ANEXO DE TRATAMENTO DE DADOS PESSOAIS

XXXX (indicar empresa do Grupo EDP)., com sede na XXXX, Cidade, Estado, CEP XXX, Brasil, inscrita no CNPJ sob nº xxxx, neste ato representada na forma de seus atos constitutivos, doravante designada "**EDP** " ou "**Controlador**"; e

XXXXXX (indicar empresa contratada), com sede na XXX, Cidade, Estado, CEP XXX, Brasil, inscrita no CNPJ sob nº xxxx, neste ato representada na forma de seus atos constitutivos, doravante designado "**XXX**" ou "**Operador"**.

EDP e **XXX** a seguir designadas individualmente "Parte" ou em conjunto "Partes".

Considerando que:

a. As Partes celebraram o Contrato de xxxx nesta data, cujo objeto consiste na XXX [finalidades de tratamento] ("**Contrato**" e "**Objeto**", respectivamente);

b. O Operador tem conhecimento de que a **EDP** é uma empresa atuante no setor de energia elétrica e, como tal, também está submetida às regras regulatórias setoriais;

c. Para a execução do Objeto, o **Operador** realizará o tratamento de dados pessoais em favor da **EDP**, nos termos definidos na Lei Federal nº 13.709/18, Lei Geral de Proteção de Dados Pessoais ("**Tratamento**" e "**LGPD**", respectivamente) e outras eventualmente aplicáveis;

d. Quando realizado em território brasileiro, o Tratamento se dará à luz da LGPD, observadas ainda as diretrizes e determinações emanadas pela Autoridade Nacional de Proteção de Dados ("**ANPD**"), regras setoriais e demais leis aplicáveis (quando em conjunto, "**Normas**");

e. O **Operador** declara possuir os recursos e salvaguardas adequados para o Tratamento e o conhecimento especializado, os quais serão empregados na execução do Objeto do Contrato, a fim de atender a todas as medidas técnicas e organizacionais relacionadas à proteção de Dados Pessoais, nos exatos termos da LGPD e demais Normas;

f. O presente Anexo e seus Apêndices dispõem sobre os requisitos necessários para garantir a segurança e a proteção dos Dados Pessoais aplicáveis ao Tratamento a ser realizado pelo **Operador**.

Resolvem as Partes aderir ao presente Anexo de Tratamento de Dados Pessoais ("Anexo") com base nos termos e condições estabelecidos a seguir, que uma vez rubricado pelas Partes passa a fazer parte integrante do Contrato:

1. DEFINIÇÕES.

1.1. Utilizam-se as seguintes definições para fins deste Anexo:

(a) "Agentes de Tratamento", "Controlador", "Operador", "Dados Pessoais", "Titulares" e "Tratamento" serão interpretados de acordo com a Lei de Proteção de Dados Aplicável.

(c) "Avaliação de impacto de proteção de dados pessoais": documento elaborado pelo Agente de Tratamento, descrevendo os processos de Tratamento de Dados Pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos Titulares, indicando quais serão as medidas, salvaguardas e mecanismos para mitigar os riscos decorrentes do Tratamento.

(d) "Incidente": Deverá ser entendido como: (a) uma investigação ou apreensão dos Dados Pessoais por funcionários públicos, ou uma indicação específica de que tal investigação ou apreensão é iminente; (b) qualquer acesso, Tratamento, eliminação, perda ou qualquer forma acidental de Tratamento ilegal dos Dados Pessoais; (c) qualquer violação da segurança da informação e/ou confidencialidade, conforme estabelecido nas Cláusulas 5 e 6 deste Anexo, levando à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso aos Dados Pessoais, ou qualquer indicação de que tal violação tenha ocorrido ou esteja prestes a ocorrer; e (d) quando, na opinião do Operador, implementar uma instrução de Tratamento recebida da EDP que possa violar as leis aplicáveis, às quais a EDP ou o Operador estão sujeitos.

(b) "Lei de Proteção de Dados Aplicável": a Lei Federal Brasileira nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais, ou LGPD, que dispõe sobre o Tratamento de Dados Pessoais e a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, bem como qualquer outra lei aplicável ao Tratamento.

(e) "Transferência Internacional de Dados": Quando houver a transferência de Dados Pessoais para país estrangeiro ou organismo internacional do qual o Brasil seja membro.

(f) "Tratamento de Dados Pessoais de Alta Escala": Quando as operações de Tratamento de Dados Pessoais afetarem uma grande quantidade de Titulares, por exemplo: (a) quando o Tratamento envolver uma base de Dados Pessoais extensa; (b) quando forem utilizadas novas tecnologias para o Tratamento de Dados Pessoais; (c) quando o Tratamento de Dados Pessoais for considerado complexo e/ou utilizar uma nova tecnologia para a sua realização.

1.2. Quaisquer termos em letras maiúsculas não definidos de outra forma neste Anexo e seus Apêndices terão o significado interpretado de acordo com os termos do Contrato ou conforme definidos na LGPD.

2. OBJETO E VIGÊNCIA DO ANEXO.

2.1. A **EDP** nomeia a/o [•] como Operador responsável pelo Tratamento descrito no Apêndice A deste Anexo.

2.2. O presente Anexo e seus Apêndices serão aplicáveis ao Tratamento a ser realizado pelo Operador no âmbito do Contrato, de acordo com os termos do Apêndice A, e regerão as obrigações mínimas quanto à proteção de Dados Pessoais a fim de estabelecer as garantias de segurança em relação à proteção dos Dados Pessoais e aos direitos dos Titulares envolvidos no Tratamento realizado pelo Operador.

2.3. Os termos do presente Anexo serão aplicados durante o Tratamento, realizado pelo Operador em benefício da **EDP**, para cumprimento do Contrato e após o término do Contrato, quando aplicável. O Apêndice A indicará as categorias de Dados Pessoais, os Titulares dos Dados e a finalidade do Tratamento dos Dados Pessoais indicados pela **EDP**.

2.4. O presente Anexo incorpora-se ao Contrato celebrado entre as Partes e vigerá a partir da data de sua assinatura, enquanto perdurarem as atividades de Tratamento, independentemente da vigência do Contrato, nos termos da Cláusula 2.3 acima.

3. OBRIGAÇÕES DO OPERADOR.

3.1. O Operador cumprirá, às suas exclusivas expensas, com a Lei de Proteção de Dados Aplicável e com as obrigações previstas no presente Anexo e seus Apêndices. O Operador ainda utilizará todos os esforços comercialmente razoáveis para cooperar com a **EDP** no cumprimento da Legislação de Proteção de Dados Aplicável, incluindo, a manutenção de registros, informações e as documentações necessárias para que a **EDP** demonstre a conformidade com a Lei de Proteção de Dados Aplicável, nos termos do Apêndice B.

3.2. O Operador tratará os Dados Pessoais, na medida do necessário, para execução do Objeto do Contrato e estritamente de acordo com as instruções fornecidas pela **EDP**, exceto quando qualquer de tais instruções contrariar a lei brasileira aplicável. Em nenhum caso, o Operador tratará Dados Pessoais para fins próprios ou de terceiros.

> **3.2.1.** Caso o Tratamento seja necessário para o cumprimento de uma obrigação legal à qual o Operador está sujeito, o Operador deverá informar a **EDP** previamente a qualquer atividade de Tratamento sobre a obrigação legal e deverá obter autorização prévia e expressa da **EDP** antes de realizar referida operação.

