Aprovisionamento Microsoft

Guia do Programa Supplier Security & Privacy Assurance (SSPA)

Versão 8

Junho de 2022

Introdução

Na Microsoft, acreditamos que a privacidade é um direito fundamental. Tendo por casa a nossa missão de encorajar cada indivíduo e organização do planeta a chegar mais longe, esforçamo-nos para conquistar e preservar a confiança dos nossos clientes todos os dias.

Fortes práticas de privacidade e segurança são críticas para a nossa missão, essenciais para a confiança do cliente e, em várias jurisdições, exigidas pela lei. Os padrões capturados nas políticas de privacidade e segurança da Microsoft refletem os nossos valores enquanto empresa e estendem-se aos nossos fornecedores (como, por exemplo, a sua empresa) que Processam dados da Microsoft em nosso nome.

O Programa Supplier Security and Privacy Assurance ("**SSPA**") é o programa empresarial da Microsoft implementado com vista ao fornecimento de instruções de processamento de dados básicas da Microsoft aos nossos fornecedores, na forma dos Requisitos de Proteção de Dados dos Fornecedores da Microsoft ("**RPD**"), disponível na página sobre o SSPA em Microsoft.com/Procurement. Tenha em atenção que os fornecedores podem ter de cumprir requisitos a nível organizacional adicionais que são decididos e comunicados fora do SSPA pelo grupo Microsoft responsável pelo envolvimento com o fornecedor.

Os termos SSPA principais encontram-se definidos nos RPD. Para saber mais sobre o programa, leia as nossas Perguntas Frequentes (FAQ) e fale com a nossa equipa global, por escrito, através do endereço de correio eletrónico SSPAHelp@microsoft.com.

Descrição Geral do Programa SSPA

O SSPA é uma parceria entre o Aprovisionamento Microsoft, os Assuntos Empresariais Externos e Legais e a Segurança Empresarial para assegurar que os princípios de privacidade e segurança são seguidos pelos nossos fornecedores.

O âmbito do SSPA abrange todos os fornecedores a nível global que Processam Dados Pessoais e/ou Dados Confidenciais da Microsoft em ligação com o desempenho desse fornecedor (por exemplo, prestação de serviços, licenças de software, serviços cloud), de acordo com os termos do contrato com a Microsoft (por exemplo, termos de Nota de Encomenda, contrato principal) ("**Realização,**" "**Rendimento**" ou "**Desempenho**").

O SSPA permite ao fornecedor fazer as escolhas de processamento de dados mais alinhadas com os bens e/ou serviços que foi contratado para Realizar. Estas seleções acionam requisitos correspondentes para fornecer garantias de conformidade à Microsoft.

Todos os fornecedores inscritos irão preencher, anualmente, um autoatestado de conformidade com os RPD.. O seu perfil de processamento de dados determina se os RPD completos forem emitidos ou se se aplicar um subconjunto de requisitos. Os fornecedores que processem dados que a Microsoft considera de maior risco também poderão ter de cumprir requisitos adicionais, por

exemplo, facultar uma verificação de conformidade independente. Os fornecedores que também constem de uma lista publicada de Subprocessadores Microsoft será pedido que facultem uma verificação de conformidade independente.

Importante: As atividades de conformidade determinam se o estado SSPA é Verde (em conformidade) ou Vermelho (sem conformidade). As ferramentas de compra da Microsoft confirmam se o estado SSPA é Verde (no caso de todos os fornecedores dentro do âmbito do programa SSPA) antes de autorizarem a realização de qualquer envolvimento.

