POLÍTICA DE PRIVACIDADE E DE GESTÃO DE TRATAMENTO DE DADOS PESSOAIS DA MITSUBISHI ELETRIC DO BRASIL COMÉRCIO E SERVIÇOS LTDA PARA PARCEIROS E FORNECEDORES

I. OBJETIVOS

A Mitsubishi Electric do Brasil Comércio e Serviços Ltda. ("MITSUBISHI") está empenhada em conduzir suas atividades em conformidade com as leis aplicáveis e padrões internacionais, visando proteger a privacidade dos dados pessoais a fim de que os dados e as informações sejam utilizados de forma e para a finalidade correta e mantidos em segurança. Esta Política de Privacidade e de Gestão de Tratamento de Dados Pessoais da MITSUBISHI para Parceiros e Fornecedores ("Política") tem por objetivo orientar e informar aos seus parceiros e fornecedores o escopo e a extensão do Tratamento de Dados Pessoais.

A gestão do Tratamento de Dados Pessoais deverá ser pautada e regida pelos conceitos, princípios, regras e padrões fornecidos e determinados por esta Política, pelas normas brasileiras e estrangeiras, pela Lei Geral de Proteção de Dados ("LGPD"), Marco Civil da Internet ("Marco Civil") e melhores práticas globais, desde sua concepção, e durante todo o seu ciclo de vida, até que seja eliminado.

É prioridade da MITSUBISHI garantir a privacidade e proteção de dados pessoais, prezando por atender e respeitar todos os princípios e normas brasileiras e estrangeiras que regulam esses direitos, bem como assegurar que seus clientes, colaboradores, fornecedores, prestadores de serviços também estejam em conformidade com tais normas, sendo obrigação de todos, portanto, o respeito e o comprometimento com esta Política.

II. ABRANGÊNCIA

Esta Política aplica-se a todos que de alguma forma poderão, em razão de eventual vínculo, associação, contrato, parceria, dentre outros com a MITSUBISHI, incluindo, mas não se limitando a revendedores, fornecedores, prestadores de serviço e parceiros no geral, efetuar tratamento de dados pessoais, assim entendidos como qualquer informação relacionada à pessoa física identificada ou identificável.

III. DEFINIÇÕES

Para os fins desta Política, os termos definidos abaixo devem ser considerados:

a) Titular do Dado Pessoal: pessoa física cujos Dados Pessoais são objeto do Tratamento;

b) Dado Pessoal: qualquer informação relacionada a uma pessoa física identificada ou identificável, portanto, todo aquele dado que identifique uma pessoa física, ou que, através da junção de dados, possa a vir identificar uma pessoa física, por exemplo, nome, RG, CPF, número de passaporte, localização, endereço, e-mail, telefone, dados de acesso à internet, etc. Neste conceito estão incluídos os Dados Pessoais Sensíveis;

c) Dado Pessoal Sensível: é uma categoria especial de dado pessoal, em razão do seu potencial discriminatório. São eles: Origem racial ou étnica; Opiniões políticas; Convicção

religiosa; Filiação a sindicato ou a organização de caráter religioso, filosófico ou político; Dado referente à saúde ou à vida sexual; Dados biométricos e Dados genéticos;

d) Dado Anonimizado: é aquele em que o titular não pode ser identificado, considerando os meios técnicos utilizados no momento do Tratamento. Dados Anonimizados não são considerados Dados Pessoais;

e) Tratamento: corresponde a toda atividade realizada com Dados Pessoais, desde a sua coleta ou acesso até a sua eliminação;

f) Terceiros: todas as partes que de alguma forma se vinculem à MITSUBISHI, incluindo, mas não se limitando a fornecedores, prestadores de serviços, parceiros, revendedores e demais terceiros que tenham acesso a informações da MITSUBISHI, sistemas de informação ou pelos quais passem dados pessoais;

g) Agentes de Tratamento: Controlador: consiste no agente a quem compete as decisões referentes ao Tratamento de Dados Pessoais; e Operador: é o agente que realiza o Tratamento de Dados Pessoais em nome do controlador;

h) Autoridade Nacional de Proteção de Dados ("ANPD"): o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados;

i) Transferência Internacional de Dados Pessoais: consiste na transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

j) Segurança da Informação: proteção de um conjunto de informações, no sentido de preservar a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações;

k) Incidente de Segurança: violação efetiva ou ameaça de violação na segurança de Dados Pessoais ou informações confidenciais envolvendo a divulgação, perda, vazamento ou tratamento indevido pelos Terceiros, seus subcontratados, ou quaisquer outras partes, que tenha resultado ou que provavelmente resultará em furto/roubo, perda acidental, quaisquer danos aos titulares, acesso não autorizado ou aquisição de Dados Pessoais ou informações confidenciais.

l) Terceiros: todos que de alguma forma poderão, em razão de eventual vínculo, associação, contrato, parceria, dentre outros com a MITSUBISHI, incluindo, mas não se limitando a revendedores, fornecedores, prestadores de serviço e parceiros no geral.

