

1 CONTEXTO E OBJETIVO

- 1.1 As Instruções aos Terceiros para o Processamento de Dados (o "**Processamento de Dados**") é parte anexa aos Contratos e demais documentos pertinentes no qual a Statkraft avaleie ser necessário para o conhecimento e aceite de seus terceiros ("Processador") que terão contato/acesso aos dados da Statkraft e/ou suas subsidiárias ("Controlador"). Statkraft e Terceiros envolvidos serão denominados como "Partes" neste documento".
- 1.2 O objetivo da Instrução aos Terceiros para Processamento de Dados é estabelecer os direitos e obrigações das Partes em relação ao processamento de dados realizado pelo Processador em nome do Controlador nos termos do Contrato principal.
- 1.3 O presente instrumento substitui quaisquer acordos ou cláusulas anteriores entre as Partes especificamente relacionados à proteção de dados.
- 1.4 Os termos e condições do Contrato Principal permanecem em pleno vigor e efeito, com exceção de quaisquer modificações especificadas nesta Instrução aos Terceiros para Processamento de Dados. Em caso de inconsistência entre o Contrato Principal e a Instrução aos Terceiros para Processamento de Dados em questões especificamente relacionadas à proteção de dados, este último prevalecerá.

2 DEFINIÇÕES

- 2.1 "**Lei de proteção de dados aplicável**": Lei aplicável de proteção de dados e privacidade, incluindo, entre outras, a LGPD, a Lei Geral de Proteção de Dados Pessoais da Noruega e a GDPR (a partir de 25 de maio de 2018).
- 2.2 "**LGPD**": Lei Geral de Proteção de Dados do Brasil, promulgada pela Lei Federal 13.709/2018.
- 2.3 "**GDPR**": Regulamento Geral de Proteção de Dados da UE 2016/679.
- 2.4 "**Cláusulas contratuais padrão**": As cláusulas contratuais padrão para a transferência de dados pessoais para processadores de dados estabelecidos em países terceiros, estabelecidas pela LGPD e/ou pela decisão da Comissão da UE de 5 de fevereiro de 2010 e/ou estabelecidas pela Comissão da UE ou por uma autoridade supervisora relevante, em conformidade com o artigo 28(7) ou 28(8) do GPDR, conforme aplicável.
- 2.5 "**Subcontratado**" ou **Subprocessador**": Outro processador de dados contratado pelo Processador.
- 2.6 "**País terceiro**": Uma região fora do território brasileiro ou do EEE que a autoridade supervisora aplicável não aprovou como oferecendo um nível adequado de proteção de dados.
- 2.7 "**Processador**": refere-se ao Operador definido pela LGPD.
- 2.8 "**Processamento de dados**": compreende o tratamento de dados definido pela LGPD.
- 2.9 Outros termos terão os significados definidos na LGPD.

3 ESCOPO

- 3.1 O objeto desta Instrução aos Terceiros para Processamento de Dados são quaisquer dados pessoais que o Processador processa em nome do Controlador.
- 3.2 A natureza e a finalidade do processamento de dados pessoais, o tipo de dados pessoais e as categorias de titulares de dados estão descritos no Anexo 1.

4 OBRIGAÇÕES GERAIS

- 4.1 O Processador deve processar os dados pessoais apenas para os fins e dentro do escopo estabelecido no Anexo 1, e de acordo com as instruções documentadas do Controlador.

5 ASSISTÊNCIA AO CONTROLADOR

- 5.1 O Processador deve auxiliar o Controlador por medidas técnicas e organizacionais apropriadas, na medida do possível, para o cumprimento das obrigações do Controlador.

6 MEDIDAS DE SEGURANÇA TÉCNICA E ORGANIZACIONAL

- 6.1 O Processador deve implementar medidas técnicas e organizacionais apropriadas para proteger os dados pessoais contra destruição acidental ou ilegal ou perda acidental, alteração, divulgação ou acesso não autorizado. No mínimo, o Processador deve tomar todas as medidas exigidas pelas leis aplicáveis, melhores práticas e orientações das autoridades de supervisão, conforme determinado nas medidas definidas ou mencionadas no [Anexo 2](#).
- 6.2 O Processador não compartilhará os dados pessoais processados de acordo com o Contrato Principal, com terceiros, sem a aprovação prévia por escrito do Controlador e, com exceção de quaisquer subprocessadores pré-aprovados, com base na necessidade de conhecimento.
- 6.3 O Processador deve garantir que todas as pessoas autorizadas a processar os dados pessoais estejam sujeitas a uma obrigação de confidencialidade. O Processador deve ser capaz de documentar a conformidade com este dever, mediante solicitação do Controlador.

