HPE Managed HPC Cloud Bursting Services Anexo II e III

Anexo II: Descrição do tratamento

1.	Descrição do tratamento	Como parte do fornecimento do HPE Managed Services, o Subcontratante pode ter acesso aos dados armazenados nas aplicações comerciais do Responsável pelo tratamento (incluindo metadados), TI e infraestrutura de rede. Estes dados podem incluir dados pessoais do Responsável pelo tratamento. Além disso, o Subcontratante utiliza uma plataforma baseada em SaaS (ou seja, a HPE Hybrid Operations Console ("HOC") para operar e gerir os ativos de TI do Cliente. A HOC é utilizada para receber e seguir os pedidos de serviços de TI do Responsável pelo tratamento. O Responsável pelo tratamento pode optar por anexar um ficheiro, que pode ou não estar encriptado, ao pedido de serviço na HOC. Este ficheiro pode incluir dados pessoais do Responsável pelo tratamento. Especificamente no contexto do HPE Managed HPC Cloud Bursting Service, o Subcontratante executa trabalhos/programas que fornecem a transferência das cargas de trabalho do Cliente dos sistemas do Cliente (localizados no local ou em centros de dados de colocação) para instâncias de cloud (ou vice-versa) utilizando uma plataforma de terceiros (ou seja, Rescale). Como parte desta tarefa, o Subcontratante terá acesso aos dados armazenados nas cargas de trabalho do Responsável pelo tratamento, uma vez que os dados não são encriptados para tratamento na plataforma de terceiros. Estes dados podem incluir dados pessoais do Responsável pelo tratamento.
2.	Tipo de dados pessoais tratados	O tipo de dados pessoais tratados dependerá dos dados que o Responsável pelo tratamento tiver armazenado nas aplicações comerciais (incluindo metadados), nas TI e na infraestrutura de rede, bem como nos ficheiros não encriptados do Responsável pelo tratamento que possam ser anexados aos pedidos de serviço na HOC e cargas de trabalho do Responsável pelo tratamento, e pode incluir dados pessoais sensíveis. Como exemplos estão incluídos, entre outros: Nome (primeiro e último), endereço, país, número de telefone, endereço de e-mail, ID do cartão de cidadão, NSS, carta de condução, dados de imigração (n.º de passaporte), data de nascimento, idade, sexo, dados biométricos, condenações penais, deficiências, informações genéticas, informações de saúde e possíveis informações de saúde protegidas nos EUA (HIPAA), religião, crenças filosóficas, orientação sexual, identificação de género e expressão, dados profissionais/sindicais, filiação do conselho de trabalhadores, origem racial ou étnica, opiniões políticas, endereço IP, ID do dispositivo, credenciais — palavra-passe, informações de geolocalização, seguimento, dados analíticos, conta bancária, cartão de crédito, cartão de débito.
3.	Categorias de dados pessoais tratados	Qualquer pessoa cujos dados pessoais sejam armazenados pelo Responsável pelo tratamento nas aplicações comerciais (incluindo metadados), TI e infraestrutura de rede, cargas de trabalho e nos ficheiros anexados aos pedidos de serviço na HOC, incluindo, sem limitação, os clientes do Responsável pelo tratamento, utilizadores finais, funcionários, adjudicatários e trabalhadores temporários.
4.	Duração do tratamento	O Subcontratante tratará os dados pessoais do Responsável pelo tratamento durante o período de vigência do Acordo e/ou de qualquer documento de transação aplicável. Esses dados serão automaticamente eliminados 90 dias após o termo ou rescisão do contrato de prestação de serviços do Responsável pelo tratamento com o Subcontratante.
5.	Medidas técnicas e de organização	O Subcontratante manterá o programa de segurança física e da informação para a proteção dos dados pessoais do Responsável pelo tratamento, tal como especificado no Anexo III, em baixo.

Anexo III: Medidas técnicas e organizacionais, incluindo medidas técnicas e organizacionais para garantir a segurança dos dados

1. Como parte do programa de segurança física e de informação do Subcontratante para a proteção dos dados pessoais do Responsável pelo tratamento ("Programa de Segurança do Subcontratante"), o Subcontratante efetua revisões periódicas das práticas de segurança em relação às normas da indústria, tais como NIST, ISO 27001 e SOC. O Subcontratante reavalia e atualiza regularmente o Programa de Segurança do Responsável pelo tratamento à medida que a indústria evolui, surgem novas tecnologias ou são identificadas novas ameaças.

