Livre blanc sur la protection des données au sein de l'UE

Novembre 2016

(Consultez le site http://aws.amazon.com/compliance/aws-whitepapers/ pour obtenir la version la plus récente de ce document et le site http://aws.amazon.com/de/data-protection/ pour obtenir la version allemande.)

Introduction

Ce document apporte des informations utiles aux clients souhaitant utiliser AWS afin de stocker des contenus comportant des données personnelles. Ce document décrit notamment la façon dont les clients peuvent utiliser les services AWS en accord avec la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et la libre circulation de ces données (« Directive »). Il a pour but d'aider les clients à comprendre :

- le mode de fonctionnement des services AWS, y compris la façon dont ils permettent aux clients de respecter la réglementation de l'Union européenne, de répondre à leurs besoins en matière de sécurité, et de chiffrer et protéger leurs contenus de toute autre manière ;
- le contrôle total que le client exerce sur les emplacements géographiques dans lesquels ses contenus peuvent être stockés et accessibles, et d'autres considérations relatives à la conformité ;
- les rôles respectifs qui incombent au client et à AWS en matière de gestion et de sécurisation des contenus stockés sur les services AWS.

Ce livre blanc est axé sur les questions habituellement posées par les clients d'AWS lorsqu'ils examinent les implications de la Directive dans le cadre de l'utilisation des services AWS pour stocker des contenus comportant des données personnelles. Il comprend également des considérations pertinentes que chaque client devra prendre en compte, telles que la nécessité pour le client de respecter les exigences spécifiques au secteur et les lois en vigueur dans d'autres juridictions dans lesquelles le client exerce son activité. Ce document est fourni à titre d'information uniquement. Il ne constitue pas un avis juridique et ne doit pas être considéré en tant que tel. Les exigences pouvant varier en fonction des clients, AWS encourage ces derniers à obtenir les conseils appropriés concernant l'implémentation de leurs environnements de protection de la confidentialité et des données et, de façon plus générale, les réglementations applicables à leur activité.

Considérations relatives aux contenus du client

Le stockage des contenus entraîne un certain nombre de considérations pratiques courantes que toutes les organisations doivent prendre en compte, notamment :

- Les contenus seront-ils sécurisés ?
- Où les contenus seront-ils stockés ?
- Qui aura accès aux contenus ?
- Quelles lois et réglementations s'appliquent aux contenus et de quelle manière peut-on s'y conformer ?

Ces considérations ne sont ni nouvelles, ni propres au cloud. Elles s'appliquent aux systèmes hébergés et utilisés en interne, ainsi qu'aux services tiers hébergés classiques. Lors de l'utilisation des services AWS, les clients gardent le contrôle de leurs contenus et ont la responsabilité, ainsi que la liberté totale, de gérer et de contrôler les exigences de sécurité des contenus qui leur sont propres, notamment :

- les contenus qu'ils choisissent de stocker sur AWS ;
- le chiffrement ou non des contenus, qu'ils soient au repos et en transit ;
- les services AWS qui seront utilisés avec les contenus ;
- la région dans laquelle les contenus seront stockés et traités ;
- le format et la structure des contenus et leur dissimulation ou anonymisation ;
- les personnes qui seront autorisées à accéder à ces contenus et la façon dont les droits d'accès sont accordés, gérés et révoqués.

Il incombe à AWS et au client d'assurer la sécurité des contenus du client en mettant en place les mesures appropriées. AWS implémente des contrôles de sécurité dans son environnement cloud sous-jacent, mais les clients AWS gardent le contrôle sur leurs contenus et la sécurité de ces derniers. Il est primordial de comprendre les rôles respectifs et différents qui incombent au client et à AWS dans le contexte des exigences de protection des données, qui peuvent s'appliquer aux données personnelles stockées sur AWS.

Sécurité des contenus du client

Le transfert de l'infrastructure informatique dans AWS signifie que le client et AWS jouent des rôles importants dans le fonctionnement et la gestion de la sécurité dans leurs sphères de responsabilité. AWS utilise, gère et contrôle les composants depuis le système d'exploitation hôte et la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles fonctionnent les services AWS. Le client est responsable de la gestion du système d'exploitation invité (y compris les mises à jour et correctifs de sécurité pour celui-ci) et des logiciels d'application associés, ainsi que de la configuration du pare-feu du groupe de sécurité fourni par AWS et d'autres fonctions liées à la sécurité. Le client se connecte généralement à l'environnement AWS via des services fournis par des tiers (par exemple, des fournisseurs d'accès à Internet). AWS ne fournit pas ces connexions et le client doit vérifier leur sécurité et les responsabilités de ces tiers envers leurs systèmes. Ce processus s'apparente à la collaboration avec un fournisseur de service de réseau qui assure la connectivité aux centres de données sur site.

Ce modèle est présenté ci-dessous, dans la Figure 1 :

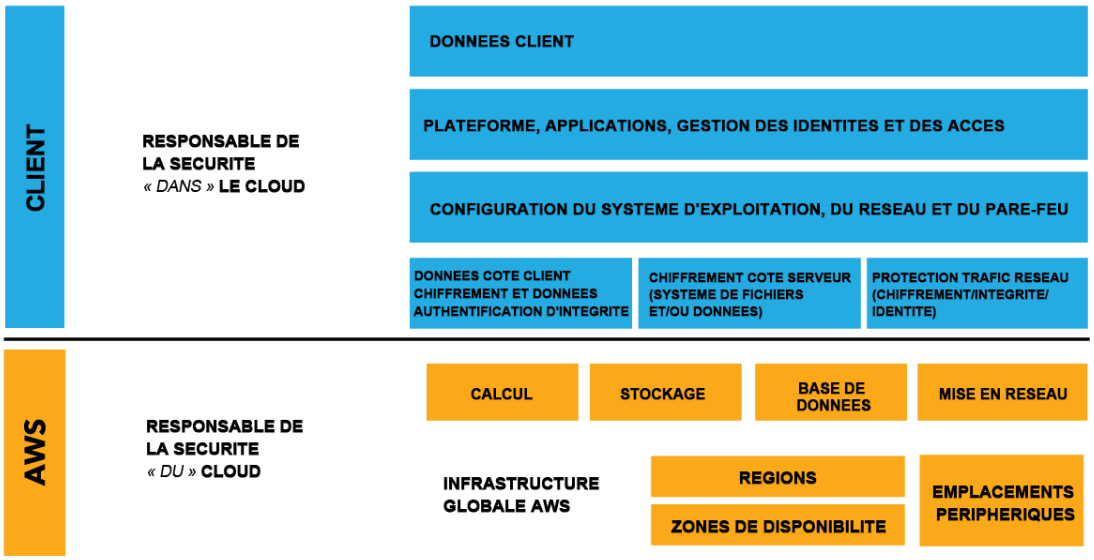

Figure 1 – Modèle de sécurité

Que signifie ce modèle pour la sécurité des contenus du client ?

