MANUAL DE INSTRUÇÃO DO TRATAMENTO DE DADOS PESSOAIS E SENSÍVEIS

MAPFRE

ÍNDICE:

Este manual regula os requisitos técnicos, procedimentos e obrigações de segurança e confidencialidade para o tratamento dos dados pessoais e sensíveis de clientes e terceiros das empresas do Grupo MAPFRE no Brasil.

1. APLICABILIDADE

Esse manual se aplica obrigatoriamente aos contratos firmados entre o Grupo MAPFRE e o OPERADOR de dados pessoais. Nos contratos firmados com outro CONTROLADOR de dados, a aplicação deste manual terá efeito de Diretriz para as atividades de tratamento. O Grupo MAPFRE figura como CONTROLADOR de dados pessoais no presente manual.

2. DEFINIÇÕES:

Os termos indicados com iniciais maiúsculas usado no presente instrumento terão os significados indicados neste item (2. Definições), salvo outra forma expressamente definida, bem como os termos definidos no singular ou plural, que terão o mesmo significado na forma descrita neste item (2. Definições).

DADO PESSOAL: Informação relacionada à pessoa natural identificada ou identificável, na forma descrita pela LGPD;

DIRETRIZ: São orientações, guias, rumos ou linhas que definem e regulam um traçado ou um caminho a seguir.

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

INFORMAÇÃO: Consiste em qualquer dado pessoal em qualquer meio, incluindo mas não se limitando à base de dados, documento(s) físico(s), eletrônico(s), magnético(s), digital(is) finalizado(s) ou em desenvolvimento, recurso(s) de informática, informação(es) comercial(is), financeira(s), estatística(s), jurídica(s), técnica(s), relacionada(s) ao(s) negócio(s) ou ao(s) empregado(s) do Grupo MAPFRE; bem como as informação(ões) relacionada(s) à segurança de tecnologia da informação: domínios, mídias, processos, políticas, procedimentos, medidas, recursos de segurança e, em geral, qualquer conhecimento ou comunicação transmitida verbalmente;

INFORMAÇÃO SENSÍVEL: Consiste em informação(es) de Dados Pessoais referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, relativa à saúde ou à vida sexual, dado genético ou biométrico, bem como àquelas Informações que, ainda que sejam públicas, foram classificadas como sendo de uso interno;

LGPD: Lei Geral de Proteção de Dados Pessoais, nº 13.709/2018;

OPERADOR: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador;

3. CONFIDENCIALIDADE:

Toda(s) a(s) informação(es), sensível(is) ou não, disponibilizada(s) pelo Grupo MAPFRE, acessada(s) ou encontrada(s) nas instalações do Grupo MAPFRE, deve(m) ser mantida(s) no mais absoluto e estrito sigilo, mesmo após o término da relação entre as partes, tendo este sigilo como validade o período de 5 (cinco) anos contados a partir do término da relação contratual. Nenhuma informação(es), sensível(is) ou não, poderá(rão) ser extraídas ou transmitidas de qualquer forma ou meio (eletrônico, mecânico, fotocópia, gravação ou outro meio) das instalações do Grupo MAPFRE, salvo se houver autorização expressa para praticá-los, de modo que se reconhece o dever de confidencialidade das informações e as obrigações relacionadas ao tratamento das informação(es), sensível(is) ou não.

4. FINALIDADE:

A(s) informação(es), sensível(is) ou não, deverá(rão) ser tratadas exclusivamente para a finalidade que constitui o objeto dos serviços contratados e, em nenhuma hipótese, poder(ão) ser utilizada(s) em atividade(s) diversa(s) ou para interesse próprio.

