ATTESTATION DE CONFORMITÉ RGPD

Madame, Monsieur,

Vous vous questionnez sur la manière dont nous appliquons les différentes dispositions du Règlement Général 2016/679 sur la Protection des Données (RGPD), et notamment sur les mesures que nous prenons en tant que sous-traitant dans le traitement des données à caractère personnel via nos solutions.

En notre qualité de sous-traitant, la société MoveWORK vous réaffirme que la protection des données de ses clients est l'une de ses plus hautes priorités, conformément à nos engagements figurant dans l'annexe de nos Conditions Générales de Vente.

Nous attestons par le présent document que depuis le 25 Mai 2018 :

a) Des nouvelles fonctionnalités ont été apportées à nos solutions, qui nous permettent de répondre aux droits et obligations apportés par la RGPD :

- Droit à l'oubli ou effacement
- Droit à la rectification
- Droit à la portabilité
- Edition de demandes de consentement

b) Avoir mis en place en interne des actions afin :

- De sensibiliser nos salariés, par le biais de multiples journées de formation, sur les enjeux et les risques liés aux libertés et à la vie privée.
- De mettre en place une politique forte d'identification, d'authentification et de sécurité des connexions.
- D'assurer une protection maximum de notre réseau informatique.
- D'obtenir une limitation des accès aux seules données utiles pour un traitement.
- De respecter un certain nombre de process pour le traitement des données dont certains nécessitent le consentement formel du client avant toute récupération et traitement de données à caractère personnel.
- D'assurer la destruction ou archivage des données après traitement.
- D'encadrer la sécurité des données avec nos sous-traitants.

Espérant avoir répondu à vos interrogations, nous restons à votre disposition pour toutes informations complémentaires.

Bien cordialement.

Borja DUQUE

-DPO MoveWORK Group-

CONFORMITE AU RGPD DE NOTRE PRESTATAIRE D'HEBERGEMENT

Note d'information de nos clients et partenaires

Mai 2018

Sommaire

Pourquoi une note d'information à l'attention des Clients et Partenaires de MoveWORK ?	4
Qu'est-ce que le RGPD ?	4
Quelles sont les raisons du choix d'AWS par MOVEWORK ?	4
Où les contenus confiés à MOVEWORK sont-ils stockés par AWS ?	6
Quelles sont les politiques d'AWS dans l'Union Européenne permettant d'assurer la conformité des services gérés par AWS au RGPD ?	6
5.1. La politique de confidentialité d'AWS	6
5.2. Le Data Processing Addendum	7
5.3. Le livre blanc sur la sécurité AWS	7
5.4. Les engagements d'AWS	7
5.5. Le programme AWS de gestion des risques et de la conformité	8
Quelles sont les auto-certifications, normes de sécurité, certifications et attestations d'organisme tiers d'AWS ?	8
6.1. L'auto-certification US Privacy Shield	8
6.2. Les normes de sécurité	8
6.3. Les certifications AWS	8
6.3.1. La certification ISO 27001 /9001	9
6.3.2. La certification ISO 27017/27018	9
6.4. Le programme d'assurance de sécurité AWS	9
Quels sont la sécurité spécifique pour les services de stockage, les fonctionnalités et les services AWS permettant le respect des exigences du RGPD ?	9
Que devez-vous savoir sur la sécurité de l'environnement du cloud AWS et les autres ressources AWS ?	10
8.1. Le cadre bien structuré de l'infrastructure d'AWS (Well-Architected Framework)	10
8.2. La sécurité de l'environnement cloud AWS et le modèle de responsabilité partagée entre AWS et ses clients	10
8.3. Les autres ressources de conformité d'AWS on-line	11

1. Pourquoi une note d'information à l'attention des Clients et Partenaires de MoveWORK ?

Compte tenu de l'adoption du RGPD et de la relation de confiance qui existe entre MOVEWORK et ses Clients et Partenaires, MOVEWORK a souhaité informer le plus largement possible ses Clients et Partenaires en matière de protection des données.

MOVEWORK par ce document matérialise sa volonté de préciser ses engagements ainsi que les engagements de son prestataire d'hébergement en matière de protection des données à caractère personnel.

L'objectif principal de ce document est de concentrer dans un document unique des informations claires, simples et précises concernant les traitements de données opérés par MOVEWORK, pour permettre à ses Clients et Partenaires de comprendre quelles sont les raisons du choix d'Amazon Web Services (AWS) par MOVEWORK, dans quel contexte leurs données sont stockées chez AWS, quelles sont les politiques d'AWS permettant d'assurer une conformité au RGPD, quelles sont les auto-certifications ou certifications, normes de sécurité ou attestations d'organismes tiers d'AWS.

