# Microsoft Procurement

## Guia do Programa Supplier Security & Privacy Assurance (SSPA)

Versão 8

Junho de 2022

# Introdução

Na Microsoft, acreditamos que a privacidade é um direito fundamental. De acordo com nossa missão de encorajar cada indivíduo e organização no planeta a chegar mais longe, esforçamo-nos para conquistar e preservar a confiança de nossos clientes todos os dias.

Fortes práticas de privacidade e segurança são cruciais para 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 nossos valores enquanto empresa e estendem-se a nossos fornecedores (como sua empresa) que processam dados da Microsoft em nosso nome.

O Programa Supplier Security and Privacy Assurance ("**SSPA**") é o programa corporativo da Microsoft implementado com vistas a oferecer instruções de processamento de dados básicos da Microsoft a nossos fornecedores em forma de Requisitos de Proteção de Dados dos Fornecedores da Microsoft ("**DPR**"), disponível na página sobre o SSPA em Microsoft.com/Procurement. Note que os fornecedores podem ter de cumprir outros requisitos ao nível organizacional, que são decididos e comunicados externamente ao SSPA pelo grupo da Microsoft responsável pelo engajamento com o fornecedor.

Os termos principais do SSPA encontram-se definidos nos DPR. Para obter mais informações sobre o programa, consulte nossas Perguntas frequentes e entre em contato por escrito com nossa equipe global através do endereço SSPAHelp@microsoft.com.

## Visão Geral do Programa SSPA

O SSPA é uma parceria entre Microsoft Procurement, os Assuntos Corporativos Externos e Legais e a Segurança Corporativa para garantir que nossos fornecedores sigam os princípios de privacidade e segurança.

O escopo do SSPA abrange todos os fornecedores em nível global que Processam Dados Pessoais ou Dados Confidenciais da Microsoft em conexão com o desempenho desse fornecedor (por exemplo: fornecimento de serviços, licenças de software, serviços em nuvem) sob os termos do contrato com a Microsoft (por exemplo: termos da Ordem de Compra, contrato principal) ("**Desempenhar**" ou "**Desempenho**").

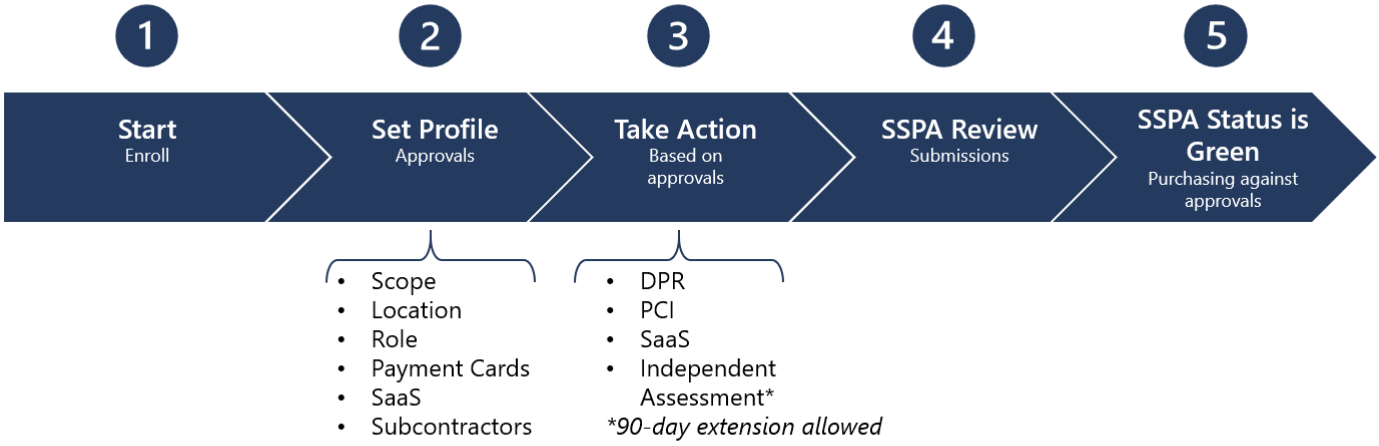
O SSPA permite ao fornecedor fazer seleções do Perfil de Processamento de Dados alinhadas aos bens ou serviços que você foi contratado para Desempenhar. Estas seleções acionam requisitos correspondentes para fornecer garantias de compliance) à Microsoft.

