ANEXO DE TRATAMENTO DE DADOS PESSOAIS

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

[XXXXXX], com sede Rua, nº, bairro, na cidade de XXX, Estado de XXXX, 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 em XXXX "**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 as medidas técnicas e organizacionais aplicáveis relacionadas à proteção de Dados Pessoais, nos exatos termos da LGPD e demais Normas;

f. O **Operador** deve tratar os dados pessoais a que tiver acesso apenas de acordo com as instruções da **CONTRATANTE** e em conformidade com estas cláusulas, e que, na eventualidade, de não mais poder cumprir estas obrigações, por qualquer razão, concorda em informar de modo formal este fato imediatamente à **CONTRATANTE,** que terá o direito de rescindir o contrato sem qualquer ônus, multa ou encargo.

g. 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.

(b) "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.

(c) "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.

(d) "Transferência Internacional de Dados": Quando houver a transferência de Dados Pessoais para país estrangeiro.

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. O presente Anexo e seus Apêndices serão aplicáveis ao Tratamento de Dados Pessoais a ser realizado pelo Operador no âmbito do Contrato 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.

2.2. 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.

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

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 razoáveis para cooperar com a **EDP** no cumprimento da Legislação de Proteção de Dados

Aplicável, incluindo, a manutenção de registros, informações e as documentações relacionadas ao Tratamento realizado no âmbito do Contrato.

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**. 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 ou regulatória à qual o Operador está sujeito, o Operador será inteiramente responsável pelas atividades decorrentes deste Tratamento.

3.3. O Operador notificará tempestivamente a **EDP** se identificar quaisquer violações à Lei Geral de Proteção de Dados Aplicável em decorrência de diretriz de Tratamento recebida da **EDP.**

3.4. Caso o Operador não possa cumprir as instruções da **EDP** por qualquer motivo, deverá informá-la tempestivamente sobre este cenário, sendo facultado as Partes acordarem pela reestruturação das obrigações e responsabilidades aplicáveis no âmbito do Contrato ou pela rescisão do mesmo, caso haja a incapacidade do Operador de cumprir com as obrigações pactuadas.

3.5. O Operador não utilizará os Dados Pessoais obtidos em razão do Contato para finalidades alheias ao objeto do Contrato salvo para cumprimento de obrigação legal ou regulatória, ou desde que os Dados Pessoais sejam anonimizados.

4. CONFIDENCIALIDADE.

4.1. 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 estão submetidos aos deveres de confidencialidade.

5. SEGURANÇA.

5.1. 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, em observância ao estado da técnica disponível, sempre com um nível de segurança compatível e adequado aos riscos que o Tratamento implica aos direitos dos Titulares dos Dados Pessoais. Devendo compreender as seguintes medidas:

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

b. 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;

c. 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;

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

e. Enviar periodicamente relatório de auditorias independentes sobre o cumprimento das disposições legais relacionadas à LGPD.

f. Enviar 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.).

5.2. O Operador deverá adotar as medidas de segurança indicadas no Apêndice B deste Anexo. Caso o Tratamento de Dados Pessoais seja enquadrado em um dos critérios definidos de Serviço Crítico, o operador ainda adotará as salvaguardas adicionais solicitadas pela EDP.

5.3. O Operador compromete-se a manter políticas de segurança da informação que sejam aptas a promover a aplicação de medidas técnicas e operacionais para segurança dos Dados Pessoais, nos termos da legislação aplicável.

5.4. A EDP terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da Operadora com as obrigações de Proteção de Dados Pessoais, sem que isso implique em qualquer diminuição de responsabilidade que a Contratada possui perante a Lei e este Anexo.

5.5. 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, desde que não violem políticas internas relacionadas a confidencialidade e estratégia de negócio. O Operador fornecerá aos auditores da EDP acesso a informação relacionada ao Tratamento objeto do Contrato, conforme solicitado pela EDP, dentro dos parâmetros legais de confidencialidade perante os demais clientes do Operador, para verificar a conformidade do Operador com este Anexo.

6. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS.

6.1. A **EDP** declara-se ciente que o Operador poderá realizar a Transferência Internacional de Dados Pessoais para cumprir com as atividades de Tratamento realizadas no âmbito do Contrato, a exemplo de armazenamento em nuvem em servidores localizados em território fora do Brasil, sempre em observância aos requisitos técnicos e à legislação e desde que comunique a **EDP** previamente acerca de tal transferência.