2. Qu'est-ce que le RGPD ?

La Commission européenne a approuvé et adopté en 2016 le Règlement général sur la protection des données (RGPD). Le RGPD est une réglementation européenne relative à la protection de la vie privée, entrée en vigueur le 25 mai 2018. Le RGPD vise à renforcer la sécurité et la protection des données personnelles dans l'Union Européenne, et à harmoniser les législations relatives à la protection des données au sein de l'UE. Le RGPD a remplacé la Directive 95/46/CE sur la protection des données personnelles, ainsi que toutes les lois nationales en lien avec celle-ci.

Le RGPD s'applique à toutes les organisations menant des activités dans l'UE et traitant des « données à caractère personnel » concernant des résidents de l'UE. Par l'expression « données à caractère personnel », il faut entendre toute information liée à une personne physique identifiée ou identifiable.

3. Quelles sont les raisons du choix d'AWS par MOVEWORK ?

Amazon Web Services (ci-après AWS) est une filiale d'Amazon.com, Inc. ou de ses sociétés affiliées («Amazon.com»). En tant que filiale d'Amazon.com, AWS utilise les pratiques de traitement des informations qui ont été adoptées par Amazon.com, et les informations de compte que recueille AWS sont régies par l'Avis de confidentialité d'Amazon.com

AWS a également annoncé sa conformité au code de conduite CISPE. Le code de conduite CISPE aide les clients de services cloud à évaluer la manière dont le fournisseur de leur infrastructure de cloud respecte les obligations de protection des données énoncées par le RGPD.

CISPE est une coalition de fournisseurs d'infrastructures de cloud (aussi appelées « Infrastructure as a Service ») qui proposent des services cloud à des clients en Europe. Le code de conduite CISPE aide les clients de services cloud à s'assurer que le fournisseur de leur infrastructure de cloud applique les normes de protection appropriées pour leurs données, conformément aux dispositions du RGPD.

Le code de conduite expose les principes auxquels les fournisseurs doivent se soumettre. Le code de conduite présente les mesures et les engagements que les fournisseurs doivent prendre afin de respecter le règlement RGPD et d'aider leurs clients à faire de même.

Le code de conduite fournit aux clients les informations relatives à la protection et à la sécurité des données dont ils ont besoin pour prendre leurs décisions en matière de conformité.

AWS garantit en outre à ses clients et donc à MOVEWORK que tous les services proposés sont conformes au règlement RGPD entré en vigueur, le 25 mai 2018. En outre, au-delà de la conformité de la plate-forme AWS, AWS s'engage également à proposer des services et ressources afin d'aider ses clients à respecter les exigences RGPD applicables à leurs activités respectives.

Le choix d'AWS par MOVEWORK se justifie par les politiques, pratiques et engagements d'AWS, normes de sécurité mises en œuvre et certifications. Pour AWS, la confiance de ses clients est sa priorité absolue. AWS est consciente du fait que, pour ses clients, la confidentialité et la sécurité des données sont primordiales. AWS déclare et reconnaît également que ce sont les clients qui sont propriétaires de leurs données et en assurent le contrôle : grâce à des outils simples mais puissants, ils peuvent définir les emplacements de stockage qui seront utilisés, sécuriser leurs données en transit ou au repos et gérer l'accès aux services et ressources AWS pour leurs utilisateurs.

En outre, MOVEWORK a également choisi AWS compte tenu des objectifs d'internationalisation de ses activités ainsi que des garanties de disponibilité et de confidentialité données par AWS.

MOVEWORK a défini les exigences opérationnelles et sa politique de migration de données. MOVEWORK a été accompagnée sur son projet par une entreprise de conseil en technologie et de solutions logicielles, parmi les leaders sur le marché des solutions digitales et cloud, avec ses experts en management d'infrastructures orientées cloud, qui a préconisé une infrastructure garantissant une disponibilité pouvant aller jusqu'à 99,999%, une maîtrise des risques et une sécurité garantie.

4. Où les contenus confiés à MOVEWORK sont-ils stockés par AWS ?

C'est MOVEWORK et elle-seule qui choisit la ou les région(s) dans lesquelles elle souhaite stocker les contenus de ses Clients et Partenaires. Ce qui lui permet de déployer des services AWS à l'emplacement ou aux emplacements répondant aux

choix de ses Clients et Partenaires, conformément aux besoins géographiques de ses Clients et Partenaires.

