**ACORDO DE COMPARTILHAMENTO DE DADOS (DADOS DA EMPRESA)**

**Data de revisão: 12 de março de 2024**

Para os fins deste Acordo de Compartilhamento de Dados (“DSA”), a entidade Merck Sharp & Dohme LLC ou afiliada que executa o contrato, ou ainda outra forma de contrato referente a este DSA (o “Contrato”) deve ser denominada “Empresa” e todas as outras partes desse Contrato devem ser denominadas “Fornecedor”. A Empresa e o Fornecedor são cada uma “Parte” e juntos as “Partes”.

Disposições gerais

1. As Partes inseridas e integrantes do Contrato poderão firmar uma ou mais ordens ou tarefas de compra, contratos de projeto, adendos de plano de projeto, declarações de trabalho, ordens de serviço ou outros termos de serviço (cada qual denominados como “Declaração de trabalho”), que regem os serviços nela contemplados (“Finalidade de Compartilhamento de Dados”).
2. As Partes pretendem complementar os termos do Contrato para garantir que todo o compartilhamento de Informações Pessoais relacionado ao Contrato seja realizado em conformidade com a Lei de Proteção de Dados, e esclarecer a função do Fornecedor como controlador independente desses dados.
3. A Parte referida no Contrato como “**MSD**”, “**CONTRATANTE**”, “**PATROCINADORA**” ou “**FORNECEDORA**” será denominada neste DSA “Empresa”.
4. A Parte referida no Contrato como “**CONTRATADA**”, “**PATROCINADA**”, “**COMPRADORA**” ou “**DISTRIBUIDORA**” será denominada neste DSA “Fornecedor”.

As Partes concordam que:

