SUMÁRIO

1. OBJETIVO

Esta Política de Gestão de Dados Pessoais tem como objetivo apresentar aos colaboradores, prestadores de serviços, parceiros e fornecedores do **GRUPO GR** as diretrizes da proteção aos dados pessoais e a importância da adoção das melhores práticas, bem como estabelecer as responsabilidades e os limites de atuação, reforçando a cultura interna e priorizando as ações necessárias, formalizando o comprometimento do **GRUPO GR** em adequar-se às leis aplicáveis, fortalecendo os negócios, as parcerias e as relações com os titulares dos dados pessoais.

2. APLICAÇÃO

Esta Política aplica-se aos colaboradores, prestadores de serviços, parceiros e fornecedores do **GRUPO GR**.

3. DEFINIÇÕES E SIGLAS

Agente de Tratamento: O controlador e o operador;

Autoridade competente: Órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da Lei de Proteção de Dados Pessoais aplicável.

Colaborador: Empregado, estagiário, menor aprendiz, ou qualquer outro indivíduo ocupante de cargo ou emprego no **GRUPO GR**.

Ciclo de Vida do Dado Pessoal: Fluxo do tratamento do dado pessoal, que envolve as ações de Coleta, Armazenamento, Uso, Compartilhamento e Eliminação do dado pessoal.

Compartilhamento de dados pessoais: Comunicação, difusão, transferência nacional ou internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos, entidades ou pessoais, e para uma ou mais modalidades de tratamento.

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

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

Dado anonimizado: Dado que não identifica de forma direta ou indireta um titular dos dados pessoais, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado pessoal: Informação relacionada à pessoa física identificada ou identificável. Para os propósitos desta Política, os dados pessoais são classificados como Informação Confidencial.

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 física.

Dados de saúde: dados sensíveis que permitem inferir informações referentes à saúde do titular.

Encarregado pelo tratamento de dados pessoais: Pessoa física ou jurídica indicada pelo **GRUPO GR** e que atua como canal de comunicação entre o **GRUPO GR** e os Titulares dos dados pessoais ou a Autoridade competente.

Legalidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.

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

Pseudonimização: é o tratamento por meio do qual um dado pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Relatório de Impacto à Proteção de Dados Pessoais: Documento que contém a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares dos dados pessoais, bem como medidas, salvaguardas e mecanismos de mitigação desses riscos.

Requisições dos Titular dos dados pessoais: Requisição do Titular dos dados pessoais acerca de seus direitos estabelecidos em lei e relativos ao tratamento dos seus dados pessoais.

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

Tratamento de Dados Pessoais: 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.

Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos do **GRUPO GR**.

Violação de Dados Pessoais: Destruição, perda, alteração, divulgação acidental ou ilegal, não autorizada ou acesso a dados pessoais transmitidos, armazenados ou de outra forma processados, resultante de incidente de segurança.

4. DOCUMENTOS DE REFERÊNCIA

Lei nº 13.709, de 14 de agosto de 2018, Lei de Proteção de Dados Pessoais;

Decreto nº 8.771, de 11 de maio de 2016, regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

Lei nº 12.965, de 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

Lei nº 12.527, de 18 de novembro de 2011, regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

5. DIRETRIZES

5.1. O Tratamento De Dados Pessoais Deve Ser Regido Pelos Princípios Abaixo.

5.1.1. Finalidade: Os dados pessoais devem ser tratados apenas para as finalidades determinadas, explícitas, legítimas e informadas antes do tratamento, não podendo ser tratados posteriormente para finalidades incompatíveis.

5.1.2. Adequação: Os dados pessoais devem ser tratados de modo adequado e pertinente às suas finalidades de uso.

5.1.3. Necessidade e Proporcionalidade: O tratamento dos dados pessoais deve ser proporcional aos objetivos do negócio, não sendo feito tratamento de tipos de dados pessoais que não sejam necessários e proporcionais aos objetivos de negócio.

As áreas que realizam o tratamento dos dados pessoais devem buscar tratar o menor volume possível de dados pessoais, devendo esse volume ser proporcional aos objetivos do negócio.

5.1.3.1. **Minimização:** Os dados pessoais tratados pelo **GRUPO GR** devem ser limitados ao mínimo necessário para execução das finalidades de tratamento informadas. Não se deve coletar dados pessoais que não têm uma finalidade definida.

5.1.3.2. **Subsidiariedade**: Deve-se sempre buscar formas alternativas (subsidiárias) de se atingir as mesmas finalidades por meios menos invasivos à privacidade do titular dos dados pessoais. Devem ser cogitados métodos alternativos ou subsidiários que levem em consideração os direitos dos titulares dos dados para o cumprimento das finalidades de tratamento.

5.1.3.3. **Limitação de armazenamento:** Os dados pessoais e registros devem ser armazenados apenas durante o período estritamente necessário de acordo com sua finalidade, com os padrões a serem estabelecidos pela Autoridade Nacional de Proteção de dados (ANPD) e de acordo com a legislação aplicável. Os dados pessoais devem ser armazenados por período limitado, sendo que o período (ou critério) estabelecido deve ser informado ao titular dos dados pessoais antes do tratamento, excetuando-se hipóteses legais nas quais seja permitido o armazenamento por maior período de tempo. O período para a guarda dos dados pessoais deve ser definido na tabela de temporalidade.

5.1.4. **Livre acesso**: Assegurar aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados pessoais.

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

5.1.6. **Transparência**: Assegurar que os titulares tenham informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados pessoais, observados os segredos comercial e industrial. Antes de realizar o tratamento de dados pessoais, o titular dos dados pessoais deve receber informação clara, concisa, inteligível, de fácil acesso e de fácil compreensão sobre a coleta, finalidade, armazenamento, compartilhamento e descarte de seus dados pessoais.

5.1.7. **Segurança:** O tratamento deve ser realizado de modo a assegurar a proteção e segurança dos dados pessoais, incluindo a proteção contra o tratamento não autorizado ou ilícito, perda, destruição ou dano acidental, devendo o **GRUPO GR** adotar medidas técnicas e organizacionais para salvaguardar a integridade, confidencialidade e disponibilidade dos dados pessoais.

