



LEI GERAL DE PROTEÇÃO DE DADOS

ADEQUAÇÕES EMPRESA AGRIPARTS PEÇAS E IMPLEMENTOS LTDA.

DA POLÍTICA DE RESPOSTA A INCIDENTES

Esta postura tem o objetivo de preparar a empresa para lidar com a gestão de um incidente de segurança garantindo que responda de forma mais rápida, organizada e eficiente ao evento, minimizando suas consequências para todos os envolvidos. O nível da resposta dependerá do tipo de dados e da complexidade do tratamento aplicado.

Afinal, o que seria incidente? Segundo o dicionário, seria primeiramente que incide, sobrevém e ainda, tem caráter acessório, secundário; incidental, superveniente. Mas, forma ampla e geral, um incidente é uma situação inesperada, capaz de alterar a ordem normal das coisas e, no caso da proteção de dados, colocar em risco dados pessoais dos indivíduos que se relacionam com a empresa.

Ainda, segundo a Autoridade Nacional de Proteção de Dados, incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração vazamento ou qualquer forma de tratamento de dados ilícita ou irregular, que tem a capacidade de colocar em risco os direitos e as liberdades dos titulares dos dados pessoais.



https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_resposta_incidentes.pdf

O **National Institute of Standards and Technology, (NIST)**, (Instituto Nacional de Padrões e Tecnologia), anteriormente conhecido como *The National Bureau of Standards*, é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos), e define um incidente de segurança como uma violação ou ameaça de violação da política de segurança computacional, política de uso aceitável ou padrões de prática de segurança, de acordo com o artigo 46 da Lei Geral de Proteção de Dados (LGPD).

Também, obedecendo ao disposto no artigo 48 da referida Lei, é obrigação do controlador comunicar à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Devendo esta comunicação ser feita em prazo razoável, conforme definição da autoridade nacional, tendo em seu conteúdo, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos; A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata;



-As medidas que foram ou que estão sendo tomadas para reverter ou mitigar os efeitos do prejuízo.

E ainda, seguindo criteriosamente o site do Governo Federal e da Autoridade Nacional de Proteção de Dados, temos também os seguintes procedimentos:

PRIMEIRO PASSO EM CASO DE INCIDENTE DE SEGURANÇA

-Avaliar internamente o incidente – natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis. Vide formulário de avaliação constante do sítio eletrônico da ANPD;

* Comunicar ao encarregado da entidade a existência do incidente, caso envolva dados pessoais;

* Comunicar ao controlador (nos termos da LGPD) a existência do incidente, caso envolva dados pessoais;

* Comunicar à ANPD e ao titular de dados pessoais (conforme art. 48 da LGPD) a existência do incidente;

* Comunicar à ETIR (equipe de tratamento de incidentes cibernéticos internos de órgãos da administração pública federal (APF)) do órgão em caso de incidentes na rede computacional;

* Comunicar ao CTIR GOV (Centro de Tratamento a Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) tem o papel de coordenar e integrar as ações destinadas à gestão de incidentes de TI em órgãos e entidades da administração pública federal (APF). Os incidentes de segurança e de privacidade estão inclusos no escopo de ação do CTIR) caso a entidade faça parte da administração pública federal, ao realizar a confirmação de um evento de incidente, deve ser realizada a comunicação ao CTIR Gov, e se necessária, deve ser realizada ação conjunta entre a entidade e o CTIR Gov para a correspondente resolução.

- Emitir o relatório final com todas as informações coletadas, as ações realizadas para o tratamento efetivo do evento e as considerações necessárias para promover a melhoria contínua no atendimento de incidentes e para atualizar o RIPD.

Com base no exposto, a Política de Resposta da Agriparts, seguirá as etapas abaixo oferecidas pelo guia da ANPD.





https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_resposta_incidentes.pdf

DA LEGITIMIDADE PARA FAZER A COMUNICAÇÃO

DE INCIDENTES

O art. 48 da LGPD determina que será obrigação do controlador comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

É comum que os controladores adotem posição de cautela, de modo que a comunicação seja efetuada mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos. Ressalte-se, ainda, que eventual e comprovada subavaliação dos riscos e danos por parte dos controladores pode ser considerada descumprimento à legislação de proteção de dados pessoais.

