts additionnels non justifiés est un frein artificiel à la portabilité des données, ce qui va à l'encontre des principes défendus par le CNLL.

Question 12 : Cas justifiant une facturation des transferts

Les transferts de données ne doivent entraîner des frais que dans des cas exceptionnels, comme une migration nécessitant des services spécifiques ou un support technique avancé. Cependant, ces coûts doivent être proportionnés, transparents et ne pas décourager les utilisateurs de migrer vers des solutions plus adaptées ou ouvertes.

Question 13 : Plafond des frais de transfert fixé à zéro

Le CNLL soutient l'idée que la portabilité des données est un droit fondamental pour éviter le verrouillage. Fixer les frais de transfert à zéro revient à aligner les pratiques tarifaires avec cet objectif, encourageant la concurrence et protégeant les utilisateurs, notamment les PME, contre des coûts excessifs. Toutefois, cela suppose que les fournisseurs intègrent les coûts nécessaires dans leurs stratégies de tarification globale et ne cherchent pas à les répercuter sous d'autres formes.

Question 14 : Caractère récurrent des transferts multi-cloud

Les transferts de données dans un environnement multi-cloud peuvent présenter des volumes variables et des besoins en flexibilité. Cependant, une infrastructure bien conçue et des outils cloud-agnostiques (comme les plateformes open source favorisées par le CNLL) peuvent

réduire la complexité technique et les coûts liés à ces transferts. Par conséquent, l'analyse de l'Autorité est valide, mais il est crucial d'encourager les solutions interopérables et ouvertes pour limiter ces contraintes.

Question 15 : Équipements ou actions spécifiques pour le multi-cloud

Les fournisseurs peuvent avoir besoin de mettre en œuvre des mécanismes d'interconnexion optimisés, tels que des passerelles API standardisées ou des services spécifiques à la synchronisation des données. Ces actions doivent toutefois s'appuyer sur des standards ouverts pour éviter des barrières techniques ou des dépendances à des solutions propriétaires, conformément aux principes du CNLL.

Question 16 : Postes de coûts liés au multi-cloud

Les principaux coûts liés au multi-cloud incluent :

- L'interconnexion entre différents fournisseurs ;
- La synchronisation des données en temps réel ;
- L'adaptation des formats ou protocoles si les standards ne sont pas respectés.

Pour allouer ces coûts, il est pertinent de s'appuyer sur des indicateurs tels que :

- Le volume de données transféré ;
- La fréquence des transferts ;
- Les exigences de latence ou de performance.

Ces éléments doivent être évalués en tenant compte des bénéfices des solutions cloud-agnostiques et de l'importance des standards ouverts.

Question 17 : Clients aux besoins spécifiques

Les clients nécessitant des transferts de très gros volumes de données ou des transferts à faible latence (e.g., dans des secteurs critiques comme la finance ou la santé) pourraient se voir imposer des coûts supplémentaires. Toutefois, ces besoins spécifiques ne doivent pas justifier des pratiques discriminatoires ou pénalisantes pour les petites structures.

Question 18 : Prestations liées au changement de fournisseur

La mise à disposition de main-d'œuvre pour soutenir le changement de fournisseur est essentielle, notamment pour :

- La préparation des données (extraction et transformation) ;
- L'assistance technique pour l'adaptation des scripts ou configurations ;
- La formation liée à l'utilisation des nouveaux outils.

Les coûts associés doivent être transparents et non utilisés comme un levier pour maintenir le

verrouillage.

Question 19 : Prestations supplémentaires dans le cadre du changement de fournisseur

Outre la mise à disposition de main-d'œuvre, les fournisseurs doivent offrir :

- Des outils standardisés d'export et de transformation des données ;
- Une documentation technique exhaustive pour garantir la portabilité ;
- Un support pour garantir une transition fluide vers des environnements multi-cloud.

Ces prestations doivent être alignées sur les principes de transparence et d'ouverture soutenus par le CNLL.

Question 20 : Remarques sur les frais de changement de fournisseur

Les frais de changement de fournisseur doivent être strictement encadrés pour éviter tout abus. Ils doivent refléter uniquement les coûts réels et nécessaires pour garantir une migration fluide, sans créer de barrières financières injustifiées, particulièrement pour les PME.

Question 21 : Liste des services cloud (IaaS)

La liste des services IaaS semble pertinente, mais il est important de préciser que ces services doivent être conçus pour faciliter la portabilité et l'interopérabilité. Les outils open source et les standards ouverts doivent être mis en avant pour éviter toute dépendance à des solutions propriétaires.

Des services complémentaires comme l'utilisation d'outils d'**Infrastructure-as-Code** (IaC) open source ou des solutions de monitoring cloud-agnostiques pourraient également être inclus dans cette définition, car ils jouent un rôle clé dans la gestion des infrastructures multi-cloud.

Question 22 : Typologies et définitions des autres services cloud mentionnés à l'article 29, I de la loi SREN

Les typologies et définitions proposées par l'Arcep (IaaS, PaaS, SaaS) sont pertinentes pour encadrer les discussions sur l'interopérabilité et la portabilité. Cependant, pour mieux refléter les enjeux du logiciel libre, il est important de souligner le rôle des **standards ouverts** et des **solutions interopérables**, particulièrement pour les services PaaS et SaaS, où les risques de verrouillage sont plus élevés. Une meilleure distinction doit être faite entre les services ouverts et propriétaires pour favoriser les choix éclairés des utilisateurs. Des définitions comme celles de L'Open Cloud Manifesto, les niveaux d'ouverture défini par l'association TIO Libre, les services cloud "loyaux", ou encore le concept de cloud "Hyper Open" (open source software + open hardware + open procedure) doivent être discutées et adoptées. Voici ce que nous proposons:

Un **service cloud réversible** est un service qui peut être reproduit librement par un tiers, sans restrictions ni coût de licence. Cela implique que le code source de ce service soit sous licence libre, et que ses procédures de mise en œuvre soient documentées.

Question 23 : Distinction entre services « standards » et « spécifiques »

La distinction entre services « standards » et « spécifiques » est utile pour évaluer les défis techniques de la migration. Cependant, il est crucial que cette distinction soit accompagnée d'un effort accru pour promouvoir les **services fondés sur des standards ouverts**, considérés comme "standards" au sens pratique. Ces services offrent une meilleure portabilité et interopérabilité, éléments essentiels pour limiter le verrouillage des fournisseurs et encourager la compétitivité, particulièrement pour les PME.

Question 24 : Couverture des besoins par les outils « cloud-agnostiques »

Les outils cloud-agnostiques répondent efficacement à certains besoins des utilisateurs, notamment pour le provisionnement des infrastructures (IaC), l'orchestration des conteneurs et l'observabilité. Cependant :

- Ces outils ne couvrent pas toujours des fonctionnalités spécifiques comme les bases de données propriétaires ou des services IA intégrés.
- Des efforts supplémentaires sont nécessaires pour étendre ces outils à des fonctionnalités plus complexes et standardiser les interfaces API des services propriétaires. Cela montre l'importance de soutenir les **solutions open source** qui permettent de combler ces lacunes.

Question 25 : Définition des actifs numériques

La liste des actifs numériques identifiée par l'Arcep est complète et pertinente, incluant les applications, métadonnées, conteneurs et machines virtuelles. Cependant, des actifs supplémentaires pourraient être pris en compte :

- **Scripts d'infrastructure as code** (Terraform, Ansible, Chef, Puppet, SaltStack, Pyinfra, BundleWrap, CFEngine...), souvent essentiels pour redéployer des environnements dans un nouveau cloud.
- **Clés et certificats de sécurité** associés aux environnements de production.
- **Dépendances externes ou modules tiers** utilisés par les applications, qui peuvent être critiques pour garantir une transition fluide.

