Requisitos de Proteção de Dados dos Fornecedores da Microsoft

Aplicabilidade

Os Requisitos de Proteção de Dados ("**RPD**") dos Fornecedores da Microsoft aplicam-se a cada um dos fornecedores da Microsoft que processem Dados Pessoais Microsoft ou Dados Confidenciais Microsoft relativamente ao desempenho desse fornecedor (por exemplo, prestação de serviços, licenças de software, serviços na nuvem) em conformidade com os termos do respetivo contrato com a Microsoft (por ex., termos de Nota de Encomenda, contrato principal) ("**Realização**," "**Rendimento**" ou "**Desempenho**").

- Em caso de conflito entre os RPD e os requisitos especificados nos acordos contratuais entre o fornecedor e a Microsoft, os RPD têm precedência, exceto quando o fornecedor identifique a disposição correta no contrato que se sobreponha ao requisito de proteção de dados aplicável (caso em que os termos do contrato têm precedência).
- Em caso de conflito entre os requisitos contidos neste documento e quaisquer requisitos legais ou estatutários, os requisitos legais ou estatutários têm precedência.
- Na eventualidade do fornecedor Microsoft operar como um Controlador, o fornecedor pode ter requisitos reduzidos no RDP.
- No caso de o fornecedor da Microsoft não processar dados pessoais da Microsoft, mas apenas dados confidenciais da Microsoft, com respeito a este RDP, o fornecedor poderá ter requisitos reduzidos.

Transferência internacional de dados

Sem limitar as suas outras obrigações, o fornecedor não qualquer transferência internacional de dados pessoais da Microsoft, exceto quando a Microsoft forneça a sua aprovação prévia por escrito, e em qualquer caso, o fornecedor deverá cumprir os Requisitos de Proteção de Dados, incluindo as Cláusulas Contratuais Padrão, ou, segundo o critério da Microsoft, outros mecanismos apropriados de transferência transfronteiriça aprovados por uma autoridade apropriada de proteção de dados ou pela Comissão Europeia, conforme o caso, e adotados ou acordados pela Microsoft. As cláusulas contratuais-tipo 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 nos termos da Lei Geral Federal de Proteção de Dados do Reino Unido, (iii) pela Suíça nos termos da 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 numa jurisdição que não a Suíça, o Reino Unido, e as jurisdições que compõem a União Europeia / Espaço Económico Europeu, serão incorporadas e vinculativas para o fornecedor a partir do dia da sua adoção. O fornecedor deverá também assegurar que todo e qualquer processador secundário (tal como definido nas Cláusulas Contratuais Padrão) também o cumpra.

Definições principais

Os seguintes termos utilizados neste RPD têm os seguintes significados. A lista de exemplos após "incluindo", "tais como", "por exemplo", "por ex.", ou similares utilizados ao longo deste RPD são interpretados para incluir "sem limitações", ou, "mas não limitados a" a menos que sejam qualificados por palavras tais como "apenas" ou "unicamente". Para obter mais definições, consulte o Glossário presente no final deste documento.

“**Responsável”** significa a entidade que determina os objetivos e meios do Processamento dos Dados Pessoais. "Responsável" inclui uma empresa, Responsável (tal como esse termo é definido no RGPD), e termos equivalentes nas Leis de Proteção de Dados, como exigido pelo contexto.

"**Cookies**" são pequenos ficheiros de texto armazenados em dispositivos por sítios web e/ou aplicações que contêm informações utilizadas para reconhecer um Sujeito de Dados ou um dispositivo.

"**Incidente de Dados**" significa (1) uma quebra de segurança que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a Dados Pessoais Microsoft ou Dados Confidenciais Microsoft transmitidos, armazenados ou processados de outra forma pelo fornecedor ou pelos seus Subcontratados, ou (2) vulnerabilidade de segurança relacionada com o tratamento de Dados Pessoais da Microsoft ou Dados Confidenciais da Microsoft pelo Fornecedor.

"**Titular dos dados**" significa uma pessoa singular identificável que pode ser identificada, direta ou indiretamente, nomeadamente através da referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online, ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

"**Direito do Titular dos Dados**" significa o direito do Titular dos Dados de aceder, apagar, editar, exportar, restringir, ou opor-se ao Processamento dos Dados Pessoais da Microsoft desse Titular dos Dados, se exigido por Lei.

"**Lei**" significa todas as leis, regras, estatutos, decretos, decisões, ordens, julgamentos, regulamentos, códigos, promulgações, resoluções e requisitos de qualquer autoridade governamental (federal, estatal, local ou internacional) tendo jurisdição. "**Ilícito**" significa qualquer violação da lei.

"**Dados Confidenciais da Microsoft**" é qualquer informação que, se comprometida através de meios de confidencialidade ou integridade, pode resultar numa perda significativa de reputação ou financeira para a Microsoft. Isto inclui produtos de hardware e software da Microsoft, aplicações de *line-of-business*, materiais de marketing de pré-lançamento, chaves de licença de produtos, e documentação técnica relacionada com produtos e serviços Microsoft.

"**Dados Pessoais da Microsoft**" significa quaisquer dados pessoais processados pela Microsoft ou em seu nome.

"**Dados Pessoais**" significa qualquer informação relativa a um Titular de Dados e qualquer outra informação que constitua "dados pessoais" ou "informações pessoais" ao abrigo da lei.