3.3. O Operador notificará imediatamente a **EDP** se, em sua opinião, qualquer instrução violar a Lei de Proteção de Dados Aplicável. Caso o Operador não possa cumprir as instruções da **EDP** por qualquer motivo, deverá informar imediatamente a **EDP** sobre a sua incapacidade de cumprir com as instruções, cabendo à **EDP** o direito de determinar a imediata suspensão do Tratamento e/ou rescindir o Contrato.

3.4. O Operador não se beneficiará comercialmente dos Dados Pessoais, além das disposições do Contrato, seu Anexo e seus Apêndices, de acordo com as instruções fornecidas pela **EDP** e não utilizará os Dados Pessoais obtidos em razão do Contato para incorporar à sua base de Dados Pessoais e/ou à base de terceiros, tampouco para prestar serviços para terceiros, sob pena de aplicação das sanções estabelecidas no Contrato, bem como a responsabilização pelas perdas e danos/penalidades advindas, nos termos da Cláusula 11 deste Anexo.

4. DIREITOS DO OPERADOR.

4.1. O Operador poderá exercer, a seu exclusivo critério, a seleção e uso dos meios que considere adequados para o Tratamento previsto no Contrato, desde que compatíveis com as boas práticas e técnicas amplamente utilizadas pelo mercado e em conformidade com os requisitos deste Anexo e seus Apêndices, bem como com as atividades de Tratamento a serem realizadas pelo Operador, aplicando-se, nesse caso, o quanto disposto na Cláusula 11.3 e 11.4 deste Anexo.

4.2. O Operador ainda deverá atender aos requisitos futuros a serem publicados pela ANPD, adotando imediatamente as medidas compatíveis para garantir a conformidade do Tratamento.

5. CONFIDENCIALIDADE.

5.1. Sem prejuízo de quaisquer acordos contratuais existentes entre as Partes, o Operador tratará todos os Dados Pessoais como confidenciais e atribuirá igual obrigação a todos os seus funcionários, agentes e/ou subcontratados envolvidos no Tratamento dos Dados Pessoais. O Operador deverá assegurar que todos os envolvidos no Tratamento, ainda que se restrinja ao acesso aos Dados Pessoais, tenham assinado um acordo de confidencialidade adequado, com regras não menos rígidas que aquelas contidas neste Anexo e na Legislação de Proteção de Dados Aplicável, e estejam de outra forma vinculados a um dever de confidencialidade ou estejam sob uma obrigação estatutária de confidencialidade.

6. SEGURANÇA.

6.1. O Operador obriga-se a aplicar as medidas técnicas e organizacionais para proteger os Dados Pessoais contra a destruição, acidental ou ilícita, a perda, a alteração, a difusão ou o acesso não

autorizados e contra qualquer outra forma de Tratamento ilícito, sempre com um nível de segurança compatível e adequado aos riscos que o Tratamento implica aos direitos dos Titulares dos Dados Pessoais, tendo em consideração as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do Tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades dos Titulares. Essas medidas devem compreender pelo menos as seguintes:

a. A pseudonimização e criptografia dos Dados Pessoais;

b. A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanecentes dos sistemas e dos serviços de Tratamento;

c. A capacidade de detectar um Incidente, com ou sem o vazamento de Dados Pessoais, resolvê-lo e relatá-lo tempestivamente, nos termos da LGPD, das diretrizes e determinações emanadas pela ANPD, Lei de Proteção de Dados Aplicável e regras setoriais;

d. A capacidade de restabelecer a disponibilidade e o acesso aos Dados Pessoais de forma tempestiva no caso de um incidente físico ou técnico, em estrita observância às Normas, no prazo máximo de 72 (setenta e duas horas), se outro menor não for disposto na Lei de Proteção de Dados Aplicável e/ou nas Normas;

e. Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do Tratamento.

6.2. O Operador deverá adotar as medidas de segurança indicadas no Apêndice B deste Anexo. Caso o Tratamento de Dados Pessoais envolva a categoria de Dados Sensíveis, o Operador ainda adotará as salvaguardas adicionais solicitadas pela EDP.

6.3. O Operador deverá manter políticas de segurança da informação por escrito que sejam totalmente implementadas e aplicáveis ao Tratamento. As políticas devem incluir, no mínimo, a atribuição de responsabilidade interna pelo gerenciamento de segurança da informação, os responsáveis organizacionais pela segurança da informação, as verificações na equipe permanente que terá acesso aos Dados Pessoais, exigir dos funcionários, fornecedores e de outros com acesso a Dados Pessoais a anuência em acordos de confidencialidade por escrito e realizar treinamentos para tornar funcionários e outros envolvidos com acesso aos Dados Pessoais conscientes dos riscos de segurança da informação apresentados pelo Tratamento.

6.4. A pedido da EDP, o Operador deverá demonstrar as medidas tomadas em conformidade com esta Cláusula 6 e deverá apresentar à EDP um relatório de auditoria independente com a avaliação dos controles e medidas de segurança relacionadas à proteção de Dados Pessoais, às suas próprias expensas. A menos que seja exigido pela ANPD ou eventual outro órgão regulador de jurisdição competente, a EDP terá direito, mediante aviso prévio de pelo menos 15 (quinze) dias, de realizar por si ou por meio de terceiro, com o qual tenha firmado um acordo de confidencialidade, a auditoria das premissas e operações do Operador relacionadas ao Tratamento.

6.5. O Operador deve cooperar com as auditorias realizadas por ou em nome da EDP e deverá conceder aos auditores da EDP acesso razoável a quaisquer instalações e dispositivos envolvidos com o Tratamento. O Operador fornecerá aos auditores da EDP acesso a qualquer informação relacionada ao Tratamento, conforme solicitado pela EDP para verificar a conformidade do Operador com este Anexo.

6.6. O Operador obriga-se a prestar assistência à EDP visando assegurar o cumprimento das suas obrigações legais relativas à segurança do Tratamento, comunicação de um Incidente, elaboração de Avaliação de Impacto sobre a Proteção de Dados e consulta prévia, ou quaisquer outras obrigações que caibam à EDP em matéria de proteção de dados, tendo em conta a natureza do Tratamento e a informação que estiver ao dispor do Operador.

7. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS.

7.1. O Operador notificará de forma prévia a EDP, nos termos e forma estabelecidos no Contrato e apêndice "A" deste Anexo, sobre a necessidade de quaisquer transferências permanentes ou temporárias de Dados Pessoais para um país terceiro, sendo que tal transferência somente será realizada após a obtenção de autorização prévia e expressa da EDP, que poderá ser negada, a seu próprio critério, sem necessidade de justificativa.

7.1.1. Caso a EDP recuse a transferência internacional de dados, caberá ao Operador fornecer uma alternativa para o Tratamento de Dados Pessoais pretendido.

7.2. Quando a EDP autorizar a transferência internacional dos Dados Pessoais obtidos para territórios fora do Brasil, o Operador garantirá que o destinatário de tais Dados Pessoais seja aceito pela EDP e que:

(a) apenas realizará o Tratamento dos Dados Pessoais de acordo com as instruções documentadas pela EDP, sem prejuízo de observância das Normas aplicáveis, que deverão prevalecer às instruções em caso de conflito;

(b) fornecerá o mesmo nível de proteção dos princípios previstos na Lei de Proteção de Dados Aplicável, especialmente, mas não se limitando àqueles dispostos nos artigos 46 a 51 da LGPD, e demais Normas aplicáveis; e

(c) caso o Operador deixe de cumprir com os requisitos previstos nos itens "a" e "b", cessará imediatamente o Tratamento de Dados Pessoais ou tomará medidas razoáveis e apropriadas para mitigar qualquer incapacidade de cumprir esta obrigação.