Question 26 : Description du processus standard de migration

La description fournie reflète bien le processus standard pour les services IaaS. Cependant,

des étapes complémentaires peuvent être nécessaires :

- Validation de la **compatibilité des configurations réseau** entre l'ancien et le nouveau fournisseur.
- Synchronisation et tests des environnements pour garantir la continuité des services avant la migration complète.
- Gestion des **dépendances logicielles** spécifiques aux applications, notamment celles non disponibles chez le fournisseur de destination.

Question 27 : Absence de difficultés techniques significatives pour les services IaaS

La migration des services IaaS est effectivement moins sujette à des difficultés techniques significatives grâce à leur standardisation relative. Toutefois, certaines situations peuvent poser problème :

- **Complexité des configurations réseau complexes**, telles que les VPN ou les pare-feu.
- Utilisation de **technologies propriétaires spécifiques** (e.g., disques virtuels non standardisés). Pour résoudre ces difficultés, il sera utile d'encourager l'utilisation d'outils open source et d'établir des normes plus strictes pour la compatibilité inter-cloud.

Question 28 : Absence de freins à l'équivalence fonctionnelle pour les services IaaS

L'absence de freins techniques majeurs à l'équivalence fonctionnelle pour les services IaaS est plausible, mais elle dépend fortement du degré d'adoption des standards ouverts. Si un fournisseur utilise des formats ou des outils propriétaires non compatibles avec des solutions standardisées (e.g., formats de disques, configurations réseau), cela peut compliquer la migration. Il est essentiel de promouvoir l'utilisation de technologies interopérables.

Question 29 : Description du processus de migration pour les services PaaS

La description est correcte, mais il convient d'ajouter les points suivants :

- **Adaptation des dépendances logicielles** : par exemple, si une base de données propriétaire est utilisée, des outils de migration ou des scripts spécifiques seront nécessaires.
- **Compatibilité des conteneurs** : si les conteneurs utilisent des configurations spécifiques à un fournisseur (e.g., services d'orchestration non standards), cela peut nécessiter une modification.
- **Tests approfondis** : avant la mise en production, des tests doivent être réalisés pour s'assurer que l'application fonctionne correctement dans le nouvel environnement.

Question 30 : Difficultés techniques de migration pour les

services PaaS

Les principales difficultés techniques sont bien liées à l'utilisation de services spécifiques au fournisseur. Toutefois, d'autres facteurs peuvent compliquer la migration :

- **Dépendances étroites avec les outils DevOps du fournisseur d'origine**, nécessitant par exemple une réécriture des pipelines CI/CD.
- **Services propriétaires intégrés**, tels que les fonctions serverless ou les APIs d'IA, difficiles à remplacer. Pour surmonter ces obstacles, il est crucial de favoriser l'utilisation de standards ouverts et d'encourager les fournisseurs à documenter clairement leurs services pour faciliter la portabilité.

Question 31 : Services spécifiques freinant la migration et recommandations

Les services spécifiques suivants posent des freins majeurs à la migration vers d'autres fournisseurs :

1. **Bases de données propriétaires** : les bases non standardisées, comme Amazon Aurora ou Google Spanner, nécessitent des adaptations complexes pour les données et les requêtes SQL.
2. **Services d'intelligence artificielle et de machine learning** : les API propriétaires (e.g., Google AI Platform, AWS SageMaker) créent une forte dépendance pour les entreprises utilisant des modèles entraînés ou des pipelines spécifiques.
3. **Outils DevOps intégrés** : les solutions CI/CD spécifiques (comme AWS CodePipeline) compliquent la réutilisation des scripts et des pipelines.
4. **Services serverless** : des solutions comme AWS Lambda avec intégrations spécifiques rendent les migrations complexes sans une réécriture substantielle des fonctions.

Recommandations :

- **Favoriser les standards ouverts** : par exemple, promouvoir des bases de données open source respectant les standards, comme par exemple PostgreSQL.
- **Imposer la documentation exhaustive des APIs** : fournir des guides de migration vers des services équivalents.
- **Encourager les outils cloud-agnostiques** : investir dans des solutions de déploiement ou d'orchestration qui réduisent la dépendance aux environnements spécifiques.
- **Priorité** : les services de bases de données devraient être harmonisés en premier, car ils sont fondamentaux pour les applications critiques.

Question 32 : Difficultés techniques de migration liées aux services auxiliaires

Les principaux services auxiliaires freinant la migration incluent :

1. **Gestion des identités et des accès (IAM)** : les politiques IAM propriétaires sont difficiles

à répliquer, et leur synchronisation entre environnements multi-cloud peut poser des risques de sécurité.

2. **Outils de surveillance et d'observabilité** : les services comme CloudWatch (AWS) ou Stackdriver (Google) utilisent des formats et des métriques non standardisés.
3. **Systèmes de gestion des coûts et de facturation** : les outils intégrés au cloud sont souvent exclusifs et ne permettent pas une vision consolidée en multi-cloud.

Recommandations :

- **Normalisation des services IAM** : développer des standards communs pour la gestion des accès (interopérabilité des politiques et outils cloud-agnostiques comme Keycloak).
- **Standardisation des métriques** : imposer l'utilisation de formats ouverts comme OpenTelemetry pour la surveillance.
- **Priorité** : la gestion des identités est critique pour la sécurité et devrait être traitée en priorité.

Question 33 : Processus standard de migration d'un logiciel SaaS

Le processus décrit par l'Autorité est globalement correct. Cependant, il manque certaines étapes clés :

1. **Évaluation des dépendances fonctionnelles** : identifier les fonctionnalités spécifiques au logiciel SaaS source pour évaluer les besoins d'adaptation.
2. **Récupération des métadonnées** : en plus des données utilisateurs, récupérer les logs d'utilisation, paramètres de configuration et données analytiques.
3. **Transformation des formats de données** : convertir les données exportées au format requis par le logiciel SaaS cible.

Question 34 : Difficultés pour la récupération des données liées à un service SaaS

Les difficultés principales incluent :

1. **Absence d'API ouvertes** : certains fournisseurs SaaS ne fournissent pas d'outils pour extraire les données de manière automatisée.
2. **Format propriétaire des données** : les données exportées peuvent nécessiter des outils spécifiques pour être lisibles.
3. **Manque de support technique** : certains fournisseurs limitent leur assistance dans le cadre d'une migration, rendant le processus plus complexe.

Contexte : ces problèmes sont exacerbés dans des environnements où les données traitées sont volumineuses ou hétérogènes (e.g., suites ERP ou CRM).

Question 35 : Détermination du périmètre des données exportables

La détermination du périmètre des données exportables est effectivement un enjeu majeur, particulièrement pour les services SaaS. Les difficultés incluent :

- **Délimitation des données générées** : certains fournisseurs incluent des données qu'ils considèrent comme leur propriété intellectuelle (e.g., algorithmes dérivés).
- **Manque de clarté contractuelle** : les contrats n'identifient pas toujours explicitement quelles données sont exportables.

Pour les autres services (IaaS, PaaS), ce problème est moins fréquent, bien que des ambiguïtés puissent exister sur les métadonnées ou les configurations spécifiques.

Question 36 : Définition du périmètre des données exportables

Le périmètre des données exportables dans les contrats doit notamment inclure :

1. **Données utilisateur** : tout contenu importé ou généré par l'utilisateur.
2. **Métadonnées associées** : paramètres de configuration, logs d'utilisation et toute donnée décrivant l'utilisation du service.
3. **Formats standardisés** : exiger que les données soient exportées dans un format ouvert et interopérable (e.g., JSON, CSV, SQL dumps).

Question 37 : Difficultés pour convenir du périmètre des données exportables

Les difficultés incluent :

1. **Propriété intellectuelle ambiguë** : certains fournisseurs revendiquent la propriété des algorithmes ou des données dérivées générées par le SaaS.
2. **Inaccessibilité des métadonnées** : les fournisseurs ne fournissent pas toujours d'accès aux journaux ou aux configurations détaillées.
3. **Lacunes dans les contrats** : peu de précisions sur le format et la granularité des données récupérables.