"**Processo**" significa qualquer operação ou conjunto de operações que seja realizada relativamente a quaisquer Dados Pessoais ou Dados Confidenciais da Microsoft, seja ou não por meios automatizados, tais como a recolha, registo, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição. "Processamento" e "Processado" terão os significados correspondentes.

"**Processador**" significa uma entidade que processa Dados Pessoais em nome de outra entidade e inclui o Provedor de Serviços, Processador (como esse termo é definido no RGPD), e termos equivalentes nas Leis de Proteção de Dados, conforme exigido pelo contexto.

"**Subcontratante**" significa um terceiro a quem o fornecedor delega as suas obrigações em relação ao contrato que cobre o respetivo Desempenho, incluindo uma filial do fornecedor que não seja contratado diretamente com a Microsoft.

"**Subprocessador**" significa um terceiro perante o qual a Microsoft se compromete a Efetuar, onde o Desempenho inclui o Processamento de Dados Pessoais da Microsoft para o qual a Microsoft é um Processador.

Resposta do fornecedor

Os fornecedores confirmam anualmente a conformidade relativamente a estes requisitos utilizando um serviço online administrado pela Microsoft. Consulte o Guia do Programa SSPA para compreender como é administrada a conformidade.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção A: Administração	
1	Cada acordo aplicável entre a Microsoft e o fornecedor (por exemplo, acordo principal, declaração de trabalho, notas de encomenda e outras notas) contém linguagem de proteção de dados pessoais e de segurança no que diz respeito aos Dados Pessoais e Confidenciais da Microsoft, conforme aplicável, incluindo proibições sobre a venda de Dados Pessoais da Microsoft e Processamento de Dados Pessoais da Microsoft fora da relação comercial direta entre a Microsoft e o fornecedor. Para as empresas que operam na qualidade de Processadores ou Subprocessadores em ligação com o Desempenho, no que diz respeito aos Dados Pessoais da Microsoft, o acordo deve incluir o objeto e a duração do Processamento, a natureza e a finalidade do Processamento, o tipo de Dados Pessoais da Microsoft e categorias dos Titulares dos Dados e as obrigações e direitos da Microsoft.	O fornecedor deve apresentar o contrato aplicável entre a Microsoft e o fornecedor. Para Processadores e Subprocessadores, as descrições de Processamento encontram-se contidas no acordo aplicável (por exemplo, declaração de trabalho, notas de encomenda). Nota: As empresas com notas de encomenda a bordo podem ter a descrição necessária das atividades de processamento adicionada mais tarde no decorrer do processo de compra.
2	Quando a Microsoft confirmar que os seus compromissos cumprem uma função de Subprocessador, o fornecedor deve possuir os acordos de proteção de dados aplicáveis em vigor junto da Microsoft. Nota: A Microsoft publicará esta designação no seu perfil quando aplicável.	Cláusulas Contratuais Padrão, Adenda de Dados de Clientes Online, e/ou Adenda de Processamento de Dados de fornecedores e Serviços Profissionais de Parceiros.
3	Atribuir responsabilidade e responsabilização pelo cumprimento do RPD a uma pessoa ou grupo designado dentro da empresa.	Indicar a função da pessoa ou grupo encarregue de assegurar o cumprimento do RPD do fornecedor da Microsoft. Um documento que descreva a autoridade e responsabilidade desta pessoa ou grupo que demonstra um papel de privacidade e/ou segurança.
4	Estabelecer, manter e realizar formação anual sobre privacidade e segurança para os colaboradores que terão acesso aos Dados Pessoais Processados pelo fornecedor relativamente à ligação com o Desempenho ou os Dados Confidenciais da Microsoft. Se a sua empresa não tiver conteúdo preparado, pode utilizar este guia e adaptá-lo à sua empresa. Nota: Os colaboradores do fornecedor podem ser obrigados a completar formações adicionais fornecidas pelas divisões da Microsoft.	Os registos anuais de assiduidade encontram-se disponíveis e podem ser fornecidos à Microsoft mediante pedido. O conteúdo da formação inclui princípios relacionados com a privacidade e segurança. A documentação de conformidade com os requisitos de formação incluirá provas de formação relacionada com requisitos regulamentares de privacidade, obrigações de segurança, e conformidade com os requisitos e obrigações contratuais aplicáveis.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção A: Administração (continuação)	
5	Processar Dados Pessoais da Microsoft apenas em conformidade com as instruções documentadas da Microsoft, incluindo cenários relativos a transferências de Dados Pessoais da Microsoft para um país terceiro ou uma organização internacional, exceto quando tal seja exigido por lei; nesse caso, o Processador ou Subprocessador (fornecedor) informará o responsável pelo tratamento (Microsoft) desse requisito legal antes do Processamento, a menos que essa lei proíba tais informações por motivos importantes de interesse público.	O fornecedor compila e mantém todas as instruções documentadas da Microsoft (por ex., acordo, declaração de trabalho ou documentação de encomenda) eletronicamente, num local facilmente acessível aos funcionários e contratantes do fornecedor que participam no Desempenho.
	Secção B: Aviso	
6	O fornecedor deve utilizar a Declaração de Privacidade da Microsoft ao recolher Dados Pessoais em nome da Microsoft. O aviso de privacidade deve ser óbvio e estar disponível para os Titulares dos Dados para os ajudar a decidir se devem, ou não, submeter os seus Dados Pessoais ao fornecedor. Nota: Quando a sua empresa é o Controlador da Atividade de Processamento, afixaria o seu próprio aviso de privacidade.	O fornecedor utiliza uma fwdlink para a Declaração de Privacidade da Microsoft atual e publicada. A Declaração de Privacidade é publicada em qualquer contexto onde os Dados Pessoais de um utilizador serão recolhidos. Se aplicável, encontra-se disponível uma versão offline, que é fornecida antes da recolha de dados. Quaisquer Declarações de Privacidade offline utilizadas são a versão mais recente, publicada e encontram-se datadas corretamente. Para os serviços de funcionários da Microsoft, é utilizado o Aviso de Privacidade de Dados da Microsoft.
7	Ao recolher dados pessoais da Microsoft através de uma chamada de voz em tempo real ou gravada, os fornecedores devem estar preparados para discutir as práticas aplicáveis de recolha, tratamento, utilização e retenção de dados com os Titulares dos Dados.	Um guião para gravações de voz inclui a forma como os Dados Pessoais da Microsoft são processados, e inclui: ▪ a recolha, ▪ utilização e ▪ retenção

