Requisitos de Proteção de Dados dos Fornecedores da Microsoft

Aplicabilidade

Os Requisitos de Proteção de Dados ("**DPR**") dos fornecedores da Microsoft se aplicam a todos os fornecedores da Microsoft que Processam Dados Pessoais da Microsoft ou Dados Confidenciais da Microsoft em conexão com a prestação de serviços desses fornecedores (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**" ou "**Prestação de Serviços**").

- Em caso de conflito entre os DPR e os requisitos especificados nos acordos contratuais entre o fornecedor e a Microsoft, os DPR terão precedência, a menos que o fornecedor identifique a disposição correta no contrato que substitui o requisito de proteção de dados aplicável (nesse caso, prevalecem os termos do contrato).
- Em caso de conflito entre os requisitos aqui contidos e quaisquer requisitos legais ou estatutários, prevalecem os requisitos legais ou estatutários.
- Caso o fornecedor da Microsoft opere como Controlador, o fornecedor poderá ter requisitos reduzidos nos DPR.
- Caso o fornecedor da Microsoft não Processe Dados Pessoais da Microsoft, mas apenas Dados Confidenciais da Microsoft, o fornecedor poderá ter requisitos reduzidos com relação a estes DPR.

Transferência Internacional de Dados

Sem limitar suas outras obrigações, o fornecedor não fará nenhuma transferência internacional de Dados Pessoais da Microsoft, a menos que a Microsoft forneça aprovação prévia por escrito e, em qualquer caso, o fornecedor deverá cumprir os Requisitos de Proteção de Dados, incluindo as Cláusulas Contratuais Padrão ou, a critério da Microsoft, outros mecanismos apropriados de transferência internacional aprovados por uma autoridade de proteção de dados apropriada ou pela Comissão Europeia, conforme aplicável, e adotados ou acordados pela Microsoft. As Cláusulas Contratuais Padrão Sucessoras adotadas (i) pela Comissão Europeia ou adotadas pela Autoridade Europeia para a Proteção de Dados e aprovadas pela Comissão Europeia, (ii) pelo Reino Unido, de acordo com a Lei Federal Geral de Proteção de Dados do Reino Unido, (iii) pela Suíça, de acordo com a Lei Federal de Proteção de Dados da Suíça, ou (iv) as cláusulas que regem a transferência internacional de dados pessoais oficialmente adotadas por um governo em uma jurisdição que não seja a Suíça, o Reino Unido e as jurisdições que compõem a União Europeia/Espaço Econômico Europeu deverão ser incorporadas e vinculativas para o fornecedor a partir do dia de sua adoção. O fornecedor também deve garantir que todos e quaisquer subprocessadores (conforme definido nas Cláusulas Contratuais Padrão) também estejam em conformidade.

Definições-chave

Os seguintes termos usados neste documento têm os seguintes significados. A lista de exemplos após "incluindo", "como", "ou seja", "por exemplo" ou similares usados em todo este documento é interpretada como incluindo "sem limitação" ou "mas não limitado a", salvo qualificação por meio de palavras como "apenas" ou "exclusivamente". Para mais definições, consulte o Glossário no final deste documento.

"**Controlador"** significa a entidade que determina as finalidades e os meios do Processamento de Dados Pessoais. "Controlador" inclui uma Empresa, um Controlador (conforme esse termo é definido no Regulamento Geral sobre a Proteção de Dados (GDPR) e termos equivalentes nas Leis de Proteção de Dados, conforme o contexto exigir.

"**Cookies**" são pequenos arquivos de texto armazenados em dispositivos por sites ou aplicativos que contêm informações usadas para reconhecer um Titular de Dados ou um dispositivo.

"**Dados Confidenciais da Microsoft**" são quaisquer informações que, se comprometidas por meio de confidencialidade ou integridade, podem resultar em perdas financeiras ou de reputação significativas para a Microsoft. Isso inclui produtos de hardware e software da Microsoft, aplicativos internos de linha de negócios, materiais de marketing de pré-lançamento, chaves de licença de produto e documentações técnicas relacionadas aos produtos e serviços da Microsoft.

"**Dados Pessoais**" significa quaisquer informações relacionadas a um Titular de Dados e quaisquer outras informações que constituam "dados pessoais" ou "informações pessoais" de acordo com a Lei.

“**Dados Pessoais da Microsoft**” significa quaisquer Dados Pessoais Processados pela Microsoft ou em nome dela.

“**Direito do Titular de Dados** ” significa o direito do Titular de Dados de acessar, excluir, editar, exportar, restringir ou refutar o Processamento dos Dados Pessoais da Microsoft desse Titular de Dados, caso seja exigido por lei.

“**Incidente de Dados**” significa (1) uma violação de segurança que leva à destruição acidental ou Ilegal, perda, alteração, divulgação não autorizada de Dados Pessoais da Microsoft ou Dados Confidenciais da Microsoft transmitidos, armazenados ou Processados pelo fornecedor ou seus Subcontratados ou acesso a eles, ou (2) uma vulnerabilidade de segurança relacionada ao manuseio do fornecedor de Dados Pessoais da Microsoft ou Dados Confidenciais da Microsoft.

“**Lei**” significa todas as leis, regras, estatutos, decretos, decisões, ordens, regulamentos, decisões, códigos, decretos, resoluções e requisitos aplicáveis de qualquer autoridade governamental (federal, estadual, local ou internacional) que tenha jurisdição. “**Ilegal**” significa qualquer violação da Lei.