Muito embora a responsabilidade e a obrigação pela comunicação à ANPD sejam do controlador, caso excepcionalmente sejam apresentadas informações pelo operador, serão devidamente analisadas pela ANPD.



**CASO OCORRA QUALQUER INCIDENTE, ABAIXO O CONTEÚDO
QUE SERÁ ENVIADO À AUTORIDADE NACIONAL DE PROTEÇÃO
DE DADOS**

As informações devem ser claras e concisas. Além do que prescreve o § 1º do artigo 48 da LGPD, recomenda-se que a comunicação contenha as seguintes informações, disponíveis no formulário de comunicação de incidentes de segurança com dados pessoais da ANPD:

***Identificação e dados:**

- Entidade ou pessoa responsável pelo tratamento.
- Encarregado de dados ou outra pessoa de contato.
- Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar.
- Informações sobre o incidente de segurança com dados pessoais:
- Data e hora da detecção.
- Data e hora do incidente e sua duração.
- Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros.
- Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados
- Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento.

Av. Dr. Vicente Salles Guimarães, nº 275, Bairro Alto Umuarama,

Uberlândia - MG, CEP- 38405-386.



- Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados.
- Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD.
- Resumo das medidas implementadas até o momento para controlar os possíveis danos.
- Possíveis problemas de natureza transfronteiriça.
- Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais serão fornecidas posteriormente.

No momento da comunicação preliminar será informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las. A ANPD também poderá requerer informações adicionais a qualquer momento.

**DA VERIFICAÇÃO E COMUNICAÇÃO AO TITULAR DOS DADOS,
SEMPRE QUE O INCIDENTE DE SEGURANÇA POSSA
ACARRETER UM RISCO OU DANO RELEVANTE AOS
TITULARES AFETADOS.**

Questões mais detalhadas será objeto de futura regulamentação e não poderão ser aqui exigidos sob pena de se inovar na LGPD. De tal sorte, pode-se extrair da lei que a

Av. Dr. Vicente Salles Guimarães, nº 275, Bairro Alto Umuarama,

Uberlândia - MG, CEP- 38405-386.



probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

O controlador avaliará internamente a relevância do risco ou dano do incidente de segurança para determinar se deverá comunicar à ANPD e ao titular. Para tanto, o portal da ANPD sugere que se responda internamente às seguintes perguntas, que adotaremos:

1. Ocorreu um incidente de segurança relacionado a dados pessoais?

☐ Sim – Próxima pergunta.

☐ Não – Não é necessário comunicar a ANPD se não houve incidente de segurança relacionado a dados pessoais.

2. Existe um risco ou dano relevante aos direitos e liberdades individuais dos titulares afetados em razão do incidente de segurança?

☐ Sim – Comunique à ANPD e ao titular.



☐ Não – A comunicação à ANPD não será necessária se o responsável pelo tratamento puder demonstrar, de forma irrefutável, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.

DO PRAZO PARA COMUNICARMOS UM INCIDENTE DE SEGURANÇA PARA A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS.

A LGPD determina que a comunicação do incidente de segurança seja feita em prazo razoável (art. 48, § 1º), e conforme regulamentação, conforme o Art. 6º e o Art. 9º da Resolução CD/ANPD nº 15, de 24 de abril de 2024 que Aprova o Regulamento de Comunicação de Incidente de Segurança, a comunicação à ANPD e ao(s) titular(es) deverá ser realizada pelo controlador no prazo de três (3) dias úteis contados da data do conhecimento do incidente, ressalvada a existência de prazo para comunicação previsto em legislação específica demonstrará transparência e boa-fé e será considerada em eventual fiscalização.

DA POLÍTICA DE RETENÇÃO E DESCARTE DE DADOS PESSOAIS

Política de retenção e descarte de dados pessoais da Agriparts Peças e Implementos Ltda., tem a responsabilidade de garantir o cumprimento à Lei Geral de Proteção de Dados Pessoais (LGPD) e seus requisitos relativos à coleta, armazenamento, recuperação e destruição de registros de dados pessoais e/ou dados sensíveis (“Dados Pessoais”). Esta política complementa, e não substitui a



Política Geral de Privacidade de Dados, como a “Política de Proteção de Dados Pessoais – Colaboradores” e as políticas de recrutamento.