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção C: Escolha e consentimento	
8	Quando aplicável, o fornecedor deve obter e registar o consentimento do Titular dos Dados para todas as suas atividades de Processamento (incluindo quaisquer atividades de Processamento novas e atualizadas) antes de recolher os Dados Pessoais do Titular dos Dados. O fornecedor monitoriza a eficácia da gestão de preferências para assegurar que o prazo para honrar uma mudança de preferência é o requisito legal local mais restritivo aplicável.	O fornecedor pode demonstrar a forma como o Titular dos Dados confere o consentimento para uma atividade de Processamento e que o âmbito do consentimento abrange todas as atividades de Processamento de Dados do fornecedor no que diz respeito aos Dados Pessoais do titular dos Dados. O fornecedor pode demonstrar a forma como um Titular dos Dados retira 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. Nota: As provas podem ser capturas de ecrã de interação do utilizador; experimentação com o serviço ou uma oportunidade de visualizar documentação técnica.
9	Os fornecedores que criam e gerem sítios web e/ou aplicações Microsoft ou sites que ostentam a marca Microsoft têm de fornecer aos Titulares de Dados aviso e escolha transparentes relativamente à utilização de cookies em conformidade com os compromissos assumidos na Declaração de Privacidade da Microsoft e com os requisitos legais locais. Exceto quando especificamente solicitado pela unidade de negócios contratante, os fornecedores devem utilizar o Banner Padrão produzido pelo 1ES para gerir os controlos de escolha. Este requisito aplica-se quando os sites se destinam a utilizadores dentro da União Europeia/Espaço Económico Europeu e outras regiões com leis de privacidade aplicáveis e onde quer que a Declaração de Privacidade da Microsoft seja utilizada. Nota: Os patrocinadores empresariais da Microsoft são obrigados a registar os sítios web da Microsoft no portal interno de Conformidade Web (http://aka.ms/wcp) para que o inventário de cookies seja catalogado e gerido.	A finalidade de cada cookie deve ser documentada e deve informar o tipo de cookie implementado. ▪ Os cookies persistentes não devem ser utilizados quando os cookies de sessão são suficientes. ▪ Quando são utilizados cookies persistentes, estes não devem ter uma data de validade que exceda 13 meses após um utilizador ter visitado o site. Validar a conformidade com a legislação da UE conforme aplicável, como por exemplo: ▪ utilização da convenção de rotulagem, "Privacidade e Cookies" para a declaração de privacidade, ▪ obter o consentimento afirmativo do utilizador antes da utilização de cookies "não essenciais" para fins tais como publicidade, e ▪ o consentimento deve expirar ou ser obtido novamente num período não inferior a 6 meses.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção D: Recolha	
10	O fornecedor deve monitorizar a recolha de Dados Pessoais e/ou Confidenciais da Microsoft para assegurar que os únicos dados recolhidos são os necessários para a Realização.	O fornecedor pode fornecer documentação que demonstre que os Dados Pessoais e/ou Confidenciais da Microsoft recolhidos são necessários para a Realização. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.
11	Antes de recolher dados de crianças (conforme definido pela jurisdição aplicável), o fornecedor deve obter o consentimento em conformidade com as leis locais de privacidade.	O fornecedor pode fornecer documentação que demonstre o consentimento dos pais/tutores. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.
	Secção E: Retenção	
12	Assegurar que os Dados Pessoais e Confidenciais da Microsoft não sejam retidos durante mais tempo do que o necessário para a sua Realização, exceto quando a retenção contínua dos Dados Pessoais e/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 ex., declaração de trabalho, nota de encomenda). O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.
13	Assegurar que, de acordo com o exclusivo critério da Microsoft, os Dados Pessoais e Confidenciais da Microsoft na posse do fornecedor ou sob o seu controlo sejam devolvidos à Microsoft ou destruídos após a conclusão do Desempenho ou a pedido da Microsoft. Dentro das aplicações, devem existir processos que garantam que, quando os dados são removidos da aplicação, quer explicitamente pelos utilizadores, quer com base noutros critérios como a idade dos dados, estes sejam eliminados de forma segura. Quando a destruição de Dados Pessoais ou Confidenciais da Microsoft é necessária, o fornecedor deve queimar, pulverizar, ou rasgar bens físicos contendo Dados Pessoais e/ou Confidenciais da Microsoft, para que a informação não possa ser lida ou reconstruída.	Manter um registo da disposição dos Dados Pessoais e Confidenciais da Microsoft (isto pode incluir a devolução à Microsoft para destruição). Se a destruição for requerida ou solicitada pela Microsoft, fornecer um certificado de destruição assinado por um responsável do fornecedor.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção F: Titulares dos dados	
	Os Titulares dos Dados têm determinados direitos ao abrigo da lei, incluindo o direito de acesso, eliminação, edição, exportação, restrição, e oposição ao Processamento dos seus Dados Pessoais ("**Direitos dos Titulares dos Dados**"). Quando um Titular dos Dados procura exercer os seus direitos ao abrigo da Lei relativamente aos seus Dados Pessoais da Microsoft, o fornecedor deve permitir à Microsoft fazer o seguinte ou executar estas ações em nome da Microsoft:	
14	Auxiliar a Microsoft, através de medidas técnicas e organizacionais adequadas, sempre que possível, a cumprir as suas obrigações de resposta aos pedidos de Titulares dos Dados que procuram exercer os seus Direitos enquanto Titulares dos Dados sem atrasos indevidos. Salvo instruções em contrário da Microsoft, o fornecedor encaminhará todos os Titulares dos Dados que contactarem diretamente o fornecedor para exercer os seus Direitos enquanto Titulares dos Dados.	O fornecedor manterá provas de processos e procedimentos documentados para apoiar a execução dos Direitos do Titular dos Dados. O fornecedor manterá evidências documentadas dos testes. As evidências serão disponibilizadas mediante pedido da Microsoft.
15	Ao responder diretamente ao Titular dos Dados ou quando o fornecedor fornece um mecanismo de autosserviço online, o fornecedor possui processos e procedimentos em vigor para identificar o Titular dos Dados que efetua o pedido.	O fornecedor documentou o método utilizado para identificar os Titulares dos Dados da Microsoft. O fornecedor fornecerá evidências documentais à Microsoft, mediante pedido.
16	Se solicitado pela Microsoft para localizar Dados Pessoais da Microsoft sobre um Titular dos Dados que não esteja disponível através de um mecanismo de autosserviço online, o fornecedor envidará um esforço razoável para localizar os dados solicitados e manter registos suficientes para demonstrar que foi realizada uma pesquisa razoável.	O fornecedor manterá evidências documentadas dos procedimentos em vigor para estabelecer se os Dados Pessoais da Microsoft estão a ser retidos e fornecerá documentação à Microsoft mediante pedido. O fornecedor mantém um registo demonstrativo das medidas tomadas para satisfazer os pedidos referentes ao Direito do Titular dos Dados. A documentação inclui: ▪ data e hora do pedido; ▪ ações efetuadas para dar resposta ao pedido, e registo de quando a Microsoft foi informada. O fornecedor fornecerá provas da manutenção de registos à Microsoft, mediante pedido.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção F: Titulares dos dados (cont.)	
