ÍNDICE

OBJETIVO

Garantir a conformidade dos processos de negócios em relação ao tratamento de dados e dados pessoais por fornecedores, parceiros e terceirizados em relação às normas internas Gerdau e regulações de proteção e privacidade de dados pessoais.

ABRANGÊNCIA

Aplica-se a todas as Áreas Corporativas e Industriais em todos prestadores de serviço, fornecedores e parceiros que utilizam, mantêm ou lidam com ativos de informação da Gerdau.

DEFINIÇÕES

Dado ou Dados: Qualquer elemento relacionado a uma informação ou ainda um conjunto de informações relacionado a um tema, um registro ou um fato, quer seja de forma estruturada ou não.

Dados Confidenciais ou Sensíveis: Informações sigilosas que podem gerar prejuízos ou impactos financeiros, legais e jurídicos se divulgadas inapropriadamente fora da organização ou por pessoas não autorizadas.

Dado Pessoal: informação relacionada à pessoa natural identificada ou identificável, tais como nome completo, data de nascimento, documentos pessoais (CPF, RG, CNH, CTPS, passaporte e título de eleitor), endereço residencial, e-mail ou endereço IP.

Dado Pessoal Sensível: Dado pessoal sobre 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**.**

Dado Anonimizado: Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Pessoa Natural: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Também conhecida como Pessoa Física**.**

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Anonimização: 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.

Tratamento de dados pessoais: É toda a operação realizada com dados pessoais, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados.

Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado ou DPO: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Autoridade Nacional de Proteção de Dados – ANPD: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

REFERÊNCIAS

- Diretriz Corporativa DC-15-A
- Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)

ASPECTOS GERAIS

Este documento descreve **as regras internas da Gerdau** para tratamento de Dados, Dados Pessoais e Dados Pessoais Sensíveis relacionados a colaboradores, clientes, fornecedores e terceiros, armazenados em sistemas de informação de propriedade da Gerdau, Tratados ou Processados por terceiros a serviço ou também prestando serviços a Gerdau.

ESCOPO E RESPONSABILIDADES

O escopo desta Política é padronizar o tratamento de dados pessoais realizados por seus Parceiros, Fornecedores e Terceirizados, fornecendo diretrizes para que eles atuem em acordo com o que dispõe as normas internas da Gerdau e as Legislações vigentes de tratamento de dados pessoais nos Países onde a Gerdau atua.

SEÇÕES E NORMAS

O Encarregado e sua função na Gerdau

A função de Encarregado de Proteção de dados é exercida por um executivo Gerdau nomeado como DPO, com o apoio de um comitê interno, formado por representantes das áreas de Segurança da Informação, Jurídico e Compliance, o qual pode ser contatado pelo endereço eletrônico dpo@gerdau.com.br

Proteção e Privacidade de Dados

Todos Fornecedores, Parceiros e Terceirizados se comprometem e tem o dever de zelar pela Proteção e Privacidade de dados da Gerdau, como também reportar incidentes ou suspeitas relacionadas a exposição indevida ou vazamentos de dados confidenciais incluindo dados pessoais de colaboradores, outros fornecedores, parceiros e/ou clientes.

É proibido o envio, armazenamento, compartilhamento de dados privados e/ou confidenciais da Gerdau em dispositivos pessoais, serviços de armazenamento, aplicativo de mensagem instantânea e compartilhamentos em nuvem vinculados a contas pessoais, bem como a divulgação de quaisquer dados dessa natureza em comentários ou notas em websites e blogs externos.

É proibido criar rotinas de trabalho que envolvam tratamento de dados, internos, privados e/ou confidenciais da Gerdau fora dos sistemas e ambientes de tecnologia oficiais da Gerdau sem a avaliação e aprovação da área de segurança da informação da Gerdau e também a aprovação do executivo responsável pelo processo, projeto e atividades atribuídos a esses Terceiros.

Princípios para tratamento de dados Pessoais

A Gerdau reconhece que a boa-fé no tratamento de dados pessoais é premissa básica e que seus parceiros e fornecedores seguem os princípios para tratamento de dados pessoais em conformidade com a LGPD, portanto todos Dados Pessoais e Pessoais Sensíveis devem ser tratados dentro dos princípios da lei listados abaixo:

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Bases legais para tratamento de dados Pessoais

No papel de Controlador, somente se realizará o tratamento de dados de forma adequada, dentro de uma das bases legais listadas abaixo:

Consentimento: mediante o fornecimento de consentimento pelo titular.

Obrigação legal: para o cumprimento de obrigação legal ou regulatória pelo controlador.

Contrato: quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Proteção a vida: para a proteção da vida ou da incolumidade física do titular ou de terceiros.