IV. DIRETRIZES E PROCEDIMENTOS:

4.1. DO TRATAMENTO DE DADOS PESSOAIS

Em caso de Tratamento de Dados Pessoais, os Terceiros deverão garantir a observância integral desta Política e da Legislação por todos os seus funcionários, representantes e/ou terceiros eventualmente envolvidos no Tratamento de Dados Pessoais e, ainda, se comprometem a:

a) Realizar o tratamento dos Dados Pessoais exclusivamente para os fins do cumprimento do contrato/parceria com a MITSUBISHI;

b) Sempre que instruído pela MITSUBISHI, corrigir, anonimizar e/ou eliminar de forma permanente quaisquer Dados Pessoais no prazo indicado pela MITSUBISHI;

c) Comunicar à MITSUBISHI em até 24 horas (ou em prazo menor, se a lei assim exigir), pelo e-mail dpo@mitsubishielectric.com.br e por telefone, toda e qualquer ocorrência de Incidente de Segurança envolvendo os Dados Pessoais, sendo que a comunicação conterá ao menos as seguintes informações, sempre que possível determiná-las: (i) a data e a causa; (ii) a descrição da natureza dos Dados Pessoais afetados (iii) as informações sobre os titulares envolvidos; (iv) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; (v) riscos e consequências relacionados ao incidente; e (vi) as medidas que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Além dos acima citados, todos os processos e procedimentos envolvendo eventual Tratamento de Dado Pessoal realizado por Terceiros deverão garantir e observar os critérios abaixo elencados.

4.2. DOS PRINCÍPIOS DO TRATAMENTO DE DADOS

Os Terceiros deverão observar, para toda e qualquer atividade que envolve Tratamento de Dados Pessoais, a boa-fé e os princípios legais do Tratamento, em especial, a finalidade, adequação e necessidade, além dos seguintes princípios:

- Minimização: se limitar a utilizar dados mínimos necessários para a realização de suas finalidades;
- Finalidade: para que o tratamento de dados seja legítimo, deverá informar ao Titular para quais finalidades específicas será realizado o Tratamento de seus dados;
- Adequação: o tratamento deve ser compatível com a finalidade informada ao Titular;
- Necessidade: o tratamento apenas poderá ser realizado quando necessário para a realização das finalidades;
- Livre Acesso: o Titular deverá sempre poder, de forma facilitada e gratuita, consultar o Terceiro a respeito da forma e da duração do Tratamento de seus Dados Pessoais;
- Qualidade dos Dados: os dados pessoais armazenados devem ser mantidos atualizados, claros e exatos;
- Transparência: todas as informações sobre a forma de tratamento dos dados pessoais devem ser claras, precisas e de fácil acesso. O Titular deve saber quais e para qual finalidade os dados pessoais estão sendo tratados pelo Terceiro;
- Segurança: o Terceiro deve sempre estar atento e tomar todas as medidas técnicas e administrativas de segurança de informação aptas a proteger os dados pessoais de acesso e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Prevenção: devem ser adotadas medidas de forma a prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais, tais como auditorias periódicas, treinamentos etc.;
- Não discriminação: impossibilidade de realização de tratamento de dados para fins discriminatórios;

- Responsabilização e Prestação de Contas: deve ser demonstrada a adoção de medidas eficazes e capazes de comprovar a observância e cumprimento de normas de proteção de dados pessoais e eficácia dessas medidas.

4.3. DAS HIPÓTESES PARA O TRATAMENTO DE DADOS PESSOAIS:

A Lei Geral de Proteção de Dados traz, como regra geral, dez hipóteses legais para que o Tratamento de Dados Pessoais seja lícito, regular e válido, ou seja, ao realizar tratamento de dados pessoais, deve-se observar se esse tratamento está dentro dessas dez hipóteses legais, caso negativo, o tratamento não será considerado lícito.