17	O fornecedor comunicará ao Titular dos Dados as medidas que essa pessoa deve tomar para obter acesso ou exercer os seus direitos relativamente aos seus Dados Pessoais da Microsoft.	O fornecedor manterá provas documentadas das comunicações e dos procedimentos de acesso aos Dados Pessoais da Microsoft. O fornecedor manterá provas documentadas e fornecerá as mesmas à Microsoft mediante pedido.
18	Registar a data e hora dos pedidos de Direitos do Titular dos Dados e as ações tomadas pelo fornecedor em resposta a tais pedidos. Se o seu pedido for negado, sob indicação da Microsoft, fornecer ao Titular dos Dados uma explicação escrita. Fornecer registos à Microsoft, mediante pedido, dos pedidos do Titular dos Dados.	O fornecedor mantém os registos dos pedidos de acesso/apagamento e das alterações de documentos efetuadas aos Dados Pessoais da Microsoft. Documentar os casos em que os pedidos são recusados e reter provas da revisão e aprovação da Microsoft. O fornecedor fornecerá provas de manutenção de registos dos pedidos e das recusas de acesso aos Dados Pessoais da Microsoft.
19	O fornecedor deve permitir à Microsoft ou obter uma cópia dos Dados Pessoais da Microsoft solicitados para o Titular dos Dados autenticados num formato adequado, impresso, eletrónico ou verbal.	O fornecedor fornece os Dados Pessoais da Microsoft ao Titular dos Dados num formato compreensível e numa forma conveniente para o Titular dos Dados e para o fornecedor.
20	O fornecedor deve tomar precauções razoáveis para assegurar que os Dados Pessoais da Microsoft divulgados à Microsoft ou a um Titular dos Dados autenticado não possam ser utilizados para identificar outra pessoa.	O fornecedor manterá provas documentadas dos procedimentos relacionados com as precauções para evitar a identificação do Titular dos Dados contrária ao Acordo. O fornecedor fornecerá provas à Microsoft, mediante pedido.
21	Se um Titular dos Dados acreditar que os seus Dados Pessoais da Microsoft não se encontram completos e exatos, o fornecedor deve escalar a questão para a Microsoft e cooperar com esta, na medida do necessário, para solucionar o problema.	O fornecedor documenta os casos de desacordo e intensifica a questão para a Microsoft. O fornecedor fornecerá à Microsoft provas documentais, mediante pedido.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção G: Subcontratantes	
	Se o fornecedor pretender utilizar um subcontratante para processar Dados Pessoais ou Confidenciais da Microsoft, o fornecedor tem de:	
22	Notificar a Microsoft antes de subcontratar serviços ou efetuar quaisquer alterações relativas à adição ou substituição de subcontratantes. Nota: Indique a sua aceitação desta obrigação, mesmo que não contrate atualmente subcontratantes, mas poderá fazê-lo no futuro.	Validar que os Dados Pessoais da Microsoft são processados apenas por empresas conhecidas da Microsoft, conforme exigido no contrato aplicável (por ex., declaração de trabalho, adenda, nota de encomenda) ou capturados na base de dados SSPA. O fornecedor pode colocar a respetiva lista de subcontratados online e incluir uma ligação para a página na base de dados SSPA.
23	Documentar a natureza e extensão dos Dados Pessoais e Confidenciais Microsoft subprocessados por subcontratantes, assegurando que a informação recolhida é necessária para a Realização.	O fornecedor mantém documentação relativa aos Dados Pessoais e Confidenciais da Microsoft revelados ou transferidos para subcontratantes. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.
24	Se a Microsoft for um controlador de Dados Pessoais da Microsoft, este deve garantir que o subcontratante utiliza os Dados Pessoais da Microsoft em conformidade com as preferências de contacto declaradas pelo Titular dos Dados.	Demonstrar como é utilizada a preferência por um Titular dos Dados Microsoft pelos subcontratantes. Fornecer documentação de apoio (por ex., capturas de ecrãs, SLA, SOW, etc.) que inclua o prazo para um subcontratante honrar uma mudança de preferência.
25	Limitar o Processamento de Dados Pessoais ou Confidenciais Microsoft pelo subcontratante aos fins necessários para cumprir o contrato do fornecedor com a Microsoft.	O fornecedor pode fornecer documentação que demonstre que os Dados Pessoais da Microsoft fornecidos a um subcontratante são necessários para a Realização. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.
26	Analisar reclamações por indicações de qualquer processamento não autorizado ou ilegal de Dados Pessoais da Microsoft.	O fornecedor pode demonstrar que existem sistemas e processos para tratar de queixas relativas à utilização não autorizada ou divulgação de Dados Pessoais da Microsoft por um subcontratante. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção G: Subcontratantes (cont.)	
27	Notificar prontamente a Microsoft ao ter conhecimento que um subcontratante processou Dados Pessoais ou Confidenciais da Microsoft para qualquer outro fim que não os relacionados com o Desempenho.	O fornecedor forneceu as instruções e os meios para um subcontratante comunicar a má utilização dos dados da Microsoft. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.
28	Se o fornecedor recolher Dados Pessoais de terceiros em nome da Microsoft, o fornecedor deve validar que as políticas e práticas de proteção de dados de terceiros são consistentes com o contrato do fornecedor com a Microsoft e os RPD.	O fornecedor pode fornecer documentação sobre a devida diligência realizada relativamente às políticas e práticas de proteção de dados de terceiros. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.
29	Tomar imediatamente medidas para mitigar qualquer dano real ou potencial causado pelo processamento não autorizado ou ilegal de dados pessoais e confidenciais da Microsoft por um subcontratante.	O fornecedor deve manter provas documentais do plano e do procedimento e fornecer provas da documentação à Microsoft, mediante pedido.
	Secção H: Qualidade	
30	O fornecedor deve manter a integridade de todos os Dados Pessoais da Microsoft, assegurando que estes se mantêm exatos, completos e relevantes para os fins declarados para os quais foram processados.	O fornecedor pode demonstrar que existem procedimentos para validar os Dados Pessoais da Microsoft quando estes são recolhidos, criados e atualizados. O fornecedor pode demonstrar que se encontram em vigor procedimentos de monitorização e amostragem para verificar a exatidão numa base contínua e correta, conforme necessário. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção I: Monitorização e aplicação	
31	O fornecedor possui um plano de resposta a incidentes que exige que o fornecedor notifique a Microsoft por requisitos contratuais ou, sem atrasos indevidos, o que ocorrer primeiro, ao tomar conhecimento de um Incidente de Dados. O fornecedor deve, mediante pedido ou indicação da Microsoft, cooperar com a Microsoft em qualquer investigação, mitigação ou reparação do Incidente, incluindo o fornecimento à Microsoft de dados, informações, acesso aos colaboradores do fornecedor, ou ao hardware necessário para realizar uma análise forense. Nota: Consulte o Guia do Programa SSPA para saber como notificar a Microsoft de um incidente.	O fornecedor possui um plano de resposta a incidentes que inclui um passo para notificar os clientes (Microsoft), conforme descrito nesta secção. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.
32	Implementar um plano de mitigação e monitorizar a resolução de cada Incidente de Dados para assegurar que sejam tomadas as medidas corretivas adequadas em tempo oportuno.	O fornecedor dispõe de procedimentos documentados que tomará para responder a um Incidente de Dados até ao respetivo encerramento. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.