6.2. Na hipótese de ocorrer 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, apenas realizará o Tratamento dos Dados Pessoais de acordo com o disposto abaixo, sem prejuízo de observância das Normas aplicáveis, que deverão prevalecer às instruções em caso de conflito;

(a) 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

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

7. AVALIAÇÃO DE IMPACTO DE PROTEÇÃO DE DADOS.

7.1. 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.

8. OBRIGAÇÃO DE INFORMAÇÃO E GESTÃO DE INCIDENTES.

8.1. Quando o Operador tiver ciência de um Incidente deverá notificá-lo à **EDP**, no prazo de até 24 (vinte e quatro) horas de sua ciência, bem como cooperar com a **EDP** com as informações necessárias para mitigar os riscos de eventual Incidente.

8.2. Na hipótese de ocorrência de Incidente em seu ambiente, o Operador compromete-se a adotar as medidas adequadas para prevenir a continuação e recorrência do Incidente, fornecendo as informações pertinentes à EDP, para que a mesma, se entender necessário, reporte eventual incidente aos titulares e à ANPD.

8.3. Quaisquer notificações de Incidentes, nos termos desta Cláusula, deverão ser endereçadas ao contato fornecido, por parte da EDP: incidente.privacidade@edpbr.com.br, seguindo o Modelo do Apêndice C e deverão conter, sempre que possível informações claras sobre o incidente, incluindo mas sem se limitar: (a) uma descrição da natureza do Incidente, incluindo, sempre que possível, as categorias e o número aproximado de registro de Titulares afetados; (b) o nome e os detalhes de contato do Encarregado de Proteção de Dados do Operador ou outro contato responsável pelas informações; (c) uma descrição das consequências prováveis do Incidente; e (d) uma descrição das medidas tomadas ou propostas a serem tomadas para tratar do Incidente, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.

9. SUBCONTRATAÇÃO.

9.1. A **EDP** declara-se ciente que o Operador poderá realizar a subcontratação das atividades de Tratamento de Dados Pessoais realizadas no âmbito do Contrato, sempre em observância aos requisitos técnicos e à legislação aplicável, devendo o Operador comunicar a **EDP** sempre que houver a subcontratação aqui estabelecida.

9.2. O Operador assegurará que o subcontratado esteja vinculado às obrigações de proteção de Dados Pessoais compatíveis com as do Operador, supervisionará sua conformidade e deverá, em particular, garantir que os subcontratados possuam 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 os termos deste Anexo.

9.3. O Operador será considerado totalmente responsável perante a **EDP** pelas atividades realizadas pelo subcontratado no âmbito do Tratamento de Dados Pessoais relacionados ao Contrato.

10. RESPONSABILIDADE E DIREITO DE REGRESSO.

10.1. Na hipótese de inadimplemento das obrigações do Operador e/ou do subcontratado assumidas neste Anexo que incorram em evento danoso aos Titulares, causado comprovadamente por ato exclusivo do Operador ou de seu subcontratado, o Operador deverá ressarcir a **EDP** pelas perdas, custos, danos, penalidades, multas e despesas (incluindo honorários advocatícios).

10.2. Na hipótese de a EDP arcar com os prejuízos decorrentes de danos gerados pela Operadora diante do descumprimento das obrigações ou responsabilidades atinentes a Proteção de Dados aqui assumidas, fica assegurado à EDP o direito de regresso contra a Operadora, sendo a responsabilidade da Operadora ilimitada nestes casos, independentemente da existência de cláusula que disponha de forma contrária.

10.3. 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 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, 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. MULTA

11.1. Na hipótese de o Operador descumprir quaisquer das obrigações previstas no presente Anexo e/ou obrigações legais relacionadas a proteção de dados pessoais, incorrerá no dever de pagar, em favor da EDP, uma multa não compensatória no valor equivalente a 2% (dois por cento) do valor total do contrato, sem prejuízo de ter que indenizar a EDP, na hipótese de a CONTRATADA:

a) Permitir a Terceiros o acesso aos dados pessoais ou efetuar qualquer comunicação, utilização ou outra forma de tratamento de dados pessoais, por si ou por terceiro, de forma diversa de medidas técnicas ou administrativas de proteção de dados convencionadas neste Anexo;

b) Destruir, perder, alterar, divulgar ou dar acesso não autorizados aos dados pessoais por falta de aplicação de medidas técnicas ou administrativas de proteção dos dados pessoais convencionados neste anexo.

c) Não notificar a **CONTRATANTE** de um incidente ou violação de Dados Pessoais na forma convencionada neste anexo;

11.2. 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. 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.