8. AVALIAÇÃO DE IMPACTO DE PROTEÇÃO DE DADOS.

8.1. Caso o Operador considere ou tenha ciência que o Tratamento poderá resultar em alto risco para os direitos e liberdades em matéria de proteção de dados dos Titulares, deverá informar imediatamente e prestar toda a assistência que a EDP possa solicitar para realizar uma Avalição de Impacto de Proteção de Dados e, se necessário, consultar a ANPD ou Órgão Regulador competente.

9. OBRIGAÇÃO DE INFORMAÇÃO E GESTÃO DE INCIDENTES.

9.1. Quando o Operador tiver ciência de um Incidente deverá notificá-lo à EDP, no prazo de até 24 (vinte e quatro) horas, bem como cooperar sempre com a EDP e seguir as suas instruções com relação a tal Incidente, a fim de permitir que a EDP realize uma investigação completa do Incidente e adote as medidas adequadas em relação ao Incidente.

9.2. Assim que o Operador tiver ciência do Incidente, deverá: (a) averiguar, corrigir, mitigar e remediar o Incidente, de acordo com as melhores práticas do mercado, Lei de Proteção de Dados Aplicável, Normas aplicáveis e instruções da EDP, incluindo a adoção de medidas adequadas para prevenir a continuação e recorrência do Incidente; e (b) fornecer as informações e a assistência necessária para permitir à EDP avaliar o Incidente e, caso necessário, notificar tempestivamente a ocorrência do Incidente e cumprir quaisquer obrigações previstas pela Legislação de Proteção de Dados Aplicável e Normas aplicáveis, como fornecer as informações sobre o Incidente à ANPD e aos Titulares afetados, comunicando imediatamente a EDP nestas hipóteses.

9.3. O Operador deve estabelecer procedimentos escritos que permitam responder prontamente à EDP sobre um Incidente. Quando houver probabilidade razoável do Incidente exigir uma Notificação de Violação de Dados Pessoais pela Lei de Proteção de Dados Aplicável e Normas aplicáveis, o Operador deverá adotar o procedimento implementado de Resposta à Incidentes, incluindo a obrigação de notificar a EDP, tempestivamente no prazo de 24 (vinte e quatro), se outro menor não for disposto na Lei de Proteção de Dados Aplicável e Normas aplicáveis ao tempo do Incidente, contados da data da ciência da ocorrência do Incidente pelo Operador.

9.4. Quaisquer notificações de Incidentes feitas à EDP, nos termos desta Cláusula 9, deverão ser endereçadas ao funcionário da EDP cujos detalhes de contato são fornecidos no Apêndice A deste Anexo e, para auxiliar a EDP no cumprimento de suas obrigações sob a Lei de Proteção de Dados Aplicável, deverá conter: (a) o preenchimento de todas as informações mínimas de acordo com o Apêndice D deste Anexo; (b) uma descrição da natureza do Incidente, incluindo, sempre que possível, as categorias e o número aproximado de registro de Titulares afetados; (c) o nome e os detalhes de contato do Encarregado de Proteção de Dados do Operador ou outro contato responsável pelas informações; (d) uma descrição das consequências prováveis do Incidente; e (e) uma descrição das medidas tomadas ou propostas a serem tomadas pelo Operador para tratar do Incidente, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.

10. SUBCONTRATAÇÃO.

10.1. O Operador não subcontratará nenhuma de suas operações de Tratamento realizadas em nome da EDP sem a autorização prévia, expressa e por escrito da EDP. Os subcontratados aprovados pela EDP deverão estar indicados no Apêndice C deste Anexo.

10.2. Quando o Operador subcontratar suas obrigações sob este Anexo, com a autorização prévia e por escrito da EDP, deverá fazê-lo somente por meio de um Contrato por escrito com o subcontratado, impondo ao subcontratado as mesmas obrigações aplicadas ao Operador delimitadas neste Anexo e seus Apêndices.

10.3. O Operador assegurará que o subcontratado esteja vinculado às obrigações de proteção de Dados Pessoais compatíveis com as do Operador sob este Anexo, supervisionará sua conformidade e deverá, em particular, impor aos subcontratados a obrigação de implementar medidas técnicas e medidas organizacionais de tal maneira que o Tratamento atenda aos requisitos da Lei de Proteção de Dados Aplicável e Normas aplicáveis.

10.4. O Operador será considerado totalmente responsável perante a EDP pelo desempenho das obrigações do subcontratado aprovado, ainda que o subcontratado descumpra as obrigações de proteção de Dados Pessoais indicadas no Contrato firmado entre o Operador e o subcontratado.

10.5. O Operador será responsável e deverá isentar a EDP de qualquer responsabilidade decorrente de qualquer violação pelo subcontratado das disposições de proteção de Dados Pessoais estabelecidas neste Anexo, em seus Apêndices e na Lei de Proteção de Dados Aplicável, devendo, ainda, indenizar a EDP, nos termos da Cláusula 11 deste Anexo.

11. RESPONSABILIDADE E DIREITO DE REGRESSO.

11.1. Na hipótese de inadimplemento de qualquer das obrigações do Operador e/ou do subcontratado assumidas neste Anexo, o Operador deverá procurar de imediato minimizar e remediar os seus efeitos e ressarcir a EDP por todos os prejuízos causados, nos termos da presente cláusula.

11.2. O Operador deverá indenizar a EDP em face de todas as perdas, custos, danos (inclusive danos indiretos e lucros cessantes), despesas (incluindo honorários advocatícios), responsabilidades, penalidades ou danos sofridos ou incorridos pela EDP como resultado da violação pelo Operador e/ou subcontratado das disposições de proteção de Dados Pessoais estabelecidas neste Anexo e seus Apêndices.

11.3. Fica expressamente estabelecido que na hipótese de a EDP ser demandada, judicial ou administrativamente, por terceiro em decorrência de ato ou omissão atribuível ao Operador e/ou subcontratado, o Operador, por si e/ou por seu subcontratado, será responsável pelo pagamento de quaisquer perdas, danos, penalidades, custos e despesas, tão logo exigíveis, no prazo estabelecido na decisão judicial ou administrativa. Na hipótese de não cumprimento da obrigação estabelecida nesta Cláusula 11.3, à critério da EDP, esta poderá pagar os valores devidos, devendo o Operador ressarci-la no prazo máximo de 5 (cinco) dias, contados da data do efetivo desembolso dos valores, devidamente corrigidos monetariamente, segundo o índice de variação do IGP-M/FGV (índice Geral de Preços da Fundação Getúlio Vargas), ou seu eventual substituto, no período compreendido entre a data do desembolso e respectivo reembolso, e acrescidos de juros de 1% (um por cento) ao mês, calculados sobre o valor já corrigido, devido e não pago pelo Operador.

11.4. Sem prejuízo ao disposto no item 11.3 acima, a EDP poderá, a seu exclusivo critério, reter e utilizar eventuais valores devidos ao Operador em razão do Contrato ou quaisquer outros instrumentos celebrados entre as Partes, ou entre o Operador e demais empresas que integrem o grupo econômico da EDP, a fim de que seja ressarcida, total ou parcialmente, das perdas, danos, penalidades, custos e despesa, conforme o estabelecido nesta Cláusula 11.