33	Quando a Microsoft é um responsável pelos Dados Pessoais da Microsoft, estabelecer um processo formal de reclamação para dar resposta a todas as reclamações sobre proteção de dados envolvendo Dados Pessoais da Microsoft.	O fornecedor possui os meios para receber reclamações que envolvem Dados Pessoais da Microsoft e possui um procedimento documentado de reclamações para tratar as mesmas. O fornecedor fornecerá provas documentais à Microsoft, mediante pedido.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção J: Segurança	
	O fornecedor deve estabelecer, implementar e manter um programa de segurança da informação que inclua políticas e procedimentos, para proteger e manter seguros os Dados Pessoais e Confidenciais da Microsoft, em conformidade com as boas práticas do setor e conforme exigido por Lei. O programa de segurança do fornecedor deve cumprir as normas capturadas abaixo, requisitos 34 a 50.	Uma certificação ISO 27001 válida é um substituto aceitável para a Secção J. Contacte a SSPA para aplicar esta substituição. Nota: Ser-lhe-á necessário fornecer a certificação.
34	Realizar avaliações anuais da segurança da rede que incluam: ▪ análise das principais alterações ao ambiente, tais como uma nova componente do sistema, topologia de rede, regras de firewall; ▪ realizar análises de vulnerabilidades; e ▪ manter registos de alterações.	O fornecedor tem possui de rede documentadas, registos de alterações e resultados de análises. Os registos de alterações necessários devem registar das alterações, fornecer informações sobre o motivo da alteração e incluir o nome e o título do autorizador designado.
35	O fornecedor deve definir, comunicar e implementar uma política de dispositivos móveis que proteja, e limite a utilização de Dados Pessoais ou Confidenciais da Microsoft acedidos ou utilizados num dispositivo móvel.	O fornecedor demonstra a utilização de uma política de dispositivos móveis em conformidade, quando o Processamento de Dados Pessoais ou Confidenciais da Microsoft necessitar da utilização de um dispositivo móvel.
36	Todos os ativos utilizados para apoiar o Desempenho devem ser contabilizados e ter um proprietário identificado. O fornecedor é responsável por manter um inventário destes ativos de informação; estabelecer uma utilização aceitável e autorizada dos ativos; e fornecer o nível apropriado de proteção dos ativos ao longo do seu ciclo de vida útil.	Inventário dos ativos de dispositivos utilizados para apoiar o Desempenho. O inventário destes ativos tem de incluir: ▪ a localização do dispositivo; ▪ a classificação de dados dos dados presentes no ativo; ▪ o registo da recuperação do ativo após a demissão do funcionário ou acordo de empresa; e ▪ registo da eliminação de suportes de armazenamento de dados quando estes já não são necessários.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção J: Segurança (cont.)	
37	Estabelecer e manter procedimentos de gestão de direitos de acesso para impedir o acesso não autorizado a quaisquer Dados Pessoais ou Confidenciais da Microsoft sob controlo do fornecedor.	O fornecedor demonstra ter implementado um plano de gestão de direitos de acesso que inclui: ▪ procedimentos de controlo de acesso; ▪ procedimentos de identificação; ▪ procedimentos de bloqueio após tentativas não sucedidas; ▪ parâmetros robustos para selecionar credenciais de autenticação; e ▪ desativação de contas de utilizadores aquando da cessação do emprego no espaço de 48 horas ▪ controlos robustos de palavras-passe que cumpram o comprimento e a complexidade das palavras-passe e impeçam a sua reutilização O fornecedor demonstra que possui um processo estabelecido para rever o acesso dos utilizadores aos Dados Pessoais e Confidenciais da Microsoft, impondo o princípio do privilégio mínimo. O processo inclui: ▪ funções de utilizador claramente definidas; ▪ procedimentos para analisar e justificar a aprovação do acesso às funções; e ▪ testar que os utilizadores dentro das funções com acesso aos dados da Microsoft possuem uma justificação documentada para estarem presentes no grupo/função.
38	Definir e implementar procedimentos de gestão de correções que dão prioridade a correções de segurança para sistemas utilizados para Processar Dados Pessoais ou Confidenciais da Microsoft. Estes procedimentos incluem: ▪ a abordagem de risco definido para dar prioridade às correções de segurança ▪ a capacidade para lidar e implementar correções de emergência; ▪ aplicabilidade ao sistema operativo e software de servidor, tais como servidor de aplicações e software de base de dados; ▪ documentar o risco que a correção atenua e rastrear quaisquer exceções; e requisitos para a desativação de software que já não é suportado pela empresa autora.	O fornecedor pode demonstrar um procedimento de gestão de correções implementado que cumpra este requisito e abranja, no mínimo, o seguinte: ▪ Atribuição da gravidade para informar a priorização. (As definições de gravidade encontram-se documentadas.) ▪ Procedimento documentado para implementar correções de emergência. ▪ Validar que não existe utilização de sistemas operativos que já não são suportados pela empresa autora. ▪ Registos de gestão de correções que rastreiem as aprovações e exceções.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção J: Segurança (cont.)	
39	Instalar software antivírus e anti-malware em equipamentos ligados à rede utilizados para processar os dados pessoais e confidenciais da Microsoft, incluindo servidores, computadores de secretária de formação e de produção para os proteger contra vírus potencialmente nocivos e aplicações de software malicioso. Atualizar as definições de anti-malware diariamente ou segundo as instruções do fornecedor de antivírus/anti-malware. Nota: Isto aplica-se a todos os sistemas operativos, incluindo Linux.	Existem registos para demonstrar que o uso de software antivírus e anti-malware está ativo. Nota: Este requisito aplica-se a todos os sistemas operativos.
40	Os fornecedores que desenvolvam software para a Microsoft devem incorporar os princípios de segurança desde a fase de conceção no processo de construção.	Os documentos de especificação técnica dos fornecedores incluem pontos de verificação para validação de segurança nos respetivos ciclos de desenvolvimento.
41	Utilizar um programa de Prevenção de Perda de Dados ("**DLP**", em inglês) para prevenir intrusões, perdas, e outras atividades não autorizadas. Os dados devem ser devidamente classificados, rotulados e protegidos e o fornecedor deve monitorizar os sistemas de informação em uso onde os Dados Pessoais ou Confidenciais da Microsoft são processados quanto a intrusões, perda, e outras atividades não autorizadas. O programa DLP, de forma mínima: ▪ requer a utilização de sistemas de deteção de intrusos (IDS) baseados na rede, anfitrião padrão da indústria e sistemas de deteção de intrusão ("**IDS**, em inglês"), se retiver dados pessoais ou confidenciais da Microsoft; ▪ requer a implementação de sistemas avançados de proteção contra intrusão ("**IPS**") configurados para monitorizar e parar ativamente a perda de dados; ▪ na eventualidade de um sistema ser violado, requer uma análise do sistema para assegurar que quaisquer vulnerabilidades residuais sejam também solucionadas; ▪ descrever os procedimentos necessários para as ferramentas de deteção de violação do sistema de monitorização; ▪ estabelece uma resposta de incidente e processo de gestão necessário a ser efetuado quando é detetado um incidente de Dados; e ▪ requer comunicações (a todos os colaboradores e subcontratados do fornecedor que estejam relacionados com o Desempenho do fornecedor) relativamente à transferência e à utilização não autorizada de Dados Pessoais ou Confidenciais da Microsoft.	Programa de DLP documentado, implementado com procedimentos em vigor para evitar intrusões, perdas e outras atividades não autorizadas (e, no mínimo, todos os itens especificados nesta secção).