**Todos os fornecedores inscritos irão preencher uma auto-atestação de conformidade com os DPR, em forma anual.** Seu Perfil de Processamento de Dados determina se são emitidos os DPR completos ou se se aplica um subconjunto de requisitos. Os fornecedores que processarem dados que a Microsoft considera de maior risco também poderão ter de cumprir outros requisitos- tais

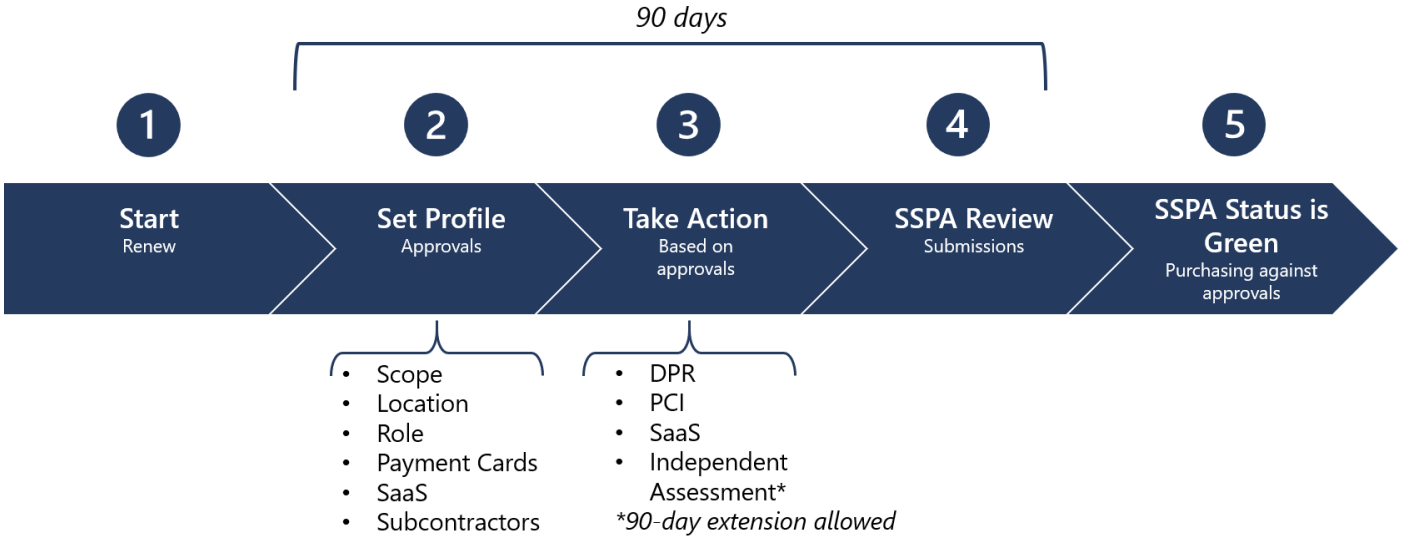
como, por exemplo, fornecer uma verificação independente de conformidade. Os fornecedores incluídos em uma lista publicada de Subprocessadores da Microsoft também deverão fornecer uma verificação independente de conformidade.

**Importante:** As atividades de conformidade determinam se o estado do SSPA é Verde (em conformidade) ou Vermelho (sem conformidade). As ferramentas de compra da Microsoft confirmam se o estado do SSPA é Verde (no caso de todos os fornecedores pertencentes ao programa SSPA) antes de autorizar-se um  engajamento a seguir em frente.