1. *Atividades de Compartilhamento de Dados*. Quanto às Informações Pessoais Processadas relacionadas ao Contrato, o teor, a natureza, o objetivo e a duração do Compartilhamento, bem como as categorias dos Titulares dos Dados envolvidos e as categorias de Informações Pessoais, estão especificados no Anexo do Contrato intitulado “Detalhes do Processamento de Dados”.
2. *Aplicabilidade*. Os termos deste DSA se aplicam a cada Declaração de Trabalho de acordo com o Contrato, salvo se especificado o contrário na Declaração de Trabalho correspondente.
3. *Obrigações do Fornecedor*. Ao processar Informações Pessoais relacionadas ao Contrato, o Fornecedor:
	1. deve cumprir a Lei de Proteção de Dados e as obrigações do Fornecedor de acordo com este DSA e, caso o Fornecedor não possa cumprir essas obrigações, deve notificar a Empresa imediatamente e adotar todas as medidas razoáveis e apropriadas consideradas necessárias pela Empresa na remediação em razão do não cumprimento.
	2. deve apenas Processar Informações Pessoais conforme especificado neste DSA e no Contrato, exceto quando:
		1. o Fornecedor obteve o consentimento prévio do Titular dos Dados;
		2. for necessário para o estabelecimento, exercício ou defesa em processos judiciais no contexto de processos administrativos, regulatórios ou judiciais específicos;
		3. for necessário para proteger os interesses principais dos Titulares dos Dados ou de outra pessoa física; ou
		4. for exigido de outra forma pela lei aplicável, caso em que o Fornecedor informará a Empresa sobre essa exigência legal, a menos que esteja proibido por essa lei aplicável, e envidará seus melhores esforços para limitar a natureza e o escopo de qualquer divulgação exigida e divulgará apenas a quantidade mínima de Informações Pessoais necessárias para cumprir a lei aplicável.
	3. não deve divulgar ou transferir Informações Pessoais a terceiros sem que esses terceiros celebrem um contrato por escrito com termos pelo menos tão protetores das Informações Pessoais, como as obrigações estabelecidas neste DSA e no Contrato.
	4. não deve vender, compartilhar, reter, usar ou divulgar Informações Pessoais além das especificadas no Contrato ou conforme autorizado de outra forma por este DSA.
	5. deve ser totalmente responsável por todos os atos ou omissões dos seus respectivos funcionários, afiliadas, agentes, subcontratados e outros representantes.
	6. deve implementar e manter programas de segurança e privacidade de informações e apropriados, determinar quais programas devem incorporar medidas físicas, técnicas e organizacionais que sejam proporcionais à natureza das Informações Pessoais processadas em relação ao Contrato, que atendam ou superem as boas práticas do setor (ou padrão superior, conforme exigido no Apêndice 1) e que protejam razoavelmente contra uma Violação de Dados Pessoais, incluindo o treinamento de todos os funcionários responsáveis pelo processamento de Informações Pessoais de maneira a atender suficientemente às exigências deste DSA. Tais medidas, descritas no Apêndice 1 e, na medida em que não forem tratadas de outra forma no Apêndice 1, compreendem:
		1. a pseudonimização e criptografia das Informações Pessoais;
		2. a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de Processamento;
		3. a capacidade de restaurar a disponibilidade e acesso a Informações Pessoais em tempo hábil em caso de um incidente físico ou técnico;
		4. um processo para testar, avaliar e estimar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do Processamento; e
		5. a capacidade de confirmar, dentro de 72 (setenta e duas) horas após a ocorrência, se um evento constitui uma Violação de Dados Pessoais.
	7. em caso de uma constatação real ou razoavelmente suspeita de Violação de Dados relacionados a Informações Pessoais sob custódia ou controle do Fornecedor ou como resultado dos atos ou omissões do Fornecedor (uma “Violação de Dados Pessoais do Fornecedor”), o Fornecedor deve:
		1. notificar a Empresa imediatamente (em qualquer caso de Violação de Dados Pessoais do Fornecedor dentro de 24 horas após conhecimento do evento);
		2. realizar uma investigação adequada e todos os esforços de remediação necessários para corrigir e prevenir a recorrência dessa Violação de Dados Pessoais do Fornecedor de maneira satisfatória para a Empresa;
		3. fornecer prontamente à Empresa todas as informações consideradas necessárias pela Empresa, para permitir que cumpra a Lei de Proteção de Dados, inclusive com relação à manutenção e registro de relatórios e todas as outras informações que a Empresa possa razoavelmente solicitar sobre uma Violação de Dados Pessoais do Fornecedor;
		4. fornecer notificação a todos os Titulares dos Dados, cujas informações pessoais podem ter sido afetadas, com o conteúdo exigido pela Lei de Proteção de Dados; e
		5. se responsabilizar exclusivamente pelos custos e despesas de qualquer uma das Partes por qualquer notificação aos Titulares dos Dados, independemente da notificação ser enviada pelo Fornecedor ou pela Empresa.
	8. deve notificar imediatamente a Empresa sem atrasos indevidos, e em qualquer hipótese, dentro de 24 (vinte e quatro) horas de:
		1. qualquer reclamação, questionamento, solicitação ou preocupação de uma autoridade competente de proteção de dados ou outra autoridade regulatória relacionada às Informações Pessoais ligadas ao Contrato; e
		2. qualquer reclamação, questionamento, solicitação ou preocupação do Titular dos Dados em relação às Informações Pessoais Processadas relacionadas ao Contrato, incluindo qualquer solicitação para exercer os direitos sob a Lei de Proteção de Dados ou a política de privacidade da Empresa ou do Fornecedor, tais como acessar (incluindo solicitações de informações sobre qualquer processamento de suas Informações Pessoais), retificar, alterar, corrigir, compartilhar, excluir ou cessar o processamento das Informações Pessoais do Titular.
	9. deve cumprir todas as medidas razoáveis e adequadas solicitadas pela Empresa, necessárias para que o Fornecedor e a Empresa cumpram suas respectivas obrigações nos termos da Lei de Proteção de Dados e deste DSA.
	10. deve reter as Informações Pessoais não mais do que o necessário para cumprir a Finalidade de Compartilhamento de Dados, salvo exigido de outra forma pela lei aplicável.
