KANTAR

Se houver uma diferença de significado entre a tradução e a versão em inglês, a versão em inglês prevalecerá.

TERMOS E CONDIÇÕES

(COMPRA DE SERVIÇOS

1. **DEFINIÇÕES**

1.1. Neste Contrato, os termos a seguir têm o seguinte significado:

1.1.1. "**Contrato**" significa juntos a Ordem de Compra e estes Termos

1.1.2. "**Afiliado**" significa qualquer entidade que, direta ou indiretamente, por meio de um ou mais intermediários, Controla, é Controlada por, ou está sob Controle comum e, no caso do Cliente, está negociando como a Kantar periodicamente, exceto a Europanel.

1.1.3. **"Informações Confidenciais"** significa todas as informações relativas aos cliente e/ou qualquer membro do Grupo Kantar, os diretores, dirigentes e funcionários, orçamentos, preços, catálogo de encomendas, metodologias, questionários, contas, finanças, matrizes e filiais do Cliente e/ou de qualquer membro do Kantar Group, Dados do Cliente e seus clientes.

1.1.4. "**Controle**" significa:

(a) a posse, direta ou indireta, do poder de dirigir a administração ou as políticas de tal entidade, seja através da propriedade de títulos com direito a voto, por contrato relativo aos direitos de voto, ou de outra forma, ou

(b) a posse, direta ou indireta, de mais de 50% (cinquenta por cento) dos títulos com direito a voto em circulação ou outra participação de propriedade dessa entidade.

.

1.1.5. "**Cliente**" significa o Afiliado da Kantar indicado na Ordem de Compra.

1.1.6. "**Dados do Cliente**" significa quaisquer dados (incluindo quaisquer Dados Pessoais relacionados à equipe, clientes ou fornecedores do Cliente ou seus clientes), documentos, textos, desenhos, diagramas, especificações, imagens (juntamente com qualquer banco de dados composto por estes) fornecidos ou disponibilizados para o Fornecedor por ou em nome do Cliente ou de seus clientes ou que o Fornecedor é obrigado a gerar, processar, armazenar ou transmitir segundo o presente Contrato.

1.1.7. "**Lei de Proteção de Dados**" significa o Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD) e a Diretiva Europeia de Privacidade e Comunicações Eletrônicas (conforme aditamento periódico) e qualquer lei que implemente

essas Diretivas em qualquer país.

1.1.8. "**Deliverables**" significa todos os produtos, itens, equipamentos e materiais a serem fornecidos como parte dos Serviços.

1.1.9. "**Taxas**" significa o montante total a ser pago pelo Cliente, conforme indicado na Ordem de Compra.

1.1.10. "**RGPD**" significa o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção dos indivíduos no que diz respeito ao tratamento de dados pessoais e da livre circulação dos referidos dados, e que revoga a Diretiva 95/46/EC do Conselho (Regulamento Geral de Proteção de Dados).

1.1.11. "**Direitos de Propriedade Intelectual**" significa todas as patentes, direitos a invenções, direitos autorais e os direitos relacionados, direitos morais, direitos de banco de dados, direitos de topografia de semicondutores, modelos de utilitário, direitos em desenhos, marcas comerciais, marcas de serviço, nomes comerciais, nomes de domínio, direitos de reputação da empresa, direitos sobre informações não divulgadas ou confidenciais, e outros direitos semelhantes ou equivalentes ou formas de proteção que podem existir agora ou no futuro em qualquer parte do mundo.

1.1.12. "**Dados Pessoais**" tem o significado atribuído no Anexo 3.

1.1.13. "**Ordem de Compra**" significa a ordem de compra anexada a estes Termos e Condições ou qualquer outra forma de comunicação escrita que faz referência ao número da Ordem de Compra e a que estes Termos e Condições aplicam-se.

1.1.14. "**Serviços**" significa os serviços especificados na Ordem de Compra ou a referência ao número da Ordem de Compra, especificando os serviços em qualquer outra forma de comunicação escrita.

1.1.15. "**Fornecedor**" significa a entidade identificada na Ordem de Compra.

1.1.16. "**Pessoal do Fornecedor**" significa todo o pessoal necessário para a execução dos Serviços.

1.1.17. "**Políticas do Fornecedor**" significa todas as políticas ou códigos de conduta aplicáveis aos fornecedores da Kantar Group Limited e suas subsidiárias diretas ou indiretas, comunicadas pelo Cliente ao Fornecedor periodicamente ou disponibilizadas em qualquer extranet operada pelo Cliente para seus fornecedores de vez em quando (que serão disponibilizadas mediante solicitação) incluindo, mas não se limitando, ao Código de Conduta Comercial da Kantar anexado a este documento como Anexo 1 e quaisquer políticas antissuborno da Kantar aplicáveis.

2. OS SERVIÇOS

2.1.1. Estes Termos e Condições aplicam-se aos Serviços.

2.1.2. A Ordem de Compra deverá ser considerada aceita assim que os Serviços forem iniciados. O Fornecedor deverá prestar os Serviços a partir da data especificada na

Ordem de Compra. O Fornecedor deverá prestar os Serviços ao Cliente em conformidade com as solicitações do Cliente periodicamente, com as Políticas do Fornecedor, melhores práticas do setor e os termos deste Contrato. O tempo para o desempenho dos Serviços é fundamental.

2.1.3. O Fornecedor garante que cada um que compõe a Equipe do Fornecedor:

(a) deverá cumprir as Políticas do Fornecedor atualizadas periodicamente

(b) seja devidamente qualificado e treinado para a prestação dos Serviços;

(c) tenha passado pela devida triagem de acordo com quaisquer instruções específicas emitidas pelo Cliente e que não tem nenhuma condenação criminal e

(d) está qualificado para trabalhar no território no qual os Serviços estão sendo prestados.

2.1.4. O Fornecedor garante, compromete-se e declara continuamente que:

(a) ele tem plena capacidade e autoridade para celebrar este Contrato e desempenhar suas obrigações segundo os termos do presente Contrato;

(b) está em conformidade com todas as leis aplicáveis, regulamentos e códigos de prática;

(c) não fará nenhum ato nem qualquer omissão em relação ao cumprimento das suas obrigações segundo o presente Contrato que afete ou possa afetar adversamente a reputação do Cliente ou de seu cliente, e

(d) os Deliverables estão completos, corretos, não infringem e cumprem em todos os aspectos o presente Contrato.

3. TARIFAS

3.1. O Fornecedor só deve ter o direito de faturar o Cliente após a conclusão dos Serviços para a satisfação razoável do Cliente.

3.2. O Cliente deverá pagar as Tarifas pelos Serviços no próximo ciclo de pagamento do Cliente após uma data que seja de 60 (sessenta) dias após o término do mês em que uma fatura válida especificando o número correto da OC for recebida. Quando os Serviços forem adquiridos do Fornecedor pelo Cliente, agindo em benefício de um cliente, o Cliente não será obrigado a efetuar o pagamento ao Fornecedor até que tenha recebido o pagamento do cliente. As Tarifas são isentas de impostos sobre vendas ou outros impostos semelhantes. O Cliente tem o direito de fazer deduções ou retenções das Tarifas quando exigido por lei.

3.3. O Fornecedor poderá cobrar juros sobre qualquer montante em atraso não contestado à taxa de 2% acima da taxa-base anual do Banco da Inglaterra.

4. RESCISÃO

4.1. O Cliente poderá rescindir este Contrato, no todo ou (com uma redução proporcional da taxa) em parte, a qualquer momento:

4.1.1. com antecedência de 30 (trinta) dias de notificação por escrito ao Fornecedor ou

4.1.2. imediatamente se o Fornecedor violar substancialmente este Contrato e não sanar a referida violação em 14 dias após o Fornecedor ter sido notificado pelo Cliente para fazê-lo ou

4.1.3. imediatamente se um pedido for feito ou se for aprovada uma resolução para a liquidação do Fornecedor, ou se o Fornecedor tiver um receptor ou o administrador nomeado de qualquer parte dos seus bens, se surgirem circunstâncias que autorizam o tribunal ou um credor a nomear um receptor ou administrador, se um tribunal emitir um pedido de liquidação ou administração, se fizer um acordo com os credores ou

4.1.4. se o Fornecedor não puder pagar suas dívidas, como e quando elas vencerem.

4.2. Mediante a expiração ou rescisão do presente Contrato ou de qualquer parte dos Serviços, o Fornecedor entregará todas as Informações Confidenciais ao Cliente e estabelecerá contato com o Cliente e/ou com terceiros para garantir uma entrega satisfatória.

4.3. A expiração ou o término deste Contrato não prejudica nenhum direito acumulado até a data da rescisão nem de quaisquer cláusulas que expressamente ou implicitamente sobrevivam à rescisão.