11.5. Nos casos em que a EDP seja considerada responsável, nos termos da Lei de Proteção de Dados Aplicável, pelo pagamento de quaisquer valores, sanções administrativas e/ou multas cuja responsabilidade originária recai sobre o Operador e/ou subcontratado, a EDP fica investida em direito de regresso sobre o Operador e/ou subcontratado no montante equivalente à totalidade dos valores, sanções administrativas e/ou multas pagas, acrescido de quaisquer eventuais despesas e encargos advindos do Incidente ou do pagamento, bem como dos encargos de correção monetária e juros nos moldes descritos na Cláusula 11.3 acima.

11.6. Em caso de conflito entre o disposto neste Anexo e no Contrato, prevalecerá o disposto neste Anexo.

12. MULTA

12.1. Na hipótese de o Operador cometer alguma das seguintes infrações, incorrerá no dever de pagar, em favor da EDP, uma multa não compensatória no valor equivalente a 5% (cinco por cento) do preço total do Contrato, sem prejuízo de ter que indenizar a EDP, nos termos da Cláusula 11 deste Anexo:

a. Permitir a terceiros o acesso aos Dados Pessoais ou efetuar qualquer comunicação, utilização ou outra forma de Tratamento, realizada por si ou por pessoas por si autorizadas ou subcontratados, que divergir desta cláusula ou for contrário às instruções da EDP;

b. Deixar de notificar a EDP de um Incidente, independentemente da ocorrência ou não de vazamento de Dados Pessoais, nos termos da Cláusula 9 deste Anexo;

c. Não devolver ou apagar os Dados Pessoais após a execução do objeto do Contrato ou de sua extinção conforme convencionado entre as Partes;

d) Deixar de cumprir, no prazo previsto para tanto, com qualquer obrigação contida neste Anexo.

12.2. A obrigação de pagamento da multa ora estipulada não depende da averiguação das perdas e dos danos sofridos pela EDP e, portanto, não é limitada pelo valor de eventuais perdas ou danos, e é cumulável com outros direitos da EDP, em particular com o direito de resolver o Contrato de imediato e de ser indenizada, nos termos da Cláusula 11 acima. A EDP poderá exigir o pagamento da multa ora estipulada por simples notificação escrita dirigida ao Operador. O Operador deverá efetuar o pagamento da multa em até 48 (quarenta e oito) horas da data de recebimento da notificação encaminhada pela EDP da maneira que vier a ser indicada em tal notificação, sob pena de sobre ela ser acrescido o valor devido a título de correção e juros moratórios de 1% (um por cento) ao mês, nos moldes do disposto na Cláusula 11.3 acima. A EDP poderá, a seu exclusivo critério, reter e utilizar eventuais valores devidos ao Operador em razão do Contrato ou quaisquer outros instrumentos celebrados entre as Partes, ou entre o Operador e demais empresas que integrem o grupo econômico da EDP, a fim de que seja ressarcida, total ou parcialmente, da multa estabelecida nesta Cláusula 12.

13. ASSISTÊNCIA à EDP.

13.1. O Operador deve auxiliar a EDP em relação às medidas técnicas e organizacionais apropriadas, para o cumprimento das obrigações da EDP, especialmente com relação ao atendimento do exercício dos direitos dos Titulares conforme a Lei de Proteção de Dados Aplicável.

13.2. O Operador prestará assistência tempestiva à EDP, às suas expensas, para permitir que a EDP responda a: (i) qualquer pedido de um Titular no exercício de qualquer um dos seus direitos ao abrigo da Lei de Proteção de Dados Aplicável; e (ii) qualquer outra correspondência, pedido ou reclamação recebida de um Titular, ANPD, órgão regulador ou outro terceiro em relação ao Tratamento. No caso de tal pedido, correspondência ou reclamação ser apresentada diretamente ao Operador (ou subcontratado), este deverá informar imediatamente à EDP, fornecendo todas as informações necessárias para que a EDP possa responder, nos termos da Lei de Proteção de Dados Aplicável.

13.3. Tendo em consideração a natureza do Tratamento e as informações disponibilizadas que são relevantes para o Tratamento descrito no Apêndice A, o Operador apoiará a EDP no cumprimento das obrigações previstas na Cláusula 6, bem como das demais obrigações da EDP previstas na Lei de Proteção de Dados Aplicável, incluindo o atendimento às notificações para a ANDP, Órgão regulador ou para os Titulares, a realização de uma Avaliação de Impacto de Proteção de Dados, e as consultas prévias perante a ANPD ou demais órgãos reguladores.

13.4. O Operador deve disponibilizar à EDP todas as informações necessárias para demonstrar a conformidade com as obrigações do Operador e/ou subcontratado e contribuir com auditorias, incluindo inspeções, conduzidas pela EDP ou outro auditor exigido/contratado por ela.

14. TÉRMINO DO CONTRATO E DEVOLUÇÃO DOS DADOS.

14.1. O Operador procederá ao Tratamento dos Dados Pessoais até a data de expiração ou término do Contrato, ou após o término do Contrato, quando aplicável, a menos que instruído de outra forma pela EDP, ou até que esses Dados Pessoais sejam devolvidos ou destruídos por instrução da EDP.

14.2. A expiração ou término deste Anexo não dispensará o Operador de suas obrigações de confidencialidade, de acordo com o Cláusula 5 deste Anexo, que permanecerá vigente após o término deste Anexo.

15. DA DEVOLUÇÃO OU DESTRUIÇÃO DE DADOS PESSOAIS.

15.1. Com a rescisão ou resilição do Contrato do qual faz parte este Anexo e seus Apêndices, mediante solicitação por escrito da EDP, ou após o cumprimento de todos os propósitos para a execução do Objeto, pelos quais nenhum Tratamento adicional é requerido, o Operador deverá excluir, destruir ou devolver todos os Dados Pessoais à EDP e destruir ou devolver quaisquer cópias existentes.

15.2. O Operador notificará todos os subcontratados que prestam suporte ao seu Tratamento sobre a extinção do Contrato e seus Anexos e assegurará que todos esses subcontratados destruam os Dados Pessoais ou devolvam os Dados Pessoais à EDP, a critério da EDP.

16. OUTRAS DISPOSIÇÕES

16.1. No caso de qualquer inconsistência entre as disposições deste Anexo e seus Apêndices, e as disposições do Contrato, as disposições deste Anexo de Tratamento de Dados e seus Apêndices prevalecerão.

16.2. As Partes se comprometem a não alterar ou modificar as disposições deste Anexo. As Partes poderão incluir cláusulas relacionadas aos negócios, quando necessário, desde que não contrariem as disposições do presente Anexo e seus Apêndices.

16.3. A EDP poderá alterar as disposições do presente Anexo para cumprimento de novas obrigações legais e/ou regulatórias publicadas pela ANPD ou Órgão regulador competente.

16.3.1. O Operador deverá informar a EDP em até 48 (quarenta e oito) horas sobre a impossibilidade de cumprimento dos novos requisitos estabelecidos pela ANPD ou órgão regulador a partir de sua notificação formal, facultando à EDP a resolução do Contrato.

16.4. Este Anexo será regido e interpretado de acordo com a lei vigente estabelecida no Contrato. Quaisquer disputas decorrentes ou relacionadas a este Anexo e seus Apêndices serão levadas exclusivamente à jurisdição competente indicada no Contrato.

Em nome do Controlador de Dados (EDP):

1. _____
Nome:
Ocupação:

Em nome do Operador de Dados:

2. _____
Nome:
Ocupação:

Apêndice A
Descrição do Tratamento de Dados em Alta Escala

O Apêndice A é parte integrante do presente Anexo e descreve o tratamento que o Operador efetuará em nome da **EDP**.

EDP

A **EDP** é responsável por fornecer ao Operador todos os dados e informações que são objeto do Contrato e deste Anexo.

