

TÍTULO: POLÍTICA DE TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

1. OBJETIVO

Este documento estabelece as diretrizes, escopo, papéis e responsabilidades para assegurar a conformidade no tratamento de dados pessoais sensíveis, inclusive na obtenção do consentimento, quando necessário, de forma específica, destacada e para finalidades específicas do titular de dados pessoais ou de seu representante legal para o tratamento dos dados pessoais sensíveis sob responsabilidade do Grupo ArcelorMittal Brasil.

2. REFERÊNCIA /COMPLEMENTAÇÃO

As diretrizes desta Política são decorrentes da Política de Proteção de Dados Pessoais bem como do Procedimento sobre Proteção de Dados e o seu detalhamento realizado por meio das práticas padrão específicas, disponíveis na intranet corporativa da ArcelorMittal Brasil.

3. APLICAÇÃO

Esta Política é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação aos colaboradores envolvidos no tratamento de Dados Pessoais sensíveis, seja o tratamento realizado por meio de sistemas de TI ou de qualquer outra maneira, incluindo o uso de sistemas terceiros ou registros em papel.

4. PUBLICAÇÃO

Esta Política deve ser publicada forma a abranger todas as Unidades Organizacionais do Grupo ArcelorMittal Brasil.

5. FREQUÊNCIA

Essa prática deve ser aplicada sempre que houver necessidade de realizar o tratamento de dados pessoais sensíveis a partir da obtenção do consentimento do titular de dados pessoais ou de seu responsável legal.

6. VIGÊNCIA

Esta prática será considerada oficialmente em vigor a partir da data da sua publicação.

7. SIGLAS/SÍMBOLOS

- **DPO** – Data Protection Officer (Encarregado de Proteção de Dados)
- **DPIA ou RIPD** - relatório de impacto à proteção de dados pessoais



ArcelorMittal

- **OneTrust** – Plataforma de Gerenciamento de Governança em Privacidade e Proteção de Dados Pessoais
- **Gerências GRC:** área de Governança, Riscos e Compliance dos segmentos (Longos, Planos, Arames, Finanças/TI), além das áreas Jurídico, Suprimentos, Auditoria Interna, Forensic.

8. DEFINIÇÕES

Ameaças – São eventos ou agentes que podem apresentar riscos aos recursos de informação da Companhia, por meio da exploração de vulnerabilidades.

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

Confidencialidade – Garantia de que a informação é acessível apenas para pessoas ou processos devidamente autorizados.

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

Dado Pessoal – Informação relacionada a pessoa natural identificada ou identificável.

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.

Disponibilidade – Garantia de que usuários ou processos devidamente autorizados tenham acesso à informação e aos recursos associados sempre que forem requisitados.

Incidente de Segurança – É toda ocorrência, imprevista e indesejável, que pode causar danos a qualquer recurso de informação.

Integridade – Garantia quanto à exatidão da informação, sem quebras e sem alterações não autorizadas, e dos respectivos métodos de processamento. Refere-se à confiabilidade.

Recursos da informação – Todo elemento que manuseia ou guarda informação.

Risco – Caracteriza-se como a probabilidade de uma ameaça explorar uma vulnerabilidade em um recurso de informação.

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

Tratamento – toda operação realizada com dados pessoais, como as que se referem 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.

Segurança da Informação – É definida como a proteção contra a perda da confidencialidade, integridade e disponibilidade da informação.

Terceiro – Pessoa Física ou jurídica que presta serviços através de instrumento de contrato, para atender as necessidades operacionais e administrativas da Companhia.

Usuário – Pessoa autorizada e capacitada para utilizar os recursos de informação da Companhia

9. RESPONSABILIDADES

Departamento de TI

- Assegurar que os recursos de T.I. relacionados a esta Política estejam disponíveis.
- Prestar suporte às Áreas de Negócio na utilização dos recursos de T.I. relacionados a presente Política.
- Aprovar os locais de armazenamento dos dados pessoais sensíveis.
- Auxiliar as Áreas de Negócio na identificação dos ativos tangíveis e intangíveis, quanto ao inventário de dados pessoais sensíveis armazenadas, seja em computadores, servidores, unidades de rede.
- Assegurar que os controles de segurança de T.I. relacionados a esta Política estejam implementados.