	11. deve manter a precisão e a integridade das Informações Pessoais compartilhadas pela Empresa, de forma consistente com a forma pela qual o Fornecedor recebeu ou coletou tais Informações Pessoais.
	12. deve manter todos os registros necessários a fim de demonstrar que essas Informações Pessoais somente foram Processadas de acordo com os avisos, consentimentos, autorizações e direitos aplicáveis e conforme permitido nos termos deste DSA, para que a Empresa e o Fornecedor possam estar em conformidade com a Lei de Proteção de Dados.
	13. nos casos em que o Fornecedor deve Processar as Informações Pessoais sobre Titulares dos Dados de qualquer país ou região com restrições sobre a transferência transfronteiriça de Informações Pessoais, o Fornecedor somente o fará em conformidade com a Lei de Proteção de Dados, o que pode incluir, sem limitação, a celebração das Cláusulas Contratuais Padrão ou mecanismos semelhantes destinados a proteger as transferências de Informações Pessoais.
	14. salvo mudanças feitas de acordo com o cumprimento de um padrão mais elevado do setor ou da Lei de Proteção de Dados, o Fornecedor deve manter em vigor e aplicar consistentemente as práticas de privacidade e segurança de dados do Fornecedor divulgadas à Empresa, em relação a devida diligência conduzida sobre essas práicas em relação a este Contrato; contanto que o Fornecedor não reduza os padrões dessas práticas, divulgando subsequentemente práticas de privacidade e segurança de dados, o que configuraria uma degradação das práticas anteriormente divulgadas. O Fornecedor declara e garante que todas as respostas por ele fornecidas, em qualquer diligência devida, são verdadeiras, precisas e completas quando feitas, e que um representante autorizado do Fornecedor concluiu tal diligência devida. O Fornecedor notificará imediatamente a Empresa sobre todas as alterações materiais nas práticas de privacidade e segurança dos dados do Fornecedor.
	15. deve, se exigido pela Lei de Proteção de Dados, nomear um Responsável por Proteção de Informações Pessoais e informar à Empresa o nome e o número de telefone dessa pessoa.
	16. deve reconhecer e concordar que a assinatura deste DSA constitui sua certificação de que entende e se compromete com as restrições dispostas neste DSA e as cumprirá.
4. *Indenização*. Sem limitar quaisquer direitos ou prerrogativas da Empresa, obrigações do Fornecedor nos termos do Contrato ou de outra forma, as Partes concordam que o Fornecedor indenizará a Empresa, suas afiliadas e seus respectivos executivos, diretores, funcionários, contratados, trabalhadores temporários, subcontratados, agentes e outros representantes (denominados “Parte Indenizada”) quanto a quaisquer perdas, danos, multas, custos ou despesas (incluindo despesas e gastos jurídicos) incorridos por essa Parte Indenizada resultante da Violação de Dados Pessoais do Fornecedor em relação às Informações Pessoais Processadas pelo Fornecedor em relação ao Contrato. Qualquer responsabilidade abordada nesta seção estará sujeita às limitações ou exclusões de responsabilidade aplicáveis no Contrato, a menos que tal responsabilidade seja resultado da negligência ou ato errado intencionalmente do Fornecedor, caso em que nenhuma limitação ou exclusão de responsabilidade será aplicada.
5. *Definições*
	1. “Lei de Proteção de Dados” significa qualquer lei aplicável de proteção de dados, segurança ou privacidade de dados, incluindo a Lei Geral de Proteção de Dados (“LGPD”) nº 13.709/18, ou quando aplicável, o Regulamento Geral de Proteção de Dados da UE e qualquer legislação nacional de implementação relacionada, Lei de Portabilidade e Responsabilidade do Seguro de Saúde, a Lei de Direitos de Privacidade da Califórnia e qualquer outra lei de proteção, privacidade e segurança de dados, a nível municipal, estadual ou federal.
	2. “Informações pessoais” significa quaisquer dados relacionados ao Contrato vinculado a um indivíduo identificado ou identificável, incluindo dados que identificam um indivíduo ou que poderiam ser usados para identificar, localizar, rastrear ou contatar um indivíduo. As Informações Pessoais incluem informações diretamente identificáveis, como nome, número de identificação ou título exclusivo do cargo, e informações indiretamente identificáveis, como data de nascimento, identificador exclusivo de dispositivos móveis ou vestíveis, informações que possam ser usadas para identificar uma residência, número de telefone, dados codificados por chave, identificadores online, como endereços IP ou atividades pessoais, comportamentos ou preferências, e inclui quaisquer dados que constituam “dados pessoais” de acordo com a Lei de Proteção de Dados.
	3. “Processamento” significa realizar qualquer operação ou conjunto de operações em Informações Pessoais ou conjuntos de Informações Pessoais, seja ou não por meios automatizados, como coleta, registro, organização, estruturação, armazenamento, acesso, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou ainda disponibilização, avaliação, análise, elaboração de relatórios, compartilhamento, alinhamento ou combinação, restrição, eliminação ou destruição.
	4. “Violação de Dados Pessoais” significa uma destruição acidental ou ilegal, perda ou alteração acidentais ou ilícitas, divulgação ou acesso não autorizados de Informações Pessoais, transmitidas, armazenadas ou processadas de outra forma.
	5. “Cláusulas Contratuais Padrão” são cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros que não foram avaliados pela Comissão Europeia como fornecendo um nível adequado de proteção aos dados pessoais, conforme publicado pela Comissão Europeia em 4 de junho de 2021, e que podem ser atualizadas periodicamente.
	6. Caso essas definições restrinjam ou reduzam o escopo das definições relacionadas à Lei de Proteção de Dados, as disposições deverão ser expandidas para corresponder às determinações da Lei de Proteção de Dados.
	7. Na ausência de uma definição nesta Seção, um termo deve ser interpretado de maneira compatível com todas as Leis de Proteção de Dados aplicáveis.
6. *Interpretação*.
	1. Os termos definidos e usados neste DSA, mas não definidos neste documento, devem ter o significado especificado em outras disposições deste Contrato.
	2. As palavras “incluir” e “incluindo” devem ser interpretadas como incluindo, entre outros.