A Agriparts Peças e Implementos Ltda. mantém conjuntos de Dados Pessoais armazenados em conformidade com requisitos contratuais, regulatórios e demais bases legais aplicáveis às modalidades de tratamentos de Dados Pessoais.

É importante que esses Registros sejam protegidos contra perda, destruição, falsificação, acesso não-autorizado e liberação não-autorizada. Para isso, uma variedade de controles é usada, como backups, controle de acesso e criptografia. Esse controle se aplica a todas as operações, pessoas e processos que constituem o sistema de informações da Agriparts Peças e Implementos Ltda., incluindo colaboradores, membros do conselho, diretores, fornecedores, clientes e terceiros que têm acesso aos dados tratados por nossa empresa.

DA CLASSIFICAÇÃO DE REGISTROS

A Agriparts Peças e Implementos Ltda. classificam os Registros em categorias que estabelecem os requisitos de retenção e de descarte para cada categoria.

Todos os Dados Pessoais serão retidos pelo tempo necessário ao cumprimento do objetivo que foram coletadas, com finalidades lícitas, específicas e informadas.

Há uma diversidade de tratamentos de Dados Pessoais cujo prazo de arquivamento não é determinado por lei, como, por



exemplo, o tempo de guarda dos Dados Pessoais de um prospecto comercial. Para tais dados, a Agriparts Peças e Implementos Ltda. estipula um prazo de guarda que seja coerente com as práticas de mercado e com a natureza do tratamento, enquanto não houver determinação específica pela autoridade reguladora.

Para demais Registros, incluindo aqueles de ordem tributária, trabalhista e previdenciária, a empresa se reserva o direito de mantê-los armazenados até o fim do prazo prescricional estipulado em lei.

DA RETENÇÃO E DESCARTE DE DADOS PESSOAIS

Para cada um dessas hipóteses, a tabela a seguir mostra o período máximo de retenção de Dados Pessoais por nossa empresa, por categoria de Registro, descrição, bem como o formato de descarte.

<u>TIPO DE DADO</u>	<u>DESCRIÇÃO</u>	<u>PERÍODO DE RETENÇÃO</u>	<u>FORMA DE DESCARTE</u>
Comercial	Prospecção Comercial (nome, RG, CPF, endereço, telefone, e-mail e whatsapp)	01 ano após contato inicial sem resposta ou prontamente, no caso de revogação do consentimento.	Eliminação pela empresa ou a qualquer tempo a pedido do titular.

Comercial	Contratos Prestação de Serviços de Fornecedores (Nome, CPF, e-mail).	05 anos a contar da data do término da relação comercial ou prontamente, em caso de exaurimento da finalidade.	Eliminação pela empresa
Comercial	Contratos Prestação de Serviços de Clientes (Nome, CPF, e-mail).	05 anos a contar da data do término da relação comercial ou prontamente, em caso de exaurimento da finalidade.	Eliminação pela empresa
Comunicação	Ações informativas ou de pesquisa, campanhas publicitárias ou promocionais	Indeterminado ou prontamente, em caso de exaurimento da finalidade ou revogação do	Eliminação pela empresa ou a qualquer tempo a pedido do

	(nome, e-mail, telefone).	consentimento.	titular
Comunicação	Fale conosco (nome, e-mail, telefone).	01 ano após contato inicial sem resposta ou prontamente, no caso de revogação do consentimento.	Eliminação pela empresa ou a qualquer tempo a pedido do titular
Fiscal	Documentos tributários.	05 anos a contar da data de emissão do documento.	Eliminação pela empresa
Trabalhista	Recrutamento e Seleção (Currículo).	01 mês após reprovação pré-entrevista, 90 dias após reprovação pós entrevista ou prontamente, no caso de revogação do consentimento.	Eliminação pela empresa ou a qualquer tempo a pedido do titular
	Telefone, e-e-	02 anos a	Eliminação



Trabalhista	email, dados bancários.	contar da data do término da relação empregatícia.	pela empresa
Trabalhista	Aviso prévio, pedido de demissão, TRCT, contribuições sindicais, aviso e recibo de férias, 13º salário, controle de frequência, CAGED, RAIS, dados de dependentes legais.	05 anos a contar da data do término da relação empregatícia.	Eliminação pela empresa
Trabalhista	Folha de pagamento, Contribuição Previdenciária – GPS.	10 anos a contar da data do término da relação empregatícia.	Eliminação pela empresa
Trabalhista	Fundo de Garantia por Tempo de	30 anos a contar da data do término da	