Encarregado pelo Tratamento de Dados Pessoais – DPO

- Prover e coordenar os esforços necessários para atingir os objetivos da presente Política.
- Reportar a implementação de diretrizes, ações e procedimentos, visando a aderência à presente Política ao Comitê de Privacidade e Proteção de Dados.
- Promover a divulgação da presente Política, bem como treinamento e cultura da informação.
- Prestar suporte às Áreas de Negócio na adequação dos processos relacionados a presente Política.
- Aprovar os relatórios de impacto à proteção de dados pessoais – DPIA dos processos de negócio que envolvam o tratamento de dados pessoais sensíveis.



ArcelorMittal

- Assegurar que os usuários com acesso aos dados pessoais sensíveis ou aos sistemas que suportam estejam cientes sobre a aplicação de leis, políticas, normas e regulamentos aplicáveis.

Áreas de Negócio

- Revisar os usuários com permissões de acesso aos dados pessoais sensíveis ou aos sistemas de informações que suportam e remover as pessoas que não precisam mais de acesso.
- Prover e coordenar os esforços necessários de seus colaboradores para atingir os objetivos da presente Política.
- Garantir que o mapeamento dos tratamentos de dados pessoais sensíveis de sua área esteja sempre atualizado

Gerências GRC – Governança, Riscos e Compliance

- Realizar o registro dos fluxos no OneTrust que envolvem dados pessoais sensíveis das áreas que estejam em seu escopo de atuação.
- Prover e coordenar os esforços necessários de seus colaboradores para atingir os objetivos da presente Política.
- Manter atualizado o mapeamento dos tratamentos de dados pessoais sensíveis.
- Executar o relatório de impacto à proteção de dados pessoais – DPIA dos processos de negócio que envolvam o tratamento de dados pessoais sensíveis.
- Realizar o monitoramento regulatório quanto à exigência de padrões técnicos mínimos que garantam a proteção e segurança de dados pessoais sensíveis.

Departamento Jurídico

- Apoiar as Áreas de Negócio e o Encarregado pelo Tratamento de Dados Pessoais - DPO no processo mapeado de conformidade legal das atividades de tratamento dos dados pessoais sensíveis.

Colaboradores

- Conhecer e cumprir todas as diretrizes desta Norma Política e instruções de trabalho relacionadas.
- Assegurar que os dados pessoais sensíveis sejam tratados apenas para necessidades comerciais legítimas ou conforme exigido por lei.
- Estar ciente das leis, políticas, normas e regulamentos aos quais os dados pessoais sensíveis estão sujeitos.
- Os dados pessoais sensíveis são tratados por meio de recursos aprovados pelo Departamento de TI.

- Efetuar a classificação dos dados pessoais sensíveis como “Acesso Restrito”.
- Executar revisões para reclassificar os dados pessoais sensíveis, conforme necessário.
- Notificar imediatamente o Encarregado pelo Tratamento de Dados Pessoais - DPO caso identifique qualquer violação no tratamento de dados pessoais sob sua responsabilidade ou não.

10. PROCEDIMENTOS

10.1. Diretrizes Gerais

Os dados pessoais sensíveis devem ser tratados somente para finalidades comerciais legítimas ou por conta de exigência legal, sempre alinhado aos princípios gerais estabelecidos em lei.

Quando constatado o tratamento de dados pessoais sensíveis, o Colaborador deve verificar a hipótese legal de tratamento indicada juntamente com o Departamento Jurídico de forma a proceder com o tratamento adequado dos dados pessoais sensíveis.

As hipóteses legais de tratamento de dados pessoais sensíveis, conforme ordenamento jurídico brasileiro vigente são:

- I. Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- II. Sem o fornecimento de consentimento, quando for indispensável para:
 - a) Cumprimento de obrigação legal ou regulatória pelo Controlador;
 - b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
 - c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
 - d) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
 - e) Proteção da vida ou da incolumidade física do titular ou de terceiros;
 - f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
 - g) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

A ArcelorMittal Brasil deve assegurar que os usuários com acesso aos dados pessoais sensíveis ou aos sistemas que suportam eles estejam cientes das leis, políticas, normas e regulamentos aplicáveis.

Os dados pessoais sensíveis devem ser classificados como “Acesso Restrito”.

10.2. Coleta dos Dados Pessoais Sensíveis

Os dados pessoais sensíveis devem ser coletados diretamente do indivíduo em questão ou através do seu responsável legal, nos termos da Política e do Procedimento de Proteção de Dados Pessoais da ArcelorMittal Brasil.