## Diagrama de Processo do SSPA: Inscrição de Novo Fornecedor




## Diagrama de Processo do SSPA: Renovação Anual de Fornecedor



# Escopo do SSPA

Para poder determinar se você (o fornecedor) Processa Dados Pessoais ou Dados Confidenciais da Microsoft, consulte a lista de exemplos nas tabelas abaixo. Leve em conta que estes são exemplos, e não uma lista final e definitiva.
**Observação:** Um gestor de negócios da Microsoft poderá solicitar uma inscrição fora desta lista, considerando 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, biométricos ou de saúde |
| Origem racial ou étnica |
| Afiliações, opiniões e crenças filosóficas, religiosas ou políticas |
| Filiação sindical |
| Vida sexual ou orientação sexual de uma pessoa natural |
| Status de imigração (visto, autorização de trabalho, etc.) |
| Identificadores emitidos pelo Governo (passaporte, carteira de motorista, visto, número do CPF, número de identificação nacional) |
| Dados precisos de localização do usuário (até 300 metros) |
| Números de contas bancárias pessoais |
| Número de cartão de crédito e data de vencimento |
| Dados de conteúdo do cliente |
| Documentos, fotografias, vídeos, música, etc. |
| Críticas ou avaliações submetidas para um produto ou serviço |
| Respostas da pesquisa |
| Histórico de navegação, interesses e favoritos |
| Escrita à tinta, digitação e emissão de voz (voz/áudio ou chat/bot) |
| Dados de credenciais (senhas, dicas de senha, nome de usuário, dados biométricos utilizados para identificação) |
| Dados do cliente associados a um caso de suporte |

| Dados capturados e gerados |
| --- |
| Dados imprecisos de localização |
| Endereço IP |
| Preferências de dispositivo e personalização |
| Uso do serviço para sites, acompanhamento de cliques em páginas Web |
| Dados de redes sociais, relações gráficas sociais |
| Dados de atividade desde dispositivos conectados, como monitores de fitness |
| Dados de contato, tais como nome, endereço, número de telefone, endereço de email, data de nascimento, contatos de dependentes e de emergência |
| Avaliação de fraude e risco, verificação de antecedentes |
| Dados de benefícios, seguro, pensão |
| Currículos, notas de entrevista/comentários |
| Metadata and telemetry |
| Dados da conta |
| Dados de instrumentos de pagamento |
| Número de cartão de crédito e data de vencimento |
| Informação do roteamento bancário |
| Número da conta bancária |
| Solicitações de crédito ou linha de crédito |
| Identificadores e documentos fiscais |
| Dados de despesas ou investimento |
| Cartões  Corporativos |
| Informações pseudonimizadas do usuário final (EUPI)<br>(Identificadores criados pela Microsoft para identificar usuários de produtos e serviços da Microsoft) |
| Identificador global exclusivo (GUID) |
| ID de passaporte do usuário ou identificador exclusivo (PUID) |
| Informações de identificação do usuário final com hash (EUII) |
| ID de sessão |
| ID de dispositivo |
| Dados de diagnóstico |
| Dados de log |

| 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 ao desenvolvimento, teste ou produção de Produtos da Microsoft ou componentes de Produtos da Microsoft<br><br>*O software, os serviços online ou o hardware da Microsoft comercializados em qualquer canal são considerados como "**Produto da Microsoft**".* |
| Informações de marketing de pré-lançamento de dispositivos da Microsoft |
| Dados financeiros corporativos da Microsoft não divulgados, sujeitos às regras da SEC |
| **Confidencial** |
| Códigos de licença de produtos da Microsoft em nome da Microsoft para distribuição através de qualquer método |
| Informações relativas ou relacionadas ao desenvolvimento ou teste de aplicativos de linha de negócios (LOB) internos da Microsoft |
| Materiais de marketing de pré-lançamento da Microsoft para software e serviços da Microsoft, como Office, SQL, Azure, etc. |
| Documentação escrita, de design, eletrônica ou impressa para quaisquer serviços ou produtos da Microsoft, tais como, por exemplo, dispositivos (guias de processos ou procedimentos, dados de configuração, etc.) |

**Importante:** Um gestor de negócios da Microsoft poderá solicitar a participação para dados não incluídos nesta lista.

# Perfil de Processamento de Dados

Os fornecedores da Microsoft têm controle sobre seu Perfil de Processamento de Dados do SSPA.

Isto permite que os fornecedores decidam a quais engajamentos desejam ser elegíveis para desempenhar. Preste especial atenção às seleções e considere as atividades de compliance que devem ser realizadas para obter-se a aprovação. **Consulte a seção "Requisitos de Garantia" abaixo e o Apêndice A.**

As unidades de negócios da Microsoft só poderão criar engajamentos com fornecedores nos casos em que a atividade de processamento de dados corresponda às aprovações que o fornecedor obteve.