Diagrama do Processo SSPA – Inscrição de Novo Fornecedor

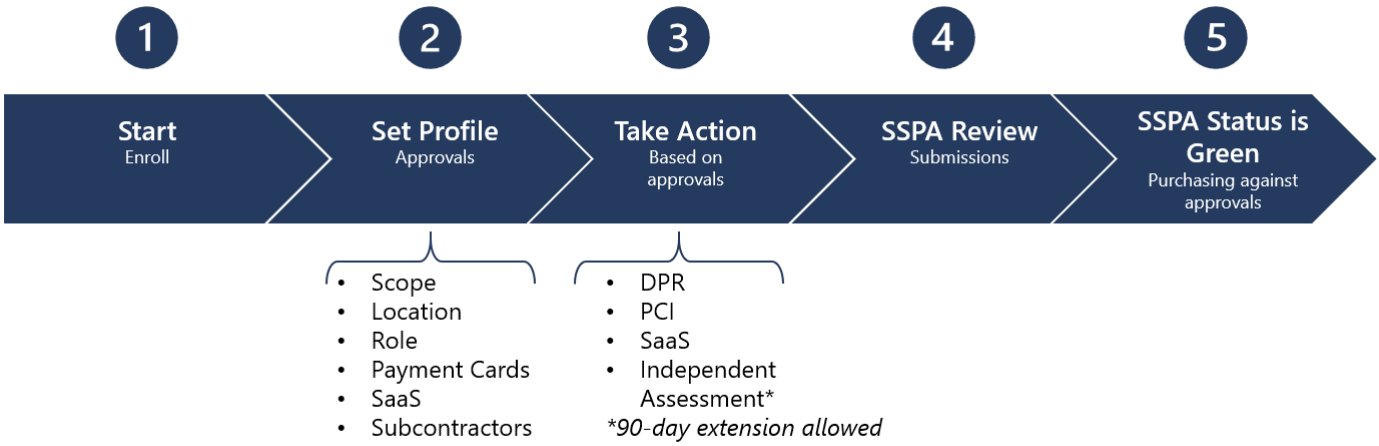
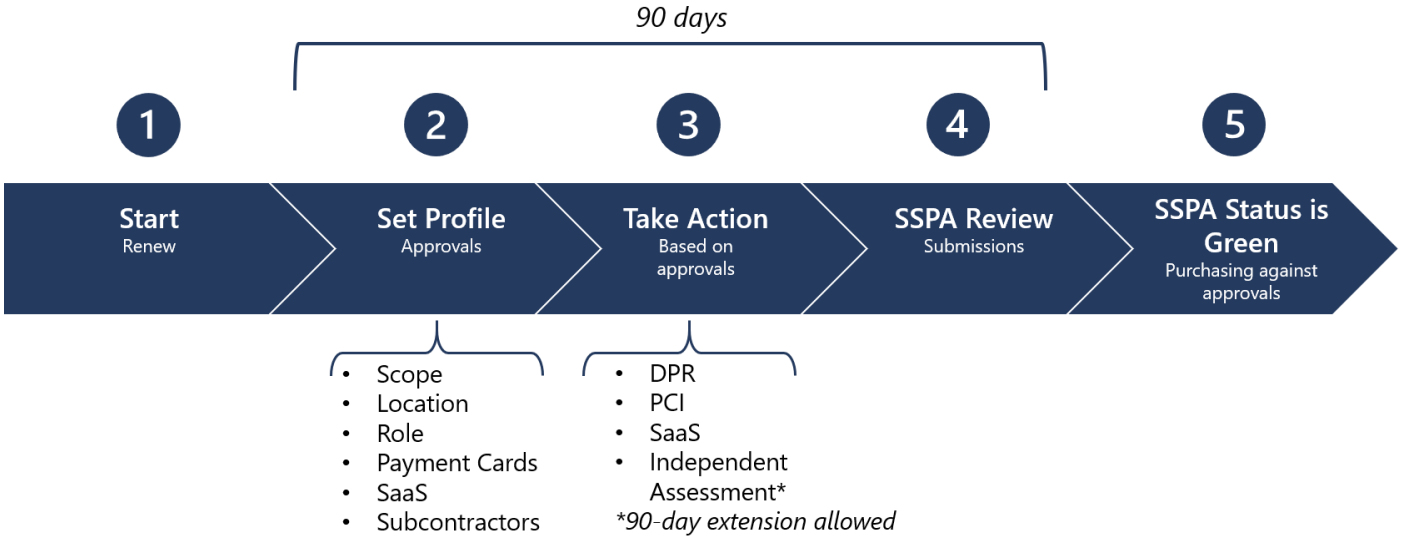


Diagrama do Processo SSPA – Renovação Anual de Fornecedor



Âmbito SSPA

Para ajudar a determinar se, na qualidade de fornecedor, Processa Dados Pessoais e/ou Dados Confidenciais da Microsoft, consulte a lista de exemplos nas tabelas abaixo. Note que estes são exemplos e não uma lista exaustiva.
Nota: um empresário Microsoft poderá solicitar uma inscrição fora desta lista tendo em conta a natureza confidencial dos dados processados.