“**Processador**” significa uma entidade que processa Dados Pessoais em nome de outra entidade e inclui um Provedor de Serviços, um Processador (conforme esse termo é definido no GDPR) e termos equivalentes nas Leis de Proteção de Dados, conforme o contexto assim o exigir.

“**Processo**” significa qualquer operação ou conjunto de operações que seja realizado em quaisquer Dados Pessoais ou Dados Confidenciais da Microsoft, seja ou não por meios automatizados, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização de qualquer outra forma, alinhamento ou combinação, restrição, apagamento ou destruição. “Processando” e “Processado” terão significados correspondentes.

“**Subcontratado**” significa um terceiro a quem o fornecedor delega suas obrigações em relação ao contrato que cobre sua Prestação de Serviços, incluindo uma afiliada do fornecedor que não tem contrato direto com a Microsoft.

“**Subprocessador**” significa um terceiro contratado pela Microsoft para Desempenhar-se, onde a Prestação de Serviços inclui o Processamento de Dados Pessoais da Microsoft, para os quais a Microsoft é um Processador.

“**Titular de Dados**” significa uma pessoa física identificável que pode ser identificada, de maneira direta ou indireta, especificamente por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social daquela pessoa física.

Resposta do Fornecedor

Os fornecedores confirmam a conformidade com esses requisitos anualmente usando um serviço online administrado pela Microsoft. Consulte o Guia do Programa SSPA para entender como é administrada a conformidade.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção A: Gestão	
1	Cada acordo aplicável entre a Microsoft e o fornecedor (por exemplo: contrato principal, declaração de trabalho, ordens de compra e outras ordens) contém linguagem de proteção de dados de privacidade e segurança com relação aos Dados Pessoais e Confidenciais da Microsoft, conforme aplicável, incluindo proibições sobre a venda de Dados Pessoais da Microsoft e o Processamento de Dados Pessoais da Microsoft além do relacionamento comercial direto entre a Microsoft e o fornecedor. No caso de empresas que operam como Processadores ou Subprocessadores em conexão com a Prestação de Serviços, com relação aos Dados Pessoais da Microsoft, o contrato deve incluir o objeto e a duração do Processamento, a natureza e a finalidade do Processamento, o tipo de Dados Pessoais da Microsoft, as categorias dos Titulares de Dados, e as obrigações e os direitos da Microsoft.	O fornecedor deve apresentar o contrato aplicável entre a Microsoft e o fornecedor. No caso de Processadores e Subprocessadores, as descrições de Processamento estão contidas no contrato aplicável (por exemplo: declaração de trabalho, ordens de compra). Observação: As empresas com ordens de compra em andamento podem ter a descrição necessária das atividades de processamento adicionadas em etapas posteriores do processo de compra.
2	Quando a Microsoft confirma que seus compromissos cumprem uma função de Subprocessador, o fornecedor deve ter contratos de proteção de dados aplicáveis em vigor com a Microsoft. Observação: A Microsoft publicará essa designação no seu perfil quando isso for aplicável.	Cláusulas Contratuais Padrão, Adendo de Dados do Cliente Online ou Adendo de Processamento de Dados de Serviços Profissionais de Fornecedores e Parceiros.
3	Atribuir a responsabilidade de conformidade com os DPR a uma pessoa ou grupo designado dentro da empresa.	Nome da função da pessoa ou grupo encarregado de garantir a conformidade com os DPR dos fornecedores da Microsoft. Um documento que descreve a autoridade e a responsabilidade dessa pessoa ou grupo que demonstra uma função de privacidade ou segurança.
4	Estabelecer, manter e realizar treinamento anual de privacidade e segurança para funcionários que terão acesso aos Dados Pessoais e Confidenciais da Microsoft Processados pelo fornecedor durante a Prestação de Serviços. Se sua empresa não tiver conteúdo preparado, você pode usar este esboço de roteiro e adaptá-lo para a sua empresa. Observação: O pessoal do fornecedor pode ser obrigado a concluir treinamentos adicionais fornecidos pelas divisões da Microsoft.	Os registros anuais de participação estão disponíveis e podem ser fornecidos à Microsoft mediante solicitação. O conteúdo do treinamento inclui princípios de privacidade e segurança. A documentação da conformidade com os requisitos de treinamento incluirá provas de treinamento em relação aos requisitos regulatórios de privacidade, obrigações de segurança e conformidade com os requisitos e obrigações contratuais aplicáveis.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção A: Gestão (cont.)	
5	Processar Dados Pessoais da Microsoft somente de acordo com as instruções documentadas da Microsoft, incluindo cenários relacionados a transferências de Dados Pessoais da Microsoft para um país terceiro ou uma organização internacional, a menos que exigido por lei; nesse caso, o Processador ou Subprocessador (fornecedor) deverá informar o controlador (Microsoft) dessa exigência legal antes do Processamento, a menos que a Lei proíba tais informações por motivos importantes de interesse público.	O fornecedor compila e mantém todas as instruções documentadas da Microsoft (por exemplo: contrato, declaração de trabalho ou documentação de pedido) eletronicamente, em um local de fácil acesso aos funcionários e contratados do fornecedor que participam do Prestação de Serviços.
	Seção B: Notificação	
6	O fornecedor deve usar a Declaração de Privacidade da Microsoft ao coletar Dados Pessoais em nome da Microsoft. O aviso de privacidade deve ser evidente e estar disponível para os Titulares de Dados para ajudá-los a decidir se devem enviar seus Dados Pessoais ao fornecedor. Observação: Quando sua empresa for o Controlador da atividade de Processamento, você deve publicar seu próprio aviso de privacidade.	O fornecedor usa um fwdlink para a atual Declaração de Privacidade da Microsoft que foi publicada. A Declaração de Privacidade é publicada em qualquer contexto em que os Dados Pessoais de um usuário sejam coletados. Caso seja aplicável, estará disponível uma versão offline, a ser fornecida antes da coleta de dados. Quaisquer Declarações de Privacidade offline usadas são apresentadas em sua versão publicada mais recente e estão datadas corretamente. No caso dos serviços de funcionários da Microsoft, é utilizado o Aviso de Privacidade de Dados da Microsoft.
7	Ao coletar Dados Pessoais da Microsoft por meio de uma chamada de voz ao vivo ou gravada, os fornecedores devem estar preparados para discutir as práticas aplicáveis de coleta, manuseio, uso e retenção de dados com os Titulares de Dados.	Um roteiro para gravações de voz inclui como são processados os Dados Pessoais da Microsoft e contém: ▪ coleta ▪ uso ▪ retenção