5. TRANSFERÊNCIA INTERNACIONAL DE DADOS:

A(s) informação(es), sensível(is) ou não, não poderá(ão) ser transferida(s) para um país terceiro ou organização internacional, sem autorização prévia e expressa do Grupo MAPFRE para fazê-lo. Para que haja a autorização do Grupo MAPFRE para a transferência internacional de dados, deverá(ão) ser informado(s) e identificado(s) o país terceiro ou a organização internacional, bem como deverá(ão) haver as garantias de segurança apropriadas, através de documentação, além de ser informado o local onde as informações, sensíveis ou não, serão armazenadas.

6. REGISTRO DAS ATIVIDADES E AVALIAÇÃO DE IMPACTO SOBRE A(S) INFORMAÇÃO(ES) E/OU INFORMAÇÃO(ES) SENSÍVEL(IS):

Deverá ser mantido o registro das operações realizadas com a(s) informação(es), sensível(is) ou não, compartilhada(s) em decorrência do contrato entre as partes, bem como, deverá ser realizado e mantido o relatório de impacto à proteção de dados, quando aplicável. Também deverá ocorrer a colaboração de uma parte à outra quando a elaboração do relatório de impacto seja necessária, assim como a colaboração mútua em eventual consulta que possa ocorrer à Autoridade Nacional, quando apropriado.

7. COOPERAÇÃO E DIREITOS DOS TITULARES DOS DADOS:

Deverá ser indicado o nome e os detalhes de contato do encarregado de proteção de dados e, se aplicável, o representante da empresa. Este encarregado ou seu representante/ procurador deverá auxiliar o Grupo MAPFRE nas respostas, garantindo o atendimento aos direitos dos titulares na forma descrita pela LGPD. Nesse sentido, o Grupo MAPFRE deverá ser comunicado imediatamente ou em até 24 (vinte e quatro horas), pelo endereço eletrônico: **protecaodedados@mapfre.com.br** juntamente com a solicitação, quando apropriado, com outras informações que possam ser relevantes para resolver a solicitação.

8. MEDIDAS DE SEGURANÇA:

Deverão ser cumpridos todos os padrões e procedimentos de segurança técnicos e organizacionais relacionados abaixo para o tratamento da(s) informação(es), sensíveis ou não:

a) Pseudonimização;

b) Criptografia;

c) Garantia da confidencialidade permanente, integridade, disponibilidade e resiliência dos sistemas e serviços de tratamento;

d) Capacidade de restaurar a disponibilidade e o acesso a(s) informação(es), sensíveis ou não, rapidamente, em caso de incidente físico ou técnico;

e) Procedimento de verificação, avaliações regulares da eficácia das medidas técnicas e organizacionais para garantir a segurança do tratamento;

f) Garantir que todas as ferramentas tecnológicas (hardware, software e comunicação) utilizadas devem ser licenciadas;

g) Proteger todas as ferramentas tecnológicas (hardware, software e comunicação) com antivírus;

h) Não conectar seus recursos à rede de comunicações pertencente ao Grupo MAPFRE, a menos que expressamente autorizado;

i) Dentro das instalações do Grupo MAPFRE, não poderão ser instalados quaisquer softwares, a não ser que haja a prévia e expressa autorização para fazê-lo pela área de segurança corporativa da MAPFRE.

9. ENCERRAMENTO:

No encerramento dos serviços e/ou nas hipóteses previstas na LGPD, a(s) informação(es), sensível(is) ou não, deverão ser destruídas imediatamente e de forma irreversível. Não obstante o acima exposto, para o atendimento das hipóteses previstas na LGPD, poderá ser mantido como, por exemplo, para o cumprimento de obrigação legal ou regulatória, devidamente bloqueado, a(s) informação(es), sensíveis ou não, transcorrido o período legal deverá(ão) esta(s) ser destruída(s).

Outrossim, no caso de encerramento, deverá ser garantido o compartilhamento dos conhecimentos técnicos, a fim de garantir a interoperabilidade para a migração da(s) informação(es), sensível(is) ou não, para outro ambiente e/ou a entrega adequada da(s) informação(es), sensível(is) ou não, se aplicável.

