

DetranRS EM DEFESA DA VIDA



GOVERNO DO ESTADO
RIO GRANDE DO SUL

PROGRAMA DE GOVERNANÇA EM **PRIVACIDADE**



PROGRAMA DE GOVERNANÇA EM **PRIVACIDADE**



EM DEFESA DA VIDA
DetranRS



SUMÁRIO EXECUTIVO

O presente documento apresenta o roteiro de atividades a serem realizadas pelas Diretorias do DETRANRS para a implementação do Programa de Governança em Privacidade no Departamento Estadual de Trânsito do Estado do Rio Grande do Sul – DETRANRS , em conformidade com o disposto na Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018).

Este Programa de Governança em Privacidade deverá ser validado previamente na Alta Administração do DETRANRS e complementado pelo Conselho de Implementação da LGPD no Poder Executivo do Estado do Rio Grande do Sul, cuja formação foi prevista no Decreto Estadual 50.5647/2020.

Tendo sua construção baseada no Guia de Elaboração de Programa de Governança em Privacidade do Grupo de Trabalho sobre a Implementação da LGPD no Poder Executivo do Estado do RS e levando em consideração a estrutura organizacional do Departamento Estadual de Trânsito do Estado do Rio Grande do Sul - DETRANRS , tem por objetivo construir um fluxo de trabalho que se adeque à nossa realidade, na condição de Órgão Executivo Estadual de Trânsito.

Reportamos que o DETRANRS , como agente de tratamento de dados controlador, trata dados pessoais e dados pessoais sensíveis nos bancos de dados transversais nacionais do RENACH, RENAAM e RENAINF, este último por delegação legal do CONTRAN. Possui ampla rede de credenciados (CRDs, CRVAs e CFCs) na condição de agente de tratamento de dados pessoais operadores, devido ao previsto no escopo do órgão em atender as diretrizes legais de sua competência previstas no Código de Trânsito Brasileiro.

Contemplam o Programa de Governança em Privacidade do DETRANRS três etapas principais, a saber:

I - Etapa de Preparação da Estratégia de Proteção de Dados

1. Designação do Encarregado de dados pessoais
2. Composição do Grupo Focal de Trabalho
3. Treinamento e Conscientização

4. Inventário dos Dados Pessoais
5. Diagnóstico de Maturidade Inicial
6. GAP Analysis (análise de lacunas)
7. Levantamento de Contratos

II – Etapa de Execução: Documentos e Implementação do Programa

1. Política de Privacidade
2. Aviso de Privacidade
3. Relatório de Impacto de Proteção de Dados
4. Plano de Resposta a Incidentes
5. Implementação do Programa

III – Etapa de Monitoramento do Programa

1. Indicadores de Desempenho
2. Gestão de Incidentes

DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Conforme define a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018), na sua Seção II (Das Boas Práticas e da Governança), art. 50, §2º, I, o Controlador poderá implementar Programa de Governança em Privacidade, observada a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados se houver vulnerabilidades não minimizadas e corrigidas. Objetivando:

- a) demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- b) ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- c) ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- d) estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- e) ter o objetivo de estabelecer relação de confiança com o titular de dados, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- f) estar integrado à estrutura geral de governança da DETRAN, além de estabelecer aplicar mecanismos de supervisão internos e externos;
- g) contar com planos de resposta a incidentes e remediação; e
- h) ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.
- i) Estabelecer dinâmicas e rotinas entre as Diretorias do DETRANRS para dar aos dados fluxos e controles quando a proteção e privacidade."

O Programa de Governança em Privacidade (PGP) define diretrizes para a gestão da segurança do tratamento dos dados pessoais no âmbito do DETRAN, nos meios físicos e

digitais, em tratamentos manuais ou automatizados, em gestão de processos e pessoas, com o propósito de proteger a privacidade dos titulares de dados pessoais.

O presente PGP norteará as ações do DETRANRS no sentido de permitir a melhoria do nível de maturidade e de conformidade à Lei Geral de Proteção de Dados Pessoais (LGPD), além de buscar contribuir com a implementação do PGP no âmbito de todo Estado do Rio Grande do Sul. A seguir detalham-se as etapas do Programa de Governança em Privacidade a serem implementadas, sob a coordenação do encarregado.

I - ETAPA DE PREPARAÇÃO DA ESTRATÉGIA DE PROTEÇÃO DE DADOS

A etapa de Preparação busca analisar e mapear todas as áreas e atividades que envolvam o tratamento de dados pessoais na Autarquia. Nesta etapa, é realizado o diagnóstico daquilo que já tem sido feito na proteção dos dados pessoais e o que ainda deverá ser realizado para definir a estratégia de adequação à Lei Geral de Proteção de Dados Pessoais.