Question 38 : Autres difficultés techniques lors d'un changement de fournisseur

- **Synchronisation des environnements en temps réel** : lors de migrations critiques, garantir la continuité des opérations peut être un défi.
- **Problèmes de compatibilité réseau** : répliquer des configurations complexes (e.g., VPN, règles de pare-feu) peut entraîner des interruptions de service.
- **Temps d'arrêt imprévus** : le transfert de grandes quantités de données peut nécessiter des temps d'arrêt prolongés.

Question 39 : Modèles d'architectures multi-cloud et interopérabilité

La description des modèles est cohérente, mais l'importance des standards ouverts devrait être davantage soulignée :

- **Interopérabilité dans les modèles intégrés** : les besoins sont critiques pour des services collaborant entre plusieurs fournisseurs.
- **Plateformes cloud-agnostiques** : encourager l'adoption de solutions open source pour standardiser les interactions.

Question 40 : Cas d'usage pour une architecture « multi-cloud intégré »

Cas d'usage :

1. **Résilience accrue** : Répartition des charges de travail entre plusieurs fournisseurs pour limiter les risques de panne.
2. **Optimisation des coûts** : Utilisation de services spécialisés de différents fournisseurs pour un même projet.
3. **Conformité réglementaire** : Hébergement des données dans des juridictions spécifiques tout en utilisant des services globaux.

Freins à l'interopérabilité :

- **Manque de standards pour les API** : Certaines solutions ne documentent pas suffisamment leurs interfaces.
- **Absence de synchronisation IAM** : Gestion complexe des accès dans un environnement multi-cloud.

Recommandations :

1. **Développer des standards européens** pour l'interopérabilité et la gestion des accès.
2. **Soutenir les outils cloud-agnostiques** qui simplifient la gestion des environnements multi-cloud.

Question 41 : Interopérabilité via des API disponibles, stables, documentées et accessibles

Oui, l'interopérabilité des services cloud repose sur la disponibilité, la stabilité, la documentation et l'accessibilité des API, pour les raisons suivantes :

1. **Disponibilité et accessibilité** : les API doivent être accessibles depuis l'extérieur des écosystèmes propriétaires pour permettre l'interconnexion avec des systèmes tiers, notamment dans des architectures multi-cloud.
2. **Documentation** : une documentation claire garantit que les utilisateurs peuvent comprendre et intégrer les API efficacement.
3. **Stabilité** : la stabilité réduit les coûts liés aux modifications imprévues, ce qui est essentiel pour maintenir des services fonctionnels dans des environnements complexes.

4. **Support des standards ouverts** : les API ouvertes et conformes à des standards garantissent l'interopérabilité et limitent le verrouillage fournisseur.

Question 42 : Informations et critères pour les API

Informations minimales dans la documentation :

1. Description des fonctionnalités de l'API.
2. Formats des données acceptées (JSON, XML, etc.).
3. Méthodes d'authentification et de sécurisation (OAuth, clés API).
4. Exemples d'utilisation avec code source.
5. Gestion des erreurs et messages de retour.
6. Changements de version (changelog).
7. Limites de performance (e.g., taux d'appels, latence).

Critères de stabilité :

- **Versionnement clair** : utilisation de numéros de version pour indiquer les modifications majeures et mineures (i.e. *semantic versioning*).
- **Préavis pour les modifications** : les mises à jour majeures doivent être annoncées avec un préavis d'au moins six mois.
- **Période de dépréciation** : les anciennes versions d'API devraient être maintenues pendant une période transitoire.
- **Tests de compatibilité** : documentation des tests pour garantir la rétrocompatibilité.

Question 43 : Autres modèles d'interopérabilité

Outre les API, les modèles suivants peuvent favoriser l'interopérabilité :

1. **Protocole standardisé** : utilisation de protocoles comme REST, GraphQL, JSON-RPC ou encore gRPC.
2. **Fichiers d'échange** : transferts de données via des formats ouverts (e.g., JSON, CSV, Parquet).
3. **Connecteurs natifs ou plug-ins** : des modules intégrés pour connecter directement les services (e.g., connecteurs pour OpenTelemetry ou Prometheus).
4. **Interopérabilité au niveau des conteneurs** : standardisation autour d'OCI pour les déploiements d'applications.

Question 44 : Enjeux techniques relatifs au changement de fournisseur et au multi-cloud

1. **Standardisation insuffisante des métadonnées** : les données descriptives liées aux configurations cloud (e.g., IAM, sécurité) manquent de standardisation.
2. **Manque d'outils de gestion multi-cloud** : les outils disponibles ne couvrent pas tous les

cas d'usage, notamment pour les architectures complexes.

3. **Latence inter-cloud** : les performances peuvent être affectées lors de l'intégration de services de différents fournisseurs.
4. **Sécurité des transferts de données** : les migrations ou synchronisations en multi-cloud augmentent les risques liés à la confidentialité et à l'intégrité des données.

Question 45 : Codes de conduite pertinents

Droits de l'utilisateur et transparence

La régulation des services cloud doit impérativement renforcer les droits des utilisateurs tout en garantissant la transparence des pratiques des fournisseurs.

Nos recommandations sont structurées autour des droits fondamentaux des utilisateurs :

- **Audits et journaux** :

- Tous les événements critiques doivent être enregistrés de manière sécurisée et accessibles aux utilisateurs (consultation en ligne ou téléchargement).
- Les mécanismes de monitoring doivent respecter la vie privée et se limiter aux aspects essentiels à la fourniture des services, avec des contrôles optionnels laissés à l'utilisateur.

- **Facturation transparente** :

- Les fournisseurs doivent proposer des factures détaillées permettant de valider les éléments de coût.
- Des mécanismes de plafonnement des dépenses doivent être disponibles pour éviter les surprises tarifaires.
- L'accès aux données de consommation, en temps réel et historiques, est crucial pour aider les utilisateurs à mieux anticiper leurs besoins.

- **Sauvegardes et accès aux données** :

- Les utilisateurs doivent pouvoir accéder à leurs données (y compris les métadonnées et configurations) en masse et sans restrictions excessives (pas de limitation en deçà de 30 jours).
- Les fournisseurs doivent garantir une redondance des données pour prévenir les pertes en cas de sinistre.

- **Interfaces (API)** :

- Les API doivent être documentées avec des spécifications ouvertes et garantir une stabilité permettant aux utilisateurs de s'adapter en cas de mise à jour ou d'obsolescence programmée.
- Une période de transition raisonnable pour les API dépréciées est indispensable.

Standards juridiques et éthiques

Les aspects juridiques et éthiques sont fondamentaux pour garantir un écosystème cloud équitable et sécurisé.

- **Contrats clairs et modifiables :**

- Les contrats doivent être rédigés dans un langage accessible, avec des clauses qui permettent à l'utilisateur de résilier facilement en cas de modifications défavorables.
- Les modifications majeures des services doivent être notifiées plusieurs mois à l'avance, en particulier pour les fermetures de services.

- **Conformité légale et protection des données :**

- Les fournisseurs doivent s'engager à notifier les utilisateurs des demandes d'accès gouvernementales (sauf interdictions légales) et clarifier les juridictions applicables.
- Les politiques de traitement des données doivent respecter les lois de protection des données (RGPD, etc.).

Sécurité et garantie de service

Une approche proactive et systémique de la cybersécurité est essentielle :

- **Sécurité des données et des accès :**

- Les authentifications fortes et les protections de transport (TLS/SSL) doivent être la norme.
- Une isolation stricte entre les utilisateurs dans des environnements multitenants doit être garantie.
- Les options de purge immédiate et sécurisée des données doivent être offertes sur demande.

- **Assurance qualité :**

- Les SLA doivent inclure des engagements explicites et contraignants, notamment sur la disponibilité et les délais de réponse (p. ex., réponse en moins d'une heure pour les incidents critiques).
- Les pénalités financières pour non-respect des SLA doivent être proportionnelles aux impacts subis par l'utilisateur.