Dados Pessoais por Tipo de Dados

Os exemplos incluem, entre outros:

Dados Confidenciais
Dados relacionados com filhos
Dados genéticos, Dados biométricos ou Dados de saúde
Origem racial ou étnica
Afiliações, opiniões e crenças Filosóficas, Religiosas ou Políticas
Filiação em sindicato
Vida sexual ou orientação sexual de uma pessoa
Estatuto de imigração (visto, autorização de trabalho, etc.)
Identificação pessoal (passaporte, carta de condução, visto, números da segurança social, números de identificação nacional)
Dados precisos de localização do utilizador (até 300 metros)
Números de contas bancárias pessoais
Número de cartão de crédito e data de expiração
Dados de Conteúdos de Cliente
Documentos, fotografias, vídeos, música, etc.
Críticas e/ou avaliações submetidas para um produto ou serviço
Respostas a inquéritos
Histórico de navegação, interesses e favoritos
Utilização de tinta digital, escrita e emissão de voz (voz/áudio e/ou chat/bot)
Dados de credenciais (palavras-passe, sugestões para palavra-passe, nome de utilizador, dados biométricos utilizados para identificação)
Dados do cliente associados a um processo de suporte

Dados Capturados e Gerados
Dados de localização imprecisos
Endereço IP
Preferências de dispositivo e personalização
Utilização de serviço para sites, controlo de cliques de página Web
Dados de redes sociais, relações gráficas sociais
Dados de atividade de dispositivos ligados, como monitores de fitness
Dados de contacto como nome, endereço, número de telefone, endereço de e-mail, data de nascimento, contactos de dependentes e de emergência
Avaliação de fraude e risco, verificação de historial
Seguros, pensão, dados de benefícios
Currículos de candidatura, notas de entrevista/comentários
Metadata and telemetry
Dados de Conta
Dados de instrumento de pagamento
Número de cartão de crédito e data de expiração
Informação de identificação bancária
Número de conta bancária
Pedidos de crédito ou linha de crédito
Documentos e identificadores fiscais
Dados de despesas ou investimento
Cartões empresariais
Dados Pseudonimizados de Utilizador Final (EUPI) (Identificadores criados pela Microsoft para identificar utilizadores de serviços e produtos Microsoft)
Identificador Exclusivo Global (GUID)
ID de Passaporte de Utilizador ou Identificador Exclusivo (PUID)
Informações Identificáveis de Utilizador Final com Hash (EUII)
IDs de sessão
IDs de dispositivo
Dados de diagnóstico
Dados de registo

Online Customer Data
Microsoft online enterprise customer (example: Azure tenant, M365 tenant…)
Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …)
Microsoft enterprise customer (on premises customer)
Support data (example: Customer originates a ticket)
Account data (example: billing data, e-commerce)
Survey/Event Registration/Training

Dados Confidenciais da Microsoft por Classe de Dados

Os exemplos incluem, entre outros:

Altamente Confidencial
Informações relativas ou relacionadas com o desenvolvimento, teste ou desenvolvimento de Produtos Microsoft ou componentes de Produtos Microsoft *O software, os serviços online ou o hardware Microsoft vendidos comercialmente em qualquer canal são considerados "**Produto Microsoft**"*
Informação de marketing de pré-lançamento de dispositivos Microsoft
Dados financeiros empresariais da Microsoft não anunciados sujeitos às regras SEC
Confidencial
Chaves de licença de produtos Microsoft em nome da Microsoft para distribuição através de qualquer método
Informações relativas ou relacionadas com o desenvolvimento ou teste de aplicações de Linha de Negócio (LOB) internas da Microsoft
Materiais de marketing de pré-lançamento da Microsoft para software e serviços Microsoft, como o Office, o SQL, o Azure, etc.
Documentação escrita, de design, eletrónica ou impressa para quaisquer serviços ou produtos Microsoft, por exemplo, dispositivos (guias de processos ou procedimentos, dados de configuração, etc.)

Importante: Um empresário Microsoft pode solicitar a participação para dados não incluídos nesta lista.

Perfil de Processamento de Dados

Os fornecedores da Microsoft têm total controlo sobre o seu perfil de processamento de dados SSPA.

Isto permite aos fornecedores decidir quais os envolvimentos para os quais pretendem ser elegíveis a Realizar. Preste especial atenção às seleções e considere as atividades de conformidade que têm de ser levadas a cabo para aprovação. **Veja a Secção "Requisitos de Garantia" abaixo e no Anexo A**.

Os grupos de negócios Microsoft só poderão criar envolvimentos com fornecedores nos casos em que a atividade de processamento de dados corresponda às aprovações que o fornecedor obteve.

Os fornecedores poderão atualizar o seu perfil de processamento de dados em qualquer altura do ano **se não houver tarefas abertas**. Quando for efetuada uma alteração, a atividade correspondente será emitida e terá de ser concluída antes de garantir as aprovações. As aprovações existentes concluídas serão aplicadas até serem concluídos requisitos recém-emitidos.