Durante o desempenho desta fase torna-se imprescindível captar o maior número de informações, com máxima precisão, de forma a entender a operacionalização do agente de tratamento, tendo o DETRANRS como controlador e garantindo maior assertividade na implantação.

Este é o momento de entender o perfil das atividades e dos servidores e credenciados, a finalidade do tratamento de dados pessoais, o tipo de dado pessoal tratado, os fluxos de trabalho, as falhas de segurança e, principalmente, identificar as dificuldades e os problemas enfrentados no tratamento de dados pessoais, através dos seguintes marcos:

1. Designação do Encarregado de Dados Pessoais

Em publicação no DOE de 02/06/2021 o servidor Márcio Pires Berr, analista direito, ID 3044068, pela Portaria DETRANRS 175/2021 foi designado como Encarregado pelo Tratamento dos Dados Pessoais, do Departamento Estadual de Trânsito do Estado do Rio Grande do Sul – DETRAN-RS, com sua qualificação e contatos divulgados no site da Autarquia.

2. Composição do Grupo de Trabalho

O Governo do Estado do Rio Grande do Sul, por força do Decreto nº 55.647/2020, em seu art. 9º, instituiu o Grupo de Trabalho que está conduzindo a implementação da LGPD em todos os órgãos estaduais. O Grupo de trabalho estadual tem como objetivo principal propor ao Conselho de Implementação da LGPD no Poder Executivo Estadual as diretrizes,

projetos, ações e metas estratégicas para a adequação do tratamento de dados pessoais realizado no âmbito da administração pública estadual, observados os regulamentos da Autoridade Nacional de Proteção de Dados - ANPD.

O DETRANRS pela complexidade das tarefas afeitas ao tema, nomeou grupo focal multidisciplinar de apoio ao Encarregado de DETRANRS de Dados Pessoais, conforme Portaria DETRAN-RS 186/2021, publicada no DOE em 23/06/2021.

3. Treinamento e Conscientização da Equipe de Trabalho

A Diretoria Administrativa e Financeira do DETRANRS , mais precisamente a Divisão de Recursos Humanos, deve manter treinamentos constantes de servidores e estagiários quanto às diretrizes da LGPD, decretos estaduais sobre o tema e principalmente acerca da PORTARIA DETRANRS nº 286/2021, publicada no DOE em 13/10/2021, que cuida da política de proteção de dados pessoais e avisos aos usuários, tendo o Encarregado de Tratamento de Dados como articulador do programa de treinamento.

Da mesma forma, a Divisão de Tecnologia da Informação - DTI deve ser capacitada para a implementação de medidas técnicas de segurança que protejam os dados pessoais tratados no âmbito da Autarquia

Aos responsáveis pelo atendimento direto ao titular de dados, como Ouvidoria-Geral e Assessoria de Comunicação - ACS do DETRANRS devem compreender bem o Programa de Governança em Privacidade, para que possa resultar, com a supervisão e interação constante com o Encarregado de Tratamento de Dados e do grupo focal, em ações de conscientização voltadas a boas práticas em governança, proteção de dados e o correto cumprimento da LGPD.

O Encarregado pelo Tratamento de Dados também deve participar e ministrar treinamentos, tanto aos representantes do controlador DETRANRS , como estagiários e servidores, bem como para os credenciados, terceirizados e demais vinculados ao DETRANRS . Os métodos de treinamento e conscientização podem variar e incluir

curso de capacitação presenciais, e-learning, reuniões com as equipes, boletins informativos, e-mails, posteres, folhetos, slogan e informações no portal eletrônico.

No âmbito estadual, temos o Decreto que regulamenta os prazos para a implementação da LGPD no Poder Executivo Estadual. O art. 12 previa a primeira fase de workshops, que foram concluídas e encerradas com o treinamento e a conscientização dos encarregados em 31 de julho de 2021. Durante a capacitação, os encarregados foram familiarizados com os conceitos trazidos na LGPD e na documentação necessária que cada órgão deve produzir para implementar efetivamente a LGPD em suas estruturas e procedimentos administrativos.

A Escola de Governo do Rio Grande do Sul passou a executar as avaliações de conformidade à LGPD, segundo padrão metodológico desenvolvido pela Secretaria de Planejamento, Governança e Gestão (SPGG), com o suporte da Procuradoria-Geral do Estado (PGE).

