

## TERMOS E CONDIÇÕES PARA TRATAMENTO DE DADOS PESSOAIS

Este Instrumento, doravante denominado **TERMOS E CONDIÇÕES PARA TRATAMENTO DE DADOS PESSOAIS**, tem por finalidade estabelecer os procedimentos, direitos e obrigações entre a **HUSQVARNA DO BRASIL INDÚSTRIA E COMÉRCIO DE PRODUTOS PARA FLORESTA E JARDIM LTDA.**, pessoa jurídica de direito privado, com endereço na Cidade de São Carlos, Estado de São Paulo, na Rua Coronel J. A de Oliveira Salles, s/n, CEP 13.570-820, inscrita no CNPJ/ME sob nº 04.098.470/0001-90, todas as suas filiais, seus Fornecedores e parceiros de negócios, durante o período de vigência do Contrato firmado entre as partes, Pedido de Compra e, qualquer relação que envolva dados pessoais, sem prejuízo de outras condições previstas na legislação pertinente.

### PREÂMBULO

A. Considerando a natureza da operação, a Prestadora terá acesso a dados pessoais e, portanto, sob a égide da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), art. 5º, XII da Constituição Federal bem como demais legislações aplicáveis ao resguardo da privacidade e proteção de dados, a PRESTADORA DE SERVIÇOS se compromete e se responsabiliza quanto ao tratamento dos dados pessoais coletados, em face do objeto deste TERMOS E CONDIÇÕES.

#### 1. Das Definições e Interpretação

##### 1.1 Neste instrumento, salvo se de outro modo exigido pelo contexto:

O termo “**Relatório de Impacto na Proteção de Dados**” terá o significado estabelecido no Artigo 5º, inciso XVII da LGPD.

O termo “**Legislação de Proteção de Dados**” refere-se à legislação brasileira, em especial, enquanto permanecer em vigor, a Lei Geral de Proteção de Dados Pessoais (Lei Nº 13.709/2018 ou “LGPD”), o Marco Civil da Internet (Lei Nº 12.965/2014 e Decreto Nº 8.771/2016), a Constituição Federal, Código Civil Brasileiro, Código Penal, Código de Defesa do Consumidor (Lei Nº 8.078/1990 e Decreto Nº 7.963/2013), suas alterações posteriores, e quaisquer outras leis e regulamentos em relação ao Tratamento, privacidade, sigilo e proteção de Dados Pessoais que sejam aplicáveis e, se aplicáveis, todas as orientações, normas, regras, portarias, regulamentos e códigos de prática e conduta emitidos pela Autoridade Nacional de Proteção de Dados (“ANPD”) ou outra entidade governamental pertinente.

O termo “**Empresa do Grupo**” refere-se, em relação a alguma pessoa jurídica, a qualquer outra pessoa jurídica que, de forma direta ou indireta, controle, seja controlada ou esteja em controle comum com a primeira, sendo que o termo “**controle**”, para os fins desta definição, refere-se à titularidade direta ou indireta de direitos de sócio que lhe assegurem, de modo permanente, a preponderância nas deliberações sociais e o poder de eleger a maioria dos administradores.

O termo “**Empregado(s)**” refere-se a qualquer funcionário, consultor, trabalhador temporário, trabalhador de agência, estagiário, empreiteiro, trabalhador cedido ou outros que sejam empregados atuais, ex-empregados ou empregados em potencial.

O termo “**Dados Pessoais Relevantes**” refere-se às categorias de Dados Pessoais estabelecidas no 0 e que sejam Tratadas em função ou de forma relacionada à prestação dos Serviços.

O termo “**Dados Pessoais Sensíveis**” refere-se às categorias de dados descritas no Artigo 5º, inciso II da LGPD.

O termo “**Tratamento**” (ou “**Tratar**” ou “**Tratado(s)**”) refere-se a qualquer operação ou conjunto de operações realizadas com Dados Pessoais ou conjuntos de Dados Pessoais, seja por meios automatizados ou não, tais como, mas não se limitando a, coleta, uso, acesso, organização, consulta, produção, alteração, recepção, classificação, utilização, reprodução, comunicação, transmissão, distribuição, tratamento, arquivamento, registro, estruturação, armazenamento, adaptação, recuperação, transferência, disponibilização, combinação, restrição, eliminação, avaliação ou controle, modificação, eliminação ou extração

O termo “**Operadora**” refere-se a qualquer pessoa natural ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador de Dados.

