

## **Consultation publique de l'ARCEP sur le projet de lignes directrices sur les coûts susceptibles d'être pris en compte dans la détermination des frais de changement de fournisseur de services informatique en nuage autres que les frais liés au transfert de données**

Amazon Web Services (« AWS ») est heureuse de pouvoir répondre à la consultation publique de l'ARCEP sur le projet de lignes directrices sur les coûts susceptibles d'être pris en compte dans la détermination des frais de changement de fournisseur, autres que les coûts liés aux transferts de données. La réponse d'AWS aborde trois points couverts par la consultation :

- La section 1 expose le point de vue d'AWS sur la portée de l'obligation de fournir une assistance raisonnable.
- La section 2 présente la position d'AWS sur la proposition de l'ARCEP de traiter les frais de stockage temporaire des données engagés dans le cadre du changement de fournisseur de la même manière que les frais de changement de fournisseur.
- La section 3 apporte certaines précisions proposées par AWS concernant la position de l'ARCEP sur les frais liés au maintien de la sécurité pendant le processus de changement de fournisseur.

### **1. Proposition de l'ARCEP concernant la portée de l'obligation de fournir une assistance raisonnable et les frais découlant de la fourniture d'une assistance raisonnable**

1.1. AWS partage en principe la position de l'ARCEP selon laquelle les frais découlant de la fourniture d'une assistance raisonnable au client au cours du processus de changement de fournisseur font partie des frais de changement de fournisseur au sens du Règlement concernant des règles harmonisées portant sur l'équité de l'accès aux données et l'utilisation des données (Règlement sur les données) du 13 décembre 2023 (« Data Act » ou « Règlement »). Toutefois, **AWS souhaite souligner que certains aspects de l'analyse de l'ARCEP sur la portée de l'obligation de fournir une assistance raisonnable nécessitent des précisions supplémentaires et, dans certains cas, des corrections, afin de garantir que la portée de l'obligation de fournir une assistance raisonnable du fournisseur d'origine ne soit pas interprétée d'une manière qui va au-delà de ce qui est requis par le Règlement, ou à créer des obligations techniquement irréalisables ou pratiquement inapplicables.**

#### ***1.2. Assistance technique pour résoudre les difficultés rencontrées au cours du processus de changement de fournisseur***

- L'ARCEP identifie « *le support technique apportée par le fournisseur d'origine lorsque le client rencontre des difficultés dans le processus de changement de fournisseur* » comme un premier exemple d'actions relevant du champ d'application de l'assistance raisonnable.
- AWS convient que lorsqu'un client rencontre des difficultés au cours du processus de changement de fournisseur qui sont imputables aux capacités du fournisseur d'origine (par exemple un service ne fonctionnant pas comme il le devrait ou une défaillance de la fonctionnalité d'extraction des données), le fournisseur d'origine a l'obligation de résoudre ces problèmes dans le cadre de son obligation de fournir une assistance raisonnable.
- Il est toutefois essentiel d'établir une distinction claire entre (i) les difficultés résultant du fait que les services du fournisseur d'origine ne fonctionnent pas comme prévu ou ne sont pas conformes aux exigences du Règlement, et (ii) les difficultés spécifiques à la charge de travail ou découlant des choix architecturaux du client, de sa stratégie de migration, de ses compétences techniques, d'une configuration incorrecte ou des spécificités de l'environnement de destination. **Cette dernière catégorie (point (ii)) ne donne pas lieu à une obligation de fourniture d'une assistance raisonnable de la part du fournisseur d'origine.** Premièrement, comme AWS l'a expliqué dans le cadre de ses précédentes contributions aux consultations d'ARCEP, le fournisseur d'origine n'a pas de visibilité sur le contenu du client hébergé sur les services