As dez hipóteses de tratamento são:

- Fornecimento de Consentimento: quando o Titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades determinadas;
- Cumprimento de Obrigação Legal: quando for necessário tratar dados pessoais em virtude de uma obrigação legal ou regulatória;
- Execução de Políticas Públicas e Estudos por Órgão de Pesquisa: essas duas hipóteses são consideradas para fins de interesse da administração ou fins de pesquisa;
- Execução de Contrato/Diligência Pré-Contratuais: o tratamento ocorre para assegurar o cumprimento da execução contratual ou de diligências pré-contratuais;
- Exercício regular de direito: quando o tratamento for necessário para um exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da Vida do Titular: se o tratamento for indispensável para a proteção da vida ou da incolumidade física;
- Tutela da Saúde: se o tratamento for realizado com a finalidade de promover procedimento por profissionais da área da saúde por entidades sanitárias, um interesse público relevante que deve ser justificado;
- Interesse Legítimo: em algumas situações, em caráter de exceção, o Terceiro pode valer-se do interesse legítimo para tratar dados pessoais, como apoio e promoção de atividades do controlador e proteção, em relação ao Titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem;
- Proteção ao crédito: a inclusão dos dados pessoais dos consumidores nos cadastros positivos poderá ser efetivada independentemente do consentimento expresso do Titular.

4.3.1. DO TRATAMENTO DE DADOS SENSÍVEIS:

Em regra, o Terceiro não deverá tratar dados pessoais sensíveis. Em alguns casos, e, somente quando estritamente necessário, o Terceiro, enquanto Controlador ou Operador de dados pessoais, pode vir a tratar dados pessoais sensíveis. Nesse caso, a Lei limita as hipóteses de tratamento ao seguinte:

- Fornecimento de Consentimento: quando o Titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades determinadas;
- Cumprimento de Obrigação Legal: quando for necessário tratar dados pessoais em virtude de uma obrigação legal ou regulatória;
- Execução de Políticas Públicas e Estudos por Órgão de Pesquisa: essas duas hipóteses são consideradas para fins de interesse da administração ou fins de pesquisa;

- Exercício regular de direito: quando o tratamento for necessário para um exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da Vida do Titular: se o tratamento for indispensável para a proteção da vida ou da incolumidade física;
- Tutela da Saúde: se o tratamento for realizado com a finalidade de promover procedimento por profissionais da área da saúde por entidades sanitárias, um interesse público relevante que deve ser justificado;
- Garantia da Prevenção à fraude e à segurança do titular: os processos de identificação e a autenticação de cadastro em sistemas eletrônicos são permitidos independentemente de consentimento, exceto no caso de prevalecerem direitos e liberdades fundamentais que exijam a proteção dos Dados Pessoais.

4.3.2. DO TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES:

Os Terceiros também poderão tratar dados de criança e adolescentes. O Tratamento demanda sempre o Consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal do menor.

4.4. DOS DIREITOS DO TITULARES:

Os Terceiros deverão garantir os direitos dos Titulares, quais sejam:

- Confirmação da existência de Tratamento e Acesso aos Dados Pessoais: o Titular poderá solicitar que o Terceiro declare se trata seus dados pessoais. Este direito tem relação com o princípio de livre acesso, ou seja, a garantia que o Titular pode de forma gratuita e facilitada consultar a respeito da forma e duração do Tratamento de seus Dados Pessoais, bem como da integridade de seus dados;
- Portabilidade dos Dados a outro fornecedor de serviço ou produto: o titular dos dados pessoais pode querer receber os dados pessoais que lhe digam respeito e que tenha fornecido ao Terceiro para que possa transmiti-los a outro responsável pelo Tratamento sem que a MITSUBISHI possa impedi-lo;
- Informação das entidades com as quais o controlador realizou uso compartilhado de dados: o titular poderá solicitar ao Terceiro que esta forneça as informações relativas ao compartilhamento de seus dados pessoais com entidades terceiras;
- Correção de dados incompletos: o Titular poderá solicitar ao Terceiro que corrija ou complemente os seus dados pessoais;
- Informação sobre a possibilidade de não fornecer consentimento: o Titular tem o direito de receber a informação a respeito da possibilidade de não fornecer o consentimento quando for realizado um tratamento de dados pessoais;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados ilicitamente: em virtude dos princípios de adequação e necessidade, o Titular poderá solicitar ao Terceiro, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados ilicitamente. Na medida do tecnicamente possível, o Terceiro anonimizará os dados pessoais dos seus Titulares e primará pela minimização de dados pessoais tratados;
- Revogação do consentimento: o Titular poderá a qualquer momento solicitar a revogação do consentimento dado ao Terceiro para o tratamento de seus dados;
- Reclamação a ANPD: o Titular poderá realizar uma reclamação juntamente à ANPD por violações ocasionais pelo Terceiro;

- Eliminação dos Dados Pessoais: o Titular poderá solicitar a eliminação de seus dados pessoais tratados pelo Terceiro. Em situações de obrigação legal ou regulatória, estes dados poderão ser retidos/armazenados;
- Oposição ao Tratamento, se irregular: o Titular poderá se opor ao Tratamento de seus Dados Pessoais, se constatado que o Tratamento é irregular.