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção C: Escolha e Consentimento	
8	Quando for aplicável, o fornecedor deve obter e registrar o consentimento do Titular de Dados para todas suas atividades de Processamento (o que inclui quaisquer atividades de Processamento novas e atualizadas) antes de coletar os Dados Pessoais desse Titular de Dados. O fornecedor monitora a eficácia da gestão de preferências para garantir que o prazo para honrar uma mudança de preferência seja o requisito legal local mais restritivo que se aplica ao caso.	O fornecedor pode demonstrar como um Titular de Dados fornece consentimento para uma atividade de Processamento e que o escopo do consentimento abrange todas as atividades de Processamento do fornecedor em relação aos Dados Pessoais desse Titular de Dados. O fornecedor pode demonstrar como um Titular de Dados consegue retirar o consentimento para uma atividade de Processamento. O fornecedor pode demonstrar como as preferências são verificadas antes do lançamento de uma nova atividade de Processamento. Observação: As provas podem ser capturas de tela de interação do usuário; experimentação com o serviço ou uma oportunidade de visualizar a documentação técnica.
9	Os fornecedores que criam e gerenciam sites da Microsoft ou aplicativos ou sites que carregam a marca da Microsoft devem fornecer aos Titulares de Dados um aviso e opções de escolha transparente sobre o uso de cookies, de acordo com os compromissos na Declaração de Privacidade da Microsoft e os requisitos legais locais. Salvo solicitação específica contrária da unidade de negócios contratante, os fornecedores devem usar o Banner Padrão produzido pela 1ES para gerenciar os controles de escolha. Esse requisito se aplica quando os sites são direcionados a usuários na União Europeia/Espaço Econômico Europeu e outras regiões com leis de privacidade aplicáveis e onde quer que a Declaração de Privacidade da Microsoft seja usada. Observação: Os solicitantes de negócios da Microsoft devem registrar os sites da Microsoft no portal interno de Compliance da Web (http://aka.ms/wcp) para que o inventário de cookies seja catalogado e gerenciado.	A finalidade de cada cookie deve ser documentada e deve informar o tipo de cookie implementado. ▪ Não devem ser usados cookies persistentes quando os cookies de sessão forem suficientes. ▪ Quando são usados cookies persistentes, eles não devem ter uma data de validade que exceda 13 meses após a visita do usuário ao site. Validar a conformidade com as leis da UE, conforme aplicável, como: ▪ uso da convenção de rotulagem, “Privacidade e Cookies” para a declaração de privacidade; ▪ consentimento afirmativo do usuário antes do uso de cookies para fins “não essenciais”, como publicidade; ▪ o consentimento deve expirar ou ser obtido novamente a cada 6 meses, no máximo.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção D: Coleta	
10	O fornecedor deve monitorar a coleta de Dados Pessoais ou Confidenciais da Microsoft para garantir que os únicos dados coletados sejam os necessários para a Prestação de Serviços.	O fornecedor pode apresentar documentação que mostre que os Dados Pessoais ou Confidenciais da Microsoft que foram coletados são necessários para a Prestação de Serviços. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.
11	Antes de coletar dados de crianças (conforme definido pela jurisdição aplicável), o fornecedor deve obter o consentimento de acordo com as leis de privacidade locais.	O fornecedor pode apresentar documentação que demonstre o consentimento dos pais/responsáveis. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.
	Seção E: Retenção	
12	Garantir que os Dados Pessoais e Confidenciais da Microsoft sejam retidos por não mais do que o necessário para a Prestação de Serviços, a menos que a retenção continuada dos Dados Pessoais ou Confidenciais da Microsoft seja exigida por lei.	O fornecedor cumpre as políticas de retenção documentadas ou os requisitos de retenção especificados pela Microsoft no contrato (por exemplo: declaração de trabalho, ordem de compra). O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.
13	Garantir que, a critério exclusivo da Microsoft, os Dados Pessoais e Confidenciais da Microsoft em posse do fornecedor ou sob seu controle sejam devolvidos à Microsoft ou destruídos após a conclusão da Prestação de Serviços ou mediante solicitação da Microsoft. Nos aplicativos, os processos devem estar em vigor para garantir que, quando os dados forem removidos do aplicativo explicitamente pelos usuários ou com base em outros acionadores, como a idade dos dados, eles sejam excluídos de forma segura. Quando for necessária a destruição de Dados Pessoais ou Confidenciais da Microsoft, o fornecedor deverá queimar, pulverizar ou triturar ativos físicos que contenham Dados Pessoais ou Confidenciais da Microsoft para que as informações não possam ser lidas ou reconstruídas.	Manter um registro da disposição dos Dados Pessoais e Confidenciais da Microsoft (isso pode incluir a devolução à Microsoft para destruição). Se a destruição for exigida ou solicitada pela Microsoft, fornecer um certificado de destruição assinado por um funcionário do fornecedor.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção F: Titulares de Dados	
	Os Titulares de Dados têm certos direitos sob a Lei, incluindo o direito de acessar, excluir, editar, exportar, restringir e refutar o Processamento de seus Dados Pessoais ("**Direitos do Titular de Dados**"). Quando um Titular de Dados procura exercer seus direitos de acordo com a Lei, em relação a seus Dados Pessoais da Microsoft, o fornecedor deve permitir que a Microsoft o faça ou desempenhe essas ações em nome da Microsoft:	
14	Auxiliar a Microsoft, por meio de medidas técnicas e organizacionais apropriadas, sempre que possível, a cumprir suas obrigações de responder a solicitações de Titulares de Dados que buscam exercer seus Direitos de Titular de Dados sem demora injustificada. A menos que indicado de outra forma pela Microsoft, o fornecedor encaminhará todos os Titulares de Dados que entrarem em contato com o fornecedor diretamente à Microsoft para exercer seus Direitos de Titular de Dados.	O fornecedor manterá provas de processos e procedimentos documentados para apoiar a execução dos Direitos de Titular de Dados. O fornecedor manterá provas documentadas de testes. As provas estarão disponíveis mediante solicitação da Microsoft.
15	Ao responder diretamente ao Titular de Dados ou quando o fornecedor apresentar um mecanismo online de autoatendimento, o fornecedor possui processos e procedimentos em vigor para identificar o Titular de Dados que faz a solicitação.	O fornecedor documentou o método usado para identificar os Titulares de Dados da Microsoft. O fornecedor apresentará provas documentadas à Microsoft mediante solicitação.