O termo “**Controladora**” refere-se o Responsável pelo Tratamento de Dados Pessoais, a quem competem as decisões referentes ao Tratamento.

O termo “**Suboperadora**” refere-se a qualquer terceiro contratado pela Prestadora de Serviços para o Tratamento de Dados Pessoais Relevantes.

1.2 Os termos “**Autoridade de Proteção de Dados**”, “**Titular de Dados**”, “**Dados Pessoais**”, “**Violação de Dados Pessoais**” e “**Autoridade Nacional**” terão os significados estabelecidos na **Legislação de Proteção de Dados**.

## **2. Objeto e Abrangência**

2.1 O presente Instrumento somente se refere ao Tratamento de Dados Pessoais Relevantes. O presente Instrumento tem por finalidade auxiliar na garantia da proteção adequada aos Dados Pessoais Relevantes. Na medida em que houver conflito entre as disposições deste Instrumento e as do Contrato de Prestação de Serviços referentes ao objeto, prevalecerá o presente instrumento.

## **3. Das Obrigações da Prestadora de Serviços**

3.1 A Prestadora de Serviços afirma e garante à Cliente que implantará medidas técnicas e institucionais adequadas para proteger os Dados Pessoais Relevantes em consonância com a Legislação de Proteção de Dados vigente, especialmente com os Artigos de 46 a 49 da LGPD. A Prestadora de Serviços garantirá que essas medidas técnicas e institucionais sejam apropriadas aos riscos específicos impostos por suas atividades de Tratamento, especialmente no que se refere à proteção dos Dados Pessoais Relevantes contra destruição, perda, alteração, divulgação inadvertida ou acesso acidental ou ilegal. A Prestadora de Serviços deverá apresentar ao cliente, quando solicitado, documentos comprobatórios dos procedimentos regulares adotados para identificar, solucionar e eliminar Incidentes de Segurança da Informação envolvendo os Dados Pessoais tratados durante a execução deste Instrumento. Ambas as partes se comprometem a cooperar uma com a outra na investigação de tais Incidentes de Segurança da Informação. A Prestadora de Serviços realizará inspeções internas regularmente a fim de confirmar o seu cumprimento das obrigações previstas neste Instrumento.

3.2 A Prestadora de Serviços compromete-se por si e por seus Suboperadores, a:

- Observar o Anexo 2 deste Instrumento que dispõe sobre – Medidas Técnicas e Institucionais de Segurança, para fazer cumprir as medidas indicadas ou similares, garantindo maior segurança e proteção aos dados que serão tratados durante a prestação de serviços;
- Apenas realizar a transferência internacional de Dados Pessoais sujeitos à LGPD para países fora do território brasileiro nas seguintes situações: A) na medida em que a transferência for necessária para a prestação dos Serviços e a Cliente tenha fornecido seu consentimento prévio e por escrito para tal transferência e B) a transferência seja feita

para um país para o qual a Autoridade Nacional de Proteção de Dados (ANPD) tenha tomado uma decisão de “adequação” para fins de transferência de dados transfronteiriça, de acordo com o Artigo 33 (I) combinado com o artigo 34 da LGPD; ou C) o nível apropriado de proteção de dados pela Prestadora de Serviços seja produzido de acordo com o Artigo 33 (II). A Prestadora de Serviços garantirá que tais transferências de Dados Pessoais (incluindo quaisquer transferências feitas por seus Suboperadores) estejam em conformidade com a Legislação de Proteção de Dados aplicável.

3.3 Caso quaisquer leis aplicáveis exijam que sejam tomadas medidas adicionais em relação a quaisquer restrições de exportação de dados para permitir a transferência internacional de Dados Pessoais, nos termos deste instrumento, para a Prestadora de Serviços (incluindo seus Subcontratados e Suboperadores), a Prestadora de Serviços cumprirá esses requisitos de proteção de dados, através dos instrumentos jurídicos adequados e ferramentas técnicas e de tecnologia necessárias para garantir a existência de salvaguardas apropriadas para essa transferência. A Prestadora de Serviços notificará a Cliente sobre quaisquer transferências de Dados Pessoais para fora do território brasileiro sujeitas aos novos requisitos de exportação de dados sem demora indevida, antes da realização da transferência.

