

Annexes II et III HPE Managed HPC Cloud Bursting Services

Annexe II : Description du traitement

<p>1. Description du traitement</p>	<p>Dans le cadre de la fourniture de HPE Managed Services, le Responsable du traitement peut accéder aux données stockées dans les applications d'entreprise (y compris les métadonnées), les ressources informatiques et l'infrastructure réseau du Contrôleur. Ces données peuvent comprendre des données personnelles du Contrôleur. De plus, le Responsable du traitement a recours à une plateforme basée sur un logiciel as-a-service (par ex. la HPE Hybrid Operations Console ou HOC) pour exploiter et gérer les actifs informatiques du Client. La console HOC sert à recevoir et à suivre les demandes de service IT provenant du Contrôleur. Le Contrôleur a la possibilité de joindre un fichier, qui peut être chiffré ou non, à sa demande de service sur la console HOC. Ces fichiers peuvent comprendre des données personnelles du Contrôleur.</p>
<p>2. Type de données personnelles traitées</p>	<p>Dans le cadre spécifique de l'offre HPE Managed HPC Cloud Bursting Service, le Responsable du traitement exécute des tâches/programmes qui assurent le transfert des charges de travail du Client depuis les systèmes du Client (situés sur site ou au sein de datacenters partagés) vers des instances cloud (ou vice-versa) à l'aide d'une plateforme tierce (Rescale, par exemple). Dans le cadre de cette tâche, le Responsable du traitement a accès aux données stockées dans les charges de travail du Contrôleur à mesure que ces données sont chiffrées pour le traitement au sein de la plateforme tierce. Ces données peuvent comprendre des données personnelles du Contrôleur.</p>
<p>2. Type de données personnelles traitées</p>	<p>Le type de données personnelles traitées dépend des données que le Contrôleur a stockées dans les applications d'entreprise (y compris les métadonnées), les ressources informatiques et l'infrastructure réseau ainsi que les fichiers non chiffrés que le Contrôleur peut avoir joints aux demandes de service sur la console HOC et peut inclure des données personnelles sensibles. Voici quelques exemples (liste non exhaustive) : Nom (prénom et nom), adresse, pays, numéro de téléphone, adresse e-mail, ID d'organisme officiel, SSN, permis de conduire, données d'immigration (numéro de passeport), date de naissance, âge, sexe, données biométriques, condamnations pénales, handicaps, informations génétiques, informations sur la santé et éventuellement informations sur la santé protégées aux États-Unis (HIPAA), religion, convictions philosophiques, orientation sexuelle, identification et expression de genre, syndicat professionnel, appartenance à un comité d'entreprise, origine raciale ou ethnique, opinions politiques, adresse IP, ID de l'appareil, identifiants, mot de passe, informations de géolocalisation, suivi, données d'analyse, compte bancaire, carte de crédit, carte de débit.</p>
<p>3. Catégories de données personnelles traitées</p>	<p>Toute personne concernée dont les données personnelles sont stockées par le Contrôleur dans les applications d'entreprise (y compris les métadonnées), les ressources informatiques, l'infrastructure réseau et les charges de travail, et les fichiers joints aux demandes de service dans la console HOC, y compris, sans limite, les clients, les utilisateurs finaux, les employés, les sous-traitants et les travailleurs temporaires du Contrôleur.</p>
<p>4. Durée du traitement</p>	<p>Le Responsable du traitement traitera les données personnelles du Contrôleur pendant la durée du Contrat et/ou du document de transaction applicable. Ces données seront purgées automatiquement au bout de 90 jours suivant l'expiration ou la résiliation du contrat de service du Contrôleur avec le Responsable du traitement.</p>
<p>5. Mesures techniques et organisationnelles</p>	<p>Le Responsable du traitement gèrera les informations et le programme de sécurité physique en vue de la protection des données personnelles du Contrôleur selon les modalités détaillées dans l'Annexe III ci-dessous.</p>

Annexe III : Mesures techniques et organisationnelles comprenant les mesures techniques et organisationnelles pour assurer la sécurité des données