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

5.1.9. **Não discriminação**: Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

5.1.10. **Responsabilização e prestação de contas**: Demonstração 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.

5.2. Bases Legais Para Tratamento De Dados Pessoais

5.2.1. O tratamento dos dados pessoais deve ser realizado de modo lícito, justo e transparente com relação ao titular dos dados pessoais.

5.2.1.1. **Dados Pessoais**: O tratamento de dados pessoais somente é permitido e, portanto, está legitimado:

5.2.1.1.1. Com o consentimento do titular dos dados pessoais, conforme detalhado no item 4. <u>É vedado o tratamento de dados pessoais mediante vício de consentimento</u>;

5.2.1.1.2. Em caso do cumprimento de uma obrigação legal ou regulatória pelo **GRUPO GR**;

5.2.1.1.3. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

5.2.1.1.4. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

5.2.1.1.5. Quando o titular dos dados pessoais é parte em contrato ou os seus dados pessoais são necessários para execução de procedimentos preliminares para se firmar o contrato;

5.2.1.1.6. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, prezando sempre pelo pedido de segredo de justiça quando envolver dado pessoal;

5.2.1.1.7. Para a proteção da vida ou da segurança física da pessoa a quem os dados pessoais se referem;

5.2.1.1.8. Para proteção da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

5.2.1.1.9. Por interesse legítimo do **GRUPO GR** ou de terceiros, sendo obrigatória a confecção de relatório de impacto à proteção de dados pessoais;

5.2.1.1.10. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

5.2.1.1.11. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

5.2.1.2. **Dados Pessoais Sensíveis:** O tratamento de dados pessoais sensíveis deve ser precedido de relatório de impacto à proteção de dados pessoais. As hipóteses legais de tratamento de dados pessoais sensíveis, conforme ordenamento jurídico brasileiro vigente, são:

5.2.1.2.1. Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

5.2.1.2.2. Sem o fornecimento de consentimento, quando for indispensável para:

5.2.1.2.2.1. Cumprimento de obrigação legal ou regulatória pelo Controlador;

5.2.1.2.2.2. Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

5.2.1.2.2.3. realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

5.2.1.2.2.4. exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

5.2.1.2.2.5. proteção da vida ou da incolumidade física do titular ou de terceiro;

5.2.1.2.2.6. tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

5.2.1.2.2.7. 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.

5.3. Dados De Saúde:

5.3.1. Os dados de saúde poderão ser compartilhados entre Controladores levando em consideração o benefício dos interesses dos titulares e se for realizado, exclusivamente, para:

5.3.1.1. prestação de serviços de saúde;

5.3.1.2. assistência farmacêutica;

5.3.1.3. assistência à saúde;

5.3.1.4. serviços auxiliares de diagnose;

5.3.1.5. serviços de terapia.

5.3.2. O tratamento de dados de saúde deverá, obrigatoriamente, permitir ao titular o direito a portabilidade dos seus dados, quando solicitada ou as transações financeiras e administrativas resultantes do uso e da prestação dos serviços.

5.4. Diretrizes Gerais Para Tratamento Dos Dados Pessoais:

5.4.1. O tratamento de dados pessoais significa toda e qualquer operação realizada pelo **GRUPO GR** com dados pessoais, a exemplo de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração entre outras operações possíveis.

5.4.2. O tratamento de dados pessoais deve ser realizado de acordo com os princípios do item 5 desta Política.

5.4.2.1. **Ciclo de vida do dado pessoal:** Todo o ciclo de vida do Dado Pessoal no **GRUPO GR** deverá estar de acordo com as diretrizes do **Anexo I** da Política, bem como diretrizes quanto à transferência internacional indicadas no Anexo II desta Política.

5.4.2.2. **Contratos:** O **GRUPO GR** na figura de Controlador, sempre que fizer uso de um Operador, deve estabelecer contrato tendo em vista as regulamentações relacionadas à privacidade e proteção de dados pessoais vigentes no país onde ocorrerá o tratamento dos dados pessoais, observando as diretrizes indicadas no Anexo III desta Política.

5.4.2.3. **Relatório de Impacto a Proteção dos Dados Pessoais (RIPD):** O relatório de impacto à proteção de dados pessoais visa a descrição dos processos de tratamento de dados pessoais e as medidas e mecanismos empregados para mitigar esses riscos pelo **GRUPO GR**.

5.4.2.3.1. Todo tratamento de dados pessoais tendo como base legal o legítimo interesse deve ser precedido de relatório de impacto à proteção de dados pessoais.

5.4.2.3.2. O relatório de impacto à proteção de dados pessoais deve ser elaborado pelo Encarregado pelo Tratamento de Dados Pessoais, com envolvimento das áreas necessárias para entendimento da elaboração deste relatório, conforme procedimento específico e, também, de acordo com as diretrizes do Anexo IV desta Política.

5.4.2.4. **Segurança da Informação**: Durante todo o ciclo de vida do dado pessoal, devem ser observadas as diretrizes de segurança existentes na Política de Segurança da Informação do **GRUPO GR**, bem como diretrizes gerais existentes na forma do Anexo V desta Política.

5.4.2.5. **Decisões Automatizadas:** As áreas devem listar os processos sob sua responsabilidade que envolvem decisões automatizadas baseada no tratamento de dados pessoais que ocorrem em sua área.

5.4.2.5.1. Toda decisão automatizada que envolve o tratamento de dados pessoais deve ter formalizada informações claras e adequadas, disponíveis aos titulares dos dados pessoais, quanto aos:

- Critérios utilizados para tomada de decisão automatizada;
- Procedimentos utilizados para a tomada de decisão automatiza;

5.4.2.5.2. O titular dos dados pessoais tem o direito de solicitar a revisão de tomada de decisão baseada em tratamento automatizado dos dados pessoais, tendo o acesso aos critérios e procedimentos, não sendo exigido que esta revisão seja por pessoa natural.

5.4.2.6. **Legítimo interesse**: O legítimo interesse deverá ser previamente analisado e validado junto ao Encarregado da Proteção de Dados Pessoais do **GRUPO GR** conforme procedimento específico, levando em consideração a proteção,

em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem:

- Fazendo coleta dos dados estritamente necessários para a finalidade pretendida;
- Garantindo total transparência ao titular quando o tratamento dos dados pessoais estiver utilizando o legítimo interesse como base; e
- Elaborando Relatório de Impacto a Proteção de Dados (RIPD) conforme orientação do item 5.4.2.3 para as atividades cuja base legal para tratamento seja legítimo interesse.

