Anexos II y III de HPE Managed HPC Cloud Bursting Services

Anexo II: descripción del procesamiento

1.	Descripción del procesamiento	Como parte de la prestación de HPE Managed Services, el Procesador podrá acceder a los datos almacenados en las aplicaciones empresariales (incluidos los metadatos), la TI y la infraestructura de red del Controlador. Esto puede incluir los datos personales del Controlador. Además, el Procesador utiliza una plataforma basada en SaaS [es decir, HPE Hybrid Operations Console («HOC»)] para operar los activos de TI del Cliente. La consola HOC se utiliza para recibir y realizar el seguimiento de las solicitudes de servicio de TI realizadas por el Controlador. El Controlador cuenta con la opción de adjuntar un archivo, que podrá ser cifrado o no, a la solicitud de servicio en la consola HOC. Este archivo puede incluir los datos personales del Controlador. Específicamente en el contexto de HPE Managed HPC Cloud Bursting Services, el Procesador ejecuta tareas/programas que proporcionan transferencias de las cargas de trabajo del Cliente de los sistemas del Cliente (en los centros de datos locales o de coubicaciones) a instancias de nube (o viceversa) usando una plataforma de terceros (por ejemplo, Rescale). Como parte de esa tarea, el Procesador tendrá acceso a los datos almacenados en las cargas de trabajo del Controlador a medida que los datos son descifrados para procesamiento en la plataforma de terceros. Esto puede incluir los datos personales del Controlador.
2.	Tipos de datos personales procesados	El tipo de datos personales procesados dependerá de los datos que haya almacenado el Controlador en las aplicaciones empresariales (incluidos los metadatos), la TI y la infraestructura de red, así como en los archivos no cifrados del Controlador que puedan estar incluidos en las solicitudes de servicio en la consola HOC y en cargas de trabajo del Controlador, y podrá incluir datos personales confidenciales. Por ejemplo, se incluyen, a título enunciativo, los siguientes: Nombre (propio y apellido), dirección, país, número de teléfono, dirección de correo electrónico, ID nacional, número de la seguridad social, permiso de conducir, datos de inmigración (n.º de pasaporte), fecha de nacimiento, edad, género, datos biométricos, condenas penales, discapacidades, información genética, información médica y posible información sanitaria protegida de EE. UU (HIPAA), religión, creencias filosóficas, orientación sexual, identificación y expresión de género, asociación profesional o sindicato, pertenencia a un comité de empresa, origen racial o étnico, opiniones políticas, dirección IP, ID de dispositivo, credenciales: contraseña, información de geolocalización, seguimiento, datos de análisis, cuenta bancaria, tarjeta de crédito, tarjeta de débito.
3.	Categorías de datos personales procesados	Cualquier sujeto de datos cuyos datos sean almacenados por el Controlador en las aplicaciones empresariales (incluidos los metadatos), la TI y la infraestructura de red, las cargas de trabajo y en los archivos adjuntos a las solicitudes de servicio en la consola HOC, incluidos, a título enunciativo, los clientes, usuarios finales, empleados, contratistas y trabajadores temporales del Controlador.
4.	Duración del procesamiento	El Procesador deberá procesar los datos personales del Controlador en el plazo de vigencia del Acuerdo o del documento de transacción aplicable. Dichos datos se eliminarán automáticamente a los 90 días de la finalización o rescisión del contrato de servicio del Controlador con el Procesador.
5.	Medidas técnicas y organizativas	El Procesador deberá mantener el programa de seguridad física y de la información para la protección de los datos personales del Controlador, tal y como se detalla en el siguiente Anexo III.

Anexo III: Medidas técnicas y organizativas, incluidas medidas técnicas y organizativas para garantizar la seguridad de los datos

1. Como parte del programa de seguridad física y de la información del Procesador para la protección de los datos personales del Controlador («Programa de seguridad del Procesador»), el Procesador realizará revisiones periódicas de las prácticas de seguridad, comparándolas con los estándares del sector, como NIST, ISO 27001 y SOC. El Procesador reevaluará y actualizará con regularidad su Programa de seguridad a medida que evolucione el sector, emerjan nuevas tecnologías o se identifiquen nuevas amenazas.