3.4 As Partes desde já reconhecem e concordam que a Cliente é Controladora e a Prestadora de Serviços é Operadora no que se refere ao Tratamento dos Dados Pessoais Relevantes. Além e não obstante nenhum outro direito ou obrigação oriunda deste Instrumento ou do Contrato de Prestação de Serviços, a Prestadora de Serviços, em relação ao Tratamento em questão, (i) somente tratará os Dados Pessoais Relevantes na medida do estritamente necessário em função deste instrumento, especificamente da forma descrita no 0 abaixo; e (ii) cumprirá, tanto por si quanto por cada um de seus Empregados, representantes e Suboperadoras o disposto na legislação vigente de Proteção de Dados.

3.5 Se, em qualquer momento, a Prestadora de Serviços tiver uma restrição legal no cumprimento das instruções da Cliente referentes ao Tratamento de Dados Pessoais Relevantes (seja em função de alteração na legislação pertinente ou nas instruções da Cliente), deverá a Prestadora de Serviços, de forma imediata:

(a) notificar tal restrição legal à Cliente, fornecendo nível razoável de detalhes quanto às instruções que não possam ser cumpridas, bem como os motivos do não cumprimento, ao máximo permitido pela legislação pertinente; e

(b) cessar todo e qualquer Tratamento dos Dados Pessoais Relevantes afetados (que não seja o mero armazenamento e manutenção da segurança desses Dados Pessoais Relevantes afetados) até que a Cliente expeça novas instruções que a Prestadora de Serviços possa cumprir.

3.6 A Prestadora de Serviços e, quando pertinente, o seu representante, deverão, em relação ao Tratamento de Dados Pessoais Relevantes:

(a) criar; manter atualizados por toda a duração do Tratamento; e guardar, pelo período estabelecido pela lei, registros completos e precisos por escrito (inclusive em formato eletrônico) de suas atividades de Tratamento, inclusive de todas as categorias de atividade de Tratamento, em relação aos Dados Pessoais Relevantes, e divulgar esses registros à Cliente ou a qualquer Autoridade Supervisora imediatamente, mediante solicitação;

(b) garantir a manutenção do sigilo dos Dados Pessoais Relevantes; tomar todas as medidas cabíveis para garantir a confiabilidade e credibilidade dos Empregados e eventuais Suboperadoras da Prestadora de Serviços, e garantir que todos os Empregados e eventuais Suboperadoras da

Prestadora de Serviços tenham se comprometido a garantir o sigilo de todos os Dados Pessoais Relevantes por eles Tratados;

(c) certificar-se de que, em cada caso em que contrate uma Suboperadora para Tratamento de quaisquer Dados Pessoais Relevantes: mantenha a Cliente informada de eventual alteração na função ou situação da Suboperadora; e celebre um contrato vinculante por escrito com a Suboperadora que imponha a esta as mesmas obrigações pertinentes à Prestadora de Serviços previstas neste Instrumento com relação ao Tratamento dos Dados Pessoais Relevantes;

(d) por solicitação e às custas da Cliente, apresentar a esta imediatamente toda a assistência técnica e institucional cabível que seja necessária para responder de forma adequada a solicitações feitas por Titular de Dados com relação ao exercício de seus direitos, assegurando ao titular dos dados o acesso facilitado as informações relacionadas ao Tratamento de Dados Pessoais de forma clara, adequada e ostensiva, garantindo que as informações sigam: (i) finalidade específica do Tratamento; (ii) forma e duração do Tratamento; (iii) identificação e contato do Controlador; e, (iv) uso compartilhado dos Dados Pessoais e sua respectiva finalidade (“Direito a Informação”).

(e) por solicitação e às custas da Cliente, apresentar a esta imediatamente toda a assistência cabível necessária para que a Cliente possa: (i) notificar violações relevantes da LGPD às respectivas Autoridades Supervisoras e/ou aos Titulares de Dados afetados; (ii) realizar Avaliações de Impacto na Proteção de Dados; e (iii) obter quaisquer autorizações necessárias da Autoridade Nacional;