AWS. L'accès au contenu du client est strictement interdit pour personnel AWS, et les systèmes AWS sont conçus d'une manière qui empêche cet accès. Les clients conçoivent, développent et exploitent leurs solutions informatiques sur AWS, en faisant des choix architecturaux propres à leurs besoins. Deuxièmement, le fournisseur d'origine n'est pas en mesure de diagnostiquer ou de résoudre les difficultés découlant des raisons mentionnées au point (ii) ci-dessus. Même dans le cas hypothétique où le fournisseur d'origine se verrait accorder l'accès par le client, la résolution de toute difficulté découlant de ces raisons nécessiterait de comprendre l'architecture informatique du client, la logique commerciale sous-jacente à ses charges de travail, ainsi que les exigences de configuration et de compatibilité de l'environnement du fournisseur de destination – autant d'éléments qui ne relèvent ni des connaissances, ni de la responsabilité du fournisseur d'origine. Comme le confirme le considérant (92) du Règlement, « *Un fournisseur d'origine de services de traitement de données n'a pas accès à l'environnement du fournisseur de destination de services de traitement de données ou n'a pas d'informations sur celui-ci* » et son obligation de fournir une assistance raisonnable doit être proportionnée. Lorsqu'un client rencontre une difficulté dans le cadre du changement de fournisseur découlant de la manière dont ses charges de travail sont structurées, de la complexité des relations de ses données, ou d'incompatibilités avec l'environnement du fournisseur de destination résultant de ses choix, il ne s'agit pas d'un problème que le fournisseur d'origine peut ou doit résoudre dans le cadre de son obligation de fournir une assistance raisonnable gratuite.

- Interpréter autrement l'obligation de fournir une assistance raisonnable reviendrait en pratique à exiger des fournisseurs d'origine qu'ils offrent gratuitement des services de conseil en migration aux clients qui changent de fournisseur, qu'ils analysent leurs charges de travail spécifiques, qu'ils donnent des conseils sur les stratégies de migration et qu'ils résolvent les problèmes découlant de l'architecture informatique du client ou d'autres choix du client, ce qui ne fait pas partie des exigences du Règlement. Comme indiqué au considérant (85) du Règlement sur les données, le changement de fournisseur est une opération menée par le client, qui consiste en plusieurs étapes, et les fournisseurs et les clients ont des niveaux de responsabilité différents selon les étapes du processus. L'obligation du fournisseur d'origine est de veiller à ce que ses services fonctionnent comme ils le devraient, conformément aux exigences du Règlement, et de résoudre toute difficulté découlant d'une défaillance des services et des capacités que le fournisseur d'origine offre. Si le client rencontre des difficultés liées à des raisons propres à sa charge de travail qui l'obligent à construire son plan de changement de fournisseur en conséquence, cela relève de la responsabilité du client lui-même, ou peut être résolu par le biais de services supplémentaires payants d'assistance à la migration que le client peut choisir de se procurer auprès du fournisseur d'origine, du fournisseur de destination ou d'un tiers, comme le prévoit expressément le considérant (89) du Règlement sur les données.

### 1.3. ***Opérations de préparation des données directement liées à l'extraction***

- L'ARCEP estime que « *les opérations de traitement des données directement liées à l'étape d'extraction sont susceptibles de relever de l'assistance raisonnable* », y compris « *la préparation des données en vue de leur extraction, en particulier leur conversion dans un format couramment utilisé et lisible par machine* ». AWS partage la position de l'ARCEP car le Règlement prévoit une obligation claire pour le fournisseur d'origine de permettre au client d'exporter ses données et ses actifs numériques exportables dans un format couramment utilisé et lisible par machine. Les opérations de préparation des données qui sont directement liées au respect de cette obligation, incluant la conversion de format si nécessaire (c'est-à-dire lorsque le format d'origine supporté par le service en question ne peut pas être exporté), relèvent bien du champ d'application de l'assistance raisonnable.

- **Cependant, l'ARCEP étend ensuite ce champ d'application pour y inclure « la vérification [du] caractère complète et intègre [des données], une fois ces données extraites ». AWS ne souscrit pas à cette position, pour les raisons suivantes :**

- a) *Après l'extraction, les données en question quittent l'environnement du fournisseur d'origine : l'étape de vérification se déroule en dehors de l'environnement du fournisseur d'origine. La formulation même de l'ARCEP reconnaît que cette vérification doit avoir lieu « une fois ces données extraites ». Le fournisseur d'origine ne dispose d'aucun moyen technique pour vérifier l'exhaustivité et l'intégrité des données qui se trouvent en dehors de son propre environnement.*

L'obligation du fournisseur d'origine en vertu du Règlement est de rendre les données disponibles à l'exportation dans un format couramment utilisé et lisible par machine, et de fournir aux clients les moyens d'exporter leurs données sous cette forme. Une fois que les données quittent l'environnement du fournisseur d'origine, celui-ci n'a aucun moyen d'effectuer une quelconque vérification sur celles-ci.

- b) *AWS n'a pas de visibilité sur les contenus des clients.* AWS définit les contenus des clients comme les logiciels (y compris les images de machine), des données, du texte, de l'audio, de la vidéo ou des images qu'un client transfère à AWS pour le traitement, le stockage ou l'hébergement par les services AWS en relation avec le compte AWS du client, ainsi que tout résultat de calculs qu'un client obtient de ce qui précède par le biais de son utilisation des services AWS. Comme indiqué ci-dessus, l'accès aux contenus des clients est strictement interdit pour personnel AWS, et les systèmes AWS sont conçus d'une manière qui empêche cet accès. Il s'agit d'un principe fondamental du *cloud computing* et d'un pilier de la confiance des clients. Sans accès au contenu même des données, AWS ne peut connaître que le volume de données qui a été transféré et le service à partir duquel ce transfert a eu lieu. AWS ne peut pas « vérifier » si les données extraites ont un caractère « complet et intègre », car cela l'obligerait à accéder, lire et analyser le contenu des données du client, ce qui constituerait une violation de ce principe fondamental.
- c) *La solution appropriée doit être initiée par le client.* Si un client estime que les données qu'il a extraites ne sont pas complètes ou ont perdu leur intégrité au cours du processus d'extraction, la bonne marche à suivre consiste pour le client à examiner les journaux d'erreurs, à réessayer et à prendre d'autres mesures de dépannage, et, si ces efforts échouent, à informer le fournisseur d'origine afin que le problème soit examiné. Si le problème est imputable à une défaillance du côté du fournisseur d'origine (par exemple, un dysfonctionnement de la fonctionnalité d'exportation), alors le fournisseur d'origine le résoudrait au titre de son obligation d'assurer le bon fonctionnement de ses services. Toutefois, cela diffère fondamentalement du fait d'imposer au fournisseur d'origine une obligation générale de vérification proactive du caractère complet et intègre de toutes les données extraites, ce qui est à la fois techniquement impossible et contraire au modèle opérationnel de base des services cloud.

- Dans la mesure où la référence de l'ARCEP à la « *vérification, une fois ces données extraites, de leur caractère complet et intègre* » vise à désigner la vérification de l'intégrité des données après leur *conversion* dans un format couramment utilisé et lisible par machine, plutôt qu'une vérification après que les données ont quitté l'environnement du fournisseur d'origine, AWS relève que les clients disposent déjà des outils nécessaires au sein de leur environnement AWS pour effectuer cette vérification avant l'extraction. Les services AWS fournissent aux clients les moyens d'examiner, de comparer et de valider leurs données au sein de leur propre environnement.

#### 1.4. « Tester » le changement de fournisseur

- L'ARCEP estime que « *la réalisation de tests afin de vérifier le fonctionnement du processus de changement de fournisseur* » relève de l'obligation de fournir une assistance raisonnable et se réfère aux clauses contractuelles types (CCT) de la Commission européenne pour soutenir la proposition selon laquelle les frais liés aux tests doivent être considérés comme des frais de changement de fournisseur. **AWS estime que cette proposition est problématique et impraticable pour plusieurs raisons. AWS souhaite donc souligner que les tests devraient être retirés du champ d'application des lignes directrices que l'ARCEP s'apprête à adopter.**

- a) L'obligation de réaliser ou de faciliter des « tests » du processus de changement de fournisseur n'est prévue par aucune disposition du Règlement, ni par ses considérants. Bien que les CCT fassent référence à des « tests », les CCT sont des instruments non contraignants qui ne créent pas d'obligations juridiques allant au-delà de celles établies par le Règlement lui-même. Se

fonder sur les CCT pour élargir la portée des obligations impératives serait incompatible avec le cadre législatif. En outre, bien qu'elles fassent référence à des « tests », les CCT ne fournissent aucune explication supplémentaire sur les points énumérés au paragraphe (b) ci-dessous, et soulèvent donc les mêmes préoccupations tout en imposant une obligation irréalisable aux fournisseurs d'origine.

- b) Ce qui constitue exactement un « test » visant à vérifier le fonctionnement du processus de changement de fournisseur n'est pas clair, car il ne s'agit pas d'un concept issu du Data Act. Ni les CCT ni les lignes directrices de l'ARCEP n'abordent les questions pratiques cruciales qui se poseraient inévitablement lors de la mise en œuvre. Par exemple, il n'est pas clair si un « test » nécessiterait d'extraire effectivement les données du client et de les transférer vers le fournisseur de destination, et si tel est le cas, ce qu'il adviendrait des données une fois celles-ci arrivées à destination après le test : le changement serait-il considéré comme complet, ou il faudrait-il le renvoyer et retransférer les données (ce qui multiplierait le volume des transferts de données, avec les frais et les implications en matière de sécurité qui en découlent) ? Savoir qui déterminerait si un test a été « réussi » n'est pas clair non plus étant donné que le fournisseur d'origine ne peut pas évaluer si les charges de travail en question fonctionnent correctement dans l'environnement du fournisseur de destination, car il n'a ni accès ni connaissance de cet environnement; comme le confirme le considérant (92) du Règlement sur les données, « *Un fournisseur d'origine de services de traitement de données n'a pas accès à l'environnement du fournisseur de destination de services de traitement de données ou n'a pas d'informations sur celui-ci* ». En outre, les conséquences d'un test jugé « infructueux » ne sont absolument pas abordées : la période de changement redémarrerait-elle, le fournisseur d'origine serait-il tenu de procéder à de nouveaux tests, et sur quelle base ces décisions seraient-elles prises ? L'absence de réponses à ces questions fondamentales démontre que le « test », tel qu'il est actuellement conçu, n'est pas une notion prévue par le Règlement pour servir de base à une obligation réglementaire. En pratique, l'introduction d'une telle obligation serait source d'une grande incertitude et de litiges potentiels entre les fournisseurs et les clients, sans base juridique claire ni cadre pratique pour les résoudre. Cela reviendrait à créer une obligation entièrement nouvelle qui ne repose sur aucun fondement législatif.
- c) La réalisation de tout test doit relever de la responsabilité du client. Les clients peuvent, à tout moment, utiliser les fonctionnalités d'exportation mises à disposition par AWS pour extraire leurs données et vérifier que leur plan de migration fonctionnera comme prévu. Le rôle du fournisseur d'origine est de s'assurer que ses fonctionnalités et services d'exportation fonctionnent correctement, et non de mener des tests de bout en bout d'un processus s'étendant sur plusieurs environnements, incluant l'infrastructure du fournisseur de destination, sur laquelle le fournisseur d'origine n'a ni contrôle, ni visibilité.

1.5. **Conclusion** : AWS soutient le principe selon lequel les frais découlant d'une « assistance raisonnable » – incluant l'assistance technique pour résoudre les problèmes imputables à l'environnement du fournisseur d'origine et les opérations de préparation des données directement liées à l'extraction dans un format couramment utilisé et lisible par machine – relèvent bien du champ d'application des frais de changement de fournisseur. **Toutefois, AWS fait respectueusement valoir que les lignes directrices de l'ARCEP devraient :**

- a) Clarifier que l'obligation de fournir une assistance raisonnable ne s'étend pas au conseil en migration propre à la charge de travail ni au dépannage de problèmes découlant des choix architecturaux du client, de sa stratégie de migration, de ses compétences techniques, d'une configuration incorrecte ou des spécificités de l'environnement de destination du client ;
- b) Supprimer la vérification des données post-extraction du champ d'application de l'assistance raisonnable, car cela est techniquement irréalisable pour le fournisseur

d'origine et nécessite des actions contraires aux principes fondamentaux de sécurité du cloud ; et

- c) Supprimer les tests du processus de changement du champ d'application de l'assistance raisonnable, car cela crée une nouvelle obligation importante sans fondement juridique au titre du Data Act, soulève des questions pratiques insolubles et doit en tout état de cause être une activité pilotée par le client compte tenu de l'absence d'accès du fournisseur d'origine aux contenus du client et à l'environnement de destination.

## **2. Proposition de l'ARCEP concernant les frais liés au stockage temporaire des données pendant le processus de changement de fournisseur**

- 2.1. L'ARCEP note que « *certaines migrations peuvent occasionner la mobilisation de ressources supplémentaires pour la réalisation du processus de changement de fournisseur* » et identifie le stockage temporaire d'une copie des données pendant le processus de changement comme un exemple de ces ressources supplémentaires. L'ARCEP considère que ce stockage temporaire peut être pris en compte pour la détermination des frais de changement de fournisseur « *lorsque ce stockage résulte d'une contrainte technique le rendant nécessaire pour la réalisation du processus* ». L'ARCEP note en outre que les clients ne devraient pas payer deux fois pour le même stockage - une première fois dans le cadre de leur utilisation normale du service cloud et une seconde fois dans le cadre du processus de changement de fournisseur. **AWS souhaite contester la qualification par l'ARCEP du stockage temporaire des données pendant le processus de changement de fournisseur comme un frais devant être pris en compte pour la détermination des frais de changement de fournisseur.**

### **Les frais de stockage temporaire sont des frais de service standard, et non des frais liés au changement de fournisseur :**

- 2.2. Le Règlement sur les données définit les frais de changement de fournisseur comme « *les frais, autres que les frais de service standard ou les pénalités de résiliation anticipée, imposés par un fournisseur de services de traitement de données à un client pour les actions requises par le présent règlement pour changer de fournisseur [...]* ». Le considérant (88) du Règlement sur les données précise en outre que les frais de changement de fournisseur « *sont destinés à répercuter les coûts que le fournisseur d'origine de services de traitement de données peut encourir en raison du processus de changement de fournisseur* ». Les exemples courants cités au considérant (88) sont « *les frais liés au transfert des données d'un fournisseur de services de traitement de données à un autre ou à une infrastructure TIC sur site (les frais de transfert des données) ou les frais encourus pour des actions de soutien spécifiques pendant le processus de changement de fournisseur* ». Le considérant (89) confirme ensuite que « *les frais de service standard afférents à la fourniture des services de traitement de données ne constituent pas des frais de changement de fournisseur. Ces frais de service standard ne sont pas susceptibles d'être supprimés et restent applicables jusqu'à ce que le contrat de fourniture des services concernés cesse de s'appliquer* ».
- 2.3. Le stockage de données, qu'il s'agisse de l'ensemble de données original stocké par un client ou d'une copie de cet ensemble de données, est un service cloud essentiel pour lequel les clients paient des frais de service standard. Ces frais sont facturés pour l'utilisation de l'infrastructure de stockage du fournisseur, quelle que soit le but de l'utilisation par le client. Un client qui stocke des données sur un service cloud paie pour les ressources de stockage consommées, que ces données soient stockées à des fins opérationnelles, de reprise après sinistre, de conformité ou dans le cadre d'un processus de changement de fournisseur. Le simple fait qu'un client continue d'utiliser des services de stockage ou crée des copies supplémentaires de ses données au cours d'un processus de changement de fournisseur ne transforme pas les frais liés à ces services de stockage en frais de changement de fournisseur au sens du Règlement.

- 2.4. Comme expliqué dans nos contributions aux consultations précédentes, les fournisseurs de services cloud structurent leur tarification afin que les clients paient des frais de service standard pour l'utilisation de leurs services, tels que le stockage et la récupération de données. Ces frais sont essentiels pour le fonctionnement et l'utilisation du service et ne sont pas spécifiques au changement de fournisseur ou à l'exportation de données. Des frais de stockage constituent des frais de service standard par excellence, facturés pour l'utilisation du service indépendamment de toute activité de changement de fournisseur. Le client utilise l'infrastructure de stockage du fournisseur, consomme des ressources de calcul et de stockage, et doit payer pour cette utilisation de la même manière que tout autre client utilisant le même service à d'autres fins.
- 2.5. La conservation de copies de données, y compris les sauvegardes ou les copies instantanées (*snapshot*), est une pratique standard et bien établie dans le secteur du *cloud computing*, et fait partie de ce que l'on appelle communément une charge de travail conforme aux bonnes pratiques d'architecture cloud. Les clients créent et conservent régulièrement des copies de données à des fins de reprise après sinistre, de continuité des activités, de conformité et de résilience opérationnelle. Ces copies sont stockées à l'aide des services de stockage standard du fournisseur et sont facturées en tant que frais de service standard. L'infrastructure de stockage consommée, les ressources de calcul utilisées et les coûts opérationnels supportés par le fournisseur sont identiques, quelle que soit l'objectif du client. Si les copies de données créées à des fins de reprise après sinistre ou de continuité des activités sont correctement facturées au titre des frais de service standard, les copies de données créées dans le cadre d'un processus de changement de fournisseur doivent être traitées de la même manière. Le Règlement ne prévoit pas d'exception aux frais de service standard en fonction de l'intention du client quant à l'utilisation du service.

**La notion de « contrainte technique » est floue et ne peut être vérifiée objectivement**

- 2.6. L'ARCEP limite le champ d'application du stockage temporaire facturable aux cas où celui-ci résulte d'une contrainte technique le rendant nécessaire pour le changement de fournisseur. Outre les préoccupations fondamentales exposées dans la section précédente, **AWS fait valoir que cette notion est floue et génère également des préoccupations pratiques.**
- 2.7. Premièrement, ce qui constituerait une « contrainte technique » dans ce contexte n'est pas clair. La décision de créer une copie temporaire des données (lors du changement de fournisseur, ou dans le cadre de leurs opérations quotidiennes comme indiqué ci-dessus) est une décision du client, motivée par ses propres préférences en matière de gestion des risques, sa stratégie de migration et ses exigences en matière de continuité des activités.
- 2.8. Deuxièmement, le fournisseur d'origine n'a aucune visibilité si un cas particulier de stockage de données résulte d'une « contrainte technique » ou des préférences propres du client. Comme expliqué précédemment, AWS n'a pas connaissance de la stratégie de migration du client, de l'architecture de l'environnement de destination, ni des raisons pour lesquelles le client pourrait choisir de conserver des copies temporaires de ses données. Le fournisseur d'origine ne peut pas déterminer si une opération de stockage donnée résulte d'une « contrainte technique » liée au processus de changement de fournisseur, car il ne connaît pas les détails du plan de changement de fournisseur du client, ni les exigences de l'environnement du fournisseur de destination.

**Risque d'abus**

- 2.9. Classer le stockage temporaire lors du changement de fournisseur en tant que charge de changement de fournisseur crée un risque d'abus au détriment des fournisseurs d'origine. Si les clients ont connaissance que le stockage consommé pendant le processus de changement de fournisseur sera gratuit, ils seront enclins à conserver des copies de leurs données sur l'infrastructure du fournisseur d'origine pendant des périodes prolongées, consommant ainsi des

ressources de stockage sans payer les frais de service standard. Cela ferait grimper les coûts pour le fournisseur d'origine, qui devrait donc *in fine* les répercuter sur tous les clients en appliquant des prix plus élevés pour les services de stockage généralement. Comme AWS l'a fait remarquer dans ses contributions précédentes, si les clients s'attendent à ne pas avoir à payer pour certains services lors de leur changement de fournisseur, ils pourraient adapter leur utilisation et exiger davantage de ces services qu'ils ne le feraient autrement, engendrant ainsi des pertes d'efficacité qui seraient finalement subies par tous les clients.

2.10. **Conclusion** : Pour les raisons exposées ci-dessus, AWS fait respectueusement valoir que les lignes directrices de l'ARCEP devraient :

- Clarifier que le stockage des données, y compris les copies temporaires, pendant le processus de changement de fournisseur constitue un service standard pour lequel s'appliquent des frais de service standard, et ne constitue pas un frais de changement de fournisseur au sens du Règlement, conformément au considérant (89) qui confirme que les frais de service standard ne sont pas susceptibles d'être supprimés et restent applicables jusqu'à ce que le contrat prenne fin ;
- Supprimer l'inclusion du stockage temporaire de données du champ des frais à prendre en compte pour la détermination des frais de changement de fournisseur, car cela est incompatible avec l'exclusion explicite des frais de service standard de la définition des frais de changement de fournisseur par le Règlement;
- Clarifier que le principe de non-double facturation reconnu par l'ARCEP serait correctement pris en compte en veillant à ce que les clients ne se voient pas facturer de frais spécifiques au changement de fournisseur en plus de leurs frais de stockage standard – au lieu de rendre la consommation de stockage gratuite pendant la période de changement de fournisseur.

### **3. Proposition de l'ARCEP concernant les frais liés au maintien de la sécurité pendant le processus de changement de fournisseur**

3.1. AWS partage la conclusion de l'ARCEP selon laquelle il n'existe pas de frais liés au maintien des garanties de sécurité pendant le processus de changement de fournisseur qui devraient être pris en compte dans la détermination des frais de changement de fournisseur, au motif que ces frais sont déjà supportés par les fournisseurs pour la prestation de leurs services. Comme l'ARCEP le note à juste titre, le Règlement exige que le fournisseur d'origine étende le niveau de sécurité auquel il s'est engagé pour ses services à tous les dispositifs techniques dont il est responsable pendant le processus de changement de fournisseur, comme le confirme le considérant (94) du Règlement. Cette obligation ne crée pas une norme de sécurité nouvelle ou supplémentaire - elle exige du fournisseur qu'il maintienne le même niveau de sécurité que celui qu'il assure déjà dans le cadre de la fourniture standard du service. Étant donné que ces frais de sécurité sont déjà supportés par le fournisseur dans le cadre de ses obligations de service courantes, ils ne devraient pas être pris en compte séparément dans les frais de changement de fournisseur. Comme AWS l'a souligné dans ses contributions aux consultations précédentes, garantir la sécurité et la qualité du transfert a certes un coût, mais contrairement aux frais liés au transfert de données, ces coûts ne découlent pas du changement de fournisseur en tant que tel et n'incluent pas de composante imputable au processus de changement. Ils sont inhérents à la fourniture de services cloud. En conséquence, **AWS soutient la position de l'ARCEP sur ce point.**

3.2. Il convient toutefois de noter que certains clients peuvent choisir d'utiliser des services de sécurité renforcés, tels qu'un chiffrement avancé ou des capacités de surveillance et de journalisation améliorées, en raison des caractéristiques spécifiques et de la sensibilité de leurs charges de travail (par exemple, les clients opérant dans des secteurs réglementés). Ces services

de sécurité renforcés sont soumis à des frais de service standard basés sur leur utilisation par le client. Le fait qu'un client continue d'utiliser ces services de sécurité renforcés pendant le processus de changement de fournisseur ne transforme pas les frais liés à ces services en frais de changement de fournisseur. Conformément au principe énoncé au considérant (89) du Règlement, les frais liés aux services de sécurité renforcés que le client a choisi d'utiliser ne constituent pas des frais de changement de fournisseur et restent applicables jusqu'à ce que le contrat de fourniture des services concernés cesse de s'appliquer, car le fournisseur d'origine peut déjà remplir son obligation de maintenir un niveau élevé de sécurité pendant le changement de fournisseur sans avoir à recourir à l'utilisation supplémentaire de ces services « renforcés ».

#### **4. Conclusion**

- 4.1. Pour les raisons exposées ci-dessus, AWS soutient que les lignes directrices de l'ARCEP devraient garantir que le périmètre des obligations du fournisseur d'origine pendant le processus de changement de fournisseur reste conforme au Règlement et ne s'étende pas au-delà de ce qui est requis, réalisable sur le plan technique ou pratique.
- 4.2. En particulier, AWS invite l'ARCEP à :
- Clarifier que l'obligation de fournir une assistance raisonnable ne s'étend pas au conseil en migration propre à la charge de travail, ni au dépannage de problèmes découlant des choix du client lui-même, et que la vérification des données après extraction et les tests du processus de changement de fournisseur ne relèvent pas de l'assistance raisonnable pour les raisons détaillées à la section 1 ; et
  - Reconnaître que dans le cas où le client souhaiterait stocker temporairement une copie de ses données exportables pendant le processus de fournisseur, cela correspond à un service standard pour lequel des frais de service standard s'appliquent, conformément à l'exclusion explicite par le Règlement des frais de service standard de la définition des frais de changement de fournisseur, comme détaillé à la section 2.

AWS remercie l'ARCEP de lui avoir donné l'opportunité de contribuer à cette consultation et se tient à sa disposition pour fournir toute information complémentaire ou clarification dont elle pourrait avoir besoin.

\*\*\*