5.5. Diretrizes De Resposta À Solicitações E Requisições

5.5.1. As diretrizes de procedimentos de resposta às requisições dos titulares dos dados pessoais serão regidas pelo Procedimento de resposta à requisição do titular dos dados pessoais, disponível na intranet ou rede interna, conforme orientações do **Anexo VI**, no tocante a:

5.5.1.1. Resposta a requisição do titular dos dados pessoais;

5.5.1.2. Acesso aos dados pessoais pelo titular dos dados pessoais;

5.5.1.3. Apagamento e/ou bloquei de tratamento dos dados pessoais por requisição do titular dos dados pessoais;

5.5.1.4. Resposta a autoridade fiscalizadora;

5.5.1.5. Resposta a autoridade judicial.

6. MANUTENÇÃO DA POLÍTICA DE GOVERNANÇA DE DADOS PESSOAIS

O **GRUPO GR** deve estabelecer compromissos organizacionais, controles, avaliação e revisão das atividades para sustentar a sua Política de Governança de Dados Pessoais, bem como manter a conformidade de suas operações.

Caberá ao Comitê de Privacidade e o Encarregado pela Proteção de Dados Pessoais estabelecerem planos de ações ao identificar eventuais lacunas nos elementos que compõe esta Política.

7. COMPROMISSOS ORGANIZACIONAIS

7.1. Diretoria

7.1.1. Cumprir e fazer cumprir esta Política e demais documentos que a compõem;

7.1.2. Analisar e aprovar a política de gestão de dados pessoais;

7.1.3. Zelar para que o **GRUPO GR** esteja adequada à legislação de proteção de dados pessoais;

7.1.4. Aprovar os investimentos em segurança da informação e proteção de dados pessoais, considerando a viabilidade, os custos, a técnica disponível e o tratamento de dados pessoais;

7.1.5. Analisar e aprovar, ou não, as exceções a esta Política, considerando os riscos que quaisquer exceções podem trazer à operação, caso vão de encontro às boas práticas em termos de proteção de dados pessoais.

7.2. Encarregado Pelo Tratamento De Dados Pessoais

7.2.1. Elaborar e/ou revisar os procedimentos internos relativos à proteção de dados pessoais;

7.2.2. Organizar e/ou ministrar treinamentos em proteção de dados pessoais aos colaboradores ou prestadores de serviço;

7.2.3. Analisar contratos que envolvam tratamento de dados pessoais, seguindo o framework legal específico aplicável a cada situação em suas particularidades;

7.2.4. Apoiar investigações para apuração de responsabilidade dos envolvidos em violações de dados pessoais e auxiliar na definição de aplicação das penalidades internas, quando necessário;

7.2.5. Avaliar e auxiliar na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais;

7.2.6. Manter mapeamento de fluxos de dados Pessoais atualizado;

7.2.7. Fazer cumprir a Tabela de Temporalidade;

7.2.8. Desenvolver plano de análise e resposta a violações de dados pessoais que identifique o tipo de violação, o número de registros afetados, quais registros foram afetados e as categorias de dados pessoais envolvidas, as notificações apropriadas e plano de mitigação dos efeitos da violação;

7.2.9. Receber as requisições dos titulares dos dados pessoais sobre privacidade e proteção de dados pessoais, bem como as comunicações da Autoridade Nacional;

7.2.10. Verificar a adequação das práticas e políticas do **GRUPO GR** no que se refere à transferência internacional de dados pessoais e ao manejo de dados pessoais sensíveis.

7.3. Comitê de Privacidade

7.3.1. Definir controles para garantir a integridade, confidencialidade e disponibilidade dos dados pessoais, conforme preceituado pela lei;

7.3.2. Definir os controles para garantir a existência de registros auditáveis de todo o ciclo de vida dos dados pessoais, desde o consentimento para o tratamento até o descarte, certificando-se que o descarte seja confirmado em dupla verificação, sempre que possível;

7.3.3. Identificar e avaliar riscos relacionados à segurança da informação e proteção de dados pessoais e propor melhorias e recursos necessários;

7.3.4. Analisar ou auxiliar na análise das violações de dados pessoais reportadas;

7.3.5. Manter comunicação com o Encarregado pelo Tratamento de Dados Pessoais sobre os aspectos relevantes à segurança da informação e proteção de dados pessoais.

7.4. Área de Tecnologia da Informação

7.4.1. Cumprir e fazer cumprir esta Política e demais documentos que a compõem;

7.4.2. Assegurar continuamente que todos os sistemas, serviços e equipamentos usados para o tratamento de dados pessoais estejam dentro de um padrão aceitável de segurança;

7.4.3. Analisar os aspectos técnicos de todo e qualquer produto ou serviço de terceiros que o **GRUPO GR** esteja considerando contratar para processar ou armazenar dados pessoais (exemplos: nuvem, hardware, equipamentos de rede);

7.4.4. Atuar de forma coordenada com o Encarregado pelo Tratamento de Dados Pessoais para viabilizar a implementação de procedimentos e rotinas necessárias para o tratamento de dados pessoais, como a dupla verificação da exclusão de dados pessoais;

7.4.5. Indicar colaborador ou prestador de serviço para supervisionar cada sistema que contenha dados pessoais coletados, utilizados ou armazenados e garantir que as medidas necessárias e apropriadas para manutenção da confidencialidade, integridade e disponibilidade dos dados pessoais estejam sendo tomadas;

7.4.6. Coletar e manter registros das atividades de tratamento de dados pessoais, desde evidências que comprovem o consentimento dos titulares dos dados pessoais (logs de consentimento, por exemplo) até registro de utilização, compartilhamento, exclusão e outros, pelo período legal exigido conforme a Tabela de Temporalidade.