16	Caso a Microsoft solicite a localização de Dados Pessoais da Microsoft sobre um Titular de Dados que não esteja disponível por meio de um mecanismo online de autoatendimento, o fornecedor fará um esforço razoável para localizar os dados solicitados e manterá registros suficientes para demonstrar que foi feita uma pesquisa razoável.	O fornecedor manterá provas documentadas de quais são os procedimentos em vigor para estabelecer se os Dados Pessoais da Microsoft estão sendo mantidos e fornecerá documentação à Microsoft mediante solicitação. O fornecedor mantém um registro para demostrar as etapas tomadas para atender às solicitações de Direitos do Titular de Dados. A documentação inclui: ▪ data e hora do pedido; ▪ medidas tomadas para responder à solicitação e registro de quando a Microsoft foi informada. O fornecedor apresentará provas de manutenção de registros à Microsoft mediante solicitação.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção F: Titulares de Dados (cont.)	
17	O fornecedor comunicará ao Titular de Dados as etapas que essa pessoa deve seguir para acessar ou exercer seus direitos em relação aos Dados Pessoais da Microsoft.	O fornecedor manterá provas documentadas das comunicações e dos procedimentos para acesso aos Dados Pessoais da Microsoft. O fornecedor manterá provas documentadas e fornecerá as mesmas provas à Microsoft mediante solicitação.
18	Registrar a data e a hora das solicitações de Direitos do Titular de Dados e as medidas tomadas pelo fornecedor em resposta a tais solicitações. Se a solicitação for negada, por orientação da Microsoft, fornecer ao Titular de Dados uma explicação por escrito. Fornecer registros das solicitações do Titular de Dados à Microsoft mediante solicitação.	O fornecedor mantém registros de solicitações de acesso/exclusão e alterações de documentos feitas nos Dados Pessoais da Microsoft. Documentar as instâncias em que as solicitações são negadas e reter provas de revisão e aprovação da Microsoft. O fornecedor apresentará provas de manutenção dos registros de solicitações e recusas de acesso aos Dados Pessoais da Microsoft.
19	O fornecedor deve habilitar a Microsoft ou obter uma cópia dos Dados Pessoais da Microsoft solicitados para o Titular de Dados autenticado em um formato impresso, eletrônico ou verbal apropriado.	O fornecedor apresenta Dados Pessoais da Microsoft ao Titular de Dados em um formato compreensível e conveniente para o Titular de Dados e para o fornecedor.
20	O fornecedor deve tomar precauções razoáveis para garantir que os Dados Pessoais da Microsoft divulgados à Microsoft ou a um Titular de Dados autenticado não possam ser usados para identificar outra pessoa.	O fornecedor manterá provas documentadas dos procedimentos relacionados às precauções para evitar a identificação do Titular de Dados contrário aos termos do Contrato. O fornecedor apresentará provas documentais à Microsoft mediante solicitação.
21	Se um Titular de Dados acreditar que seus Dados Pessoais da Microsoft não estão completos nem são precisos, o fornecedor deverá encaminhar o assunto para a Microsoft e cooperar com a Microsoft conforme necessário para resolver o problema.	O fornecedor documenta os casos de divergência e encaminha o problema para a Microsoft. O fornecedor apresentará à Microsoft provas documentais mediante solicitação.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção G: Subcontratados	
	Se o fornecedor pretender usar um subcontratado para Processar Dados Pessoais ou Confidenciais da Microsoft, o fornecedor deverá:	
22	Notificar a Microsoft antes de subcontratar serviços ou fazer quaisquer alterações relativas à adição ou à substituição de subcontratados. Observação: Indicar sua aceitação desta obrigação mesmo que você não contrate subcontratados atualmente, mas possa fazê-lo no futuro.	Validar que os Dados Pessoais da Microsoft sejam Processados apenas por empresas conhecidas pela Microsoft conforme exigido no contrato aplicável (por exemplo: declaração de trabalho, adendo, ordem de compra) ou capturados no banco de dados do SSPA. O fornecedor pode publicar sua lista de subcontratados online e incluir um link para a página no banco de dados do SSPA.
23	Documentar a natureza e a extensão dos Dados Pessoais e Confidenciais da Microsoft Subprocessados por subcontratados, garantindo que as informações coletadas sejam necessárias para a Prestação de Serviços.	O fornecedor mantém a documentação relativa aos Dados Pessoais e Confidenciais da Microsoft divulgados ou transferidos para os subcontratados. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.
24	Quando a Microsoft for controlador de Dados Pessoais da Microsoft, garantir que o subcontratado use os Dados Pessoais da Microsoft de acordo com as preferências de contato declaradas pelo Titular de Dados.	Demonstrar como uma preferência do Titular de Dados da Microsoft é utilizada por subcontratados. Fornecer documentação de suporte (por exemplo: captura de tela, SLA, SOW, etc.) que inclua o prazo para um subcontratado honrar uma alteração de preferência.
25	Limitar o Processamento de Dados Pessoais ou Confidenciais da Microsoft pelo subcontratado aos fins necessários para cumprir o contrato do fornecedor com a Microsoft.	O fornecedor pode apresentar documentação que mostre que os Dados Pessoais da Microsoft fornecidos a um subcontratado são necessários para a Prestação de Serviços. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.
26	Analisar as reclamações que indiquem qualquer Processamento não autorizado ou Ilegal de Dados Pessoais da Microsoft.	O fornecedor pode demonstrar que existem sistemas e processos para tratar reclamações relacionadas ao uso não autorizado ou à divulgação de Dados Pessoais da Microsoft por um subcontratado. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção G: Subcontratados (cont.)	
27	Notificar a Microsoft imediatamente ao saber que um subcontratado Processou Dados Pessoais ou Confidenciais da Microsoft para qualquer finalidade diferente daquelas relacionadas à Prestação de Serviços.	O fornecedor apresentou as instruções e os meios para um subcontratado relatar o uso indevido dos dados da Microsoft. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.
28	Se o fornecedor coletar Dados Pessoais de terceiros em nome da Microsoft, o fornecedor deverá validar se as políticas e as práticas de proteção de dados de terceiros são consistentes com o contrato do fornecedor com a Microsoft e os DPR.	O fornecedor pode apresentar documentação da devida diligência realizada em relação às políticas e às práticas de proteção de dados de terceiros. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.
29	Tomar medidas imediatas para mitigar qualquer dano real ou potencial causado pelo Processamento não autorizado ou Ilegal de Dados Pessoais e Confidenciais da Microsoft por parte de um subcontratado.	O fornecedor deve manter provas documentais do plano e dos procedimentos e fornecer provas da documentação à Microsoft mediante solicitação.