Se as tarefas recém-executadas não forem concluídas dentro do período permitido de 90 dias, o

estado SSPA ficará a VERMELHO (sem conformidade) e a conta estará em risco de ser desativada dos sistemas de Faturas a Pagamento da Microsoft

Aprovações de Processamento de Dados	
1	Âmbito de Processamento de Dados ▪ Confidencial ▪ Pessoal, Confidencial
2	Localização de Processamento de Dados ▪ Na Microsoft ou no Cliente ▪ No Fornecedor
3	Função de Processamento de Dados ▪ Controlador (Controlador Independente ou Conjunto) ▪ Processador ▪ Subprocessador (Designado pela Microsoft)
4	Processamento de Cartões de Pagamento ▪ Sim ▪ Não Aplicável
5	Software como Serviço ▪ Sim ▪ Não Aplicável
6	Utilização de Subcontratantes ▪ Sim ▪ Não Aplicável

Considerações de Aprovação

Âmbito de Processamento de Dados

Confidencial

Selecione esta aprovação se o Desempenho do fornecedor envolver o Processamento de apenas Dados Confidenciais da Microsoft.

Se selecionar esta aprovação, não será elegível para envolvimentos de processamento de Dados Pessoais.

Pessoal, Confidencial

Selecione esta aprovação se o Desempenho do fornecedor envolver o Processamento de Dados Pessoais e Dados Confidenciais da Microsoft.

Localização de Processamento

Na Microsoft ou no Cliente

Selecione esta aprovação se o Desempenho do fornecedor envolver o Processamento de dados da parte do fornecedor dentro do ambiente da rede Microsoft, em que os membros da equipa utilizem credenciais de acesso *@microsoft.com*, ou dentro do ambiente de um cliente da Microsoft.

Não selecione esta opção nas seguintes circunstâncias:

- O fornecedor gere uma instalação offshore (OF) designada pela Microsoft.
- O fornecedor fornece os recursos à Microsoft e trabalha periodicamente dentro e fora da rede Microsoft. A localização de processamento do trabalho fora da rede é considerada "no fornecedor".

No Fornecedor
Se a condição "Na Microsoft ou no Cliente" (conforme descrito acima) não se aplicar, selecione esta opção.

_____

Função de Processamento de Dados

Controlador (abrange controladores independentes e conjuntos)

Selecione esta aprovação se **todos** os aspetos do Desempenho pelo fornecedor cumprirem a definição de função de processamento de dados de Controlador (ver os RPD).

Se selecionar esta aprovação, não será elegível para processamento de Dados Pessoais com a designação de função de "Processador". Se um fornecedor for um Processador e um Controlador da Microsoft, não selecione "Controlador"; selecione "Processador".

Processador

Esta é a função de processamento mais comum quando os fornecedores processam dados em nome da Microsoft. Reveja as definições de Processador nos RPD.

Subprocessador

Um Subprocessador é um terceiro perante o qual a Microsoft se compromete a Realizar, onde o Desempenho inclui o Processamento de Dados Pessoais da Microsoft para o qual a Microsoft é um Processador. Os fornecedores não podem autoidentificar-se como Subprocessadores na Microsoft, uma vez que isto requer a pré-aprovação por equipas internas de Privacidade. Os fornecedores só podem ser Subprocessadores quando a Microsoft é o Processador de Dados e o fornecedor Processa os Dados Pessoais qualificados da Empresa. Os subprocessadores terão requisitos adicionais de contrato e de conformidade, incluindo uma Adenda de Proteção de Dados e uma Avaliação Independente (ver abaixo).

Processamento de Cartões de Pagamento

Selecione esta aprovação se qualquer parte dos dados Processados pelo fornecedor incluir dados para suportar o processamento de cartões de crédito ou outros cartões de pagamento em nome da Microsoft.

Esta aprovação permite a um fornecedor participar em envolvimentos de processamento de cartões de pagamento.

_____

Software

O Aprovisionamento Microsoft orienta os Compradores através de um processo de entrada para todas as compras de software, o que inclui várias verificações incluindo a triagem SSPA para decidir se o fornecedor que fornece o software está dentro do âmbito da gestão SSPA. (Os Compradores da Microsoft podem consultar os passos delineados na página interna Software ProcureWeb e Serviço Cloud para obter mais informações). Caso seja necessário SSPA, os fornecedores podem também ter de identificar que se aplica a escolha do perfil "Software como Serviço" (SaaS). Para fornecedores inscritos no programa SSPA, isto pode ser feito ao completar o Perfil de Processamento de Dados no Portal de Conformidade de Fornecedores da Microsoft.