Na hipótese de descarte de qualquer suporte tecnológico, este deverá destruído ou apagado usando todas as medidas cabíveis para impedir a recuperação subsequente das informações.

10. SUBCONTRATAÇÃO:

Não subcontratar nenhum dos serviços que fazem parte do objeto da contratação que envolva o tratamento da(s) informação(es), sensíveis ou não, a menos que haja a prévia e expressa autorização do Grupo MAPFRE. Caso seja autorizada a subcontratação, o(a) contratado(a) deverá informar a todo(s) o(s) subcontratado(s), sendo integralmente responsável pelo(s) subcontratado(s) e, consequentemente, sobre o(s) empregado(s), preposto(s), representante(s) designado(s) pelo(s) subcontratado(s) para a execução do(s) serviço(s), inclusive, responsabilizando-se pelo repasse de toda a informação e treinamento sobre a(s) a(s) obrigação(es) estabelecida(s) neste documento. Nesse sentido, o subcontratado se sujeitará às mesmas condições (instruções, obrigações, medidas de segurança etc.) e aos mesmos requisitos formais submetidos ao contratado em relação ao tratamento adequado da(s) informação(s), sensíveis ou não, bem como a garantia dos direitos dos titulares de dados. No caso de descumprimento do subcontratado(a), o(a) contratado(a) permanecerá totalmente responsável perante ao Grupo MAPFRE em relação ao cumprimento das obrigações estabelecidas neste instrumento.

O(s) empregado(s), preposto(s), representante(s) ou terceiro(s) designado(s) para o tratamento das informação(es), sensíveis ou não, deverá(ão) se comprometer, expressamente e por escrito, a respeitar a confidencialidade e a cumprir as medidas de segurança contidas neste instrumento, devendo ter sido informados de tais medidas.

Caso as credenciais de acesso físico ou lógico aos sistemas ou instalações pertencentes ao Grupo MAPFRE sejam fornecidas ao(s) empregado(s), preposto(s), representante(s) ou terceiro(s) designado(s), elas não poderão ser divulgadas ou transferidas em qualquer caso, pois são de cunho pessoal e intransferível.

O(A) contratado(a) e o(a) subcontratado(a) devem manter, à disposição do Grupo MAPFRE, a documentação que comprove o cumprimento das obrigações estabelecidas no item anterior.

Na hipótese de alocação de mão de obra dentro das instalações do Grupo MAPFRE, deverá(ão) ser comunicado(s) previamente os Dados Pessoais da(s) pessoa(s) natural(is) que vier(em) a ser designada(s) para os serviços contratados, bem como deverão ser informados de que os sistemas do Grupo MAPFRE podem ser monitorados, registrando os acessos efetuados e que os recursos computacionais, entre os quais e-mail e internet, são uma ferramenta de trabalho facilitada pelo Grupo MAPFRE e destinada

exclusivamente às funções associadas aos serviços contratados. Todo o monitoramento, investigação e registro de recursos informáticos realizados para esse fim sempre serão realizados com o devido respeito pela dignidade e privacidade da pessoa natural;

Tanto os contratados quanto os subcontratados deverão comunicar imediatamente/a partir do conhecimento ou da suspeita de incidentes ocorridos/a ocorrer que afetem a segurança da(s) informação(es), sensíveis ou não, relacionadas ao Grupo MAPFRE, de acordo com as normas e procedimentos que deverão estabelecer para esse fim;

11. TRATAMENTO DE INFORMAÇÃO(ES) SENSÍVEL(IS):

11.1. ACESSO E IDENTIFICAÇÃO DE USUÁRIO: Para o acesso à(s) informação(es) sensível(is), deverá conter uma lista atualizada com a identificação e a autenticação de usuários. O acesso deverá ser autorizado e com tentativas repetidas de acesso para as informações não autorizadas, sendo que cada tentativa de acesso, pelo menos as informações como o usuário, a data e a hora em que foi feita deverão ser salvas, autorizadas ou negadas. Da mesma forma, serão constantes as atualizações realizadas sobre os registros, mantendo-as por no mínimo 2 (dois) anos. Quando o controle de acesso for baseado em senhas, deverá haver um procedimento de alocação, distribuição e armazenamento que garantirá sua confidencialidade, bem como deverá(ão) ser alteradas periodicamente, sendo que em nenhum caso será superior a 1 (um) ano.