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção J: Segurança (cont.)	
42	Comunicar imediatamente os resultados da investigação a partir da resposta a incidentes à alta direção e à Microsoft.	Devem estar implementados sistemas e processos para comunicar à Microsoft os resultados da investigação da resposta a incidentes.
43	Os administradores de sistemas, os funcionários de operações, a direção e terceiros devem submeter-se a uma formação anual de segurança.	Estabelecer um programa de formação de segurança que inclua: ▪ formação anual para resposta a incidentes; e ▪ eventos simulados e mecanismos automatizados para facilitar uma resposta eficaz a situações de crise. ▪ Consciencialização relativamente à prevenção de incidentes, tais como os riscos associados à transferência de software malicioso.
44	O fornecedor deve assegurar que os processos de planeamento de cópias de segurança protegem os Dados Pessoais e Confidenciais da Microsoft contra a utilização, acesso, divulgação, alteração e destruição não autorizados.	O fornecedor pode demonstrar procedimentos de resposta e recuperação documentados, detalhando a forma como a organização irá gerir um evento prejudicial e manter a sua segurança de informação a um nível pré-determinado, com base em objetivos de continuidade de segurança de informação aprovados pela gestão. O fornecedor pode demonstrar que definiu e implementou procedimentos para efetuar periodicamente cópias de segurança, armazenar em segurança e recuperar eficazmente dados críticos.
45	Estabelecer e testar a continuidade do negócio e planos de recuperação após desastres.	Um plano de recuperação após desastres tem de incluir o seguinte: ▪ Critérios definidos para determinar se um sistema é crítico para o funcionamento do negócio do fornecedor. ▪ Listar os sistemas críticos com base nos critérios definidos que devem ser visados para a recuperação em caso da ocorrência de um desastre. ▪ Procedimento de recuperação após desastre definido para cada sistema crítico que assegura que um engenheiro que não conheça o sistema possa recuperar o pedido em menos de 72 horas. ▪ Testes anuais (ou mais frequentes) e revisão dos planos de recuperação em caso de catástrofe para assegurar que os objetivos de recuperação possam ser atingidos.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção J: Segurança (cont.)	
46	Autenticar a identidade de um indivíduo antes de lhe conceder acesso aos Dados Pessoais ou Confidenciais da Microsoft e assegurar que o acesso é limitado, em particular, ao âmbito de atividade do indivíduo permitido para apoiar o Desempenho.	Assegurar que todos os IDs de utilizadores são únicos e que cada um tem um método de autenticação padrão da indústria, como o Azure Active Directory. O acesso elevado (privilégios administrativos ou outros tipos de privilégios melhorados) deve exigir a utilização de um segundo fator, tal como um cartão inteligente ou um autenticador baseado no telefone. Programa documentado de segurança da informação que cubra o processo para assegurar que o acesso de todos os funcionários e subcontratados do fornecedor aos Dados Pessoais ou Confidenciais da Microsoft não seja superior ou mais longo do que o necessário para apoiar o Desempenho.
47	O fornecedor deve proteger todos os dados Processados em ligação com o seu Desempenho em trânsito através das redes com encriptação utilizando o protocolo Transport Layer Security ("**TLS**") ou o Internet Protocol Security ("**IPsec**"). Estes métodos encontram-se descritos na norma NIST 800-52 e NIST 800-57; podendo também ser utilizada uma norma industrial equivalente. O fornecedor deve recusar a entrega de quaisquer Dados Pessoais ou Confidenciais da Microsoft transmitidos por meios não encriptados.	O processo de criação, implantação e substituição do TLS ou outros certificados deve ser definido e aplicado.
48	Todos os dispositivos do fornecedor (computadores portáteis, estações de trabalho, etc.) que irão aceder, ou manusear Dados Pessoais ou Confidenciais da Microsoft devem utilizar encriptação baseada em disco.	Encriptar todos os dispositivos para satisfazer o BitLocker ou outra solução de encriptação de disco equivalente da indústria para todos os dispositivos clientes utilizados para tratar Dados Pessoais ou Confidenciais da Microsoft.