2. El Programa de seguridad del Procesador se compone, al menos, de lo siguiente:

   2.1 El Procesador mantiene estándares de seguridad física diseñados para prohibir el acceso físico no autorizado a las instalaciones y los equipos del Procesador utilizando las siguientes prácticas:

   - El acceso físico a las instalaciones se limita a los empleados, subcontratistas y visitantes autorizados del Procesador
   - A los empleados, subcontratistas y visitantes autorizados del Procesador se les brindan tarjetas de identificación que deben usar mientras se encuentran en las instalaciones
   - El acceso a las instalaciones del Procesador, incluidos el equipo y las áreas restringidos en las instalaciones, se monitorea continuamente
   - El acceso al centro de datos donde se alojan los datos personales del Controlador se registra, monitorea y rastrea; y
   - Los centros de datos se protegen con sistemas de alarma y cámaras de vídeo.

   2.2 El Procesador mantiene el control de acceso al entorno de TI relevante, de conformidad con las mejores prácticas del sector. Estos controles incluyen, a título enunciativo, requisitos en relación con los principios de privilegios mínimos, y la complejidad y el uso de contraseñas.

   2.3 La infraestructura del Procesador debe contar con versiones razonablemente actualizadas de los programas de software de seguridad de los sistemas, entre los que se pueden incluir cortafuegos de host, protección antivirus, así como parches y definiciones de virus actualizados. El Procesador mantiene registros de eventos relacionados con la infraestructura, incluidos los sistemas de detección de intrusiones, para monitorear, detectar y notificar patrones de uso inadecuado, actividades sospechosas, usuarios no autorizados y otros riesgos de seguridad.

3. A petición del Controlador, el Procesador revisará con este un resumen de las evaluaciones de vulnerabilidad. Durante las evaluaciones de vulnerabilidad, el Controlador no podrá ver ni acceder de ningún otro modo a los registros y/o procesos: (a) que no estén directamente relacionados con los servicios; (b) de modo que incumpla la legislación aplicable; y/o (c) de modo que se infrinjan las obligaciones de confidencialidad y seguridad del Procesador con un tercero.

4. Los empleados y contratistas han recibido formación sobre las políticas de privacidad y seguridad del Procesador y se les ha informado de sus responsabilidades en materia de seguridad y privacidad. Los empleados y contratistas del Procesador están obligados por contrato a mantener la confidencialidad de los datos personales del Controlador y a cumplir las políticas, normas o requisitos aplicables del Procesador en relación con el procesamiento de los datos personales del Controlador. El incumplimiento de estas políticas, normas o requisitos estará sujeto a investigación, que puede tener como resultado la adopción de medidas disciplinarias e incluir la rescisión del contrato laboral o de colaboración por parte del Procesador.

5. En caso de que el Procesador confirme una vulneración de la seguridad que haya provocado la destrucción, pérdida, alteración o revelación sin autorización de, o el acceso a, los datos personales del Controlador («Incidente de seguridad»), el Procesador actuará de la siguiente manera:

   5.1 Sin mayor demora, notificará al Controlador el Incidente de Seguridad. El Procesador deberá mantener informado en todo momento al Controlador sobre el estado del Incidente de Seguridad hasta que el asunto haya quedado resuelto. En los informes se incluirán, entre otros aspectos, una descripción del Incidente de seguridad, las acciones que se hayan tomado y los planes para la resolución del problema. Si el Controlador conoce de algún Incidente de Seguridad que vaya a afectar a los servicios, el Controlador deberá notificárselo inmediatamente al Procesador y facilitarle la información pertinente sobre el alcance del Incidente de Seguridad.

   5.2 A petición y cargo del Controlador: (i) ofrecer una asistencia razonable al Controlador en la notificación de cualquier vulneración de seguridad a la autoridad supervisora competente bajo las leyes de privacidad aplicables al Controlador; y (ii) ofrecer asistencia razonable al Controlador a la hora de comunicar cualquier filtración de datos a los sujetos de los datos en aquellos casos en los que la filtración tenga como resultado un alto riesgo para los derechos y libertades de los individuos.

Chat con Ventas

Hewlett Packard Enterprise

© Copyright 2023 Hewlett Packard Enterprise Development LP. La información que contiene este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de Hewlett Packard Enterprise figuran en las declaraciones expresas de garantía incluidas en los mismos. Nada de lo que aquí se indica debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se hará responsable de los errores u omisiones técnicos o editoriales que pudiera contener el presente documento.

a50009607ESE