	3. No cumprimento das suas obrigações ao abrigo do Acordo de Serviço e deste DSA, as Partes reconhecem que a política corporativa da MSD e das suas Afiliadas exige que os negócios da MSD sejam conduzidos de acordo com a letra e o espírito de qualquer Lei de Proteção de Dados aplicável, incluindo o Regulamento Geral sobre a Proteção de Dados da UE. No caso de ambas as Partes não estarem sujeitas às mesmas Leis de Proteção de Dados, espera-se que ambas as Partes cumpram todas as normas de proteção de dados razoavelmente relevantes contidas em tais leis.
	4. Em relação à Finalidade de Compartilhamento de Dados nos termos do Contrato, o Fornecedor pode Processar as Informações Pessoais de uma ou mais das afiliadas da Empresa. Nesse caso, qualquer uma dessas afiliadas da Empresa será considerada um “Controlador” de Informações Pessoais e um terceiro beneficiário deste DSA terá o direito de confiar e fazer cumprir todos os direitos e proteções concedidos à Empresa nos termos deste DSA, independentemente da afiliada ser nomeada como parte do Contrato ou do DSA.
	5. Este DSA é incorporado e faz parte do Contrato.
	6. No caso e na medida em que houver qualquer conflito entre os termos do Contrato e este DSA, os termos deste DSA prevalecerão, exceto se os termos do Contrato garantirem mais proteção às Informações Pessoais Processadas no escopo do Contrato. Neste caso, os termos mais protetores do Contrato prevalecerão.
	7. Na hipótese e na medida de qualquer conflito entre os termos deste DSA e as Cláusulas Contratuais Padrão, os termos da Cláusulas Contratuais Padrão prevalecerão.
	8. Salvo expressamente alterado neste documento, os termos do Contrato permanecerão em pleno vigor e efeito.
	9. Se este DSA for redigido em inglês e em um idioma estrangeiro, no caso de diferenças entre o texto em inglês e o texto no idioma estrangeiro, o texto em inglês prevalecerá.
	10. As cláusulas e outros títulos neste DSA são somente para conveniência de referência e não devem constituir uma parte ou de outra forma afetar o significado ou a interpretação deste DSA.
	11. Os Anexos e Apêndices a este DSA devem ser considerados parte integrante deste DSA na mesma medida, como se tivessem sido transcritos expressamente neste DSA.
	12. As disposições deste DSA são separáveis. Se qualquer frase, cláusula ou disposição for inválida ou inexequível no todo ou em parte, tal invalidade ou inexequibilidade afetará somente essa frase, cláusula ou disposição e o restante deste DSA permanecerá em pleno vigor e efeito.
	13. Este DSA rege qualquer Processamento de Informações Pessoais relacionadas à Finalidade de Compartilhamento de Dados e complementa os termos do Contrato aplicável à essa Finalidade, exceto quando Empresa e o Fornecedor celebraram outro DSA aplicável para garantir a Finalidade de Compartilhamento de Dados.
	14. Este DSA pode ser celebrado em qualquer número de vias que, em conjunto, constituirão um mesmo contrato. Qualquer Parte pode celebrar este DSA firmando tal via.
	15. Este DSA constitui o acordo integral entre as Partes em relação ao assunto deste DSA (na medida do permitido por lei) e substitui todas as representações anteriores ou acordos orais ou escritos entre as Partes em relação a esse assunto, desde que nada neste DSA e nenhuma das Partes esteja tentando excluir qualquer responsabilidade por declarações fraudulentas.
	16. As disposições de lei e jurisdição aplicáveis do Contrato serão aplicáveis a este DSA.
7. *Limites em atualizações*.
	1. Quando as Partes renovarem, alterarem, emitirem uma nova Declaração de Trabalho sob, ou de qualquer forma modificarem o Acordo ou qualquer Declaração de Trabalho sob o Acordo (um "Evento Gatilho"), o documento mais recente sob "Data Sharing Addendum (Company Data)" localizado em <https://www.msdprivacy.com/privacyterms/> irá substituir e sobrepor os termos deste DSA até o próximo Evento Gatilho, a menos que uma objeção seja apresentada dentro de 30 dias após a ocorrência do evento gatilho. Não obstante o exposto, pode haver situações que exijam uma alteração imediata dos termos deste DSA, o que só ocorrerá por motivos articulados em 7(b), e só será feito de boa fé e após garantir que os novos termos ou termos modificados se limitem àqueles necessários para cumprir com a nova Lei de Proteção de Dados aplicável, jurisprudência ou orientações emitidas pelas autoridades de proteção de dados relevantes.
	2. No evento de qualquer um dos seguintes cenários ocorrer, as Partes concordam imediatamente com os termos mais recentes postados no endereço acima, a menos que uma objeção seja apresentada dentro de 30 dias após o aviso da Empresa sobre os novos termos fornecidos a todas as entidades que solicitaram receber aviso em privacy\_updates@msd.com:
		1. a Lei de Proteção de Dados aplicável foi atualizada de maneira que os termos contratuais existentes deste DSA sejam inadequados para satisfazer os requisitos da lei atualizada,
		2. há uma mudança na Lei de Proteção de Dados aplicável e as Partes têm um interesse razoável e legítimo em alterar esses termos devido à mudança da lei, por exemplo e sem limitação, removendo requisitos que não são mais necessários, ou
		3. há nova jurisprudência ou orientações emitidas pelas autoridades de proteção de dados relevantes que têm um efeito comparável a uma mudança na lei descrita em (i) ou (ii) acima.
8. *Aplicabilidade dos apêndices*. As Cláusulas Contratuais Padrão aqui anexadas como Apêndice 2 e os anexos no Apêndice 3 só devem ser aplicáveis na medida em que forem exigidos pela Lei de Proteção de Dados aplicável. As Partes concordam em cumprir tais cláusulas e adendos unicamente na medida em que estejam alinhados e sejam exigidos pelos requisitos da Lei de Proteção de Dados aplicável em cada respectiva jurisdição.
9. *Notificação*. Notificações fornecidas nos termos deste DSA (cada uma, “Notificação”) devem ser feitas por escrito. As notificações fornecidas neste DSA devem ser fornecidas de acordo com as disposições de notificação do Contrato aplicável, juntamente com cópia(s) enviadas por e-mail à Empresa, para msd\_privacy\_office@msd.com, com uma linha de assunto “DSA Notificação do Fornecedor” ou no caso de uma Violação de Dados Pessoais “Urgente: Notificação de Violação de Dados Pessoais”.