	Serviço – FGTS, Guia de Recolhimento do FGTS e Informações à Previdência Social – GFIP, Guia de Recolhimento Rescisório do FGTS e da Contribuição Social – GRFC	relação empregatícia	Eliminação pela empresa
Trabalhista	Termo de Compromisso de Estágio, atestado escolar.	05 anos a contar da data do término do contrato de estágio.	Eliminação pela empresa
Segurança	Informações de acesso aos sistemas da Digital Seller através de <i>login</i> e senha).	Durante o contrato de emprego.	Eliminação pela empresa

ELIMINAÇÃO PELA AGRIPARTS LTDA

Av. Dr. Vicente Salles Guimarães, nº 275, Bairro Alto Umuarama,
Uberlândia - MG, CEP- 38405-386.



Ao final do período de temporalidade de armazenamento e desde que não exista uma razão válida para a manutenção das informações, os dados pessoais mantidos em cópias físicas serão destruídos como resíduo confidencial e aqueles mantidos eletronicamente serão eliminados dos sistemas da empresa e de terceiros contratados.

Existência de processos judiciais ou administrativos ou mesmo investigações em andamento são motivos válidos para manutenção dos dados na base da empresa e, nesses casos, independente de consentimento, o período de armazenamento poderá ser prorrogado.

Caso a empresa tenha o interesse em estender o prazo de armazenamento e não se enquadrando o caso nos casos acima de excludente de consentimento, deverá notificar os titulares dos Dados Pessoais por escrito e com antecedência razoável da data de término do período de retenção, de forma a renovar o consentimento no tratamento.

Na hipótese do titular dos dados pessoais optar por exercer seu direito de eliminação dessas informações, seus dados pessoais deverão ser descartados prontamente pela empresa, excetuadas as hipóteses de cumprimento de obrigação legal ou regulatória.



POLÍTICA DE PRIVACIDADE

Sobre esta política de cookies

Esta Política de Cookies explica o que são cookies e como os usamos, os tipos de cookies que usamos, ou seja, as informações que coletamos usando cookies e como essas informações são usadas e como controlar as preferências de cookies. Para obter mais informações sobre como usamos, armazenamos e mantemos seus dados pessoais seguros, consulte nossa Política de Privacidade.

Você pode, a qualquer momento, alterar ou retirar seu consentimento da Declaração de Cookie em nosso site.

Saiba mais sobre quem somos, como você pode nos contatar e como processamos dados pessoais em nossa Política de Privacidade.

Seu consentimento se aplica aos seguintes domínios:
www.agripartsltda.com.br.

Seu estado atual: Não foi dado consentimento. Gerenciar consentimento.

O que são cookies?

Cookies são pequenos arquivos de texto usados para armazenar pequenas informações. Eles são armazenados em seu dispositivo quando o site é carregado em seu navegador. Esses cookies nos ajudam a fazer o site funcionar corretamente, torná-lo mais seguro, fornecer uma melhor experiência do usuário e entender

Av. Dr. Vicente Salles Guimarães, nº 275, Bairro Alto Umuarama,
Uberlândia - MG, CEP- 38405-386.



como o site funciona e analisar o que funciona e onde precisa ser melhorado.

Como usamos cookies?

Como a maioria dos serviços online, nosso site usa cookies primários e de terceiros para diversos fins. Os cookies primários são principalmente necessários para o funcionamento correto do site e não coletam nenhum de seus dados de identificação pessoal.

Os cookies de terceiros usados em nosso site são principalmente para entender como o site funciona, como você interage com nosso site, mantendo nossos serviços seguros, fornecendo anúncios que são relevantes para você e, em suma, proporcionando-lhe um usuário melhor e melhor experiência e ajuda a agilizar suas futuras interações com nosso site.

Que tipos de cookies usamos?

Essencial: Alguns cookies são essenciais para que você possa experimentar todas as funcionalidades do nosso site. Eles nos permitem manter as sessões do usuário e prevenir quaisquer ameaças à segurança. Eles não coletam ou armazenam nenhuma informação pessoal. Por exemplo, esses cookies permitem que você faça login em sua conta, adicione produtos à sua cesta e finalize a compra com segurança.