En effet, les centres de données d'AWS sont conçus sous forme de clusters dans diverses régions du monde. Les clients ont accès à seize régions AWS à travers le monde, dont trois dans l'Union européenne - l'Irlande (Dublin), Le Royaume-Uni (Londres) et l'Allemagne (Francfort). MOVEWORK dispose donc de la faculté de choisir d'utiliser une seule région, toutes les régions ou une combinaison de plusieurs régions.

MOVEWORK a choisi la région Europe et le centre de données d'AWS situé en Irlande. MOVEWORK se réserve le droit de changer de centre de données, au sein de la région Europe.

AWS garantit à MOVEWORK qu'elle ne procédera pas au déplacement et à la réplication des contenus confiés par MOVEWORK en dehors de la ou des régions choisie(s) par MOVEWORK, sauf en cas d'obligation légale ou de nécessité de procéder à la maintenance des services AWS dans le but de pouvoir les proposer aux clients d'AWS et à leurs utilisateurs finaux.

5. Quelles sont les politiques d'AWS dans l'Union Européenne permettant d'assurer la conformité des services gérés par AWS au RGPD ?

5.1. La politique de confidentialité d'AWS

La politique de confidentialité d'AWS décrit la façon dont AWS collecte et utilise les informations liées à un compte qu'elle gère. AWS gère des dizaines de programmes de conformité dans son infrastructure.

Cela signifie que la part des exigences de MOVEWORK et de ses Clients et Partenaires, relevant de la responsabilité d'AWS en tant que prestataire de services, est couverte par cette politique de confidentialité et l'ensemble des politiques décrites par la suite.

La politique de confidentialité d'AWS peut être consultée et téléchargée on-line [ici](#).

5.2. Le Data Processing Addendum

Le « Data Processing Addendum » d'AWS, qui comprend les clauses types de la Commission européenne a été approuvé par le groupe de travail de l'Article 29. Le groupe de travail de l'Article 29 a estimé que le « [Data Processing Addendum](#) » d'AWS respectait les exigences de la directive 95/46/CE sur la protection des données personnelles en ce qui concerne les clauses types. Cela signifie que le « Data Processing Addendum » d'AWS n'est pas considéré comme « ad hoc ». Pour en savoir plus, consultez l'approbation du « Data Processing Addendum » d'AWS par le groupe de travail de l'Article 29.

5.3. Le livre blanc sur la sécurité AWS

AWS met en œuvre une approche de sécurité dès la conception (Security by Design, SbD).

La sécurité dès la conception est une approche en matière d'assurance de sécurité qui formalise la conception de compte AWS, automatise les contrôles de sécurité et rationalise les audits. Au lieu de contrôler la sécurité rétroactivement, la sécurité dans la conception assure un contrôle de la sécurité intégré tout au long du processus de gestion informatique d'AWS.

5.4. Les engagements d'AWS

Les engagements d'AWS en matière de confidentialité et de la sécurité des données comprennent les éléments suivants :

STOCKAGE : AWS permet à ses clients de choisir la ou les régions AWS dans lesquelles le contenu sera stocké. AWS ne procède pas au déplacement ni à la réplification du contenu de ses clients en dehors de la ou des régions choisies par le client, sauf en cas d'obligation légale ou de nécessité de procéder à la maintenance des services AWS dans le but de pouvoir les proposer à nos clients et à leurs utilisateurs finaux.

ACCES ET CONTROLE DU CONTENU : Avec AWS, c'est MOVEWORK qui :
Détermine l'emplacement de stockage des contenus de ses Clients et Partenaires (type et région géographique du stockage).

Choisit l'état de sécurisation des contenus de ses Clients et Partenaires. AWS propose également le chiffrement avancé des contenus en transit ou au repos, ainsi qu'une option permettant à MOVEWORK de gérer ses propres clés de chiffrement.

Gère l'accès aux contenus et aux services et ressources AWS via des utilisateurs, groupes, autorisations et informations d'identification qu'ils contrôlent eux-mêmes.

DIVULGATION DE CONTENU : AWS ne divulgue aucun contenu de ses clients, sauf en cas d'obligation légale ou pour respecter un ordre juridique valide et exécutoire provenant d'un organisme gouvernemental ou réglementaire.

ASSURANCE DE SECURITE : AWS a développé un programme d'assurance de sécurité dont certains éléments de protection de la sécurité et processus de contrôle sont validés par de nombreuses instances d'évaluation indépendantes.