(f) imediatamente na rescisão ou vencimento do Contrato de Prestação de Serviços, (i) solicitar instruções da Cliente quanto à possível exclusão ou devolução dos Dados Pessoais Relevantes; (ii) excluir ou devolver, de forma permanente e segura (conforme instruções da Cliente), todos os Dados Pessoais Relevantes que estejam na posse ou controle da Prestadora de Serviços ou de alguma de suas Suboperadoras, em 30 (trinta) dias da rescisão ou vencimento do Contrato de Prestação de Serviços, salvo por disposição contrária da legislação pertinente do Brasil e (iii) certificar-se de que suas Suboperadoras tomem as mesmas medidas;

(g) por solicitação e às custas da Cliente, apresentar imediatamente a esta todas as informações necessárias para que a Cliente possa comprovar o cumprimento de suas obrigações quanto à LGPD, na medida em que a Prestadora de Serviços possa prestar essas informações; e por solicitação da Cliente, permitir imediatamente e colaborar com auditorias, inclusive inspeções, realizadas pela Cliente ou auditor por ela indicado; e

(h) notificar a Cliente imediatamente e, em qualquer caso, em 24 (vinte e quatro) horas, do(a): (i) ciência de qualquer Violação a Dados Pessoais que afete os Dados Pessoais Relevantes; (ii) ciência de qualquer violação significativa a esta Cláusula 3; ou (iii) recebimento de qualquer correspondência ou comunicado de qualquer Titular de Dados, Autoridade Supervisora, terceiro, juiz, tribunal, órgão regulador ou governamental com jurisdição competente à qual a Prestadora de Serviços esteja sujeita, relacionadas ao Tratamento de Dados Pessoais Relevantes.

(i) cooperar totalmente com a Cliente para facilitar a investigação e a correção de uma Violação de Dados, incluindo, sem limitação, (i) a disponibilização de servidores à Cliente ou ao representante por ela designado; e (ii) preservar todas as informações e evidências relacionadas à Violação de Dados incluindo, entre outros, a suspensão de limpeza (*overwriting*) ou exclusão rotineiras de dados ou arquivos de *log*. A Prestadora de Serviços não deverá informar terceiros sobre qualquer Violação de Dados sem antes obter o consentimento por escrito da Cliente, exceto conforme estritamente exigido pela Legislação de Proteção de Dados ou por uma intimação, ordem judicial ou outro documento legal similar emitido judicialmente ou pela ANPD, hipóteses em

que a Prestadora de Serviços, exceto se proibido por lei, notificará a Cliente antes de informar quaisquer terceiros e cooperará com a Cliente na organização das informações divulgadas limitado ao exigido pela Legislação de Proteção de Dados. A Prestadora de Serviços deverá reembolsar à Cliente os custos incorridos pelo mesmo para responder, remediar e/ou mitigar os danos causados por uma Violação de Dados ou para acompanhar uma reclamação de um Titular de Dados ou regulador, que sejam decorrentes de, ou relacionados à, violação pela Prestadora de Serviços de suas obrigações decorrentes do Contrato de Prestação de Serviços, deste instrumento ou da legislação pertinente. A Prestadora de Serviços deverá tomar todas as medidas corretivas necessárias e apropriadas, inclusive conforme instruído pela Cliente ou pela Legislação de Proteção de Dados, para remediar ou mitigar qualquer Violação de Dados.

3.7 A Prestadora de Serviços continuará sendo a responsável principal pelos atos e omissões de seus Empregados, representantes e Suboperadoras. Todas as violações a esta Cláusula 3 por parte dos Empregados, representantes e Suboperadoras da Prestadora de Serviços serão consideradas atos da própria Prestadora de Serviços. Não há nada no presente Instrumento que desonere a Prestadora de Serviços de sua responsabilidade pelos atos ou omissões de seus Empregados, representantes e Suboperadoras com relação aos Dados Pessoais Relevantes.

3.8 A Prestadora de Serviços deverá, proteger e manter a Cliente e seus diretores, conselheiros e funcionários ilesos de e contra todas e quaisquer reclamações, custos, danos, multas, perdas, responsabilidades, despesas e honorários advocatícios (em conjunto, "Reclamações"), na medida em que tais Reclamações (inclusive de Titulares dos Dados, autoridades de proteção de dados ou outros órgãos reguladores) sejam causadas, decorram ou estejam relacionadas (i) a qualquer violação da Legislação Aplicável de proteção de dados pela Prestadora de Serviços ou (ii) ao uso dos Serviços, pela Cliente ou seus afiliados, nas condições estabelecidas no Contrato. Esta obrigação é passível de indenização e subsistirá à rescisão, encerramento ou expiração do Contrato por qualquer motivo.