Para efeitos de conformidade com o programa SSPA, ver o SaaS de uma forma geral para incluir também a plataforma como serviço (PaaS) e a infraestrutura como serviço (IaaS). (Para saber mais sobre o SaaS, ver esta explicação.)

Software como Serviço(SaaS)

O Software como Serviço (SaaS) permite que os utilizadores se liguem e utilizem aplicações baseadas na cloud através da Internet.

A Microsoft define **Software como Serviço (SaaS)** como um software baseado num código comum utilizado num modelo "um para muitos" numa base de pagamento por utilização ou como uma subscrição baseada em indicadores de utilização O fornecedor de serviços na cloud desenvolve e mantém software baseado na cloud, fornece atualizações automáticas de software e disponibiliza software aos seus clientes através da Internet, numa base de um para muitos e com pagamento à medida que se vai utilizando. Este método de entrega e licenciamento de software permite o acesso online ao software através de uma subscrição em vez de ser comprado e instalado em cada computador individual.

Nota: A maioria dos fornecedores SaaS terá de adicionar a aprovação do Subcontratante no Supplier Compliance Portal da Microsoft se os Dados Pessoais ou os Dados Confidenciais da Microsoft estiverem alojados numa plataforma de terceiros.

Utilização de Subcontratantes

Selecione esta aprovação se o fornecedor utilizar Subcontratantes para Realizar (consulte as definições nos RPD).

Isto inclui também os Freelancers (ver os RPD).

Requisitos de Garantia

Requisitos com base nas Aprovações de Perfil

As aprovações selecionadas no seu Perfil de Processamento de Dados auxiliam o SSPA na avaliação do nível de risco de envolvimento(s) da Microsoft. Os requisitos de conformidade SSPA diferem com base no Perfil de Processamento de Dados e aprovações associadas. Esta secção explica os diferentes requisitos SSPA.

Existem também combinações que podem aumentar ou reduzir os requisitos de conformidade. As combinações estão reunidas no Anexo A e isto é o que pode esperar executar a partir do Supplier Compliance Portal da Microsoft quando concluir o seu perfil. Pode sempre validar a forma como o seu cenário se encaixa nesta estrutura ao pedir uma revisão de equipa do SSPA.

Ação: localize o seu perfil de aprovação no Anexo A e reveja os requisitos de garantia e opções de Garantia Independente correspondentes, se aplicáveis.

Importante: Se o seu perfil inclui Software como Serviço (SaaS), Subcontratantes, alojamento de sites ou cartões de pagamento, será necessária uma garantia adicional.

Autoatestado com os RPD

Todos os fornecedores inscritos no programa SSPA terão de efetuar um autoatestado de conformidade com os RPD dentro de 90 dias após receção do pedido. Este pedido será feito anualmente, mas poderá ser mais frequente se o perfil de processamento de dados for atualizado a meio do ano. As contas de fornecedores mudarão para um estado SSPA de Vermelho (sem conformidade) se o período de 90 dias for excedido. As novas ordens de compra dentro do âmbito não podem ser processadas antes de o estado SSPA ficar Verde (em conformidade).

Os fornecedores recentemente inscritos terão de cumprir os requisitos para garantir um estado SSPA de Verde (em conformidade) antes de os envolvimentos poderem começar.

Importante: A equipa SSPA não está autorizada a providenciar extensões para esta tarefa.

Os representantes autorizados que concluírem o autoatestado deverão garantir que têm informações suficientes de especialistas na matéria para responderem com confiança a cada requisito. Para além disso, ao adicionar o respetivo nome a um formulário SSPA, estão a certificar que leram e compreenderam os RPD. Os fornecedores podem sempre adicionar outros contactos à ferramenta online para auxiliar na conclusão dos requisitos.

O Representante Autorizado (ver definição nos RPD) deve:

1. Determinar os requisitos aplicáveis.
2. Publicar uma resposta para cada requisito aplicável.
3. Assinar e enviar o atestado através do Supplier Compliance Portal da Microsoft.

Aplicabilidade

É esperado que os fornecedores respondam a todos os requisitos aplicáveis dos RPD emitidos segundo o Perfil de Processamento de Dados. É esperado que, dentro dos requisitos emitidos, alguns não se apliquem aos bens ou serviços que o fornecedor fornece à Microsoft. Podem ser marcados como "não aplicável" com um comentário detalhado para os revisores SSPA validarem.