7 UTILIZAÇÃO DE SUBPROCESSADORES

- 7.1 O Processador só pode contratar um subcontratado com a autorização específica por escrito do Controlador, a critério exclusivo do Controlador. Os subcontratados autorizados, se houver, estarão listados no [Anexo 3](#).
- 7.2 O processamento de dados pessoais em nome do Controlador deve ser feito apenas por meio de um contrato por escrito com o subcontratado que imponha obrigações de proteção de dados apropriadas ao subcontratado.
- 7.3 O Processador permanece totalmente responsável perante o Controlador pelo desempenho das obrigações dos subcontratados.

8 TRANSFERÊNCIA INTERNACIONAL DE DADOS

- 8.1 O Processador só pode transferir dados pessoais para um país terceiro ou uma organização internacional, mediante instruções documentadas do Controlador.

9 VIOLAÇÕES DE DADOS PESSOAIS

- 9.1 No caso de violação da Instrução aos Terceiros para Processamento de Dados ou dos regulamentos de privacidade aplicáveis, incluindo qualquer situação de acessos não autorizados e situações acidentais ou ilegais de destruição, perda, alteração, comunicação, disseminação ou qualquer forma de tratamento impróprio ou ilegal relacionado a esta Instrução aos Terceiros para Processamento de Dados, o Processador deverá notificar imediatamente o Controlador, por escrito, sobre a violação, o mais tardar 36 horas após tomar conhecimento. A notificação de uma violação de dados pessoais deve, na medida do relevante, no mínimo descrever a natureza da violação de dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de titulares de dados em questão, e as categorias e o número aproximado de registros de dados pessoais em questão.

- 9.2 Em caso de violação de dados pessoais, o Controlador é o único responsável por notificar a autoridade supervisora relevante e os titulares dos dados. O Processador não deve comunicar informações relacionadas a uma violação de dados pessoais ao público ou a terceiros.

10 AUDITORIAS

- 10.1 O Processador deve permitir e contribuir com auditorias das operações de processamento do Processador conduzidas pelo Controlador ou outro auditor determinado pelo Controlador. O Processador também deve permitir e contribuir com essas auditorias por uma autoridade supervisora, quando aplicável.
- 10.2 Uma parte deve cobrir seus próprios custos associados a uma auditoria. No entanto, se uma auditoria revelar desvios significativos das obrigações estabelecidas nesta Instrução aos Terceiros para Processamento de Dados, todos os custos da auditoria serão suportados pelo Processador, incluindo custos razoáveis do Controlador e de outro auditor determinado pelo Controlador.

11 INDENIZAÇÃO

- 11.1 O Processador indenizará e isentará o Controlador de e contra quaisquer custos e perdas causadas por qualquer reclamação de terceiros de que o processamento de dados pessoais provoca uma violação da lei de proteção de dados aplicável, e a reclamação seja causada pela violação do Processador de suas obrigações decorrentes desta Instrução aos Terceiros para Processamento de Dados de processamento de dados.
- 11.2 A indenização está condicionada a (i) que o Controlador notifique prontamente o Processador da reclamação e (ii) ao Processador seja dada a possibilidade de cooperar com o Controlador na defesa e solução da reclamação.

12 PRAZO E RESCISÃO

- 12.1 Esta Instrução aos Terceiros para Processamento de Dados de Processamento de Dados permanecerá em vigor enquanto o Processador processar dados pessoais em nome do Controlador nos termos do Contrato Principal.
- 12.2 Após a expiração ou rescisão, o Processador, à escolha do Controlador, excluirá ou devolverá todos os dados pessoais ao Controlador, excluirá quaisquer cópias e comprovará ao Controlador que o fez, a menos que a lei aplicável exija que o Processador armazene os dados pessoais. Nesse caso, o Processador armazenará com segurança, mas não processará efetivamente os dados pessoais, e excluirá os dados pessoais assim que permitido por lei.