3.9 Fica assegurado à Cliente, nos termos da lei, o direito de regresso em face da Prestadora de Serviços no caso de danos causados por esta em decorrência do descumprimento das obrigações aqui assumidas em relação a Proteção dos Dados. A responsabilidade da Prestadora de Serviços diante do referido descumprimento é ilimitada, não produzindo nenhum efeito qualquer outra cláusula que disponha de forma contrária.

3.10 A Prestadora de Serviços deverá levar em consideração os princípios de proteção de dados e privacidade desde a sua concepção (*by design*) e por padrão (*by default*) com relação às suas ferramentas, produtos, serviços, plataformas ou aplicativos associados aos Serviços.

#### **4. Prazo e rescisão**

4.1 O presente Instrumento entrará em vigência a partir da Data de Entrada em Vigor, rescindindo-se automaticamente por ocasião da rescisão ou vencimento do Contrato de Prestação de Serviços. Não obstante a rescisão deste Instrumento, de alguma das disposição deste ou do Contrato de Prestação de Serviços, as obrigações da Prestadora de Serviços previstas na Cláusula 3 e nesta Cláusula 4 permanecerão em pleno vigor e efeito por todo o período em que a Prestadora de Serviços continue a Tratar quaisquer Dados Pessoais Relevantes. Além disso, as obrigações da Prestadora de Serviços de manutenção de registros de suas atividades de Tratamento, estabelecidas neste Instrumento, continuarão em pleno vigor e efeito pelo período nele declarado.

4.2 A Cliente terá o direito de rescindir o presente Instrumento e o Contrato de Prestação de Serviços imediatamente, mediante notificação por escrito à Prestadora de Serviços, caso esta esteja em violação significativa ou persistente deste instrumento e tal violação não seja sanada

(se sua correção for possível) em 10 (dez) dias úteis após recebimento de notificação da Cliente referente a essa violação.

## **5. Notificações**

Qualquer notificação feita em relação ao Contrato deverá ser entregue por escrito e em mãos, ou enviada por serviço regular de correspondência ou e-mail, com aviso de recebimento, para o endereço de contato estabelecido no início deste documento, ou para outro endereço, número ou endereço de e-mail que o destinatário em questão tenha indicado. A notificação terá sua realização acusada quando o comunicado for efetivamente recebido pelo destinatário. Qualquer notificação enviada à Cliente deverá ser com cópia para Husqvarna do Brasil, A/C: Encarregado de Privacidade de Dados do Grupo, [privacidade@husqvarnagroup.com](mailto:privacidade@husqvarnagroup.com), Avenida Manuel Bandeira, n.º 291, Bloco B, 1º Pavimento, Conjuntos 22 e 23(A), Vila Leopoldina - São Paulo/SP - 05317-020.

## **6. Legislação Pertinente**

6.1 As Partes contratantes do presente Instrumento submetem-se à eleição de foro estipulada no Contrato de Prestação de Serviços com relação às controvérsias e ações oriundas deste instrumento. O presente Instrumento será regido e interpretado em consonância com a legislação brasileira para os fins do Contrato de Prestação de Serviços.

## **Anexo 1 – Atividades de Tratamento de Dados**

### **Escopo das atividade de Tratamento**

O cumprimento das obrigações da Prestadora de Serviços no Contrato de Prestação de Serviços envolverá as seguintes atividades de Tratamento, mas não se limitando a:

- atividades necessárias à prestação dos Serviços previstos no Contrato de Prestação de Serviços;
- relatórios estatísticos;
- correção e detecção de erros;
- melhorias e atualizações dos Serviços;
- serviços analíticos;

### **Duração do Tratamento**

O Tratamento dos Dados Pessoais Relevantes continuará por todo o prazo deste Instrumento e por outros períodos complementares permitidos expressamente ou obrigatórios: (i) neste Instrumento; ou (ii) na Legislação Pertinente.