10.3. Consentimento

Nos fluxos mapeados no OneTrust que a base legal para o tratamento for o consentimento, será necessário obter o consentimento do titular dos dados pessoais para realizar o tratamento pretendido.

O Colaborador responsável pelo processo de negócio deverá obter, previamente ao tratamento pretendido, o consentimento de forma específica e destacada do titular ou de seu responsável legal, de acordo com o formulário que se encontra no <ANEXO I>.

Quando se tratar de base legada, o consentimento nos moldes da LGPD deverá ser obtido, ainda que posteriormente, para que possa se dar continuidade ao tratamento. Caso o titular dos dados recuse em fornecer o seu consentimento, o tratamento deverá ser cessado.

Os colaboradores da ArcelorMittal Brasil, responsáveis pelos fluxos de dados sensíveis, devem arquivar os formulários ou o log do sistema autorizando o tratamento de dados pessoais sensíveis durante o período previsto na Tabela de Temporalidade de cada área.

A ArcelorMittal Brasil deve implementar mecanismos para verificar se o consentimento coletado para o tratamento de dados pessoais sensíveis foi fornecido pelo titular ou pelo seu responsável legal.

É vedado o tratamento dos dados pessoais sensíveis mediante vício de consentimento, ou seja, quando o titular foi induzido em erro, não pretendia dar o consentimento ou foi enganado, a ArcelorMittal Brasil não poderá tratar seus dados, como por exemplo na hipótese em que o titular receber inúmeras informações sobre o tratamento de seus dados em sistema virtual e ao final da página o check de verificação e consentimento estiver pré-marcado, não permitindo que o titular marque por conta própria o campo.

A **ArcelorMittal Brasil** deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais sensíveis de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

10.4. Armazenamento

Os dados pessoais sensíveis devem estar armazenados apenas nos locais aprovados pela ArcelorMittal Brasil, sempre que possível no menor número de locais possíveis e que eventuais cópias e/ou duplicações sejam realizadas somente em casos extremamente necessários.

Os dados pessoais sensíveis armazenados nos diretórios de rede devem possuir controle de acesso, permitindo somente usuários autorizados a acessarem tais diretórios.

Os dados pessoais sensíveis não devem ser copiados para dispositivos externos sem a aplicação de controles criptográficos, a exemplo de pendrives, celulares, CDs, DVDs ou quaisquer outros dispositivos móveis que possam ser comprometidos.

10.5. Transmissão

As transmissões de dados pessoais sensíveis devem ocorrer somente por meios que assegurem um canal seguro de transmissão, a exemplo, mas não limitado à:

- I. Protocolos de criptografia na transmissão de arquivos por sistemas;
- II. Protocolos de criptografia na configuração na utilização de protocolos de transferência de arquivos.

Deve ser observada as diretrizes e disposições da Procedimento de Controles Criptográficos da ArcelorMittal, que conta com outros procedimentos necessários para a transmissão.

Em casos de extrema necessidade, quando não for possível realizar a transmissão dos dados pessoais sensíveis por outro meio, sendo necessária troca de dados pessoais sensíveis por e-mail, o Colaborador deve:

- Realizar a criptografia dos arquivos e enviar o arquivo contendo os dados pessoais sensíveis criptografado mediante tecnologia de criptografia assimétrica;
- Realizar o envio da chave privada por sistema seguro de envio, preferencialmente não o próprio e-mail.

10.6. Acesso/Uso dos Dados



ArcelorMittal

As áreas de negócio, com o suporte do Departamento de TI, devem assegurar que somente usuários com os devidos acessos e permissões para tratamento de dados pessoais sensíveis tenham acesso e façam uso de tais dados, mediante a criação de restrições por usuário das aplicações internas.

A Área de Negócio deve realizar uma **revisão trimestral** dos usuários com permissões de acesso aos dados pessoais sensíveis ou aos sistemas de Informações que suportam e remover as pessoas que não precisam mais de acesso.