2. O Programa de Segurança do Subcontratante consiste no seguinte:

   2.1 O Subcontratante mantém padrões de segurança física concebidos para proibir o acesso físico não autorizado às instalações e equipamentos do Responsável pelo tratamento, utilizando as seguintes práticas:

   - O acesso físico às localizações é limitado aos funcionários do Subcontratante, fornecedores subcontratados e visitantes autorizados
   - Os funcionários do Subcontratante, fornecedores subcontratados e visitantes autorizados recebem cartões de identificação que devem ser usados quando se encontram nas instalações
   - Monitorização do acesso às instalações do Subcontratante, incluindo áreas restritas e equipamento dentro das instalações
   - O acesso ao data center onde os dados pessoais do Responsável pelo tratamento estão alojados é registado, monitorizado e seguido; e
   - Os centros de dados estão protegidos com sistemas de alarme e câmaras de vídeo.

   2.2 O Subcontratante mantém o controlo de acesso ao ambiente de TI relevante em conformidade com as melhores práticas da indústria. Estes controlos incluem, mas não se limitam a, requisitos relativos aos princípios do menor privilégio e da complexidade e utilização da palavra-passe.

   2.3 A infraestrutura do Subcontratante tem versões razoavelmente atualizadas do software de segurança do sistema, que podem incluir uma firewall do anfitrião, proteção antivírus e correções e definições de vírus atualizadas. O Subcontratante mantém registos de eventos que envolvem a infraestrutura, incluindo sistemas de deteção de intrusão para monitorizar, detetar e comunicar padrões de utilização indevida, atividades suspeitas, utilizadores não autorizados e outros riscos de segurança.

3. Mediante pedido, o Subcontratante analisará com o Responsável pelo tratamento um resumo das avaliações de vulnerabilidade. As avaliações de vulnerabilidade não conferem ao Responsável pelo tratamento o direito de visualizar ou, de qualquer forma, aceder a registos e/ou processos: (a) não diretamente relacionados com os serviços; (b) que violem a legislação aplicável; e/ou (c) que violem as obrigações de confidencialidade e segurança do Responsável pelo tratamento perante terceiros.

4. Os funcionários e adjudicatários recebem formação sobre as políticas de privacidade e segurança do Subcontratante e são informados das suas responsabilidades relativamente às práticas de privacidade e segurança. Os funcionários e adjudicatários do Subcontratante estão contratualmente obrigados a manter a confidencialidade dos dados pessoais do Responsável pelo tratamento e a cumprir as políticas, normas ou requisitos aplicáveis do Subcontratante relativamente ao tratamento dos dados pessoais do Responsável pelo tratamento. O não cumprimento destas políticas, normas ou requisitos será objeto de investigação, que poderá resultar em medidas disciplinares, até e incluindo a cessação do emprego ou do contrato por parte do Subcontratante.

5. Caso o Subcontratante confirme uma violação de segurança que leve à destruição acidental ou ilegal, perda, alteração ou divulgação não autorizada de, ou acesso a, dados pessoais do Responsável pelo tratamento ("Incidente de Segurança"), o Subcontratante irá:

   5.1 Notificar, sem demora injustificada, o Responsável pelo tratamento do Incidente de Segurança. O Subcontratante fornecerá ao Responsável pelo tratamento atualizações sobre o estado do Incidente de Segurança até que o assunto tenha sido resolvido. Os relatórios incluirão, entre outros, uma descrição do Incidente de Segurança, as medidas tomadas e os planos de correção. Se o Responsável pelo tratamento tomar conhecimento de um Incidente de Segurança que afete os serviços, o Responsável pelo Tratamento notificará imediatamente o Subcontratante desse facto e informá-lo-á do âmbito do Incidente de Segurança.

   5.2 A pedido e a expensas do Responsável pelo tratamento, (i) prestar assistência razoável ao Responsável pelo tratamento na notificação de uma violação da segurança à autoridade de controlo competente nos termos da legislação em matéria de proteção da privacidade aplicável ao Responsável pelo tratamento; e (ii) prestar assistência razoável ao Responsável pelo tratamento na comunicação de uma violação de dados às pessoas em causa, nos casos em que a violação de dados seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas.

Converse agora (vendas)

Hewlett Packard Enterprise

© Copyright 2023 Hewlett Packard Enterprise Development LP. A informação aqui incluída está sujeita a alteração sem aviso prévio. As únicas garantias para os produtos e serviços da Hewlett Packard Enterprise estão definidas nas declarações de garantia expressa que acompanham esses produtos e serviços. Nada do que aqui está contido deve ser interpretado como constituindo uma garantia adicional. A Hewlett Packard Enterprise não poderá ser responsabilizada por erros técnicos ou editoriais, ou por omissões neste documento.

a50009607PTE