Estatísticas: Esses cookies armazenam informações como o número de visitantes do site, o número de visitantes únicos, quais páginas do site foram visitadas, a origem da visita, etc. Esses dados



nos ajudam a entender e analisar o desempenho do site e onde precisa de melhorias.

Como posso controlar as preferências de cookies?

Caso decida alterar suas preferências posteriormente durante a sessão de navegação, você pode clicar na guia “Política de Privacidade e Cookies” em sua tela. Isso exibirá o aviso de consentimento novamente, permitindo que você altere suas preferências ou retire totalmente o seu consentimento.

Além disso, diferentes navegadores fornecem métodos diferentes para bloquear e excluir cookies usados por sites. Você pode alterar as configurações do seu navegador para bloquear / excluir os cookies. Para saber mais sobre como gerenciar e excluir cookies, visite wikipedia.org, www.allaboutcookies.org.

Essa política está disponível tanto no sítio eletrônico da empresa, quanto entregue a todos aos colaboradores individualmente, através de protocolo e impresso na sede da empresa para livre acesso.

DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Todas as informações coletadas, acessadas, armazenadas, compartilhadas ou descartadas no exercício das atividades realizadas pelos colaboradores e parceiros, são de propriedade e direito de uso exclusivo da Agriparts Peças e Implementos Ltda, onde seus colaboradores e parceiros devem zelar para que as informações inseridas nos sistemas, ou quando enviadas ao cliente, sejam livres de erro, transparentes e inequívocas.

Av. Dr. Vicente Salles Guimarães, nº 275, Bairro Alto Umuarama,

Uberlândia - MG, CEP- 38405-386.



O acesso aos dados será sempre limitado à jornada de trabalho de cada colaborador e quaisquer documentos não poderão sair da empresa sem o registro no livro de protocolo, seja físico ou digital.

A equipe deve utilizar apenas os programas instalados e aprovados pelo operador, e jamais utilizar de programas estranhos e/ou pirateados, e ainda, toda vez que ele se afastar eventualmente da empresa na posse de aparelho remoto deverá bloquear o dispositivo.

Os programas de antivírus deverão ser atualizados semanalmente e todos os dados deverão ser salvos em rede ou na nuvem.

Qualquer suspeita de mal funcionamento ou mesmo tentativa de acesso por dispositivos estranhos ao sistema deverão ser reportados imediatamente ao controlador ou encarregado.

O uso do correio eletrônico da Agriparts Peças e Implementos Ltda. é estritamente para fins corporativos e relacionados às atividades do colaborador/parceiro dentro da organização, ficando terminantemente proibido o uso de correios eletrônicos particulares, a exemplo de Hotmail, Gmail ou outro, para o envio e recebimento de informações da empresa, parceiros e seus clientes.

Essa política está disponível tanto no sítio eletrônico da empresa, quanto entregue a todos aos colaboradores



individualmente, através de protocolo e impresso na sede da empresa para livre acesso.

DA POLÍTICA DE TRATAMENTO DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

Vamos a alguns esclarecimentos primeiramente:

Dados pessoais: São informações de pessoas naturais vivas que, direta ou indiretamente, identificam um indivíduo.

A informação direta é aquela que permite a imediata individualização da pessoa.

A informação indireta é a que permite por meio da reunião de informações, chegar à identificação do sujeito.

Para facilitar o entendimento vejamos os exemplos:

Identificação direta: um cliente, ao fazer uma compra online, informa seu nome completo e CPF, ou seja, a loja virtual com essas informações consegue identificar o indivíduo que realizou a compra.

Identificação indireta: uma empresa não cadastrou o nome completo ou o CPF de um cliente, a princípio, a companhia não teria como identificá-lo. Porém, utilizando outras informações que possui, é possível descobrir sua identidade. Tais como: profissão, endereço, gênero, ou qualquer outro dado que ajude a identificá-lo.



Em outras palavras, a identificação indireta ocorre quando associamos informações, que isoladamente não conseguem identificar um indivíduo, para descobrirmos a identidade de uma pessoa.

Dados pessoais sensíveis: São aqueles dados que podem causar discriminação a uma pessoa, por isso merecem maior proteção.