Por e em nome do Controlador:

Por e em nome do Processador:

Assinatura: _____

Assinatura: _____

Nome:

Nome:

Data:

Data:

ANEXO 1: ESCOPO DO PROCESSAMENTO

Objetivo do processamento (o porquê)

<Inserir a finalidade. Exemplo: *O objetivo do processamento é para que o Processador cumpra suas obrigações nos termos do Contrato Principal*>

Natureza e objeto do processamento (como)

<Insira uma descrição ou faça referência a partes relevantes do Contrato Principal ou anexos do Contrato Principal. Exemplo: *hospedagem de dados em uma plataforma baseada em nuvem*>

Categorias de titulares de dados (quem)

<Inserir categorias de titulares de dados. Exemplos: *Colaboradores atuais, antigos e potenciais do Controlador; colaboradores atuais, antigos e potenciais dos clientes do Controlador*>

Categorias de dados pessoais (o quê)

<Inserir categorias de dados pessoais. Exemplos: *Nome, data de nascimento, sexo, detalhes de contato, funções/cargo comercial, nome do empregador, períodos de emprego e serviço para aposentadoria, salário, natureza e detalhes dos acordos atuais e passados dos valores das pensões, contribuições de pensão, benefícios dos empregados, estado civil, dados do beneficiário, dados bancários, número do seguro nacional e/ou status de doença, transações, educação e outras qualificações profissionais, informações de crédito, relacionamento com autoridades e funcionários governamentais, familiares imediatos, informações recebidas através de pesquisas em fontes públicas e discussões/entrevistas, detalhes técnicos (incluindo, por exemplo, string do agente do usuário, modelo e fabricante do dispositivo, ID do anúncio, endereço IP); detalhes de comportamento (incluindo, por exemplo, URLs visitadas, eventos acionados em ações definidas, como carregamentos de páginas, cliques, logins e compras); dados de localização geográfica (estimativa agregada com base no endereço IP coletado) e categorias semelhantes de dados pessoais*>

Classificações de categorias especiais de dados (se relevante)

<Inserir classificações de categorias especiais de dados. Exemplos: *origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, associação a sindicatos, processamento de dados genéticos ou biométricos com o objetivo de identificar exclusivamente uma pessoa, dados relativos à saúde ou dados relativos à orientação sexual de uma pessoa*>

ANEXO 2: MEDIDAS DE SEGURANÇA TÉCNICA E ORGANIZACIONAL

O Processador deve, no mínimo, tomar todas as medidas estabelecidas ou mencionadas abaixo. Sem a aprovação por escrito do Controlador, o Processador não pode alterar essas medidas de maneira a reduzir o nível de segurança. O Processador trabalhará continuamente para melhorar suas medidas de segurança e mantê-las atualizadas com os desenvolvimentos tecnológicos.

Medidas de segurança física - continuidade do serviço

O Processador deve garantir que as instalações onde os dados pessoais estão sendo processados tenham as medidas técnicas e organizacionais necessárias para garantir a segurança física e ambiental. Tais medidas devem incluir pelo menos métodos para:

- proteger ativos de informações contra acesso físico não autorizado,
- gerenciar, monitorar e registrar a movimentação de pessoas dentro e fora das instalações; e
- proteção contra riscos ambientais, como danos causados por calor, fogo e água.

Medidas técnicas de segurança

O Processador deve ter procedimentos em relação a incidentes para garantir que os diferentes problemas sejam investigados, respondidos, mitigados e notificados ao Controlador.

O Processador deve ter controles de segurança de rede.

Antivírus e antimalware

A proteção antimalware deve ser fornecida em todas as estações de trabalho e servidores. Os arquivos de definição de vírus nos servidores devem ser atualizados regularmente, conforme apropriado.

Qualquer dispositivo infectado ou suspeito de infecção deve ser colocado em quarentena ou desconectado de outros dispositivos, até que esteja devidamente livre de malware.

Gerenciamento de usuários

O Processador deve gerenciar o acesso eletrônico com base nos níveis de autoridade e funções de trabalho, por exemplo

- conceder acesso com base na necessidade de conhecer e no menor privilégio,
- uso de IDs e senhas exclusivos para todos os usuários,
- revisão periódica e
- revogar ou alterar o acesso imediatamente quando o emprego termina ou ocorrem alterações nas funções do trabalho.

O acesso será solicitado apenas com base na necessidade de conhecimento.

Todos os usuários aprovados devem receber um ID de usuário exclusivo para facilitar uma trilha de auditoria da atividade do usuário.

O Processador deve ter controles de senha projetados para gerenciar e controlar a força, a validade e o uso da senha. A política de senhas deve garantir que as senhas:

- não sejam armazenadas em formato legível nos sistemas de computador do Processador;
- sejam trocadas regularmente;
- tenham complexidade definida;
- tenham um patamar de histórico para impedir a reutilização de senhas recentes; e
- as senhas iniciais devem ser alteradas após o primeiro uso.

**Instruções aos Terceiros para
Processamento de Dados**



ANEXO 3: SUBPROCESSADORES APROVADOS (se aplicável)

Nome da empresa	Endereço da empresa	Local de processamento (país)