### **Titulares de dados**

Os Dados Pessoais Relevantes referem-se às seguintes categorias de Titular de Dados:

- Empregados;
- Clientes (ou os Empregados desses clientes);
- fornecedores e subfornecedores (ou os Empregados desses fornecedores);
- revendedores, varejistas, representantes, corretores e outros parceiros de operação conjunta (ou os Empregados dessas partes);

### **Categorias de Dados Pessoais Relevantes**

Os Dados Pessoais Relevantes a seguir poderão ser Tratados pela Prestadora de Serviços:

- nome;
- data de nascimento;
- gênero;
- endereço de e-mail;
- número de telefone;
- vínculo empresarial;
- localização (somente o país);
- dados de *login*;
- endereço de IP;
- histórico de uso;
- metadados;

## **Atividades de Tratamento de Dados**

São as seguintes as Finalidades do Tratamento dos Dados Pessoais Relevantes:

- Possibilitar a identificação e contato com o Titular para fins deste Instrumento
- Possibilitar a elaboração de contratos, quando aprovados pelo Titular.
- Possibilitar o envio ou fornecimento ao Titular seus produtos e serviços, de forma remunerada ou gratuita.
- possibilitar a promoção de seus produtos e serviços dentro dos limites deste Instrumento
- realização de pesquisas com titulares
- validar a identidade dos titulares
- Monitorar e detectar o uso indevido dos serviços, objeto deste Instrumento
- Melhorar e otimizar os serviços prestados
- Cumprimento da legislação vigente

## **Contatos para questionamentos referentes à proteção de dados**

Cliente:

Husqvarna do Brasil  
A/C Encarregado de Privacidade de Dados do Grupo  
Avenida Manuel Bandeira, n.º 291, Bloco B, 1º Pavimento,  
Conjuntos 22 e 23(A), Vila Leopoldina  
São Paulo/SP  
05317-020.  
[privacidade@husqvarnagroup.com](mailto:privacidade@husqvarnagroup.com)

Prestadora de Serviços:

Dados constantes no contrato e ou/ pedido de compra.



## Anexo 2 – Medidas Técnicas e Institucionais de Segurança

### (A) Controle de acesso físico ao recinto

Medidas técnicas e institucionais para controlar o acesso físico ao recinto e às instalações, particularmente para identificar os Empregados autorizados na entrada:

Portas com trava em todas as entradas / saídas (ex.: travas eletrônicas; travas físicas etc.)

Presença de Empregados da segurança (ex.: segurança na área da recepção).

Sistemas de controle de acesso (ex.: segurança biométrica; segurança por cartão de acesso etc.)

Sistemas de CFTV

Sistemas de alarme contra invasão

Outras medidas físicas de segurança para proteger os sistemas de TI (ex.: sala de servidores particionada etc.)

### (B) Controle de acesso a sistemas de TI

Medidas técnicas e institucionais de segurança projetadas para garantir a identificação e autenticação daqueles usuários com acesso aos respectivos sistemas de TI:

Sistemas de segurança de TI que exijam dos usuários individuais o uso de nomes de usuário exclusivos

Sistemas de segurança de TI que exijam o uso de senhas fortes / complexas

Sistemas de segurança de TI que exijam o uso de autenticação multifatorial

Outras exigências de *login* no sistema de aplicativos específicos

Alterações de senha obrigatórias em intervalos fixos (ex.: a cada 6 meses)

Aplicação de criptografia de última geração em todos os dados “em trânsito”

Aplicação de criptografia de última geração em todos os dados “parados”

Travamento automático de terminais e dispositivos de TI após períodos sem uso, com obrigação de inserção de senhas para “despertar” o terminal ou dispositivo

Bancos de dados de senhas sujeitos a forte criptografia / *hashing*

Auditorias regulares de procedimentos de segurança (ex.: certificações da série ISO 27000)

Treinamento dos funcionários sobre o acesso a sistemas de TI

**(C) Controle de acesso a Dados Pessoais**

Medidas técnicas e institucionais de segurança projetadas para garantir a identificação e autenticação daqueles usuários com acesso aos Dados Pessoais Relevantes:

Restrição de direitos de “Leitura” em sistemas que contenham Dados Pessoais a funções especificadas entre os Empregados

Restrição de direitos de “Edição” em sistemas que contenham Dados Pessoais a funções ou perfis especificados entre os Empregados

Registro de todas as tentativas de acesso a sistemas que contenham Dados Pessoais (ex.: registro de endereços de IP e tentativas de combinação de senha e nome de usuário)

Criptografia de última geração em unidades e mídias que contenham Dados Pessoais (ex.: uso do Sophos SafeGuard; TrueCrypt etc.)