4.5. COLETA DE DADOS PESSOAIS:

4.5.1. Toda e qualquer coleta de Dados Pessoais por Terceiros deve limitar-se ao requisito mínimo para fins lícitos, identificados e específicos, devendo os Titulares, sempre que a Lei requisitar, serem informados do uso e suas finalidades. Ainda que tornados públicos, os dados pessoais a que tiverem acesso os Terceiros não poderão ser utilizados para finalidade diversa do cumprimento do contrato entre o Terceiro e a MITSUBISHI e desta Política.

4.5.2. Os Terceiros não poderão repassar a outros a responsabilidade sobre o Tratamento de Dados Pessoais que sejam fornecidos pela MITSUBISHI, tratados em nome desta ou em razão do contrato com a MITSUBISHI, sem a autorização da MITSUBISHI, sendo que ainda que autorizado o repasse, o Terceiro deverá assegurar o cumprimento de todas as condições previstas nesta Política e na Legislação, permanecendo o Terceiro integralmente responsável por qualquer omissão ou falha no cumprimento de qualquer condição. Incluem-se, nesta regra, quaisquer subcontratados dos Terceiros.

4.6. USO, DIVULGAÇÃO, TRANSFERÊNCIA E RETENÇÃO DOS DADOS PESSOAIS:

4.6.1 Os Dados Pessoais tratados não devem ser utilizados ou divulgados para terceiros para fins diversos daqueles para os quais foram coletados, exceto com o consentimento do titular ou conforme exigido por lei. Toda e qualquer transferência deve ficar registrada, sendo responsabilidade do Terceiro conhecer o ciclo de vida do Dado Pessoal.

4.6.2 Os Dados Pessoais podem ser transferidos internacionalmente desde que tal transferência não descumpra a finalidade e esta Política e desde que: (i) o receptor possuir um grau de proteção de dados pessoais igual ou superior ao Brasil e; (ii) haja garantia de cumprimento das proteções ora previstas.

4.6.3. Qualquer transferência internacional de Dados Pessoais deve ser feita com a autorização prévia da MITSUBISHI, por escrito, e ainda que autorizada, o Terceiro deverá observar estritamente esta Política e a Legislação sobre o tema.

4.6.4 Os Dados Pessoais não devem ser retidos por mais tempo do que o necessário. Assim, o período de retenção dos Dados Pessoais varia de acordo com a finalidade pela qual o dado é utilizado. Dessa forma, a retenção deve ser apenas pela duração necessária para cumprir os fins identificados ou conforme obrigações legais e regulatórias que obrigam a retenção dos dados.

4.6.5 Após a expiração da finalidade ou a retirada do consentimento, o Terceiro deve apagar ou anonimizar os dados pessoais dos titulares.

4.6.6. Os Terceiros não cederão, doarão, venderão, alugarão, nem negociarão ou repassarão, de qualquer forma, a outras empresas ou terceiros, os Dados Pessoais a que tiver acesso durante ou em razão do contrato com a MITSUBISHI.

4.7. SEGURANÇA DA INFORMAÇÃO:

Os Terceiros devem garantir a segurança e a proteção dos Dados Pessoais objetos de Tratamento, levando em consideração a proteção contra:

- Perda ou roubo;
- Acesso, uso, divulgação ou transferência não autorizada; e
- Alteração de dados não autorizada.

4.7.1. Caso seja registrada qualquer queixa, reclamação e/ou informação pelos Titulares dos dados, a MITSUBISHI deve ser notificada em até 24 horas (ou em prazo menor, se a lei assim exigir) no e-mail dpo@mitsubishielectric.com.br e por telefone, e eventual resposta e comunicado ao Titular deve ser validada previamente pela MITSUBISHI.

4.7.2. Os Terceiros deverão treinar seus funcionários em questões de privacidade e sobre o cumprimento dessa Política e garantir que quaisquer subcontratados que terão acesso aos Dados Pessoais, utilizarão referidas informações nos limites desta Política. Os Terceiros garantem que tais subcontratados estão vinculados a estas obrigações por acordos escritos, que exigem a proteção dos Dados Pessoais, de forma tão protetiva quanto exigida nesta Política. Os subcontratados são quaisquer terceiros que processem Dados Pessoais e cujos serviços sejam utilizados pelos Terceiros em conexão com os serviços ou parceria com a MITSUBISHI.