12. DA DEVOLUÇÃO OU DESTRUIÇÃO DE DADOS PESSOAIS.

12.1. Com a rescisão ou resilição do Contrato do qual faz parte este Anexo e seus Apêndices, o Operador deverá promover em até 30 dias contados da data da rescisão ou resilição, a exclusão, destruição ou devolução, em seus ambientes ou de seus subcontratados, dos Dados Pessoais exclusivamente recepcionados pela **EDP**, ressalvado o direito de o Operador permanecer com os Dados Pessoais por prazo superior para fins de cumprimento de obrigação legal ou regulatória, ou exercício regular de direitos.

12.2. Além do disposto no item 12.1. o OPERADOR deverá 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.

12.2. A expiração ou término deste Anexo não dispensará o Operador de suas obrigações de confidencialidade, de acordo com o Cláusula 4 deste Anexo, que permanecerá vigente após o término deste Anexo.

13. OUTRAS DISPOSIÇÕES

13.1. 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.

13.2. Caso exista modificação dos textos legais ou de qualquer outro de forma que exija modificações na estrutura da prestação de serviços ou na execução das atividades ligadas a este Contrato, as Partes deverão adequar-se às condições vigentes.

13.3. As Partes concordam que só poderão alterar as disposições contidas neste anexo, mediante a celebração de termo aditivo.

13.4. 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.

Cidade/UF , [*] de [*] de 2023.

[RAZÃO SOCIAL DA EDP]

Nome:	**Nome:**
Cargo:	**Cargo:**

[RAZÃO SOCIAL DO FORNECEDOR/CONTRATADA(O)]

Nome:	**Nome:**
Cargo:	**Cargo:**

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 EDP:

Nome	
E-mail	
Telefone	
Endereço	

Operador

O Operador é responsável pelas atividades de Tratamento de Dados Pessoais descritas no objeto do Contrato e neste Apêndice.

Contato Operador:

Nome	
E-mail	
Telefone	
Endereço	

Categoria do Titular

Os Dados Pessoais tratados referem-se à(s) seguinte(s) categoria(s) de Titular de Dado:

Acionistas		**Potenciais Clientes**	
Beneficiários		**Potenciais Colaboradores EDP (Candidatos)**	
Clientes		**Representantes Legais de Clientes**	
Colaboradores EDP		**Representantes Legais de Colaboradores EDP**	
Estatutários		**Representantes Legais de Terceiros**	
Ex-Clientes		**Terceiros**	
Ex-Colaboradores		**Vice Presidentes e Diretores EDP**	
Familiares de Colaboradores EDP		**Voluntários Externos**	
Membros do Conselho			
Outros		(especificar)	

Dados Pessoais

Os Dados Pessoais a tratar dizem respeito às seguintes informações:

Dados Pessoais	

Dados pessoais sensíveis

Os Dados Pessoais Sensíveis a serem tratados dizem respeito às seguintes informações:

Origem racial ou étnica		**Filiação a sindicato ou a organização de caráter religioso, filosófico ou político**	
Convicção religiosa		**dado referente à saúde ou à vida sexual**	
Opinião política		**Dado genético ou biométrico**	

Não aplicável	

Operações de Tratamento

Os Dados Pessoais serão sujeitos às seguintes atividades básicas de tratamento:

Coleta		**Reprodução**		**Eliminação**	
Produção		**Transmissão**		**Avaliação ou controle da informação**	
Recepção		**Distribuição**		**Modificação**	
Classificação		**Processamento**		**Comunicação**	
Utilização		**Arquivamento**		**Transferência**	
Acesso		**Armazenamento**		**Difusão ou Extração**	
Outros		(especificar)			

Natureza e finalidade do Tratamento de Dados

Os Dados Pessoais serão tratados para as seguintes finalidades:

Finalidade	

Apêndice B

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

O presente Apêndice estabelece condições de segurança específicas que devem ser observadas, conforme aplicável no âmbito da execução do Contrato, sem prejuízo as demais disposições já previstas no Anexo.

Este Apêndice somente será aplicável caso seja constatado que o Operador, nos termos do objeto do Contrato celebrado com a EDP, realize a atividades de tratamento de dados que podem ser consideradas como atividades críticas.