De acordo com a lei, dados sensíveis são aqueles envolvem:

Origem racial ou étnica;

Convicção religiosa;

Opinião política;

Filiação a sindicato ou a organização de caráter religioso;

Filosófico ou político;

Dado referente à saúde ou à vida sexual;

Dado genético ou biométrico, quando vinculado a uma pessoa natural.

Nossa empresa não coleta este tipo de dado para o exercício de suas atividades.

OBS. NESTE PONTO FICA REFORÇADO QUE NÃO EXISTE TRATAMENTO DE DADOS POR NOSSA EMPRESA, DE CRIANÇAS E ADOLESCENTES, ATÉ MESMO, POR CUMPRIR, EM NOSSO SEGUIMENTO O ARTIGO 104 D CÓDIGO CIVIL.

Art. 104. A validade do negócio jurídico requer:

Av. Dr. Vicente Salles Guimarães, nº 275, Bairro Alto Umuarama,
Uberlândia - MG, CEP- 38405-386.



I – agente, capaz:

II - objeto lícito, possível, determinado ou determinável;

III - forma prescrita ou não defesa em lei.

DA POLÍTICA DE ANONIMIZAÇÃO DE DADOS

Conceito: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Na forma do artigo 18 da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), o TITULAR de DADOS PESSOAIS, tem direito a obter do CONTROLADOR, em relação aos dados tratados, a qualquer momento e mediante requisição, a

d) ANONIMIZAÇÃO, BLOQUEIO ou ELIMINAÇÃO de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD ou nesta política;

Dentre outros.

Na hipótese em que o requerimento objetivar a correção, eliminação, anonimização ou bloqueio dos dados, caso estes tenham sido compartilhados com terceiro, o CONTROLADOR informará imediatamente o beneficiário do compartilhamento para que igualmente atenda à solicitação do titular.

As partes declaram ciência de que os dados fornecidos pelo titular, uma vez anonimizados, não são considerados DADOS



PESSOAIS, como estabelece o artigo 12 da Lei Geral de Proteção de Dados.

DA POLÍTICA DE TRANSFERÊNCIA/COMPARTILHAMENTO

DE DADOS PESSOAIS

Conceito de “uso compartilhado de dados pessoais”: Conforme a LGPD, o uso compartilhado pode ser entendido como as situações em que os dados pessoais são comunicados, difundidos, transferidos internacionalmente ou interconectados.

Caso o controlador precise comunicar ou compartilhar dados pessoais com terceiros, deve obter consentimento expresso do titular para esse fim, exceto em situações já previstas em lei que dispensam tal autorização. É importante que o pedido de consentimento seja visível e deixe explícito para o titular a finalidade da transferência de dados.

Existem algumas situações em que o consentimento é dispensado – uma dessas hipóteses é quando os dados tratados já foram tornados públicos pelo titular.

Caso a necessidade ocorra, será disponibilizada esta uma aba no sítio eletrônico, conforme apresentada abaixo, para que possamos buscar o consentimento o titular ao mesmo tempo seguindo à risca a letra da lei.



TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

Este documento visa registrar a manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus dados pessoais para finalidade específica, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Ao clicar em aceite o presente termo, o Titular consente e concorda que a empresa Agriparts Peças e Implementos Ltda., inscrita no CNPJ sob o número - CNPJ: 07.898.362/0001-90, através de seu administrador **LEONARDO TADEU MARTELLETO DENIPOTI**, doravante denominado Controlador, tome decisões referentes ao tratamento de seus dados pessoais, bem como realize o tratamento de seus dados pessoais, envolvendo operações como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Dados Pessoais

O Controlador fica autorizado a tomar decisões referentes ao tratamento e a realizar o tratamento dos seguintes dados pessoais do Titular:

Nome completo.

Sexo

Av. Dr. Vicente Salles Guimarães, nº 275, Bairro Alto Umuarama,
Uberlândia - MG, CEP- 38405-386.



Data de nascimento.

Profissão

Estado civil.

Endereço completo.

Números de telefone, WhatsApp e endereços de e-mail.

Finalidades do Tratamento dos Dados

O tratamento dos dados pessoais listados neste termo tem as seguintes finalidades:

- Possibilitar que o Controlador identifique e entre em contato com o Titular para fins de relacionamento comercial.
- Possibilitar que o Controlador elabore contratos comerciais e emita cobranças contra o Titular.
- Possibilitar que o Controlador envie ou forneça ao Titular seus produtos e serviços, de forma remunerada ou gratuita.
- Possibilitar que o Controlador estruture, teste, promova e faça propaganda de produtos e serviços, personalizados ou não ao perfil do Titular.