Contato da EDP

[Informações de contatos]

Nome:

E-mail:

Endereço

Operador

O Operador é responsável pelas atividades de Tratamento de Dados Pessoais descritas no objeto do Contrato e neste Apêndice. As atividades de Tratamento de Dados Pessoais realizadas pelo Operador envolvem os seguintes processos:

[inserir a descrição dos processos de tratamento realizados pelo Operador]

Contato do Operador

[Informações de contatos]

Titular

Os Dados Pessoais tratados referem-se à categoria de [inserir o Titular do Dado].

Categorias de Dados Pessoais

Os Dados Pessoais a tratar dizem respeito às seguintes categorias: [inserir o descritivo de dados].

Dados sensíveis

Os Dados Pessoais a serem tratados dizem respeito aos seguintes Dados Sensíveis: [inserir o descritivo de dados].

Operações de Tratamento

Os Dados Pessoais serão sujeitos às seguintes atividades básicas de Tratamento: [Coleta, Acesso, Uso, Compartilhamento, Armazenamento e Exclusão]

Natureza e finalidade do Tratamento de Dados

Os Dados Pessoais serão tratados para as seguintes finalidades:

Apêndice B

Instruções Documentadas: Medidas de Segurança e Obrigações de Informação e Documentação

O **Operador** deverá atender as instruções documentadas na letra [•] do presente Apêndice, a saber:

a. Prestadores de serviço de criticidade alta que utilizam os sistemas de tecnologia da informação da EDP

1. Para efeitos da cláusula 6 do Anexo de Tratamento de Dados Pessoais do qual o presente Apêndice faz parte, o **Operador** deverá assegurar, no âmbito do Tratamento de Dados Pessoais por conta da **EDP**, a implementação das seguintes medidas de segurança técnicas e organizativas complementares:

i. Identificação, divulgação e documentação das funções e obrigações dos colaboradores e terceiros que terão acesso aos Dados Pessoais;
ii. Manutenção de um registro escrito das atividades de Tratamento de Dados Pessoais realizadas em favor da **EDP**, conforme requisitos da LGPD;
iii. Manutenção de um registro interno escrito que garanta que as pessoas alocadas na prestação de serviços à **EDP** se comprometeram por escrito a manter a confidencialidade dos Dados Pessoais a que tiveram acesso, que conhecem as regras e procedimentos que devem ser adotados relativamente ao tratamento de dados pessoais e que participaram em ações de formação sobre esta matéria;
iv. Manutenção de um registro interno escrito, que garanta que as pessoas alocadas foram informadas e consentiram de forma específica, expressa e por escrito na comunicação dos seus Dados Pessoais à **EDP** para a finalidade específica de gestão de acesso a instalações e sistemas de informação da **EDP**, caso aplicável;
v. Manutenção de um registro interno escrito que garanta que as pessoas alocadas foram informadas e consentiram de forma expressa, específica e por escrito na gravação de chamadas telefônicas que intervêm, caso aplicável;
vi. Manutenção de um registro interno escrito que garanta que as pessoas alocadas na prestação de serviços à **EDP** declararam por escrito que foram informadas de que os seus Dados Pessoais foram comunicados à **EDP** para quaisquer outras finalidades de Tratamento relevantes (por exemplo, controle de qualidade etc.);
vii. Definição e implementação de um procedimento de registro escrito de incidentes;
viii. Implementação de um procedimento de inventário e controlo da entrada e saída de suportes e documentos;
ix. Definição dos critérios de arquivo de suportes e dos dispositivos para armazenamento desses suportes;

x. Nomeação de um responsável pela segurança ou de um Encarregado de Proteção de Dados, que deverá ser designado sempre que a lei a isso obrigue;
xi. Definição e implementação de controles de acesso físico;
xii. Aplicação de políticas e procedimentos de segurança da EDP;
xiii. Definição e implementação de um procedimento para a destruição ou devolução de Dados Pessoais e documentos, de forma segura e confidencial (tornando impossível recuperá-los mais tarde e certificando a ausência de cópias), quando a relação contratual termine (exceto quando exista a obrigação de conservar os Dados Pessoais por um período adicional, caso em que os Dados Pessoais e documentos devem ser bloqueados).

2. Adicionalmente, para efeitos do Anexo e de seus Apêndices, o **Operador** obriga-se a:

i. Informar imediatamente a **EDP** se, em sua opinião, alguma instrução violar a LGPD ou outras disposições em matéria de proteção de dados;
ii. Enviar o registro de atividades de tratamento realizadas em favor da **EDP**;
iii. Enviar uma declaração por escrito ou cópia do registro interno escrito que as pessoas a seu cargo declararam por escrito que se obrigaram a manter a confidencialidade dos Dados Pessoais a que tiveram acesso, que conhecem as regras e procedimentos que devem ser adotados relativamente ao Tratamento de Dados Pessoais, que participaram em ações de formação sobre esta matéria e que foram informadas e consentiram de forma específica e expressa nos casos em que os seus Dados Pessoais tenham sido comunicados à **EDP** para as finalidades de gestão de acesso a sistemas da **EDP**, gravação de chamadas telefônicas, controle de qualidade e outras finalidades relacionadas com os serviços do **Operador**;
iv. Enviar de forma periódica uma declaração por escrito ou um auto certificação de cumprimento das disposições legais e das obrigações convencionadas com a **EDP** em matéria de proteção de dados;
v. Prestar informação e enviar documentação de suporte à **EDP** sobre qualquer reclamação recebida dos Titulares dos dados e medidas adotadas para a sua resolução;
vi. Prestar informação e enviar documentação de apoio à **EDP** de quaisquer pedidos, consultas ou inspeções promovidas pela ANPD ou Órgão regulador competente em matéria de proteção de Dados Pessoais, das ações desenvolvidas e das respectivas consequências;
vii. Enviar à **EDP** o relatório de auditorias periódicas independentes sobre o cumprimento das disposições legais relacionadas à LGPD, auditorias as quais devem ser realizadas pelo menos a cada 2 (dois) anos;
viii. Obter certificação independente de conformidade com a LGPD (quando estiverem disponíveis mecanismos de certificação);

ix. Aderir a código de conduta sobre proteção de Dados Pessoais, em conformidade com a LGPD, e enviá-lo à **EDP**;

x. Enviar de forma periódica à **EDP** informação relativa ao sistema de gestão do cumprimento de obrigações legais de proteção de dados (modelo de governança, identificação do encarregado de proteção de dados, políticas e procedimentos implementados, registro de atividades de tratamento realizadas em favor da **EDP**, descrição das medidas técnicas e organizacionais implementadas, planos de ação de melhoria etc.);

xi. Enviar prova de ter destruído ou devolvido os Dados Pessoais e documentos, de forma segura e confidencial (impossibilitando a sua posterior recuperação e certificando a ausência de cópias), quando do término da relação contratual (exceto quando exista uma obrigação de conservação dos dados por um período adicional, caso em que devem ser bloqueados os dados e os documentos).

b) Prestadores de serviços de criticidade média que utilizam os sistemas de tecnologia da informação da EDP

