

A100 Badging and Security Briefing Points

A. Points d'information généraux :

- Le badgeage dans et hors des zones sécurisées est nécessaire, et le non-respect des procédures de badgeage entraînera une alarme.
- N'apportez aucun média ou appareil électronique dans le Data Hall (DH) tel que des ordinateurs portables, des téléphones portables, des montres intelligentes, des clés USB...etc.
- Des casiers sont disponibles à la porte d'entrée du Data Hall (à l'extérieur) au cas où vous auriez besoin de sécuriser des objets avant d'entrer.
- Ayez toujours votre badge clairement affiché sur vous (en utilisant des cordons si possible).
- Ne partagez pas et ne prêtez pas votre badge. Si un badge est perdu, signalez-le immédiatement à A100 Security.
- Ne vous reposez/relâchez pas près des poignées de porte/barres de poussée.
- Ne branchez/chargez pas un appareil sur une prise de courant à proximité de l'une de nos portes, contactez la sécurité si nécessaire.
- **Contrôle** : tous les visiteurs doivent être contrôlés par des détecteurs de métaux lorsqu'ils entrent et sortent du Data Hall.
- **La photographie et l'enregistrement vidéo/audio** sont interdits dans toutes les salles/espaces A100.
- **Pour les utilisateurs de badges temporaires** (badges Smart Hand), remettez personnellement votre badge temporaire au bureau de sécurité, et non à un agent de sécurité en patrouille.
- **Evacuation du site** (en cas d'alarme incendie par exemple) : évacuez immédiatement par la sortie de secours disponible la plus proche, utilisez le BGU (Break Glass Unit) pour déverrouiller la porte si nécessaire.

B. Procédures de badgeage :

I. Procédures de badgeage d'entrée (IN) - Data Hall :

1. Appelez la sécurité via l'interphone disponible à la porte du Data Hall.
2. À votre arrivée, l'agent de sécurité vous contrôle au point de contrôle RZN.
3. L'agent de sécurité s'assurera que la porte est bien fermée et sécurisée, puis frappera 3 fois.
4. Saisissez votre code PIN sur le clavier du lecteur puis présentez votre badge A100.
5. L'agent de sécurité saisira son code PIN et présentera son badge immédiatement après vous.
6. L'agent de sécurité ouvrira la porte et vous entrerez tous les deux dans le Data Hall, puis fermez la porte derrière vous.

II. Procédures de badgeage de sortie (OUT) - Data Hall :

- 7.appelez la sécurité via les interphones disponibles à la porte du Data Hall.
- 8.À votre arrivée, l'agent de sécurité vous contrôle au point de contrôle RZN.
- 9.L'agent de sécurité s'assurera que la porte est bien fermée et sécurisée, puis frappera 3 fois.
- 10.Passez votre badge A100 sans ouvrir la porte. Aucun code PIN n'est requis sur le lecteur de badge Out.
- 11.L'agent de sécurité présentera son badge immédiatement après vous.
- 12.L'agent de sécurité ouvrira la porte et vous sortirez tous les deux puis fermerez la porte derrière vous.

III. Procédure de badgeage d'entrée ou de sortie dans les salles autres que les Data Halls:

- 13.Assurez-vous que la porte est complètement fermée et sécurisée.
- 14.Frappez 3 fois, entrez votre code PIN et présentez votre badge A100. (Aucun code PIN n'est requis pour sortir).
- 15.Assurez-vous d'obtenir le **VOYANT VERT** et de franchir la porte.
- 16.Assurez-vous que la porte est bien fermée derrière vous.

C. Accès d'urgence au Data Hall : (le cas échéant)

Dans le cas où un accès d'urgence est nécessaire pour entrer dans le Data Hall, utilisez les portes étiquetées **Sev2/LSE** pour avoir un accès immédiat **sans faire obstacle à l'entrée**.

Veuillez suivre la procédure de badgeage suivante :

- 1.Assurez-vous que la porte est complètement fermée et sécurisée.
- 2.Frappez 3 fois, entrez votre code PIN et présentez votre badge A100.
- 3.Assurez-vous d'obtenir le **VOYANT VERT** puis franchissez la porte ;
- 4.Assurez-vous que la porte est bien fermée derrière vous.

A la fin de l'intervention d'urgence dans le Data Hall, appelez la sécurité via les interphones disponibles aux portes du Data Hall. La sécurité vous contrôlera au point de contrôle RZN à la sortie et la procédure normale de badgeage sera suivie pour sortir.

Note:

Le titulaire du badge et son responsable s'assureront de demander le niveau d'accès approprié permettant l'utilisation appropriée des portes Sev2/LSE le cas échéant.