Até o momento, foram realizadas diversas reuniões técnicas no Grupo de Trabalho (GT) de implementação da LGPD, no âmbito do Poder Executivo Estadual, contando com 467 participações, entre ao vivo e gravadas. O GT prossegue com as reuniões de trabalho e orientação para a rede de todos os encarregados do Poder Executivo Estadual¹. Sendo que o Encarregado do DETRANRS já realizou o treinamento completo ministrado e relatado acima.

4. Mapeamento de dados pessoais

O mapeamento de dados pessoais ou “inventário de dados”, já confeccionado pelo DETRANRS, é uma planilha eletrônica que contempla como é realizado o tratamento de dados pessoais dentro da DETRAN. O IDP permite identificar áreas-chave, papéis e responsabilidades para o Programa de Governança em Privacidade.

¹ Consulta em 19/08/2021. Disponível em: <https://www.pge.rs.gov.br/pge-encerra-serie-de-workshops-para-capitacao-em-protacao-de-dados-pessoais>

O inventário deve e está organizado em torno do ciclo de vida dos dados - coleta, uso, transferências, retenção e destruição. Idealmente, deve contemplar todas as atividades de tratamento previstas na LGPD (coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração).

Algumas perguntas que o inventário de dados deve responder de forma atualizada são:

- a) Que categorias de dados pessoais são tratadas?
- b) Qual a finalidade do tratamento?
- c) Qual o contexto do tratamento?
- d) Qual a origem e destino dos dados pessoais?
- e) Qual o volume de dados pessoais armazenados?
- f) Por quanto tempo os dados pessoais são armazenados?
- g) Qual o formato dos dados? Estão armazenados de forma estruturada ou não estruturada?
- h) Com quem os dados pessoais são compartilhados (interna e externamente)?

O IDP do DETRANRS foi realizado individualmente, diante da especificidade, por cada Divisão e deve sofrer atualizações periódicas, conforme prevê a Portaria DETRANRS 286/2021, podendo ser visto na rede interna do DETRAN, pasta Y, comissões, DPO, PGP.

5. Diagnóstico de Maturidade Inicial

O Diagnóstico de Maturidade tem por objetivo fazer um levantamento do “status” em que se apresenta o órgão em relação à sua adequação com a LGPD. O Diagnóstico de maturidade Inicial, realizado pela DETRANRS para adequação à LGPD.

6. GAP Analysis (análise de lacunas)

Outra etapa para análise da realidade organizacional é entender qual a situação do atual

do gerenciamento de privacidade e proteção de dados pessoais frente às legislações aplicáveis, identificando as lacunas legais. Essa análise permite identificar quais lacunas existem para a correta adequação às legislações aplicáveis.

As operações de tratamento devem ser identificadas e avaliadas ao longo de todo o DETRAN, e uma boa prática é a identificação de riscos e deficiências, bem como a identificação de recomendações para saná-los. De forma similar ao inventário de dados, planilhas que identificam práticas vigentes também são bastante importantes.

Algumas das perguntas que esse segundo mapeamento pode contemplar, levantadas pela DETRANRS, seriam com base nos artigos da LGPD, os abaixo colocados:

- a) Qual a base legal para o tratamento dos dados pessoais (art. 7º da LGPD)?
- b) Existem dados pessoais sensíveis sendo tratados (art. 11º)?
- c) Se sim, quais as bases legais e quais as medidas de segurança para sua proteção adicional?
- d) Existem dados pessoais de crianças e adolescentes sendo tratados (art. 14º)? Há necessidade de consentimento parental? Quais as medidas para confirmar a obtenção desse consentimento?
- e) Quais os procedimentos para eliminação de dados pessoais? Quais as exceções legais aplicáveis para armazenamento de dados além do período pré-estabelecido (art. 16)?
- f) Quais os procedimentos que permitam aos titulares de dados serem informados e exercerem seus direitos (art. 18)?
- g) As regras para tratamento de dados pessoais pelo poder público são cumpridas (arts. 23 a 27)?
- h) Há operações de transferência internacional de dados pessoais? Se sim, para onde são enviados, quais as entidades envolvidas, qual o procedimento? Qual a base legal para a transferência internacional (art. 33)?
- i) Existe registro das operações de tratamento de dados pessoais? Como esse registro é atualizado (art. 37)?
- j) Foi realizada uma análise de riscos preliminar das operações de tratamento? Há

necessidade de elaboração de um Relatório de Impacto de Proteção de Dados (art. 38)? Este relatório foi elaborado?

- k) Existe encarregado de proteção de dados pessoais? Quais suas competências (art. 41)?
- l) Quais medidas de segurança, técnicas e administrativas são adotadas para proteger os dados pessoais de acessos não autorizados e outras situações acidentais ou ilícitas - destruição, perda, alteração, comunicação, tratamento inadequado ou ilícito (art. 46)?
- m) Quais os procedimentos para responder a incidentes de segurança/vazamento de dados pessoais (art. 48)?