As informações de controle registradas deverão ser revisadas pelo menos uma vez por mês e, no caso de problemas detectados, deverá ser realizado um relatório discriminando os problemas identificados para o representante do Grupo MAPFRE.

11.2. INVENTÁRIO DE MÍDIA: Todas as mídias serão inventariadas pelo tipo de informação que contêm e que podem ser identificada nelas, através de um sistema de rotulagem que permite a identificação de seu conteúdo dificultando o acesso de pessoas não envolvidas nos serviços executados. Os arquivos ou cópias temporárias para as informações sensíveis, em qualquer formato, criados exclusivamente para a execução de trabalhos temporários ou auxiliares, também deverão obedecer ao nível de segurança que lhes corresponde e devem ser excluídos ou destruídos quando não forem mais necessários para cumprir o objeto do contrato.

11.3. ARMAZENAMENTO DE INFORMAÇÃO EM ESPAÇOS FÍSICOS: O acesso aos espaços onde o equipamento físico que suporta os sistemas tecnológicos que processam as informações sensíveis e/ou informações (Centros de Tratamento de Dados, Salas de Reprografia, etc.) será permitido somente mediante autorização prévia. Os armários, arquivos ou outros itens nos quais as informações sensíveis são armazenadas devem estar localizados em áreas protegidas, trancados com chave ou outro dispositivo

equivalente, devendo ser mantidos fechados. Caso nas instalações físicas não seja possível cumprir o disposto acima, medidas alternativas devem ser tomadas, devidamente notificadas, para serem incluídas nos procedimentos.

11.4. TRANSFERÊNCIA NACIONAL DE INFORMAÇÕES SENSÍVEIS: A saída de suportes fora das instalações deve ser autorizada prévia e expressamente pelo Grupo MAPFRE. Deverá haver um registro de entradas e saídas de mídia que permite, direta ou indiretamente, saber: o tipo de suporte, a data, a hora, o remetente e o número de unidades incluídas na remessa, o tipo de informação, a forma de remessa e as pessoas responsáveis pelo recebimento ou entrega. Sempre que a transferência de informações ou documentação for realizada, serão adotadas as medidas destinadas ao impedimento de roubo, manipulação, perda ou acesso inadequado. As distribuições dos suportes serão realizadas usando mecanismos que garantem que as informações não sejam acessíveis ou manipuladas durante o transporte.

12. GERENCIAMENTO DE INCIDENTES:

Um processo deverá ser implementado para a notificação e gerenciamento de incidentes que afete(m) a(s) informação(es), sensíveis ou não, o qual possa identificar e registrar o tipo de incidente, data, detecção, quem o notifica, os efeitos dele derivados, data da solução, descrição da solução, etc. Este sistema deverá incluir as recuperações das informações feitas, indicando a pessoa que as executou, os dados restaurados e, quando apropriado, quais dados foram necessários para registrar manualmente no processo de recuperação.