D. Comment prévenir les alarmes ?

- ✓ Assurez-vous toujours que vous utilisez le badge fourni par A100 avec les bons niveaux d'accès.
- ✓ Ne pas talonner. Ne permettez pas à quelqu'un d'autre de vous talonner par une porte sécurisée.
- ✓ Ne dépassez pas votre période d'accès autorisée.
- ✓ N'utilisez ou n'actionnez jamais une porte sécurisée sans recevoir "accès accordé" avec le **VOYANT VERT**
- ✓ Assurez-vous toujours que la porte est bien fermée et sécurisée derrière vous.
- ✓ N'utilisez pas les issues de secours sauf en cas d'urgence.
- ✓ N'autorisez jamais une autre personne à utiliser votre badge.
- ✓ Si vous perdez votre badge, prévenez immédiatement la sécurité.
- ✓ Si vous présentez votre badge et qu'un **VOYANT ROUGE** apparaît ou que vous entendez une alarme :
NE REPRESENTEZ PAS le badge, contactez A100 Site Security et suivez les instructions.
- ✓ Si vous faites glisser votre badge A100 et que vous ne franchissez pas la porte, **NE PRESENTEZ PAS** à nouveau le badge, contactez la sécurité du site A100 et suivez les instructions.

Nom et prénom : Entreprise : Date :

DCSM/Personnel de sécurité ayant suivi les points d'information sur la sécurité :

« Je reconnaiss par la présente avoir reçu les points d'information sur la sécurité ci-dessus et collecté les badges A100 Visitor, YELLOW, GREEN, BLUE » :

Signature:

CDG Security Induction Acknowledgment

Smart Hand Badges – Visitor Badges

J'accepte de me conformer aux exigences de sécurité d'Amazon et aux procédures d'attribution de badges de sécurité au sein des installations AWS.

La formation d'initiation à la sécurité est obligatoire pour tous les badges Smart Hand et Visitor.

Exceptions : Les employés/entrepreneurs de COLO sont dispensés de signer l'accord de non-divulgation - NDA (DAVOS).

- i. Je confirme avoir signé un accord de non-divulgation (NDA).
- ii. Je confirme avoir regardé et compris les vidéos d'information sur la sûreté et la sécurité.
- iii. Je confirme avoir été formé sur la façon de badger correctement et de passer les portes sur le site sans déclencher d'alarme et je comprends parfaitement toutes les procédures de sécurité.
- iv. Je signe ce document en réception de ma formation initiale.
- v. J'accepte d'être recyclé si je viole la procédure de badgeage ou provoque une alarme.
- vi. Je comprends que mon accès pourrait être immédiatement suspendu/retiré si je ne respecte pas la procédure de badgeage ou si je déclenche une alarme.

Prénom : _____

Nom : _____

Entreprise : _____

Date du briefing : _____

Signature: _____

Informé par S/O Nom : _____

Signature: _____

Accusé de réception des règles régissant l'accès aux centres de données à l'échelle mondiale

Entente cliquable (1 sur 4)

Amazon autorise l'accès à ses centres de données conformément aux conditions du présent Accusé de réception des règles régissant l'accès aux centres de données d'Amazon à l'échelle mondiale et à chacune des politiques citées en référence (le présent « Accusé de réception ») ou à toute autre exigence pouvant être fournie de temps à autre par Amazon ou ses sociétés affiliées (« Amazon »), le cas échéant. En signant cet Accusé de réception, vous reconnaissiez l'avoir lu attentivement, compris et accepté. Les conditions résumées dans le présent document ne modifient pas, ne complètent pas, ni ne remplacent les conditions des politiques qui y sont citées en référence. Vous reconnaissiez que les documents de politique mentionnés dans cet Accusé de réception étaient disponibles pour que vous puissiez en prendre connaissance avant de signer. Les documents relatifs aux politiques mentionnés sont disponibles à la demande à l'accueil de chaque centre de données.

Confidentialité. Vous vous engagez à préserver la confidentialité et assurer la protection de toute information obtenue en accédant aux centres de données, systèmes ou équipements d'Amazon. Cela s'applique à toutes les informations identifiées comme confidentielles ou exclusives ou qui, étant donné la nature de ces informations ou la façon dont elles sont divulguées, devraient raisonnablement être considérées comme confidentielles ou exclusives (y compris, mais sans s'y limiter, toutes les informations relatives à la technologie, aux clients, aux plans d'affaires, aux installations, aux activités marketing et aux finances d'Amazon). Vous reconnaissiez avoir lu et compris tout accord de confidentialité applicable entre vous et Amazon ou votre employeur.

Restrictions relatives aux appareils électroniques personnels (AEP). Les AEP sont soumis à la politique d'Amazon sur les AEP et sont interdits dans un centre de données considéré comme une « zone rouge ». Les AEP comprennent, mais sans s'y limiter, les ordinateurs portables, les appareils photo, les téléphones cellulaires, les montres intelligentes, les bracelets d'activités, les montres électroniques, les produits technovestimentaires et les clés USB. Conformément à la politique d'Amazon sur les AEP et lorsque les lois locales l'autorisent, les appareils non autorisés détectés pendant un contrôle de sécurité peuvent être réinitialisés et/ou détruits. Vous reconnaissiez, comprenez et consentez à ces restrictions et politiques liées aux AEP.