**APÊNDICE 1 – Medidas de Segurança da Tecnologia da Informação**

1. Definições – Quando usadas neste Anexo, cada um dos seguintes termos definidos terá a definição dada abaixo para esse termo. Termos definidos usados neste Anexo, mas não definidos aqui, terão o significado especificado no Contrato.
	1. “Informação da Empresa” significa qualquer informação da Empresa ou de qualquer das Afiliadas da Empresa ou de seus respectivos fornecedores, clientes ou outros parceiros de negócios fornecidos para, obtidos por, criados ou gerados por ou de outra forma processados pelo Fornecedor ou qualquer dos prestadores de serviços subcontratados pelo Fornecedor em conexão com qualquer um dos Serviços e qualquer outra informação a ser tratada como confidencial sob o Contrato.
	2. “Violação de Dados” significa perda, transmissão ou divulgação acidental, e ou uma transmissão, destruição, alteração, uso, ou acesso não autorizados , relativamente a qualquer Informação da Empresa.
	3. “Ponto Final” significa qualquer computador, incluindo qualquer laptop ou desktop, dispositivo móvel, equipamento de laboratório, servidor ou outro dispositivo nos Sistemas do Fornecedor, incluindo qualquer um hospedado num site de terceiros (por exemplo, fornecedor do serviço de “nuvem”).
	4. “Evento de Notificação” significa qualquer evento, incluindo uma Violação de Dados, que requer a notificação de indivíduos ou entidades sob quaisquer Leis.
	5. “Evento de Segurança” significa qualquer (A) Violação de Dados, (B) Evento de Notificação, (C) Acesso não autorizado ou interferência com as operações dos Sistemas do Fornecedor ou (D) Violação das obrigações de segurança do Fornecedor sob este Anexo, o no âmbito do Contrato ou quaisquer Leis.
	6. “Software Fornecido” significa qualquer *software* fornecido ou usado em conexão com qualquer um dos Serviços, incluindo qualquer *software* entregue para, ou instalado em qualquer computador, incluindo qualquer *laptop* ou *desktop*, dispositivo móvel, equipamento de laboratório, servidor, outro dispositivo ou outro componente, ligado aos sistemas de informação da Empresa ou de qualquer das Afiliadas da Empresa.
	7. “Sistemas do Fornecedor” significa as redes do Fornecedor e todos os seus sistemas, incluindo Software Fornecido, (A) fornecidos ou usados em conexão com qualquer um dos Serviços, (B) nos quais qualquer Informação da Empresa ou entregáveis ou trabalho em progresso para a Empresa ou suas Afiliadas, é armazenado ou de outra forma processado, ou a partir do qual é possivel aceder a essa informação ou trabalhos, (C) conectados à informação, rede ou outros sistemas da Empresa ou de suas Afiliadas ou a partir dos quais a informação, rede ou outros sistemas da Empresa ou de suas Afiliadas podem ser acedidos, ou (D) aos quais qualquer dos anteriores pode estar conectado ou a partir dos quais qualquer dos anteriores pode ser acedido
2. Segurança de Rede - O Fornecedor deverá manter políticas, procedimentos e controles de segurança de rede e deverá realizar atividades de segurança de rede, consistentes com as melhores práticas na indústria do Fornecedor, mas que incluam no mínimo provisionamento de *firewall* de rede, controles de detecção e prevenção de intrusão, controles de proteção contra ataques de negação de serviço distribuído (DDoS) e avaliações de vulnerabilidade e testes de penetração realizados regularmente, de acordo com as melhores práticas na indústria do Fornecedor (mas não menos frequentemente do que anualmente). Em nenhum caso, as políticas, procedimentos ou controles de segurança de rede do Fornecedor aplicados à proteção das Informações da Empresa e dos Sistemas do Fornecedor serão menos rigorosos e protetores do que aqueles aplicados pelo Fornecedor à proteção de suas próprias informações e seus outros sistemas de natureza semelhante.
3. Segurança de Aplicação - Com base na natureza dos serviços prestados, se aplicável, o Fornecedor deverá ter processos e controles do ciclo de vida de desenvolvimento de *software* ("Processo SDLC") que regem o desenvolvimento e as alterações de qualquer Software do Fornecedor, incluindo atualizações, *upgrades, patches*, melhorias, correções de *bugs*, modificações, melhorias, correções, revisões, lançamentos e outras alterações. O Processo SDLC deve, no mínimo, incluir práticas reconhecidas e comparáveis de desenvolvimento seguro de *software* padrão da indústria. O Fornecedor deve seguir um processo de gestão e manutenção de *patches* que garanta que os Sistemas de Informação do Fornecedor estejam atualizados com a segurança e funcionalidade apropriadas. O Fornecedor deve remediar e retestar qualquer vulnerabilidade identificada de maneira oportuna, proporcional ao risco e dentro dos prazos fornecidos nas Políticas e Procedimentos do Fornecedor.
4. Segurança de Dados - Com base na natureza dos serviços prestados, se aplicável, o Fornecedor deve manusear, armazenar e processar as Informações da Empresa, de acordo com práticas e padrões da indústria reconhecidos e comparáveis, como os estabelecidos no parágrafo 11 (incluindo PCI DSS, conforme aplicável) e de acordo com todas as Leis. O Fornecedor deve estabelecer e manter salvaguardas razoáveis contra uma Violação de Dados. Além de e sem limitar quaisquer outras obrigações do Fornecedor, o Fornecedor deve armazenar todas as Informações da Empresa de acordo com as melhores práticas na indústria do Fornecedor e em conformidade com todas as Leis, e deve usar medidas de segurança que atendam às melhores práticas na indústria do Fornecedor, incluindo criptografia e *firewalls*, para proteger as Informações da Empresa de uma Violação de Dados. Quando o Fornecedor armazena Informações da Empresa numa instalação fora da sua localização, o Fornecedor deve ter cumprido todos os termos do Contrato ou de qualquer outro contrato executado em conexão com o Contrato, relacionado à divulgação de Informações da Empresa a terceiros ou ao envolvimento de terceiros para fornecer ou auxiliar na prestação de produtos ou serviços, e o Fornecedor deve usar uma instalação de armazenamento fora da sua localização, que seja razoavelmente aceitável para a Empresa e que deve, sem limitar o acima escrito, estar em total conformidade com todas as disposições deste Anexo. Além disso, o fornecimento de tal instalação de armazenamento fora do local do Fornecedor deve ser formalizada por um acordo de confidencialidade escrito entre o Fornecedor e o Prestador desse local de armazenamento, que contenha termos não menos rigorosos do que os do Contrato ou qualquer contrato executado em conexão com o Contrato e que protege todas as Informações da Empresa armazenadas nele.