Lorsqu'il évalue la sécurité d'une solution de cloud, il est important que le client comprenne et fasse la différence entre les éléments suivants :

- les mesures de sécurité que le fournisseur de service de cloud (AWS) implémente et utilise, la « sécurité ***du*** cloud » ;
- les mesures de sécurité que le client implémente et utilise, en lien avec la sécurité du contenu du client et les applications qui utilisent les services AWS, la « sécurité ***dans*** le cloud ».

AWS gère la sécurité ***du*** cloud, mais la sécurité ***dans*** le cloud incombe au client, car celui-ci conserve le contrôle des mesures de sécurité qu'il choisit d'implémenter pour protéger ses propres contenus, plateformes, applications, systèmes et réseaux, comme il le ferait pour les applications d'un centre de données sur site. Dans le cadre de ses différentes offres de service, AWS fournit à ses clients une sélection de mesures de sécurité. Nos clients peuvent également choisir d'utiliser des solutions de sécurité tierces. Les clients d'AWS sont entièrement libres de concevoir leur architecture de sécurité pour répondre à leurs besoins de conformité. Cette possibilité constitue une différence essentielle par rapport aux solutions d'hébergement traditionnelles, dans lesquelles le fournisseur décide de l'architecture. AWS permet au client de déterminer si les mesures de sécurité doivent être implémentées, et si oui, de choisir les mesures de sécurité à implémenter dans le cloud et de décider si elles conviennent à l'entreprise. Si, par exemple, une architecture offrant une disponibilité plus grande est nécessaire pour la protection des données, le client peut ajouter des systèmes redondants, des sauvegardes, des emplacements, des liaisons de réseau montantes, etc., pour créer une architecture à haute disponibilité plus résistante. Si un accès restreint aux données est requis, les contrôles d'AWS permettent au client d'implémenter les concepts de gestion des droits d'accès au niveau du système et via le chiffrement au niveau des données. AWS fournit ainsi au client des contrôles directs sur de nombreux éléments, qui constituent des mesures techniques et organisationnelles du point de vue de la sécurité des données.

Présentation de la sécurité DU cloud

AWS est responsable de la gestion de la sécurité de l'environnement cloud sous-jacent. L'infrastructure du cloud AWS a été conçue pour être l'un des environnements de calcul de cloud les plus flexibles et sécurisés. Elle a pour objectif d'offrir une disponibilité optimale tout en permettant une séparation complète du client. Elle offre une plateforme extrêmement évolutive et fiable, qui permet aux clients de déployer des applications et des contenus rapidement et en toute sécurité, sur une échelle mondiale étendue si nécessaire. Les services AWS ignorent les contenus, dans le sens où ils offrent le même niveau de sécurité élevé à tous les clients, quels que soient le type de contenus stockés ou la région géographique de stockage. Ne connaissant pas les données stockés par les clients dans les services AWS, AWS ne peut pas faire la distinction entre les données personnelles et tout autre type de données stocké par un client dans le cadre des contenus de ce dernier.

Les centres de données d'AWS, de classe mondiale et hautement sécurisés, font appel à une surveillance électronique à la pointe de la technologie et à des systèmes de contrôles d'accès multifacteurs. Ils sont surveillés 24h/24, 7j/7 par des gardiens de la sécurité formés, et l'accès est strictement autorisé sur la base de privilèges inférieurs, limités à des buts d'administration du système. Pour obtenir la liste complète de toutes les mesures de sécurité intégrées à l'infrastructure, aux plateformes et aux services de cloud centraux d'AWS, lisez notre livre blanc Présentation des processus de sécurité.

Nous sommes vigilants quant à la sécurité de notre environnement cloud sous-jacent et avons implémenté des mesures techniques et organisationnelles sophistiquées contre tout accès non autorisé. Les clients peuvent valider les contrôles de sécurité en place dans l'environnement AWS grâce aux certifications et rapports d'AWS, comprenant les rapports AWS Service Organization Control (SOC) 1 et 2, la certification ISO 27001 et les rapports de conformité PCI-DSS. Ces rapports et certifications sont produits par des auditeurs tiers indépendants et attestent de l'efficacité de conception et de fonctionnement des contrôles de sécurité d'AWS. Les certifications et rapports de conformité AWS applicables peuvent être demandés à l'adresse https://aws.amazon.com/compliance/contact. Vous trouverez plus d'informations sur les certifications, les rapports de conformité AWS et le respect des bonnes pratiques et normes sur le site de conformité d'AWS.

AWS fournit un addendum relatif au traitement des données pour aider les clients à répondre à leurs obligations de protection des données. AWS peut également ajouter les Clauses Contractuelles Types 2010/87/EU (souvent appelées « Clauses Types ») à l'addendum relatif au traitement des données d'un client si ce dernier en a besoin pour transférer des données personnelles de l'UE vers un pays situé en dehors de l'Espace économique européen.