5.5. Le programme AWS de gestion des risques et de la conformité

Grâce au programme de gestion des risques et de la conformité d'AWS, MOVEWORK est en mesure d'intégrer les contrôles AWS au sein de son cadre de gouvernance. Les informations fournies par AWS dans le cadre de son programme de gestion des risques et de la conformité permettent à MOVEWORK de documenter un cadre exhaustif de gouvernance et de contrôle où AWS tient un rôle majeur.

L'environnement de contrôle d'AWS est soumis à diverses évaluations des risques à la fois externes et internes. AWS a également établi un cadre relatif à la sécurité de l'information et des politiques basées sur les objectifs de contrôle COBIT (Control Objectives for Information and related Technology).

Le programme de gestion des risques et de la conformité d'AWS présente l'intégralité des certifications, procédures et contrôles, attestations, établis ou gérés par AWS. Seules les certifications majeures sont rappelées dans le titre 6 ci-après.

6. Quelles sont les auto-certifications, normes de sécurité, certifications et attestations d'organismes tiers d'AWS ?

AWS a obtenu différentes certifications et attestations d'organismes externes de certification et met en œuvre des normes de sécurité, des politiques, procédures et contrôles qui permettent de garantir la conformité au RGPD.

6.1. L'auto-certification US Privacy Shield

Amazon.com, Inc. et 4 autres de ses filiales, dont AWS a obtenu une certification au Privacy Shield du Ministère du commerce américain en date du 21 octobre 2016.

6.2. Les normes de sécurité

L'infrastructure informatique qu'AWS fournit à ses clients, et donc à MOVEWORK, est conçue et gérée conformément aux bonnes pratiques de sécurité et à une grande variété de normes de sécurité informatique, notamment :

- SOC 1/SSAE 16/ISAE 3402 (anciennement SAS 70)
- SOC 2
- SOC 3
- PCI DSS, niveau 1.

Le rapport de sécurité SOC3 pour la période du 1er octobre 2016 au 31 mars 2017 peut être téléchargé ci-après (§ 8.2 de la présente note d'information).

6.3. Les certifications AWS

AWS a également obtenu de nombreuses certifications et notamment :

- ISO 9001 / ISO 27001
- FISMA, DIACAP et FedRAMP
- DOD CSM, niveaux 1-5
- ITAR
- FIPS 140-2
- MTCS, niveau 3AWS.

6.3.1. La certification ISO 27001 /9001

AWS applique des normes de sécurité rigoureuses, telles que la norme ISO 27001/9001. En outre, AWS applique également les rapports SOC 1/2/3 et la norme PCI DSS de niveau 1.

La certification ISO 27001/9001 délivrée à AWS le 11 décembre 2013 peut être téléchargée en cliquant [ici](#).

6.3.2. La certification ISO 27017/27018

La norme ISO 27017 donne des informations sur les aspects de la sécurité de l'information du cloud computing, en recommandant la mise en œuvre de contrôles de sécurité de l'information spécifiques au cloud qui complètent les recommandations des normes ISO 27002 et ISO 27001.

La certification ISO 27017 délivrée à AWS le 01 10 2015 peut être téléchargée en cliquant [ici](#).

La norme ISO 27018 est la première norme internationale spécifique à la protection des données personnelles dans le cloud. La conformité d'AWS avec la norme ISO 27018 a été validée par une instance d'évaluation indépendante.

La certification ISO 27018 délivrée à AWS le 01 10 2015 peut être téléchargée en cliquant [ici](#).

6.4. Le programme d'assurance de sécurité AWS

AWS a développé un programme d'assurance de sécurité faisant appel à d'autres bonnes pratiques globales concernant la confidentialité et la protection des données, afin d'aider ses clients à s'établir et travailler au mieux dans leur environnement de contrôle de la sécurité.

7. Quels sont la sécurité spécifique pour les services de stockage, les fonctionnalités et les services AWS permettant le respect des exigences du RGPD ?

AWS a développé une sécurité spécifique pour les différents services gérés pour ses clients et en particulier pour les services de stockage.

La sécurité est intégrée par AWS à chaque couche de l'infrastructure AWS, mais également dans chacun des services disponibles sur cette infrastructure et en particulier pour les services de stockage.

Le livre blanc d'AWS d'août 2015 présente pour chaque service géré par AWS les processus de sécurité mis en œuvre.