	Seção H: Qualidade	
30	O fornecedor deve manter a integridade de todos os Dados Pessoais da Microsoft e garantir que permaneçam precisos, completos e relevantes para os propósitos declarados para os quais foram Processados.	O fornecedor pode demonstrar que existem procedimentos para validar os Dados Pessoais da Microsoft quando eles são coletados, criados e atualizados. O fornecedor pode demonstrar que os procedimentos de monitoramento e amostragem estão em vigor para verificar a precisão continuamente e fazer correções, conforme necessário. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção I: Monitoramento e Execução	
31	O fornecedor tem um plano de resposta a incidentes que exige que ele notifique a Microsoft de acordo com os requisitos contratuais ou sem atrasos indevidos, o que ocorrer primeiro, ao tomar conhecimento de um Incidente de Dados. O fornecedor deve, a pedido ou orientação da Microsoft, cooperar com a Microsoft em qualquer investigação, mitigação ou remediação do Incidente, o que inclui fornecer à Microsoft dados, informações, acesso ao pessoal do fornecedor ou hardware necessário para realizar uma análise forense. Observação: Consulte o Guia do Programa SSPA para saber como notificar a Microsoft sobre um incidente.	O fornecedor tem um plano de resposta a incidentes que inclui uma etapa para notificar os clientes (Microsoft), conforme descrito nesta seção. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.
32	Implementar um plano de remediação e monitorar a resolução de cada Incidente de Dados para garantir a aplicação oportuna de medidas corretivas apropriadas.	O fornecedor tem procedimentos documentados que serão necessários para responder a um Incidente de Dados até o seu encerramento. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.
33	Quando a Microsoft for controlador de Dados Pessoais da Microsoft, estabelecer um processo formal para responder a todas as reclamações sobre proteção de dados que envolvam Dados Pessoais da Microsoft.	O fornecedor tem meios para receber reclamações relacionadas com os Dados Pessoais da Microsoft e possui um procedimento documentado para tratar as reclamações. O fornecedor oferecerá provas documentais à Microsoft mediante solicitação.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção J: Segurança	
	O fornecedor deve estabelecer, implementar e manter um programa de segurança de informações que inclua políticas e procedimentos para proteger e manter seguros os Dados Pessoais e Confidenciais da Microsoft, de acordo com as boas práticas do setor e conforme exigido por lei. O programa de segurança do fornecedor deve atender aos padrões capturados abaixo, requisitos 34-50.	Uma Certificação ISO 27001 válida é um substituto aceitável para a Seção J. Entre em contato com a SSPA para solicitar esta substituição. Observação: Você precisará fornecer a certificação.
34	Realizar avaliações anuais de segurança de rede que incluam: ▪ revisão das principais alterações no ambiente, como um novo componente do sistema, topologia de rede, regras de firewall; ▪ varreduras de vulnerabilidades; ▪ manutenção de registros de alterações.	O fornecedor documentou avaliações de rede, registros de alterações e resultados de varredura. Os registros de alterações necessários devem rastrear as alterações, fornecer informações sobre o motivo da alteração e incluir o nome e o cargo do aprovador designado.
35	O fornecedor deve definir, comunicar e implementar uma política de dispositivo móvel que proteja e limite o uso de Dados Pessoais ou Confidenciais da Microsoft acessados ou usados em um dispositivo móvel.	O fornecedor demonstra o uso de uma política de dispositivo móvel compatível quando o Processamento de Dados Pessoais ou Confidenciais da Microsoft requer o uso de um dispositivo móvel.
36	Todos os ativos usados para dar suporte à Prestação de Serviços devem ser contabilizados e ter um proprietário identificado. O fornecedor é responsável por manter um inventário desses ativos de informações, estabelecer o uso aceitável e autorizado dos ativos e fornecer o nível adequado de proteção para os ativos ao longo de seu ciclo de vida.	Inventário de ativos de dispositivos usados para dar suporte à Prestação de Serviços. O inventário desses ativos deve incluir: ▪ localização do dispositivo; ▪ classificação dos dados sobre o ativo; ▪ registro de recuperação de ativos em caso de rescisão de contrato de trabalho ou de negócios; ▪ registro de eliminação de mídia de armazenamento de dados quando não for mais necessário.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção J: Segurança (cont.)	
37	Estabelecer e manter procedimentos de gerenciamento de direitos de acesso para impedir o acesso não autorizado a quaisquer Dados Pessoais ou Confidenciais da Microsoft sob controle do fornecedor.	O fornecedor demonstra que implementou um plano de gerenciamento de direitos de acesso que inclui: ▪ procedimentos de controle de acesso; ▪ procedimentos de identificação; ▪ procedimentos de bloqueio após tentativas mal sucedidas; ▪ parâmetros robustos para selecionar credenciais de autenticação; ▪ desativação das contas de usuários após 48 horas da rescisão do contrato de trabalho; ▪ controles de senha fortes que reforçam o comprimento e a complexidade da senha e evitam a reutilização. O fornecedor demonstra que possui um processo estabelecido para revisar o acesso do usuário a Dados Pessoais e Confidenciais da Microsoft, aplicando o princípio do privilégio mínimo. O processo inclui: ▪ funções de usuário claramente definidas; ▪ procedimentos para revisar e justificar a aprovação de acesso à funções; ▪ testar que os usuários em funções com acesso a dados da Microsoft tenham uma justificativa documentada para estar no grupo/função.
38	Definir e implementar procedimentos de gerenciamento de patches que priorizem patches de segurança para sistemas usados para Processar Dados Pessoais ou Confidenciais da Microsoft. Esses procedimentos incluem: ▪ abordagem de risco definida para priorizar patches de segurança; ▪ capacidade de processar e implementar patches de emergência; ▪ aplicabilidade ao sistema operacional e ao software de servidor, como servidor de aplicativos e software de banco de dados; ▪ documentação do risco que o patch mitiga e rastreio de quaisquer exceções; ▪ requisitos para a desativação de software que não é mais suportado pela empresa de autoria.	O fornecedor pode demonstrar um procedimento de gerenciamento de patches implementado que atenda a esse requisito e cubra, no mínimo, o seguinte: ▪ Definição de gravidade para informar a priorização. (As definições de gravidade são documentadas.) ▪ Procedimento documentado para implementar patches de emergência. ▪ Validação, não há uso de sistemas operacionais que não são mais suportados pela empresa de autoria. ▪ Registros de gerenciamento de patches que rastreiam aprovações e exceções.