1. Para efeitos da cláusula 6 do Anexo de Tratamento de Dados Pessoais, o **Operador** deverá aplicar, no âmbito do Tratamento de Dados Pessoais realizados em favor da **EDP**, as seguintes medidas de segurança técnicas e organizativas complementares:

i. Identificação, divulgação e documentação das funções e obrigações dos colaboradores e terceiros com acesso aos Dados Pessoais;

ii. Manutenção por escrito de todas as atividades de Tratamento de Dados Pessoais realizadas em favor da **EDP**, conforme requisitos da LGPD;

iii. Manutenção de um registro interno que garanta que as pessoas envolvidas se comprometeram por escrito a manter a confidencialidade dos Dados Pessoais que tiveram acesso, que conheçam as regras e procedimentos que devem ser adotados, que consentiram de forma específica, expressa e por escrito na comunicação dos seus dados pessoais à **EDP** para gestão de acessos a sistemas de informação da **EDP**, controle de qualidade ou outras finalidades relacionadas com os serviços do **Operador**;

iv. Definição e implementação de um procedimento de registro de incidentes;

v. Implementação de um procedimento de inventário e controle da entrada e saída de suportes e documentos;

vi. Definição dos critérios do arquivo de suportes e dos dispositivos para armazenamento desses suportes;

vii. Nomeação de um responsável de segurança ou de um Encarregado de Proteção de Dados (DPO), encarregado que deverá ser nomeado sempre que a lei obrigar;

viii. Definição e implementação de controles de acesso físico;

ix. Aplicação de políticas e procedimentos de segurança da **EDP**;

2. Adicionalmente, para os efeitos do Anexo e de seus Apêndices , o **Operador** obriga-se a:

i. Informar imediatamente a **EDP** se, em sua opinião, uma instrução violar a LGPD ou outras disposições em matéria de proteção de dados;

ii. Enviar o registro de atividade de Tratamento realizadas em favor da **EDP**;

iii. Enviar uma declaração por escrito ou cópia do registro interno que garanta que as pessoas alocadas na prestação de serviços tenham se comprometido por escrito a manter a confidencialidade dos Dados Pessoais Tratados, que conhecem as regras e procedimentos que devem ser adotados, que participaram de ações de formação sobre esta matéria e que foram informadas e consentiram no s casos em que seus dados tenham sido comunicados à **EDP** para as finalidades de gestão de acessos a sistemas de informação da **EDP**, controle de qualidade ou outras finalidades relacionadas com os serviços do **Operador**;

iv. Enviar de forma periódica declaração por escrito ou um auto de certificação de cumprimento das disposições legais e de cumprimento das obrigações convencionadas com a **EDP** em matéria de proteção de dados;

v. Prestar e informação e enviar documentação de suporte à **EDP** sobre qualquer reclamação recebida dos Titulares e medidas adotadas para a sua resolução;

vi. Prestar informação e enviar documentação de apoio à **EDP** de quaisquer pedidos, consultas ou fiscalizações promovidas pela ANPD e/ou Órgão Regulador competente em matéria de proteção de Dados Pessoais, das ações desenvolvidas e das respectivas consequências.

c) Prestadores de serviço de criticidade alta que utilizam os sistemas de tecnologia da informação próprios

1. Para efeitos do Anexo e de seus Apêndices, o **Operador** deverá aplicar, no âmbito do Tratamento de Dados Pessoais por conta da **EDP**, as seguintes medidas de segurança técnicas e organizacionais complementares:

i. Identificação, divulgação e documentação das funções e obrigações dos colaboradores e terceiros com acesso a Dados Pessoais;

ii. Manutenção de um registro escrito de todas as atividades de Tratamento realizadas em favor da **EDP**, conforme requisitos da LGPD;

iii. Manutenção de um registro interno que garantia que as pessoas a seu cargo se comprometeram por escrito a manter a confidencialidade dos Dados Pessoais a que tiverem acesso, que conhecem as regras e procedimentos que devem ser adotados, que participaram em ações de formação sobre esta matéria e que foram informadas e consentiram de forma específica, expressa e por escrito na comunicação dos seus Dados Pessoais à **EDP** para a gestão de acessos a sistemas de informação da **EDP**, controle de qualidade ou outras finalidades relacionadas com os serviços do **Operador**;

iv. Definição e implementação de um procedimento de identificação e autenticação dos usuários;
v. Definição e implementação de um procedimento para controlar o acesso aos Dados Pessoais;
vi. Definição e implementação de um procedimento de registro de incidentes;
vii. Definição e implementação de um procedimento de cópia de segurança (backup);
viii. Definição de uma equipe responsável pela gestão de Incidentes para detectar Incidentes e para gerir o impacto e a resolução da ocorrência, com regime de cobertura de 24x7x365;
ix. Adoção de prazo de retenção para os logs pertinentes protegidos e retidos por pelo menos XX (XXX) meses para análise forense;
x. Adoção dos princípios de "Privacy by Design" e "Privacy by Default" durante a execução das atividades;
xi. Implementação de um procedimento de inventário e controle de entrada e saída de suportes e documentos;
xii. Definição dos critérios de arquivo de suportes e dos dispositivos para armazenamento desses suportes;
xiii. Definição e implementação de controles de segurança periódicos para testar, avaliar e valorizar regularmente a eficácia de medidas técnicas e organizacionais para garantir a segurança do Tratamento;
xiv. Nomeação de um responsável pela segurança ou de um Encarregado de Proteção de Dados (DPO), que será designado sempre que a lei exigir;
xv. Definição e implementação de controle de acesso físico;
xvi. Definição e implementação de um plano de continuidade do serviço;
xvii. Definição e implementação de um procedimento de pseudoanonimização dos Dados Pessoais nos casos em que seja tecnicamente possível;
xviii. Definição e implementação de um procedimento de encriptação de suportes;
xix. Definição e implementação de um procedimento de anonimização de Dados Pessoais nos casos em que seja tecnicamente possível;
xx. Definição e implementação de um procedimento para registrar o acesso aos Dados Pessoais;
xxi. Definição e implementação de um procedimento de encriptação das comunicações;
xxii. Definição e implementação de um procedimento de cópia de segurança (backup) e recuperação.
xxiii. Realização de auditorias periódicas independentes programadas, pelo menos a cada 2 (dois) anos, ao cumprimento das disposições legais relativas à proteção de Dados Pessoais e segurança da informação, incluindo a LGPD/Certificação independente do cumprimento da LGPD (quando estejam disponíveis mecanismos de certificação);
xxiv. Adesão a um código de conduta sobre proteção de dados pessoais, de acordo com a LGPD, quando aplicável;
xxv. Definição e implementação de um procedimento para a destruição ou devolução dos Dados Pessoais e documentos, de forma segura e confidencial (tornando impossível

recuperá-los mais tarde e certificando a ausência de cópias), quando a relação contratual termine (exceto quando exista a obrigação de conservar os Dados Pessoais por um período adicional, caso em que os Dados Pessoais e documentos devem ser bloqueados);

xxvi. Definição, comunicação e implementação pelo **Operador** de políticas que protejam e limitem o acesso a Dados Pessoais e/ou Dados Sensíveis de clientes ou colaboradores da **EDP**;

xxvii. Comprovação de que os administradores de sistemas, equipe de operações, gestão e terceiros recebem formação adequada sobre segurança da informação, LGPD e demais Normas aplicáveis, ao menos anualmente;

xxviii. Realização de avaliações periódicas de segurança de rede que incluam:

a. Revisão das principais alterações no ambiente, como um novo componente do sistema, topologia de rede, regra de firewall etc.;
b. Análises de vulnerabilidade;
c. Verificação da manutenção dos registos de alterações, informações sobre os motivos das alterações, inclusão de um revisor e aprovador das mudanças.