#	Requisitos de Proteção de Dados dos Fornecedores da Microsoft	Evidência de conformidade
	Secção J: Segurança (cont.)	
49	Os sistemas e procedimentos (utilizando as normas industriais atuais, tais como as descritas na norma **NIST 800-111)** devem estar em utilização para encriptar em repouso (quando armazenados) todo e qualquer Dados Pessoais e/ou Confidencial da Microsoft; os exemplos incluem, mas não estão limitados a: ▪ dados de credenciais (por exemplo, nomes de utilizador/palavras-passe) ▪ dados de instrumentos de pagamentos (por exemplo, números de cartões de créditos e contas bancárias) ▪ Dados pessoais relacionados com imigração ▪ dados de perfil médico (por exemplo, números de registos médicos ou marcadores ou identificadores biométricos, tais como ADN, impressões digitais, retinas e íris oculares, padrões de voz, padrões faciais e medições das mãos, utilizados para efeitos de autenticação) ▪ dados identificadores emitidos pelo governo (por exemplo, números da segurança social ou da carta de condução) ▪ dados pertencentes a clientes Microsoft (por exemplo, SharePoint, documentos do O365, clientes OneDrive) ▪ material relacionado com produtos Microsoft não anunciados ▪ Data de Nascimento ▪ Informações de perfil de crianças ▪ dados geográficos em tempo real ▪ morada pessoal física (não profissional) ▪ números de telefone pessoais (não profissionais) ▪ religião ▪ opiniões políticas ▪ orientação/preferência sexual ▪ respostas a questões de segurança (por exemplo, 2fa, reposição de palavra-passe) ▪ nome de solteira da mãe	Verificar se os Dados Pessoais e Confidenciais da Microsoft se encontram encriptados em repouso.
50	Anonimizar todos os Dados Pessoais da Microsoft utilizados num ambiente de desenvolvimento ou teste.	Os Dados Pessoais da Microsoft não devem ser utilizados em ambientes de desenvolvimento ou teste; quando não existir alternativa, estes devem ser anonimizados para impedir a identificação dos Titulares dos Dados ou o uso indevido dos Dados Pessoais. Nota: Os dados anonimizados são diferentes dos dados apresentados sob pseudónimo. Dados anónimos são os dados que não se referem a uma pessoa singular identificada ou identificável, quando o titular dos dados dos dados pessoais não é ou deixou de ser identificável.