Restrictions relatives à l'enregistrement. L'enregistrement à l'intérieur ou autour des centres de données d'Amazon n'est pas permis et est soumis à la politique du bâtiment relative aux enregistrements. L'enregistrement comprend, mais sans s'y limiter, la capture d'enregistrements sonores, d'enregistrements visuels et de vidéos, la radiodiffusion, la transmission et toute autre activité similaire dans les locaux du centre de données ou dans tout autre lieu lié aux activités d'Amazon. Conformément à la politique du bâtiment relative aux enregistrements et lorsque les lois locales l'autorisent, les appareils non autorisés détectés pendant le contrôle de sécurité peuvent être réinitialisés et/ou détruits. Les photographies requises pour des raisons opérationnelles peuvent être exemptées de cette restriction à condition qu'une exemption soit accordée par écrit au préalable par un agent de sécurité compétent d'Amazon, conformément à la politique du bâtiment relative aux enregistrements d'Amazon, qui décrit le processus d'obtention des exemptions nécessaires. Vous reconnaissiez avoir lu et compris la politique du bâtiment relative aux enregistrements et le risque d'inspection, de réinitialisation et/ou de destruction des photographies ou des appareils non autorisés.

Enregistrement de télévision en circuit fermé (TCF). Amazon exploite des caméras de vidéosurveillance dans ses centres de données, conformément à la politique de vidéosurveillance d'Amazon (et à l'éventuelle déclaration de confidentialité des centres de données applicable à votre emplacement). La politique de vidéosurveillance d'Amazon décrit en détail les pratiques de vidéosurveillance dans les centres de données d'Amazon. Vous reconnaissiez avoir lu et compris la Politique de vidéosurveillance d'Amazon applicable (et l'éventuelle déclaration de confidentialité des centres de données applicable à votre emplacement).

Contrôle de la protection des biens (PB). Toutes les personnes qui entrent dans une zone considérée comme une « zone rouge » d'un centre de données d'Amazon ou qui en sortent devront passer par un poste de contrôle de la protection des biens (PB). Le personnel et l'équipement seront inspectés de manière à trouver tout dispositif de stockage de médias afin d'empêcher le retrait intentionnel ou non des biens de l'entreprise et des stocks d'Amazon. Pendant l'inspection, si le détecteur de métal ou le détecteur à main s'active, vous devez attendre qu'un agent de sécurité donne d'autres instructions et vous devez vous conformer aux demandes subséquentes. Il est interdit d'entrer dans la zone rouge ou d'en sortir sans avoir au préalable appliqué la procédure de détection des métaux ou des médias. Au besoin, veuillez communiquer avec un directeur de la sécurité du centre de données pour présenter une demande médicale d'exemption du contrôle. Le non-respect de la détection des médias avant d'entrer dans la zone rouge ou d'en sortir peut entraîner le retrait immédiat ou la cessation de l'accès aux centres de données ou à d'autres installations d'Amazon. Vous reconnaissiez avoir lu et compris les pratiques d'Amazon en matière de contrôle de la protection des biens.

Conformité en matière de santé et de sécurité. La conformité à toutes les exigences réglementaires régionales applicables en matière d'environnement, de santé et de sécurité et aux exigences générales du centre de données d'Amazon en matière de sécurité du site est obligatoire. Vous acceptez d'obéir à tous les avertissements, panneaux et étiquettes de sécurité affichés. Des chaussures conformes à la norme ASTM F2413, ou l'équivalent local, doivent être portées dans toutes les zones des centres de données, à l'exception des bureaux et des parkings. Aucune nourriture ni boisson n'est autorisée dans une zone à risque. Il est interdit de courir ou de faire du chahut, d'utiliser des armes ou de fumer à l'intérieur du centre de données ou à proximité de tout équipement à risque. Vous reconnaissiez avoir lu et compris les pratiques d'Amazon en matière de conformité à la santé et à la sécurité, et que le non-respect de toutes les exigences peut entraîner un refus ou une révocation d'accès.

Utilisation des périphériques réseau et sans fil. Vous acceptez de lire, d'accepter et de respecter toutes les restrictions et normes énumérées dans la norme Wi-Fi isolée d'Amazon, la politique de sécurité de l'utilisation du réseau et des appareils d'Amazon et la politique de norme de sécurité sans fil des centres de données d'AWS.

Traitement des données personnelles. Amazon collectera certaines données personnelles vous concernant à l'avance et au cours de votre visite dans ses centres de données. Cela comprendra des informations sur les processus d'accès de sécurité du balayage des badges d'Amazon, les informations nécessaires à la sécurité des installations d'Amazon, les informations nécessaires à Amazon pour assurer votre sécurité pendant votre visite ou pour qu'Amazon se conforme à ses obligations en matière de santé et de sécurité, ainsi que l'utilisation du Wi-Fi dans les installations d'Amazon. Vous pouvez demander l'accès à vos données personnelles collectées par Amazon conformément à la législation applicable et à la politique de



Confidentiel Amazon

vidéosurveillance d'Amazon (et à l'éventuelle déclaration de confidentialité des centres de données applicable à votre emplacement).

En signant ce document ou en cliquant sur « J'accepte », vous reconnaisssez et acceptez les conditions de cet Accusé de réception des règles régissant l'accès aux centres de données d'Amazon à l'échelle mondiale et vous confirmez que vous respecterez toutes les politiques d'Amazon associées.