5. Armazenamento de Dados - Com base na natureza dos serviços prestados, se aplicável, todas e quaisquer Informações da Empresa serão manuseadas, armazenadas e processadas apenas em recursos de computação e armazenamento designados pelo Fornecedor. As Informações da Empresa só serão manuseadas, armazenadas ou processadas em um *laptop* ou dispositivo móvel, se (A) for um *laptop* ou dispositivo móvel do Fornecedor, (B) o Fornecedor criptografar todas as Informações da Empresa nesse *laptop* ou dispositivo móvel de acordo com os padrões de criptografia no parágrafo 7 abaixo e (C) esse *laptop* ou dispositivo móvel estiver sujeito a controles de Endpoint consistentes com práticas e padrões da indústria reconhecidos e comparáveis, como os estabelecidos no parágrafo 11. As Informações da Empresa não serão manuseadas, armazenadas ou processadas num dispositivo portátil, exceto conforme previsto na frase imediatamente acima. O Fornecedor deve armazenar todos os *backups* das Informações da Empresa como parte de seus processos de backup e recuperação designados, e tais backups das Informações da Empresa devem ser criptografados de acordo com este Anexo, incluindo os requisitos deste parágrafo 5 e parágrafo 7 abaixo.
6. Transmissão de Dados - Com base na natureza dos serviços prestados, se aplicável, qualquer transmissão ou troca eletrônica de Informações da Empresa ocorrerá por meios seguros (usando HTTPS ou SFTP ou equivalente) que estejam de acordo com práticas e padrões da indústria reconhecidos e comparáveis, como os estabelecidos no parágrafo 11, e somente de acordo com o parágrafo 7 abaixo.
7. Criptografia de Dados - Com base na natureza dos serviços prestados, se aplicável, além de e sem limitar quaisquer outras obrigações do Fornecedor, o Fornecedor concorda que qualquer Informação da Empresa composta por Informações Pessoais sujeitas à proteção sob qualquer Lei ou composta por informações sujeitas à proteção sob o atual Padrão de Proteção de Dados da Indústria de Cartões de Pagamento, incluindo todos os dados de *backup* da Empresa, será mantida de forma criptografada, usando uma solução de criptografia comercialmente suportada. O Fornecedor concorda que as soluções de criptografia serão implantadas que criptografam as Informações da Empresa de acordo com práticas e padrões da indústria reconhecidos e comparáveis, como os estabelecidos no parágrafo 11, mas não com menos que uma chave de 128 bits para criptografia simétrica e uma chave de 2048 (ou maior) bit para criptografia assimétrica.
8. Reutilização de Dados - Com base na natureza dos serviços prestados, se aplicável, o Fornecedor usará todas e quaisquer Informações da Empresa exclusivamente para fins de prestação dos Serviços. O Fornecedor não distribuirá, reutilizará ou compartilhará noutras aplicações, ambientes ou unidades de negócios do Fornecedor qualquer Informação da Empresa.
9. Manuseio de Dados no Final do Acordo - Com base na natureza dos serviços prestados, se aplicável, além de e sem limitar quaisquer outras obrigações do Fornecedor, a pedido da Empresa e exceto conforme de outra forma previsto no Contrato, após o expirar ou rescisão antecipada do Contrato, todas as Informações da Empresa na posse ou controle do Fornecedor ou de qualquer dos afiliados, subcontratados, prestadores de serviços, agentes ou outros consultores do Fornecedor serão destruídos ou devolvidos, conforme a Empresa escolher.
10. Notificação de Violação de Segurança - Além de, e sem limitar quaisquer outras obrigações do Fornecedor, o Fornecedor notificará a Empresa de um Evento de Segurança real ou razoavelmente suspeito dentro de 24 (vinte e quatro) horas após tomar conhecimento de tal Evento de Segurança real ou razoavelmente suspeito. O Fornecedor notificará a Empresa de tal Evento de Segurança real ou razoavelmente suspeito, contactando a equipe de Segurança da Empresa por telefone (+1-704-345-6700 – Escolha a Opção 1) e e-mail Global Operations Center globalopscnt@merck.com. O Fornecedor fornecerá informações e assistência que a Empresa possa razoavelmente solicitar em relação a um Evento de Segurança, incluindo informações de causa raiz.
11. Padrões da Indústria - Os padrões da indústria geralmente reconhecidos incluem, mas não estão limitados aos atuais padrões e *benchmarks* estabelecidos e mantidos pelos seguintes:
	1. Centro para Segurança na Internet - veja [http://www.cisecurity.org](http://www.cisecurity.org/)
	2. Indústria de Cartões de Pagamento / Padrões de Segurança de Dados (PCI/DSS) – veja <http://www.pcisecuritystandards.org/>
	3. Instituto Nacional de Padrões e Tecnologia - veja [http://csrc.nist.gov](http://csrc.nist.gov/)
	4. Norma de Gestão de Segurança da Informação Federal (FISMA) - veja [http://csrc.nist.gov](http://csrc.nist.gov/)
	5. Série ISO/IEC 27000 - veja <http://www.iso27001security.com/>
	6. Organização para o Avanço dos Padrões de Informação Estruturada (OASIS) – veja <http://www.oasis-open.org/>
	7. O Projeto de Segurança de Aplicações Web Abertas (OWASP) – veja [http://www.owasp.org](http://www.owasp.org/)
	8. O CWE (Common Weakness Enumeration) - veja [http://cwe.mitre.org](http://cwe.mitre.org/) ou CWE/SANS Top 25 Programming Errors - <http://cwe.mitre.org/top25/>
	9. O Instituto SANS - veja [http://www.sans.org](http://www.sans.org/)
	10. Erros de Software Mais Perigosos <http://www.sans.org/top25-programming-errors/>