5. AUDITORIA

5.1. O Fornecedor deverá manter em seu principal local de negócios livros e registros reais e precisos dos Serviços (incluindo, mas não se limitando, a planilhas, registros de reclamações, faturas, despesas, custos, notas de crédito) em conformidade com os princípios geralmente aceitos de contabilidade e de retenção de documentos durante a vigência deste Contrato e por um período de 6 anos após o término dele e permitir que o Cliente e/ou seu cliente ou o representante autorizado do Cliente inspecione tais registros, mediante aviso por escrito razoável para fins de avaliação do cumprimento deste Contrato (incluindo, sem limitação, as restrições estabelecidas na Cláusula 10). Se, como resultado de uma auditoria, o Cliente descobrir qualquer pagamento em excesso em relação aos Serviços ou qualquer outra não conformidade com os termos deste Contrato, o Fornecedor deverá, o mais rapidamente possível, corrigir a referida não conformidade às suas próprias custas e reembolsar ao Cliente o montante total de qualquer pagamento em excesso e os custos da auditoria.

6. RESPONSABILIDADE E INDENIZAÇÃO

6.1. Nada no presente Contrato excluirá nem limitará a responsabilidade da cada uma das partes em relação a quaisquer reclamações:

6.1.1. por morte ou ferimentos pessoais causados por negligência da referida parte ou

6.1.2. resultante de qualquer fraude, incluindo falsas declarações feitas por essa parte ou

6.1.3. pelas quais a responsabilidade não possa ser legalmente excluída ou limitada ou

6.1.4. por qualquer indenização fornecida pelo Fornecedor ao Cliente segundo este Contrato ou

6.1.5. por qualquer violação por parte do Fornecedor das Cláusulas 8 a 10, inclusive, ou 12.1, ou

6.1.6. por qualquer falha intencional ou deliberada por parte do Fornecedor.

6.2. Sujeito à Cláusula 6.1, o Cliente não será responsável por quaisquer danos indiretos, especiais ou consequenciais nem por lucros cessantes (diretos ou indiretos), danos à reputação, perda de negócios, perda de receita ou perda de economias antecipadas.

6.3. O Fornecedor deverá indenizar o Cliente contra todas as perdas, custos, responsabilidades, danos, despesas, reclamações e processos incorridos e/ou sofridos pelo Cliente em decorrência de ou com relação a:

6.3.1. qualquer violação deste Contrato ou

6.3.2. qualquer perda ou dano à propriedade do Cliente durante a prestação dos Serviços ou

6.3.3. qualquer ato ou omissão negligente por parte do Fornecedor, Equipe do Fornecedor e/ou subcontratados ou seus funcionários em conexão com este Contrato ou

6.3.4. qualquer alegação de que o uso dos Deliverables e/ou Serviços viola os Direitos de Propriedade Intelectual de qualquer terceiro.

6.4. Sujeito às Cláusulas 6.1 e 6.2, a responsabilidade total agregada do Cliente decorrente de ou relacionada a este Contrato (seja em contrato, ato ilícito extracontratual, incluindo negligência ou de outra forma) não deve exceder um montante igual ao das Tarifas pagas ou a serem pagas ao Fornecedor pelo Cliente de acordo com este Contrato nos 12 (doze) meses anteriores ao evento que desencadeou tal responsabilidade.

6.5. Sujeito às Cláusulas 6.1 e 6.2, a responsabilidade total agregada do Fornecedor decorrente ou relacionada a este Contrato (seja em contrato, ato ilícito excontratual, incluindo negligência ou de outra forma) não deve exceder R$ 48.900.000,00 (quarenta e oito milhões e novecentos mil reais) por reivindicação.

7. **SEGURO**

7.1. O Fornecedor deverá contratar e manter com uma seguradora terceirizada respeitável um seguro para cobrir as obrigações e responsabilidades do Fornecedor nos termos do presente Contrato e:

7.1.1. no que diz respeito à sua responsabilidade pública, por um valor mínimo de R$ 4.890.000,00 para qualquer evento e ilimitado no período de seguro relevante;

7.1.2. no que diz respeito à sua responsabilidade do empregador, por um valor mínimo de R$ 24.450.000,00 para qualquer evento e ilimitado no período de seguro relevante;

7.1.3. no que diz respeito à sua responsabilidade de indenização profissional, por um valor mínimo de R$ 4.890.000,00 para qualquer evento e ilimitado no período de seguro relevante.

7.2. Cada referida apólice deve indicar o Cliente como segurado adicional e deve conter uma cláusula de indemnização aos diretores. Cada referida apólice não deve solicitar contribuição e não deve ser superior a qualquer outro seguro disponível para o Cliente. O Cliente não será responsável em relação aos descontos a serem pagos, e os referidos descontos não devem ser inferiores a R$ 244.500,00.

7.3. O Fornecedor deve fazer um seguro adicional, conforme o Cliente solicitar razoavelmente periodicamente**.**

8. **PROTEÇÃO DE DADOS**

8.1. Se a prestação de Serviços requerer o tratamento de Dados Pessoais por parte do Fornecedor em nome do Cliente, o Fornecedor:

8.1.1. cumprirá a Lei de Proteção de Dados;

8.1.2. agirá somente segundo as instruções do Cliente como controlador de dados;

8.1.3. cumprirá o Anexo 2 (Adendo de Segurança de Informações);

8.1.4. respeitará o Anexo 3 (Proteção de Dados: RGDP).

8.2. O Fornecedor deverá indenizar o Cliente contra todas as perdas, responsabilidades, reivindicações, despesas, danos e custos sofridos ou incorridos pelo Cliente como resultado da falha do Fornecedor em cumprir a Cláusula 8 da Lei de Proteção de Dados e as cláusulas do Anexo 3.

8.3. O Fornecedor deverá respeitar as condições específicas exigidas pelo RGPD com relação a quaisquer Serviços que exijam o processamento de Dados Pessoais conforme estabelecido no Anexo 3.

8.4. O Fornecedor garante que deve dispor de medidas que incorporam a norma de segurança de informações ISO/IEC 27001 ou qualquer outra norma equivalente que a substitua de tempos em tempos.

9. **DIREITOS DE PROPRIEDADE INTELECTUAL**

9.1. Sujeito à Cláusula 9.2, o Cliente deverá possuir os Direitos de Propriedade Intelectual sobre os Deliverables e o Fornecedor, por meio deste, cede de forma irrevogável e incondicional com o título de total garantia ao Cliente todos e quaisquer Direitos de Propriedade Intelectual, mediante a criação deles, com relação aos Deliverables. O Fornecedor deverá, e providenciará que a Equipe do Fornecedor renuncie em favor do Cliente de forma absoluta e irrevogável seus direitos morais (se houver) em relação a tais Deliverables.

9.2. Nada neste Contrato destina-se a afetar a propriedade dos materiais do Fornecedor usados ou desenvolvidos por ele de forma independente dos Serviços ou metodologias genéricas do Fornecedor, ferramentas, tecnologia ou processos que são usados por ele (mas não desenvolvidos por ele) no desempenho dos Serviços (juntos constituem os “Materiais Preexistentes do Fornecedor“). Se os Materiais Preexistentes do Fornecedor (ou parte deles) forem incorporados nos Deliverables ou se forem necessários para usar ou explorar os Serviços, o Fornecedor, por meio deste, concede ao Cliente uma licença perpétua, mundialmente válida, irrevogável, não exclusiva e isenta de royalties para usar os Materiais Preexistentes do Fornecedor para permitir que o Cliente obtenha o benefício total dos Serviços.

9.3. O Fornecedor garante e declara que ele tem o direito de ceder ou licenciar todos os Direitos de Propriedade Intelectual concedidos ou atribuídos segundo o presente Contrato e que a concessão e os termos de sua respectiva cessão ou licença não devem infringir os Direitos de Propriedade Intelectual de qualquer terceiro.

9.4. O Fornecedor não adquire nenhum direito, titularidade de direito ou interesse em nenhum Direito de Propriedade Intelectual de propriedade ou licenciado por algum terceiro ao Cliente em virtude deste Contrato, e o Fornecedor reconhece que todos os Direitos de Propriedade Intelectual continuam sendo propriedade do Cliente e/ou de seus licenciadores.

10. **PROIBIÇÃO DE SUBORNO**

10.1. O Fornecedor deverá cumprir o Foreign Corrupt Practices Act, 15 U.S.C. §78dd-2 (o “FCPA”) e o UK Bribery Act 2010 (o "UKBA") e devem exigir a conformidade com o FCPA e o UKBA por parte de suas empresas do grupo, associados e cada um dos seus respectivos diretores, funcionários, agentes e intermediários ou de qualquer parte que estiver prestando um serviço para o Cliente (cada um deles uma "Pessoa Associada").

10.2. O Fornecedor não deve adquirir e deverá providenciar que cada Pessoa

Associada não deverá, direta ou indiretamente, solicitar, concordar em receber ou aceitar um auxílio financeiro ou outro em violação de seu direito legal nem induzi-la a exercer sua influência para afetar ou influenciar qualquer ato ou decisão (incluindo o desempenho inadequado de qualquer função) por parte dela nem para obter ou manter negócios para o Cliente. O Fornecedor deverá notificar o Cliente por escrito imediatamente se tiver conhecimento de qualquer violação do FCPA, UKBA ou desta Cláusula 10.