Nom en caractères d'imprimerie _____

Signature _____

Date _____

**Accord de confidentialité****Entente cliquable (2 sur 4)**

Dans le présent accord de confidentialité, les références à « Amazon », « nous », « notre » et « nos » désignent la société Amazon qui exploite le centre de données Amazon que vous fréquentez en tant qu'employé, stagiaire, agent, consultant, sous-traitant, fournisseur, travailleur intérimaire ou visiteur autorisé (collectivement, « vous »). Lorsque vous êtes dans un centre de données d'Amazon, vous pouvez recevoir des informations relatives à Amazon qui ne sont pas connues du grand public (les « Informations confidentielles »). Les Informations confidentielles peuvent concerner, entre autres, la technologie, les installations, les actifs, les systèmes, les clients, les fournisseurs, les plans d'affaires, les finances et d'autres informations d'Amazon, qui doivent être traitées raisonnablement comme étant confidentielles. Une Information confidentielle peut être contenue dans des documents tangibles comme des dessins, des données, des spécifications, des rapports et des programmes informatiques, ou peut prendre la forme d'une connaissance non écrite. En tant qu'entreprise de haute technologie, Amazon doit protéger les Informations confidentielles contre l'utilisation et la divulgation non autorisées.

Vous convenez (i) que toutes les Informations confidentielles resteront la propriété exclusive d'Amazon, (ii) que vous pouvez utiliser les Informations confidentielles pour fournir les services liés à votre visite au centre de données et à aucune autre fin, (iii) que vous ne divulguerez aucune Information confidentielle à toute personne, entreprise ou autre tierce partie, (iv) que vous limiterez la possession, la connaissance et l'utilisation des Informations confidentielles aux personnes autorisées par Amazon à recevoir des Informations confidentielles et qui ont besoin de connaître les Informations confidentielles précises, (v) que vous aviserez Amazon immédiatement dès la découverte de toute utilisation ou divulgation non autorisée d'Informations confidentielles ou toute autre violation du présent accord, et (vi) à la demande d'Amazon, vous livrerez à Amazon tous les documents contenant des Informations confidentielles et, à votre gré, vous fournirez à Amazon une attestation écrite de conformité. Vous acceptez également de ne divulguer à Amazon aucune Information confidentielle ou exclusive à vous ou à toute autre personne ou société. Vous devrez vous conformer au présent accord pendant cinq (5) ans à compter de la date d'acceptation des présentes conditions.

Si toute clause de cet accord est réputée nulle en vertu des lois en vigueur, cette nullité n'influence pas les autres clauses de cet accord qui peuvent être appliquées sans la clause nulle. De plus, tous les termes et conditions de cet accord seront considérés exécutoires dans toute la mesure du possible dans le cadre des lois applicables, et, quand cela est nécessaire, le tribunal doit réformer tous les termes ou conditions pour leur donner un tel effet. Si une disposition du présent accord est incompatible avec une disposition de l'accord de confidentialité (le « Contrat parent »), le cas échéant, entre Amazon ou ses sociétés affiliées et l'employeur actuel du soussigné, le conflit sera résolu en faveur du Contrat parent.

Amazon s'appuie sur votre engagement à respecter strictement le présent accord. Toute violation du présent accord peut causer des préjudices substantiels et irréparables à Amazon. En conséquence, sans limiter la portée de tout autre recours, le présent accord est spécialement exécutoire par Amazon. Le présent accord sera interprété conformément aux lois internes de l'État de Washington, aux États-Unis.

Tout manquement de la part d'Amazon à veiller à ce que vous respectiez strictement toute clause du présent accord ne constitue pas une renonciation au droit d'Amazon d'appliquer ultérieurement cette clause ou toute autre clause du présent accord.

En signant ce document ou en cliquant sur « J'accepte », vous convenez et acceptez les conditions du présent accord de confidentialité et vous vous conformerez aux politiques d'Amazon associées.

Nom en caractères d'imprimerie _____

Signature _____

Date _____

Formation à la sûreté et à la sécurité

Entente cliquable (3 sur 4)