Os fornecedores poderão atualizar seu Perfil de Processamento de Dados em qualquer momento do ano **se não houver tarefas pendentes**. Quando for efetuada uma alteração, a atividade correspondente será emitida e terá de ser concluída antes de garantir-se 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 status do SSPA ficará  Vermelho (sem conformidade), e a conta estará em risco de ser desativada dos sistemas de Contas a Pagar da Microsoft.

| Aprovações de Processamento de Dados | |
|---|---|
| 1 | Escopo de Processamento de Dados<br>▪ Confidencial<br>▪ Pessoal, confidencial |
| 2 | Localização de Processamento de Dados<br>▪ Na Microsoft ou no cliente<br>▪ No fornecedor |
| 3 | Função de Processamento de Dados<br>▪ Controlador (controlador independente ou conjunto)<br>▪ Processador<br>▪ Subprocessador (designado pela Microsoft) |
| 4 | Processamento de Cartões de Pagamento<br>▪ Sim<br>▪ Não aplicável |
| 5 | Software como Serviço<br>▪ Sim<br>▪ Não aplicável |
| 6 | Uso de Subcontratados<br>▪ Sim<br>▪ Não aplicável |

# Considerações de Aprovação

## Escopo de Processamento de Dados

Confidencial

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

Se você selecionar esta aprovação, não estará qualificado para engajamentos com processamento de Dados Pessoais.

Pessoal, confidencial

Selecione esta aprovação se o Desempenho (prestação de serviços) 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 (prestação de serviços) do fornecedor envolver o Processamento de Dados de parte dele, dentro do ambiente da rede da Microsoft, no qual os membros da equipe utilizam credenciais de acesso @microsoft.com ou dentro do ambiente de um cliente da Microsoft.

Não selecione esta opção nas seguintes circunstâncias:

- O fornecedor gerencia uma instalação offshore (OF) designada pela Microsoft.
- O fornecedor disponibiliza os recursos à Microsoft e trabalha periodicamente dentro e fora da rede da 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 aspectos do Desempenho (prestação de serviços) da parte do fornecedor cumprirem a definição de função de processamento de dados do Controlador (consulte os DPR).

Se você selecionar esta aprovação, não estará qualificado para o 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.  Verifique as definições de Processador nos DPR.

**Subprocessador**

Um Subprocessador é um terceiro contratado pela Microsoft para Desempenhar-se (prestar serviços), onde o Desempenho (prestação de serviços) inclui o Processamento de Dados Pessoais da Microsoft, para os quais a Microsoft é um Processador. Os fornecedores não podem se auto-identificar como Subprocessadores na Microsoft porque isso requer uma pré-aprovação dos times de Privacidade internas. Os fornecedores só poderão ser Subprocessadores quando a Microsoft for o Processador de

Dados e o fornecedor Processar Tipos qualificados de Dados Pessoais da Empresa. Os Subprocessadores terão outros requisitos de compliance e de contrato, inclusive um Adendo de Proteção de Dados e uma Avaliação Independente (consulte 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 engajamentos de processamento de cartões de pagamento.

_____

## Software

O time de Procurement  da Microsoft direciona os Compradores através de um processo  para todas as compras de software. Isto inclui várias verificações, dentre elas, a triagem do SSPA para decidir se o fornecedor do software está no escopo do SSPA (os Compradores da Microsoft podem consultar os passos descritos na página interna Serviço em Nuvem e Software ProcureWeb para obter mais informações). Se o SSPA for requerido, é possível que os fornecedores também devam identificar que a escolha do perfil do 'Software como Serviço' (SaaS) seja aplicável. Os fornecedores inscritos no SSPA podem fazê-lo ao completar o Perfil de Processamento de Dados no Portal de Compliance de Fornecedores da Microsoft.

Para fins de conformidade com o SSPA, considere o SaaS de forma abrangente para incluir, também, a plataforma como serviço (PaaS) e a infraestrutura como serviço (IaaS). (Para obter mais informações sobre o SaaS, veja esta explicação.)

## Software como Serviço (SaaS)

O Software como Serviço (SaaS) permite que os usuários utilizem aplicativos baseados em nuvem e a eles se conectem pela Internet.