Glossário

"**Representante Autorizado**" é uma pessoa que possui o nível de autoridade apropriado para assinar em nome da empresa. Esta pessoa teria os conhecimentos necessários sobre privacidade e segurança ou teria consultado um perito no assunto antes de submeter a sua resposta a uma ação do Programa SSPA. Além disso, ao adicionarem o seu nome a um formulário SSPA, certificam que leram e compreenderam os RPD.

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

"**Freelancer**" significa os indivíduos que desempenham tarefas ou serviços mediante pedido, que são angariados através de plataformas digitais ou de outros meios.

"RGPD" refere-se ao Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a 95/46/CE (Regulamento Geral sobre Proteção de Dados).

"**Requisitos de Proteção dos Dados de Privacidade**" refere-se ao RGPD, o EUDPR, as Leis Locais de Proteção de Dados da UE/EEE, a Lei de Privacidade do Consumidor da Califórnia, Cal. Cod. Civil § 1798.100 et seq. ("*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 com (a) privacidade e segurança de dados; ou (b) a utilização, recolha, retenção, armazenamento, segurança, divulgação, transferência, eliminação, e outro processamento de quaisquer Dados Pessoais.

"**Cláusulas Modelo UE**" e "**Cláusulas Contratuais-tipo**" referem-se (i) às cláusulas-tipo de proteção de dados para a transferência de dados pessoais para processadores estabelecidos em países terceiros que não asseguram um nível adequado de proteção de dados, conforme descrito no artigo 46º do RGPD e aprovado pela decisão da Comissão Europeia (UE) 2021/914 de 4 de Junho de 2021; (ii) quaisquer cláusulas contratuais-tipo sucessoras adotadas pela (a) Comissão Europeia, (b) Autoridade Europeia para a Proteção de Dados e aprovadas pela Comissão Europeia, (c) Reino Unido nos termos da Lei Geral Federal de Proteção de Dados do Reino Unido, (d) Suíça nos termos da Lei Federal de Proteção de Dados da Suíça, ou (e) por um governo numa jurisdição que não a Suíça, o Reino Unido, e as jurisdições que compõem a União Europeia / Espaço Económico Europeu, onde as cláusulas regem a transferência internacional de dados pessoais, serão incorporadas e vinculativas para o fornecedor a partir do dia da sua adoção.

"**Alojamento de sítios web**" Um serviço de alojamento de sítios web é um serviço online que cria e/ou mantém sítios web em nome da Microsoft sob o domínio Microsoft, ou seja, o fornecedor fornece todos os materiais e serviços necessários para a criação e manutenção de um sítio, tornando-o acessível na Internet. O "fornecedor de serviços de alojamento web" ou "anfitrião web" é o fornecedor que fornece as ferramentas e serviços necessários para que o sítio web ou página web possa ser visto na Internet, tais como, cookies ou web beacons para publicidade.