1. Dans le cadre des informations du Responsable du traitement et du programme de sécurité physique pour la protection des données personnelles du Contrôleur (« Programme de sécurité du Responsable du traitement »), le Responsable du traitement procède à des examens périodiques des pratiques de sécurité par rapport aux normes de l'industrie, telles que les normes NIST, ISO 27001 et SOC. Le Responsable du traitement réévalue et met à jour le Programme de sécurité du Responsable du traitement de façon régulière, en fonction de l'évolution de l'industrie, de l'émergence de nouvelles technologies ou de l'identification de nouvelles menaces.
2. Le Programme de sécurité du Responsable du traitement comprend au moins les éléments suivants :
 - 2.1. Le Responsable du traitement gère des normes de sécurité physique permettant d'interdire l'accès physique non autorisé aux infrastructures physiques et aux équipements du Responsable du traitement à l'aide des pratiques suivantes :
 - Accès physique aux sites limité aux employés du Responsable du traitement, aux sous-traitants et aux visiteurs autorisés ;
 - Remise aux employés du Responsable du traitement, sous-traitants et visiteurs autorisés de cartes d'identification, qu'ils doivent porter pendant qu'ils se trouvent sur site ;
 - Surveillance de l'accès aux infrastructures physiques du Responsable du traitement, y compris les zones restreintes et les équipements situés dans les infrastructures physiques ;
 - Consignation, surveillance et suivi des accès au datacenter où les données personnelles du Contrôleur sont hébergées ; et
 - Alarmes système et caméras vidéo pour sécuriser les datacenters.
 - 2.2. Le Responsable du traitement gère un contrôle de l'accès à l'environnement informatique pertinent conformément aux meilleures pratiques de l'industrie. Ces contrôles incluent, sans s'y limiter, les prérequis spécifiques aux principes du moindre privilège et à la complexité et l'utilisation des mots de passe.
 - 2.3. L'infrastructure du Responsable du traitement présente des versions à jour raisonnables des logiciels de sécurité du système, qui peuvent inclure un pare-feu hôte, une protection antivirus, ainsi que des correctifs et des définitions de virus à jour. Le Responsable du traitement maintient des journaux des événements liés à l'infrastructure, y compris des systèmes de détection d'intrusion pour surveiller, détecter et signaler les comportements abusifs, les activités suspectes, les utilisateurs non autorisés et autres risques liés à la sécurité.
3. Sur demande, le Responsable du traitement examinera avec le Contrôleur un résumé des évaluations des vulnérabilités. Les évaluations des vulnérabilités n'autorisent pas le Contrôleur à visualiser ou à accéder d'une manière quelconque aux documents et/ou aux processus : (a) non liés directement aux services ; (b) en violation avec les lois applicables ; et/ou (c) en violation avec les obligations de confidentialité et de sécurité du Responsable du traitement relevant d'une tierce partie.
4. Les employés et les sous-traitants sont formés aux politiques de confidentialité et de sécurité du Responsable du traitement et sensibilisés sur leurs responsabilités par rapport aux pratiques de confidentialité et de sécurité. Les employés et les sous-traitants du Responsable du traitement sont contractuellement tenus de maintenir la confidentialité des données personnelles du Contrôleur et de se conformer aux politiques, normes ou prérequis applicables du Responsable du traitement concernant le traitement des données personnelles du Contrôleur. Le non-respect de ces politiques, normes ou prérequis fera l'objet d'une enquête, qui pourra se traduire par une mesure disciplinaire pouvant inclure et aller jusqu'à la cessation de l'emploi par le Responsable du traitement.

5. Si le Responsable du traitement constate une faille de sécurité provoquant une destruction, une perte ou une altération accidentelle ou illégale ou la divulgation ou la consultation non autorisée (« Incident de sécurité ») des données personnelles du Contrôleur, le Responsable du traitement :
- 5.1. Sans retard injustifié, informera le Contrôleur de l'Incident de sécurité. Le Responsable du traitement tiendra le Contrôleur informé du statut de l'Incident de sécurité jusqu'à la résolution de la situation. Les rapports comprendront, sans s'y limiter, une description de l'Incident de sécurité, les mesures prises et des plans de remédiation. Si le Contrôleur a connaissance d'un Incident de sécurité qui affecte les services, le Contrôleur informera rapidement le Responsable du traitement de cet incident et indiquera au Responsable du traitement l'ampleur de l'Incident de sécurité.
- 5.2. À la demande et aux frais du Contrôleur, le Prestataire (i) apportera une assistance raisonnable au Contrôleur en signalant la faille de sécurité à l'autorité de supervision compétente en vertu des lois sur la confidentialité applicables au Contrôleur ; et (ii) apportera une assistance raisonnable au Contrôleur en signalant la faille de sécurité aux personnes concernées dans les cas où il est probable que la faille de sécurité compromette considérablement les droits et les libertés des personnes.

Visiter [HPE.com](https://www.hpe.com)

[Live Chat](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Les informations figurant dans le présent document sont sujettes à modification sans préavis. Les seules garanties relatives aux produits et services Hewlett Packard Enterprise sont stipulées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucune information du présent document ne saurait être considérée comme constituant une garantie supplémentaire. Hewlett Packard Enterprise décline toute responsabilité en cas d'erreurs ou d'omissions de nature technique ou rédactionnelle dans le présent document.

a50009607FRE, Rév. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