8. Que devez-vous savoir sur la sécurité de l'environnement du cloud AWS et les autres ressources AWS ?

8.1. Le cadre bien structuré de l'infrastructure d'AWS (Well-Architected Framework)

AWS a intégré très tôt dans son offre, l'éducation de ses clients à de meilleures pratiques architecturales pour la conception et l'exploitation fiables, des systèmes

sécurisés, efficaces et rentables dans le cloud. AWS a développé le cadre Well Architected.

AWS Solutions Architects a des années d'expérience dans l'architecture de solutions à travers une grande variété de secteurs d'activité verticaux et d'utilisations, et dans la conception et l'examen de milliers d'architectures de ses clients sur AWS.

Le cadre Well Architected d'AWS est basé sur cinq piliers : la sécurité, la résistance, l'efficacité des performances, l'optimisation des coûts et l'excellence opérationnelle.

Le cadre Well Architected d'AWS a été développé pour aider les architectes en matière de cloud à concevoir des applications dotées d'architectures présentant des niveaux optimaux de sécurité, de performance, de résistance et d'efficacité.

8.2. La sécurité de l'environnement cloud AWS et le modèle de responsabilité partagée entre AWS et ses clients

Les responsabilités dans le Cloud en termes de sécurité sont partagées entre AWS et MOVEWORK, titulaire d'un compte chez AWS. Les responsabilités en termes de conformité sont partagées entre AWS et MOVEWORK.

AWS est responsable de la protection de l'infrastructure globale qui exécute tous les services offerts dans le Cloud AWS. La protection de cette infrastructure est la priorité absolue d'AWS. AWS est également responsable de la configuration de la sécurité de ses produits considérés comme des services gérés.

Les produits AWS entrant dans la catégorie de l'infrastructure en tant que service (IaaS), tels qu'Amazon EC2, Amazon VPC et Amazon S3, sont entièrement sous le contrôle de MOVEWORK et nécessitent que MOVEWORK réalise toutes les tâches de configuration et de gestion de la sécurité nécessaires. A titre d'exemple, pour les instances EC2, MOVEWORK est responsable de la gestion du système d'exploitation invité (notamment les mises à jour et les correctifs de sécurité), de tous logiciels ou utilitaires installés sur les instances, ainsi que de la configuration du pare-feu fourni par AWS sur chaque instance. Par conséquent, MOVEWORK est responsable des mêmes tâches de sécurité qui sont mises en œuvre habituellement, quel que soit l'emplacement des serveurs.

8.3. Les autres ressources de conformité d'AWS on-line

Si vous souhaitez en savoir davantage sur la sécurité de l'environnement du cloud AWS et sur les autres ressources de conformité d'AWS, vous pouvez consulter en ligne les ressources suivantes :

AWS – Amazon Privacy Notice (Avis de confidentialité) du 31 août 2017

<https://www.amazon.com/gp/help/customer/display.html?nodeId=468496>

AWS – Rapport SOC 3 (Pour la période du 1er octobre 2016 au 31 mars 2017)

https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

AWS – Livre blanc sur la protection des données dans l'UE - Novembre 2016

https://d0.awsstatic.com/whitepapers/compliance/FR_Whitepapers/AWS_EU_Data_Protection_Whitepaper_FR.pdf

AWS - AWS Well-Architected Framework – Novembre 2016

http://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

Les 5 piliers d’AWS du cadre Well-Architected :

- pilier Sécurité :

<https://d0.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf>

- pilier fiabilité :

<https://d0.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf>

- pilier efficacité des performances :

<https://d0.awsstatic.com/whitepapers/architecture/AWS-Performance-Efficiency-Pillar.pdf>

- pilier optimization des coûts :

<https://d0.awsstatic.com/whitepapers/architecture/AWS-Cost-Optimization-Pillar.pdf>

pilier excellence opérationnelle : DISPONIBLE PROCHAINEMENT sur le site d’AWS.

AWS – Livre blanc sur les risques et la conformité – Décembre 2015

https://d0.awsstatic.com/whitepapers/compliance/FR_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_FR.pdf

AWS – Security by design – Novembre 2015

https://d0.awsstatic.com/whitepapers/compliance/Intro_to_Security_by_Design.pdf

AWS - Automating Governance

A Managed Service Approach to Security and Compliance on AWS – Août 2015

https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

AWS - Présentation des processus de sécurité – Août 2015

https://d0.awsstatic.com/whitepapers/Security/FR_Whitepapers/AWS_Security_Whitepaper_FR.pdf

AWS – Chiffrement des données – Novembre 2014

https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf