

Réponses d’AWS à la Consultation publique de l’ARCEP sur la régulation des services d’informatique en nuage (*cloud*)

Date : 16 Décembre 2024

Questions 39 à 54 : Réduire les difficultés techniques liées au changement de fournisseur et au recours simultané à plusieurs fournisseurs de services cloud (Sections 3.1.3-3.2.4)

39. Que pensez-vous de la description présentée par l’Autorité des différents modèles d’architectures *multi-cloud* et des besoins d’interopérabilité correspondants ?

39.1 Bien que les modèles décrits par l’ARCEP tiennent compte de différentes situations dans lesquelles les clients sont susceptibles d'utiliser les services de plusieurs fournisseurs, AWS ne croit pas qu'ils correspondent à la description de l'interopérabilité fournie par le Data Act. AWS considère que les cas d’usage particuliers des clients couverts par les exigences d’interopérabilité prévues par le Data Act devraient être déterminés conformément à la description fournie par le Data Act.

[SDA]

(a) [SDA]

(b) [SDA]

39.2 [SDA]

[SDA]

39.3 [SDA]

(a) [SDA]

(b) [SDA]

(i) [SDA]¹

(ii) [SDA]

39.4 [SDA]

40. Pour quels cas d’usage, présents ou futurs, une architecture « *multi-cloud* intégré » vous semble-t-elle particulièrement souhaitable ? Identifiez-vous des freins à l’interopérabilité empêchant d’y parvenir ? Le cas échéant, quels sont ces freins,

¹ [SDA]

que recommanderiez-vous de mettre en œuvre pour les limiter ces freins et selon quelles priorités ?

- 40.1 AWS renvoie à ses réponses précédentes, notamment à la Question 39 *supra* concernant la portée des exigences d'interopérabilité du Data Act pour les services de traitement de données. [SDA]
- 40.2 AWS souhaite également souligner que les potentiels défis auxquels les clients peuvent être confrontés lors de l'utilisation d'une architecture « *multi-cloud* intégré » peuvent ne pas être dus à un manque d'interopérabilité entre les fournisseurs de services *cloud*. La mise en place d'un système informatique d'entreprise fonctionnant sur un *multi-cloud* intégré requiert naturellement que les données circulent entre de nombreux systèmes différents. Une telle exigence peut souvent soulever des défis opérationnels susceptibles de fragiliser l'intégrité de la solution recherchée. Ces défis opérationnels sont inhérents à l'intégration de plusieurs environnements informatiques et ne sont pas causés par des problèmes spécifiques ou des restrictions imposées par les fournisseurs de services *cloud*. Plus précisément ²:
- (a) Latence des données accrue : Lorsqu'une solution unique est répartie entre plusieurs fournisseurs de services *cloud*, les informations peuvent devoir parcourir plusieurs centaines de kilomètres sur Internet pour passer d'un service à l'autre. La latence et les coûts augmentent en raison du temps supplémentaire nécessaire au transfert des données entre les fournisseurs de services *cloud*. En pratique, l'augmentation de la latence d'une charge de travail, passant d'un temps inférieur à une milliseconde à quelques millisecondes, voire à une dizaine de millisecondes, peut affecter négativement le résultat pour les clients, qui s'attendent à ce que leurs services fonctionnent instantanément.
 - (b) Problèmes liés à la gouvernance des données : La circulation constante des données entre différents systèmes engendre une multitude de problèmes de gouvernance des données. Par exemple, dans le cas d'une application analysant des transactions volumineuses, les principales exigences sont l'enregistrement et l'analyse des transactions de manière fiable, rapide et dans l'ordre de leur apparition. Cependant, tout transfert de données entre fournisseurs de services *cloud* augmentera, non seulement, la latence de manière significative, mais sera également susceptible de remettre en cause la capacité des utilisateurs à suivre la traçabilité des données et d'introduire des distorsions de données³. Lorsque qu'une application de transaction à haut volume, c'est-à-dire une application conçue pour traiter un grand nombre de transactions, envoie un flux de données vers plusieurs emplacements, il est difficile de garantir que chaque emplacement recevra les transactions dans le même ordre, ce qui peut créer des enregistrements divergents.
 - (c) Problèmes liés à la sécurité des données et à la protection de la vie privée : Lorsqu'une solution unique est répartie entre plusieurs fournisseurs

² Voir également les explications d'AWS concernant les considérations de sécurité des services de management d'identité et d'accès au paragraphe 51.6.

³ La « traçabilité des données » (*data lineage*) désigne la capacité à suivre l'historique des données analysées, notamment leur origine, leur mouvement et leurs transformations, à mesure qu'elles passent par les différentes étapes d'un *pipeline* de données ou d'un processus analytique. La « distorsions des données » décrit les changements introduits dans les caractéristiques des données analysées au fil du temps.

informatiques, les composants de la solution doivent communiquer entre eux *via* plusieurs passerelles, ce qui peut augmenter le risque de mauvaises configurations ou d'autres erreurs pouvant entraîner des fuites ou des pertes de données.

- (d) Points de défaillance multiples : Pour qu'une configuration *multi-cloud* intégrée fonctionne correctement, les fournisseurs de services *cloud* doivent inclure plusieurs points d'accès dans chacun de leurs services, par exemple, afin de permettre aux données et aux commandes de circuler rapidement entre les fournisseurs de services *cloud*. L'existence de plusieurs points d'accès peut augmenter les risques liés à la sécurité et introduire plusieurs points de défaillance potentiels. En cas de problème de performance de la solution, il est nécessaire de consulter plusieurs fournisseurs, chacun n'ayant de visibilité que sur certaines parties de la solution.

40.3 En d'autres termes, l'intégration *multi-cloud* ne constitue pas une fin en elle-même car elle n'est pas toujours la solution la plus efficace ou bénéfique pour les clients. Le *multi-cloud* présente à la fois des avantages et des inconvénients qui varient en fonction du client et du cas d'usage. Les clients ne sont réellement incités à adopter le *multi-cloud* que lorsqu'une telle architecture apporte une amélioration significative en termes de performance ou de coûts et d'économies. Cela est particulièrement vrai pour les architectures *multi-cloud* intégrées, qui peuvent nécessiter un transfert de données plus important par charge de travail unique par rapport à d'autres architectures *multi-cloud*. En conséquence, (i) certains clients, mais pas tous, choisissent une architecture *multi-cloud intégrée* ; et (ii) les clients ne choisissent pas une architecture *multi-cloud* intégrée pour toutes leurs charges de travail.

41. Partagez-vous la compréhension de l'Autorité selon laquelle l'interopérabilité des services *cloud* requiert des API disponibles, stables, documentées et accessibles depuis l'extérieur de l'écosystème de leur fournisseur ? Pourquoi ?

41.1 Oui, AWS partage la compréhension de l'ARCEP selon laquelle l'interopérabilité des services *cloud* requiert des API disponibles, stables, documentées et accessibles depuis l'extérieur des offres de leur fournisseur. Les API jouent un rôle important pour permettre l'interopérabilité entre les services *cloud* pour plusieurs raisons, telles que :

- (a) Protocoles de communication définis : Les API fournissent des protocoles clairs et définis pour que les différents systèmes logiciels puissent communiquer, permettant ainsi aux services de différents fournisseurs d'interagir efficacement tout en conservant leurs caractéristiques et innovations propres.
- (b) Abstraction : Les API masquent la complexité sous-jacente d'un service, en présentant une interface simplifiée avec laquelle d'autres services peuvent facilement s'intégrer.
- (c) Flexibilité et modularité : Les API bien conçues permettent une intégration flexible et des solutions modulables, s'adaptant aux changements tant du service du fournisseur que des systèmes d'intégration.

41.2 AWS considère que l'exigence de garantir que les API conçues par les fournisseurs pour leurs clients soient stables, documentées et accessibles par est déjà traitée par le Data Act et la Loi SREN. Plus précisément, l'article 30 paragraphe 2 du Data Act prévoit que les fournisseurs de services de traitement de données (autres que les services qui concernent des ressources informatiques modulables et variables limitées à des « 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 et exige que 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. L'article 28, II, 3 de la Loi SREN prévoit une disposition similaire reflétant la même exigence.

42. **Afin de favoriser l'interopérabilité des services de *cloud*, pouvez-vous détailler :**

- **Quelles informations minimales devraient être renseignées à votre sens dans la documentation des API pour assurer une interopérabilité entre services *cloud* ?**
- **Selon quels critères estimez-vous qu'une API est suffisamment stable ? Quelles conditions les mises à jour de ces API devraient-elles respecter afin de permettre à l'utilisateur d'anticiper et d'adapter son usage de ces services ?**

42.1 AWS est d'avis que le Data Act offre déjà des orientations sur les informations minimales qui devraient être renseignées dans la documentation de l'API pour assurer une interopérabilité entre les services *cloud*. Comme mentionné *supra*, l'article 30 paragraphe 2 du Data Act requiert que les interfaces ouvertes « *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* ». Conformément à cette exigence et sur le fondement des meilleures pratiques du secteur, AWS estime que les informations suivantes devraient généralement être renseignées dans la documentation des API :

- Points de terminaison d'API et leurs objectifs : URL spécifiques où les demandes d'API sont envoyées, accompagnées d'explications sur la fonction de chaque point de terminaison.
- Formats des requêtes et des réponses : descriptions détaillées des formats et structures de données utilisés dans les requêtes et les réponses (par exemple, JSON, XML).
- Méthodes d'authentification : informations sur la façon d'authentifier et d'autoriser les requêtes d'API.
- Codes d'erreur : listes des codes d'erreur possibles que l'API peut renvoyer, accompagnées d'explications sur la signification de chaque code.
- Exemples d'appels et de réponses d'API de base : exemples de requêtes et de réponses API pour aider les développeurs à comprendre comment utiliser l'API.

- Protocoles pris en charge (par exemple, informations sur les méthodes HTTP prises en charge par l'API (par exemple, GET, POST, PUT, DELETE))
 - Spécifications du format de données : détails sur les formats de données utilisés dans les interactions impliquant les API (par exemple, JSON, XML).
 - Support SDK disponible : informations sur les SDK de langage de programmation disponibles pour le service.
- 42.2 Toutefois, il convient de noter que le niveau de détail et la présentation de ces informations sont susceptibles de légèrement varier entre les services en raison de l'évolution et de la maturité des services, de leur complexité, des exigences spécifiques qui leur sont propres ou du niveau d'intégration interservices avec d'autres services offerts par le fournisseur. Les fournisseurs devraient continuer à disposer de cette flexibilité dans le cas où l'ARCEP adopterait des règles sur les informations minimales devant être mises à la disposition des clients via les API des services, dans le cadre de l'article 28, II, 3 de la Loi SREN.
- 42.3 [SDA] Compte tenu de ce qui précède, AWS estime qu'une API mise à la disposition des clients peut généralement être considérée comme stable si elle remplit les conditions suivantes :
- [SDA]
 - Un préavis est donné en amont des mises à jour majeures⁴.
 - Le système de versionnage est cohérent.
 - De la documentation ainsi que les informations nécessaires sont mises à la disposition des clients pour leur permettre de s'adapter aux mises à jour.
- 42.4 Il est important de noter que l'approche adoptée peut varier en fonction de la nature de la mise à jour, du service concerné et des considérations de sécurité potentielles. [SDA]
- 42.5 Si les API conçues pour être utilisées par les clients doivent être stables et garantir la rétrocompatibilité, AWS tient à souligner que la gestion interne des services de *cloud* requiert davantage de flexibilité. [SDA] Le Data Act et la Loi SREN n'imposent pas aux fournisseurs de partager la manière dont ils exécutent les actions demandées par ceux qui interagissent avec l'API, ou d'ouvrir leurs systèmes internes et les interfaces entre ces systèmes. Une telle interprétation dépasserait non seulement l'exigence relative aux interfaces ouvertes prévue à l'article 30, paragraphe 2 du Data Act, mais elle ralentirait également de manière significative la vitesse à laquelle les fournisseurs offrent des améliorations de la fonctionnalité et de la sécurité des services, aboutissant ainsi à une situation impraticable et n'offrant aucun avantage supplémentaire aux clients.
- 42.6 [SDA]

⁴ [SDA]

42.7 À titre d'illustration, AWS met à disposition l'API de son service *Amazon Simple Storage Service* (« **S3** ») sous une licence *open source* et publie la documentation adéquate⁵ pour permettre à ses clients (et aux autres fournisseurs) de créer des applications utilisant S3 ou de développer des logiciels directement compatibles avec l'API de S3. [SDA]

43. Identifiez-vous d'autres modèles d'interopérabilité entre systèmes informatiques que les API ? Le cas échéant, lesquels ?

43.1 Comme décrit dans les réponses précédentes, outre la mise à disposition publique des API de ses services, AWS a pris diverses mesures pour faciliter l'interopérabilité et permettre la communication de système à système ainsi que l'échange de données entre différents fournisseurs.