Interopérabilité et portabilité

L'interopérabilité technique et juridique est un élément central des codes de conduite pour un écosystème cloud ouvert et compétitif :

- **Standards ouverts :**

- L'utilisation de standards établis (REST APIs, formats d'échange de données standardisés) doit être prioritaire.
- Les formats propriétaires ne doivent pas entraver l'innovation ni la flexibilité des utilisateurs.

- **Portabilité des données :**

- Les fournisseurs doivent garantir la migration sans obstacle technique ou tarifaire.
- Les utilisateurs doivent conserver la propriété de leurs données, y compris les métadonnées et configurations associées.

- **Projets soutenant l'interopérabilité :**

- L'intégration de bibliothèques open source, tels qu'Apache Libcloud, peut favoriser des transitions simplifiées entre différents fournisseurs.

Gouvernance et pratiques éthiques

Les principes éthiques doivent sous-tendre la gouvernance des fournisseurs de cloud pour assurer une conduite équitable :

- **Transparence sur la localisation des données :**

- Les utilisateurs doivent être informés des emplacements physiques de stockage et de traitement de leurs données, avec une préférence pour des solutions localisées selon leurs besoins.

- **Évolutions des standards :**

- Les fournisseurs doivent participer activement au développement de standards ouverts tout en respectant les normes établies.

S'ils intègrent ces principes dans un cadre de régulation structuré, les codes de conduite peuvent contribuer à bâtir un écosystème cloud **sécurisé, transparent, interopérable et centré sur l'utilisateur**, renforçant ainsi la confiance et la compétitivité des solutions européennes. Ces recommandations sont cohérentes avec les initiatives anciennes comme l'Open Cloud Manifesto ou TIO Libre, tout en les adaptant aux enjeux actuels de souveraineté et de cybersécurité.

Question 46 : Mesures pour l'équivalence fonctionnelle

Mesures actuelles :

- **Templates standardisés** pour les configurations d'infrastructure.
- **Outils IaC cloud-agnostiques** comme Terraform, Ansible, Chef, Puppet, SaltStack, Pyinfra, BundleWrap ou CFEngine, pour simplifier la migration.

Recommandations :

1. **Fournir des guides détaillés** pour répliquer les configurations sur des plateformes tierces.
2. **Normaliser les formats des machines virtuelles et conteneurs** pour une réutilisation facile.

Question 47 : Informations minimales dans l'offre de référence

technique

1. **Description fonctionnelle des services** : caractéristiques et cas d'usage.
2. **Compatibilité** : formats de données, protocoles et standards supportés.
3. **Exigences matérielles et logicielles** : dépendances pour les déploiements.
4. **Plan de migration** : étapes techniques et outils recommandés.
5. **Limites techniques** : restrictions ou incompatibilités potentielles.

Question 48 : Utilisation de l'offre de référence technique pour la spécificité des services

L'offre de référence technique est un bon moyen d'informer les utilisateurs sur la spécificité des services. Harmoniser sa présentation favorisera la transparence et facilitera les comparaisons entre fournisseurs. Les éléments spécifiques à inclure sont notamment :

- Caractère exclusif ou standardisé d'un service.
- Indicateurs de compatibilité multi-cloud.
- Support aux outils cloud-agnostiques.

Question 49 : Normalisation des services IaaS

L'analyse de l'Autorité selon laquelle il existe un faible besoin de normalisation supplémentaire dans les services IaaS est globalement recevable, notamment en raison des efforts déjà engagés dans la communauté open source depuis le projet Compatible One en 2010, et des solutions existantes qui tendent à promouvoir des standards. Cependant, pour maximiser l'interopérabilité, réduire les dépendances propriétaires et renforcer l'écosystème européen, certaines initiatives supplémentaires de normalisation mériteraient d'être soutenues.

Axes prioritaires pour la normalisation des services IaaS

1. Standards de configurations réseau

- **Enjeu** : Les configurations réseau (règles de pare-feu, VPN, routage, load balancing, etc.) varient largement entre les fournisseurs, créant des barrières à la migration et aux déploiements multi-cloud.
- **Propositions** :
 - Harmoniser les formats et protocoles utilisés pour les configurations réseau.
 - Adopter des API standardisées pour la gestion des ressources réseau virtuelles (inspirées, par exemple, par les initiatives issues du projet Open Daylight).
 - Soutenir les travaux autour de SDN (Software Defined Networking) dans des environnements ouverts.

2. Formats de stockage

- **Enjeu** : L'absence de standards interopérables pour les snapshots, disques virtuels et objets de stockage freine la réversibilité et la portabilité.

- **Propositions :**
 - Favoriser l'adoption de formats de stockage ouverts tels que VMDK, QCOW2 et l'interopérabilité entre différents systèmes de fichiers distribués (GlusterFS, Ceph, Minio, etc.).
 - Normaliser les API d'accès au stockage pour garantir la portabilité des volumes et objets entre fournisseurs.

3. Interopérabilité des API IaaS

- **Enjeu :** Les API propriétaires limitent la flexibilité des utilisateurs et rendent complexes les stratégies multi-cloud.
- **Propositions :**
 - Soutenir des frameworks d'abstraction comme par exemple **Apache Libcloud**, qui permet une gestion unifiée des ressources IaaS sur plusieurs fournisseurs.
 - Travailler sur des standards API communs pour les opérations fondamentales (création de machines virtuelles, gestion des réseaux, provisionnement de ressources).
 - Promouvoir des initiatives telles que le **Cloud Infrastructure Management Interface (CIMI)** de la DMTF, qui fournit un modèle standard pour la gestion des infrastructures cloud.

4. Observabilité et monitoring

- **Enjeu :** L'observabilité des performances varie selon les fournisseurs, compliquant la gestion et le suivi des environnements multi-cloud.
- **Propositions :**
 - Adopter des standards tels qu'**OpenTelemetry** pour collecter et analyser les données de performance et de logs dans des environnements hétérogènes.
 - Standardiser les métriques de base pour les services IaaS (CPU, mémoire, stockage, réseau) afin de garantir une comparaison uniforme.

5. Gestion des identités et des accès (IAM)

- **Enjeu :** Les systèmes IAM sont souvent fermés, avec des mécanismes spécifiques à chaque fournisseur.
- **Propositions :**
 - Normaliser les mécanismes d'authentification et de fédération d'identités (par exemple, via des standards tels que SAML ou OpenID Connect).
 - Encourager l'interopérabilité des politiques IAM entre fournisseurs, facilitant ainsi les stratégies multi-cloud.

Enjeux stratégiques

1. Souveraineté numérique

- La normalisation des IaaS permettrait de renforcer la souveraineté numérique européenne en réduisant la dépendance aux hyperscalers nord-américains.
- En adoptant des standards ouverts, les solutions européennes pourraient garantir une

meilleure portabilité des données et des services, contribuant ainsi à la réinternalisation des données critiques.

2. Compétitivité européenne

- La création d'un écosystème cohérent de standards IaaS permettrait de stimuler l'innovation en Europe, notamment pour les PME et startups. Cela renforcerait l'offre locale face à des géants comme AWS ou Azure.

Impact attendu des efforts de normalisation

- **Facilitation des migrations** : une harmonisation des configurations réseau, des formats de stockage et des API, simplifierait les migrations entre fournisseurs, réduisant les coûts et les délais.
- **Interopérabilité accrue** : des API standardisées et des outils d'abstraction comme Apache Libcloud faciliteraient l'intégration des stratégies multi-cloud.
- **Sécurité renforcée** : une observabilité normalisée contribuerait à une meilleure gestion des risques opérationnels et de cybersécurité.