As submissões RPD são revistas pela equipa SSPA para verificação de seleções de "não aplicável", "conflito jurídico local" ou "conflito contratual" face aos requisitos emitidos. A equipa SSPA poderá pedir esclarecimento sobre uma ou mais seleções. Conflitos contratuais e jurídicos locais só serão aceites se as referências de apoio forem facultadas e o conflito for claro.

Requisito de Avaliação Independente

Consulte os Requisitos por Aprovações no Anexo A para ver as aprovações de processamento de dados que acionam este requisito.

Os fornecedores têm a opção de alterar as aprovações ao atualizar o respetivo Perfil de Processamento de Dados. Contudo, se o fornecedor tiver uma função de Processamento de Dados de "Subprocessador", o fornecedor não pode alterar esta aprovação e será obrigado a ter uma Avaliação Independente realizada anualmente.

Para garantir as aprovações que requerem uma verificação de conformidade independente, os fornecedores terão de selecionar um assessor independente para validar a conformidade com os RPD. O assessor deve preparar uma carta de consultoria para fornecer garantias de conformidade à Microsoft. Esta carta deve ser não qualificada e todos os problemas de não conformidade deverão ser resolvidos e remediados antes da carta de confirmação ser submetida ao Supplier Compliance Portal da Microsoft para revisão da equipa SSPA. Os assessores podem descarregar um modelo de carta de consultoria aprovado, que está anexado ao PDF "Assessores Preferenciais" disponível aqui.

O **Anexo A** inclui alternativas de certificação aceitáveis se optar por não utilizar um assessor independente para confirmar a conformidade com os RPD (quando aplicável, por exemplo, para fornecedores de SaaS, fornecedores de alojamento de sites ou fornecedores com Subcontratantes). As normas ISO 27701 (privacidade) e ISO 27001 (segurança) são utilizadas para proporcionar um mapeamento próximo para os RPD.

Se o Fornecedor for um prestador de cuidados de saúde nos Estados Unidos ou entidade coberta, aceitaremos um relatório HITRUST para cobertura de privacidade e segurança.

O SSPA pode executar uma avaliação independente manualmente se houver circunstâncias para além dos acionadores padrão que mereçam diligências devidas adicionais. Os exemplos incluem um pedido da divisão de privacidade ou segurança; validação de remediação de incidente de dados; requisito de execução automatizada de direitos do requerente dos dados.

Orientações sobre como abordar este requisito:

1. O envolvimento tem de ser realizado por um assessor com formação técnica suficiente e conhecimentos da matéria que permitam uma avaliação adequada da conformidade.
2. Os assessores terão de estar inscritos na International Federation of Accountants (IFAC, Federação Internacional de Contabilistas) ou no American Institute of Certified Public Accountants (AICPA, Instituto Americano de Revisores Oficiais de Contas) ou terão de estar certificados por outras entidades de segurança e privacidade relevantes, como a International Association of Privacy Professionals (IAPP, Associação Internacional de Profissionais de Privacidade) ou a Information Systems Audit and Control Association (ISACA, Associação de Controlo e Auditoria de Sistemas de Informação).
3. O assessor tem de utilizar os RPD mais recentes e estes incluem as provas necessárias para validar cada requisito. **Os fornecedores terão de fornecer as suas respostas aprovadas mais recentemente de atestado dos RPD ao assessor.**
4. No que respeita aos fornecedores recentemente inscritos, o assessor irá testar a estrutura dos controlos do processo. Em todos os restantes casos, o assessor irá testar a eficácia dos controlos.
5. O âmbito do envolvimento de avaliação está limitado aos Dados Pessoais da Microsoft e/ou Dados Confidenciais da Microsoft em ligação com o Desempenho desse fornecedor.
6. O âmbito do envolvimento está limitado a todas as atividades de processamento de dados dentro do âmbito executadas no número de conta de fornecedor que recebeu o pedido. Se o fornecedor selecionar mais de uma conta de fornecedor em simultâneo, a **carta de atestado terá de incluir a lista de contas de fornecedores incluídas na avaliação e endereços associados.**
7. A carta submetida ao SSPA não pode incluir declarações de que o fornecedor não pode cumprir os Requisitos de Proteção de Dados indicados Estes problemas têm de ser corrigidos antes da submissão da carta.

O SSPA disponibilizou uma lista de assessores preferenciais. Estas empresas estão familiarizadas com a realização de avaliações SSPA. Os fornecedores terão de pagar esta avaliação e os custos variam conforme a escala e o âmbito do processamento de dados.