#	Requisitos de Proteção de Dados dos fornecedores da Microsoft	Provas de conformidade
	Seção J: Segurança (cont.)	
39	Instalar software antivírus e antimalware em equipamentos conectados à rede usados para Processar Dados Pessoais e Confidenciais da Microsoft, incluindo servidores, desktops de produção e treinamento para proteção contra vírus potencialmente prejudiciais e aplicativos de software malicioso. Atualizar as definições de antimalware diariamente ou conforme indicado pelo fornecedor de antivírus/antimalware. Observação: Isso se aplica a todos os sistemas operacionais, incluindo o Linux.	Existem registros para mostrar que o uso de software antivírus e antimalware está ativo. Observação: Este requisito se aplica a todos os sistemas operacionais.
40	Os fornecedores que desenvolvem software para a Microsoft devem incorporar princípios de segurança por design no processo de criação.	Os documentos de especificações técnicas do fornecedor incluem pontos de verificação para validação de segurança em seus ciclos de desenvolvimento.
41	Implementar um programa de prevenção contra perda de dados (“ **DLP** ”) para evitar invasões, perdas e outras atividades não autorizadas. Os dados devem estar devidamente classificados, rotulados e protegidos, e o fornecedor deve monitorar os sistemas de informação que estejam em uso onde os Dados Pessoais ou Confidenciais da Microsoft são Processados quanto a intrusões, perdas e outras atividades não autorizadas. O programa DLP, no mínimo: ▪ requer o uso de sistemas de detecção de intrusão (“**IDS**”) baseados em nuvem, de rede e de host padrão do setor se você reter Dados Pessoais ou Confidenciais da Microsoft; ▪ requer a implementação de sistemas de proteção contra intrusões (“**IPS**”) avançados, configurados para monitorar e interromper ativamente a perda de dados; ▪ caso um sistema seja violado, requer a análise do sistema para garantir que quaisquer vulnerabilidades residuais também sejam abordadas; ▪ descreve os procedimentos necessários para monitorar as ferramentas de detecção de comprometimento do sistema; ▪ estabelece um processo de resposta e gestão de incidentes que deve ser executado quando é detectado um incidente de dados; ▪ requer comunicações (a todos os funcionários e subcontratados do fornecedor que estão sendo excluídos da Prestação de Serviços do fornecedor) sobre o download e o uso não autorizado de Dados Pessoais ou Confidenciais da Microsoft.	Um programa DLP documentado implementado com procedimentos para evitar intrusões, perdas e outras atividades não autorizadas (e, no mínimo, todos os itens especificados nesta seção).