Para fins do disposto acima, serão considerados como serviços críticos, aqueles cujo tratamento de dados contenha no mínimo, um dos critérios a seguir, independentemente de qual ambiente os dados serão tratados:

- **Dados Pessoais Sensíveis** – Conforme conceito disposto no art. 5º, inciso II da LGPD e que constituem dados que podem revelar informações sensíveis sobre o titular e, portanto, devem ser resguardados com proteção ainda maior durante o seu tratamento.
- **Alto volume de Dados Pessoais** - Grande quantidade de dados tratados, bem como variedade destes, o número específico dependerá do fluxo e da atividade contratada no cenário concreto.
- **Tecnologias emergentes** – Quando a contratação envolver o uso de tecnologia emergente que possa causar danos aos titulares, como por exemplo o uso de reconhecimento facial.
- **Dados de vigilância** – Tratamento que envolva o uso dos dados pessoais para vigilância ou controle em ambientes monitorados.
- **Decisões automatizadas** – Quando a contratação envolver o uso de decisões automatizadas em relação aos titulares, como por exemplo definição de perfis de consumo, de crédito, dentre outros.
- **Tratamento relevante** – Hipótese na qual o tratamento está atrelado à eventuais sistemas da EDP relevantes à execução das atividades desta, como sistemas de folha de pagamento.
- **Transferência internacional de dados** – Fornecedores que realizam a transferência internacional de Dados Pessoais sob controle da EDP.
- **Subcontratação** - Quando o fornecedor contratado se utilizar de terceiros no tratamento dos dados, conhecidos como “suboperadores”.

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

a) Prestadores de <u>serviço crítico</u> que utilizam os <u>sistemas de tecnologia da informação da EDP</u>

Para efeitos da cláusula 5 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 que realizar em nome 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 conscientização e aprimoramento sobre a matéria.

iv. Manutenção de um registro interno escrito, que garanta que as pessoas alocadas foram informadas e que o compartilhamento dos dados pessoais destas com a **EDP** foi realizado com a adoção de base legal adequada, para a finalidade específica de gestão de acesso a instalações e sistemas de informação da **EDP** e para quaisquer outras finalidades de Tratamento relevantes (por exemplo, controle de qualidade etc.) caso aplicável, sempre informado de forma expressa e transparente;

v. Manutenção de um registro interno escrito que garanta que as pessoas alocadas foram informadas sobre a gravação de chamadas telefônicas que intervêm, caso aplicável;

vi. Definição e implementação de um procedimento de registro escrito de incidentes;

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

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

ix. Nomeação de um responsável pela segurança ou de um Encarregado de Proteção de Dados, nos termos previstos na legislação aplicável;

x. Definição e implementação de controles de acesso físico;

xi. Observância por si e por seus funcionários sobre as políticas e procedimentos de segurança da EDP;

xii. 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 ressalvada a manutenção por períodos superiores para o cumprimento de obrigação legal ou regulatória.

b) Prestadores de <u>serviço não crítico</u> que utilizam os <u>sistemas de tecnologia da informação da EDP</u>

Para efeitos da cláusula 5 do Anexo de Tratamento de Dados Pessoais, o **Operador** deverá aplicar, no âmbito do Tratamento de Dados Pessoais realizados em nome 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 nome 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 e que o compartilhamento dos dados pessoais destas com a **EDP** foi realizado com a adoção de base legal adequada **,** para a finalidade de 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), nos termos previstos na legislação aplicável;

viii. Definição e implementação de controles de acesso físico;

ix. Observância por si e por seus funcionários das políticas e procedimentos de segurança da **EDP**;

c) Prestadores de <u>serviço crítico</u> que utilizam os <u>sistemas de tecnologia da informação próprios</u>

Para efeitos da cláusula 5 do Anexo de Tratamento de Dados Pessoais, o **Operador** deverá aplicar, no âmbito do Tratamento de Dados Pessoais em nome 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 nome 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 conscientização e aprimoramento sobre a matéria e que foram informadas e que o compartilhamento dos dados pessoais destas com a **EDP** foi realizado com a adoção de base legal adequada, 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, conforme aplicável;

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), nos termos previstos na legislação aplicável;

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. 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);

xxiv. 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;

xxv. 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.

xxvi. 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;

xxvii. 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**;

xxviii. 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*;

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

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

xxxi. 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;

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

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

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

xxxv. 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.

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

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

d) Prestadores de <u>serviço não crítico</u> que utilizam os <u>sistemas de tecnologia da informação próprios</u>

Para efeitos da cláusula 5 do Anexo de Tratamento de Dados Pessoais, o **Operador** deverá aplicar, no âmbito do Tratamento de Dados Pessoais realizados em nome 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 nome 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, e que o compartilhamento dos dados pessoais destas com a **EDP** foi realizado com a adoção de base legal adequada, = 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), nos termos previstos na legislação aplicável.

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

xviii. 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.

xix. 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;

xx. 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**;

xxi. 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*;

xxii. 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;

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

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

xxv. 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;

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

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

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

xxix. 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.