xxix. Comprovação de que todos os ativos de tecnologia utilizados são contabilizados e possuem um proprietário identificado. O **Operador** é responsável por manter um inventário desses ativos, estabelecer o uso aceitável e autorizado dos ativos, e fornecer um nível adequado de proteção para os ativos ao longo de seu ciclo de vida;

xxx. Estabelecimento e manutenção de procedimentos de gerenciamento de acesso lógico definindo perfis e grupos de acessos de acordo com a necessidade, para impedir o acesso não autorizado a qualquer Dado Pessoal e/ou Dado Pessoal Sensível de clientes ou colaboradores da **EDP** sob controle do **Operador**;

xxxi. Definição e implementação de procedimentos de gerenciamento de patches e gestão de vulnerabilidades que priorizem a segurança dos sistemas utilizados para Tratar Dados Pessoais e/ou Dados Pessoais Sensíveis de clientes e/ou colaboradores da **EDP**. Esses procedimentos devem incluir:

a. Abordagem de risco definido para priorizar patches de segurança;
b. Capacidade de lidar com e implementar correções de emergência;
c. Aplicabilidade ao sistema operacional e software de servidor, como servidor de aplicativos e software de banco de dados;
d. Documentação do risco que o patch mitiga e rastrear quaisquer exceções;
e. Instalação de software antivírus e antimalware em equipamentos ligados à rede utilizada para processar informações de clientes e/ou colaboradores da **EDP**, incluindo, entre outros, servidores, computadores de produção e de formação para proteger de vírus potencialmente nocivos e de aplicações de software malicioso;
f. Atualização das definições de antimalware diariamente ou de acordo com as instruções do fornecedor de antivírus/antimalware;

xxxii. Garantia da existência de processos de planejamento de cópia de segurança que protejam os Dados Pessoais da **EDP** contra a utilização, acesso, divulgação, alteração e destruição não autorizadas;

xxxiii. Estabelecimento e teste dos planos de continuidade do negócio e recuperação após desastres;

xxxiv. Garantia de que os Dados Pessoais, quando estão em tráfego entre sistemas ou bases de dados utilizam mecanismos de segurança. Por exemplo: protocolo Https;

xxxv. Confirmação de que todos os dispositivos (portáteis, estações de trabalho, etc.) que irão acessar ou processar Dados Pessoais ou confidenciais de clientes e/ou colaboradores da EDP têm aplicado criptografia em disco, incluindo, quando for o caso, equipamentos BYOD;

xxxvi. Manutenção de arquivos físicos com Dados Pessoais de clientes e/ou colaboradores da EDP em um ambiente de acesso controlado;

xxxvii. Anonimização de todos os Dados Pessoais da EDP usados em um ambiente de desenvolvimento ou teste;

xxxviii. Inclusão dos serviços em nuvem em um inventário de ativos;

xxxix. Manutenção de registro em vigor na hipótese de o Operador fazer uso de serviço em nuvem. O registro deve:

a. identificar todos os serviços em nuvem em uso;
b. detalhar o perfil de segurança das informações do serviço;
c. detalhar os recursos de proteção de informações do serviço.

xl. Cumprimento dos requisitos de disponibilidade no design da solução em nuvem e aplicados no contrato;

2. Adicionalmente, para efeitos do disposto no Anexo e de seus Apêndices, o Operador obriga-se a:

i. Informar imediatamente a EDP se, em sua opinião, uma instrução violar a LGPD ou outras disposições em matéria de proteção de dados;

ii. Enviar o registro de atividade de Tratamento realizadas em favor da EDP;

iii. Enviar uma declaração por escrito ou cópia do registro interno que garanta que as pessoas alocadas na prestação de serviços tenham se comprometido por escrito a manter a confidencialidade dos Dados Pessoais Tratados, que conhecem as regras e procedimentos que devem ser adotados, que participaram de ações de formação sobre esta matéria e que foram informadas e consentiram no s casos em que seus Dados Pessoais tenham sido comunicados à EDP para as finalidades de gestão de acessos a sistemas de informação da EDP, controle de qualidade ou outras finalidades relacionadas com os serviços do Operador;

iv. Enviar de forma periódica declaração por escrito ou um auto de certificação de cumprimento das disposições legais e de cumprimento das obrigações convencionadas com a EDP em matéria de proteção de dados;

v. Prestar e informação e enviar documentação de suporte à EDP sobre qualquer reclamação recebida dos Titulares dos Dados Pessoais e medidas adotadas para a sua resolução;

vi. Prestar informação e enviar documentação de apoio à EDP de quaisquer pedidos, consultas ou inspeções promovidas pela ANPD ou Órgão Regulador competente em

matéria de proteção de dados pessoais, das ações desenvolvidas e das respectivas consequências;

vii. Enviar à **EDP** o relatório das auditorias periódicas independentes sobre o cumprimento das disposições legais relativas à proteção de Dados Pessoais, incluindo a LGPD;

viii. Obter certificação independente de conformidade com a LGPD (quando estejam disponíveis mecanismos de certificação);

ix. Obter relatórios de execução de análise de vulnerabilidades e testes de intrusão *(pentest);*

x. Garantir que os subcontratados atendam aos mesmos requisitos de segurança aplicados ao **Operador** pela **EDP.**

xi. Aderir a código de conduta sobre proteção de Dados Pessoais, em conformidade com a LGPD, e enviá-lo à **EDP**;

xii. Enviar de forma periódica à **EDP** informação relativa ao sistema de gestão do cumprimento de obrigações legais de proteção de dados (modelo de governança, identificação do Encarregado de Proteção de Dados (DPO), políticas e procedimentos implementados, registro de atividades de Tratamento realizadas em favor da **EDP**, descrição das medidas técnicas e organizativas implementadas, planos de ação de melhoria etc.);

xiii. Enviar prova de ter destruído e devolvido os Dados Pessoais e documentos, de forma segura e confidencial (impossibilitando a sua posterior recuperação e certificando a ausência de cópias), quando termina a relação contratual (exceto quando exista uma obrigação de conservação dos dados por um período adicional, caso em que devem ser bloqueados os dados/documentos).

d) Prestadores de serviço de criticidade média que utilizam os sistemas de tecnologia da informação próprios

1. Para efeitos do Anexo e seus Apêndices, o **Operador** deverá aplicar, no âmbito do Tratamento de Dados Pessoais realizados em favor da **EDP**, as seguintes medidas de segurança técnicas e organizativas complementares:

i. Identificação, divulgação e documentação das funções e obrigações dos colaboradores e terceiros com acesso aos Dados Pessoais;

ii. Manutenção por escrito de todas as atividades de Tratamento de Dados Pessoais realizadas em favor da **EDP**, conforme requisitos LGPD;

iii. Manutenção de um registro interno que garanta que as pessoas envolvidas se comprometeram por escrito a manter a confidencialidade dos Dados Pessoais que tiveram acesso, que conheçam as regras e procedimentos que devem ser adotados, que consentiram de forma específica, expressa e por escrito na comunicação dos seus Dados Pessoais à **EDP** para gestão de acessos a sistemas de informação da **EDP**, controle de qualidade ou outras finalidades relacionadas com os serviços do **Operador**;

iv. Definição e implementação de um procedimento de identificação e autenticação dos usuários;

v. Definição e implementação de um procedimento para controlar o acesso aos Dados Pessoais;

vi. Definição de um procedimento de registro de incidentes;

vii. Definição e implementação de um procedimento de cópia de segurança (backup);

viii. Implementação de um procedimento de inventário e controle da entrada e saída de suportes e documentos;

ix. Definição dos critérios de arquivo de suportes e dos dispositivos para armazenamento desses suportes;

x. Obtenção de relatórios de execução de análise de vulnerabilidades e testes de intrusão *(pentest);*

xi. Garantia de que os Subcontratados atendam aos mesmos requisitos de segurança aplicados ao Operador pela EDP.