A Microsoft define o **Software como Serviço (SaaS)** como software baseado em código comum, utilizado em um modelo "um para muitos" em uma base de pagamento por uso ou como uma assinatura baseada em métricas de uso. O fornecedor do serviço em nuvem desenvolve e mantém software baseado em nuvem, oferece atualizações de software automáticas e disponibiliza o software a seus clientes através da Internet em uma base de "um para muitos" e de pagamento conforme o uso. Com este método de entrega e licenciamento de software, é possível acessar o software online através de uma assinatura em vez de comprá-lo e instalá-lo em cada computador individual.

**Observação:** A maioria dos fornecedores de SaaS deverá adicionar a aprovação como Subcontratado no Portal de compliance) de Fornecedores da Microsoft, caso os Dados Pessoais ou os Dados Confidenciais da Microsoft se hospedarem em uma plataforma de terceiros.

### Uso de Subcontratados

Selecione esta aprovação se o fornecedor utilizar Subcontratados para o Desempenho (a prestação de serviços) (consulte as definições nos DPR).

Isto também inclui Freelancers (consulte os DPR).

# Requisitos de Garantia

## Requisitos com base nas Aprovações de Perfis

As aprovações selecionadas em seu Perfil de Processamento de Dados auxiliam o SSPA na avaliação do nível de risco no(s) compromisso(s) da Microsoft. Os requisitos de compliance do SSPA diferem com base nas aprovações de Perfil de Processamento de Dados e associadas. Nesta seção, explicam-se os diferentes requisitos do SSPA.

Existem também combinações que podem aumentar ou reduzir os requisitos de compliance. As combinações são capturadas no Apêndice A, e isto é o que você pode esperar executar a partir do Portal de Compliance de Fornecedores da Microsoft, ao completar seu perfil. Sempre é possível validar o modo como seu cenário se adapta a esta estrutura, ao solicitar uma revisão de equipe do SSPA.

**Ação:** Localize seu perfil de aprovação no Apêndice A e examine os requisitos de garantia e opções de Garantia Independente correspondentes, se aplicáveis.

**Importante:** Se seu perfil incluir Software como Serviço (SaaS), subcontratados, hospedagem em site ou cartões de pagamento, será necessária uma garantia adicional.

## Autoatestado com os DPR

Todos os fornecedores inscritos no SSPA terão de preencher um autoatestado de conformidade com os DPR dentro de 90 dias após recebimento da solicitação. Esta solicitação será feita anualmente, mas poderá ser mais frequente perante uma atualização semestral do Perfil de Processamento de Dados. As contas de fornecedores mudarão para um estado do SSPA Vermelho (não conforme) se o período de 90 dias for excedido. As novas ordens de compra no escopo não poderão ser processadas  até queo estado SSPA fique Verde (em conformidade).

Os fornecedores recentemente inscritos terão de cumprir os requisitos emitidos para garantir um estado do SSPA Verde (em conformidade) antes de os compromissos terem início.

**Importante:** O time de SSPA não está autorizado a providenciar extensões para esta tarefa.

Os representantes autorizados que preencherem o autoatestado deverão garantir que possuem informações suficientes de especialistas na matéria para responderem com confiança a cada requisito. Além do mais, ao adicionar-se o respectivo nome a um formulário do SSPA, certificam que leram e

compreenderam os DPR. Os fornecedores podem adicionar outros contatos à ferramenta online para auxiliar no cumprimento dos requisitos.

O Representante Autorizado (consulte a definição nos DPR) deve:

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

# Aplicabilidade

Espera-se que os fornecedores respondam a todos os requisitos aplicáveis dos DPR 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 oferece à Microsoft. Podem ser marcados como "não aplicável" com um comentário detalhado para os revisores do SSPA validarem.

As submissões dos DPR são examinadas pela equipe do SSPA para verificação de seleções de "não aplicável", "conflito jurídico local" ou "conflito contratual", em face aos requisitos emitidos. A equipe do SSPA poderá pedir esclarecimento sobre uma ou mais seleções. Os conflitos contratuais e jurídicos locais só serão aceitos se as referências de suporte forem apresentadas e o conflito for claro.

# Requisito de Avaliação Independente

Consulte a seção Requisitos por Aprovações no Apêndice 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 respectivo Perfil de Processamento de Dados. No entanto, se o fornecedor tiver uma Função de Processamento de Dados de “Subprocessador”, não poderá alterar esta aprovação e deverá realizar uma Avaliação Independente em forma anual.