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

Apêndice C

Template de Reporte de Incidente

Este Apêndice destina-se a ser usado quando ocorrer algum tipo de incidente que afete a segurança da informação do Grupo EDP, incluindo aqueles que potencialmente afetam os dados pessoais compartilhados.

Todo e qualquer incidente deverá ser endereçado para: incidente.privacidade@edpbr.com.br, contendo as informações necessárias abaixo:

REPORTE DE INCIDENTE

Tipo de Comunicação	Para Comunicação Parcial
☐ Completa ☐ Parcial	☐ Preliminar ☐ Complementar

Empresa / Fornecedor	
Nome	
CNPJ	

Responsável / Encarregado de Dados / DPO	
Nome	
E-mail	
Telefone	

Informações do Incidente			
Data de Detecção	--/--/----	Hora de Detecção	--:--
Data de Comunicação	--/--/----	Hora de Comunicação	--:--
Data de Resolução	--/--/----	Hora de Resolução	--:--
Descrição	[Descreva de forma resumida como o incidente de segurança de dados pessoais ocorreu]		
Tipo de Incidente	☐ Visualização Indevida ☐ Acesso Indevido ☐ Cópia dos dados ☐ Dados Criptografados	☐ Dados Comprados ☐ Dados Vendidos ☐ Expostos Publicamente ☐ Outros [especificar]	
Causa do Incidente	☐ Falha Humana ☐ Falha de Segurança Lógica ☐ Falha de Segurança Física	☐ Vulnerabilidade em Infraestrutura ☐ Falha de Configuração de Software ☐ Outros [especificar]	
	☐ Não tenho conhecimento ou certeza [justifique]		

Consequências ou Riscos do Incidente	☐ Sanções Administrativas ☐ Financeiros ☐ Direitos e Liberdades Individuais ☐ Fuga de Investidores ☐ Danos Reputacionais e de Imagem	☐ Ações Judiciais Individuais ☐ Ações Judiciais coletivas ☐ Quebra de Confiança com o consumidor ☐ Outros [especificar]
Consequencias Trasfronteiriças		

Natureza dos Dados Afetados	
☐ Origem Racial ou Étnica ☐ Convicção Religiosa ☐ Opinião Política ☐ Filiação a Sindicato ☐ Dado referente à Saúde ☐ Dado Genético ou Biométrico	☐ Dados financeiros ☐ Nomes de usuário ou senhas de sistemas de informação ☐ Dado de geolocalização ☐ Filiação a organização de caráter religioso, filosófico ou político ☐ Dado referente à vida sexual ☐ Dado de Comprovação de identidade oficial (RG, CPF, CNH)
☐ Outros [especificar]	
Localização dos Dados Afetados	☐ Brasil ☐ Exterior [informar o país]
Os Dados Pessoais afetados permitem A identificação direta dos Titulares?	☐ Sim ☐ Não [justificar]
Realizado Relatório de Impacto?	☐ Sim ☐ Não [justificar]

Tipo de Titulares Afetados	
☐ Funcionários ☐ Prestadores de Serviço ☐ Clientes / Consumidores	☐ Crianças e Adolescentes ☐ Parceiros Subcontratados ☐ Outros [especificar]
☐ O Incidente de segurança pode acarretar riscos ou dano relevante aos titulares ☐ Não tenho certeza sobre o nível de riscos do incidente de segurança	
Considerando os titulares afetados, independente da ocorrência ou não de transferência internacional, o incidente pode trazer consequências transfronteiriças (implicações com legislações internacionais)?	☐ Sim [justificar] ☐ Não [justificar]

Considerando os titulares afetados, na sua avaliação, o incidente pode...	[especificar]

Medidas de Segurança, Técnicas e Administrativas	
Tomadas após a ciência do incidente	[especificar]
Tomadas para reverter ou mitigar os efeitos do prejuízo do incidente	[especificar]
Medidas ainda serão adotadas	[especificar]

Comunicação do Incidente ao Controlador	
Realizada dentro do prazo de 24 horas após ciência do Incidente?	☐ Sim [justificar] ☐ Não [justificar]
Data da comunicação	--/--/----
Informar quem Comunicou	
Informar quais meios utilizados	
Comunicação do Incidente à Autoridade Nacional	
Realizada comunicação à ANPD?	☐ Sim [justificar] ☐ Não [justificar]
Data da comunicação	--/--/----
Informar quem Comunicou	
Informar quais meios utilizados	
Comunicação do Incidente aos titulares	
Realizada comunicação aos titulares?	☐ Sim [justificar] ☐ Não [justificar]
Data da comunicação	--/--/----
Informar quem Comunicou	
Informar quais meios utilizados	

Outras informações relevantes
[descrever]