- **Vidéo de formation sur la sûreté et la sécurité :** <https://d26hlm42fohrnh.cloudfront.net/story.html> (lien accessible dans le corps des contrats par courriel).
- **Constater un problème, avertir :** Si vous prenez connaissance d'un problème susceptible d'affecter la sécurité de tout membre du personnel ou la sécurité du centre de données, veuillez contacter le personnel de la Sécurité physique.
- **Sécurité :** La sécurité est notre priorité absolue. Tous les travaux doivent respecter les exigences de sécurité des centres de données d'AWS :
 - Respecter toutes les lois et normes de sécurité pertinentes ;
 - Adopter des pratiques de travail sans danger en toutes circonstances ;
 - Suivre les procédures de sécurité appropriées ;
 - S'assurer que le gestionnaire du site est informé à l'avance de tous les changements d'état dans le centre de données ; et
 - Informer le gestionnaire du site de tout nouveau danger non prévu à l'origine avant de démarrer des travaux.
- **Accès :** La sécurité couvrira votre accès au site pour ce qui est strictement nécessaire à la réalisation de votre travail.
- Les **badges** doivent être portés à tout moment. Ne partagez pas ou ne prêtez pas votre badge. Toute perte de badge doit immédiatement être signalée à la Sécurité physique. Le personnel muni d'un badge de visiteur doit être accompagné à tout moment.
- Il est nécessaire de **passer son badge** pour entrer dans des zones sécurisées et pour en sortir, et le non-respect de ces procédures déclenchera une alarme. Si une alarme retentit, restez sur le site de l'alarme et attendez que la Sécurité physique arrive. Si vous ne pouvez pas sortir d'une pièce et que vous n'avez aucun moyen de communiquer, vous pouvez utiliser l'évacuation d'urgence au bout de 10 minutes.
 - **Pour éviter qu'une alarme anti-retour ne se déclenche :** 1) passez par la porte lorsque l'accès est autorisé ; 2) ne suivez pas de trop près la personne située devant vous ; et 3) ne dépassez pas votre période d'accès autorisée.
 - **Pour éviter qu'une alarme de porte forcée ne se déclenche :** 1) soyez attentif aux panneaux de porte sécurisés ; 2) n'utilisez pas les issues de secours sauf en cas d'urgence ; et 3) ne touchez jamais une porte sécurisée sans passer votre badge et sans voir s'afficher « accès autorisé ».
 - **Pour éviter qu'une alarme de maintien de porte ouverte ne se déclenche :** 1) tirez toujours la porte jusqu'à ce qu'elle se referme après être entré ; 2) ne maintenez aucune porte ouverte plus de 60 secondes ; et 3) ne vous appuyez pas contre une porte ouverte.
- **Le contrôle de la protection des biens (PB)** pour les dispositifs de stockage de médias est exigé pour toutes les personnes et tous les équipements entrant dans les zones d'une salle de données et en sortant. Des exceptions au contrôle pour des équipements limités peuvent être demandées par le biais de la Sécurité physique, et des mesures d'adaptation médicales ou autres peuvent être demandées par le biais des RH.
- **La photographie** et l'enregistrement vidéo/audio sont interdits sur les campus des centres de données sans autorisation écrite préalable.

En signant ce document ou en cliquant sur « J'accepte », vous reconnaissiez : 1) avoir vu ou reçu et compris les vidéos ou documents de formation sur la sûreté et la sécurité ; et 2) avoir examiné les lignes directrices citées et que vous vous y conformerez.

Nom en caractères d'imprimerie _____

Signature _____

Date _____

Déclaration de confidentialité sur les centres de données d'Amazon dans l'Union européenne (UE)

Entente cliquable (4 sur 4)

Dans la présente Déclaration de confidentialité sur les centres de données d'Amazone dans l'UE et au Royaume-Uni (« Déclaration »), les références à « Amazon », « nous », « notre » et « nos » désignent la société Amazon qui exploite le centre de données Amazon que vous fréquentez en tant qu'employé, stagiaire, agent, consultant, sous-traitant, fournisseur, travailleur intérimaire ou visiteur autorisé (collectivement, « vous »). Amazon et ses sociétés affiliées seront désignées collectivement sous le nom de « Groupe Amazon ». Pour le personnel Amazon basé dans l'UE et au Royaume-Uni, veuillez également consulter la Déclaration de confidentialité du personnel Amazon basé dans l'EU sur Inside Amazon.

Nous savons que vous êtes attentifs à la façon dont nous utilisons vos informations et vous remercions de votre confiance pour les traiter de manière rigoureuse et raisonnable. Cette Déclaration décrit la manière dont nous collectons, utilisons et transférons (collectivement « traitons ») vos données personnelles.

1. Est-ce que cette Déclaration vous concerne ?

Cette Déclaration s'applique à toute personne visitant un centre de données Amazon, que vous soyez ou non un employé Amazon. Nous traiterons vos informations personnelles comme décrit dans cette Déclaration et dans nos autres politiques et procédures connexes relatives à la protection et à la sécurité des données.

2. Qui est le responsable du traitement ?

Le responsable du traitement est Amazon, ce qui signifie que nous décidons comment et pourquoi vos données personnelles sont traitées. L'entité spécifique agissant à titre de contrôleur est décrite dans l'Annexe de la présente déclaration. Pour obtenir les coordonnées des personnes de contact en cas de questions sur vos droits par rapport à cette Déclaration, veuillez consulter la section « Questions et interrogations » ci-dessous.

3. Comment et pourquoi traitons-nous vos données personnelles ?

Les données personnelles que nous recueillons auprès de vous ou par l'intermédiaire de nos systèmes facilitent votre accès à nos centres de données et renforcent leur sécurité. Le tableau ci-dessous contient des détails sur les données personnelles que nous pouvons collecter à votre sujet, la base juridique sur laquelle nous nous appuyons pour traiter ces données et les finalités pour lesquelles nous les traitons.