Le 6 mars 2015, l'addendum relatif au traitement des données d'AWS, y compris les Clauses Types, a été approuvé par le groupe des autorités européennes compétentes en matière de protection des données, également connues sous le nom de Groupe de travail « Article 29 ». Cette approbation signifie que tout client AWS qui a besoin des Clauses Types peut maintenant considérer que l'addendum relatif au traitement des données d'AWS offre des engagements contractuels suffisants pour permettre la circulation des flux de données internationaux dans le respect de la Directive. Pour en savoir plus sur l'approbation par le Groupe de travail « Article 29 », veuillez visiter la page web de la Commission nationale pour la protection des données du Luxembourg ici : http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

Outre l'addendum relatif au traitement des données et les Clauses Types, les clients qui souhaitent transférer leurs données personnelles depuis des régions de l'UE d'AWS vers des régions des Etats-Unis bénéficient de la participation d'AWS au bouclier de protection des données UE-Etats-Unis. Amazon.com, Inc., avec certaines de ses filiales américaines, notamment AWS, sont certifiés dans le cadre du bouclier de protection des données UE-Etats-Unis du 21 octobre 2016. Le bouclier de protection des données UE-Etats-Unis n'a aucun impact sur la façon dont les clients utilisent ou gèrent AWS, mais fournit le mécanisme supplémentaire approuvé par l'UE pour le transfert des données personnelles depuis l'UE vers les Etats-Unis. Pour en savoir plus sur les obligations des fournisseurs de services américains dans le cadre du site web du bouclier de protection des données UE-Etats-Unis, veuillez consulter le site web de la Commission européenne ici : http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm et le site web du bouclier de protection des données UE-Etats-Unis ici : https://www.privacyshield.gov/welcome.

Présentation de la sécurité DANS le cloud

Les clients gardent le contrôle de leurs contenus lors de la fourniture de services AWS. Les clients, et non AWS, déterminent quels contenus ils stockent dans AWS, contrôlent la façon dont ils configurent leur environnement et sécurisent leurs contenus, décident de chiffrer ou non leurs contenus qu'ils soient au repos et en transit, des personnes ayant accès à ces contenus et des données d'identification qui seront requises (comprenant l'utilisation de l'authentification multi-facteurs), ainsi que des fonctions et outils de sécurité supplémentaires et de leur utilisation.

Etant donné que nos clients conservent le contrôle de leur sécurité, ils sont également responsables de la sécurité de tous les éléments que leur organisation place sur AWS, ou qu'ils connectent à leur infrastructure AWS, par exemple le système d'exploitation invité, les applications sur leurs instances de calcul et les contenus stockés et traités dans les services de stockage, de plateforme et de base de données d'AWS.

Les clients peuvent configurer leurs services AWS pour tirer parti d'une large gamme de fonctions, outils et contrôles de sécurité facultatifs afin de protéger leurs contenus, y compris des outils de gestion des identités et des accès sophistiqués, les configurations disponibles, les fonctionnalités de sauvegarde, les fonctionnalités de sécurité, le chiffrement et la sécurité du réseau. AWS fournit un large éventail de fonctions de sécurité pour aider ses clients à concevoir, implémenter et utiliser leur propre environnement AWS sécurisé. Les clients peuvent également utiliser leurs propres outils et contrôles de sécurité tiers. Voici quelques exemples de mesures que les clients peuvent prendre pour sécuriser leurs contenus :

- stratégies de mot de passe rigoureuses, avec affectation d'autorisations appropriées aux utilisateurs et mesures strictes pour protéger leurs clés d'accès ;
- pare-feu et segmentation de réseau appropriés, notamment Virtual Private Cloud, le chiffrement de contenu, l'utilisation du SSL et l'architecture correcte des systèmes pour diminuer les risques de perte de données et d'accès non autorisé ;
- schémas de redondance et stratégies de sauvegarde appropriés pour atténuer le risque de perte ou d'indisponibilité de données.

Tous ces facteurs sont contrôlés par les clients, et non AWS. AWS n'a aucune visibilité sur les contenus placés par les clients sur AWS et ne modifie pas les paramètres de configuration du client ; ceux-ci sont déterminés et contrôlés par les clients. Les clients décident des contenus à placer dans le cloud AWS et sont donc les seuls à pouvoir déterminer le niveau de sécurité approprié pour les données qui y sont stockées.

Pour permettre aux clients d'intégrer des contrôles de sécurité AWS dans leurs infrastructures de contrôle existantes et les aider à concevoir et à exécuter des évaluations de sécurité relatives à la façon dont leur organisation utilise les services AWS, AWS publie un certain nombre de livres blancs relatifs à la sécurité, à la gouvernance, aux risques et à la conformité, ainsi que différentes listes de contrôle et bonnes pratiques. Les clients peuvent également concevoir et exécuter librement des évaluations de la sécurité selon leurs propres préférences, et ils peuvent demander l'autorisation d'effectuer des analyses sur l'infrastructure du cloud (si ces analyses se limitent aux instances de calcul du client et n'enfreignent pas la politique d'utilisation acceptable d'AWS).

Régions AWS

Les centres de données AWS sont conçus sous forme de clusters dans divers pays à travers le monde. Nous appelons « région » chacun de nos clusters de centre de données dans un pays donné. Les clients ont accès à quatorze régions AWS à travers le monde, dont deux au sein de l'Union européenne, en Irlande (Dublin) et en Allemagne (Francfort). Ils peuvent choisir d'utiliser une seule région, toutes les régions ou une combinaison de plusieurs régions. La Figure 2 présente l'emplacement des régions AWS :

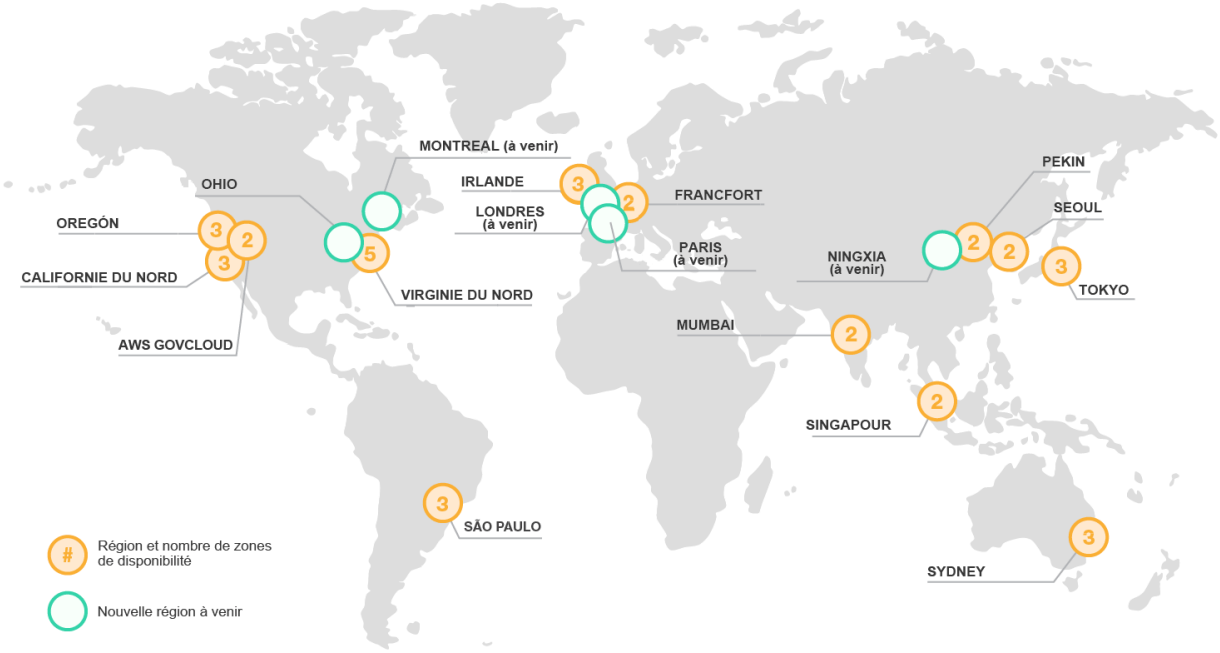

Figure 2 – Régions mondiales d'AWS

Les clients d'AWS choisissent la ou les régions AWS dans lesquelles ils hébergeront leur contenu. Cela permet aux clients qui ont des exigences spécifiques en termes de géographie d'établir leurs environnements dans l'emplacement ou les emplacements de leur choix. Par exemple, les clients AWS en Europe peuvent choisir de déployer leurs services AWS exclusivement dans la région de l'UE (Allemagne). Si le client fait ce choix, ses contenus seront stockés en Allemagne, sauf s'il sélectionne une autre région AWS.

Les clients peuvent répliquer et sauvegarder du contenu dans plusieurs régions, mais AWS ne déplace pas le contenu du client en dehors de la ou des régions qu'il a choisies.

Comment les clients peuvent-ils sélectionner leur(s) région(s) ?

Lorsque le client utilise l'AWS Management Console ou envoie une demande via une API AWS, il identifie la ou les régions particulières dans lesquelles il souhaite utiliser les services AWS. La Figure 3 (Sélection de régions mondiales AWS) offre un exemple du téléchargement de contenus sur un service de stockage AWS ou de l'apport de ressources de calcul grâce à l'AWS management console.

Figure 3 – Sélection de régions mondiales AWS dans l'AWS Management Console

Les clients peuvent également indiquer la région AWS à utiliser pour leurs ressources informatiques, en profitant de la fonctionnalité Amazon Virtual Private Cloud (VPC). Amazon VPC permet au client de mettre en service une section du cloud AWS où il peut lancer des ressources AWS dans un réseau virtuel qu'il a défini. Grâce à Amazon VPC, les clients peuvent définir une topologie de réseau virtuel qui ressemble fortement à un réseau traditionnel qu'ils pourraient utiliser dans leur centre de données.

Toutes les ressources de calcul et autres lancées par le client dans le VPC se trouveront dans la région qu'il aura choisie.

Contrôles du client et accès à ses contenus

Contrôle du client sur les contenus

Les clients utilisant AWS gardent le contrôle sur leurs contenus dans l'environnement AWS. Ils peuvent :

- déterminer où ils se trouveront, par exemple le type d'environnement de stockage et son emplacement géographique ;
- contrôler le format de ces contenus, par exemple du texte simple, masqué, anonymisé ou chiffré, grâce au chiffrement fourni par AWS ou un mécanisme de chiffrement tiers choisi par le client ;
- gérer d'autres contrôles d'accès, tels que la gestion des identités et des accès et les données d'identification de sécurité ;
- contrôler l'utilisation du SSL, de Virtual Private Cloud et d'autres mesures de sécurité du réseau pour éviter tout accès non autorisé.

Ceci permet aux clients AWS de contrôler le cycle de vie complet de leurs contenus sur AWS, et de gérer ceux-ci en accord avec leurs propres besoins spécifiques, comme la classification, le contrôle d'accès, la conservation et la suppression des contenus.

Accès aux contenus du client

AWS n'accède pas aux contenus du client, sauf si cela s'avère nécessaire pour lui fournir les services AWS que le client a sélectionnés. AWS n'accède aux contenus du client pour aucune autre raison.

AWS n'a pas connaissance des contenus que les clients choisissent de stocker sur AWS. Il ne fait pas non plus la distinction entre les données personnelles et les autres types de contenus. AWS traite donc tous les contenus du client de la même façon. Ainsi, les contenus du client bénéficient des mêmes mesures de sécurité rigoureuses d'AWS, qu'ils contiennent des données personnelles ou non. AWS met simplement à disposition les services de calcul, de stockage, de base de données et de réseau sélectionnés par le client avec les meilleures mesures de sécurité de leur catégorie, appliquées à l'infrastructure de cloud fournie par AWS. Le client peut ensuite se baser sur cette sécurité d'infrastructure selon ses propres exigences.

Droits d'accès du gouvernement

Les clients posent souvent des questions relatives aux droits d'accès des autorités gouvernementales nationales et étrangères en ce qui concerne les contenus présents dans les services de cloud. Ils s'inquiètent souvent des problèmes de souveraineté des données et se demandent notamment si les gouvernements peuvent avoir accès à leurs contenus et dans quelles circonstances. Les lois locales qui s'appliquent dans la juridiction où se trouvent les contenus sont un facteur important pour certains clients. Cependant, ils doivent également tenir compte du fait que des lois d'autres juridictions peuvent s'appliquer à eux, selon l'endroit où ils (ou leurs clients) exercent leur activité. Les clients doivent demander conseil pour comprendre l'application des lois pertinentes pour leur entreprise et leurs opérations.

Lorsque des inquiétudes ou questions sont soulevées concernant les droits d'accès des gouvernements nationaux ou étrangers pour les contenus stockés sur le cloud, il est important de comprendre que les autorités gouvernementales pertinentes peuvent avoir le droit d'émettre des demandes relatives à ces contenus, conformément aux lois qui s'appliquent déjà au client. Par exemple, une entreprise travaillant dans le pays X peut être soumise à une demande légale d'informations, même si les contenus sont stockés dans le pays Y. Généralement, une autorité gouvernementale cherchant à accéder aux données d'une entité adressera toute demande d'information directement à cette entité plutôt qu'au fournisseur de cloud.

Généralement, les Etats membres de l'UE possèdent une législation permettant aux organismes d'application de la loi publique et de la sécurité nationale d'accéder à ces informations. Les organismes d'application de la loi étrangers peuvent également travailler avec les organismes d'application de la loi publique et de la sécurité nationale pour obtenir l'accès à ces informations au sein de l'UE. La plupart des pays ont mis en place des processus (dont des traités d'assistance judiciaire mutuelle) qui permettent le transfert d'informations à d'autres pays, suite à des demandes d'informations appropriées et légales (par exemple, en lien avec des actes délictueux). Cependant, il est important de noter que certains critères doivent être remplis selon la loi en vigueur pour qu'une demande d'accès par l'organisme d'application de la loi pertinent soit acceptée. Par exemple, l'agence gouvernementale demandant l'accès devra sans doute démontrer qu'elle a une raison valide de demander à un tiers l'autorisation d'accéder à ses contenus, et il pourra lui être demandé d'obtenir une décision judiciaire ou un mandat.

La plupart des pays ont mis en place des lois d'accès aux données qui visent à avoir une application extraterritoriale. Le Patriot Act est un exemple de loi américaine avec portée extraterritoriale, souvent mentionnée dans le contexte des services de cloud. Il est semblable aux lois de nombreux autres pays développés, qui permettent aux gouvernements d'obtenir des informations en lien avec des enquêtes liées au terrorisme international et à d'autres problèmes de renseignements étrangers. Toute demande de documents selon le Patriot Act nécessite une décision judiciaire démontrant que la demande respecte la loi, par exemple en prouvant qu'elle est associée à des enquêtes légitimes.

Stratégie d'AWS

Quels que soient la provenance d'une demande de contenu d'un client ou l'identité de ce dernier, AWS est toujours vigilant quant à la protection des contenus de ses clients. AWS ne divulguera pas les contenus de ses clients sauf en cas d'obligation face à un ordre légalement valable et exécutoire, tel qu'une assignation à comparaître ou une décision judiciaire. Les autorités administratives ou américaines non gouvernementales doivent utiliser les procédures internationales reconnues, telles que les traités d'assistance juridique réciproque avec le gouvernement américain, pour obtenir des commandements valables et contraignants. Nous examinons attentivement chaque demande pour authentifier sa précision et vérifier qu'elle respecte la loi en vigueur. Nous nous opposerons aux demandes dont la portée est excessive, qui dépassent l'autorité du demandeur ou ne respectent pas totalement la loi en vigueur. Si nous sommes obligés de divulguer le contenu d'un client, nous en informerons ce dernier auparavant pour lui donner la possibilité de chercher une protection face à la divulgation, sauf si la loi l'interdit.

Protection des données dans l'UE : la Directive

Nous évoquons ci-dessous les obligations contenues dans la Directive[1]. La Directive établit un certain nombre d'exigences de protection des données, qui s'appliquent lors du traitement des données personnelles. Dans ce contexte, le « traitement » inclut toute opération ou tout ensemble d'opérations effectué sur les données personnelles. Selon la Directive, les « données personnelles » sont définies comme des informations à partir desquelles un individu vivant peut être identifié ou identifiable (nommé « personne concernée »). De plus, la Directive fait la distinction entre (a) le « contrôleur des données », c'est-à-dire la partie qui détermine les objectifs et moyens du traitement des données personnelles, et (b) le « responsable du traitement des données », c'est-à-dire la partie qui traite les données personnelles pour le compte du contrôleur.

Le contrôleur de données doit veiller à ce que son traitement des données personnelles respecte les obligations de protection des données. Par exemple, il doit vérifier que les données personnelles sont traitées de façon équitable et légale. Il doit également s'assurer qu'elles sont protégées contre tout traitement non autorisé ou illégal.

AWS sait que ses services sont utilisés dans le cadre de différentes opérations commerciales et que plusieurs parties peuvent être impliquées dans une chaîne d'approvisionnement. En règle générale, cependant, lorsque les contenus du client stockés grâce aux services AWS contiennent des données personnelles :

- Le client sera le contrôleur en lien avec les données personnelles, s'il détermine l'objectif dans lequel les données seront traitées et s'il a choisi leur mode de traitement.
- Le client sera responsable du traitement en lien avec ces données personnelles s'il traite simplement les données personnelles sur le réseau AWS, pour le compte de et selon les souhaits d'un tiers (qui peut être le contrôleur, un autre tiers dans la chaîne d'approvisionnement ou une personne agissant dans une capacité purement nationale).

En tant que fournisseur d'infrastructure de service autonome entièrement placé sous le contrôle du client, comprenant le « traitement » et le mode de traitement des données, AWS fournit uniquement les services d'infrastructure aux clients qui souhaitent charger et traiter des contenus sur le réseau AWS. Dans ce contexte, AWS n'a pas de visibilité ou de connaissance relative aux éléments que les clients téléchargent sur son réseau, et ignore donc si ces contenus contiennent des données personnelles ou non. Les clients AWS peuvent également utiliser le chiffrement afin de rendre leurs contenus incompréhensibles pour AWS. AWS ne traite pas les contenus du client, sauf si nécessaire pour lui fournir les services (ou respecter la loi ou un ordre valable et exécutoire).

AWS a également mis en place des systèmes, procédures et stratégies pour éviter tout accès aux contenus du client par les employés d'AWS. De plus, pour les clients qui souhaitent traiter des

[1] Gardez à l'esprit que la Directive ne s'applique pas aux organisations établies directement dans les Etats membres de l'UE. Les Etats membres de l'UE doivent à la place implémenter la Directive dans leur législation nationale. Par conséquent, il peut exister des différences entre la nature précise des obligations selon les différents Etats membres. Les clients doivent donc demander conseil quant aux lois nationales applicables à leur cas.

données personnelles, AWS fournit un addendum relatif au traitement des données pour aider les clients à répondre à leurs obligations de protection des données. AWS peut également ajouter les Clauses Types à l'addendum relatif au traitement des données d'un client si ce dernier en a besoin pour transférer des données personnelles de l'UE vers un pays situé en dehors de l'Espace économique européen.

Le 6 mars 2015, l'addendum relatif au traitement des données d'AWS, y compris les Clauses Types, a été approuvé par le groupe des autorités européennes compétentes en matière de protection des données, également connues sous le nom de Groupe de travail « Article 29 ». Cette approbation signifie que tout client AWS qui a besoin des Clauses Types peut maintenant considérer que l'addendum relatif au traitement des données d'AWS offre des engagements contractuels suffisants pour permettre la circulation des flux de données internationaux dans le respect de la Directive. Pour en savoir plus sur l'approbation par le Groupe de travail « Article 29 », veuillez visiter la page web de la Commission nationale pour la protection des données du Luxembourg ici :
http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

Le contrôleur de données est responsable de l'implémentation des mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre la destruction accidentelle ou illégale, ou encore la perte accidentelle, l'altération, la divulgation ou l'accès non autorisé. Lorsque le traitement est effectué par un responsable du traitement de données pour le compte du contrôleur de données, ce dernier est également responsable du choix d'un responsable du traitement offrant des mesures techniques et organisationnelles suffisantes pour régir le traitement à effectuer.

Nous récapitulons dans le tableau ci-dessous certains des principes fondamentaux de protection de données, que les clients prennent généralement en compte dans ce contexte. Nous évoquons également des aspects des services AWS relatifs à ces principes. Dans ce tableau, nous supposons que le client d'AWS sera le contrôleur de données. Cependant, comme mentionné ci-dessus, nous reconnaissons qu'il peut exister de nombreuses circonstances dans lesquelles le client d'AWS sera le responsable du traitement des données. Dans ces situations, cependant, le client d'AWS pourra tout de même trouver utiles les informations ci-dessous, dans le contexte de sa propre relation avec le contrôleur.

Principe de protection des données	**Récapitulatif de l'obligation de protection des données**	**Considérations**
Equité	Les personnes concernées doivent recevoir des informations précises et complètes sur l'identité du contrôleur, la finalité du traitement et toute autre information nécessaire pour garantir un traitement équitable.	**Client :** il (ou son client) décide des informations collectées et de la finalité d'utilisation de ces informations. Dans de nombreux cas, le client sera en relation directe avec les personnes concernées et sera donc le mieux placé pour communiquer directement avec elles. En outre, le client doit connaître la portée de tout avis précédemment communiqué aux personnes concernées. **AWS :** AWS n'exerce aucun contrôle sur les types de contenus que le client choisit de stocker dans AWS et sur la finalité de cette action. AWS ne connaît pas ces contenus (et ignore notamment s'il contiennent ou non des données personnelles). AWS n'a aucun moyen d'identifier les personnes concernées ou de contacter celles dont le client a choisi de stocker les données personnelles sur l'infrastructure AWS, et ne peut donc fournir aucune information aux personnes concernées.
Base juridique	Le contrôleur doit disposer d'une base juridique pour son traitement et celle-ci doit respecter au moins l'un des critères exposés dans la Directive.	**Client :** lorsqu'il décide s'il doit traiter des données personnelles et pour quelle finalité, le client doit déterminer si ce traitement respecte au moins l'un des critères de la Directive. Ceux-ci nécessitent, par exemple, que la personne concernée ait donné son consentement, ou que le traitement soit nécessaire pour la réalisation d'un contrat dont la personne concernée est une partie. **AWS :** tel qu'établi ci-dessus, AWS n'exerce aucun contrôle sur les types de contenus que le client choisit de stocker dans AWS (il ignore notamment s'ils comportent des données personnelles ou non). AWS ne détermine pas l'architecture que le client choisit de générer en associant les offres de service AWS, ni si elle est appropriée ou non pour les besoins spécifiques du client. AWS ne joue aucun rôle dans la prise de décision concernant le traitement de ces données et la finalité recherchée. Ainsi, AWS ne peut pas déterminer s'il existe une base juridique pour le traitement.

Limitation de finalité	Les données personnelles ne peuvent être collectées que dans des buts spécifiés, explicites et légitimes ; elles ne peuvent pas être traitées davantage d'une manière qui soit incompatible avec ces buts.	**Client :** il détermine quelles données personnelles sont collectées et dans quel but elles seront utilisées. Lorsqu'il prend cette décision, le client doit s'assurer qu'il possède un but spécifié, explicite et légitime. Le client décide si les données seront par la suite traitées à d'autres fins ; il peut procéder à une évaluation pour s'assurer de la compatibilité de celles-ci avec le but initial **AWS :** AWS n'exerce aucun contrôle sur les finalités pour lesquelles le client utilise son contenu et le stocke dans le cloud AWS. Dans la mesure où le contenu du client inclut des données personnelles, AWS traite uniquement ces données pour fournir au client les services AWS que celui-ci a sélectionnés (excepté dans les cas limités où AWS doit respecter la loi ou une décision officielle).
Droits des personnes concernées	Les personnes concernées doivent pouvoir accéder à leurs données personnelles et obtenir la rectification, la suppression ou le blocage de celles dont le traitement ne respecte pas la Directive..	**Client :** le client garde le contrôle du contenu stocké sur AWS et peut ainsi déterminer la façon dont les sujets peuvent accéder à leurs données personnelles incluses dans ce contenu. De même, le client est le mieux placé pour répondre à la demande ou plainte d'un sujet de données quant à la légalité de ses activités de traitement des données. **AWS :** comme expliqué ci-dessus, AWS n'exerce aucun contrôle sur les types de contenu que le client choisit de stocker dans AWS ni sur les buts fixés. AWS ne dispose d'aucune connaissance de ce contenu (ni ne sait s'il comporte ou non des données personnelles). AWS ne peut pas identifier ou contacter les sujets de données dont le client a choisi de stocker les données personnelles dans AWS (sauf dans le cas où le client lui-même est concerné) et ne peut ainsi fournir aucune information aux sujets de données concernés. AWS n'a pas la capacité de relier les données stockées sur AWS et une personne en particulier. Ces informations sont exclusivement sous le contrôle du client.

Exactitude	Les contrôleurs de données doivent s'assurer que les données personnelles sont exactes et, si nécessaire, tenues à jour.	**Client :** le client contrôle les données personnelles qu'il choisit de stocker sur AWS. Il est ainsi responsable de la vérification et de la préservation de leur exactitude (et peut les mettre à jour ou les corriger si nécessaire). De plus, le client gère la sécurité « dans » le cloud et en est responsable. Par conséquent, il peut garantir qu'il a implémenté les mesures appropriées pour protéger les données de tout risque de corruption. **AWS :** AWS n'exerce aucun contrôle sur les types de contenu que le client choisit de stocker dans AWS et ne possède aucune connaissance de ce contenu. AWS ne saisit ni ne modifie de données au nom du client. Par conséquent, AWS ne peut ni vérifier l'exactitude des données ni les mettre à jour. Cependant, le rapport SOC 1 Type 2 inclut des détails sur les contrôles qu'AWS exerce pour assurer l'intégrité des données au niveau de l'environnement cloud sous-jacent.
Sécurité des données	Les contrôleurs de données doivent mettre en place des mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre la destruction involontaire ou illégale, la perte accidentelle, l'altération, et la divulgation ou l'accès non autorisés.	**Client :** seul le client est en mesure de déterminer si une architecture de sécurité particulière qu'il conçoit ou implémente est adaptée à quelque type de contenu que ce soit incluant des données personnelles. Les clients sont responsables de la sécurité ***dans*** le cloud, y compris de celle de leur contenu (et des données personnelles qui y sont incluses) et de l'implémentation d'une architecture appropriée à l'aide des offres de service AWS. En particulier, les clients sont responsables (a) de la configuration correcte des services AWS, (b) de l'utilisation correcte des contrôles disponibles en lien avec les services et (c) de l'adoption correcte des mesures qu'ils considèrent comme nécessaires au maintien des contrôles de sécurité appropriés et à la sauvegarde de leurs données personnelles (par exemple, en utilisant la technologie de chiffrement pour protéger les données personnelles contre tout accès non autorisé et pour l'archivage quotidien). **AWS :** AWS est responsable de la gestion de la sécurité ***de*** l'environnement cloud sous-jacent. Pour obtenir la liste complète de toutes les mesures de sécurité intégrées à l'infrastructure, aux plateformes et aux services principaux du cloud AWS, lisez notre livre blanc Présentation des processus de sécurité[3]. AWS fait appel à des auditeurs externes pour vérifier l'efficacité de ses mesures de sécurité, y compris la sécurité des centres de données physiques à partir desquels AWS fournit ses services. Sur demande écrite du client et signature d'un accord de non-divulgation, AWS fournit aux clients un récapitulatif du rapport des auditeurs, afin que le client puisse raisonnablement vérifier les mesures de sécurité prises par AWS. AWS fournit aussi ce résumé aux autorités de protection des données, sur demande.

Conservation des données	Les données personnelles ne doivent pas être conservées (sous une forme identifiable) plus longtemps que nécessaire pour les buts pour lesquels elles ont été collectées ou traitées.	**Clients :** le client décide de la finalité de l'utilisation des données personnelles stockées dans le cloud AWS et, par conséquent, de la durée nécessaire de leur conservation. Le client peut supprimer ou rendre anonymes les données personnelles lorsqu'elles ne sont plus nécessaires. **AWS :** AWS ignore si les données stockées comprennent des données personnelles, ainsi que les buts dans lesquels le client traite les données qu'il a stockées dans le cloud. En conséquence, AWS ne peut pas déterminer la durée nécessaire de conservation des données pour atteindre ce but. Lorsqu'un client supprime son contenu des services AWS, ce dernier est rendu illisible ou est désactivé. Les zones de stockage sous-jacentes du réseau AWS qui étaient utilisées pour stocker le contenu sont effacées, avant d'être récupérées et écrasées, conformément aux politiques standard et aux délais de suppression d'AWS. Les procédures d'AWS comprennent également un processus de mise hors service sécurisé, effectué avant la suppression du support de stockage utilisé pour fournir les services AWS. Dans le cadre de ce processus, le support de stockage est démagnétisé ou effacé, puis physiquement détruit ou rendu inactif, en accord avec les pratiques standard du secteur.
Transfert	Les données personnelles ne doivent être transférées vers aucun pays ou territoire en dehors de l'espace économique européen, sauf si ce pays ou territoire garantit un niveau adéquat de protection des droits et libertés des sujets de données en termes de traitement des données personnelles.	**Client :** le client peut choisir les régions AWS dans lesquelles se trouveront le contenu et les serveurs. Le client peut choisir de déployer ses services AWS exclusivement dans les régions AWS de l'UE, en Allemagne ou en Irlande. **AWS :** AWS ne déplace pas le contenu du client en dehors des régions choisies par le client, sauf si nécessaire pour respecter la loi ou un décret officiel. AWS fournit un addendum relatif au traitement des données pour aider les clients à répondre à leurs obligations de protection des données. AWS peut également ajouter les clauses types à l'addendum relatif au traitement des données d'un client si ce dernier en a besoin pour transférer ses données personnelles de l'UE vers un pays situé en dehors de l'espace économique européen. Le 6 mars 2015, l'addendum relatif au traitement des données d'AWS, clauses types incluses, a été approuvé par le groupe des autorités européennes compétentes en matière de protection des données, également connues sous le nom de Groupe de travail Article 29. Cette approbation signifie que tout client AWS qui a besoin des Clauses Types peut maintenant considérer que l'addendum relatif au

		traitement des données d'AWS offre des engagements contractuels suffisants pour permettre la circulation des flux de données internationaux dans le respect de la Directive. Pour en savoir plus sur l'approbation par le Groupe de travail « Article 29 », veuillez visiter la page web de la Commission nationale pour la protection des données du Luxembourg ici : http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html Outre l'addendum relatif au traitement des données et les clauses types, les clients qui souhaitent transférer leurs données personnelles depuis les régions AWS de l'UE vers les régions des Etats-Unis tirent avantage de la participation d'AWS au bouclier de protection des données UE-Etats-Unis. Le bouclier de protection des données UE-Etats-Unis n'a aucun impact sur la façon dont les clients utilisent ou gèrent AWS, mais fournit le mécanisme supplémentaire approuvé par l'UE pour le transfert des données personnelles depuis l'UE vers les Etats-Unis. Pour en savoir plus sur les obligations des fournisseurs de services américains dans le cadre du site web du bouclier de protection des données UE-Etats-Unis, veuillez consulter le site web de la Commission européenne ici : http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm et le site web du bouclier de protection des données UE-Etats-Unis site web du bouclier de protection des données UE-Etats-Unis ici : https://www.privacyshield.gov/welcome.

Violations des données

Comme les clients assurent la gestion et le contrôle des données personnelles lorsqu'ils utilisent AWS, il leur incombe de surveiller leur propre environnement afin de détecter toute violation de confidentialité et d'en informer les régulateurs et individus concernés, comme requis par la loi applicable. Seul le client peut gérer cette responsabilité.

Les clients contrôlent leurs propres clés d'accès et déterminent quelles sont les personnes autorisées à accéder à leur compte AWS. AWS n'a aucune visibilité sur les clés d'accès ou sur les personnes autorisées ou pas à se connecter à un compte. Le client est donc responsable de la surveillance de l'utilisation, du mauvais emploi, de la distribution ou de la perte des clés d'accès.

Si nécessaire selon la loi applicable, AWS informera rapidement le client si AWS a effectivement connaissance d'une violation confirmée des normes de sécurité AWS ayant trait au réseau AWS.

Sous-traitants

AWS fait appel à un certain nombre de sous-traitants tiers pour l'aider à fournir ce service. Cependant, nos sous-traitants n'ont pas accès au contenu des clients. De plus, nous ne faisons appel qu'à des sous-traitants auxquels nous faisons confiance et nous utilisons des protections contractuelles appropriées, que nous surveillons pour nous assurer du respect des normes requises.

Fournisseurs de services tiers du client

Tel qu'indiqué précédemment dans ce document, l'environnement AWS est également relié aux autres services fournis directement par des tiers (par exemple, fournisseurs de services Internet). Ces tiers sont responsables de leurs propres systèmes, sécurité incluse, et AWS n'est pas responsable de leurs activités.

Autres considérations

Ce livre blanc ne traite pas d'autres lois liées à la confidentialité, en dehors de la Directive, qui peuvent être également pertinentes pour les clients, notamment certaines exigences spécifiques au secteur. Les lois et réglementations de confidentialité et de protection des données applicables aux clients dépendent de plusieurs facteurs : le lieu où un client exerce son activité, le secteur industriel dont il relève, le type de contenu qu'il souhaite stocker, la provenance du contenu ou le lieu de stockage, par exemple.

Les clients préoccupés par leurs obligations réglementaires de confidentialité doivent d'abord veiller à identifier et comprendre les exigences qui leur sont applicables, et rechercher des conseils appropriés.

Commentaires finaux

Pour AWS, la sécurité est toujours la priorité absolue. Nous offrons des services à des centaines de milliers d'organismes aussi divers que des entreprises, des établissements éducatifs ou des agences gouvernementales, et ce dans plus de 190 pays. Parmi nos clients figurent des fournisseurs de services financiers ou de soins de santé. Ils nous confient certaines de leurs informations les plus sensibles, dont les données de santé personnelles ou les états financiers.

Les services AWS sont conçus pour offrir aux clients la flexibilité nécessaire à la configuration et au déploiement de leurs solutions, ainsi qu'au contrôle de leur contenu, y compris le lieu et le mode de stockage, et les personnes autorisées à y accéder. Les clients d'AWS peuvent développer leurs propres applications sécurisées et stocker leur contenu en toute sécurité sur AWS.

Ressources supplémentaires

Pour aider les clients à mieux comprendre comment satisfaire à leurs exigences de confidentialité et de protection des données, nous les encourageons à lire les livres blancs, les bonnes pratiques, les listes de contrôle et les guides traitant des risques, de la conformité et de la sécurité, publiés sur le site web AWS. Cette documentation est disponible aux adresses http:/aws.amazon.com/compliance et http://aws.amazon.com/security.

AWS offre également une formation pour aider les clients à concevoir, développer et utiliser des applications disponibles, efficaces et sécurisées sur le cloud AWS, et à maîtriser les services et solutions AWS. Nous offrons gratuitement des vidéos de formation, des ateliers d'autoformation et des formations assurées par un instructeur. Pour plus d'informations sur la formation AWS, consultez http://aws.amazon.com/training/.

Les certifications AWS certifient les compétences et connaissances techniques associées aux bonnes pratiques de développement d'applications sécurisées et fiables basées sur le cloud à l'aide de la technologie AWS. Pour plus d'informations sur les certifications AWS, consultez http://aws.amazon.com/certification/.

Pour plus d'informations, contactez AWS à l'adresse https://aws.amazon.com/contact-us/ ou contactez votre représentant AWS local.