7. Levantamento de Contratos

Além do mapeamento de todas as atividades cotidianas das divisões do DETRANRS, faz-se necessário realizar um levantamento dos contratos firmados pelo DETRANRS. No decorrer do processo, todos os contratos e convênios analisados deverão ser aditados e apostilados para que passem a incluir obrigações com a LGPD e boas práticas de governança e proteção de dados.

II - ETAPA DE EXECUÇÃO: DOCUMENTOS E IMPLEMENTAÇÃO DO PROGRAMA

A etapa de Execução compreende a elaboração dos Documentos de Privacidade e a implementação do Programa de Governança em Privacidade. Embora a LGPD não exija a criação do Programa de Governança em Privacidade, ela o recomenda aos operadores e controladores, sendo que os decretos estaduais obrigam que o DETRANRS tenha o seu PGP.

O programa prevê métodos, regime de funcionamento, procedimentos de garantia à proteção de dados, normas de segurança, padrões técnicos, ações educativas e medidas de fiscalização interna. Esta etapa busca promover o gerenciamento de direitos individuais, o consentimento e a redução de responsabilidade por violação dos dados².

Neste roteiro, os seguintes documentos são destacados:

- a) política de privacidade, de uso interno;
- b) aviso de privacidade, para usuários externos;
- c) relatório de impacto de proteção de dados - RIPD;
- d) plano de resposta a incidentes;
- e) plano de treinamento e conscientização de colaboradores.

No âmbito do Estado do Rio Grande do Sul, nos termos do Decreto nº 55.987/2021, que instituiu a política de proteção de dados no Poder Executivo, tem-se a previsão de que haverá uma plataforma tecnológica transversal, à cargo da Secretaria de Planejamento, Governança e Gestão, para a governança dos dados pessoais³. Mas no hiato para a

² Lei 12.527/2011 (Lei de Acesso à Informação):

Art. 7º O acesso à informação de que trata esta Lei compreende, entre outros, os direitos de obter: [...]

VI - informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; [...]

Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas [...]

IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;

³ **Art. 6º** A Secretaria de Planejamento, Governança e Gestão - SPGG, providenciará plataforma tecnológica transversal para a governança dos dados pessoais no âmbito da administração pública direta, autárquica e fundacional, de modo que se possa monitorar, de forma permanente e integrada, a conformidade de todos os órgãos e as entidades estaduais à LGPD.

Parágrafo único. Os órgãos e as entidades estaduais não deverão contratar plataformas tecnológicas próprias para governança dos

constituição da plataforma, torna-se de grande importância se ter controle das ações de atendimento, com fito de bem atender a LGPD.

1. Política de privacidade

O DETRANRS tem sua política de privacidade e proteção de dados e avisos aos usuários já publicada na PORTARIA DETRANRS nº 286/21. A política de privacidade é um documento interno dirigido os servidores, estagiários e credenciados. No caso do DETRANRS , que todos devem obediência a portaria, isso significa que tanto a equipe de servidores públicos, comissionados, credenciados e ou equipe de terceirizados, assim como toda e qualquer contratada que venha a prestar serviços ou fornecer produtos mediante licitação ou contratação direta, inclusive convênios, deve respeitar a portaria informada.

Este documento informa como os dados pessoais são tratados, armazenados e transmitidos para atender às necessidades organizacionais e as legislações aplicáveis, definindo todos os aspectos relativos à proteção de dados.

Esta política de privacidade deve ser considerada por toda o DETRANRS – do mais alto nível de governança institucional até às equipes operacionais, estagiários, terceirizados, credenciados e contratados/conveniados.

São componentes de uma política de privacidade:

- a) Objetivo: porque a política existe e metas a serem alcançadas;
- b) Escopo: que recursos (pessoas, processos e tecnologias) a política protege;
- c) Responsabilidades: quais papéis são responsáveis por quais atividades relacionadas à proteção de dados,
- d) Conformidade: estrutura para garantir a adequação às normas aplicáveis, incluindo políticas e procedimentos complementares (ex. política de controle de

dados pessoais, salvo prévia autorização do Conselho de Implementação da LGPD no Poder Executivo Estadual, que analisará os riscos de incompatibilidade entre a solução tecnológica proposta e a plataforma transversal do Estado.

acesso) e regime de sanções disciplinares por desrespeito à política de privacidade.