43.2 Comme également indiqué dans la réponse à la Question 29 *supra* (paragraphe 29.5), AWS met à disposition un grand nombre de kits de développement logiciel (*Software Development Kits* ou « **SDK** ») et d'API sous licence *open source*, et utilise des protocoles, des interfaces, des API et des formats de données ouverts pour l'ensemble de ses services⁶. Les kits SDK sont des ensembles d'outils conçus pour aider les développeurs d'applications et de logiciels à créer des langages de programmation spécifiques. Ils fournissent des modules, des composants, des packages et des outils prédéfinis permettant aux développeurs de créer, de tester et de déployer des applications logicielles. Les kits SDK comprennent souvent des composants tels que des débogueurs, des compilateurs et des bibliothèques permettant de créer du code qui s'exécute sur un système d'exploitation ou un langage de programmation spécifique. Ces composants permettent aux développeurs de gagner un temps considérable, consacré auparavant au codage et au débogage en partant de zéro. Les kits SDK contiennent également des ressources telles que de la documentation, des tutoriels et des guides, ainsi que des API et des cadres pour accélérer le développement d'applications. Pour le *cloud computing*, les développeurs utilisent les kits SDK pour l'intégration avec un environnement *cloud* dans le langage de leur choix ou pour la création et le déploiement d'applications *cloud*⁷. Les kits SDK d'AWS permettent aux clients d'intégrer plus facilement les services AWS dans leurs applications avec une API adaptée au langage de programmation de leur choix. AWS propose des kits SDK pour de nombreuses technologies et langages de programmation courants, facilitant ainsi pour les clients le recours aux services AWS depuis leurs applications dans le langage ou pour la technologie en question⁸. Les kits SDK d'AWS simplifient également le codage en fournissant des API adaptées aux langages spécifiques pour les services AWS. Par exemple, les clients peuvent utiliser AWS SDK pour .NET⁹, AWS SDK pour Python (Boto3)¹⁰ et AWS SDK pour Ruby¹¹ lorsqu'ils créent des applications web sur AWS.

⁵ Voir : <https://docs.aws.amazon.com/AmazonS3/latest/API/Welcome.html>.

⁶ Voir : https://aws.amazon.com/fr/developer/tools/?nc1=f_dr.

⁷ Voir : <https://aws.amazon.com/what-is/sdk/>.

⁸ Pour la liste des kits SDK d'AWS, voir : <https://aws.amazon.com/fr/developer/tools/>.

⁹ Voir : <https://aws.amazon.com/fr/sdk-for-net/>.

¹⁰ Voir : <https://aws.amazon.com/fr/sdk-for-python/>.

¹¹ Voir : <https://aws.amazon.com/fr/sdk-for-ruby/>.

- 43.3 De plus, AWS publie une documentation complète, incluant, lorsque cela est pertinent, les différences entre les divers services AWS et l'*open source* sous-jacent. Cela permet aux clients et aux autres fournisseurs de services *cloud* d'élaborer des solutions qui interagissent avec ces services.
- 43.4 En outre, AWS met en œuvre de nombreuses initiatives concrètes pour informer et former ses clients sur les aspects techniques de ses services et sur l'intégration de ces derniers avec ceux d'autres fournisseurs de services *cloud*. Par exemple, AWS fournit des explications sur le langage de programmation utilisé par divers outils disponibles pour développer sur AWS, et documente les modifications apportées à l'*open source* sous-jacent de ses services *open source* gérés. Chaque service AWS est accompagné d'une documentation complète détaillant précisément son fonctionnement. AWS publie également des articles de blog et des études de cas pour guider les clients sur l'utilisation de ses services ou la migration de diverses charges de travail et types d'applications vers d'autres environnements *cloud*.
- 43.5 Enfin, comme AWS l'a expliqué dans sa réponse à la Question 24 *supra*, ses services permettent l'utilisation de divers protocoles, interfaces et formats de données standards. AWS a réalisé des investissements considérables dans la technologie des conteneurs et mène plusieurs initiatives propres en matière d'*open source*. Ces efforts contribuent à l'interopérabilité de plusieurs manières :
- (a) Les protocoles et interfaces standards permettent à différents systèmes de communiquer en utilisant des méthodes largement reconnues, ce qui facilite l'intégration entre les services AWS et d'autres systèmes.
 - (b) La possibilité d'utiliser des formats de données courants permet l'échange de données entre différentes plates-formes et différents services.
 - (c) La technologie des conteneurs, telle que Docker et Kubernetes, dont l'utilisation est permise par AWS au travers de services tels qu'*Amazon Elastic Container Service* (« **Amazon ECS** ») et *Amazon Elastic Kubernetes Service* (« **Amazon EKS** »), permet aux applications de fonctionner de manière cohérente dans différents environnements, améliorant ainsi la portabilité et l'interopérabilité.
 - (d) Les initiatives *open source* d'AWS contribuent à la communauté technologique au sens large, en se concentrant souvent sur des outils et des bibliothèques susceptibles d'améliorer l'interopérabilité entre différents environnements *cloud*.
- 43.6 En conclusion, bien que les API soient essentielles pour l'interopérabilité, l'approche adoptée par AWS inclut un éventail plus large de technologies et de pratiques. Cette stratégie multifacette, qui comprend la mise à disposition de kits SDK en *open source*, la possibilité d'utiliser des protocoles et de formats standards, les technologies de conteneurs et la fourniture d'une documentation complète, facilite l'interopérabilité tant au sein d'AWS qu'avec des systèmes et services externes.

44. Identifiez d'autres enjeux et difficultés techniques relatifs au changement de fournisseur et au développement du *multi-cloud* ?