Pseudonimização segura dos dados

Treinamento dos funcionários sobre o acesso a Dados Pessoais

**(D) Controle de divulgação de Dados Pessoais**

Medidas técnicas e institucionais para transporte, transmissão e comunicação ou armazenamento de dados em mídias, bem como para verificação subsequente:

Restrições sobre direitos de transferência em sistemas que contenham Dados Pessoais

Redes de dados seguras (ex.: VPNs criptografadas)

Criptografia de última geração em todos os sistemas usados para envio de Dados Pessoais (ex.: e-mail criptografado; FTP criptografado etc.)

Registro de todas as transferências de dados em toda a rede

Criptografia de SSL para todos os portais de acesso à Internet

Proteção de mídias e recipientes de armazenamento de dados durante o transporte físico

Criptografia forçada de todas as unidades utilizadas para retirada dos dados da rede

Treinamento dos funcionários sobre transferências de Dados Pessoais

**(E) Controle de mecanismos de inserção**

Medidas técnicas e institucionais de segurança para permitir o registro e posterior análise de informações sobre a ocorrência de inserções nos sistemas de dados (ex.: edição, inclusão, exclusão etc.) e o responsável por elas, como:

Registros de todas as inserções em sistemas de contenham Dados Pessoais

Restrição de direitos de “Edição” em sistemas que contenham Dados Pessoais a funções especificadas entre os Empregados

Registro de todas as tentativas frustradas de edição de Dados Pessoais

Contratos vinculantes por escrito com todos os funcionários que Tratem Dados Pessoais e que lhes imponham obrigações de sigilo rigorosas

Revisões regulares do cumprimento dos contratos correspondentes

Treinamento dos funcionários sobre a edição de Dados Pessoais

**(F) Controle de fluxos de trabalho entre Controladoras e Operadoras**

Medidas técnicas e institucionais para segregação das responsabilidades entre Controladoras e Operadoras que Tratem os Dados Pessoais Relevantes como:

Contratos vinculantes por escrito que rejam a nomeação e as responsabilidades das Operadoras que tenham acesso aos Dados Pessoais Relevantes

Contratos vinculantes por escrito que rejam a alocação das responsabilidades de cumprimento da proteção de dados entre todas as Controladoras que tenham acesso aos Dados Pessoais Relevantes

Revisões regulares do cumprimento dos contratos correspondentes

Treinamento dos funcionários sobre o Tratamento de Dados Pessoais

**(G) Mecanismos de controle para garantir a disponibilidade dos Dados Pessoais Relevantes**

Medidas técnicas e institucionais para garantir a disponibilidade e acessibilidade física e eletrônica dos Dados Pessoais Relevantes, como:

Procedimentos documentados de recuperação de desastres  
Existência de procedimentos seguros de *backup*, com execução regular de *backups*  
Múltiplas instalações e locais de *backups*  
Alimentação elétrica interrompível nas instalações de *backups*  
Segurança física das instalações de *backups* (ex.: estabelecimento seguro; Empregados da área de segurança etc.).  
Sistemas de alarme de segurança nas instalações de *backups*  
Segurança eletrônica das instalações de *backups* (ex.: *firewalls*; software antivírus etc.)  
Controles ambientais nas instalações de *backups* (ex.: resfriamento; controles de umidade etc.)  
Proteção contra incêndio em instalações de *backups* (ex.: sistemas *sprinklers*; portas corta-fogo etc.)  
Anonimização ou exclusão seguras dos Dados Pessoais que já não sejam necessários para os fins do Tratamento legal  
Treinamento dos funcionários sobre *backups* e recuperação de desastres

**(H) Mecanismos de controle para garantir a separação entre os Dados Pessoais Relevantes e outros dados**

Medidas técnicas e institucionais para garantir que os Dados Pessoais Relevantes sejam armazenados e Tratados separadamente dos demais, como por exemplo, mas não se limitando a:

Separação lógica entre os dados reais ou de produção e os dados de *backup* e dos dados de desenvolvimento ou teste  
Separação lógica entre as unidades que contenham Dados Pessoais Relevantes e os sistemas com outros dados  
Separação entre os Empregados que Tratem os Dados Pessoais Relevantes e os outros Empregados  
Treinamento dos funcionários na separação de dados

**(I) Certificação**

Certificação e auditoria regular externa/interna de segurança para avaliar de forma objetiva as medidas de segurança.

---