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção J: Segurança (cont.)	
42	Comunicar imediatamente os resultados da investigação da resposta a incidentes à alta administração e à Microsoft.	Devem estar implementados sistemas e processos para comunicar os resultados da investigação da resposta a incidentes à Microsoft.
43	Os administradores de sistemas, a equipe de operações, a gerência e terceiros devem receber um treinamento anual de segurança.	Estabelecer um programa de treinamento de segurança que inclua: ▪ treinamento anual sobre a resposta a incidentes; ▪ eventos simulados e mecanismos automatizados para facilitar uma resposta eficaz a situações de crise; ▪ conscientização sobre a prevenção de incidentes, como riscos associados ao download de software malicioso.
44	O fornecedor deve garantir que os processos de planejamento de backup protejam os Dados Pessoais e Confidenciais da Microsoft contra o uso, o acesso, a divulgação, a alteração e a destruição não autorizados.	O fornecedor pode demonstrar procedimentos documentados de resposta e recuperação, que incluam pormenores sobre como a organização gerenciará um evento disruptivo e manterá a segurança de informações em um nível predeterminado com base em objetivos de continuidade de segurança de informações aprovados pela administração. O fornecedor pode demonstrar que definiu e implementou procedimentos para fazer backup periodicamente, armazenar com segurança e recuperar dados críticos com eficiência.
45	Estabelecer e testar planos de continuidade do negócio e de recuperação após desastres.	Um plano de recuperação após desastres deve incluir o seguinte: ▪ Critérios definidos para determinar se um sistema é crítico para a operação do negócio do fornecedor. ▪ Lista dos sistemas críticos com base nos critérios definidos que devem ser direcionados para recuperação em caso de desastre. ▪ Procedimento de recuperação após desastres definido para cada sistema crítico que garante que um engenheiro que não conhece o sistema possa recuperar o aplicativo em menos de 72 horas. ▪ Teste e revisão anuais (ou mais frequente) dos planos de recuperação após desastres para garantir que os objetivos de recuperação possam ser alcançados.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção J: Segurança (cont.)	
46	Autenticar a identidade de um indivíduo antes de lhe conceder acesso a Dados Pessoais ou Confidenciais da Microsoft e garantir que o acesso seja limitado ao escopo de atividade do indivíduo específico a quem foi permitido dar suporte à Prestação de Serviços.	Garantir que todos os ID de usuário sejam exclusivos e que cada um tenha um método de autenticação padrão do setor, como o Azure Active Directory. O acesso elevado (administrativo ou outros tipos de privilégios aprimorados) deve exigir o uso de um segundo fator, como um cartão inteligente ou um autenticador baseado em telefone. Programa documentado de segurança de informações que abrange o processo para garantir que o acesso de todos os funcionários e subcontratados do fornecedor a Dados Pessoais ou Confidenciais da Microsoft não seja maior ou mais longo do que o necessário para dar suporte à Prestação de Serviços.
47	O fornecedor deve proteger todos os dados Processados em conexão com sua Prestação de Serviços em trânsito através de redes com criptografia usando Transport Layer Security ("**TLS**") ou Internet Protocol Security ("**IPsec**"). Esses métodos são descritos no NIST 800-52 e no NIST 800-57; também é possível utilizar um padrão do setor equivalente. O fornecedor deve recusar a entrega de quaisquer Dados Pessoais ou Confidenciais da Microsoft transmitidos por meios não criptografados.	O processo de criação, implantação e substituição de TLS ou de outros certificados deve ser definido e aplicado.
48	Todos os dispositivos do fornecedor (laptops, estações de trabalho, etc.) que acessarão ou processarão Dados Pessoais ou Confidenciais da Microsoft devem utilizar criptografia baseada em disco.	Criptografar todos os dispositivos para atender a BitLocker ou outra solução de criptografia de disco equivalente do setor em todos os dispositivos clientes usados para processar Dados Pessoais ou Confidenciais da Microsoft.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Provas de Conformidade
	Seção J: Segurança (cont.)	
49	Devem estar em vigor sistemas e procedimentos (que sigam os padrões atuais do setor, como os descritos no padrão **NIST 800-111**) para criptografar em repouso (quando armazenados) todos e quaisquer Dados Pessoais ou Confidenciais da Microsoft; os exemplos incluem, mas não estão limitados a: ▪ dados de credenciais (por exemplo: nome de usuário/senhas); ▪ dados do instrumento de pagamento (por exemplo: números de cartão de crédito e contas bancárias); ▪ dados pessoais relacionados com a imigração; ▪ dados de perfil médico (por exemplo: números de registros médicos ou marcadores ou identificadores biométricos, como DNA, impressões digitais, retinas e íris dos olhos, padrões de voz, padrões faciais e medições de mãos usados para fins de autenticação); ▪ dados de identificação emitidos pelo governo (por exemplo: números de CPF ou carteira de motorista); ▪ dados pertencentes a ferramenta/clientess da Microsoft (por exemplo: SharePoint, documentos O365, clientes OneDrive); ▪ material relacionado a produtos Microsoft não anunciados; ▪ data de nascimento; ▪ informações de perfil de crianças; ▪ dados geográficos em tempo real; ▪ endereço físico pessoal (não comercial); ▪ números de telefone pessoais (não comerciais); ▪ religião; ▪ opiniões políticas; ▪ orientação/preferência sexual; ▪ respostas a perguntas de segurança (por exemplo: 2fa, redefinição de senha); ▪ nome de solteira da mãe.	Verificar se os Dados Pessoais e Confidenciais da Microsoft estão criptografados em repouso.
50	Anonimizar todos os Dados Pessoais da Microsoft usados em um ambiente de desenvolvimento ou teste.	Os Dados Pessoais da Microsoft não devem ser usados em ambientes de desenvolvimento ou teste; quando não houver alternativa, eles devem ser anonimizados para evitar a identificação dos Titulares de Dados ou o uso indevido dos Dados Pessoais. Observação: Os dados anonimizados são diferentes dos dados pseudonimizados. Os dados anonimizados são dados que não se relacionam com uma pessoa física identificada ou identificável em que o titular de dados pessoais não é ou deixou de ser identificável.