Question 50 : Normalisation des services PaaS

La normalisation des services PaaS pourrait jouer un rôle clé dans la simplification des migrations, l'interopérabilité entre plateformes et le développement d'architectures multi-cloud. L'objectif n'est pas de freiner l'innovation, mais de fournir un socle commun pour certains services critiques, tout en favorisant la flexibilité et l'efficacité pour les utilisateurs. Une normalisation bien ciblée peut notamment faciliter l'adoption des principes des "12 Factor Apps", qui promeuvent des pratiques modernes pour le développement d'applications cloud-native. Une réflexion par rapport au manifeste initial des "12-Factor Apps", paru en 2011, semble néanmoins nécessaire pour intégrer les évolutions des pratiques identifiées dans le manifeste, ainsi que d'autres pratiques qui se sont démocratisées depuis.

Cf. par exemple: [https://lab.abilian.com/Tech/Cloud/The 12 Factor App/](https://lab.abilian.com/Tech/Cloud/The%2012%20Factor%20App/) (<https://lab.abilian.com/Tech/Cloud/The%2012%20Factor%20App/>)

Axes de normalisation prioritaires

1. Bases de données managées

Les bases de données managées sont souvent au cœur des applications PaaS, mais leur hétérogénéité rend leur migration complexe.

- **Recommandations** :
 - Harmoniser les formats de sauvegarde et d'exportation pour permettre une portabilité aisée entre différents fournisseurs.
 - Développer des standards ouverts pour les API de gestion des bases de données, couvrant les tâches courantes telles que les sauvegardes, la restauration et la configuration des accès.

2. Outils DevOps et CI/CD

Les pipelines de déploiement continu (CI/CD) sont essentiels pour les workflows modernes, mais leurs configurations diffèrent largement entre plateformes.

- **Recommandations :**

- Définir des standards pour les pipelines CI/CD afin d'assurer leur compatibilité multi-cloud.
- Promouvoir l'interopérabilité entre les outils de gestion des conteneurs (pris au sens large), des orchestrateurs et des systèmes de versioning.
- Encourager l'utilisation d'outils cloud-agnostiques (et notamment de logiciels libres) basés sur des standards ouverts pour l'automatisation des déploiements.
- Encourager l'utilisation d'outils de build reproductibles.

3. Stockage d'objets et systèmes de fichiers managés

Le stockage est un autre composant clé des services PaaS, souvent lié aux bases de données et aux applications.

- **Recommandations :**

- Développer des standards pour l'accès, la gestion et la portabilité des objets stockés.
- Uniformiser les API et les protocoles de stockage afin de simplifier les échanges entre différentes plateformes cloud.

4. Messaging et services de file d'attente

Les systèmes de messagerie (e.g., queues, pub/sub) sont souvent des services spécifiques aux fournisseurs, mais leur standardisation améliorerait l'interopérabilité.

- **Recommandations :**

- Promouvoir des protocoles standards comme AMQP ou MQTT pour les systèmes de messagerie cloud.
- Normaliser les formats des messages et des configurations pour réduire les efforts d'adaptation lors des migrations.

5. Environnements de runtime

Les environnements de runtime, souvent utilisés pour déployer des applications sans gérer l'infrastructure sous-jacente, présentent des divergences importantes entre fournisseurs.

- **Recommandations :**

- Standardiser les formats de configuration des environnements (e.g., variables d'environnement, dépendances).
- Aligner les pratiques sur les principes des **12 Factor Apps**, notamment en garantissant :
 - La portabilité des configurations via des environnements standardisés.
 - La gestion des dépendances à travers des formats ouverts et documentés.

Les principes des 12 Factor Apps comme base de normalisation

Les **12 Factor Apps** définissent un cadre pour le développement et le déploiement d'applications modernes en cloud. Leur intégration dans la normalisation des services PaaS

peut offrir un cadre pratique pour l'interopérabilité et la portabilité. Parmi les facteurs les plus pertinents pour la normalisation :

- **Gestion des configurations** : standardiser les mécanismes pour la gestion centralisée des configurations.
- **Dépendances explicites** : encourager des formats ouverts pour la gestion des dépendances des applications (e.g., fichiers manifestes standardisés).
- **Portabilité** : s'assurer que les environnements d'exécution et de stockage respectent des standards qui permettent un transfert facile entre clouds.
- **Logs unifiés** : normaliser les formats de journalisation pour une intégration aisée avec des outils tiers.

Impact attendu

1. **Facilitation des migrations** : une normalisation ciblée des services PaaS réduira les efforts techniques pour migrer les applications et leurs dépendances entre différents fournisseurs.
2. **Amélioration de l'innovation ouverte** : des standards ouverts inciteront les développeurs et les fournisseurs à innover tout en restant interopérables.
3. **Renforcement de la souveraineté numérique** : en promouvant des standards basés sur des principes ouverts, les acteurs européens pourront réduire leur dépendance à des solutions propriétaires non européennes.
4. **Réduction des coûts** : en minimisant les besoins d'adaptation des applications et des workflows DevOps, les utilisateurs réaliseront des économies significatives.

En résumé: la normalisation des services PaaS, lorsqu'elle est axée sur des besoins et services stratégiques comme les bases de données, les outils DevOps ou les environnements de runtime, offre un levier puissant pour une interopérabilité accrue et une adoption généralisée des bonnes pratiques cloud-native.

Question 51 : Normalisation des services auxiliaires

La normalisation des services auxiliaires constitue une étape clé pour faciliter la portabilité et l'interopérabilité dans les environnements multi-cloud. Ces services, bien que non centraux, jouent un rôle fondamental dans la gestion et l'efficacité des infrastructures cloud. Une approche normalisée permettrait de réduire les coûts liés aux migrations et à l'interopérabilité, tout en renforçant la sécurité et la cohérence des politiques dans un contexte multi-fournisseurs.

Avis favorable sur la normalisation des services IAM (Identity and Access Management)

Les systèmes de gestion des identités et des accès (IAM) sont essentiels pour garantir la sécurité et le contrôle des environnements cloud. Cependant, les différences fonctionnelles et techniques entre les implémentations des différents fournisseurs constituent un frein à leur adoption dans des architectures multi-cloud ou lors de migrations.

Objectifs de normalisation :

- **Réduction des écarts fonctionnels** entre les solutions IAM des fournisseurs afin d'assurer une meilleure interopérabilité des politiques de gestion des identités et des droits d'accès.
- **Priorisation de standards pour la synchronisation des politiques d'accès** : permettre aux utilisateurs de synchroniser facilement leurs règles d'accès, rôles et permissions entre plusieurs fournisseurs, tout en minimisant les risques de désalignement ou de failles de sécurité.
- **Promotion de protocoles ouverts et standards** (e.g., SAML, OpenID Connect, OAuth...) pour garantir une intégration fluide et interopérable dans les environnements multi-cloud et hybrides.

Autres services auxiliaires à normaliser

1. Observabilité et monitoring

- L'observabilité, qui inclut le monitoring, le logging et le traçage des performances, est un enjeu majeur pour les entreprises utilisant plusieurs fournisseurs. Les outils et les formats propriétaires compliquent la centralisation et la corrélation des données issues de plusieurs environnements.
- **Recommandation** :
 - Adopter et promouvoir des standards ouverts tels qu'**OpenTelemetry** pour unifier les mécanismes de collecte, de traitement et d'analyse des métriques et des journaux.
 - Encourager l'utilisation de formats standardisés pour les rapports de performances et les événements (e.g., JSON pour les logs structurés).

2. Facturation et gestion des coûts

- La transparence des coûts dans des architectures multi-cloud est entravée par des formats de facturation différents entre fournisseurs. Cette disparité complique la gestion budgétaire et le pilotage des ressources.
- **Recommandation** :
 - Harmoniser les formats des rapports de facturation, en utilisant des structures communes pour les coûts associés aux ressources (e.g., CPU, stockage, bande passante).
 - Introduire des standards pour les API de facturation, permettant l'extraction automatisée des données financières dans des outils tiers de gestion des coûts.

3. Orchestration et automatisation

- Les outils d'automatisation des déploiements (e.g., scripts d'infrastructure-as-code) et de gestion des workflows cloud varient largement entre fournisseurs, compliquant l'intégration dans des environnements multi-cloud.
- **Recommandation** :
 - Encourager des standards ouverts pour l'orchestration, tels que des schémas uniformisés pour les fichiers de configuration des infrastructures.

4. Gestion des configurations et politiques

- Les services cloud proposent souvent des outils pour centraliser et automatiser les configurations, mais ces outils sont rarement compatibles entre plateformes.
- **Recommandation :**
 - Normaliser les formats des configurations des systèmes cloud pour simplifier la migration et l'administration dans des environnements hétérogènes.

Impact attendu

- **Simplification des migrations et interopérabilité accrue** : en éliminant les obstacles techniques liés à la variabilité des services auxiliaires, les entreprises pourront facilement changer de fournisseur ou utiliser plusieurs environnements cloud simultanément.
- **Réduction des coûts** : une normalisation des services auxiliaires limite les ajustements coûteux lors des transitions ou des intégrations.
- **Amélioration de la cybersécurité** : une synchronisation harmonisée des politiques d'accès et une visibilité centralisée grâce à des outils normalisés renforcent la résilience des systèmes.

La normalisation des services auxiliaires doit être envisagée de manière prioritaire, en se concentrant sur les domaines critiques comme les IAM, l'observabilité et la facturation. Ces efforts contribueront à renforcer la compétitivité et la souveraineté numérique des acteurs européens tout en favorisant une adoption élargie des infrastructures cloud interopérables.

Question 52 : Normalisation des structures et formats de données SaaS

La normalisation des structures et des formats de données pour les services SaaS est essentielle pour garantir la portabilité et l'interopérabilité entre solutions. Cela permet aux utilisateurs de migrer leurs données efficacement, sans perte ni verrouillage, tout en favorisant l'adoption de standards ouverts. Les domaines prioritaires incluent :

1. ERP (Enterprise Resource Planning)

Les solutions ERP gèrent des données complexes et critiques (financières, ressources humaines, logistiques, etc.). La normalisation dans ce domaine devrait viser :

- **Formats communs pour les exports/imports de données** : définir des schémas pour les transactions, les inventaires ou les rapports financiers.
- **Interopérabilité des modules spécifiques** (e.g., gestion des stocks, gestion de la paie) entre plateformes, en garantissant que les données respectent des modèles standards lisibles et adaptables.

2. CRM (Customer Relationship Management)

Les outils CRM stockent des informations stratégiques sur les clients, les ventes et les interactions. La normalisation ici pourrait inclure :

- **Formats standards pour les données clients** (e.g., contacts, historiques d'interactions, opportunités de vente).

- Harmonisation des schémas pour les workflows automatisés et les rapports d'analyse.

3. Solutions de collaboration et suites bureautiques

Les plateformes de collaboration et de productivité incluent des outils pour la gestion des documents, des communications et du partage d'informations. Pour favoriser la portabilité :

- **Utilisation de formats ouverts pour les documents** (e.g., ODF - Open Document Format, ou autres standards reconnus).
- Normes pour les échanges entre calendriers, messageries et fichiers collaboratifs afin de garantir leur intégration dans des environnements hétérogènes.

4. Respect et extension des standards ouverts

Il est essentiel d'encourager l'utilisation de standards ouverts existants et d'en développer de nouveaux, lorsque nécessaire :

- **Adoption universelle des formats ouverts** pour les documents, les bases de données et les exports structurés (e.g., JSON ou XML standardisés pour les données SaaS).
- Participation active à des initiatives internationales pour la définition de standards spécifiques à des secteurs verticaux (e.g., santé, éducation).

Recommandations

- **Création d'un cadre européen pour la normalisation des données SaaS** : les acteurs publics devraient piloter des efforts de standardisation, en collaboration avec les associations industrielles et les acteurs du logiciel libre, pour définir des formats unifiés dans les secteurs clés.
- **Encouragement à l'interopérabilité via la régulation** : les fournisseurs de SaaS devraient être incités à documenter leurs formats et interfaces dans des standards ouverts et accessibles. Cela inclurait la publication d'API bien définies et conformes à ces standards.
- **Mise en place de certifications SaaS** : un label certifiant la conformité des fournisseurs SaaS aux standards ouverts pourrait guider les utilisateurs vers des solutions favorisant l'interopérabilité et la portabilité.

En normalisant les structures et les formats des données SaaS, on réduira les risques de verrouillage, favorisera la concurrence et soutiendra un écosystème numérique plus ouvert et résilient.

Question 53 : autres commentaires sur les enjeux soulevés dans la consultation

Ne pas se laisser piéger par des définitions approximatives ou biaisées des standards ouverts

Un **standard ouvert**, conformément à la définition stricte de l'**European Interoperability Framework ("EIFv1", 2005)**, est une spécification technique formalisée et indépendante, permettant à tout acteur d'y accéder et de l'implémenter **librement** (sans restrictions

juridiques, opérationnelles ou financières).

Le CNLL souligne que, pour garantir la souveraineté numérique et éviter les verrouillages fournisseurs, il est essentiel d'appuyer les infrastructures numériques sur des **standards ouverts au sens strict** (i.e. conforme à l'EIFv1), notamment pour les interfaces de communication, les formats de données et les protocoles.

Source: <https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/2021-11/EIFV1.0.pdf> (<https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/2021-11/EIF%20V1.0.pdf>)

Contexte:

In June 2002, European heads of state adopted the eEurope Action Plan 2005 at the Seville summit. It calls on the European Commission "to issue an agreed interoperability framework to support the delivery of pan-European eGovernment services to citizens and enterprises". This framework would address information content and recommend technical policies and specifications to help connect public administration information systems across the EU. The Action Plan also stipulated that the Framework would "be based on open standards and encourage the use of open source software"

La définition à retenir:

The following are the minimal characteristics that a specification and its attendant documents must have in order to be considered an open standard:

- The standard is adopted and will be maintained by a not-for-profit organisation, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties (consensus or majority decision etc.).
- The standard has been published and the standard specification document is available either freely or at a nominal charge. It must be permissible to all to copy, distribute and use it for no fee or at a nominal fee.
- The intellectual property - i.e. patents possibly present - of (parts of) the standard is made irrevocably available on a royalty-free basis.
- There are no constraints on the re-use of the standard.

Critères d'un standard ouvert selon l'EIFv1

Les critères clés pour un standard ouvert, que la régulation des services cloud devrait systématiquement promouvoir ou imposer, incluent :

1. Spécifications publiées et accessibles librement :

- Toute documentation liée au standard doit être publique, sans restriction financière ni juridique. Cela garantit que tout acteur, qu'il soit une PME, une administration ou un particulier, puisse implémenter et utiliser le standard.

2. Compatibilité avec des implémentations concurrentes :

- Un standard ouvert ne favorise aucun acteur spécifique et permet des implémentations multiples, y compris dans des logiciels libres, pour garantir la concurrence et la diversité des offres.

3. Neutralité technique et absence de brevet bloquant :

- Aucun brevet essentiel au fonctionnement du standard ne doit restreindre son utilisation de quelque façon que ce soit. Les brevets doivent impérativement être disponibles sous une licence libre de redevance (*royalty-free*) et non sous une licence RAND (*Reasonable And Non Discriminatory*) ou FRAND (*Fair, Reasonable And Non Discriminatory*).

4. Gouvernance indépendante et transparente :

- Le développement et la maintenance du standard doivent être supervisés par une organisation ouverte, où toutes les parties prenantes ont une influence égale.

5. Interopérabilité comme finalité principale :

- Le standard doit être conçu pour maximiser la capacité d'interaction entre différents systèmes et solutions, qu'elles soient propriétaires ou libres. (NB: comme on va le voir plus loin, cette notion de finalité rejoint la notion d' "interopérabilité opposable").

Le piège de l'EIFv2

Il est crucial de s'appuyer sur l'EIFv1 (2005) comme cadre de référence pour définir un standard ouvert, et non sur l'EIFv2 (2010), qui a relâché certaines exigences clés sous l'influence de lobbies extra-européens. Les concessions faites dans l'EIFv2 ont réduit la portée effective de l'interopérabilité et de la neutralité technologique, avec un impact négatif sur la souveraineté numérique.

Les insuffisances de l'approche strictement normative

La définition d'un standard ouvert dans la LCEN (2004) reste insuffisamment cadrée. Elle définit un standard ouvert comme "tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre".

Cette définition soulève deux problèmes majeurs :

- Elle ne définit pas précisément les "restrictions" ce qui ouvre la porte à une incertitude juridique.
- Elle n'impose pas explicitement une obligation d'interopérabilité vérifiable ou opposable.

Il serait donc utile de préciser cette définition de la manière suivante:

"On entend par standard ouvert tout protocole de communication, d'interconnexion ou d'échange et tout format de données dont les spécifications techniques sont publiques, accessibles sans restriction de mise en œuvre, et exemptes de royalties ou de conditions commerciales discriminatoires, garantissant ainsi leur adoption libre. Le standard ouvert doit inclure une documentation complète permettant son implémentation, ainsi que des mécanismes assurant et vérifiant son interopérabilité opposable."

L'interopérabilité opposable

L'idée d'**interopérabilité opposable** introduite ici est une réponse stratégique et pragmatique à des problématiques complexes liées à l'interopérabilité dans des écosystèmes comme les ERP, les clouds ou les télécoms. Cette approche reconnaît les limites des standards techniques, notamment leur rigidité et leur tendance à privilégier des acteurs dominants, tout en se concentrant sur les moyens concrets d'assurer une interopérabilité réelle, adaptable et vérifiable.

Analyse de la situation

1. Standards vs Réalité :

- **Imposition des standards** : L'adoption forcée de certains standards complexes peut favoriser les acteurs dominants qui disposent des ressources nécessaires pour les mettre en œuvre rapidement et efficacement, ou qui imposent comme "standard" leur propre implémentation pré-existante, tandis qu'elle pénalise les petits acteurs, qui peuvent s'avérer incapables de supporter les coûts de conformité ou de développement associés. Il convient donc de respecter un équilibre entre la nécessité d'un cadre normatif clair pour garantir l'interopérabilité et la préservation d'un écosystème concurrentiel et inclusif, où les standards doivent rester accessibles, évolutifs et proportionnés aux capacités des différents acteurs. Une solution consiste à privilégier des approches flexibles comme l'interopérabilité opposable, qui impose des résultats mesurables sans contraindre à une implémentation technologique unique, tout en favorisant la neutralité technique et la liberté d'innovation.
- **Respect apparent des standards** : Les grands fournisseurs ont les moyens de "faire semblant", en créant des implémentations partielles, volontairement non interopérables, ou en introduisant des dépendances propriétaires dans leurs solutions.
- **Diversité des standards ouverts** : Afin de stimuler l'innovation et les petits acteurs, la diversité des normes ouvertes devrait être protégée plutôt qu'empêchée, pour autant qu'elles répondent à des exigences d'interopérabilité applicables.

2. Les bugs et l'interopérabilité :

- Les écarts entre les spécifications théoriques des standards et leur mise en œuvre pratique proviennent souvent de bugs, qui peuvent être dus à des erreurs involontaires ou, dans certains cas, à des stratégies délibérées pour limiter l'interopérabilité (cf. par exemple le code AARD, inséré par Microsoft dans une version bêta de Windows 3.1 pour détecter et provoquer une erreur cryptique sur DR-DOS, afin de dissuader l'utilisation de ce système concurrent, déclenchant une controverse documentée par

des mémos internes, un procès et une accord transactionnel de 280 millions de dollars: https://en.wikipedia.org/wiki/AARD_code (https://en.wikipedia.org/wiki/AARD_code). Les divergences dans l'interprétation des spécifications techniques contribuent également à des problèmes de compatibilité.

- Ces problèmes sont exacerbés par l'absence de mécanismes efficaces pour contraindre les fournisseurs à corriger leurs implémentations défectueuses. Les utilisateurs finaux ou les petits acteurs n'ont souvent aucun moyen de recours pour faire valoir leur droit à une interopérabilité effective.

3. Contexte du cloud :

- Contrairement aux télécoms, où les standards (comme ceux du 3GPP ou de l'IETF) assurent une interconnexion globale grâce à un cadre largement imposé, le domaine du cloud est beaucoup plus fragmenté. Les notions mêmes de "service", "interopérabilité" ou "portabilité" y sont floues et souvent définies de manière différente selon les fournisseurs. Cette fragmentation est aggravée par l'absence de normes universelles ou contraignantes et par la coexistence d'approches propriétaires, rendant difficile l'établissement d'un écosystème cohérent et réellement interopérable.
- Dans ce contexte, une définition claire et opposable de l'interopérabilité, associée à des mécanismes de validation pratiques (tests d'interopérabilité, certifications), est essentielle pour éviter les pratiques de verrouillage fournisseur et garantir la portabilité des services, données et applications.

Interopérabilité opposable : Une approche pragmatique

L'idée centrale derrière l'**interopérabilité opposable** est de permettre à toute partie prenante, quelle que soit sa taille, de **contraindre un fournisseur à respecter des principes d'interopérabilité**. Cela s'appuie sur :

1. Définition claire des attentes :

- Plutôt que d'imposer des standards techniques précis, il s'agit de définir des résultats mesurables. Exemple : un client doit pouvoir exporter et réutiliser ses données dans un format ouvert et lisible par des outils tiers.

2. Mécanismes de vérification et de recours :

- Les fournisseurs doivent être tenus responsables de leurs implémentations, avec des mécanismes permettant de :
 - Vérifier la conformité de leurs services à des principes définis.
 - Exiger des corrections en cas de non-conformité.
 - Imposer des pénalités dissuasives en cas de manquements délibérés ou répétés.

3. Environnement d'exécution compatible :

- Fournir un cadre où les acteurs (petits ou grands) peuvent tester et valider l'interopérabilité. Exemple : une suite de test librement utilisable et/ou une implémentation de référence.

4. Neutralité technologique :

- La notion d'“interopérabilité opposable” laisse la porte ouverte à diverses solutions technologiques, tout en imposant des résultats concrets.

Exemple d'application dans le cloud

Dans le contexte du cloud, l'interopérabilité opposable pourrait inclure :

- **Interopérabilité des données :**
 - Obligation de fournir des API ouvertes permettant d'exporter les données sans dépendances propriétaires.
- **Portabilité des services :**
 - Possibilité pour un utilisateur de déplacer une charge de travail ou une application d'un fournisseur à un autre, sans modification majeure.
- **Interopérabilité des API :**
 - Documentation claire et tests automatisés pour vérifier que les API fonctionnent comme annoncé.
- **Recours en cas de litige :**
 - Une organisation tierce ou un cadre juridique permettant d'arbitrer les différends techniques.

Protéger les petits acteurs

L'interopérabilité opposable, en mettant l'accent sur les droits et les mécanismes de recours, donne aux petits acteurs les outils pour :

- Faire respecter leurs droits face à des géants souvent peu enclins à respecter les standards ou à corriger des bugs.
- Développer des solutions innovantes sans se heurter à des barrières techniques artificiellement élevées.

L'interopérabilité opposable est une approche qui recentre le débat sur l'efficacité pratique, en évitant le piège de la standardisation rigide ou imposée. Elle permettrait de maintenir un écosystème ouvert et innovant, tout en donnant aux acteurs – grands et petits – des moyens concrets de garantir la compatibilité et la portabilité de leurs solutions. En adoptant ce concept, on pourrait répondre aux défis actuels du cloud, des ERP et au-delà, tout en protégeant la diversité et l'équité dans les marchés numériques.

Exemples concrets de standards ouverts pertinents dans le cloud

Voici quelques exemples (parmi des centaines, et donc uniquement à titre d'illustration) de **vrais standards ouverts** essentiels dans le contexte du cloud et des architectures numériques :

1. OpenAPI (ex-Swagger) :

- Spécification standardisée pour la conception d'API RESTful. Permet de documenter les API de manière unifiée et d'assurer leur interopérabilité.