10.7. Mapeamento de Atividades de Processamento de Dados Pessoais Sensíveis

A ArcelorMittal Brasil deve manter atualizado registro de todas as atividades de tratamento de dados pessoais sensíveis, contendo, no mínimo:

- a) Unidade da ArcelorMittal Brasil na qual ocorre o tratamento;
- b) O departamento responsável pela atividade de tratamento (processo de negócio);
- c) O nome da atividade de tratamento, com identificador único (ID);
- d) A classificação do titular de dados pessoais envolvidos no tratamento (por exemplo, empregado, cliente, terceiro, fornecedor, etc.);
- e) A finalidade do tratamento;
- f) A hipótese legal utilizada no tratamento;
- g) Se houver, o registro do consentimento do titular;
- h) Tempo de retenção do dado pessoal sensível tratado.

10.8. Exigências Legais

A ArcelorMittal Brasil, no tratamento de dados pessoais sensíveis, deve considerar a elaboração do Relatório de impacto à proteção de dados pessoais - DPIA, avaliando o risco aos direitos e liberdades fundamentais do titular de dados pessoais.

A ArcelorMittal Brasil deve realizar monitoramento regulatório, como por exemplo através de áreas de auditoria interna, compliance e riscos, quanto à exigência de padrões técnicos mínimos que garantam a proteção e segurança de dados pessoais sensíveis.

Os dados pessoais sensíveis devem ser descartados assim que atingida a finalidade do tratamento, somente sendo permitido o armazenamento dos dados conforme disposto na tabela de temporalidade da ArcelorMittal Brasil. Em caso de descarte, deve ser consultado o procedimento específico para descarte da ArcelorMittal Brasil.

11. PENALIDADES



ArcelorMittal

Nos casos em que houver violação desta Política, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento, rescisão contratual e eventuais processos cíveis e/ou criminais, quando aplicáveis.

A tentativa ou o efetivo descumprimento das diretrizes aqui estabelecidas, quando constatada, deve ser tratada como uma violação.

Anexo I – Formulário de consentimento para o tratamento de dados pessoais sensíveis

ANEXO I - TERMO DE CONSENTIMENTO PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Controlador dos dados pessoais: [Qualificação da Unidade da Arcelor], inscrito no CNPJ/MF sob o n.º[xxx.xxx.xxx/xxxx-xx], com sede [endereço];

Titular dos dados pessoais: [Qualificação do titular do dado pessoal: Nome, documento de identificação]

O Controlador dos dados pessoais apresenta a você, titular dos dados pessoais, as informações sobre como os seus dados pessoais sensíveis serão tratados.

Tratamento de Dados Pessoais Sensíveis. O Controlador dos dados pessoais irá realizar a coleta dos dados pessoais sensíveis que você irá fornecer por meio do <<indicar o canal de coleta dos dados pessoais>>, para as seguintes finalidades:

- i. <<informar especificamente todas as finalidades para o devido tratamento>>;
- ii.

Controlador dos dados pessoais pode realizar o tratamento dos meus dados pessoais sensíveis abaixo:

- i. <<informar especificamente quais dados sensíveis estão sendo tratados>>;

Compartilhamento. O Controlador dos dados pessoais fica autorizado a fazer o uso compartilhado dos meus dados pessoais sensíveis com outros Agentes de Tratamento, caso seja necessário para as finalidades descritas neste Termo, observados os princípios e garantias estabelecidos pela Lei Geral de Proteção de Dados Pessoais e outras legislações aplicáveis ao caso.



ArcelorMittal

Confidencialidade. O Controlador dos dados pessoais tem o compromisso de tratar os seus dados pessoais sensíveis com sigilo, mantendo-os em ambiente seguro e não sendo utilizados para qualquer fim que não os descritos acima.

Armazenamento dos dados. Os seus dados pessoais sensíveis poderão ser armazenados, mesmo após o término do tratamento, para (i) cumprimento de obrigação legal ou regulatória pelo Controlador dos dados pessoais.

Canais de atendimento. Você pode utilizar o canal “Fale Conosco” através do link <https://www.arcelormittal.com.br/fale-conosco> disponibilizado pelo Controlador dos dados pessoais para tirar dúvidas ou realizar as requisições relacionadas ao tratamento de seus dados pessoais.

Revogação. Tenho conhecimento de que, a qualquer tempo, posso revogar o meu consentimento ora fornecido.

Após ler e compreender as informações acima, autorizo o Controlador dos dados pessoais a realizar o tratamento de meus dados pessoais sensíveis estabelecidos no presente documento, declarando que sou capaz e respondo por meus atos ou sou o responsável legal do titular, investido de poderes de representação conforme as leis brasileiras.

Local, Data

Titular de Dados Pessoais