Glossário

“Cláusulas Modelo da UE” e “Cláusulas Contratuais Padrão” significam (i) as cláusulas padrão de proteção de dados para a transferência de dados pessoais para processadores estabelecidos em países terceiros que não garantem um nível adequado de proteção de dados, conforme descrito no Artigo 46 do GDPR e aprovado pela decisão da Comissão Europeia (UE) de 2021/914 de 4 de junho de 2021; (ii) as cláusulas contratuais padrão sucessoras adotadas (a) pela Comissão Europeia, (b) pela Autoridade Europeia para a Proteção de Dados e aprovadas pela Comissão Europeia, (c) pelo Reino Unido, de acordo com a Lei Federal Geral de Proteção de Dados do Reino Unido, (d) pela Suíça, de acordo com a Lei Federal de Proteção de Dados da Suíça, ou (e) por um governo em uma jurisdição que não seja a Suíça, o Reino Unido e as jurisdições que compõem a União Europeia/Espaço Econômico Europeu onde as cláusulas regem a transferência internacional de dados pessoais deverão ser incorporadas e vinculativas para o fornecedor a partir do dia de sua adoção.

“EUDPR” significa o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, sobre a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e sobre a livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE.

"Freelancer" se refere aos indivíduos que desempenham tarefas ou serviços sob demanda, que são adquiridos por meio de plataformas digitais ou outros meios.

“Hospedagem de Sites” Um serviço de hospedagem de sites é um serviço online que cria ou mantém sites em nome da Microsoft sob o domínio da Microsoft, ou seja, o fornecedor oferece todos os materiais e os serviços necessários para a criação e a manutenção de um site e o torna acessível na Internet. O “provedor de serviço de hospedagem na web” ou “web host” é o fornecedor que oferece as ferramentas e os serviços necessários para visualizar o site ou a página web na Internet, como Cookies ou web beacons para publicidade.

"GPDR" significa o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, sobre a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/EC (Regulamento Geral sobre a Proteção de Dados).

“Representante Autorizado” é uma pessoa que possui o nível apropriado de autoridade para assinar em nome da empresa. Essa pessoa deve ter os conhecimentos necessários de privacidade e segurança ou ter consultado um especialista no assunto antes de enviar sua resposta a uma ação do Programa SSPA. Além disso, ao adicionar seu nome a um formulário SSPA, eles estão certificando que leram e entenderam os DPR.

“Requisitos de Proteção de Dados de Privacidade” significa o GDPR, o EUDPR, as Leis Locais de Proteção de Dados da UE/EEE, a Lei de Privacidade do Consumidor da Califórnia, Cal. Código Civil § 1798.100 e segs. (“*CCPA*”), a Lei de Proteção de Dados do Reino Unido de 2018 e quaisquer leis, regulamentos e outros requisitos legais relacionados ou subsequentes aplicáveis no Reino Unido, e quaisquer leis, regulamentos e outros requisitos legais aplicáveis relacionados a (a) privacidade e segurança de dados; ou (b) o uso, a coleta, a retenção, o armazenamento, a segurança, a divulgação, a transferência, a eliminação e outros processamentos de quaisquer Dados Pessoais.