Para garantir as aprovações que requeiram uma verificação independente de conformidade, os fornecedores terão de selecionar um assessor independente para validar a conformidade de acordo aos DPR. 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 resolver-se e corrigir-se antes da carta de confirmação ser enviada ao Portal de Compliance de Fornecedores da Microsoft para revisão da equipe do SSPA. Os representantes podem baixar um modelo de carta de consultoria aprovado, que é anexado ao PDF “Assessores Preferenciais”, disponível aqui.

O **Apêndice A** inclui alternativas de certificação aceitáveis se você decidir não utilizar um assessor independente para verificar a conformidade com os DPR (quando aplicável, por exemplo, para fornecedores de SaaS, fornecedores de hospedagem em site ou fornecedores com Subcontratados). As normas ISO 27701 (privacidade) e ISO 27001 (segurança) são utilizadas para proporcionar um mapeamento próximo para os DPR.

Se o Fornecedor for Profissional de Saúde nos Estados Unidos ou uma entidade coberta, aceitaremos um relatório da HITRUST para cobertura de segurança e privacidade.

O SSPA pode realizar uma avaliação independente manualmente se houver circunstâncias para além dos requisitos padrão que mereçam devidas diligências adicionais. Exemplos disso são uma solicitação dos times de privacidade ou segurança, a validação da correção de incidentes de dados e o requisito de execução automatizada dos direitos do titular dos dados.

**Orientações sobre como abordar este requisito:**

1. O compromisso deve ser assumido 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 Federação Internacional de Contabilistas (IFAC) ou no Instituto Americano de Contadores Públicos Certificados (AICPA), ou terão de estar certificados por outras entidades de segurança e privacidade pertinentes, tais como a Associação Internacional de Profissionais de Privacidade (IAPP) ou a Associação de Auditoria e Controle de Sistemas de Informação (ISACA).
3. O assessor deve utilizar os DPR mais recentes como provas necessárias para validar cada requisito. **Os fornecedores precisarão apresentar suas respostas aprovadas mais recentes de atestado dos DPR, ao assessor.**
4. No que respeita aos fornecedores recentemente inscritos, o assessor irá testar o design dos controles do processo. Nos casos restantes, o assessor testará a eficácia dos controles.
5. O escopo do engajamento de avaliação está limitado aos Dados Pessoais ou aos Dados Confidenciais da Microsoft em ligação com o Desempenho (a prestação de serviços) desse fornecedor.
6. O escopo do compromisso está limitado a todas as atividades de processamento de dados no escopo, executadas no número de conta de fornecedor que recebeu a solicitação. Se o fornecedor selecionar mais de uma conta de fornecedor em simultâneo, a **carta de atestado deverá conter a lista de contas de fornecedores incluídas na avaliação e endereços associados.**
7. A carta enviada ao SSPA não deve incluir declarações de que o fornecedor não possa cumprir os Requisitos de Proteção de Dados indicados. Estes problemas devem ser corrigidos antes do envio da carta.

O SSPA disponibilizou uma lista de assessores preferenciais disponíveis. Estas empresas estão familiarizadas com a realização de avaliações do SSPA. Os fornecedores deverão pagar esta avaliação, e os custos variarão conforme a escala e o escopo do processamento de dados.

# Requisito de Certificação do PCI DSS

O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) é uma estrutura sólida para desenvolver a segurança de dados de cartões de pagamento, que inclui prevenção, detecção e reação adequadas a incidentes de segurança. A estrutura foi desenvolvida pelo Conselho de Padrões de Segurança do PCI, uma organização da indústria autorreguladora. O objetivo dos

requisitos do PCI DSS é identificar as vulnerabilidades da tecnologia e dos processos que impõem riscos à segurança dos dados do titular do cartão que são processados.

A Microsoft deve cumprir estes padrões. Se um fornecedor processar informações de cartão de pagamento em nome da Microsoft, requeremos provas do cumprimento destes padrões. Consulte o Conselho de Padrões de Segurança do PCI para compreender os requisitos definidos pela organização do PCI.