Requisito de certificação do PCI DSS

O Padrão de Segurança de Dados de Cartões de Pagamento (PCI DSS) é uma estrutura para desenvolver uma segurança de dados de cartões de pagamento robusta que inclui prevenção, deteção e reação adequadas a incidentes de segurança. A estrutura foi desenvolvida pelo PCI Security Standards Council, uma organização da indústria autorreguladora. O objetivo dos requisitos do PCI DSS é identificar as vulnerabilidades de tecnologia e processos que colocam riscos à segurança dos dados do titular do cartão que são processados.

A Microsoft tem de cumprir estes padrões. Se um fornecedor processar informação de cartão de pagamento em nome da Microsoft, requeremos um comprovativo do cumprimento destes padrões. Consulte o PCI Security standards council para compreender os requisitos definidos pela organização PCI.

Consoante o volume de transações processadas, será pedido ao fornecedor que tenha um Assessor de Segurança Qualificado que certifique a conformidade ou que possa preencher um formulário de autoavaliação.

As marcas de cartão de pagamento definem os limiares para o tipo de avaliação, normalmente:

- Nível 1: providencie uma certificação do PCI DSS de Assessor de Terceiros
- Nível 2 ou 3: providencie um Questionário de Autoavaliação do PCI DSS (SAQ) assinado por um representante do fornecedor.

Submeta a certificação aplicável e que cumpre os requisitos de PCI.

Requisito de Software como Serviço

Os fornecedores que cumprem a definição SaaS incluída no Perfil de Processamento de Dados podem ser obrigados a fornecer uma certificação ISO 27001 válida, se tal for exigido no Acordo de Serviços da Microsoft Cloud.

Os revisores da SSPA irão validar se a sua apresentação cumpre a obrigação contratual.

Não submeta uma certificação do centro de dados. Esperamos que a certificação ISO 27001 se aplique ao(s) serviço(s) de software registado(s) no seu contrato com a Microsoft.

Utilização de Subcontratantes

A Microsoft considera a utilização de subcontratantes um fator de elevado risco. Os fornecedores que utilizam subcontratantes que irão processar os Dados Pessoais e/ou Confidenciais da Microsoft devem divulgar esses subcontratantes. Além disso, o fornecedor deve também divulgar os países onde esses dados pessoais serão processados por cada subcontratante.

Incidentes de dados

Se um fornecedor tomar conhecimento de um incidente relacionado com a privacidade ou dados de segurança, os fornecedores devem informar a Microsoft, conforme detalhado nos RPD. O fornecedor deve informar a Microsoft conforme detalhado e definido nos RPD.

Comunicar um incidente de dados através do SupplierWeb ou por e-mail SuppIR@microsoft.com

Não se esqueça de incluir:

- Data do incidente de dados:
- Nome do fornecedor:
- Número do fornecedor:
- Contacto(s) notificado(s) da Microsoft:
- PO associado, se aplicável/disponível:
- Resumo do incidente de dados:

Anexo A

Requisitos com base nas Aprovações de Perfil

#	Perfil	Requisitos de Garantia	Opções de Garantia Independente
1	**Âmbito**: Pessoal, Confidencial **Localização de Processamento:** Na Microsoft ou no Cliente **Função de Processamento:** Processador ou Controlador **Classe de Dados:** Confidencial **ou** Altamente Confidencial **Cartões de Pagamento:** Não Aplicável **SaaS:** Não Aplicável **Utilização de Subcontratantes:** Não Aplicável **Alojamentos de Sites:** Não Aplicável	Autoatestado de conformidade com os RPD	
2	**Âmbito:** Confidencial **Localização de Processamento:** No Fornecedor **Função de Processamento:** N/A **Classe de Dados:** Confidencial **Cartões de Pagamento:** Não Aplicável **SaaS:** Não Aplicável **Utilização de Subcontratantes:** Não Aplicável **Alojamentos de Sites:** Não Aplicável	Autoatestado de conformidade com os RPD	
3	**Âmbito**: Confidencial **Localização de Processamento:** No Fornecedor **Função de Processamento:** Processador **Classe de Dados:** Altamente Confidencial **Cartões de Pagamento:** Não Aplicável **SaaS:** Não Aplicável **Utilização de Subcontratantes:** Não Aplicável **Alojamentos de Sites:** Não Aplicável	Autoatestado de conformidade com os RPD **e** Garantia Independente de conformidade	Opções de Garantia Independente: 1. Concluir uma Avaliação Independente segundo os RPD **ou** 2. Submeter ISO 27001