11. **MATERIAIS DO CLIENTE**

11.1. A titularidade de direito sob qualquer propriedade do Cliente ou de um cliente do Cliente fornecida ao Fornecedor para o desempenho dos Serviços deve permanecer com o Cliente ou com seus clientes (conforme aplicável).

11.2. Sujeito a um aviso prévio razoável, o Cliente ou seu cliente terá direito a retomar a posse de sua propriedade do Fornecedor a qualquer momento.

11.3. O Fornecedor deve manter a segurança de qualquer propriedade do Cliente ou de qualquer cliente do Cliente em seu poder e não dispor de ou de parte do que está em seu poder sem o consentimento por escrito do Cliente ou de seus clientes, salvo disposição em contrário exigida para o desempenho dos Serviços.

11.4. Por meio deste, o Fornecedor renuncia a qualquer garantia ou outro direito que ele possa ter sobre qualquer propriedade do Cliente ou de um cliente do Cliente e deve manter o mesmo livre de todos os gravames e outros encargos.

11.5. O Fornecedor só deverá usar a propriedade do Cliente ou de qualquer cliente do Cliente em conexão com o desempenho dos Serviços a que se referem.

12. **LEI DE ESCRAVIDÃO MODERNA**

12.1. O Fornecedor garante que nem o Fornecedor, nem qualquer de seus diretores, empregados, agentes ou subcontratados:

12.1.1. cometeu um delito segundo a Lei de Escravidão Moderna de 2015 (um "Crime de MSA");

12.1.2. foi notificado de que está sujeito a uma investigação com relação a um suposto Crime de MSA ou acusação segundo a Lei de Escravidão Moderna de 2015;

12.1.3. está ciente de quaisquer circunstâncias em sua cadeia de suprimento que poderia dar origem a uma investigação com relação a um suposto Crime de MSA ou acusação segundo a Lei de Escravidão Moderna de 2015;

12.1.4. deve estar em conformidade com a Lei de Escravidão Moderna de 2015;

12.1.5. deve notificar o Cliente imediatamente por escrito se tomar conhecimento ou tiver motivo para acreditar que ele ou qualquer um de seus diretores, empregados, agentes ou subcontratados violaram ou possivelmente violaram qualquer das obrigações do Fornecedor segundo a Cláusula 12.

13. **DISPOSIÇÕES GERAIS**

13.1. O Fornecedor deve, durante este Contrato, e por um período de 5 anos após a vigência dele, manter o sigilo de todas as Informações Confidenciais e não deverá usar nem divulgar tais Informações Confidenciais a qualquer terceiro, exceto se for estritamente necessário para executar os Serviços ou se exigido por lei.

13.2. Nenhuma das partes pode ceder, subcontratar ou, de alguma forma, transferir quaisquer direitos ou obrigações de acordo com o referido Contrato sem o consentimento prévio por escrito da outra parte, exceto se o Cliente puder ceder seus direitos a

qualquer subsidiária (direta ou indireta) da The Kantar Group Ltd.

13.3. Cada cláusula deste Contrato pode ser autônoma e distinta das outras. A invalidade ou inexequibilidade de uma cláusula específica não prejudica as outras cláusulas do presente Contrato.

13.4. Qualquer falha em exercer ou qualquer atraso no exercício de um direito ou recurso previsto neste Contrato, na lei ou na equidade não constituirá uma renúncia de direitos nem recursos ou ainda uma renúncia de quaisquer outros direitos ou recursos.

13.5. Nada no presente Contrato deve ser interpretado como a criação ou implicação de uma parceria ou relação de agenciamento entre as partes.

13.6. Este Contrato constitui o acordo integral e o entendimento entre as partes no que diz respeito aos assuntos tratados e substitui qualquer acordo anterior entre as partes com relação a essas questões. Este Contrato só poderá ser alterado, por escrito, com o consentimento do Cliente e do Fornecedor.

13.7. Nenhuma pessoa que não seja uma parte no presente Contrato tem quaisquer direitos concedidos na Lei de Contratos de 1999 (Direitos de Terceiros).

13.8. Qualquer aviso que deva ser dado segundo este Contrato deve ser por escrito e só deverá ser considerado válido se for enviado para a outra parte no endereço da ordem de Compra pessoalmente, por meio de correio registado ou entrega especial.

13.9. Este Contrato e quaisquer obrigações extracontratuais serão regidos pelas leis da Inglaterra, e as partes concordam em submeter qualquer litígio à jurisdição não exclusiva dos tribunais ingleses. A versão em inglês deste Contrato e qualquer aviso ou outro documento relacionado a este Contrato prevalecerão em caso de conflito.

CRONOGRAMA 1 : CÓDIGO DE CONDUTA NOS NEGÓCIOS DA KANTAR

A Kantar e suas empresas operam em vários mercados e países em todo o mundo. Em todos os casos, nós respeitamos as leis nacionais e quaisquer outras leis com alcance internacional, tais como a UK Bribery Act, a US Foreign Corrupt Practices Act e a UK Modern Slavery Act, quando pertinente, e códigos de conduta do setor. Temos o compromisso de agir de maneira ética em todos os aspectos de nosso negócio e de manter os mais elevados padrões de honestidade e integridade.

Esperamos e exigimos que todos os nossos parceiros de negócios, incluindo os fornecedores, tenham o mesmo compromisso com o comportamento ético e, portanto, pedimos que você confirme estar de acordo com nosso Código de Conduta nos Negócios (na primeira coluna), conforme alterações, onde necessário, para entidades que não sejam da Kantar (na segunda coluna).

Esperamos que todos os nossos fornecedores usem sistemas adequados para facilitar e monitorar a conformidade com esses padrões e a adesão às leis locais e internacionais aplicáveis.

Esperamos que os nossos fornecedores demonstrem seu compromisso com os princípios do presente código e tenham um processo contínuo de gerenciamento de riscos para identificar as práticas ambientais, relacionadas à saúde e segurança e práticas laborais, além de riscos éticos associados às operações dos fornecedores.

Os fornecedores devem incentivar a equipe a informar problemas sem medo de ameaças ou represálias. Os fornecedores devem tomar as medidas adequadas, conforme necessário.

Os fornecedores devem colocar em prática normas equivalentes a este Código para sua própria Cadeia de Suprimento.

Código da Kantar	**O que a Kantar espera de seus fornecedores**
Nós, os funcionários e a equipe de todas as da Kantar Group (“o Grupo”) reconhecemos nossas obrigações em relação a todos aqueles que participam do nosso sucesso, incluindo proprietários, clientes, funcionários e fornecedores.	Você confirma que reconhece nossas obrigações e não atuará em detrimento de tais obrigações.
As informações sobre nossa empresa devem ser comunicadas de forma clara e precisa, de forma não discriminatória e em conformidade com os regulamentos locais.	Você confirma que tratará as informações sobre a Kantar Group conforme descrito a seguir.
Selecionamos e promovemos membros da nossa equipe com base em suas qualificações e mérito, sem qualquer discriminação ou preocupação quanto à raça, religião, nacionalidade, cor, sexo, orientação sexual, identidade ou expressão de gênero, idade ou deficiência.	Você confirma que tem políticas equivalentes na sua organização.
Acreditamos que um local de trabalho deve ser seguro e civilizado, e que o emprego deve ser escolhido livremente. Não toleraremos assédio sexual, discriminação ou comportamento ofensivo de qualquer natureza, isso inclui o rebaixamento persistente de indivíduos por meio de palavras ou ações, a exibição ou distribuição de material ofensivo ou o uso ou posse de armas na Kantar ou nas instalações do cliente.	Você confirma que tem políticas equivalentes na sua organização e para a sua cadeia de suprimentos, e que respeitará o nosso local de trabalho e as pessoas como descrito. Em especial: • O emprego deve ser escolhido livremente; o trabalho forçado ou compulsório, ou qualquer outra forma de escravidão moderna, não pode ser

	usada; • Os trabalhadores não devem ser forçados a fornecer passaportes ou identidades emitidas pelo governo como condição de emprego; • Trabalho infantil não pode ser usado; • As remunerações pagas aos trabalhadores devem cumprir com todas as leis de remuneração aplicáveis; • As semanas de trabalho não devem exceder o máximo estabelecido pela legislação local; • Os trabalhadores não devem sofrer tratamento desumano, incluindo assédio sexual, abuso sexual, punição corporal, coerção física ou abuso verbal; • A Kantar espera que seus fornecedores criem e promovam condições de trabalho seguras para todos os trabalhadores; • A exposição do trabalhador a riscos físicos deve ser eliminada sempre que possível, ou, pelo menos, controlada; • Os fornecedores devem ter procedimentos em vigor adequados para lidar com emergências que podem afetar os trabalhadores; e • Devem haver sistemas em vigor para gerenciar, rastrear e relatar lesões e doenças ocupacionais.
Não toleraremos o uso, posse ou distribuição de drogas ilícitas ou que nosso pessoal relate a ocorrência de trabalho sob a influência de drogas ou álcool.	Você confirma que tem políticas equivalentes na sua organização e que respeitará o nosso local de trabalho e as pessoas conforme descrito.
Trataremos de todas as informações relativas aos negócios do Grupo, ou aos seus clientes, como confidenciais. Em particular, a prática de "insider trading" é expressamente proibida, e informações confidenciais não devem ser usadas para ganho pessoal;	Você confirma que concorda com a nossa política em relação às nossas informações.
Estamos empenhados em proteger os dados do consumidor, do cliente e dos funcionários de acordo com as leis nacionais e códigos do setor.	Você confirma que tem compromissos equivalentes em sua organização que cobrem todas as informações de e relacionadas aos nossos negócios e a de nossos parceiros no negócio.
Nós não criaremos conscientemente uma obra	Sempre que relevante, confirme se você tem