Segundo 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 as delimitações para o tipo de avaliação, em geral:

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

Envie a certificação aplicável que atenda aos requisitos do PCI.

## Requisitos de Software como Serviço

É possível que os fornecedores que se enquadram na definição de SaaS incluída no Perfil de Processamento de Dados devam fornecer uma certificação ISO 27001 válida, caso exigida no Contrato de Serviços em Nuvem da Microsoft.

Os revisores do SSPA validarão se seu envio atende às obrigações contratuais.

Não envie uma certificação de datacenter. Esperamos a certificação ISO 27001 correspondente ao(s) serviço(s) de software indicado(s) em seu contrato com a Microsoft.

## Uso de Subcontratados

A Microsoft considera que o uso de subcontratantes é um fator de alto risco. Os fornecedores que recorrerem a subcontratados para Processar Dados Pessoais ou Confidenciais da Microsoft devem informá-los. Além do mais, o fornecedor também deve informar os países onde esses dados pessoais serão processados por cada subcontratado.

## Incidentes de Dados

Se um fornecedor tomar conhecimento de um incidente de dados de privacidade ou segurança, terá de informar à Microsoft, conforme indicado de forma detalhada nos DPR. O fornecedor deve informar a Microsoft conforme detalhado e definido nos DPR.

Informe um incidente de dados utilizando o SupplierWeb ou enviando um email para SuppIR@microsoft.com.

Certifique-se de incluir:

- Data do incidente de dados:
- Nome do fornecedor:
- Número do fornecedor:
- Contato(s) da Microsoft notificado(s):
- Ordem de compra associada, se aplicável/disponível:
- Resumo do incidente de dados:

# Apêndice A

## Requisitos com base nas Aprovações de Perfis

| N.º | Perfil | Requisitos de Garantia | Opções de Garantia Independente |
|---|---|---|---|
| 1 | **Escopo:** Pessoal, confidencial<br>**Localização de Processamento:** Na Microsoft ou no cliente<br>**Função de Processamento:** Processador ou controlador<br>**Classe de dados:** Confidencial **ou** altamente confidencial<br>**Cartões de Pagamento:** Não aplicável<br>**SaaS:** Não aplicável<br>**Uso de Subcontratados:** Não aplicável<br>**Hospedagem em Site:** Não aplicável | Autoatestado de conformidade com os DPR | |
| 2 | **Escopo:** Confidencial<br>**Localização de Processamento:** No fornecedor<br>**Função de Processamento:** Não aplicável<br>**Classe de dados:** Confidencial<br>**Cartões de Pagamento:** Não aplicável<br>**SaaS:** Não aplicável<br>**Uso de Subcontratados:** Não aplicável<br>**Hospedagem em Site:** Não aplicável | Autoatestado de conformidade com os DPR | |
| 3 | **Escopo:** Confidencial<br>**Localização de Processamento:** No fornecedor<br>**Função de Processamento:** Processador<br>**Classe de dados:** Altamente confidencial<br>**Cartões de Pagamento:** Não aplicável<br>**SaaS:** Não aplicável<br>**Uso de Subcontratados:** Não aplicável | Autoatestado de conformidade com os DPR<br>**e**<br>Garantia Independente de Conformidade | Opções de Garantia Independente:<br>1. Realizar uma Avaliação Independente segundo os DPR **ou**<br>2. Enviar a certificação ISO 27001 |