Em caso de incidentes de segurança que envolvam informação(es), sensíveis ou não, ou possam acarretar risco ou danos aos titulares de dados, o Grupo MAPFRE deverá ser imediatamente notificado e, em qualquer caso, antes do período máximo de 24 (vinte e quatro) horas contadas do conhecimento do fato, por e-mail no endereço **incidentesdeseguranca@mapfre.com.br** juntamente com todas as informações relevantes para a documentação e comunicação do incidente, sendo que, se disponível, deverão conter ao menos as seguintes informações:

a) Descrição da natureza de violação da segurança dos dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de titulares envolvidos e a natureza dos dados pessoais afetados;

b) O nome e os detalhes de contato do encarregado de proteção de dados, de acordo com a LGPD ou representante/procurador indicado por este para contato do Grupo MAPFRE;

c) Descrição dos riscos relacionados ao incidente e das possíveis consequências da violação da segurança dos dados pessoais;

d) Indicação de todas as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais;

e) Descrição das medidas adotadas ou propostas para remediar os efeitos do incidente de segurança envolvendo dados pessoais, incluindo, se apropriado, as medidas adotadas para mitigar os possíveis efeitos negativos;

Se não for possível fornecer as informações descritas acima simultaneamente, as informações deverão ser fornecidas gradualmente, sem demora injustificada.

13. BACKUP E RECUPERAÇÃO DE INFORMAÇÃO(ES), SENSÍVEIS OU NÃO:

Sempre que houver a realização de qualquer atividade de tratamento de informações sensíveis, o que implica variação, deve-se:

a) Fazer cópias de segurança semanais;

b) Estabelecer procedimentos para a recuperação da(s) informação(es) sensível(is) que garantam a todo momento sua reconstrução no estado em que estavam no momento da perda ou destruição;

c) Verificar semestralmente a definição, operação e aplicação correta dos procedimentos de backup e recuperação;

d) Os testes de implantação ou modificação dos sistemas tecnológicos não serão realizados em hipótese alguma com dados reais, a menos que seja garantido o nível de segurança correspondente ao tratamento realizado, este seja registrado nos procedimentos e feito um backup prévio;

e) Se houver uma perda ou destruição que afete informações parcialmente automatizadas, no caso de recuperá-las manualmente (registrá-las), deve haver um registro fundamentado desse fato;

f) Manter cópias de segurança da(s) informação(es) sensível(is) e do procedimento de recuperação em um local diferente daquele em que o equipamento de computador que as trata está localizado, o que deve, em todos os casos, cumprir as medidas de segurança exigidas neste documento;

Nos casos de destruição, perda, difusão ou alteração acidental ou ilegal da(s) informação(es), sensíveis ou não, bem como comunicação ou acesso não autorizado delas, deve-se garantir um nível de segurança adequado ao risco definido com base na: (i) avaliação de risco; (ii) regulamentos atuais em vigor e que, dependendo da natureza da(s) informação(es), sensíveis ou não, tratada(s), a qualquer momento, sejam especificados neste instrumento, ou qualquer outro que o complemente, modifique ou substitua no futuro, (iii) nas normas internacionais e mecanismos de certificação obrigatórios que, se aplicáveis, como o PCI DSS, em relação aos dados do cartão de crédito.

14. AUDITORIA:

O Grupo MAPFRE se reserva ao direito de verificar, a qualquer momento, a conformidade com os procedimentos, medidas e controles de segurança exigidos neste instrumento, inclusive por meio de auditorias e testes de segurança em relação a sistemas de informação, comunicações, arquivos, regulamentos legais de proteção de dados pessoais, etc., bem como os procedimentos que suportam a execução deste contrato, mesmo quando todas as atividades ou parte delas são realizadas nas instalações e/ou com os recursos do Grupo MAPFRE, mediante solicitação por escrito, sendo que, neste último caso, com pelo menos 48 (quarenta e oito) horas de antecedência. Será disponibilizado ao Grupo MAPFRE todas as informações necessárias para demonstrar o cumprimento de suas obrigações, bem como para permitir a adequada realização de auditorias ou inspeções pelo Grupo MAPFRE ou outro auditor autorizado por ela e apoiar em eventuais consultas à Autoridade supervisora, quando apropriado.

MAPFRE

Versão 2.0

Manual de Instrução do Tratamento de Dados Pessoais e Sensíveis