que contenha instruções, sugestões ou imagens ofensivas à decência pública em geral e dará a devida consideração para o impacto do nosso trabalho em segmentos minoritários da população, seja essa minoria por raça, religião, nacionalidade, cor, sexo, orientação sexual, identidade ou expressão de gênero, idade ou deficiência,	padrões equivalentes para o seu trabalho.
Não realizaremos trabalhos que se destinam ou que foram concebidos para enganar, incluindo no que se refere às questões sociais, ambientais e de direitos humanos.	Sempre que relevante, confirme se você tem padrões equivalentes para o seu trabalho.
Consideraremos o potencial de clientes ou trabalho para prejudicar a reputação do Grupo antes de assumi-los. Isso inclui danos à reputação decorrentes da associação com os clientes que participam de atividades que contribuem para o abuso dos direitos humanos.	Essa situação está relacionada somente a membros da Kantar Group.
Não nos envolveremos direta ou indiretamente para ganho pessoal ou familiar em nenhuma atividade que concorra com as empresas do Grupo ou com nossas obrigações com relação a qualquer uma dessas empresas.	Essa situação está relacionada somente a membros do Kantar Group.
Não vamos dar, oferecer nem aceitar propinas, em dinheiro ou de outra forma, para ou de qualquer terceiro, incluindo, mas não se restringindo a funcionários do governo, clientes e corretores ou seus representantes. Coletivamente garantimos que todos os funcionários compreendam essa política por meio de treinamentos, comunicados e pelo exemplo;	Isso se aplica diretamente a você.
Não aceitaremos para nosso benefício pessoal mercadorias ou serviços de valor superior ao valor nominal de fornecedores, possíveis fornecedores nem de terceiros.	Isso se aplica diretamente a você.
Não teremos qualquer conflito de interesse pessoal ou familiar de interesse nas nossas empresas ou com nossos fornecedores ou outros terceiros com os quais fazemos negócios.	Você deve ter políticas equivalentes em sua organização.
Não é permitido fazer contribuições corporativas de qualquer natureza, incluindo a prestação de serviços ou o fornecimento de materiais por um preço inferior ao valor de mercado, a políticos, partidos políticos ou sindicatos, sem a aprovação prévia por escrito da diretoria da Kantar.	Você deve ter a sua própria política sobre tais contribuições, juntamente com os procedimentos de autorização apropriados.
Continuaremos lutando para fazer uma contribuição positiva para a sociedade e o meio ambiente: mantendo elevados padrões de éticosa de marketing; respeitando os direitos humanos em nosso negócio, na nossa cadeia de suprimento e por meio do nosso trabalho com os clientes; respeitando o meio ambiente; apoiando	Você deve ter políticas equivalentes em sua orgnaização. Em especial: • Os fornecedores devem cumprir com a Lei de Escravidão Moderna do Reino Unido;

as organizações comunitárias; apoiando o desenvolvimento dos funcionários; e gerenciando riscos significativos em nossa cadeia de suprimentos. Nossa Política de Sustentabilidade e Política de Direitos Humanos fornecem mais detalhes sobre os nossos compromissos nestas áreas.	• Os fornecedores devem obter todas as autorizações ambientais relevantes, inclusive para resíduos e emissões; Os fornecedores devem se esforçar para evitar a poluição por meio da implementação de medidas de conservação em suas instalações e processos, reciclando, reutilizando e substituindo materiais.

Confirmamos que observamos o Código de Conduta nos Negócios da Kantar, conforme modificado para a nossa organização. Se tomarmos conhecimento de qualquer violação, particularmente em relação a suborno ou presentes ou serviços inadequados para ou de sua organização ou quaisquer terceiros, ou em relação a outros assuntos que possam prejudicar a reputação da Kantar diretamente ou por associação, lhe informaremos imediatamente.

Assinatura:

Nome:

Cargo:

Organização:

Data:

CRONOGRAMA 2 : ADENDO DE SEGURANÇA DE INFORMAÇÕES

1. **INTRODUÇÃO.**

1.1. Este Anexo de Requisitos de Segurança (este "**Anexo**") estabelece os requisitos básicos de segurança de informações do Fornecedor, conforme necessário, para garantir a confidencialidade, disponibilidade e integridade das Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente. O fornecedor deve obedecer a estes requisitos em todo o desempenho do Fornecedor de serviços segundo este Contrato.

2. **TERMINOLOGIA.**

2.1. Como usado neste Anexo, cada um dos termos a seguir (se usados com inicial maiúscula ou com todas as letras em minúsculo) tem o significado correspondente estabelecido abaixo. Outro termo com inicial maiúscula aqui utilizado, mas não definido neste documento, deve ser entendido na acepção do presente Contrato.

2.2. **Prestador de Serviços** significa um subcontratado, prestador de serviços independente, prestador de serviços ou agente do Fornecedor que armazena, processa, controla ou tem acesso a qualquer Informação Confidencial do Cliente e Informações Confidenciais do cliente do Cliente.

2.3. **Informações Confidenciais do Cliente** significa quaisquer Informações Confidenciais do Cliente e Informações Confidenciais do cliente do Cliente que incluem Dados Pessoais [e-mail, nome etc.], informações sobre saúde, informações financeiras ou informações de holdings de investimentos.

2.4. **Criptografia** significa a transformação reversível de dados do formato original (texto comum) para um formato ofuscado (texto cifrado) como um mecanismo para proteger a confidencialidade, integridade e/ou autenticidade das informações. A criptografia exige um algoritmo de criptografia e uma ou mais chaves de criptografia.

2.5. **Armazenar** significa armazenar, arquivar, fazer backup e/ou realizar quaisquer atividades semelhantes.

3. **REVISÕES DE SEGURANÇA.**

3.1. O Fornecedor deve fornecer ao Cliente o direito a uma revisão no local do programa de segurança do Fornecedor anualmente para todo o período que o Fornecedor processar, armazenar ou de outra forma tiver acesso a Informações Confidenciais do Cliente e Informações Confidenciais do cliente do Cliente. O Fornecedor programará imediatamente (mas em nenhum caso 30 (trinta) dias após o recebimento de solicitação do Cliente para agendar e realizar tal revisão) a referida revisão em uma data de comum acordo.

3.2. O Fornecedor deve fornecer ao Cliente acesso às políticas, aos procedimentos e a qualquer outra documentação relevante do Fornecedor e à Equipe do Fornecedor, conforme razoavelmente necessário para facilitar as referidas revisões. O Fornecedor deve apresentar um plano de correção para o Cliente no prazo de 30 (trinta) dias após a conclusão dessa revisão, e o Fornecedor deverá corrigir cada problema em tempo hábil, de acordo com um cronograma de correção acordado pelas partes.

4. **REQUISITOS ESPECÍFICOS DE SEGURANÇA.**

4.1. **Política de Segurança**

O Fornecedor deverá manter um conjunto abrangente de políticas e procedimentos de segurança por escrito que abranjam, no mínimo:

4.1.1. o compromisso do Fornecedor com a segurança de informações;

4.1.2. classificação de informações, rotulagem e manuseamento, e as referidas políticas e procedimentos relacionados à manipulação de informações devem descrever os métodos admissíveis para a transmissão de informações, armazenamento e destruição, e esses métodos não devem proteger menos do que aqueles estabelecidos nas Diretrizes de Proteção de Informações do Fornecedor ao Cliente estabelecidos abaixo;

4.1.3. o uso aceitável dos bens do Fornecedor, incluindo sistemas de computação, redes e mensagens;

4.1.4. gestão de incidentes de segurança da informação, incluindo a notificação de violação de dados e a coleta de procedimentos de provas;

4.1.5. regras de autenticação para o formato, o conteúdo e o uso de senhas para usuários finais, administradores e sistemas;

4.1.6. controles de acesso, incluindo revisões periódicas dos direitos de acesso;

4.1.7. medidas disciplinares para a Equipe que não cumprir essas políticas e procedimentos e

4.1.8. os temas descritos no restante desta Seção 4 de uma maneira consistente com os requisitos aplicáveis para tais tópicos conforme estabelecido na Seção 4.

O fornecedor deverá notificar a Kantar sobre quaisquer alterações fundamentais nas suas políticas em até 30 (trinta) dias.

4.2. **Responsabilidade pelo Programa de Segurança de Informações do Fornecedor**

O Fornecedor deve manter uma responsabilidade de segurança de informações, com a equipe designada para manter o programa de segurança de informações do fornecedor e executar o gerenciamento de riscos de informações.