Mediante solicitação razoável da Empresa, o Fornecedor permitirá que a Empresa audite a conformidade do Fornecedor com os requisitos listados acima. O Fornecedor corrigirá quaisquer falhas para cumprir os requisitos, assim que razoavelmente possível.

**APÊNDICE 2**

Caso a Empresa esteja exportando Informações Pessoais de forma que o Módulo 1 das Cláusulas Contratuais Padrão seja necessário, os seguintes termos se aplicam:

*O texto localizado no corpo do Módulo 1 (Controlador para Controlador) das Cláusulas Contratuais Padrão anexadas à Decisão de implementação da Comissão (UE) 2021/914 de 4 de junho de 2021 são incorporados por referência. Os aspectos opcionais são descritos abaixo:*

1. *Cláusula 7 (cláusula de ancoragem) omitida.*
2. *Para a Cláusula 11, o texto opcional foi omitido.*
3. *Para a Cláusula 17, a opção 1 foi escolhida, sendo os Países Baixos o Estado-membro.*
4. *Para a Cláusula 18, a escolha do Foro foi os Países Baixos.*

**ANEXO 1 AO APÊNDICE 2**

**A. LISTA DE PARTES**

*Consulte o Contrato*

**B. DESCRIÇÃO DA TRANSFERÊNCIA**

*Consulte o Anexo do contrato intitulado “Detalhes do Processamento de Dados”.*

**C. AUTORIDADE SUPERVISORA COMPETENTE**

****Commission Nationale de l'Informatique et des Libertés - CNIL****
3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07
Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
Website: [**http://www.cnil.fr/**](http://www.cnil.fr/)

**ANEXO 2 AO APÊNDICE 2 – MEDIDAS TÉCNICAS E ORGANIZACIONAIS**

Consulte o Apêndice 1 do DSA ao qual essas Cláusulas estão anexadas. Além disso, o importador de dados deve garantir que todos os Dados Pessoais sejam pseudonimizados e criptografados quando apropriado. Além disso, ao receber uma solicitação de uma autoridade governamental relativa aos Dados Pessoais objetos dessas Cláusulas, os Importadores de Dados e suas Afiliadas garantem que (i) as demandas de acesso por serviços de inteligência ou autoridades semelhantes nos EUA ou em outros lugares, e (ii) qualquer “dever de divulgação”, os dados pessoais descritos no Anexo 1B serão contestados pelo importador de Dados e suas Afiliadas de acordo com as leis e regulamentos aplicáveis antes da extração.

**APÊNDICE 3**

**Requisitos legais adicionais de estado, país, região e província**

**ADENDO DO REINO UNIDO: Lei de Proteção de dados de 2018**

O Apêndice 3 deste documento se incorpora, por referência, ao Adendo de Transferência de Dados Internacionais às Cláusulas Contratuais Padrão da Comissão da UE, versão B1.0, em vigor desde 21 de março de 2022, e deve ser considerado integralmente executado por todas as partes do Contrato, abrangendo todas as transferências aplicáveis, de acordo com o DSA, e incluindo todas as Cláusulas Obrigatórias da Parte 2.

**ADENDO DA SUÍÇA: FADP**

1. Na medida em que as transferências de dados descritas no Apêndice 2 estão sujeitas ao FADP, as referências ao GDPR devem ser entendidas como referências à Lei Federal Suíça sobre Proteção de Dados (“FADP”).
2. Durante o período exigido pela FADP, os dados pessoais das entidades jurídicas devem ser protegidos de acordo com essas Cláusulas da mesma maneira que são configuradas as proteções para os titulares dos dados.
3. Cláusula 13: Supervisão paralela
	1. Quando a transferência de dados for regida pela FADP: A Comissão Federal de Proteção e Informações de Dados (“FDPIC”) é o órgão supervisor competente;
	2. Quando a transferência de dados for regida pela GDPR: Os critérios da Cláusula 13(a) devem ser aplicados.
4. Cláusula 18(c): Escolha do Foro e jurisdição: Um titular dos dados, que tem sua residência habitual na Suíça, também pode acionar processos legais contra o exportador de dados e/ou importador de dados para os tribunais da Suíça.

**ADENDO DO CANADÁ: Lei de Quebec 25**

* + - 1. Qualquer notificação exigida neste DSA em relação a uma Violação de Dados Pessoais e qualquer notificação semelhante exigida pelo Contrato também será exigida para qualquer evento que constitua uma violação ou tentativa de violação deste DSA pelo Fornecedor.
			2. Se for necessário coletar consentimento em conexão aos termos deste DSA, o Fornecedor também deverá reter a evidência de todos os consentimentos por três (3) anos após o término do Contrato.