| | | | |
|---|---|---|---|
| | **Hospedagem em Site:** Não aplicável | | |

| N.º | Perfil | Requisitos de Garantia | Opções de Garantia Independente |
|---|---|---|---|
| 4 | **Escopo:** Pessoal, confidencial<br>**Localização de Processamento:** No fornecedor<br>**Função de Processamento:** Processador<br>**Classe de dados:** Altamente confidencial<br>**Cartões de Pagamento:** Não aplicável<br>**SaaS:** Não aplicável<br>**Uso de Subcontratados:** Não aplicável<br>**Hospedagem em Site:** Não aplicável | Autoatestado de conformidade com os DPR<br>**e**<br>Garantia Independente de Conformidade | Opções de Garantia Independente:<br>1. Realizar uma Avaliação Independente segundo os DPR<br>2. Avaliação Independente segundo as seções A-I dos DPR e a norma ISO 27001<br>**ou**<br>3. Enviar as certificações ISO 27701 **e** ISO 27001 |
| 5 | **Escopo:** Pessoal, confidencial<br>**Localização de Processamento:** No fornecedor<br>**Função de Processamento:** Processador<br>**Classe de dados:** Confidencial<br>**Cartões de Pagamento:** Não aplicável<br>**SaaS:** Não aplicável<br>**Uso de Subcontratados:** Não aplicável<br>**Hospedagem em Site:** Não aplicável | Autoatestado de conformidade com os DPR | |
| 6 | **Escopo:** Pessoal, confidencial<br>**Localização de Processamento:** No fornecedor<br>**Função de Processamento:** Controlador<br>**Classe de dados:** Altamente confidencial ou confidencial<br>**Cartões de Pagamento:** Não aplicável | Autoatestado de conformidade com os DPR | |

| | | | |
|---|---|---|---|
| | **SaaS:** Não aplicável<br>**Uso de Subcontratados:** Não aplicável<br>**Hospedagem em Site:** Não aplicável | | |

| N.º | Perfil | Requisitos de Garantia | Opções de Garantia Independente |
|---|---|---|---|
| 7 | **Escopo:** Pessoal, confidencial<br>**Localização de Processamento:** Qualquer<br>**Função de Processamento:** Subprocessador (esta função é determinada pela Microsoft, o perfil dirá "Aprovação do subprocessador: sim")<br>**Classe de dados:** Altamente confidencial ou confidencial<br>**Cartões de Pagamento:** Não aplicável<br>**SaaS:** Não aplicável<br>**Uso de Subcontratados:** Não aplicável<br>**Hospedagem em Site:** Não aplicável | Autoatestado de conformidade com os DPR<br>**e**<br>Garantia Independente de Conformidade | Opções de Garantia Independente:<br>1. Realizar uma Avaliação Independente segundo os DPR<br>2. Avaliação Independente segundo as seções A-I dos DPR e a norma ISO 27001<br>**ou**<br>3. Enviar as certificações ISO 27701 **e** ISO 27001 |

| N.º | Perfil | Requisitos de Garantia | Opções de Garantia Independente |
|---|---|---|---|
| Impacto de adicionar SaaS, Subcontratados, Hospedagem em Site: | | | |
| 8 | **Escopo:** Pessoal, confidencial<br>**Localização de Processamento:** No fornecedor<br>**Função de Processamento:** Processador<br>**Classe de dados:** Altamente confidencial ou confidencial<br>**Cartões de Pagamento:** Não aplicável<br>**Subcontratados:** SIM ou<br>**SaaS:** SIM ou<br>**Hospedagem em Site:** SIM | Autoatestado de conformidade com os DPR<br>**e**<br>Garantia Independente de Conformidade | Opções de Garantia Independente:<br>1. Realizar uma Avaliação Independente segundo os DPR<br>2. Avaliação Independente segundo as seções A-I dos DPR e a norma ISO 27001<br>**ou**<br>3. Enviar as certificações ISO 27701 **e** ISO 27001 |
| 9 | **Escopo:** Pessoal, confidencial<br>**Localização de Processamento:** No fornecedor<br>**Função de Processamento:** Controlador<br>**Classe de dados:** Altamente confidencial ou confidencial<br>**Cartões de Pagamento:** Não aplicável<br>**Subcontratados:** SIM ou<br>**SaaS:** SIM ou<br>**Hospedagem em Site:** SIM | Autoatestado de conformidade com os DPR | |

| N.º | Perfil | Requisitos de Garantia | Opções de Garantia Independente |
|---|---|---|---|
| Garantia adicional para Cartões de Pagamento e SaaS | | | |
| 10 | Quaisquer dos anteriores perfis e **Cartões de Pagamento** | Os requisitos anteriores aplicáveis **e** garantia do Setor de Cartões de Pagamento (PCI) | Enviar a certificação do PCI DSS |
| 11 | Quaisquer dos anteriores perfis e **Software como Serviço (SaaS)** | Requisitos anteriores aplicáveis **e** envio da certificação ISO 27001 contratualmente obrigatória que abrange os serviços funcionais. | Enviar uma certificação ISO 27001 com cobertura funcional do(s) serviço(s) prestado(s). |