Compartilhamento de Dados

O Controlador fica autorizado a compartilhar os dados pessoais do Titular com outros agentes de tratamento de dados, caso seja necessário para as finalidades listadas neste termo, observados os princípios e as garantias estabelecidas pela Lei nº 13.709.

Segurança dos Dados

O Controlador responsabiliza-se pela manutenção de medidas de segurança, técnicas e administrativas aptas a proteger os

Av. Dr. Vicente Salles Guimarães, nº 275, Bairro Alto Umuarama,

Uberlândia - MG, CEP- 38405-386.



dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Em conformidade ao art. 48 da Lei nº 13.709, o Controlador comunicará ao Titular e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao Titular.

Término do Tratamento dos Dados

O Controlador poderá manter e tratar os dados pessoais do Titular durante todo o período em que os mesmos forem pertinentes ao alcance das finalidades da atividade da empresa.

Os Dados pessoais anonimizados, sem possibilidade de associação ao indivíduo, poderão ser mantidos por período indefinido.

O Titular poderá solicitar via e-mail ou correspondência ao Controlador, a qualquer momento, que sejam eliminados os dados pessoais não anonimizados do Titular. O Titular fica ciente de que poderá ser inviável ao Controlador continuar o fornecimento de produtos ou serviços ao Titular a partir da eliminação dos dados pessoais.

Direitos do Titular

O Titular tem direito a obter do Controlador, em relação aos dados por ele tratados, a qualquer momento e mediante

Av. Dr. Vicente Salles Guimarães, nº 275, Bairro Alto Umuarama,

Uberlândia - MG, CEP- 38405-386.



requisição: I – confirmação da existência de tratamento; II – acesso aos dados; III – correção de dados incompletos, inexatos ou desatualizados; IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei nº 13.709; V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei nº 13.709; VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX – revogação do consentimento, nos termos do § 5º do art. 8º da Lei nº 13.709.

Direito de Revogação do Consentimento

Este consentimento poderá ser revogado pelo Titular, a qualquer momento, mediante solicitação via e-mail ou correspondência ao Controlador.



DA POLÍTICA DE BACKUP

O controlador e o responsável do setor de tecnologia da informação já criaram e sempre atualizam as determinações/parâmetros, e realizando todos os procedimentos específicos, conforme as características das informações, dos sistemas e das ferramentas de geração de backup, devendo considerar os seguintes pilares:

I- O armazenamento seguro, adequado e eficaz em instalações locais e remotas das mídias;

II- Aplicação de criptografia e restrição de acesso ao material armazenado;

III- O traslado seguro das informações que terão armazenamento remoto;

IV- O descarte seguro de mídias e ferramentas de geração de backups obsoletos, depreciados e danificados, considerando a eliminação definitiva de seu conteúdo e, quando necessário, a destruição do suporte físico.

Além das outras medidas de proteção, que são:

*Controle de acesso restrito aos administradores;

*Criptografia dos dados em repouso (AES-256);

*Criptografia no tráfego dos dados (HTTPS / TLS 1.3);



- *Prevenção e detecção de intrusão;
- *Firewall de proteção para o Sistema de Gestão que monitora filtra e bloqueia tentativas de ataque; e Backup em real time;
- *Política de senha e autenticação de múltiplo fator.

DA POLÍTICA PARA ARQUIVAMENTO, RETENÇÃO E EXCLUSÃO DE HISTÓRICOS

A Agriparts Peças e Implementos Ltda., reforça a importância de se armazenar todas as informações coletadas, que possibilita buscar um norte mais confiável nas análises de mercado e observa dois requisitos praticamente para arquivar e reter informações, o primeiro a data do dado, por se tratar de cliente/titular antigo e fiel,(comercialmente falando), o segundo, para relevância dos dados, é a data do último acesso.

As informações que ultrapassam muitos anos são descartadas conforme tabela de descarte na tabela de categorias especificada acima.

O armazenamento adotado pela empresa é o híbrido, se efetiva tanto no dispositivo físico da empresa quanto em nuvem.