Política de **Privacidade**

DRM-RJ
DEPARTAMENTO DE RECURSOS MINERAIS

GOVERNO DO ESTADO
RIO DE JANEIRO

Cláudio Bomfim de Castro e Silva
Governador do Estado do Rio de Janeiro

Fernanda Pereira Curdi
Secretária de Estado de Desenvolvimento Econômico, Indústria, Comércio e Serviços (SEDEICS)

Luiz Claudio Almeida Magalhães
Presidente do Departamento de Recursos Minerais (DRM)

Comitê de Privacidade

Mariana Cristina Santiago Ouchana
Diretoria de Administração e Finanças

Pauline de Araújo Guimarães
Assessoria Jurídica

Nelson Oliveira dos Santos Cunha
Auditoria e DPO

Bruno Santos da Silva
Coordenadoria de Finanças

Helio Edson da Costa Britto Junior
Assessoria de Informática

Juliana Zonzin Araujo
Assessoria de Gestão de Pessoas

Marianna Pinheiro Costa
Auditoria

GOVERNO DO ESTADO RIO DE JANEIRO

DRM-RJ
DEPARTAMENTO DE RECURSOS MINERAIS

DEPARTAMENTO DE RECURSOS MINERAIS
DO ESTADO DO RIO DE JANEIRO

ELABORAÇÃO DO DOCUMENTO

Encarregado pelo Tratamento de Dados Pessoais
Nelson Oliveira dos Santos Cunha

Sumário

PREÂMBULO

Esta política tem por objetivo estabelecer conceitos, princípios, diretrizes e requisitos relacionados ao tratamento de dados pessoais no âmbito do Departamento de Recursos Minerais do Estado do Rio de Janeiro – referido daqui em diante apenas como DRM-RJ – delineando a implementação de controles e processos destinada a contínuas melhorias na seara da privacidade e proteção de dados, aculturando internamente sobre a proteção de dados pessoais.

A presente política está baseada nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27001:2022, NBR ISO/IEC 27701:2019 e NBR ISO/IEC 29100:2020, reconhecidas mundialmente como códigos de prática para a gestão da Segurança da Informação e Privacidade, bem como nas legislações vigentes, tanto no âmbito Estadual quanto no âmbito Federal, inclusive na Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), na Lei nº 12.965, de 23 de junho de 2014, denominada Marco Civil da Internet, e no Decreto nº 48.891, de 24 de Janeiro de 2024, denominado Política de Governança em Privacidade e Proteção de Dados Pessoais do estado do Rio de Janeiro.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta Política de Privacidade visa explicitar as diretrizes aplicadas no âmbito do DRM-RJ para garantir um tratamento de dados pessoais seguro e responsável, mediante observância das legislações vigentes e regulações pertinentes que versam sobre privacidade, proteção de dados pessoais e segurança da informação, assegurando os direitos conferidos aos titulares.

Art. 2º - A Política de Privacidade do DRM-RJ aplica-se a todo e qualquer servidor ou funcionário, pertencente aos quadros do órgão ou seus prestadores de serviço, nas suas diversas formas, aos fornecedores, parceiros e cidadãos, sendo cada um, no seu respectivo papel de atuação, responsável por proteger a privacidade e a integridade dos dados pessoais tratados pelo órgão, zelando pelo respeito aos princípios basilares da Proteção de Dados Pessoais, previstos na Constituição da República Federativa do Brasil, em seu art. 5º, 0 e objetiva para facilitar a compreensão de todos os envolvidos nas operações de tratamento de dados dos titulares. É dever de todos os servidores e colaboradores do DRM-RJ realizarem a leitura do documento e aplicá-lo no desempenho de suas atribuições.

SEÇÃO I
TERMOS E DEFINIÇÕES

Art. 4º - Para melhor compreensão da lei e normas a serem aplicadas é necessário conceituar os termos e definições utilizadas na atividade de tratamento de dados pessoais. Para os fins desta política, considera-se:

1. agentes de tratamento: são pessoas físicas ou jurídicas, de direito público ou privado, que realizam o tratamento de dados pessoais, podendo ser classificado como controlador ou operador;
2. anonimização: meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta Política de Privacidade visa explicitar as diretrizes aplicadas no âmbito do DRM-RJ para garantir um tratamento de dados pessoais seguro e responsável, mediante observância das legislações vigentes e regulações pertinentes que versam sobre privacidade, proteção de dados pessoais e segurança da informação, assegurando os direitos conferidos aos titulares.

Art. 2º - A Política de Privacidade do DRM-RJ aplica-se a todo e qualquer servidor ou funcionário, pertencente aos quadros do órgão ou seus prestadores de serviço, nas suas diversas formas, aos fornecedores, parceiros e cidadãos, sendo cada um, no seu respectivo papel de atuação, responsável por proteger a privacidade e a integridade dos dados pessoais tratados pelo órgão, zelando pelo respeito aos princípios basilares da Proteção de Dados Pessoais, previstos na Constituição da República Federativa do Brasil, em seu art. 5º, 0 e objetiva para facilitar a compreensão de todos os envolvidos nas operações de tratamento de dados dos titulares. É dever de todos os servidores e colaboradores do DRM-RJ realizarem a leitura do documento e aplicá-lo no desempenho de suas atribuições.

SEÇÃO I
TERMOS E DEFINIÇÕES

Art. 4º - Para melhor compreensão da lei e normas a serem aplicadas é necessário conceituar os termos e definições utilizadas na atividade de tratamento de dados pessoais. Para os fins desta política, considera-se:

I. agentes de tratamento: são pessoas físicas ou jurídicas, de direito público ou privado, que realizam o tratamento de dados pessoais, podendo ser classificado como controlador ou operador;

II. anonimização: meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

III. armazenamento: é a ação ou resultado de manter ou conservar em repositório um dado;

IV. Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) em todo o território nacional;

V. Aviso de Privacidade: é o documento em que a organização comunica a um titular ou a um grupo de titulares, como seus dados pessoais são tratados, quais são os tipos utilizados, para qual(is) finalidade(s), com quem são compartilhados, quais medidas de segurança são adotadas, por qual período, dentre uma série de outras informações responsáveis por garantir transparência para os donos dos dados pessoais;

VI. coleta: é o recolhimento de dados com finalidade específica;

VII. controlador: é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

IX. cookies: são pequenos arquivos que são salvos no computador dos usuários de internet a armazenar as preferências e outras informações usadas nas páginas da web que visitam;

X. crianças e adolescentes: considera-se criança a pessoa até 12 (doze) anos de idade incompletos, e adolescente aquela de 12 (doze) anos de idade completos até 18 (dezoito) anos de idade incompletos;

XI. dado anonimizado: dado relativo a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento;

XII. dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

XIII. dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, bem como dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural;

XIV. due diligence: procedimento prévio de avaliação em privacidade aplicado aos terceiros com os quais se pretende contratar;

XV. eliminação: é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XVI. encarregado de dados: trata-se da pessoa indicada pelo controlador ou pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

XVII. violação de dados pessoais: qualquer evento adverso confirmado que viole a segurança de dados pessoais. Estes incidentes podem incluir acesso não autorizado, acidental ou ilícito, que resulte na destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados inadequada ou ilícita;

XVIII. operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador — cujas instruções, limitações e finalidades impostas devem ser obedecidas, em conformidade com as disposições da LGPD;

XIX. Política de Privacidade: normas e processos internos que assegurem o cumprimento abrangente da legislação de proteção de dados pessoais, estabelecidos e implementados pelo agente de tratamento;

XX. pseudonimização: tratamento por meio do qual um dado 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;

XXI. titular de dado pessoal: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XXII. tratamento de dados pessoais: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle, modificação, comunicação, transferência, difusão ou extração da informação.

SEÇÃO II
PRINCÍPIOS DE PRIVACIDADE

Art. 5º - O tratamento de dados pessoais ocorrerá sempre em concordância com a boa-fé e os seguintes princípios:

I. finalidade: o tratamento de dados deverá ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II. adequação: o tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III. necessidade: o tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

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

V. qualidade dos dados: é também uma garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

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

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

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

IX. não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X. responsabilização e Prestação de Contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Art. 6º - Os princípios enumerados no art. 6º da política devem ser cumulativamente observados durante todo ciclo de tratamento de dados pessoais operacionalizado pelo DRM-RJ, norteando a atuação de todos seus servidores, terceirizados, prestadores de serviço e qualquer outra pessoa que possa tratar os dados pessoais no âmbito do DRM-RJ.

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS
SEÇÃO I DAS BASES LEGAIS

Art. 7º - O tratamento de dados pessoais deve ser realizado em observância às hipóteses legais previstas na LGPD e condicionada à persecução do interesse público, consoante dispõe o art. 23 da LGPD e o art. 7º do Decreto Estadual nº 48.891/2024. Art. 8º - É de suma importância que os titulares, por meio de canal acessível e facilitado, exerçam seus direitos (art. 18 da LGPD) e obtenham as informações relativas aos seus dados pessoais tratados no âmbito do DRM-RJ ou em razão de suas atividades, bem como as finalidades específicas, operações realizadas e duração do tratamento, salvo em casos em que haja disposição legal em sentido oposto. Parágrafo único. Nos casos em que haja tratamento de dados pessoais para fins exclusivos de Segurança Pública, segurança do estado ou em atividades de investigação e repressão de infrações penais, as regras presentes neste caput não se aplicarão, conforme o art. 4º, III da LGPD.

Art. 9º - O DRM-RJ, em relação aos tratamentos de dados pessoais realizados e os supervenientes, deverá adotar as diretrizes abaixo: § 1º Os tratamentos serão sempre enquadrados em uma das hipóteses legais de dados pessoais e dados pessoais sensíveis, enumeradas, respectivamente, no art. 7º e art. 11 da LGPD, considerando em qualquer hipótese a persecução do interesse público previsto no art. 23 da LGPD. § 2º O DRM-RJ deverá avaliar de forma prévia ao tratamento de dados pessoais que pretenda iniciar qual hipótese a autorizativa aplicável para ele. Caso haja possível risco ou dúvida quanto à legitimidade do tratamento, o encarregado poderá realizar, de maneira prévia, a Análise de Impacto à Privacidade (PIA). No caso de processos já em andamento, deverá proceder com a identificação, registro e respectivo enquadramento. § 3º Deverá ser especificada a necessidade e a finalidade específica do tratamento de dados pessoais, garantindo a aderência aos princípios da adequação e da transparência. § 4º A finalidade específica deve ser indicada e pautada em fundamentações claras e legítimas, a partir de situações concretas, e somente serão tratados os dados estritamente necessários para essa finalidade. § 5º O DRM-RJ deverá assegurar que os tratamentos de dados pessoais estejam em conformidade com a legislação aplicável e contenham uma base legal adequada. § 6º O titular dos dados pessoais deverá ser comunicado sobre a nova finalidade de tratamento, antes do momento em que a informação for tratada ou usada pela primeira vez para um novo objetivo. § 7º Nos comunicados direcionados a qualquer tipo de titular de dados, internos ou externos, o DRM-RJ deverá utilizar uma linguagem clara e apropriada, que seja de fácil entendimento do titular. § 8º O DRM-RJ deverá seguir as diretrizes expostas no art. 14 da LGPD para o tratamento de dados pessoais de crianças e adolescente. Assim, deve-se avaliar, de forma prévia, qual é a hipótese autorizativa aplicável ao tratamento de dados pessoais de menores de idade e as condições para que isso ocorra, sempre zelando pela proteção desse grupo de titulares.

SEÇÃO II
DO DIREITO DOS TITULARES

Art. 10 - O titular do dado pessoal tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva. O DRM-RJ deverá atender as solicitações dos titulares de dados, garantindo o exercício dos direitos abaixo elencados:

I. acesso: o DRM-RJ deverá garantir o acesso ao titular dos dados pessoais sempre que solicitado, informando qual meio necessário para solicitação, como será a validação da sua identificação para requisição e definindo um prazo para atendimento;

I. acesso: o DRM-RJ deverá garantir o acesso ao titular dos dados pessoais sempre que solicitado, informando qual meio necessário para solicitação, como será a validação da sua identificação para requisição e definindo um prazo para atendimento;

II. confirmação de tratamento de Dados: o DRM-RJ, sempre que solicitado, deverá confirmar, caso ocorra, a existência de tratamento de dados pessoais ao seu titular;

III. correção de dados: o DRM-RJ, sempre que solicitado, deverá realizar a correção de dados incompletos, inexatos ou desatualizados;

IV. anonimização, bloqueio ou eliminação: o DRM-RJ, independente de provocação, mas sempre que solicitado, deverá anonimizar, bloquear ou eliminar dados desnecessários, excessivos ou tratados em desconformidade com a lei;

V. portabilidade de dados: o DRM-RJ precisará realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa pelo usuário;

VI. eliminação de dados: sempre que solicitado pelo titular e não havendo disposição legal contrária que exija a sua manutenção, o DRM-RJ deverá realizar a eliminação dos dados tratados que tiveram o consentimento como hipótese legal de tratamento;

VII. informações sobre compartilhamento: o titular obterá informações sobre os terceiros com as quais o DRM-RJ compartilhar os seus dados;
VIII. não fornecimento do consentimento: o titular deverá ser informado sobre a possibilidade de não fornecer o consentimento, bem como sobre as consequências em caso de negativa;
IX. revogação: nos casos de tratamentos embasados no consentimento, o titular poderá, sempre que desejar, revogar o consentimento.

SEÇÃO III DO TRATAMENTO DE DADOS PESSOAIS

Art. 11 - A LGPD, em seu art. 5º, inciso X, considera tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".
Art. 12 - Para realizar o tratamento de dados pessoais, o DRM-RJ deverá verificar se há alguma hipótese legal que os autorize, devendo também avaliar previamente cada novo caso de tratamento que pretenda realizar, identificando as hipóteses legais autorizativas aplicáveis, documentando aquelas que forem aplicadas.
Art. 13 - O consentimento será considerado nulo, caso as informações fornecidas ao titular sejam genéricas, tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
Art. 14 - Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o titular deverá ser informado previamente sobre as mudanças de finalidade, podendo revogar o consentimento, caso discorde com as alterações.

Art. 15 - Independente do enquadramento em uma ou mais hipóteses legais, o tratamento deverá seguir os princípios expostos na LGPD, sob pena de ser considerado irregular.

Art. 16 - As medidas técnicas e administrativas que serão adotadas para proteger os dados pessoais também deverão ser registradas.

Art. 17 - As medidas que serão adotadas para prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção) deverão ser identificadas e registradas

SEÇÃO IV
DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Art. 18 - A lei autoriza o tratamento de dados sensíveis apenas em situações indispensáveis. Isso traz para o controlador o ônus da prova da alegada indispensabilidade. Ademais, é necessário que o DRM-RJ conheça as hipóteses para tratamento de dados pessoais sensíveis:

I. consentimento fornecido pelo titular através da manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

II. cumprimento de obrigação legal ou regulatória pelo controlador;

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

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

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

VI. proteção da vida ou da incolumidade física do titular ou de terceiros;

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

VII. 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.

SEÇÃO V
MINIMIZAÇÃO DE DADOS COLETADOS

Art. 19 - O DRM-RJ realizará os tratamentos de dados pessoais respeitando o princípio minimização de dados, sempre restringindo o tratamento dos dados pessoais à finalidade específica.

Art. 20 - É imprescindível conceber e implementar procedimentos necessários, minimizando os dados tratados e o número de partes interessadas e ainda, as pessoas a quem são divulgados os dados pessoais ou quem tem permissão para tratá-los.

Art. 21 - O DRM-RJ deverá usar ou oferecer como opções-padrão, sempre que possível, interações e transações que não envolvam a identificação de titulares de dados pessoais, reduzam seus comportamentos e limitem a vinculação de dados pessoais coletados.

Art. 22 - O descarte dos dados pessoais deverá ser tecnicamente realizado após o término de seu tratamento, em atendimento ao previsto no art. 16 da LGPD.

SEÇÃO VI
ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Art. 23 - Segundo a LGPD, dado anonimizado é o dado que, considerados os meios técnicos razoáveis no momento do tratamento, perde a possibilidade de associação, direta ou indireta, a um indivíduo. Portanto, não incide a LGPD.Art. 24 - A pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso, por exemplo, de chave criptográfica, mantida separadamente em ambiente controlado e seguro, nos moldes do art. 13, § 4º da LGPD. O dado pseudonimizado é considerado dado pessoal para fins de incidência da LGPD.

SEÇÃO VII
TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

Art. 25 - A LGPD determina, em seu art. 14, que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse. Requerendo para tanto, um consentimento específico e em destaque, dado por ao menos um dos pais ou pelo responsável legal. As hipóteses que dispensam o consentimento mencionado acima ocorrem quando:

I. a coleta for necessária para contatar os pais, ou o responsável legal, ou, ainda, para a própria proteção da criança ou adolescente – nesses casos, os dados deverão ser utilizados uma única vez, vedados o armazenamento e o seu repasse a terceiros;

II. o tratamento de dados for imprescindível para o exercício de direitos da criança ou adolescente ou para lavratura de registros públicos.

Parágrafo único. Nos casos em que os dados pessoais de crianças e adolescentes forem tratados para os fins exclusivos de Segurança Pública, segurança do estado ou atividades de investigação e repressão de infrações penais, as exigências aqui elencadas não serão aplicáveis, não excluída, entretanto, a conformidade aos princípios gerais de proteção e os direitos do titular previstos no art. 4º, § 1º, da LGPD

SEÇÃO VI
DA COLETA

Art. 26 - O DRM-RJ deverá fornecer informações que permitam que os titulares de dados pessoais entendam quais elementos de dados pessoais estão sendo coletados, aderindo 15 ao princípio da necessidade, limitando a coleta dentro do limite da lei aplicável e estritamente necessário e para os objetivos especificados.

Art. 27 - Os dados não deverão ser coletados indiscriminadamente. A quantidade e os tipos de dados coletados devem ser limitados ao necessário para cumprir os objetivos especificados pelo controlador.

Art. 28 - O DRM-RJ documentará todo dado pessoal coletado, bem como sua justificativa para fazê-lo e práticas de manuseio de informações.

Art. 29 - Os dados pessoais serão coletados por meios éticos e legais e armazenados em ambiente seguro e controlado, pelo prazo exigido pela lei ou regulamentação vigente.

Art. 30 - O DRM-RJ fornecerá as informações que permitam que os titulares entendam quais elementos de dados pessoais estão sendo coletados, mesmo quando a coleta de elementos particulares de dados pessoais.

SEÇÃO VII
DO AVISO DE PRIVACIDADE

Art. 31 - O Aviso de Privacidade é o documento de comunicação que direciona informações quanto ao tratamento de dados pessoais aos titulares de uma categoria específica. Exemplos: servidores, cidadãos atendidos, representantes de parceiros comerciais ou institucionais, prestadores de serviço, dentre outros.

Art. 32 - Os Avisos de Privacidade deverão ser ofertados à ciência dos titulares nos canais de comunicação, locais físicos e sistemas do DRM-RJ em que ocorram coleta de dados pessoais. No caso de dados pessoais recebidos por compartilhamento vindo de outros órgãos, instituições ou empresas, o DRM-RJ deverá se certificar de que a comunicação ao titular quanto a esse compartilhamento foi feita de maneira efetiva.

§ 1º Os Avisos de Privacidade deverão abordar os seguintes tópicos:

I. introdução e propósito: breve explanação sobre o propósito do aviso e a importância da proteção de dados pessoais;

II. informações de contato: detalhes de contato do órgão responsável pela coleta e processamento dos dados pessoais;

III. dados coletados: lista dos tipos de dados coletados, incluindo exemplos específicos, como nome, endereço, e-mail, dentre outros;

IV. finalidades da coleta: apresentação das razões pelas quais os dados são coletados e como serão utilizados;

V. bases legais: descrição das bases legais nas quais a empresa se baseia para processar os dados pessoais;

VI. compartilhamento de dados: informações sobre como e com quem os dados pessoais são compartilhados;

VII. transferências internacionais: informações sobre o envio ou recebimento de dados pessoais de agentes de tratamento fora do Brasil;

VIII. segurança de dados: descrição das medidas de segurança implementadas para proteger os dados pessoais contra acesso não autorizado, uso indevido, perda ou alteração etc.

IX. retenção de dados: informações sobre quanto tempo os dados pessoais serão mantidos e os critérios usados para determinar o período de retenção;

X. direitos do titular dos dados: lista com os direitos que os titulares dos dados têm em relação aos seus dados pessoais tratados;
XI. contatos e canais de comunicação: apresentação dos contatos do encarregado de dados e dos canais para requisições dos titulares de dados pessoais;
XII. alterações no Aviso de Privacidade: informação aos titulares quanto à possibilidade de alteração do Aviso de Privacidade e como eles serão informados quanto a essas alterações.

SEÇÃO VIII
DA TRANSFERÊNCIA, DO USO COMPARTILHADO E DO COMPARTILHAMENTO DE DADOS PESSOAIS

Art. 33 - Devido à natureza da atividade exercida pelo DRM-RJ é possível o compartilhamento de dados pessoais. Na distribuição ou divulgação dos dados pessoais para dentro e para fora da fase de compartilhamento é preciso mapear os ativos envolvidos do DRM-RJ.
Art. 34 - O compartilhamento de dados do DRM-RJ deverá atender as finalidades específicas e base legais que justificam o tratamento.
Art. 35 - O DRM-RJ deverá observar o princípio da segurança, previsto no art. 6º, VII da LGPD, as ferramentas a serem contratadas e/ou desenvolvidas deverão assegurar a adoção de medidas técnicas aptas a garantir a proteção dos dados pessoais, bem como a privacidade dos titulares.
Art. 36 - O DRM-RJ somente poderá transferir ou receber dados pessoais em que haja a celebração de um contrato ou outro instrumento formal vinculante com o terceiro participante do tratamento conforme disposto no art. 23, inciso IV da LGPD.
Art. 37 - A transferência, o uso compartilhado e o compartilhamento de dados pessoais com outros entes públicos atenderão a finalidades específicas de execução de políticas públicas e de exercício das suas atribuições legais. Portanto, deverão respeitar os princípios de proteção de dados pessoais e os direitos dos titulares previstos na LGPD.

SEÇÃO IX
DA GESTÃO DE TERCEIROS

Art. 38 - Ao trabalhar com um terceiro (fornecedor ou parceiro), a respectiva área do DRM-RJ deverá celebrar um instrumento formal que regule a relação entre as partes, incluindo as boas práticas e adequação a LGPD. Ao selecionar terceiros, o DRM-RJ deverá atentar as seguintes boas práticas:

I. avaliação quanto ao fornecimento, pelo terceiro, de medidas de segurança técnica e organizacional necessárias para realizar um tratamento em conformidade com todas as leis de proteção de dados aplicáveis;
II. elaboração de contrato escrito ou documentado de outra forma que defina inequivocamente os direitos e obrigações do Controlador e do Operador (para verificar a definição desses, consulte nossa Cartilha) que estejam em conformidade com as leis aplicáveis de proteção de dados;
III. exigência do DRM-RJ para que os terceiros tratem os dados pessoais com o mesmo nível de seriedade que o órgão executa as suas atividades de tratamento.
Art. 39 - Dentro dos processos de Gestão de Terceiros, o DRM-RJ poderá aplicar questionários de due diligence para avaliação de seus parceiros comerciais. Além disso, o DRM-RJ deverá programar auditorias recorrentes para serem aplicadas aos terceiros contratantes com o órgão. O objetivo é manter um acompanhamento constante quanto a implementação e execução de boas práticas de segurança e privacidade por estes órgãos, instituições ou empresas.

SEÇÃO X
PRAZO DE RETENÇÃO DE DADOS PESSOAIS

Art. 40 - O DRM-RJ deverá manter os dados pessoais armazenados em concordância com os prazos legais e em consonância com os Princípios da Necessidade e da Finalidade elencados no art. 6º da LGPD. Para isto, deverá atentar-se as seguintes orientações:
I. se o armazenamento não for necessário para a finalidade e não houver obrigação legal de mantê-los, os dados deverão ser excluídos de acordo com a finalidade relacionado ao processo de tratamento;
II. o armazenamento pelo DRM-RJ será definido por períodos estabelecidos por leis e regulações aplicáveis às atividades exercidas;
III. pelo tempo necessário para o exercício regular de direitos em processos judiciais e administrativos;
IV. o DRM-RJ também pode manter dados pessoais de forma anonimizada, ou seja, sem que estejam ou possam ser relacionados a um titular de dados, por períodos maiores, para análise estatística e pesquisa.
Art. 41 - Para tanto, o DRM-RJ implementará uma Política de Retenção de Dados Pessoais e dará publicidade para os responsáveis pela gestão e armazenamento deles. A Política de Retenção de Dados Pessoais deverá, dentre outros, abordar os seguintes

I. finalidade da retenção;
II. legislação e regulamentações;
III. categoria dos dados retidos;
IV. métodos de armazenamento;
V. período de retenção;
VI. processos de exclusão;
VII. transparência e consentimento;
VIII. responsabilidade e prestação de contas.

SEÇÃO XI
DAS TRANSFERÊNCIAS INTERNACIONAIS

Art. 42 - A transferência internacional de dados consiste no envio ou recebimento de dados pessoais para empresas, órgãos ou instituições localizadas fora do território brasileiro.
Art. 43 - Para que as transferências ocorram, o DRM-RJ comunicar de forma prévia e clara ao titular quais dados pessoais serão transferidos e para quais finalidades. Ainda, informará quais países estarão envolvidos e o grau de proteção que eles oferecem ao mesmo.
Art. 44 - Ademais, o DRM-RJ deverá comprovar a garantia dos princípios e direitos do titular durante todo este tratamento, tendo, como análise importante, a avaliação quanto à legislação que deverá ser igual ou superior aos apresentados pela LGPD.
Art. 45 - O controlador poderá oferecer e comprovar garantias de cumprimento dos princípios, por meio do uso de cláusulas contratuais especificas para transferência, cláusulas padrão contratuais, normas corporativas globais, selos e certificados de conduta emitidos.

CAPÍTULO III
DA GESTÃO DOS DADOS PESSOAIS
SEÇÃO I
MEDIDAS DE SEGURANÇA

Art. 46 - O DRM-RJ deverá adotar as medidas de segurança técnicas e administrativas necessárias para realizar o tratamento de dados pessoais, oferecendo segurança ao titular, protegendo os dados pessoais, sob sua autoridade, com controles apropriados nos níveis operacionais, funcional e estratégico, a fim de assegurar a integridade, confidencialidade e disponibilidade dos dados pessoais. Para além destas medidas, deverá proteger contra riscos de acesso não autorizado, destruição, uso, modificação, ou divulgação não autorizados por todo o seu ciclo de vida.

Art. 47 - Para tanto, o DRM-RJ deverá elaborar e manter atualizada à sua realidade a sua Política de Segurança da Informação, formulada de acordo com as boas práticas internacionais sobre o tema, em especial a ABNT NBR ISO 27001 e 27701, baseando ainda, os seus controles em requisitos legais aplicáveis, normas de segurança, resultados de análises de riscos sistêmicos, como descrito na ABNT NBR ISO 31000.

Art. 48 - O DRM-RJ deverá formular um procedimento de avaliação de terceiros, para que a escolha dos operadores de dados pessoais seja pautada em evidências que atestem a aplicação de controles organizacionais e adequação à LGPD no mesmo nível do DRM-RJ.

Art. 49 - O acesso aos dados pessoais deverá ser feito apenas por aqueles que necessitam deles para o cumprimento de suas obrigações, a fim de executar as funções que desempenham.

Art. 50 - O DRM-RJ deverá elaborar um plano para aplicação de auditorias recorrentes, a fim de identificar e solucionar os riscos e vulnerabilidades descobertos pelas avaliações de riscos de privacidade e proteção de dados pessoais.

Art. 51 O - DRM-RJ deverá elaborar e implementar planos e procedimentos para gestão e tratamento de violação de dados pessoais, bem como criar um canal para receber notificações de possíveis incidentes de segurança e/ou privacidade.

SEÇÃO II
AVALIAÇÃO DE RISCOS DE PRIVACIDADE

Art. 52 - A avaliação de risco de privacidade é um processo realizado para identificar e avaliar riscos específicos de privacidade e proteção de dados pessoais.

Art. 53 - O DRM-RJ deverá definir a metodologia de risco que irá empregar em suas operações, pautando-a em frameworks consolidados no mercado, como a ISO 27001, 27002 e 27701, bem como o NIST Privacy Framework, dentre outros.

Art. 54 - A metodologia deverá ser aplicada para avaliar os riscos nas operações de tratamento de dados pessoais, para que as possíveis vulnerabilidades sejam identificadas e respectivos controles sejam implementados.

SEÇÃO III
POLÍTICAS DE COOKIES

Art. 55 - O DRM-RJ deverá adotar como boa prática a Política de Cookies. Trata-se de uma ferramenta importante para fornecer informações sobre atividade on-line dos titulares.

Art. 56 - Desta forma, o DRM-RJ deverá sinalizar na Política de Cookies quais cookies são utilizados (cookies proprietários e terceiros); quais dados são coletados pelos cookies; qual finalidade do uso dos cookies; e como o usuário pode obter mais informações sobre os cookies de terceiros utilizados no serviço.
Art. 57 - Recomenda-se que a referida política seja informada para o titular de dados pessoais, por meio de uma janela pop-up, ao acessar o serviço/site. A política deverá disponibilizar a opção de desabilitar a coleta de cookies conforme sua preferência, salvo aqueles estritamente necessários. Além disso, a política deverá identificar as bases legais utilizadas, de acordo com cada finalidade/categoria de cookie, utilizando o consentimento como principal base legal, exceção feita aos cookies estritamente necessários, que podem ter como base as outras hipóteses legais.
Art. 58 - A política também deverá fornecer informações precisas e específicas sobre os dados que cada cookie rastreia, bem como sobre sua finalidade, em linguagem simples e, quando for o caso, antes que o consentimento seja recebido.
Art. 59 - Nos casos em que o consentimento for a base legal utilizada para a coleta de cookies e posterior tratamento dos respectivos dados, o DRM-RJ deverá documentar e armazenar o consentimento recebido dos usuários. A revogação do consentimento deverá ser tão fácil quanto sua concessão.
Art. 60 - Os usuários deverão poder acessar os serviços, mesmo quando recusarem a coleta de cookies não considerados como estritamente necessários.

SEÇÃO IV
CONSCIENTIZAÇÃO E CAPACITAÇÃO

Art. 61 - O DRM-RJ deverá dispor de um Plano de Conscientização e capacitação dos seus colaboradores e terceiros da organização na temática de proteção de dados pessoais e privacidade nos moldes previstos na LGPD, a fim de ampliar cada vez mais a cultura do respeito à privacidade e à proteção de dados pessoais.
Art. 62 - Os colaboradores que possuírem acesso aos dados pessoais tratados pelo DRM-RJ deverão participar continuamente de programas de conscientização, cujos eventos deverão possuir listas de chamada para conferência.

SEÇÃO V
TEMPORALIDADE

Art. 63 - Esta política deverá ser revisada e atualizada sempre que necessário ou, obrigatoriamente, no prazo de um ano a contar da data da sua última publicação, a fim de garantir a contínua evolução do Programa de Privacidade do DRM-RJ.