**ADITAMENTO DOS EMIRADOS ÁRABES UNIDOS: Lei Federal nº 45 de 2021 sobre a Proteção de Dados Pessoais**

1. Na medida em que as transferências de dados descritas no Apêndice 2 estejam sujeitas à Lei Federal nº 45 de 2021 dos Emirados Árabes Unidos sobre a Proteção de Dados Pessoais ("PDPL"), a menos e até que o Gabinete de Dados dos EAU emita as suas próprias cláusulas contratuais padrão para legitimar a transferência de Informação Pessoal para fora dos Emirados Árabes Unidos e as Partes tenham celebrado tais cláusulas contratuais padrão, as Partes concordam que as Cláusulas Contratuais Padrão anexadas ao presente como Apêndice 2 se aplicarão, mutatis mutandis, em relação a tais transferências, para proporcionar as salvaguardas adequadas para a Informação Pessoal e os Titulares dos Dados. Para estes efeitos: a. As referências ao "Regulamento (UE) 2016/679", "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 (Regulamento Geral sobre a Proteção de Dados)" e "esse Regulamento" são substituídas por "PDPL". b. As referências a artigos específicos do "Regulamento (UE) 2016/679" são substituídas pelo artigo ou secção equivalente do PDPL. c. As referências à "União Europeia", "União", "UE", "Estado-Membro da UE", "Estado-Membro" e "UE ou Estado-Membro" são todas substituídas por "Emirados Árabes Unidos". d. A "autoridade supervisora competente" e a "autoridade supervisora" são ambas substituídas pelo "Gabinete de Dados". e. Qualquer litígio decorrente das Cláusulas Contratuais Padrão será regido pelas leis dos Emirados Árabes Unidos e resolvido pelos tribunais dos Emirados Árabes Unidos. As Partes concordam em submeter-se à jurisdição desses tribunais. f. Em caso de inconsistência ou conflito entre o PDPL e as Cláusulas Contratuais Padrão anexadas ao presente como Apêndice 2, aplica-se o PDPL. g. Se o significado das Cláusulas Contratuais Padrão anexadas ao presente como Apêndice 2 não for claro na medida em que se aplicam a transferências de Informação Pessoal para fora dos EAU, ou se houver mais de um significado, aplica-se o significado que mais se alinha com o PDPL.
2. Se o Gabinete de Dados dos EAU emitir as suas próprias cláusulas contratuais padrão para legitimar a transferência de Informação Pessoal para fora dos Emirados Árabes Unidos, as Partes negociarão de boa fé com vista a acordar e implementar as cláusulas contratuais padrão o mais rapidamente possível. Quando as Partes celebrarem cláusulas contratuais padrão de acordo com a frase anterior, tais cláusulas contratuais padrão substituirão, em relação a transferências de Informação Pessoal sujeitas ao PDPL fora dos Emirados Árabes Unidos, as Cláusulas Contratuais Padrão anexadas ao presente como Apêndice 2, como as salvaguardas adequadas implementadas para proporcionar salvaguardas adequadas para a Informação Pessoal e os Titulares dos Dados em relação às transferências.
3. A Empresa pode revogar o seu acordo em estar vinculada pelas Cláusulas Contratuais Padrão anexadas ao presente como Apêndice 2, mediante notificação por escrito ao Fornecedor, caso o Gabinete de Dados adote uma decisão de adequação que cubra a transferência de Informação Pessoal a que se aplicam as Cláusulas Contratuais Padrão, ou caso a Empresa determine de outra forma que se aplicam outras salvaguardas adequadas em relação à transferência. A partir da data de qualquer notificação emitida pela Empresa, de acordo com a frase anterior, as Cláusulas Contratuais Padrão anexadas ao presente como Apêndice 2 deixarão de se aplicar às transferências de Informação Pessoal sujeitas ao PDPL fora dos Emirados Árabes Unidos.

**ADENDO DO BRASIL: LGPD - Cláusulas Contratuais Padrão**

As Cláusulas Contratuais Padrão do Brasil (“SCCs”) sob a Lei Geral de Proteção de Dados (Lei Geral de Proteção de Dados – “LGPD”) devem ser cumpridas onde dados de residentes brasileiros são processados, ou quando qualquer transferência de dados exigir sua aplicação. As partes concordam em adotar as SCCs em sua totalidade, conforme emitidas pela Autoridade Nacional de Proteção de Dados do Brasil (“ANPD”), salvo modificação conforme permitido expressamente pelas cláusulas. Tais SCCs são incorporadas por referência ao Acordo, com as seguintes seleções feitas onde mais de uma opção de texto é apresentada:

OPÇÃO B é selecionada para a Seção 3.1. O Importador pode realizar uma Transferência Posterior de Dados Pessoais sujeita à Transferência Internacional de Dados regida por estas Cláusulas, nos casos e condições descritos abaixo e nas disposições da CLÁUSULA 18.

OPÇÃO A é selecionada para a Seção 4.1. Sem prejuízo do dever de assistência mútua e das obrigações gerais das Partes, a Parte Designada abaixo será a principal responsável por cumprir as seguintes obrigações estabelecidas nestas Cláusulas:

a) Responsável por publicar o documento fornecido na CLÁUSULA 14:

[x] Exportador [ ] Importador

b) Responsável por responder a solicitações dos Titulares de Dados tratadas na CLÁUSULA 15:

[x] Exportador [ ] Importador

c) Responsável por notificar o incidente de segurança previsto na CLÁUSULA 16:

[x] Exportador [ ] Importador

**ADENDO DA ARÁBIA SAUDITA: PDPL - Cláusulas Contratuais Padrão**

As Cláusulas Contratuais Padrão da Arábia Saudita (“SCCs”) sob a Lei de Proteção de Dados Pessoais (“PDPL”) devem ser incorporadas onde dados de residentes sauditas são processados, onde uma transferência de dados está sujeita à jurisdição saudita ou onde a lei saudita exige o cumprimento das SCCs sauditas. A versão das SCCs alinhada com o tipo de modelo descrito no Anexo 2 é aplicável em sua totalidade e está incorporada ao Acordo por referência.