4.3. **Auditorias, Revisão e Monitoramento do Programa de Segurança de Informações do Fornecedor**

O Fornecedor deve monitorar e revisar regularmente o programa de segurança de informações do Fornecedor para garantir que as proteções sejam adequadas para limitar os riscos para as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente.

4.4. **Gerenciamento de Informações e Ativos**

O Fornecedor deverá:

4.4.1. manter um inventário de todas as Informações Confidenciais do Cliente e Informações Confidenciais do cliente do Cliente que o Fornecedor processa ou armazena;

4.4.2. manter um inventário de ativos de software e computação física que o Fornecedor usa para desempenhar suas atividades segundo este Contrato e

4.4.3. seguir as Diretrizes de Proteção de Informações do Fornecedor do Cliente (definidas abaixo) durante o tratamento, processamento e armazenamento das Informações Confidenciais do Cliente e das Informações Confidenciais do cliente do Cliente.

4.5. **Segurança Física e Ambiental**

O Fornecedor deverá:

4.5.1. restringir a entrada nas áreas do Fornecedor nas quais as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente são armazenadas, acessadas ou processadas exclusivamente para a equipe autorizada do Fornecedor para tal acesso;

4.5.2. implementar as melhores práticas de sistemas de infraestruturas razoáveis, incluindo sistemas de combate a incêndios, refrigeração e energia, sistemas de emergência e de segurança dos funcionários;

4.5.3. fornecer controles de entrada física em todas as áreas nas quais as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente são armazenadas, acessadas ou processadas para que sejam compatíveis com a susceptibilidade das Informações Confidenciais do Cliente e das Informações Confidenciais do cliente do Cliente;

4.5.4. monitorar regularmente as áreas nas quais as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente são tratadas, armazenadas e/ou processadas

4.6. **Assuntos Relacionados aos Funcionários**

O Fornecedor deverá:

4.6.1. executar verificações de histórico criminal de cada pessoa da equipe do Fornecedor (incluindo Prestadores de Serviços, se for permitido por lei, que tenha acesso às Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente, exceto na medida limitada ou proibida pelas leis aplicáveis; essas verificações de histórico devem ser realizadas antes de permitir que tal indivíduo acesse as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente, e o Fornecedor não deverá permitir que qualquer indivíduo que não tenha uma verificação de histórico satisfatória acesse as Informações Confidenciais do Cliente nem as Informações Confidenciais do cliente do Cliente;

4.6.2. treinar sua nova equipe (incluindo Prestadores de Serviços) sobre o uso aceitável e o tratamento das informações confidenciais do Fornecedor e as informações confidenciais de outras empresas a quem o Fornecedor confiou as referidas informações (como Informações Confidenciais do Cliente e Informações Confidenciais do cliente do Cliente);

4.6.3. proporcionar treinamento e educação de segurança e privacidade de dados para sua equipe (incluindo Prestadores de Serviços) e manter um registro da equipe que concluiu tal treinamento e

4.6.4. implementar um procedimento de cancelamento de registro e registro de usuário formal para conceder e revogar acesso a serviços e sistemas de informação do Fornecedor e, mediante a rescisão de qualquer membro da equipe do Fornecedor (incluindo Prestadores de Serviços), o Fornecedor deverá revogar o acesso de tal indivíduo às Informações Confidenciais do Cliente e às Informações Confidenciais do cliente do Cliente assim que possível, mas em nenhum caso superior a 2 (dois) dias úteis após a rescisão do indivíduo.

4.7. **Comunicações e Operações**

O Fornecedor deverá:

4.7.1. realizar backups regulares suficientes para restabelecer os serviços para o Cliente nos tempos de recuperação acordados (ou, se nenhum tempo de recuperação

específico tiver sido acordado pelas partes, em um período de tempo comercialmente razoável);

4.7.2. criptografar toda a mídia de backup contendo Informações Confidenciais do Cliente e Informações Confidenciais do cliente do Cliente em conformidade com as Diretrizes de Proteção de Informações do Fornecedor do Cliente estabelecidas abaixo;

4.7.3. não armazenar nem reproduzir nenhuma Informação Confidencial do Cliente nem nenhuma Informação Confidencial do cliente do Cliente fora das instalações do Fornecedor, sem obter o consentimento prévio do Cliente;

4.7.4. não transmitir, transferir nem fornecer quaisquer Informações Confidenciais do Cliente e Informações Confidenciais do cliente do Cliente a qualquer terceiro ou fornecer a qualquer terceiro acesso a quaisquer Informações Confidenciais do Cliente ou Informações Confidenciais do cliente do Cliente, sem obter o consentimento prévio do Cliente;

4.7.5. se as atividades descritas nas cláusulas anteriores 4.7.3 e 4.7.4 forem aprovadas pelo Cliente, mantenha um inventário de terceiros e/ou locais fora das instalações do Fornecedor que armazenam ou replicam qualquer Informação Confidencial do Cliente e Informações Confidenciais do cliente do Cliente, os terceiros que recebem ou recebem acesso a Informações Confidenciais do Cliente ou a Informações Confidenciais do cliente do Cliente, a fim de armazenar, replicar, fornecer ou fornecer acesso a Informações Confidenciais do Cliente e a Informações Confidenciais do cliente do Cliente, a maneira na qual as referidas Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente foram transmitidas ou, de outra forma, fornecidas a esse terceiro, a transmissão e o método de criptografia/proteção ou o protocolo (se aplicável) usado na transmissão ou, de outra forma, fornecer as referidas Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente, uma descrição das Informações Confidenciais do Cliente e das Informações Confidenciais do cliente do Cliente que eram transmitidas ou de outra forma fornecidas a esse terceiro, o nome do funcionário do Cliente que aprovou tal acordo e a data em que a aprovação foi obtida;

4.7.6. ao apagar ou destruir as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente, empregue procedimentos de destruição de dados que atendam os excedam os padrões do Departamento de Defesa dos EUA para a Limpeza Segura de Dados (DOD 5220.22M). O Fornecedor deverá, o mais rapidamente possível, apagar ou destruir qualquer ou todas as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente mediante a solicitação por escrito do Cliente;

4.7.7. seguir as Diretrizes de Proteção de Informações do Fornecedor do Cliente estabelecidas abaixo, incluindo aquelas relacionadas à criptografia, ao transmitir ou transportar as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente;

4.7.8. usar a criptografia de disco rígido para todos os dispositivos móveis nos quais as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente são armazenadas ou que são utilizados pela equipe do Fornecedor para acessar quaisquer Informações Confidenciais do Cliente e Informações Confidenciais do cliente do Cliente; e esta criptografia deve estar em conformidade com as Diretrizes de Proteção de Informações do Fornecedor do Cliente estabelecidas abaixo;

4.7.9. manter atualizada a prevenção e detecção de malwares nos servidores do Fornecedor e/ou nas plataformas do usuário final que transmitem, acessam, processam ou armazenam as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente;

4.7.10. manter um perímetro de internet protegido e infraestrutura segura usando firewalls, antivírus, antimalware, sistemas de detecção de intrusão e outras tecnologias de proteção conforme comercialmente razoável e

4.7.11. implementar o gerenciamento de patches regulares e manutenção do sistema para todos os sistemas do Fornecedor que transmitem, acessam, processam ou armazenam as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente.

4.8. **Controle de Acesso**

O Fornecedor deverá:

4.8.1. cumprir as melhores práticas para a autenticação do usuário; se as senhas forem usadas para autenticar indivíduos ou processos automatizados que acessam Informações Confidenciais do Cliente e Informações Confidenciais do cliente do Cliente, tais senhas cumprirão as melhores práticas atuais para uso, criação, armazenamento e proteção de senha. (Consulte as Diretrizes de Proteção de Informações do Fornecedor do Cliente abaixo).

4.8.2. assegurar que os IDs de usuário sejam exclusivos para os indivíduos e não sejam compartilhados e sejam removidos em até 48 horas após o cancelamento de um usuário com o Fornecedor ;

4.8.3. atribuir direitos de acesso com base na sensibilidade das Informações Confidenciais do Cliente e das Informações Confidenciais do cliente do Cliente, as exigências de trabalho do indivíduo e a "necessidade de saber" do indivíduo para as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente;

4.8.4. analisar os direitos de acesso da equipe do Fornecedor (incluindo Prestadores de Serviços) pelo menos anualmente para assegurar que as restrições com relação às necessidades de saber estejam atualizadas;

4.8.5. rever regularmente relatórios de entrada do usuário nas instalações do Fornecedor que abrigam as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente e

4.8.6. não deixar as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente sem supervisão em desktops, impressoras ou em qualquer outro lugar de uma forma desprotegida nas instalações do Fornecedor.