xii. Definição e implementação de controles de segurança periódicos para testar, avaliar e valorizar regularmente a eficácia de medidas técnicas e organizativas para garantir a segurança do Tratamento;

xiii. Nomeação de um responsável pela segurança ou de um Encarregado de Proteção de Dados (DPO), que deverá ser nomeado se a lei a isso obrigar;

xiv. Definição e implementação de controles de acesso físico;

xv. Definição e implementação de um plano de continuidade do serviço;

xvi. Definição e implementação de um procedimento de pseudoanonimização dos Dados Pessoais nos casos em que seja tecnicamente possível.

xvii. Definição, comunicação e implementação pelo Operador de políticas que protejam e limitem o acesso a Dados Pessoais e/ou Dados Pessoais Sensíveis de clientes ou colaboradores da EDP;

xviii. Comprovação de que os administradores de sistemas, equipe de operações, gestão e terceiros receberam formação sobre segurança da informação e LGPD, ao menos anualmente;

xix. Realização de avaliações periódicas de segurança de rede que incluam:

a. Revisão das principais alterações no ambiente, como um novo componente do sistema, topologia de rede, regra de firewall, etc;
b. Realização de análises de vulnerabilidade;
c. Manutenção de registos de alterações, informações sobre os motivos das alterações, inclusão der um revisor e aprovador das mudanças.

xx. Comprovação de que todos os ativos de tecnologia utilizados são contabilizados e possuem um proprietário identificado. O Operador é responsável por manter um inventário desses ativos, estabelecer o uso aceitável e autorizado dos ativos, e fornecer um nível adequado de proteção para os ativos ao longo de seu ciclo de vida;

xxi. Estabelecimento e manutenção de procedimentos de gerenciamento de acesso lógico definindo perfis e grupos de acessos de acordo com a necessidade (segregação de

funções), para impedir o acesso não autorizado a qualquer Dado Pessoal e/ou Dado Pessoal Sensível de clientes e/ou colaboradores da EDP sob controle do Operador;

xxii. Definição e implementação de procedimentos de gerenciamento de patches e vulnerabilidade que priorizem a segurança dos sistemas utilizados para processar Dados Pessoais e/ou Dados Pessoais Sensíveis de clientes ou colaboradores da EDP. Esses procedimentos devem incluir:
   a. Abordagem de risco definido para priorizar patches de segurança;
   b. Capacidade de lidar com e implementar correções de emergência;
   c. Aplicabilidade ao sistema operacional e software de servidor, como servidor de aplicativos e software de banco de dados;
   d. Documentação do risco que o patch mitiga e rastrear quaisquer exceções;
   e. Instalação de software antivírus e antimalware em equipamentos ligados à rede utilizada para processar informações de clientes ou colaboradores da EDP, incluindo, entre outros, servidores, computadores de produção e de formação para proteger de vírus potencialmente nocivos e de aplicações de software malicioso;
   f. Atualização das definições de antimalware diariamente ou de acordo com as instruções do fornecedor de antivírus/antimalware;

xxiii. Garantia da existência de processos de planejamento de cópia de segurança que protejam os Dados Pessoais da EDP contra a utilização, acesso, divulgação, alteração e destruição não autorizadas;

xxiv. Estabelecimento e teste dos planos de continuidade do negócio e recuperação após desastres;

xxv. Garantia de que os Dados Pessoais quando estão em tráfego entre sistemas ou bases de dados utilizam mecanismos de segurança. Por exemplo: protocolo Https;

xxvi. Confirmação de que todos os dispositivos (portáteis, estações de trabalho, etc.) incluindo, quando for o caso, equipamentos BYOD que irão acessar ou processar Dados Pessoais ou confidenciais de clientes ou colaboradores da EDP têm aplicado criptografia em disco;

xxvii. Manutenção de arquivos físicos com Dados Pessoais de clientes ou colaboradores da EDP em um ambiente de acesso controlado;

xxviii. Anonimização de todos os dados da EDP usados em um ambiente de desenvolvimento ou teste;

xxix. Inclusão dos serviços em nuvem em um inventário de ativos;

xxx. Manutenção de um registro em vigor, na hipótese de o Operador fazer uso de serviço em nuvem.. O registro deve:
   a. identificar todos os serviços em nuvem em uso;
   b. detalhar o perfil de segurança das informações do serviço;
   c. detalhar os recursos de proteção de informações do serviço.

xxxi. Cumprimento dos requisitos de disponibilidade no design da solução em nuvem e aplicados no contrato;

2. Adicionalmente, para os efeitos do Anexo e de seus Apêndices, o **Operador** obriga-se a:

i. Disponibilizar à **EDP** todas as informações necessárias para demonstrar o cumprimento das obrigações estabelecidas na LGPD, bem como permitir e contribuir para a realização de auditorias, incluindo inspeções, por parte da **EDP** ou de outro auditor autorizado pela **EDP**;

ii. Informar imediatamente a **EDP** se, em sua opinião, uma instrução violar a LGPD ou outras disposições em matéria de proteção de dados;

iii. Enviar o registro de atividades de Tratamento realizadas em favor da **EDP**;

iv. Enviar uma declaração por escrito ou cópia do registro interno que garanta que os colaboradores e terceiros alocados na prestação de serviços declararam por escrito que se obrigaram a manter a confidencialidade dos Dados Pessoais a que tiveram acesso, que conhecem as regras e procedimentos que devem ser adotados, que participaram em ações de formação sobre esta matéria e que foram informadas e consentiram nos casos em que seus Dados Pessoais tenham sido comunicados à **EDP** para gestão de acessos a sistemas de informação da **EDP**, controle de qualidade ou outras finalidades relacionadas com os serviços do **Operador;**

v. Enviar de forma periódica uma declaração escrita ou auto de certificação de cumprimento das disposições legais e de cumprimento das obrigações convencionadas com a **EDP** em matéria de proteção de dados;

vi. Prestar informação e enviar documentação de suporte à **EDP** sobre qualquer reclamação recebida dos Titulares e medidas adotadas para a sua resolução;

vii. Prestar informação e enviar documentação de apoio à **EDP** de quaisquer pedidos, consultas ou inspeções promovidas pela ANPD e/ou Órgão Regulador competente em matéria de proteção de Dados Pessoais, das ações desenvolvidas e das respectivas consequências.

Apêndice C

Subcontratados aprovados

Nome do subcontratado	Tratamento realizado pelo subcontratado	Territórios

Apêndice D

Template de Reporte de Incidente

Empresa	
Responsável de Contato (ou Encarregado/DPO)	
E-mail	
Telefone	
Data de detecção do incidente	
Data/Hora de comunicação ao responsável de Tratamento	
Estado do incidente	
Data de resolução	

Hora de resolução		
Tipo de incidente		Obs:
Natureza do incidente		Obs:
Descrição		Obs:
Causa do Incidente		Obs:
Consequências do Incidente		Obs:
Medidas de segurança prévias ao incidente		Obs:

Medidas corretivas/mitigadoras		Obs:
Número estimado de Titulares afetados		Obs:
Tipo de Titulares afetados		Obs:
Tipo de Dados Pessoais afetados		Obs:
Os Dados Pessoais afetados permitem a identificação direta dos Titulares?		Obs:
Inteligibilidade dos Dados Pessoais		Obs:

Recursos a subcontratantes (especificar)		Obs:
Existência de fluxos internacionais de Dados Pessoais fora do território brasileiro		Obs:
Outras informações relevantes		