7.5. Área Jurídica

7.5.1. Participar previamente dos processos de contratação e aquisição de produtos e serviços do **GRUPO GR**, validando as minutas visando que atendam aos controles de proteção de dados pessoais aplicáveis;

7.5.2. Apoiar o Encarregado pelo Tratamento de Dados Pessoais quanto a possiblidades de tratamento de dados pessoais no exterior, auxiliando no entendimento de validação do nível de proteção de dados pessoais do país destino;

7.5.3. Analisar, com apoio do Encarregado pelo Tratamento de Dados Pessoais, possiblidade de compartilhamento de dados pessoais para outros países, validando o nível de proteção de dados pessoais do país destino;

7.5.4. Elaborar comunicados oficiais de respostas à Autoridade Fiscalizadora e Autoridades Judiciais Competentes, com apoio do Encarregado pelo Tratamento de Dados Pessoais;

7.5.5. Fornecer orientação a Diretoria, colaboradores ou prestadores de serviço, com apoio do Encarregado pelo Tratamento de Dados Pessoais, quanto a medidas a serem tomadas no caso de violação de dados pessoais.

7.6. Área de Recursos Humanos

7.6.1. Promover, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, a cultura de proteção de dados pessoais no **GRUPO GR**, realizando campanhas de capacitação e divulgação da proteção dos dados pessoais;

7.6.2. Assegurar a divulgação e a disponibilidade dos documentos que compõem esta Política e outras políticas internas para proteção de dados pessoais no **GRUPO GR**;

7.6.3. Assegurar que os colaboradores que tratam dados pessoais tenham assinado Cláusulas de Confidencialidade que incluam disposições específicas para o tratamento de dados pessoais;

7.6.4. Estipular controles de proteção de dados pessoais especificamente relacionados aos processos de contratação, desligamento (ou encerramento de prestação de serviços), modificação de atividades (incluindo a promoção) e afastamentos (incluindo férias e quaisquer licenças ou suspensões).

7.7. Área - Marketing

7.7.1. Elaborar, com o apoio do Encarregado pelo Tratamento de Dados Pessoais, campanhas de conscientização e materiais de divulgação e alerta relacionados a proteção de dados pessoais;

7.7.2. Analisar e aprovar a forma das comunicações relacionadas à proteção de dados pessoais;

7.7.3. Responder, seguindo as orientações do Encarregado pelo Tratamento de Dados Pessoais, eventuais questionamentos de veículos de imprensa;

7.7.4. Submeter à análise do Encarregado pelo Tratamento de Dados Pessoais textos e comunicados sobre privacidade e proteção de dados pessoais, antes de sua publicação.

7.8. Gestores

7.8.1. Cumprir, fazer cumprir e gerenciar o cumprimento desta Política e demais documentos complementares por parte de seus colaboradores ou prestadores de serviço;

7.8.2. Assegurar que qualquer dado pessoal só poderá ser recebido, tratado, excluído ou compartilhado por sua área mediante notificação ao Encarregado pelo Tratamento de Dados Pessoais;

7.8.3. Garantir a observação desta Política e da legislação competente pelos parceiros de negócio que recebam dados pessoais enviados por sua área, devendo:

- Obter documentos (procedimentos internos de segurança da informação, treinamento aplicado aos colaboradores ou prestadores de serviços que manuseiam os dados pessoais, lista de controle de acesso, por exemplo) e garantias (acordo de confidencialidade assinado pelos colaboradores, cláusulas contratuais, dentre outras) do parceiro de negócio que confirmem a segurança no manuseio dos dados pessoais sob responsabilidade do **GRUPO GR**;
- Firmar Acordo de Confidencialidade com o parceiro de negócios;
- Requerer, por meio de contrato, que o parceiro de negócios obtenha aprovação prévia e por escrito do **GRUPO GR** antes de qualquer subcontratação para fins de tratamento de dados pessoais sob responsabilidade do **GRUPO GR**, independente de previsão legal nesse sentido;
- Requerer, por meio de contrato, que o parceiro de negócios se abstenha de utilizar os dados pessoais sob responsabilidade do

GRUPO GR para qualquer outro propósito, e que, após concluído o objeto do contrato, que sejam devolvidos e/ou eliminados todos os dados pessoais enviados ou compartilhados pelo **GRUPO GR** ao parceiro.

7.8.4. Preparar e manter atualizada uma lista com todas as categorias de dados pessoais tratados em sua área, e submeter essa lista ao Encarregado pelo Tratamento de Dados Pessoais;

7.8.5. Assegurar que os dados pessoais são coletados, usados ou gerenciados apenas por colaboradores ou prestadores de serviços autorizados, devendo:

- Classificar os dados pessoais tratados em sua área como confidenciais;
- Aprovar acessos aos colaboradores ou prestadores de serviço diretamente envolvidos nas atividades que demandam os dados pessoais;
- Assegurar que os colaboradores ou prestadores de serviço sob sua supervisão realizem treinamentos em proteção de dados pessoais e conheçam as políticas internas do **GRUPO GR**;
- Atuar em parceria com as demais áreas do **GRUPO GR** para identificar as vulnerabilidades e ameaças à proteção de dados pessoais nos processos e atividades de sua responsabilidade;
- Assegurar que os dados pessoais sob a responsabilidade do **GRUPO GR** sejam utilizados com cuidado e de acordo com as orientações legais aplicáveis;

7.8.6. Ao identificar violações de dados pessoais ou qualquer ação duvidosa, comunicar o Encarregado pelo Tratamento de Dados Pessoais imediatamente.

7.9. Colaboradores E Prestadores De Serviço

7.9.1. Cumprir e fazer cumprir, manter-se atualizado com esta Política e demais documentos que a compõem;

7.9.2. Tratar os dados pessoais sob responsabilidade do **GRUPO GR** somente para fins autorizados, de forma ética e legal, respeitando os direitos do titular dos dados pessoais e de acordo com as orientações desta Política e da legislação aplicável;

7.9.3. Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados pessoais acessados ou manipulados, não utilizando, enviando, transmitindo ou compartilhando indevidamente estes dados pessoais, em qualquer local ou mídia, inclusive na Internet;

7.9.4. Cumprir a legislação vigente e demais instrumentos regulamentares relacionados à proteção de dados pessoais;

7.9.5. Reportar formalmente ao Encarregado pelo Tratamento de Dados Pessoais quaisquer eventos relativos à violação ou possibilidade de violação de dados pessoais ou atividades suspeitas de que tiver conhecimento;

7.9.6. Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais no **GRUPO GR**;

7.9.7. Reportar formalmente ao Encarregado pelo Tratamento de Dados Pessoais quaisquer eventos relativos à violação dados pessoais ou atividades suspeitas, por meio do e-mail contato.lgpd@grupogr.com.br .

8. ANEXOS

Anexo I - Ciclo De Vida Do Dado Pessoal

Anexo II - Transferência Internacional De Dados Pessoais

Anexo III - Contratos

Anexo IV - Relatório De Impacto À Proteção De Dados Pessoais

Anexo V – Segurança Da Informação

Anexo Vi - Diretrizes De Resposta À Solicitações E Requisições

ANEXO I - CICLO DE VIDA DO DADO PESSOAL

Em todas as etapas do ciclo de vida do dado pessoal, o **GRUPO GR** deve estar apta a demonstrar, no mínimo, as seguintes informações quando o tratamento for realizado, ***respeitando o princípio da Transparência***:

- A qualificação do **GRUPO GR** e seus dados de contato;
- O canal de contato com o Encarregado pelo Tratamento de Dados Pessoais do **GRUPO GR**;
- As finalidades específicas e forma de tratamento;
- O Tempo de retenção dos dados pessoais, levando em consideração a finalidade do tratamento (devendo estar de acordo com a lei e a tabela de temporalidade);
- Demais Controladores com as quais o **GRUPO GR** realiza o uso compartilhado de dados pessoais, tanto entidades públicas como privadas;
- Se o tratamento dos dados pessoais se baseia em interesse legítimo do **GRUPO GR** ou de terceiros;
- Se ocorrerá a transferência de dados pessoais para outro país (incluindo-se por meio do armazenamento em nuvem em que o hardware se localiza em outro país) e, neste caso, se há salvaguardas adequadas para a transferência internacional;
- Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato;
- Quando o consentimento do titular dos dados pessoais for necessário, dispor acerca da possibilidade de não fornecimento de consentimento e sobre as consequências que a negativa pode ocasionar, bem como possibilitar que o titular revogue o consentimento, nos termos da legislação aplicável.
- A existência de decisões automatizadas, incluindo a definição de perfis, além de informações úteis relativas à lógica utilizada, a importância e as consequências previstas de tal tratamento para o titular dos dados pessoais;
- Os direitos do titular dos dados pessoais, como a confirmação da existência do tratamento, acesso aos dados pessoais, correção de dados pessoais incompletos, inexatos

ou desatualizados, portabilidade dos dados pessoais, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a legislação aplicável;

- Os riscos, regras e garantias associadas ao tratamento dos dados pessoais, bem como os meios que o titular dos dados pessoais dispõe para exercer os seus direitos relativamente a esse tratamento;

- Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direitos, o titular dos dados pessoais será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os seus direitos.

COLETA

A coleta do dado pessoal significa a entrada do dado pessoal no **GRUPO GR**, podendo ser feita por meio de sistemas da informação ligados a sites, aplicativos, recebimento de arquivos, aquisição de base de dados bem como no ambiente físico como pelo preenchimento de formulários, listas ou pelo registro de uma conversa presencial, por chat, troca de mensagens, e-mails ou por telefone, por exemplo.

Coleta tendo como base legal o consentimento:

- Quando o tratamento dos dados pessoais se basear no consentimento do titular, este deve ser dado mediante manifestação de vontade livre de que o titular concorda com o tratamento de dados pessoais da forma declarada.

- O consentimento pode ser dado de modo escrito, digital ou oral, sendo fundamental que o **GRUPO GR** registre e comprove o consentimento do titular (ônus da prova).

- O consentimento para tratamento de dados pessoais sensíveis deve ser possível de ser coletado de forma específica e destacada, para finalidades específicas.

- O silêncio, opções pré-validadas, generalistas ou a omissão NÃO são consideradas manifestações de consentimento.

- A <<Área de Tecnologia da Informação>> do **GRUPO GR** deve realizar a gestão do consentimento nos casos em que o tratamento ocorra na hipótese legal de tratamento o consentimento do titular.

- Se o consentimento do titular dos dados pessoais for dado no contexto de uma declaração escrita que diga também respeito a outras finalidades de tratamento, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente das demais finalidades de modo inteligível, destacado, de fácil acesso e em linguagem clara e simples.

- O titular dos dados pessoais deve ser informado previamente sobre o seu direito de revogar o consentimento a qualquer momento. A revogação do consentimento deve ser oferecida de maneira simples, clara e facilitada, de preferência pela mesma via de coleta do consentimento.

- O titular dos dados pessoais deve ser informado previamente das consequências da revogação do consentimento.

- A revogação do consentimento não compromete a licitude do tratamento já efetuado com base no consentimento previamente dado e deverá ser realizado por procedimento gratuito e facilitado.

Consentimento de Crianças e Adolescentes:

- O tratamento de dados pessoais de crianças e adolescentes deve ocorrer somente se o consentimento for dado por pelo menos um dos pais ou pelo responsável legal.

- Cada área responsável por este tratamento deve coletar a evidência de cumprimento do disposto acima para fins de formação de prova.

ARMAZENAMENTO

1.1. O armazenamento dos dados pessoais pode ser feito de modo físico (guarda de crachás, cartões, fichas, papeis com anotações à mão, formulários, notas fiscais, contratos e outros documentos em papel, por exemplo) ou digital (em mídias como CD, DVD, Blu-Ray, HD externo, pendrive, cartão de memória SD, nas plataformas digitais do **GRUPO GR** ou em serviço contratado para esta finalidade).

1.2. No caso de armazenamento fora do Brasil, a < Área de Tecnologia da Informação> por garantir o tratamento dos dados pessoais deve estar atenta para o país em que o hardware se localiza e, localizando-se no exterior, deve-se acionar a Assessoria Jurídica do **GRUPO GR** para verificar se há amparo legal e contratual para que os dados pessoais estejam armazenados esse país.

1.3. Os meios físicos e digitais de armazenamento dos dados pessoais devem assegurar a sua qualidade, devendo ser mantidos exatos e atualizados, de acordo com a necessidade para o cumprimento da finalidade de tratamento.

1.4. Quando o titular dos dados pessoais solicitar a correção ou atualização de seus dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais, após análise da requisição, deve acionar a < Área de Tecnologia da Informação> para assegurar que os meios físicos e digitais onde esses dados pessoais foram replicados e armazenados sejam também atualizados.

USO

1.5. O uso dos dados pessoais deve ser realizado dentro dos limites das finalidades legitimadas na coleta. Caso haja a necessidade de realizar o tratamento do dado pessoal para outra finalidade diversa da informada no momento da coleta, é necessário verificar:

- Qualquer ligação entre a finalidade para a qual os dados pessoais foram coletados e a finalidade do novo tratamento;
- O contexto em que os dados pessoais foram tratados (a relação entre o titular dos dados pessoais e o **GRUPO GR**);
- Se o dado coletado está sendo compartilhado com demais Agentes de Tratamento;
- A natureza dos dados pessoais (se há dados pessoais sensíveis envolvidos);
- As consequências do novo tratamento para o titular dos dados pessoais, e
- A existência de medidas de proteção adequada, como anonimização.

1.6. Essas informações devem ser encaminhadas ao Encarregado pelo Tratamento de Dados Pessoais para que defina se o novo tratamento já está ou não legitimado, e, caso não esteja, ele deve propor as estratégias de como este tratamento pode ser legitimado antes de ser realizado.

1.7. O titular dos dados pessoais deve ser informado sobre esse novo tratamento antes de ser realizado.

1.8. O legítimo interesse deverá ser previamente analisado pelo Encarregado pelo Tratamento de Dados Pessoais conforme procedimento específico.

COMPARTILHAMENTO

1.9. O compartilhamento de dados pessoais ou de documentos/arquivos com dados pessoais em território nacional pode ser feito para Agentes de Tratamento autorizados, com as medidas de segurança indicadas pela < Área de Tecnologia da Informação> e somente para as finalidades de uso ou tratamento prévia e devidamente informadas e legitimadas junto ao titular dos dados pessoais.

1.10. O compartilhamento de dados pessoais com demais Agentes de Tratamento, excetuando-se o compartilhamento realizado para cumprimento de obrigações legais, somente poderá ocorrer caso estes tenham firmado contratos com cláusulas referentes à Proteção de Dados Pessoais, conforme disposto no **Anexo III** desta Política.

1.11. No caso de impossibilidade de celebração de Contrato ou Aditivo com a parte em questão, devem ser adotados controles mitigatórios em relação à segurança e proteção do tratamento dos dados pessoais.

1.12. O compartilhamento de dados pessoais cujo tratamento tenha como hipótese legal o consentimento somente poderá ocorrer com o consentimento do titular dos dados pessoais que esteja ciente deste compartilhamento, sendo que aquele consentimento deve ser coletado anteriormente ao início do tratamento dos dados pessoais.

1.13. Os dados pessoais anonimizados podem ser transferidos para terceiros, desde que respeitados os requisitos de tratamento disposto na legislação aplicável.

1.14. O compartilhamento de dados pessoais deve ocorrer somente por canais com medidas de segurança aplicadas.

ELIMINAÇÃO DOS DADOS PESSOAIS

1.15. Os dados pessoais devem ser armazenados por período limitado, levando em consideração a finalidade específica do tratamento.

1.16. Após cumprida a finalidade do tratamento e findo o prazo de armazenamento determinado pela tabela de temporalidade, os dados podem ser eliminados de modo seguro, sejam eles registrados em meios físicos ou digitais.

1.17. A eliminação dos dados pessoais poderá ser realizada também a pedido do titular do dado ou da Autoridade Nacional de Proteção de Dados.

1.18. Devem ser seguidas as definições indicadas no procedimento de eliminação de dados seguro.

1.19. A conservação dos dados pessoais após atingida sua finalidade é possível nos casos de cumprimento de obrigação legal ou regulatória por parte do **GRUPO GR**.

1.20. A solicitação de eliminação do dado pessoal pelo titular não será possível quando o dado já tiver sido anonimizado.

1.21. A solicitação também não poderá ser realizada no caso de cumprimento de obrigação legal quanto ao armazenamento destes dados para fins regulatórios, respeitada a tabela de temporalidade.

ANEXO II - TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

Caso os dados pessoais tenham a previsão de serem transferidos para outro país, a possibilidade de compartilhamento com outro Controlador deverá ser submetida à análise do Encarregado pelo Tratamento de Dados Pessoais, pela < Área de Tecnologia da Informação> e a ao Jurídico, de modo que possam avaliar se o país de destino possui grau de proteção de dados que esteja adequado ao ordenamento jurídico brasileiro.

Se o Controlador Receptor oferecer e comprovar garantias de cumprimento dos direitos do titular, a transferência internacional de dados também poderá ser possível na forma de (i) cláusulas contratuais específicas para determinada transferência; (ii) cláusulas-padrão contratuais;(iii) normas corporativas globais; e (iv) selos, certificados e códigos de conduta emitidos pela Autoridade Nacional de Proteção de Dados.

A transferência internacional de dados pessoais também pode ocorrer a partir das finalidades elencadas abaixo:

- Quando a transferência for necessária para a proteção da vida do titular ou de terceiros;
- Quando a Autoridade Nacional autorizar a transferência;
- Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional
- Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente está de outras finalidades;
- Para cumprimento de obrigação legal ou regulatória pelo **GRUPO GR**;
- Quando necessária para execução de contrato e procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

ANEXO III - CONTRATOS

O **GRUPO GR,** na figura de Controladora, sempre que fizer uso de um Operador, deve estabelecer contrato tendo em vista as regulamentações relacionadas à privacidade e proteção de dados pessoais vigentes no país onde ocorrerá o tratamento dos dados pessoais.

O **GRUPO GR,** na figura de Controladora, deve assegurar que todos os contratos que envolvam serviços e/ou sistemas nos quais haja tratamento e/ou armazenamento de dados pessoais por Operador contenham, no mínimo, os seguintes itens:

- Obrigatoriedade legal de atuar respeitando legislação vigente no local de tratamento e/ou armazenamento dos dados pessoais, em especial a Lei 13.709 ("Lei Geral de Proteção de Dados Pessoais").
- Diretrizes de tratamento:
    - Assunto do tratamento;
    - Duração do tratamento;
    - Natureza e propósito do tratamento;
    - Tipos de dados pessoais envolvidos;
    - Categorias de dados pessoais envolvidos;
    - Forma de coleta dos dados pessoais;
    - Forma de armazenamento dos dados pessoais;
    - Qualquer tipo de tratamento fora do especificado acima será considerado descumprimento do contrato.
- Procedimentos a serem tomados no caso de requisições de titulares dos dados pessoais;
- Obrigatoriedade acerca de manutenção de confidencialidade dos dados pessoais;
- Adoção de medidas de segurança técnicas e organizacionais para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais que passem por tratamento;

- Adoção de medidas de anonimização, pseudonimização (quando aplicável) e criptografia dos dados pessoais conforme a necessidade do tratamento em questão;
- Obrigatoriedade de registro das operações de tratamento de dados pessoais, conforme serviço ou contrato em questão. A exemplo de registro de tratamento de dados pessoais, devem ser armazenados, quando possível, no mínimo, as seguintes informações:
    - Ação realizada;
    - Identificação de usuários do sistema;
    - Dados de IP no momento da ação;
    - Data/hora da ação, com referência UTC (*Universal Time Coordinated*), sendo que os relógios de seus sistemas estão sincronizados com a hora legal brasileira e de acordo com o protocolo NTP (ntp.br) de sincronização dos relógios; e,
    - Identificador de sessão da conexão utilizada, quando possível.
- Adoção de medidas técnicas e organizacionais contra destruição, acidental ou ilícita, perda, alteração indevida, comunicação ou difusão não autorizada, acesso não autorizado em relação aos dados pessoais que passem por tratamento;
- Necessidade de autorização do **GRUPO GR** quanto à subcontratação de Operadores;
- Envio de relatórios sobre o monitoramento do tratamento de dados pessoais, a incluir, mas não limitado, as seguintes informações:
    - O status dos sistemas de tratamento de dados pessoais;
    - As medidas de segurança;
    - O tempo de inatividade registrado das medidas técnicas de segurança;
    - A (não) conformidade estabelecida com as medidas organizacionais;
    - Quaisquer eventuais violações de dados pessoais e/ou incidentes de segurança;
    - As ameaças percebidas à segurança e aos dados pessoais; e,

- As melhorias exigidas e/ou recomendadas.

- Notificação do **GRUPO GR** em até 24 horas sobre:
  - Qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de dados pessoais;
  - Qualquer descumprimento das obrigações contratuais relativas ao tratamento dos dados pessoais;
  - Qualquer violação de segurança na contratada ou dos demais operadores;
  - Quaisquer exposições ou ameaças em relação à conformidade com a proteção de dados pessoais.
- Fornecer informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança.
- Definição clara quando à propriedade dos dados pessoais.
- Autorização do **GRUPO GR** quanto à tratamento de dados pessoais no exterior.
- Devolução dos dados pessoais, em até 30 dias, no caso de:
  - Solicitação do **GRUPO GR**;
  - Rescisão do contrato;
  - Término do Contrato.
- Direito de regresso diante de eventuais danos causados pela contratada em decorrência de descumprimento de contrato.

ANEXO IV - RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

O relatório de impacto à proteção de dados pessoais visa a descrição dos processos de tratamento de dados pessoais e as medidas e mecanismos empregados para mitigar esses riscos pelo **GRUPO GR**.

Todo tratamento de dados pessoais tendo como hipótese legal o legítimo interesse deve ser precedido de relatório de impacto à proteção de dados pessoais.

O relatório de impacto à proteção de dados pessoais deve ser elaborado pelo Encarregado pelo Tratamento de Dados Pessoais, com o envolvimento das áreas necessárias para entendimento da elaboração deste relatório, conforme procedimento específico, e deve conter no mínimo:

- Descrição das operações de tratamento que podem gerar riscos às liberdades civis e os direitos fundamentais dos titulares dos dados;
- Finalidade das operações de tratamento de dados pessoais;
- Categorias de dados pessoais coletados;
- Existência ou não da coleta de dados pessoais sensíveis;
- Categorias de titulares dos dados pessoais
- Fontes e origens dos dados pessoais;
- Finalidade de tratamento por categoria de dado pessoal;
- Hipótese legal de tratamento.
    - Sendo a base legal o consentimento do titular dos dados pessoais, especificar forma de obtenção, armazenamento e meios de retirada do consentimento.
- Presença de tratamento de dados pessoais baseada no legítimo interesse. Havendo legítimo interesse envolvido, definir:
    - Finalidade a ser atingida com o tratamento dos dados pessoais;
    - Legitimidade da finalidade a ser alcançada;
    - Situação concreta;

- Coleta do mínimo e estritamente necessário para alcance da finalidade pretendida;
- Existência de outras bases legais que não sejam o legítimo interesse para tratamento dos dados pessoais;
- Compatibilidade do tratamento com a expectativa do titular dos dados pessoais;
- Compatibilidade do tratamento com direitos e liberdades fundamentais do titular dos dados pessoais;
- Garantia de transparência do tratamento realizado;
- Mecanismos de oposição ao tratamento de dados pessoais disponíveis ao titular dos dados pessoais;
- Medidas de mitigação de risco aplicáveis, por exemplo, anonimização dos dados pessoais a depender da finalidade a ser alcançada.

- Descrição e avaliação de risco aos titulares dos dados pessoais, estabelecendo:
  - Descrição detalhada do risco;
  - Fundamentação legal;
  - Grau do risco (alto, médio e baixo);
  - Probabilidade do risco se materializar.
- Medidas existentes para endereçar os riscos envolvidos no tratamento dos dados pessoais, incluindo:
  - Ações de mitigação;
  - Medidas de segurança da informação aplicáveis;
  - Grau do risco após a implementação das ações de mitigação e medidas de segurança da informação aplicáveis.
- Projetos e/ou funções de negócio nos quais o referido tratamento de dados pessoais está

inserido.

- Período de armazenamento e retenção dos dados pessoais.
- Medidas para adequar o tratamento às legislações existentes de tratamento de dados pessoais.

ANEXO V - SEGURANÇA DA INFORMAÇÃO

Durante todo ciclo de vida do dado pessoal devem ser observadas as diretrizes de segurança existentes na Política de Segurança da Informação e Comunicação do **GRUPO GR**.

A < Área de Tecnologia da Informação> deve assegurar a confidencialidade, integridade e disponibilidade do dado pessoal em todos os meios de armazenamento e transmissão dos dados pessoais, a partir de:

- Controles técnicos de segurança envolvidos, como:

  a) Firewall;
  b) Criptografia;
  c) Uso de VPN para acesso aos dados fora das dependências do **GRUPO GR**;
  d) Controles de acesso;
  e) Autenticação em dois fatores;
  f) Gerenciadores de senha.

- Assegurar de que somente pessoas e Agentes de Tratamento autorizados tenham acesso aos dados pessoais (em observância à necessidade e relevância da concessão do acesso);

- Adoção de medidas de segurança da informação para assegurar que os dados pessoais se mantenham íntegros (sem alterações indevidas), exatos, completos e atualizados;

- Garantia de que os dados pessoais sejam acessíveis e utilizáveis pelas pessoas e entidades autorizadas sempre que sejam necessários;

- Registro de logs e trilhas de auditoria do ciclo de vida do dado pessoal;

- Criptografia, pseudonimização e anonimização dos dados pessoais;

- Manutenção de backup e testes de restore;

- Treinamento em proteção de dados pessoais e supervisão da adoção das práticas ensinadas.

ANEXO VI - DIRETRIZES DE RESPOSTA À SOLICITAÇÕES E REQUISIÇÕES

RESPOSTA A REQUISIÇÃO DO TITULAR DOS DADOS PESSOAIS

Os procedimentos de resposta às requisições dos titulares dos dados pessoais serão regidos pelo procedimento de resposta à requisição do titular dos dados pessoais, disponível na intranet ou rede interna.

Todos os colaboradores ou prestadores de serviço têm o dever de notificar o Encarregado pelo Tratamento de Dados Pessoais, sem demora injustificada, sobre qualquer requisição recebida do titular dos dados pessoais, antes de responder a requisição, buscando, sempre que possível, orientações acerca de melhores práticas na comunicação a ser estabelecida com o titular dos dados pessoais.

Em casos de dúvida e situações específicas, o colaborador ou prestador de serviço deve encaminhar a requisição ao Encarregado pelo Tratamento de Dados Pessoais, para que este responda da forma mais adequada perante a legislação específica aplicável e às boas práticas estipuladas internamente ou observadas no mercado.

ACESSO AOS DADOS PESSOAIS PELO TITULAR DOS DADOS PESSOAIS

O titular dos dados pessoais pode requerer a qualquer momento acesso aos seus dados pessoais, devendo o colaborador ou prestador de serviço da área responsável pelo tratamento assegurar que a identidade do titular dos dados pessoais seja comprovada conforme procedimento de resposta à requisição do titular dos dados pessoais.

A requisição e posterior acesso aos dados pessoais deve ocorrer, preferencialmente, de modo eletrônico, exceto quando o titular dos dados pessoais expressamente requerer o envio dos dados pessoais de modo físico ou divulgação de modo oral.

Podem ser utilizados recursos visuais para tornar as informações ainda mais inteligíveis e de fácil compreensão.

APAGAMENTO E/OU BLOQUEIO DE TRATAMENTO DOS DADOS PESSOAIS POR REQUISIÇÃO DO TITULAR DOS DADOS PESSOAIS

O titular dos dados pessoais pode requerer a qualquer momento o apagamento e/ou bloqueio do tratamento de seus dados pessoais, devendo o colaborador ou prestador de serviço da área responsável pelo tratamento encaminhar a requisição de

apagamento/bloqueio ao Encarregado pelo Tratamento de Dados Pessoais para que possam ser adotadas as medidas conforme os procedimentos indicados no procedimento de resposta à requisição do titular dos dados pessoais.

Para apagamento de dados pessoais armazenados em backups, deve ser avaliado o custo, recursos alocados e esforço razoável para que seja feito este apagamento.

Na impossibilidade deste apagamento, o titular deve ser informado sobre esta decisão, explicando os motivos pelos quais estes dados pessoais não poderão ser apagados.

A área de TI deve estabelecer mecanismos quando da restauração de dados pessoais que impeçam que sejam restauradas ao ambiente lógico os dados pessoais de titular dos dados pessoais que tenha solicitado seu apagamento.

RESPOSTA A AUTORIDADE FISCALIZADORA

Os colaboradores ou prestadores de serviço têm o dever de notificar o Encarregado pelo Tratamento de Dados Pessoais e a Assessoria Jurídica do **GRUPO GR**, sem demora injustificada, e antes de responder à Autoridade, sobre qualquer ordem ou requisição relativa à privacidade e proteção de dados pessoais recebida de autoridade fiscalizadora.

RESPOSTA À AUTORIDADE JUDICIAL

Os colaboradores ou prestadores de serviço têm o dever de notificar imediatamente o Encarregado pelo Tratamento de Dados Pessoais e a Assessoria Jurídica do **GRUPO GR** sobre qualquer ordem ou determinação de autoridade judicial relativa a dados pessoais de que tome conhecimento.

Quando requisitado por meio de ordem judicial, caberá ao Jurídico fornecer quaisquer esclarecimentos e entregar as informações demandadas pela Autoridade, sem demora injustificada, podendo requisitar o apoio do Encarregado pelo Tratamento de Dados Pessoais caso entenda como necessário.

Caso se faça necessário o acesso a dados pessoais e informações com acesso restrito ou moderado, caberá ao Jurídico acionar o Encarregado pelo Tratamento de Dados Pessoais e as Áreas Responsáveis para que estas forneçam acesso temporário (seguindo as diretrizes estabelecidas pelas Política de Segurança da Informação), possibilitado assim o cumprimento de ordem judicial de forma tempestiva.

Quando a Autoridade determinar a necessidade de prestação de esclarecimentos, caberá ao Jurídico buscar junto ao Encarregado pelo Tratamento de Dados Pessoais e com os colaboradores ou prestadores de serviço que tenham envolvimento no fluxo de dados pessoais, solicitando relatórios, fazendo entrevistas, e buscando compilar o máximo de informações pertinentes para estruturar uma resposta adequada e concisa.