4.9. **Desenvolvimento de Aplicativos; Análises de Vulnerabilidade e Testes de Penetração**

O Fornecedor deverá:

4.9.1. implementar uma metodologia de desenvolvimento segura que incorpore a segurança em todo o ciclo de desenvolvimento;

4.9.2. desenvolver e aplicar padrões de codificação seguros;

4.9.3. executar revisões de código seguro usando ferramentas de varredura automatizadas para todos os aplicativos voltados para uso externo e para

qualquer software desenvolvido pelo Fornecedor (ou por um Prestador de Serviços) e entregue ao Cliente;

4.9.4. realizar análises de vulnerabilidade pelo menos uma vez por trimestre para todos os aplicativos voltados para uso externo que recebem, acessam, processam ou armazenam Informações Confidenciais do Cliente e Informações Confidenciais do cliente do Cliente; mediante solicitação do Cliente, o Fornecedor deverá confirmar por escrito que o Fornecedor executou com êxito as análises de vulnerabilidade;

4.9.5. usar uma empresa externa terceirizada de testes de segurança para realizar testes de penetração pelo menos uma vez por ano para todos os aplicativos voltados para uso externo que recebem, acessam, processam ou armazenam as Informações Confidenciais do Cliente; tais testes de penetração devem ser realizados pelo fornecedor de testes do Fornecedor que foi aprovado pelo Cliente; a pedido do Cliente, o Fornecedor deverá confirmar por escrito que o Fornecedor executou com sucesso os referidos testes de penetração; e o Fornecedor deverá corrigir todos os problemas substanciais descobertos no decurso de tais testes de penetração conduzidos por ou em nome do Fornecedor em 30 (trinta) dias ou, se tal problema não puder ser corrigido no período de 30 (trinta) dias, em um período de tempo mutuamente acordado pelo Fornecedor e o Cliente.

4.10. **Prestadores de Serviços**

O Fornecedor deverá:

4.10.1. tomar medidas razoáveis para selecionar e manter os Prestadores de Serviços capazes de manter medidas de segurança para proteger as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente em conformidade com as leis e os regulamentos aplicáveis e de uma forma não menos protetora do que as exigências definidas no presente Contrato, incluindo este Anexo; e manter com cada Prestador de Serviços um contrato por escrito exigindo que ele implemente e mantenha tais medidas de segurança;

4.10.2. não fornecer a nenhum Prestador de Serviços nem permitir que qualquer Prestador de Serviços acesse, processe, armazene, exiba ou de outra forma interaja com quaisquer Informações Confidenciais do Cliente ou Informações Confidenciais do cliente do Cliente sem obter o consentimento prévio do Cliente;

4.10.3. ser responsável perante o Cliente por todos os atos e omissões de qualquer Prestador de Serviços, incluindo qualquer falha de um Prestador de Serviços em cumprir as cláusulas do presente Contrato, incluindo este Anexo e

4.10.4. executar regularmente uma revisão de cada Prestador de Serviços que inclui uma revisão das práticas e políticas de segurança de informação do Prestador de Serviços.

5. **GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.**

5.1. O Fornecedor deverá:

5.1.1. criar, testar e manter um processo de resposta a incidentes de segurança da informação, que inclui, entre outras coisas, processos de preservação de provas, informando e trabalhando com representantes legais, órgãos do governo e as partes semelhantes, conforme apropriado, e realizando análises forenses;

5.1.2. notificar o Cliente por escrito, de qualquer brecha de segurança da informação envolvendo as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente, incluindo qualquer suspeita de acesso não

autorizado ou acesso real às Informações Confidenciais do Cliente ou às Informações Confidenciais do cliente do Cliente ou de um incidente de segurança em ou envolvendo os sistemas, hardware, equipamentos, dispositivos ou computadores nos locais de um Prestador de Serviços ou de outra forma envolvendo a equipe de um Prestador de Serviços; o Fornecedor deverá fornecer notificação de qualquer incidente imediatamente, mas isso deve ocorrer impreterivelmente em 24 (vinte e quatro) horas após à data em que o Fornecedor tomar consciência do referido incidente. Posteriormente, o Fornecedor deve fornecer ao Cliente atualizações regulares sobre a investigação e a mitigação de tal evento. O Fornecedor deve permitir que o Cliente ou seus representantes participem em todos os aspectos da investigação. O Fornecedor será responsável por todos os custos incorridos por qualquer das partes relacionadas com esses incidentes, incluindo mas não se limitando, a notificação aos titulares dos dados afetados, investigações forenses, monitoramento de crédito dos titulares de dados e outros esforços corretivos e legais e

5.1.3. para cada incidente, fornecer ao Cliente uma notificação final por escrito, no prazo de 10 (dez) dias após o encerramento de tais incidentes por parte do Fornecedor, incluindo informações detalhadas sobre a causa principal de tal incidente, as medidas tomadas e os planos para evitar a ocorrência de um evento semelhante no futuro.

6. **GERENCIAMENTO DE CONTINUIDADE DOS NEGÓCIOS.**

6.1. O Fornecedor deverá:

6.1.1. estabelecer e manter um plano de continuidade de negócios abrangente ("BCP") que abranja a restauração de tecnologia e das operações de negócios no caso de um evento imprevisto;

6.1.2. testar ou revisar o seu BCP pelo menos uma vez ao ano do modo que considerar apropriado, a seu exclusivo critério,

7. **CONFORMIDADE.**

7.1. O Fornecedor deverá:

7.1.1. cumprir as Diretrizes de Proteção de Informações do Fornecedor do Cliente estabelecidas abaixo;

7.1.2. estabelecer e manter um acordo mútuo sobre as políticas e as práticas de manutenção de registros e destruição de dados aplicáveis às Informações Confidenciais do Cliente e às Informações Confidenciais do cliente do Cliente e de quaisquer informações produzidas no curso de ou de outra forma relacionados com as atividades do Fornecedor nos termos do presente Contrato;

7.1.3. criar um código de ética e exigir que os funcionários o analisem e reconheçam anualmente (exceto se e na medida proibida por lei).

8. **ACOMPANHAMENTO DE AÇÕES DE GERENCIAMENTO DE RISCOS**

8.1. Se o Cliente tiver realizado anteriormente uma revisão de segurança do Fornecedor e/ou em uma ou mais de suas instalações (ou nas de seus Prestadores de Serviços, conforme aplicável) e, como resultado dessa revisão de segurança, itens de preocupação foram identificados pelo Cliente, o Fornecedor deverá:

8.1.1. caso ainda não o tenha feito, cooperar razoavelmente com o Cliente para desenvolver imediatamente um plano de gerenciamento de riscos mutuamente acordado para remediar tais itens de preocupação e

8.1.2. implementar as ações especificadas no plano de gerenciamento de riscos no máximo na data correspondente estabelecida em tal plano de gestão de riscos.

8.2. O plano de gerenciamento de riscos para a revisão de segurança mais recente está estabelecido abaixo ou, se o plano abaixo estiver em branco, deve ser estabelecido em outro documento preparado e acordado pelas partes.

PLANO DE GERENCIAMENTO DE RISCOS		
Nível de preocupação	Plano de ação	Data
ALTO		
MÉDIO		
BAIXO		

9. **ROUBO DE IDENTIDADE.**

Se o Fornecedor processar, tratar ou tiver acesso a Informações Pessoais, o Fornecedor deverá notificar prontamente o Cliente se, durante o período de atividades do Fornecedor nos termos do presente Contrato, os funcionários do Fornecedor tomaram conhecimento de qualquer possível roubo de identidade relacionado com os indivíduos aos quais as Informações Pessoais se referem.

10. **ATUALIZAÇÕES.**

O Cliente pode atualizar este Adenda de Segurança de Informações a qualquer momento, mediante um prazo de 30 (trinta) dias de antecedência por escrito ao Fornecedor. Caso o Fornecedor acredite que ele não pode cumprir tais atualizações, o Fornecedor deverá notificar o Cliente por escrito em 30 (trinta) dias estabelecendo os itens específicos para os quais o Fornecedor não pode atender. Nesse caso, o Cliente reserva-se o direito de encerrar todo ou qualquer serviço ou projeto com o Fornecedor, sem responsabilidade ou penalidade por conta de tal rescisão.

ANEXO 1

DIRETRIZES DE PROTEÇÃO DE INFORMAÇÕES DO FORNECEDOR DO CLIENTE

Classificação de Informações do Cliente e Matriz de Tratamento

resume alguns requisitos específicos aplicáveis ao transmitir (ou transferir), armazenar ou destruir as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente, incluindo Informações Confidenciais do Cliente.