Catégorie d'informations	Base juridique du traitement	Finalité du traitement
Nous pouvons collecter les informations d'identification suivantes auprès des <u>employés Amazon</u> : - vos nom et prénom ; - votre identifiant d'employé Amazon ; - votre identifiant d'utilisateur Amazon ; et - le numéro figurant sur votre badge d'accès.	Il est nécessaire que nous traitions ces informations dans nos intérêts légitimes afin d'assurer la sécurité de nos centres de données, et nous considérons que les mesures prises sont proportionnées et n'ont pas d'incidence excessive sur votre vie privée.	Nous avons besoin de ces informations pour gérer l'accès à nos centres de données et pour assurer la sécurité de nos centres de données de manière plus générale.
Si vous n'êtes <u>pas un employé Amazon</u> , nous pouvons collecter tout ou partie des informations d'identification suivantes auprès de vous : - vos nom et prénom ; - votre sexe ; - votre date de naissance ; - une photographie ; - une photocopie de votre pièce d'identité ; - le numéro d'immatriculation de votre véhicule ; - votre adresse postale professionnelle ; - votre numéro de téléphone ; - votre adresse e-mail ; - le nom de votre employeur ; et - le numéro figurant sur votre badge d'accès.	Il est nécessaire que nous traitions ces informations dans nos intérêts légitimes afin d'assurer la sécurité de nos centres de données, et nous considérons que les mesures prises sont proportionnées et n'ont pas d'incidence excessive sur votre vie privée.	Nous avons besoin de ces informations pour gérer l'accès à nos centres de données et pour assurer la sécurité de nos centres de données de manière plus générale.
Nous pouvons recueillir des données de santé limitées auprès de vous lorsque vous remplissez le <u>formulaire d'exemption médicale volontaire</u> approprié et (le cas échéant) lorsque vous nous fournissez un certificat médical ou à la suite d'un accident ayant impliqué votre santé et votre sécurité.	Si vous travaillez pour Amazon, nous ne pouvons collecter et traiter vos données de santé limitées à la suite d'un incident de santé et de sécurité que lorsque ce traitement est nécessaire pour nous permettre de respecter nos obligations en vertu de la législation du travail ou d'autres lois applicables, ou d'exécuter notre contrat de travail avec vous.	Nous avons besoin de ces informations pour respecter nos obligations en matière de santé et de sécurité et, dans certaines situations, pour pouvoir répondre à votre demande d'exemption de tout ou d'une partie de nos procédures de sécurité (par exemple, les détecteurs de métaux) pour des raisons de santé.

Catégorie d'informations	Base juridique du traitement	Finalité du traitement
	<p>Il peut vous être demandé d'accepter notre politique de collecte et d'utilisation de vos données de santé limitées lorsque vous remplissez le formulaire d'exemption médicale volontaire approprié ou à la suite d'un accident ayant impliqué votre santé et votre sécurité si vous êtes en mesure de le faire (sinon, nous pouvons agir sur la base des intérêts vitaux des personnes si vous n'êtes pas en mesure de donner votre consentement).</p>	
Nos centres de données sont dotés d'un réseau de vidéosurveillance, et vous pouvez être personnellement identifiable sur les images de vidéosurveillance . Veuillez consulter la section 4 ci-dessous pour de plus amples renseignements.	<p>Il est nécessaire que nous traitions ces informations dans nos intérêts légitimes afin d'assurer la sécurité de nos centres de données, et nous considérons que les mesures prises sont proportionnées et n'ont pas d'incidence excessive sur votre vie privée.</p>	<p>Nous devons enregistrer et stocker les images de vidéosurveillance afin d'assurer la sécurité de nos locaux, de protéger le personnel et les visiteurs, de faciliter l'identification des personnes qui enfreignent les politiques de sécurité d'Amazon et, dans certains cas, de nous conformer aux exigences légales et de contribuer à la prévention et à la détection des infractions.</p>
Nous pouvons recueillir des données de santé, telles que votre température et vos symptômes de maladie, avant d'entrer dans le bâtiment. Nous recueillons également les coordonnées à des fins de recherche des contacts.	<p>Nous pouvons traiter ces informations pour nos intérêts légitimes et afin de respecter nos obligations en matière de santé et de sécurité en tant qu'employeur</p>	<p>Nous devons traiter ces données personnelles pour lutter contre la propagation de la COVID-19, dans le cadre des mesures que nous avons prises face à la pandémie.</p>
Nous pouvons collecter des données sur les systèmes d'accès (y compris des données lenel) et des données sur votre utilisation du Wi-Fi auprès de vous pendant que vous vous trouvez dans le centre de données.	<p>Il est nécessaire que nous traitions ces informations dans nos intérêts légitimes afin d'assurer la sécurité de nos centres de données, et nous considérons que les mesures prises sont proportionnées et n'ont pas d'incidence excessive sur votre vie privée.</p> <p>Il peut également être nécessaire que nous traitions ces informations afin de nous conformer à nos obligations légales et réglementaires, y compris dans le but de présenter des réclamations ou d'engager des poursuites pénales ou de vous défendre dans le cadre de celles-ci.</p>	<p>Nous devons traiter ces données pour assurer la sécurité de nos centres de données et assurer le respect des politiques d'Amazon. Si vous êtes impliqué dans un incident de sécurité ou y avez assisté, nous pouvons recueillir des informations supplémentaires aux fins de l'enregistrement et du traitement de l'incident.</p>
Nous pouvons recueillir les informations nécessaires pour assurer votre sécurité et celle d'autrui pendant votre visite ou pour nous conformer à nos obligations en matière de santé et de sécurité.	<p>Il peut vous être demandé d'accepter notre politique de collecte et d'utilisation de vos données de santé limitées lorsque vous nous les communiquez, ou lorsque nous vous les demandons, ou lorsque nous traitons des données en rapport avec un accident ayant impliqué votre santé et votre sécurité si vous êtes en mesure de le faire (sinon, nous pouvons agir sur la base des intérêts vitaux des personnes si vous n'êtes pas en mesure de donner votre consentement).</p> <p>Pour les employés, il est nécessaire que nous traitions ces informations dans nos intérêts légitimes afin d'assurer la sûreté et la sécurité de nos centres de données, et nous considérons que les mesures prises sont proportionnées et n'ont pas d'incidence excessive sur votre vie privée.</p>	<p>Nous traitons les données de sûreté et de sécurité afin de vous protéger contre les accidents du travail et de rendre votre lieu de travail plus sûr.</p>