- 44.1 AWS souhaiterait profiter de cette occasion pour souligner que la capacité des services de *cloud* à s'intégrer avec d'autres services – qu'il s'agissent de services tiers ou d'offres de première partie d'AWS – et, par conséquent, tout éventuel problème ou difficulté technique lié au changement de fournisseur et au développement du *multi-cloud* dépendent de nombreux facteurs. Ces derniers incluent notamment les différences dans les technologies sous-jacentes, les fonctionnalités de chaque service, la complexité de chaque service, la difficulté technique posée par l'intégration, la manière dont l'architecture informatique du client a été configurée et des considérations telles que la disponibilité, la sécurité, la redondance et le temps de latence.
- 44.2 Des difficultés techniques peuvent survenir en raison des différences fondamentales dans la manière dont les fournisseurs de services *cloud* conçoivent et gèrent leurs services *cloud*, comme par exemple des différences dans les approches retenues, les API, les mises en œuvre techniques, les outils, les cadres, les méthodologies et les meilleures pratiques adoptées. Par exemple, AWS a choisi de créer trois Zones de Disponibilité par région et dispose donc d'une infrastructure sous-jacente et d'API différentes de celles d'autres fournisseurs de services *cloud*. Ce choix a été motivé par la conviction d'AWS quant à la meilleure façon d'offrir à ses clients une disponibilité et une résilience accrues. Bien que cela puisse imposer une charge technique en cas de changement de fournisseur de services informatiques à un autre, par exemple pour gérer la transformation des logiciels sur différentes couches de virtualisation (par exemple, de Kernel-based Virtual Machine à un serveur ESXI de VMware) et différents systèmes d'exploitation (par exemple, de UNIX à Linux) ou bases de données (par exemple, de Postgre à SQL), l'approche choisie par AWS pour ses services *cloud* est l'une des raisons principales pour lesquelles les clients choisissent AWS. Ce type de différenciation est le résultat naturel de la concurrence entre les différents fournisseurs, chacun cherchant la meilleure façon d'offrir un service ou une fonctionnalité à leurs clients, conduisant ainsi à des produits différenciés. Innover en proposant de nouveaux services et fonctionnalités implique un niveau naturel de différenciation, car ces nouveaux services et fonctionnalités ont tendance à être sensiblement différents des anciens. En d'autres termes, le caractère différencié des fonctionnalités et des interfaces est le signe de l'existence d'une concurrence intense entre les fournisseurs, chacun adoptant une approche innovante différente pour répondre aux besoins de ses clients. Par exemple, la plupart des fournisseurs de services *cloud* proposent des services de stockage de données. Ces derniers répondent tous à un même besoin fondamental, à savoir le stockage des données. Néanmoins, au-delà de ce besoin, les clients recherchent également, entre autres, des solutions économiques ainsi qu'une haute disponibilité et durabilité des données. Par conséquent, les fournisseurs de services de *cloud* cherchent à se différencier sur ces aspects en offrant des fonctionnalités innovantes ou en se spécialisant dans un type de stockage particulier.
- 44.3 À la lumière de ces considérations, AWS fait valoir que l'ARCEP ne devrait pas automatiquement attribuer les difficultés techniques liées au changement de fournisseurs ou aux cas d'utilisation simultanée à un manque d'interopérabilité. Beaucoup de ces difficultés découlent des complexités inhérentes aux services informatiques, des différences dans les approches technologiques et des exigences spécifiques des architectures des clients. Dès lors, AWS ne s'attend pas, et

ne pense pas que les clients s'attendent, à ce que ces difficultés soient entièrement résolues par les règles et modalités sur l'interopérabilité qui seront adoptées en vertu de l'article 28, II, 3 de la Loi SREN. Bien que l'interopérabilité soit importante, il est essentiel de reconnaître que certaines différences techniques et défis sont le résultat naturel de l'innovation et de la diversité des approches adoptées pour résoudre des problèmes technologiques complexes.

44.4 [SDA]

45. Parmi les codes de conduite et recommandations d'application volontaire dont vous auriez connaissance, pouvez-vous indiquer les préconisations qui vous semblent pertinentes afin de préciser les règles et modalités de mise en œuvre des exigences essentielles prévues au II de l'article 28 de la loi SREN ?

45.1 Bien qu'AWS n'ait connaissance d'aucun autre code de conduite ou recommandations non contraignantes qui traite directement les exigences essentielles prévues à l'article 28, II de la Loi SREN, AWS estime que le secteur du *cloud* a déjà développé de manière spontanée une série de solutions et de normes d'interopérabilité efficaces et des spécifications *open source*. Ces standards, spécifications et bonnes pratiques sectorielles, qui ont émergé au cours de l'évolution naturelle du marché du *cloud*, sont pertinentes pour l'ARCEP au moment où elle élabore des règles et des modalités d'application des exigences essentielles, notamment en matière de spécifications d'interopérabilité et de portabilité.

45.2 Compte tenu de ce qui précède, AWS recommande vivement l'approche suivante pour répondre à l'exigence concernant l'adoption de spécifications d'interopérabilité et de portabilité prévue par la Loi SREN:

- (a) S'appuyer, autant que possible, sur des protocoles standards du secteur déjà en vigueur ou des spécifications *open source* largement acceptées par le secteur, et avoir recours à l'élaboration de nouvelles normes par le biais d'un processus de normalisation formel par l'intermédiaire d'organismes de normalisation en dernier recours uniquement, et si ces nouvelles normes sont nécessaires, proportionnées et qu'elles n'entravent pas l'innovation. AWS constate que lorsqu'une demande d'interopérabilité est exprimée par les clients, le secteur y répond, tout en conservant l'agilité nécessaire pour adopter de nouvelles solutions qui satisfont aux besoins des clients. Cette approche correspond également à celle décrite dans le considérant (100) du Data Act, qui prévoit qu'il « *est également nécessaire que la Commission s'appuie sur les acteurs du marché pour élaborer des spécifications d'interopérabilité ouvertes pertinentes afin de suivre le rythme rapide de l'évolution technologique dans ce secteur. Ces spécifications d'interopérabilité ouvertes peuvent ensuite être adoptées par la Commission sous la forme de spécifications communes* ».
- (b) Se concentrer sur le fait de rendre possible les communications et les interactions entre les « services du même type », conformément aux exigences d'interopérabilité du Data Act, comme expliqué en réponse à la Question 39 *supra*.
- (c) Regrouper les spécifications d'interopérabilité en fonction de catégories de services considérés comme étant « du même type », afin de permettre l'échange

et l'utilisation de données entre les services de chaque catégorie respective, dans la mesure où le Data Act exige « *l'interopérabilité entre différents services de traitement de données couvrant le même type de service* ». Par exemple, si les « services d'analyse de données » étaient définis comme un type de service distinct, des spécifications seraient adoptées pour s'appliquer à ce type de service. Par conséquent, les services d'analyse de données d'un certain fournisseur pourraient transférer des données vers et depuis les services d'analyse du même type d'un autre fournisseur dans un format que l'autre service peut utiliser, et *vice versa*, étant donné qu'ils se conformeraient tous deux aux spécifications communes adoptées pour cette catégorie de services.

- (d) Adopter des règles et modalités de mise en œuvre demeurant à un haut niveau de généralité plutôt que d'être exagérément détaillées, afin d'éviter des conséquences indésirables sur l'innovation. L'introduction de spécifications ou de normes plus détaillées applicables aux services de *cloud* risquerait de freiner l'innovation, c'est-à-dire le facteur qui a permis de rendre le marché du *cloud computing* si dynamique et capable de répondre aux besoins des clients. Dans les marchés innovants, les acteurs doivent être libres d'expérimenter de nouvelles technologies, de comprendre ce qui fonctionne le mieux pour une solution donnée, et de s'écarter de cette compréhension lorsque les circonstances changent et que la solution existante n'est plus optimale. Certaines technologies sont devenues des normes *de facto* pour les fournisseurs et les utilisateurs de services *cloud*, car elles fonctionnent efficacement dans de nombreux cas d'usage et permettent aux clients d'élaborer les solutions qu'ils souhaitent sans entraver les progrès technologiques. En d'autres termes, le secteur développe spontanément des normes lorsqu'elles sont nécessaires et ces normes peuvent continuer à évoluer au fil du temps, au fur et à mesure que la technologie se développe, comme relevé *supra*. Plus les normes imposées seront détaillées, moins les fournisseurs de services *cloud* (et les clients) auront de flexibilité pour innover. Cela freinera les solutions nouvelles, plutôt que de permettre qu'elles soient testées par le marché. Par conséquent, les règles et procédures qui seront adoptées par l'ARCEP (et, à terme, par la Commission européenne dans le cadre du Data Act) devraient être assez souples pour permettre de tels développements. L'objectif devrait être d'établir une base de référence pour l'interopérabilité qui permette de poursuivre l'expérimentation et la différenciation, plutôt que de s'enfermer prématurément dans des normes détaillées qui pourraient rapidement devenir obsolètes et trop contraignantes.

45.3 AWS estime que de plus amples consultations sont nécessaires afin de parvenir à une conclusion sur les spécifications d'interopérabilité ouvertes qui pourront finalement être adoptées conformément au paragraphe 45.4(a) *supra*. AWS considère toutefois que les exemples suivants de protocoles standards ou de solutions *open source* pourraient être pris en considération dans ce contexte. AWS comprend qu'une deuxième phase d'échanges aura lieu et se tient à la disposition de l'ARCEP pour parvenir à des spécifications d'interopérabilité pertinentes.

- (a) REST et HTTP APIs permettant d'utiliser OpenID Connect (« **OIDC** ») et OAuth 2.0,

- (b) Les protocoles de sécurité Internet (par exemple, SSL/TLS), les certificats (par exemple, les certificats X.509 SSL/TLS) et les chiffrements ou *ciphers* (par exemple, RSA *ciphers*),
- (c) Appareils et clients qui utilisent le MQTT et le MQTT sur WebSocket,
- (d) Protocoles de communication sécurisés pour publier des messages et s'y abonner, ainsi que des appareils et des clients qui utilisent le protocole HTTPS pour publier des messages,
- (e) Configuration du service utilisant les formats de fichiers JSON ou YAML,
- (f) Interfaces JDBC et ODBC,
- (g) Protocoles RTMP standards pour la diffusion en continu à faible latence,
- (h) Support pour un langage de programmation courant, tel que C++, Go, Java, JavaScript, Kotlin, NET, Node.js, PHP, Python, Ruby, Rust ou Swift,
- (i) Pour les services de base de données, support pour les moteurs de base de données et des systèmes de gestion *open source*, tels que PostgreSQL, MariaDB, Redis, Memcached, Elasticsearch, Apache Hive, Apache Hbase, Hadoop et Cassandra,
- (j) Conteneurs et solutions de gestion des conteneurs standards, comme Docker et Kubernetes, et
- (k) Protocoles d'identité tels que Security Assertion Markup Language (« **SAML** ») 2.0 and System for Cross-domain Identity Management (« **SCIM** ») v2.0.

45.4 [SDA]

45.5 Finalement, AWS souligne que l'Association des Fournisseurs de Services d'Infrastructure Cloud en Europe (*Cloud Infrastructure Service Providers in Europe* ou CISPE) a annoncé l'adoption d'un nouveau Cadre de Changement de Fournisseur Cloud (ou *Cloud Switching Framework*)¹² au 1^{er} août 2024 afin d'accompagner les fournisseurs de services d'infrastructure *cloud* dans leur mise en conformité et la mise en valeur des services conformes aux exigences de changement de fournisseur, d'utilisation simultanée et de portabilité des données prévues par le Data Act. Le Cadre contribue également à préciser les rôles et les responsabilités de chaque partie impliquée dans le processus de changement de fournisseur ou dans le cas de l'utilisation simultanée. AWS estime que le Cadre est appelé à devenir un outil important pour établir une compréhension commune du processus qui intervient lorsqu'un client passe d'un fournisseur à un autre, ou utilise les services de plusieurs fournisseurs de manière simultanée, ce qui permettrait de mettre en œuvre de manière pratique les exigences du Data Act – comme prévoit le considérant (79) du Data Act. Bien que le Cadre ne couvre pas spécifiquement les exigences d'interopérabilité du Data Act pour les services du même type, AWS estime qu'il peut constituer une source de référence pour les travaux

¹² Voir : <https://cispe.cloud/portability>

de l'ARCEP pour l'élaboration des règles et des modalités de mise en œuvre des exigences essentielles de la Loi SREN en matière de portabilité des actifs numériques et des données exportables, et de l'exigence de mise à disposition gratuite aux clients et aux fournisseurs de services *cloud* tiers d'interfaces ouvertes.

46. Quelles sont les mesures actuellement mises en œuvre par les fournisseurs de services *cloud* afin de faciliter une équivalence fonctionnelle entre services IaaS qui couvrent le même type de fonctionnalités ? Quelles mesures supplémentaires permettraient de faciliter cette équivalence fonctionnelle ?

- 46.1 Comme également indiqué en réponse à la Question 28 *supra*, AWS partage le constat de l'ARCEP selon lequel il n'existe pas de barrières techniques empêchant les clients de réaliser l'équivalence fonctionnelle pour les « services IaaS ». AWS aide ses clients à réaliser l'équivalence fonctionnelle grâce à diverses informations, de la documentation et des supports éducatifs mis à leur disposition. Compte tenu des circonstances particulières à chaque client (notamment les clients qui utilisent des « éléments d'infrastructures » dotés d'une architecture personnalisée unique, qui ont souvent recours aux services de professionnels spécialisés en matière de *cloud*), AWS estime que si les clients sont suffisamment informés sur les capacités des éléments d'infrastructure qu'ils utilisent, ils peuvent obtenir des résultats comparables lorsqu'ils déplacent leurs charges de travail vers les services d'un autre fournisseur du même type.
- 46.2 Parce que les clients souhaitent disposer d'une certaine flexibilité et utiliser plusieurs options différentes pour répondre à leurs différents besoins informatiques, AWS doit permettre aux clients de procéder facilement à la migration de tout ou partie de leurs charges de travail vers et depuis les services d'AWS. Par conséquent, AWS a consacré d'importantes ressources dans ce domaine et a développé une gamme de formations et de conseils.
- (a) AWS publie régulièrement des articles de blog consacrés au thème de la migration et fournit des conseils expliquant comment déplacer des charges de travail vers ou depuis AWS. Par exemple, AWS a publié des articles de blog qui montrent aux clients comment déployer des charges de travail à partir d'AWS vers des instances de calcul et des machines virtuelles dans un autre *cloud*, ou *vice versa*¹³.
- (b) AWS informe en permanence les clients sur la manière dont ils peuvent minimiser le coût du changement de fournisseur en planifiant, concevant et testant la « réversibilité », c'est-à-dire la capacité d'un client à récupérer et à déplacer des données d'un environnement informatique à un autre. Par exemple, dans un livre blanc intitulé « *Unpicking Vendor Lock-in* », AWS décrit les principes de réversibilité que les clients doivent prendre en compte lorsqu'ils utilisent des services informatiques et montre aux clients la manière dont ils peuvent utiliser les services d'AWS pour favoriser la réversibilité et la portabilité de leurs données¹⁴.

¹³ Voir : <https://aws.amazon.com/fr/blogs/devops/how-to-deploy-workloads-in-a-multicloud-environment-with-aws-developer-tools/>.

¹⁴ Voir : <https://docs.aws.amazon.com/whitepapers/latest/unpicking-vendor-lock-in/how-the-aws-cloudhelps-to-eliminate-lock-in.html>.

- (c) La documentation publique d'AWS comprend également des informations sur l'interopérabilité et la réversibilité de ses services. AWS inclut ci-dessous des liens vers une partie de la documentation rassemblée pour des exemples de services généralement classés comme « services IaaS »

Pour *Elastic Compute Cloud* (« EC2 ») :

- https://docs.aws.amazon.com/fr_fr/vm-import/latest/userguide/what-is-vmimport.html
- <https://aws.amazon.com/fr/ec2/vm-import/>
- https://docs.aws.amazon.com/fr_fr/AWSEC2/latest/UserGuide/concepts.html
- <https://aws.amazon.com/fr/ec2/faqs/>
- https://docs.aws.amazon.com/fr_fr/appconfig/latest/userguide/appconfig-integration-ec2.html#appconfig-integration-ec2-retrieving-data

Pour *Amazon Simple Storage Service* (« S3 ») :

- https://docs.aws.amazon.com/fr_fr/AmazonS3/latest/userguide/download-objects.html
- https://docs.aws.amazon.com/fr_fr/apigateway/latest/developerguide/integrating-api-with-aws-services-s3.html
- <https://docs.aws.amazon.com/AmazonS3/latest/userguide/developing-rest-api.html>
- <https://aws.amazon.com/fr/blogs/storage/one-way-to-migrate-data-from-azure-blob-storage-to-amazon-s3/>
- <https://aws.amazon.com/fr/blogs/storage/migrating-oracle-cloud-infrastructure-object-storage-to-amazon-s3-using-aws-datasync/>
- https://docs.aws.amazon.com/fr_fr/AmazonS3/latest/userguide/access-grants.html
- <https://aws.amazon.com/fr/blogs/networking-and-content-delivery/secure-hybrid-access-to-amazon-s3-using-aws-privatelink/>
- https://docs.aws.amazon.com/fr_fr/datasync/latest/userguide/transferring-other-cloud-storage.html

- (d) Concernant la mise en réseau, au niveau du protocole, les services d'AWS reposent sur des protocoles de mise en réseau standards à l'échelle du secteur qui sont interopérables par définition, notamment, le *Border Gateway Protocol* (ou « BGP ») et *Transmission Control Protocol/Internet Protocol* (ou « TCP/IP »). Cela signifie que les ressources AWS d'un client sont en mesure de communiquer avec d'autres ressources informatiques sur d'autres réseaux utilisant ces protocoles, sans transformations ou conversions supplémentaires qui ajouteraient des coûts, de la latence et de la complexité. Par exemple, lorsque les clients souhaitent intégrer des produits *Software-Defined Wide Area Network* (ou « SD-WAN ») tiers à AWS Cloud WAN, ils peuvent le faire sans protocoles de tunnel (*tunnelling*) spécialisés. Dans le cadre de la définition de l'équivalence fonctionnelle du Data Act, cette approche de la mise en réseau permet aux clients de rétablir un niveau minimum de fonctionnalité en termes de communication réseau et d'intégration dans un nouvel environnement.

47. Quelles informations minimales devrait contenir, selon vous, l'offre de référence technique d'interopérabilité prévue par la loi SREN afin de permettre la bonne information des utilisateurs ?

47.1 AWS renvoie à sa réponse à la Question 48 ci-dessous.

48. Que pensez-vous de la proposition d'utiliser l'offre de référence technique d'interopérabilité pour informer les utilisateurs de la spécificité des services *cloud*, et d'en harmoniser la forme ?

48.1 AWS partage l'avis de l'ARCEP selon lequel la diversité des fonctionnalités offertes par les fournisseurs de services de *cloud* témoigne de la dynamique d'innovation dans le secteur. Elle peut permettre aux fournisseurs de se différencier en apportant des services plus performants ou plus adaptés aux besoins des utilisateurs.

48.2 Cependant, comme expliqué dans ses réponses précédentes, AWS n'est pas d'accord avec la proposition de l'ARCEP d'établir une distinction entre les services *cloud* « standards » et « spécifiques » selon que d'autres fournisseurs offrent ou non des services équivalents, et de déterminer les exigences de transparence imposées aux fournisseurs en fonction de la catégorie à laquelle le service appartient. De plus, même si une telle distinction entre les services *cloud* était adoptée, AWS considère qu'il n'est pas réaliste d'exiger des fournisseurs qu'ils incluent des déclarations ou des comparaisons de leurs services avec les « services équivalents » d'autres fournisseurs dans leur offre de référence technique d'interopérabilité. Cette approche présenterait plusieurs inconvénients importants :

- (a) Cela obligerait les fournisseurs à mener un travail continu et complexe de surveillance du secteur pour déterminer si leurs services ont des « équivalents », une opération qui est loin d'être simple compte tenu du rythme rapide de l'innovation dans le secteur du *cloud*¹⁵.
- (b) Ce travail devrait être effectué pour tous les fournisseurs, ce qui créerait une charge onéreuse pour chacun d'entre eux.
- (c) Comme expliqué dans la réponse à la Question 23 *supra*, un service apparemment « standard » peut en réalité avoir des fonctionnalités uniques. Une comparaison granulaire des fonctionnalités pourrait s'avérer excessivement lourde pour les fournisseurs et potentiellement trompeuse pour les utilisateurs.

48.3 AWS partage le constat de l'ARCEP sur le fait qu'une harmonisation à haut niveau de l'offre de référence technique d'interopérabilité serait positive pour répondre aux besoins et obligations respectifs des clients et des fournisseurs. Outre les exigences concernant la documentation relative aux API et kits SDK décrites dans ses réponses aux Questions 42 et 43 *supra*, AWS suggère

¹⁵ Le secteur des services *cloud* connaît une évolution croissante ainsi que l'entrée de nouveaux acteurs. De nombreux nouveaux fournisseurs sont apparus ces dernières années, y compris ceux faisant partie du mouvement « *neo cloud* », ainsi que des entrants inattendus tels que des détaillants se lançant dans les services *cloud*. Par exemple, Lidl, une chaîne internationale de magasins alimentaires à bas prix d'origine allemande, a récemment annoncé son entrée sur le marché des fournisseurs de services *cloud*.

d'inclure les éléments suivants dans l'offre de référence technique d'interopérabilité :

- Description du service : description claire et détaillée de la fonctionnalité du service et de ses principales caractéristiques.
 - Formats de données et normes : informations sur les formats de données et les normes standards du secteur qu'il est possible d'utiliser dans le cadre du service.
 - Capacités d'exportation et d'importation : détails sur les fonctionnalités d'exportation et d'importation de données, y compris sur les formats qu'il est possible d'utiliser.
 - Usages courants de l'interopérabilité : exemples et détails sur les cas d'usage courants pour lesquels le service est interopérable avec les offres d'autres fournisseurs du même type de service.
 - Protocoles qui peuvent être utilisés : protocoles standards du secteur et spécifications techniques qu'il est possible d'utiliser dans le cadre du service, le cas échéant.
 - Toute autre référence à la documentation et documents publiés par le fournisseur sur la manière dont le service interagit avec les services du même type offerts par d'autres fournisseurs¹⁶.
- 48.4 Bien qu'AWS apprécie l'intention de l'ARCEP d'améliorer la transparence et la comparabilité, AWS met en garde contre une harmonisation trop stricte des offres de référence. Le secteur des services *cloud* se caractérise par une innovation et une différenciation rapide. Une normalisation excessive du format des offres de référence risquerait de ne pas refléter les propositions de valeur uniques des différents services et pourrait potentiellement nuire aux clients en limitant la capacité des fournisseurs à présenter leurs services de manière optimale. Au lieu de cela, AWS suggère une approche qui assure la fourniture constante des informations essentielles sur l'interopérabilité et la portabilité, tout en permettant une certaine souplesse dans le choix de la manière dont les fournisseurs présentent les caractéristiques uniques de leurs services.

49. Partagez-vous le constat de l'Autorité quant au faible besoin de normalisation supplémentaire des services IaaS ? Dans le cas contraire, quels services et aspects de ces services devraient faire l'objet de travaux de normalisation, sous quelles formes et pour quelles raisons ?

49.1 AWS considère qu'une normalisation des services IaaS n'est pas nécessaire. AWS souligne également qu'en vertu du Data Act, les services qui concernent des ressources informatiques modulables et variables limitées à des « éléments d'infrastructure » sont soumis à l'exigence d'équivalence fonctionnelle prévue à l'article 30, paragraphe 1, et

¹⁶ Par exemple, voir : <https://aws.amazon.com/blogs/database/perform-a-two-step-database-migration-from-an-on-premises-oracle-database-to-amazon-rds-for-oracle-using-rman/>.

ne seront pas couverts par les spécifications communes ou les normes harmonisées d'interopérabilité que la Commission européenne doit adopter.

50. Partagez-vous l'analyse de l'Arcep concernant le besoin de normalisation des services PaaS ? Le cas échéant, quels services et aspects des services PaaS devraient faire l'objet de travaux de normalisation, sous quelles formes et pour quelles raisons ?

50.1 Bien qu'AWS ne soit pas d'accord avec la suggestion d'une distinction entre les services *cloud* « standards » et « spécifiques », AWS salue l'approche nuancée de l'ARCEP qui diminue le nombre de services PaaS susceptibles de faire l'objet d'un éventuel travail de normalisation, en fonction de la nature « standard » ou « spécifique » du service concerné, et, si ce dernier est considéré « spécifique », en fonction de son potentiel d'innovation. Cependant, AWS a des préoccupations concernant la praticité et les conséquences potentielles d'une telle approche.

50.2 AWS estime qu'il est difficile, voire impossible, pour une autorité de régulation, un client ou même un fournisseur de services *cloud* de prédire exactement le potentiel d'innovation d'un service donné. L'histoire de la technologie abonde d'exemples de services ou de fonctionnalités qui semblaient de niche au départ, mais se sont ensuite avérés révolutionnaires, et *vice versa*. Tenter d'établir une distinction entre les services en fonction de leur potentiel d'innovation perçu pourrait entraîner des conséquences inattendues, voire étouffer l'innovation que cette distinction vise à protéger.

50.3 AWS fait valoir que la « fabrication » de nouvelles normes pour les services *cloud*, en particulier pour les outils PaaS, n'ayant pas émergées spontanément avec la pratique, doit être abordée avec prudence. L'adoption de telles normes pourrait freiner, voire mettre fin, au développement d'outils PaaS, si les développeurs étaient obligés de permettre l'utilisation des outils PaaS par tous les fournisseurs de services *cloud*, parce qu'ils pourraient ne pas avoir les ressources nécessaires pour se conformer à cette obligation. Par conséquent, plutôt que de faire appel à un organisme de normalisation pour élaborer des normes applicables aux services PaaS, AWS propose, comme expliqué *supra* dans sa réponse à la Question 45, de donner la priorité à la formalisation des protocoles et normes développés par le secteur et largement acceptés par celui-ci, pour les services PaaS concernés. AWS accueillerait favorablement l'opportunité de contribuer à l'évaluation et à l'identification des services PaaS susceptibles d'être soumis à ce processus, ainsi qu'à la sélection des protocoles et des spécifications appropriés. Une démarche collaborative permettrait de tirer parti de l'expertise du secteur pour garantir que les spécifications adoptées sont à la fois pratiques et bénéfiques pour les clients du *cloud*.

51. Que pensez-vous d'initier des travaux de normalisation sur les services auxiliaires, notamment sur les services IAM ? Outre ce type de services, d'autres services auxiliaires devraient-ils faire l'objet de tels travaux et selon quelles priorités ?

51.1 AWS n'est pas d'accord avec la proposition d'initier des travaux de normalisation sur les services auxiliaires, en particulier sur les services IAM. Comme indiqué dans sa réponse à la Question 22 *supra*, AWS soutient que (i) le niveau d'adoption des protocoles d'identité standards actuel permet aux clients d'intégrer l'authentification et l'autorisation d'identité sur plusieurs

clouds publics¹⁷, et (ii) les services et outils de facturation et d'observabilité ne posent pas de difficultés techniques à la capacité des clients de changer ou d'utiliser plusieurs fournisseurs de manière simultanée.

- 51.2 Par exemple, en ce qui concerne les protocoles d'identité standard, AWS en fait la promotion et les soutient. Les clients peuvent provisionner (c'est-à-dire synchroniser) automatiquement leurs informations d'identité depuis leur fournisseur d'identité vers *IAM Identity Center* en utilisant le protocole SCIM v2.0¹⁸, qui est standard dans le secteur. AWS teste les intégrations de l'*Identity Center* avec des services IAM tiers couramment utilisés tels qu'Okta, OneLogin et Microsoft Entra ID, et fournit des instructions détaillées à ses clients pour leur permettre de connecter leurs services¹⁹. IAM permet également aux clients d'utiliser la norme SAML v2.0 reconnue dans le secteur ou la norme OIDC pour accéder directement à AWS²⁰. Amazon Cognito prend en charge la fédération avec les *pools* d'identités Amazon Cognito et prend en charge SAML 2.0, OIDC et certains fournisseurs d'identité sociaux OAuth 2.0²¹.
- 51.3 Ainsi, les clients peuvent utiliser des services tiers pour stocker leurs identités, et les services AWS ou des applications externes pour gérer et utiliser ces identités.
- 51.4 [SDA]
- 51.5 Lorsque les solutions standards présentent des lacunes, AWS a cherché des solutions, notamment en développant la politique de langage Cedar pour les autorisations²² et en créant Open Cybersecurity Schema Framework (OCSF), un consortium pour une connexion de sécurité interopérable.²³
- 51.6 En ce qui concerne les préoccupations de l'ARCEP sur les potentiels risques de sécurité liés à la migration ou à l'utilisation simultanée en raison du manque d'interopérabilité entre les systèmes IAM, il est important, pour la sécurité des clients, d'assurer une cohérence entre les fournisseurs de cloud en matière d'autorisation et d'authentification. [SDA]. Les services de gestion des identités et des accès sont fondamentaux pour la posture de sécurité des clients. Toute initiative de normalisation dans ce domaine doit accorder la priorité à la sécurité et permettre des mises à jour ainsi que des développements techniques rapides afin de réagir promptement aux vulnérabilités et menaces émergentes. Une normalisation trop rigide serait susceptible d'entraver la capacité d'un fournisseur à déployer rapidement des mises à jour de sécurité essentielles ou

¹⁷ Voir aussi notre réponse à la Question 32 *supra*.

¹⁸ Voir https://docs.aws.amazon.com/fr_fr/singlesignon/latest/userguide/provision-automatically.html.

¹⁹ Voir https://docs.aws.amazon.com/fr_fr/singlesignon/latest/userguide/tutorials.html. Par exemple, les instructions de connexion à Okta sont disponibles ici : https://docs.aws.amazon.com/fr_fr/singlesignon/latest/userguide/gs-okta.html.

²⁰ Voir https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/id_roles_providers_saml.html pour l'utilisation de SAML et https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/id_roles_providers_create_oidc.html pour l'utilisation de OIDC

²¹ Voir https://docs.aws.amazon.com/fr_fr/cognito/latest/developerguide/external-identity-providers.html pour les instructions.

²² Voir <https://www.cedarpolicy.com/en>. Voir aussi la réponse à la Question 32, paragraphe 32.3.

²³ Voir <https://github.com/ocsf>.

des fonctionnalités de sécurité innovantes, exposant ainsi potentiellement les clients à un risque accru. Par conséquent, bien que l'interopérabilité soit importante, elle ne doit pas être réalisée au détriment de l'agilité qui est nécessaire pour maintenir des mesures de sécurité robustes dans les services de gestion des identités et des accès, où les considérations de sécurité sont particulièrement sensibles.

- 51.7 En tout état de cause, AWS estime que toute initiative de normalisation des services d'identité devrait être fondée sur l'adoption de spécifications d'interopérabilité ouvertes, reposant sur les protocoles standards du secteur, ou des spécifications *open source* déjà largement acceptées par le secteur, plutôt que sur de nouvelles normes qui seraient élaborées par un organisme de normalisation. Si l'ARCEP décidait néanmoins de créer de nouvelles normes, malgré l'opinion d'AWS énoncée *supra*, AWS serait disposée à contribuer à l'évaluation et à l'identification des protocoles et spécifications appropriés. Cette approche collaborative permettrait de tirer parti de l'expertise du secteur pour garantir que les spécifications adoptées soient à la fois pratiques et bénéfiques pour les clients du *cloud*.

52. Que pensez-vous du besoin de normaliser notamment les structures et les formats d'échanges de données entre des services SaaS du même type ? Le cas échéant, quels types de services SaaS devraient faire l'objet de tels travaux en priorité ? Pour quelle raison ?

- 52.1 AWS pense que les exigences relatives aux données exportables et aux actifs numériques prévues par le Data Act et Loi SREN répondront aux préoccupations de l'ARCEP concernant les services SaaS. En application du Data Act, tous les fournisseurs de services de traitement de données, y compris les fournisseurs de SaaS, devront rendre les données exportables et les actifs numériques accessibles aux clients dans un format structuré, couramment utilisé et lisible par machine. Tant que les formats de données du fournisseur d'origine respectent ces conditions, le fait que le fournisseur de destination utilise un format différent ne devrait pas être considéré comme un obstacle technique au changement de fournisseur.
- 52.2 AWS souligne que la normalisation des services SaaS, en particulier au niveau sémantique, pose des difficultés considérables. La normalisation sémantique exige un accord de l'ensemble du secteur sur la signification et l'interprétation des données. Or, il est difficile de parvenir à tel accord compte tenu de la diversité et de l'évolution rapide des offres de SaaS.
- 52.3 Plutôt que d'entreprendre une normalisation complète des services SaaS, AWS suggère l'adoption d'une approche concentrée sur les normes techniques de niveau inférieur pour faciliter l'interopérabilité sans freiner l'innovation :
- (a) Prioriser les efforts de normalisation sur les normes techniques génériques relatives au transport, à la syntaxe et à la structure, comme HTTP, REST et XML.

- (b) Éviter de normaliser la sémantique et les détails spécifiques aux services, car ce sont des aspects qui permettent aux fournisseurs de différencier leurs offres et stimulent l'innovation.

53. Avez-vous d'autres commentaires sur les enjeux soulevés dans cette consultation publique ?

N/A

54. Au-delà de tous les sujets abordés dans les sections précédentes de cette consultation, quels autres enjeux relatifs à la régulation des services *cloud* mériteraient, selon vous, d'être portés à l'attention de l'Arcep ?

54.1 [SDA]

54.2 AWS tient à remercier l'ARCEP de l'écoute et du dialogue déjà initié en amont de cette consultation et se réjouit de la perspective de continuer à échanger avec l'ARCEP dans les semaines et mois à venir. Nous saluons l'ouverture démontrée dans l'analyse et les questions de la consultation qui tentent d'apporter une réglementation proportionnée et ciblée, garantissant que le secteur du cloud reste innovant et profite à l'ensemble de l'économie.