Classificação de Informações	**Exemplos**	**Transmissão**	**Armazenamento**	**Destruição**
As Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente que não sejam as Informações Confidenciais do Cliente	Estratégias e planos de negócios; Relatórios de auditoria; Informações de marketing de pré-lançamento; O software proprietário do Cliente; Especificações técnicas ou arquiteturas	Por meios eletrônicos: criptografe quando transmitidas por redes públicas ou forem transferidas para fora das instalações do Fornecedor em mídia portátil ou dispositivos ou outros meios eletrônicos; Impressão: envie por courier (incluindo o serviço de entrega noturno) ou correio registrado com número de rastreamento.	Limite o acesso apenas à equipe autorizada; realize revisões de direitos de acesso trimestralmente. Preferencialmente, criptografe os dados quando estiverem em armazenamento.	Eletrônico: use DOD 5220.22M ou procedimentos equivalentes. Impressão: fragmentos
Informações Confidenciais do Cliente	Informações Pessoais (como nome, e-mail, telefone, endereço para correspondência, SSN ou número de conta) Informações financeiras pessoais) Informações pessoais sobre saúde	O mesmo do descrito acima	Limite o acesso apenas à equipe autorizada; realize revisões de direitos de acesso trimestralmente. É obrigatório fazer a criptografia dos dados no armazenamento.	O mesmo do descrito acima

Criptografia

A seguir, estão estabelecidos os algoritmos de criptografia preferenciais do Cliente no momento, além dos algoritmos de criptografia mais aceitáveis. O Fornecedor deverá utilizar um dos algoritmos de criptografia preferidos ao criptografar as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente, a menos que não seja razoavelmente possível, caso em que o Fornecedor deverá utilizar um dos algoritmos de criptografia aceitáveis adicionais ao criptografar as Informações Confidenciais do Cliente e as Informações Confidenciais do cliente do Cliente.

Algoritmos de Criptografia Preferidos		
Finalidade	**Algoritmos**	**Comprimento Mínimo da Chave (Bits)**
Troca de Chaves	RSA Diffie-Hellman	Preferencialmente 2048, se não for possível, 1024
Proteção de Dados	AES no modo CBC 3DES no modo CBC EDE3	Preferencialmente 256, se não for possível, 128 168
Hash	SHA-256	N/D
HMAC	HMAC SHA-256	256
Assinatura Digital	RSA com SHA-256 DSA com SHA-256	Preferencialmente 2048, se não for possível, 1024

Algoritmos de Criptografia Aceitáveis Adicionais		
Finalidade	**Algoritmos**	**Comprimento Mínimo da Chave (Bits)**
Proteção de Dados	AES no modo CTR RC4 RC5 no modo CBC Blowfish no modo CBC CAST-128 no modo CBC IDEA no modo CBC	Preferencialmente 2048, se não for possível, 128
Hash	Preferencialmente SHA-2, se não for possível, SHA-1 MD5 nunca deve ser usado a menos que seja necessária uma exceção por conta da tecnologia.	N/D
HMAC	Preferencialmente HMAC SHA-2, se não for possível, SHA-1	160 128

	MD5 nunca deve ser usado a menos que seja necessária uma exceção por conta da tecnologia.	
Assinatura Digital	ECC com SHA-256, SHA-2 Preferencialmente RSA com SHA-2, se não for possível, SHA-1, Preferencialmente DSA com SHA-2, se não for possível, SHA-1	160 min Preferencialmente 2048, se não for possível, 1024

Diretrizes de Autenticação com Base em Senha

Todas as senhas administradas ou controladas pelo Fornecedor (ou pelo Prestador de Serviços) devem atender às seguintes diretrizes:

Área	Diretriz
Comprimento mínimo de senha	8 caracteres
Complexidade de senha	2 dos 4 tipos de caracteres (superior, inferior, dígitos, especiais), que não sejam facilmente associados com um indivíduo ou processo, não encontradas em um dicionário e que não representem um padrão. É recomendável que as senhas contenham de 3 a 4 tipos de caracteres
Duração máxima da senha	No máximo 90 dias
Histórico mínimo de senhas	1 dia
Proteção em trânsito	Obrigatória. As senhas devem ser criptografadas em trânsito.
Proteção em armazenamento	Obrigatória. As senhas devem ser aprovadas em hash usando um algoritmo de hash (consulte a tabela acima).

CRONOGRAMA 3

PROTEÇÃO DE DADOS

1. **DEFINIÇÕES**

1.1. Neste Anexo 3, os termos usados, mas não de outra forma definidos neste Contrato, têm os significados dados no RGPD.

1.1.1. **Dados Pessoais no Escopo** significa qualquer Dado Pessoal que é processado pelo Fornecedor na prestação de Serviços ou ao realizar as suas outras obrigações segundo o presente Contrato;

1.1.2. **Proteção dos Dados** significa proteções administrativas, técnicas e físicas que protegem contra ameaças ou perigos para a integridade e segurança da destruição acidental ou não autorizada, perda, alteração ou uso e acesso não autorizado aos Dados Pessoais no Escopo e que cumprem as melhores práticas do setor;

1.1.3. **Termos de Modelo** significa as cláusulas contratuais padrão aprovadas pela decisão da Comissão Europeia em 5 de fevereiro de 2010 (2010/87/UE) com relação às cláusulas contratuais padrão aplicáveis à transferência de Dados Pessoais para Processadores estabelecidos em países terceiros (mas que devem excluir quaisquer cláusulas contratuais, designadas pela Comissão Europeia como opcionais na decisão), conforme alterado ou substituído de tempos em tempos pela Comissão Europeia;

1.1.4. **"Subprocessador"** significa qualquer terceiro designado pelo Fornecedor para Processar Dados Pessoais no Escopo em nome do Cliente em conexão com o Contrato;

1.1.5. Os termos **"Controlador", "Titular dos Dados", "Estado-membro", "Dados Pessoais", "Processamento", "Processador"** e **"Autoridade de Supervisão"** terão o mesmo significado que no RGPD, e seus termos cognatos serão interpretados de acordo com o mesmo; uma referência à transferência de dados para fora de qualquer país ou território inclui, sem limitação, acessar remotamente dados fora desse país ou território;

1.1.6. a referência à Lei Aplicável na Cláusula 2.1.4 do Contrato deverão se limitar à União Europeia ou à lei do Estado-membro à qual o Fornecedor está sujeito, na medida em que essas Cláusulas se apliquem com relação aos Dados Pessoais no Escopo e cujo Processamento deles está sujeito à lei da União Europeia ou de um Estado-membro;

2. **OBRIGAÇÕES**

2.1. Tanto o Fornecedor quanto o Cliente deverão sempre cumprir suas obrigações segundo todas as Leis de Proteção de Dados e todas as

Políticas de Fornecedores aplicáveis com relação a este Contrato.

2.2. O Fornecedor não terá direito a utilizar ou de outra forma processar nenhum Dado Pessoal no Escopo para qualquer finalidade que não seja a prestação dos Serviços e para executar as suas outras obrigações segundo este Contrato.

2.3. Responsabilidades das partes. As partes reconhecem e concordam que, com relação ao processamento de Dados Pessoais no Escopo, o Cliente é o Controlador, o Fornecedor é o Processador e só pode contratar Subprocessadores de acordo com o requisito estabelecido na seção 2.8.4 abaixo.

2.4. O Fornecedor deverá:

2.4.1. processar os Dados Pessoais no Escopo somente em conformidade com as instruções por escrito do Cliente;

2.4.2. notificar imediatamente o Cliente quando tiver conhecimento de quaisquer erros ou imprecisões em quaisquer Dados Pessoais no Escopo;

2.4.3. certificar-se de que, exceto se for indicado de outra forma por escrito pelo Cliente ou exigido pela Lei de Proteção de Dados, qualquer cópia dos Dados Pessoais no Escopo na posse ou sob o controle do Fornecedor, de qualquer Subprocessador ou da equipe de qualquer Fornecedor será permanentemente destruída quando eles não for mais necessária para o desempenho das obrigações por parte do Fornecedor segundo o presente Contrato;

2.4.4. garantir que os Dados Pessoais no Escopo sejam acessíveis somente à equipe do Fornecedor que: (i) precise ter acesso a dados para desempenhar suas funções no desempenho das obrigações do Fornecedor nos termos deste Contrato; (ii) tenha sido devidamente treinada sobre os requisitos da Lei de Proteção de Dados aplicável ao Processamento, cuidado e tratamento dos dados e (iii) está sujeita a obrigações legais ou contratuais de confidencialidade em relação aos Dados Pessoais no Escopo e

2.4.5. sujeito à Cláusula 2.15, dê ao cliente tal cooperação, assistência e informação e assine todos os documentos que eles podem solicitar para auxiliá-los a cumprir suas obrigações segundo a Lei de Proteção de Dados, na medida em que eles se relacionam com qualquer Dado Pessoal no Escopo

2.4.6. e coopere e cumpra as orientações ou decisões de qualquer Autoridade de Supervisão em relação a esses dados, e, em cada caso, no devido tempo para auxiliar o Cliente e atender a qualquer limite de tempo imposto pela Lei de Proteção de Dados ou pela Autoridade de Supervisão.

2.5. Com relação aos Dados Pessoais no Escopo, cujo Processamento está sujeito às leis da União Europeia ou de um Estado-membro, o Fornecedor deverá:

2.5.1. não transferir, e deve assegurar que nenhum

Subprocessador transfira, os referidos dados para fora de qualquer país ou território, nem exigir que nenhum Cliente faça tal transferência, exceto:

2.5.2. entre os estados-membros da União Europeia, da Área Econômica Europeia

2.5.3. mediante instruções por escrito do Cliente e sujeito a quaisquer restrições adicionais razoável definidas pelo Cliente e a qualquer momento em relação a uma transferência deste tipo, entrar imediatamente (ou exigir, em caso de transferência de ou para um Subprocessador, que o Subprocessador celebre) um contrato com o Fornecedor nos Termos de Modelo sem alterações, mas concluído da maneira que o Cliente possa estipular de forma razoável ou outro formulário que as Partes podem acordar por escrito.