Vous avez le droit de vous opposer au traitement de vos informations personnelles sur la base de nos intérêts légitimes à tout moment. Cependant, il est peu probable que nous vous autorisions à accéder à nos centres de données si nous ne pouvons pas utiliser vos données de la manière requise — reportez-vous à la section 10.

4. Où est-ce qu'Amazon obtient mes données personnelles ?

Nous pouvons obtenir des informations d'identification pertinentes auprès de vous ou de votre employeur ou de votre responsable avant votre visite, dans le cadre du processus de demande d'accès à notre centre de données. Nous pouvons également collecter ces informations directement auprès de vous sur Internet et/ou en personne au centre de données, lorsque vous remplissez la feuille de présence et/ou l'accord d'accès applicable et que vous suivez les procédures d'accès à notre site (par exemple en ce qui concerne les vérifications d'identité) ou lorsque vous vous trouvez dans nos locaux ou utilisez nos systèmes.

Nous pouvons recevoir des **données de santé limitées** de vous, de votre employeur ou de votre responsable avant votre visite (le cas échéant), afin de traiter votre demande d'exemption de tout ou d'une partie de nos procédures de contrôles de sécurité, ou pour répondre à d'autres craintes en matière de santé dont vous nous faites part. Nous pouvons également recevoir des données de santé limitées de votre part lorsque cela s'avère nécessaire pour respecter nos obligations en matière de santé et de sécurité ou à la suite d'un incident de santé et de sécurité vous impliquant.

Les **images de vidéosurveillance** sont collectées dans nos centres de données conformément à la loi et aux procédures et politiques approuvées relatives à l'installation de caméra, à l'utilisation, au stockage et au transfert des images. Une autorisation préalable est requise avant d'autoriser quelqu'un de l'extérieur à accéder aux images de vidéosurveillance. Nous examinons régulièrement l'utilisation de la vidéosurveillance pour nous assurer qu'elle demeure nécessaire, appropriée et proportionnée compte tenu des risques de sécurité présents.

Pour des raisons de sécurité, nous sommes également en mesure de suivre l'accès à des zones spécifiques de notre centre de données lors de votre visite munie de votre badge.

5. Partageons-nous vos informations personnelles avec des tiers ?

Les sociétés de notre Groupe

Nous pouvons partager vos données personnelles avec d'autres sociétés du Groupe Amazon qui œuvrent à garantir la sécurité sur le lieu de travail ou à faire respecter la sécurité dans nos centres de données ou pour des raisons d'administration du groupe, par exemple lorsque nous utilisons des systèmes ou des processus centralisés. Les données personnelles ne seront partagées dans l'ensemble du Groupe Amazon que dans certaines circonstances et dans la mesure où la loi le permet. Chaque fois que nous avons besoin de partager vos données personnelles, nous le ferons uniquement en cas de nécessité absolue et avec des employés sélectionnés qui peuvent raisonnablement avoir besoin de ces informations pour accomplir des tâches relevant de leurs responsabilités professionnelles. Amazon prend les mesures appropriées pour s'assurer que ce personnel est lié par des obligations de confidentialité en ce qui concerne vos données personnelles.

Divulgation aux fournisseurs de services et à des tiers

Dans certaines circonstances, nous partageons et/ou sommes tenus de partager vos données personnelles avec des tiers en dehors du Groupe Amazon, aux fins décrites ci-dessus et conformément aux lois sur la protection des données applicables. Ces parties agiront en tant que responsables du traitement tiers de vos données personnelles de plein droit, et elles seront tenues de respecter les lois applicables en matière de protection des données. Nous nous assurerons pour tout tiers auquel nous avons recours qu'il peut fournir des garanties suffisantes concernant la confidentialité et la sécurité de vos données. Nous imposons à ces tiers de se conformer aux exigences pertinentes des lois applicables dans le cadre d'un tel arrangement.

Ces tiers sont :

- nos fournisseurs de services de sécurité ;
- nos assureurs ;
- les autorités publiques et les organes chargés de faire respecter la loi (comme la police ou les procureurs) ;
- les conseillers externes (tels que les conseillers juridiques ou les comptables) ;
- les autorités chargées de la protection des données.

6. Amazon transfère-t-elle des données personnelles vers des pays en dehors de l'EEE ?

Nous transférons également les données personnelles que nous traitons vers des pays en dehors de l'Espace économique européen (« EEE ») (ou du Royaume-Uni si vous êtes au Royaume-Uni), par exemple lorsque l'un de nos fournisseurs de services (y compris les sociétés du Groupe Amazon) emploie du personnel ou utilise des équipements basés en dehors de l'EEE (ou du Royaume-Uni si vous êtes au Royaume-Uni). Nous avons mis en place des garanties concernant la protection de votre vie privée et de vos droits et libertés fondamentaux, et l'exercice de vos droits, par exemple. Lorsque nous transférons des données personnelles vers un pays qui n'a pas reçu de décision d'adéquation de la part de la Commission européenne, nous mettons en place des clauses contractuelles types, dont de plus amples informations peuvent être fournies sur demande. Veuillez consulter les coordonnées de la section « Questions et interrogations » ci-dessous.

7. Comment assurons-nous la protection de vos informations personnelles ?

Nous maintenons en place des mesures de protection physiques, électroniques et procédurales pour préserver la confidentialité, l'intégrité et la disponibilité de vos données personnelles. Nous avons notamment pris des mesures de sécurité contre le traitement illégal ou non autorisé des données personnelles, et contre la perte accidentelle ou la détérioration des données personnelles.

8. Quelle est la durée de conservation de vos informations personnelles ?

Nous conservons les données personnelles conformément aux politiques de conservation des données convenues. En règle générale, nous conserverons :

Type de données	Durée de conservation
Vos données d'identification personnelles	Pendant un maximum de 18 mois à compter du jour de la collecte.



Images de vidéosurveillance	Sauf autorisation par la loi en vigueur, pendant une période ne dépassant pas celle prévue dans la Politique de vidéosurveillance.
Données des systèmes d'accès	Sauf indication contraire de la loi locale, pendant au plus 12 mois à compter du jour de la collecte.
Données de santé limitées	Sauf autorisation par la loi en vigueur, pendant une période ne dépassant pas 3 ans à compter de la fin de notre relation avec vous.

Nous pouvons parfois avoir besoin de conserver une copie de vos informations personnelles plus longtemps, si nous enquêtons sur un incident de sécurité dans le centre de données dans lequel vous vous êtes rendu ou pour nous conformer à des exigences légales ou réglementaires, y compris pour présenter des demandes en justice ou engager des poursuites pénales ou pour vous défendre dans le cadre de celles-ci. Nous ne conserverons pas vos informations personnelles plus longtemps que nécessaire.

9. Quels sont mes droits en vertu des lois applicables en matière de protection des données ?

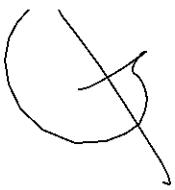
Vous avez le droit de demander l'accès, la rectification ou la suppression de vos données personnelles, de demander la portabilité des données, et, en fonction des lois de votre pays, de définir des instructions relatives à la gestion de vos données personnelles après votre décès. Dans certains cas, vous avez également le droit de vous opposer au traitement de vos données personnelles ou d'en demander la restriction. Lorsque nous traitons vos données personnelles sur la base de votre consentement, vous pouvez le retirer à tout moment. Pour faire une demande en tant que personne concernée, veuillez nous contacter à l'adresse EU-privacy-DSR@amazon.com. Ces droits sont tous soumis à diverses exemptions et restrictions. Si vous souhaitez exercer l'un de ces droits, veuillez nous contacter en utilisant les coordonnées figurant à la section 10.

10. Questions et interrogations

Pour plus d'informations sur la façon dont nous utilisons vos informations ou pour faire une demande concernant vos droits en matière de protection des données, veuillez nous envoyer un e-mail à l'adresse suivante : EU-privacy-DSR@amazon.com. Si vous avez des préoccupations concernant la protection de votre vie privée, veuillez nous contacter en nous envoyant une description détaillée et nous essaierons de résoudre votre problème. Vous pouvez également déposer une plainte auprès d'une autorité de surveillance. Si vous avez des préoccupations concernant la protection de votre vie privée, veuillez nous contacter en nous envoyant une description détaillée et nous essaierons de résoudre votre problème. Vous pouvez également déposer une plainte auprès d'une autorité de surveillance.

Annexe – Responsables du traitement des données

Pays	Entité opérationnelle d'AWS
Autriche	Amazon Data Services Austria GmbH
Belgique	Amazon Data Services Belgium SRL
Bulgarie	Amazon Data Services Bulgaria LLC
Croatie	Amazon Data Services Zagreb d.o.o.
République tchèque	Amazon Data Services Czech Republic s.r.o.
Danemark	Amazon Data Services Denmark ApS
Finlande	Amazon Data Services Finland Oy
France	Amazon Data Services France SAS
Allemagne	A100 ROW GmbH
Grèce	Amazon Data Services Greece
Hongrie	Amazon Data Services Hungary Korlátolt Felelősségi Társaság
Irlande	Amazon Data Services Ireland Ltd.
Italie	Amazon Data Services Italy S.R.L.
Lettonie	Amazon Data Services Latvia SIA
Pays-Bas	Amazon Data Services Netherlands N.V.
Norvège	Amazon Data Services Norway AS
Pologne	Amazon Web Services Poland sp. z o. o.
Portugal	Amazon Data Services, Portugal, Lda
Roumanie	Amazon Data Services Romania S.R.L.
Slovénie	Amazon Data Services, podatkovne storitve, d.o.o.
Espagne	Amazon Data Services Spain, S.L.U.

Confidentiel Amazon

Suède	Amazon Data Services Sweden AB
Royaume-Uni	Amazon Data Services UK Limited

9 septembre 2021