4.7.3. Os Terceiros implementaram e deverão garantir que seus subcontratados implementem, determinados procedimentos e políticas para a confidencialidade, privacidade, segurança, recuperação em caso de desastre e proteção de Dados Pessoais (coletivamente "Políticas de Segurança"), a fim de garantir a conformidade constante dos Terceiros com todas as leis, normas e regulamentos aplicáveis sobre a proteção de Dados Pessoais, sejam federais, estaduais e/ou locais. Os Terceiros deverão manter – e deverão garantir que os seus subcontratados mantenham – a conformidade com as Políticas de Segurança durante todo o período de tratamento de Dados Pessoais.

4.7.4 As Políticas de Segurança do Terceiros deverão levar em consideração, no mínimo, os tópicos mencionados no Anexo I desta Política.

4.7.5. Os Dados Pessoais e informações confidenciais devem ser tratados em consistência com os termos desta Política, do contrato ou acordo de confidencialidade com a MITSUBISHI e leis aplicáveis, não devendo ser postados, exibidos ou colocados à disposição em uma rede ou plataformas não segura.

4.7.6. Os Terceiros indenizarão, defenderão e isentarão a MITSUBISHI de quaisquer Reclamações originárias de ou relativas a quaisquer violações desta Política pelos Terceiros ou por quaisquer de seus subcontratados, bem como quaisquer limitações de responsabilidade ou outras exclusões de danos previstas em contrato com respeito às Reclamações não serão aplicáveis para o propósito de Incidentes de Segurança.

4.7.7. Os Terceiros deverão notificar a MITUSBISHI prontamente, e em qualquer hipótese, no prazo máximo de até 24 horas, no e-mail dpo@mitsubishielectric.com.br e por telefone, no caso de os Terceiros tomarem ciência de violação efetiva ou ameaça de violação na segurança de Dados Pessoais ou informações confidenciais envolvendo a divulgação, perda, vazamento ou

tratamento indevido pelos Terceiros, seus subcontratados, ou quaisquer outras partes, que tenha resultado ou que provavelmente resultará em furto/roubo, perda acidental, quaisquer danos aos titulares, acesso não autorizado ou aquisição de Dados Pessoais ou informações confidenciais, (ou seja, um Incidente de Segurança). Os Terceiros deverão prontamente investigar e informar a MITSUBISHI sobre a data e causa de um Incidente de Segurança, e deverão providenciar todas as informações relevantes à MITSUBISHI, nos termos da cláusula 4.1. c desta Política. Os Terceiros deverão cooperar integralmente – e deverão garantir que seus subcontratados cooperem – com a MITSUBISHI, às custas dos Terceiros, para investigar e remediar qualquer Incidente de Segurança envolvendo os Dados Pessoais. Os Terceiros e a MITSUBISHI acordarão mutuamente sobre as medidas de mitigação necessárias a serem adotadas pelos Terceiros. Os Terceiros deverão reembolsar a MITSUBISHI por todos os custos, multas e indenizações efetivos incorridos pela MITSUBISHI na resposta e mitigação de danos causados por um Incidente de Segurança causado por si ou seus Subcontratados, incluindo os custos de notificações e remediação.

V. CONSIDERAÇÕES FINAIS:

Qualquer dúvida ou questionamento em relação a esta Política devem ser encaminhados ao e-mail dpo@mitsubishielectric.com.br para resolução.

Barueri, SP, 23 de Julho de 2021.

* * *

Anexo I
Segurança da Informação

Os Terceiros deverão implantar Políticas de Segurança da informação, as quais deverão ser seguidas por todos os seus funcionários, representantes e subcontratados, e deverão, minimamente, conter procedimentos para garantir o seguinte:

a) impressão, armazenamento, manuseio e destruição/descarte seguros de documentos confidenciais e dados pessoais, sejam eletrônicos ou físicos;

b) controles de segurança nos sistemas de informação, para evitar acessos não autorizados e invasões;

c) planos de gestão de incidentes de informação;

d) gestão segura de controles de acesso, com revisões periódicas e restrições de acesso somente a pessoas que o necessitam, seja nos documentos físicos ou eletrônicos;

e) sigilo de informações confidenciais e dados pessoais;

f) compartilhamento seguro de informações, seja via e-mail, telefone, ou outros meios;

g) segurança no uso da internet e aplicações;

h) segurança no uso das estações de trabalho, redes internas e mídias de armazenamento;

i) classificação de informações.

* * *