2. OAuth 2.0 :

- Protocole d'authentification standard ouvert pour sécuriser les autorisations et les accès.

3. ISO/IEC 19941:2017 :

- Norme sur la portabilité des services de cloud computing, essentielle pour garantir la migration entre fournisseurs.

4. ODF (Open Document Format) :

- Format standard ouvert pour les documents bureautiques, garantissant leur interopérabilité et leur pérennité.

5. DNS (Domain Name System) :

- Un exemple fondamental de standard ouvert dans l'infrastructure réseau.

Alignement avec les problématiques soulevées par l'Arcep

Dans le cadre de cette consultation, les standards ouverts sont directement liés aux questions d'interopérabilité, de portabilité et de lutte contre le verrouillage fournisseur. Ils sont particulièrement cruciaux pour les :

1. API des services cloud :

- Toutes les API devraient être conçues et documentées selon des standards ouverts comme OpenAPI, garantissant leur accessibilité à toute solution compatible.

2. Formats de données :

- Les données échangées dans des services SaaS ou multi-cloud devraient respecter des formats standardisés (ex. JSON, XML) qui permettent leur traitement indépendant du fournisseur.

3. Protocole de migration et de portabilité :

- Les normes comme ISO/IEC 19941:2017 devraient être systématiquement adoptées et renforcées pour encadrer les transferts de données et d'applications entre fournisseurs.

Recommandations pour l'Arcep

1. Fonder toute approche normative sur les standards ouverts :

- Dans le cadre de la mise en application de la loi SREN et des lignes directrices à établir, il est impératif que l'interopérabilité et la portabilité reposent sur des standards ouverts au sens strict (EIFv1) , en excluant toute dépendance technologique ou juridique.

2. Intégrer l'EIFv1 comme cadre de référence :

- L'Arcep pourrait se référer à l'EIFv1 (ou tout autre document qui en reprend les

principes) pour définir clairement ce qu'est un standard ouvert et en garantir l'application dans l'écosystème numérique français.

3. Adopter un cadre juridique pour l'interopérabilité opposable :

- Imposer des obligations de test, de documentation complète et de mise en œuvre vérifiable pour garantir l'interopérabilité effective des services cloud.

4. Encourager la participation active des acteurs européens :

- Les organismes français et européens doivent jouer un rôle clé dans la définition et la maintenance de ces standards, afin de garantir qu'ils répondent aux besoins locaux et qu'ils ne favorisent pas les intérêts de fournisseurs non européens. Les organismes nationaux doivent se préserver des influences des acteurs extra-européens.

5. Promouvoir l'éducation sur les standards ouverts :

- Sensibiliser les acteurs, en particulier les PME, sur l'importance des standards ouverts et leur rôle dans la souveraineté numérique.

Pour garantir une régulation efficace et durable, l'Arcep doit promouvoir les **standards ouverts** au sens de l'EIFv1 comme un pilier central des exigences en matière d'interopérabilité et de portabilité. Cela permettra de renforcer la souveraineté numérique, d'encourager l'innovation locale et de prévenir les pratiques de verrouillage fournisseur, tout en offrant un cadre technologique stable et pérenne.

Question 54 : Autres enjeux pour la régulation des services cloud

Promotion des solutions cloud européennes

L'un des leviers clés pour renforcer la souveraineté numérique européenne consiste à garantir un accès équitable des PME européennes aux marchés publics. Cela inclut notamment :

- **Réservation de quotas dans les marchés publics** : imposer un pourcentage minimum dédié aux fournisseurs européens, en particulier les PME, afin de stimuler la croissance des solutions locales et d'encourager l'innovation au sein de l'écosystème européen.
- **Favorisation des solutions basées sur des standards ouverts et des technologies libres** : ces critères doivent devenir prioritaires dans les appels d'offres, garantissant ainsi que les services choisis renforcent l'indépendance technologique et minimisent les risques de verrouillage fournisseur.

Ces mesures soutiendraient les entreprises locales tout en réduisant la dépendance vis-à-vis des hyperscalers non européens.

Cyber-résilience : une approche technique et systémique

La cyber-résilience va bien au-delà des obligations réglementaires : elle repose sur une combinaison d'approches techniques, organisationnelles et stratégiques pour garantir la continuité des services en cas de cyberattaque ou de défaillance. Les architectures multi-cloud et les services cloud doivent intégrer cette notion au cœur de leur conception. Cela implique :

- **Approche systémique** : les fournisseurs doivent être tenus de mettre en place des mécanismes pour détecter, isoler et répondre rapidement aux incidents affectant les services cloud. Cela inclut la prise en compte des interconnexions entre les services pour éviter tout effet domino en cas de panne ou de compromission.
- **Standards de sécurité spécifiques pour les environnements multi-cloud** : il est essentiel d'établir des cadres spécifiques aux architectures multi-cloud, notamment en ce qui concerne la synchronisation des politiques de gestion des accès (IAM) et la gestion sécurisée des flux de données entre fournisseurs.
- **Transparence en matière de cybersécurité** : les fournisseurs devraient être capables de démontrer leurs mesures de sécurité et leur capacité à gérer des scénarios de crise, selon l'approche qui leur est proche (et qui peut être différenciée).
- **Encourager l'innovation locale dans la cybersécurité** : les PME européennes spécialisées dans la cybersécurité doivent être soutenues, notamment par la commande publique, pour développer des solutions adaptées aux besoins spécifiques des services cloud européens.

En promouvant une cyber-résilience active et holistique, on réduit les vulnérabilités tout en renforçant la confiance des utilisateurs dans les solutions européennes.

Suivi et transparence des pratiques tarifaires

Les coûts liés aux services cloud, et en particulier aux **transferts de données** (sortants et entrants), restent une source de préoccupations majeures pour les utilisateurs. Pour limiter les pratiques de verrouillage économique et favoriser une concurrence saine :

- **Encadrement des frais de transfert de données** : établir des plafonds pour les frais de sortie de données afin de limiter l'effet de verrouillage, tout en garantissant une juste compensation des fournisseurs pour leurs coûts réels.
- **Transparence des modèles de tarification** : les fournisseurs devraient être tenus de publier des grilles tarifaires détaillées et accessibles, incluant les coûts directs et indirects des transferts de données, les frais de stockage et les services auxiliaires.
- **Mécanismes d'évaluation** : créer un observatoire indépendant des pratiques tarifaires, capable de surveiller les écarts et les abus, en particulier ceux favorisant des acteurs non européens ou faussant les conditions de concurrence.

Recommandations complémentaires pour la régulation des services cloud

1. **Encourager l'interopérabilité par les standards ouverts** : les autorités de régulation doivent s'assurer que l'ensemble des interfaces, des formats de données et des protocoles utilisés dans les services cloud soient compatibles avec des standards ouverts reconnus, conformément à la définition de l'EIFv1.
2. **Garantir la portabilité des données et des services** : renforcer les mécanismes qui permettent aux utilisateurs de migrer facilement leurs données et applications d'un fournisseur à un autre, y compris dans des environnements multi-cloud.
3. **Promotion d'un cadre européen pour la certification cloud** : développer des labels clairs qui garantissent qu'un fournisseur respecte des critères européens en matière de

souveraineté, d'interopérabilité, de durabilité et de sécurité. Ce cadre doit favoriser l'approche européenne de l'innovation.

4. Favoriser l'émergence de solutions cloud locales dans des secteurs critiques :

soutenir les initiatives ciblées, comme celles axées sur la santé, l'éducation ou les services publics, afin de créer des solutions cloud locales et adaptées aux besoins des citoyens et des administrations, en imposant une préférence et/ou des quotas pour ces solutions.

Ce n'est qu'en abordant ces enjeux avec une approche systémique que la régulation des services cloud pourra devenir un levier stratégique pour renforcer la souveraineté numérique et stimuler une innovation durable et équitable en Europe.