Tutela da saúde: para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Legítimo interesse: Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Processo judicial: para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Dados de acesso público: Tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Da propriedade dos Dados Pessoais tratados

Os Dados Pessoais sempre serão de propriedade do Titular, nunca dos agentes de tratamento, o que inclui a Gerdau e seus colaboradores e prestadores de serviço.

Compartilhamento de Dados Pessoais com terceiros

O compartilhamento de Dados Pessoais e Pessoais sensíveis com terceiros é autorizado somente quando previsto em um contrato de prestação de serviço, termo de confidencialidade (NDA) ou documento similar do terceiro que receberá os Dados Pessoais.

Recebimento de Dados Pessoais de terceiros

O recebimento de dados pessoais de outras empresas ou terceiros é autorizado somente quando existe um contrato de prestação de serviço ativo, entre a Gerdau e o terceiro.

O tratamento de Dados Pessoais Sensíveis

O tratamento de Dados Pessoais Sensíveis requer uma maior proteção do que os demais Dados Pessoais e por isso o tratamento deve ocorrer, sempre que for possível, com o fornecimento de consentimento expresso pelo titular. Todo tratamento de Dados Pessoais Sensíveis que não for possível coletar o consentimento, deve se enquadrar à umas das bases legais descritas no capítulo 3.2 dessa norma.

É proibido armazenar nos dispositivos de trabalho ou dispositivos pessoais (celular) mensagens instantâneas), assim como em serviços de armazenamento vinculado à conta pessoa e aplicativo de mensagem instantânea, Dados Pessoais Sensíveis, tais como, fotografias, imagens de biometria, dados médicos (atestado de saúde, exames) entre outros.

Tratamento de Dados Pessoais desnecessários ou abusivos

Todo tratamento de Dados Pessoais deverá ter uma finalidade, e os dados a serem tratados deverão ser apenas os necessários para esta finalidade.

Procedimentos no caso de encerramento de contrato de prestação de serviços ou parceria com a Gerdau

Quando um contrato prestação de serviços, parceria ou outro instrumento que regule sua relação com a Gerdau for encerrado, a pessoa física ou jurídica que tem acesso à Dados Pessoais e teve a relação com a Gerdau encerrada, não poderá compartilhar ou realizar uma cópia dessas informações. Caso tenha em sua posse Dados Pessoais que obteve da Gerdau, deverá reuni-los e devolvê-los, ou ainda, seguir as orientações da Gerdau para eliminação ou anonimização deles.

Ocorrências relativas aos Dados Pessoais

Qualquer ocorrência que possa ser associada a um descumprimento da LGPD com os Dados Pessoais da qual tiver conhecimento, tais como, mas sem limite, vazamento, destruição, perda, alteração ou comunicação indevida, deve ser comunicada imediatamente ao DPO, assim como qualquer intimação ou solicitação de autoridade que receba em sua área ou departamento.

Cumprimento e uso adequado de ferramentas de segurança

As regras estabelecidas na presente Política não dispensam o colaborador de cumprimento das regras estabelecidas na Diretriz Corporativa de Segurança da Informação DC-15A da Gerdau.

Todos devem manter os Dados Pessoais, a que tiverem acesso, seguros e íntegros, mediante a adoção de práticas, sistemas e ferramentas disponibilizados pelos times de Tecnologia e de Segurança da Informação.

Uso de dados de Criança

É proibido o tratamento de Dados Pessoais de menores de 12 (doze) anos, exceto no caso de cumprimento de lei ou regulamento.

Da concessão de acesso aos sistemas informáticos que contenham Dados Pessoais

O acesso a Dados Pessoais deve ser protegido contra acesso não autorizado. As regras para concessão de acesso a dados pessoais seguem as disposições descritas na Diretriz Corporativa de Segurança da Informação 15-A, seção 3.6 - Norma de Gestão de Acessos e Identidades.

CASOS OMISSOS

Todo assunto não previsto neste documento deve ser encaminhado para aprovação, ao gestor do contrato, área de suprimentos e/ou área Global de Segurança da Informação.

Orientações Gerais

Todas as transações realizadas pelas empresas parcerias e/ou fornecedores devem:

- Respeitar os princípios do Código de Ética e Conduta da Gerdau, bem como dos profissionais e sociedades com as quais a Gerdau se relaciona.
- Cumprir as determinações de Legislação e Órgãos Reguladores pertinentes ao negócio.
- Atender aos requisitos ambientais, de saúde e segurança do trabalho e suas respectivas legislações vigentes.
- Em caso de dúvidas ou necessidade de informação adicional, deve-se procurar orientação com as seguintes instâncias:
    - Gestor da Área ou Gestor da Unidade responsável pelo Contrato
    - Área de Segurança da Informação ou de Tecnologia e Digital

DocuSigned by:
Vitor de Gusmao Sena
C5930C20D278412...

VITOR DE GUSMAO SENA
CISO GERDAU
GERENTE GERAL DE SEGURANÇA DA INFORMAÇÃO