2.6. Com relação aos Dados Pessoais no Escopo não entrarem na Cláusula 2.5, mas o Processamento deles estar sujeito a qualquer Lei de Proteção de Dados que proíbe ou restringe (a) a transferência de Dados Pessoais no Escopo para qualquer país ou território ou (b) o Processamento dos referidos Dados Pessoais no Escopo em qualquer país ou território, o Fornecedor não deverá transferir nem Processar os Dados Pessoais no Escopo em violação de qualquer proibição ou restrição.

2.7. O Fornecedor deverá:

2.7.1. em todo o momento manter (e manter o responsável pela proteção de dados do Cliente informado por escrito da identidade de) uma Pessoa do Fornecedor que seja responsável por auxiliar o Cliente a responder a solicitações recebidas dos Titulares dos Dados ou de qualquer Autoridade de Supervisão;

2.7.2. garantir que a Pessoa do Fornecedor mencionada na Cláusula 2.7.1 sempre responderá prontamente e razoavelmente às solicitações mencionadas na Cláusula, levando em conta plenamente os requisitos pertinentes da Legislação de Proteção de Dados com relação à resposta oportuna e

2.7.3. não tomar medidas em relação a qualquer solicitação conforme indicado na Cláusula 2.7.1, exceto segundo as instruções por escrito do Cliente aplicável.

2.8. O Fornecedor deverá:

2.8.1. não divulgar nem transferir nenhum Dado Pessoal no Escopo a nenhum terceiro, salvo para divulgação ou transferência:

2.8.2. feita nas instruções por escrito do Cliente e de acordo com a Cláusula 2.5;

2.8.3. na medida exigida pela Lei de Proteção de Dados ou de qualquer outra cláusula do presente Contrato;

2.8.4. no que diz respeito a qualquer processamento dos Dados Pessoais no Escopo por parte de um Subprocessador:

(a) cumprir as disposições da cláusula 13.2 do

contrato (cessão, prestação de serviços);

(b) certificar-se de que o processamento do prestador de serviços seja realizado segundo um contrato por escrito, impondo ao subprocessador as mesmas obrigações que são impostas ao fornecedor segundo este Anexo 3 (Proteção de Dados: RGPD);

(c) obter que o Subprocessador execute e observe as referidas obrigações e

(d) se o Cliente assim o solicitar, providenciar que o Subprocessador celebre um contrato por escrito com o Cliente), impondo ao Subprocessador as mesmas obrigações que são impostas ao Fornecedor segundo este Anexo 3 (Proteção de Dados: RGPD).

2.9. O Fornecedor:

2.9.1. deve adotar, implementar e manter Proteções de Dados, incluindo, como parte das Proteções dos Dados, procedimentos e práticas de segurança para impedir o acesso não autorizado ou acidental ou a destruição, perda, modificação, utilização ou divulgação de Dados Pessoais no Escopo;

2.9.2. garante ao Cliente que o Fornecedor tem políticas, procedimentos e práticas de segurança por escrito compatíveis com as obrigações de segurança de dados do Fornecedor segundo a Lei de Proteção de Dados;

2.9.3. deverá manter e impor as Proteções de Dados em cada instalação a partir da qual o Fornecedor presta os Serviços e com relação a qualquer e a todas as redes que processam os Dados Pessoais no Escopo e

2.9.4. deverá analisar e rever as Proteções de Dados de tempos em tempos de acordo com as práticas prevalecentes do setor e conforme solicitado de forma razoável pelo Cliente (e deverá fornecer imediatamente os detalhes de tais Proteções de Dados revisadas para o Cliente mediante solicitação por escrito).

2.10. No caso de qualquer acesso acidental ou não autorizado ou de uso ou divulgação de quaisquer Dados Pessoais no Escopo, ou se o Fornecedor acreditar de forma razoável que houve tal acesso, uso ou divulgação ou que há risco de ocorrer (que deve incluir, sem limitação, a perda de ou a incapacidade de localizar definitivamente qualquer mídia, dispositivo ou equipamento em que os Dados Pessoais no Escopo estão ou podem estar armazenados), o Fornecedor deverá:

2.10.1. notificar o Cliente sem demora e, em qualquer caso, no prazo de 24 (vinte e quatro) horas, fornecendo detalhes razoáveis do impacto sobre

o acesso, uso ou divulgação por parte do Cliente e a medida corretiva tomada e a ser tomada pelo Fornecedor;

2.10.2. Sujeito à Cláusula 2.15, tomar imediatamente todas as medidas necessárias e ações corretivas adequadas para remediar as causas subjacentes de acesso, uso ou divulgação;

2.10.3. tomar quaisquer medidas relativas ao acesso, uso ou divulgação exigidas pela Lei de Proteção de Dados incluindo, sem limitação, mediante solicitação do Cliente, fornecer avisos aos titulares dos dados cujos dados pessoais tenham sido afetados, seja ou não tal notificação exigida pela Lei de Proteção de Dados e

2.10.4. se o acesso, uso ou divulgação não permitir o acesso a informações financeiras dos titulares dos dados ou levar a um risco razoável de roubo de identidade ou fraude, o Fornecedor deverá fornecer, por um período razoável de tempo não inferior a 1 (um) ano, serviços de monitoramento de crédito por qualquer titular de dados.

2.11. Além de quaisquer direitos de auditoria previstos no Contrato e mediante solicitação do Cliente, e sujeito a critérios razoáveis do Cliente, o Fornecedor permite ao Cliente (por conta própria ou em nome de seus clientes) ou a um auditor independente instruído pelo Cliente de auditar e revisar o programa de segurança da informação, as instalações de processamento de dados e o programa de conformidade de proteção de dados do Fornecedor, e dos Subprocessadores aprovados, para verificar a conformidade com esta Schedule 3 (Proteção de dados: RGPD), Lei de Proteção de Dados e obrigações do Cliente ou dos próprios clientes do Cliente ("Auditoria de Segurança e Proteção de Dados").

2.12. Essa Auditoria de Segurança e Proteção de Dados pode incluir testes projetados para violar o programa de segurança da informação e medidas de segurança associadas (incluindo teste de penetração de segurança) do Fornecedor, ou do Subprocessador aprovado, e deve ser conduzida com um aviso prévio por escrito não inferior a 10 dias.

2.13. Se o Cliente razoavelmente acreditar que os resultados de uma Auditoria de Segurança e Proteção de Dados identificam uma fraqueza nas medidas de segurança adotadas pelo Fornecedor, ou pelo Subprocessador aprovado, o Fornecedor deve avaliar essa fraqueza e fornecer uma solução adequada para a satisfação do Cliente dentro dos prazos acordados pelo Cliente.

2.14. O Fornecedor reconhece que qualquer órgão regulador ou seu agente pode periodicamente auditar o Fornecedor, ou quaisquer Subprocessadores aprovados, e que essa auditoria não deve estar sujeita a nenhuma das restrições estabelecidas nestas Cláusulas 2.11, 2.12, 2.13 e 2.14.

2.15. Cliente:

2.15.1. é responsável por instruir o Fornecedor a tomar tais medidas no Processamento de Dados Pessoais em nome do Cliente conforme seja razoavelmente necessário para o desempenho das

obrigações do Fornecedor segundo este Contrato e

2.15.2. autoriza o Fornecedor, na medida permitida pela Lei de Proteção de Dados, a fornecer instruções equivalentes aos Subprocessadores em nome do Cliente.

2.16. Os custos e as despesas incorridos pelo Fornecedor, em conformidade com as Cláusulas 2.4, 2.10.2, 2.10.3 e 2.10.4 devem ser assumidos:

2.16.1. pelo Fornecedor, nos casos em que a medida que deve ser tomada pelo Fornecedor resultar na violação deste Contrato ou qualquer negligência, ato ilícito ou fraudulento ou omissão do Fornecedor, incluindo o não cumprimento do RGPD, por qualquer Subprocessador ou pela Equipe do Fornecedor e

2.16.2. pelo Cliente em outros casos.

2.17. O Fornecedor, a qualquer momento, mediante solicitação do Cliente, deverá devolver todos os Dados Pessoais dos quais o Cliente é o único Controlador de Dados e que são Processados pelo Fornecedor em nome do Cliente nos termos do Contrato, para o Cliente e/ou, a pedido do Cliente, excluir os mesmos de seus sistemas, exceto cópias de backup que o Fornecedor ou seus Afiliados devam manter para cumprir com as leis ou requisitos regulamentares aplicáveis, desde que essas cópias sejam mantidas de forma confidencial e seguras, de acordo com este Cronograma 3 (Proteção de Dados)

Assinado por e em nome do Fornecedor

ASSINADO _____

NOME _____

CARGO _____

NOME DO FORNECEDOR _____

DATA _____