#	Perfil	Requisitos de Garantia	Opções de Garantia Independente
4	**Âmbito:** Pessoal, Confidencial **Localização de Processamento:** No Fornecedor **Função de Processamento:** Processador **Classe de Dados:** Altamente Confidencial **Cartões de Pagamento:** Não Aplicável **SaaS:** Não Aplicável **Utilização de Subcontratantes:** Não Aplicável **Alojamentos de Sites:** Não Aplicável	Autoatestado de conformidade com os RPD **e** Garantia Independente de conformidade	Opções de Garantia Independente: 1. Concluir uma Avaliação Independente segundo os RPD, 2. Avaliação Independente segundos as secções A-I dos RPD e ISO 27001, **ou** 3. Submeter ISO 27701 **e** ISO 27001
5	**Âmbito:** Pessoal, Confidencial **Localização de Processamento:** No Fornecedor **Função de Processamento:** Processador **Classe de Dados:** Confidencial **Cartões de Pagamento:** Não Aplicável **SaaS:** Não Aplicável **Utilização de Subcontratantes:** Não Aplicável **Alojamentos de Sites:** Não Aplicável	Autoatestado de conformidade com os RPD	
6	**Âmbito:** Pessoal, Confidencial **Localização de Processamento:** No Fornecedor **Função de Processamento:** Controlador **Classe de Dados:** Altamente Confidencial ou Confidencial **Cartões de Pagamento:** Não Aplicável **SaaS:** Não Aplicável **Utilização de Subcontratantes:** Não Aplicável **Alojamentos de Sites:** Não Aplicável	Autoatestado de conformidade com os RPD	

#	Perfil	Requisitos de Garantia	Opções de Garantia Independente
7	**Âmbito:** Pessoal, Confidencial **Localização de Processamento:** Qualquer **Função de Processamento:** Subprocessador (Esta função é determinado pela Microsoft - o perfil indicará "Aprovação de Subprocessador: Sim") **Classe de Dados:** Altamente Confidencial ou Confidencial **Cartões de Pagamento:** Não Aplicável **SaaS:** Não Aplicável **Utilização de Subcontratantes:** Não Aplicável **Alojamentos de Sites:** Não Aplicável	Autoatestado de conformidade com os RPD **e** Garantia Independente de conformidade	Opções de Garantia Independente: 1. Concluir uma Avaliação Independente segundo os RPD, 2. Avaliação Independente segundos as secções A-I dos RPD e ISO 27001, **ou** 3. Submeter ISO 27701 **e** ISO 27001

#	Perfil	Requisitos de Garantia	Opções de Garantia Independente
Impacto de adicionar o SaaS, Subcontratantes, Alojamentos de sites			
8	**Âmbito:** Pessoal, Confidencial **Localização de Processamento:** No Fornecedor **Função de Processamento:** Processador **Classe de Dados:** Altamente Confidencial ou Confidencial **Cartões de Pagamento:** Não Aplicável **Subcontratantes:** SIM ou **SaaS:** SIM ou **Alojamentos de Sites:** SIM	Autoatestado de conformidade com os RPD **e** Garantia Independente de conformidade	Opções de Garantia Independente: 1. Concluir uma Avaliação Independente segundo os RPD, 2. Avaliação Independente segundos as secções A-I dos RPD e ISO 27001, **ou** 3. Submeter ISO 27701 **e** ISO 27001
9	**Âmbito:** Pessoal, Confidencial **Localização de Processamento:** No Fornecedor **Função de Processamento:** Controlador **Classe de Dados:** Altamente Confidencial ou Confidencial **Cartões de Pagamento:** Não Aplicável **Subcontratantes:** SIM ou **SaaS:** SIM ou **Alojamentos de Sites:** SIM	Autoatestado de conformidade com os RPD	

#	Perfil	Requisitos de Garantia	Opções de Garantia Independente
Garantia adicional de Cartões de Pagamento e SaaS			
10	Quaisquer dos anteriores perfis e **Cartões de Pagamento**	Os requisitos anteriores aplicáveis **e** garantia PCI (Payment Card Industry)	Submeter Certificação PCI DSS
11	Quaisquer dos perfis acima e **Software como Serviço (SaaS)**	Requisitos anteriores aplicáveis **e** submissão da certificação ISO 27001 contratualmente obrigatória que abrange os serviços funcionais.	Submeter uma certificação ISO 27001 com cobertura funcional do(s) serviço(s) prestado(s)