2. Aviso de privacidade

O aviso de privacidade é uma comunicação externa para titulares de dados que não estão vinculados ao DETRANRS . No caso do DETRANRS , os titulares fornecem seus dados pessoais à Autarquia para realização de serviços de trânsito. Este aviso descreve como será a coleta, o uso, o compartilhamento e a retenção com base na política de privacidade da DETRANRS . O seu objetivo é permitir que o indivíduo tome decisões informadas sobre o uso de seus dados pessoais pelo DETRANRS e está presente na PORTARIA DETRANRS 286/21.

3. Relatório de Impacto de Proteção de Dados

O Relatório de Impacto de Proteção de Dados - RIPD, já confeccionado pelo DETRANRS , é a análise dos riscos à proteção de dados associados ao tratamento de dados pessoais em relação a um determinado projeto, produto ou serviço. O RIPD também deve sugerir ou fornecer ações corretivas ou mitigações necessárias para evitar ou mitigar esses riscos.

Nem toda atividade enseja a necessidade de um RIPD e a LGPD deixou em aberto para a autoridade supervisora, a ANPD, determinar hipóteses em que este relatório seria necessário. Contudo, uma boa prática é conduzir o RIPD sempre que determinado projeto tenha o potencial de altos riscos para os direitos e liberdades dos indivíduos. Como previsto na Portaria DETRANRS 286/21 é responsabilidade da DTI providenciar pela execução do RIPD sempre que houver o desenvolvimento inaugural de novo programa que envolva tratamento de dados pessoais.

O inventário de dados pessoais e o gap analysis são dois procedimentos importantes nessa etapa preparatória do RIPD.

Para fins de elaboração do RIPD, é necessário: identificar o escopo do tratamento, determinar os requisitos de proteção de dados relevantes (princípios, bases legais,

direitos dos titulares, etc.), acessar o risco (identificação, análise e avaliação do risco) e elaborar o plano tratamento do risco.

Quanto ao monitoramento do RIPD, é necessário, além de preparar e publicar o relatório, implementar um plano de tratamento de risco, revisando-o sempre quando necessário.

4. Plano de Resposta a Incidentes

Por mais precavida que sejam as unidades internas, elas sempre estarão sujeitas a riscos inerentes à sua atividade, o que inclui riscos de vazamento de dados. A existência de um plano de respostas a incidentes (PRI) forte é o diferencial para que o DETRANRS esteja preparado para lidar com vazamentos de dados, garantindo a proteção dos dados de titulares e evitando sanções administrativas.

O PRI deve fornecer instruções que auxiliem a identificar se um determinado incidente de segurança é também um vazamento de dados, ou seja, se o incidente detectado acarreta risco ou dano relevante aos titulares de dados. Caso positivo, as regras da LGPD se aplicarão, o que inclui obrigações de comunicação à autoridade nacional e aos titulares de dados sobre o incidente (art. 48). Algumas das informações que um PRI deve conter são:

- a) instruções para garantir o sigilo de informações sensíveis quanto ao vazamento;
- b) definição de funções e responsabilidades de unidades organizacionais durante o vazamento;
- c) escalonamento de possíveis problemas e relato de atividades suspeitas;
- d) classificações de gravidade de incidentes;
- e) orientações para comunicações externas (por exemplo, com reguladores, fornecedores de serviços, seguradoras, titulares, etc.).

Os riscos de vazamento de dados, no âmbito da DETRANRS, estão na sua maioria relacionados aos sistemas corporativos e departamentais utilizados, bem como na gestão de pessoas e processos, nos primeiros se sabe que sempre existe a possibilidade de uma

ameaça (hackers) tenha acesso a dados pessoais. Diante disso, como há uma padronização de sistemas no âmbito do Poder Executivo Estadual e no DETRANRS a cargo da PROCERGS, conclui-se que, provavelmente haverá um PRI que abarcará todas as secretarias estaduais e para o DETRAN, inclusive.

5. Implementação do Programa

Uma vez estruturado e aprovado o Programa de Governança em Privacidade, este deve ser implementado por todas as unidades (divisões, coordenadorias e assessorias). É importante que todos os servidores, sob orientação do encarregados e do setor LGPD, conduzam esforços para garantir que as políticas e procedimentos estabelecidos sejam corretamente aplicados pelos demais membros da equipe do seu setor, seja com a aval do setor LGPD (a ser criado pela Autarquia, conforme pedido a Direção-Geral pelo Encarregado), se assim entender a alta administração da casa.

O gerenciamento do ciclo de vida dos dados deve possuir todos os processos, padrões e funções bem definidos e registrados, cabendo a DPO do DETRANRS e ou ao setor LGPD o monitoramento. Os recursos devem ser disponibilizados para garantir, entre outras atividades, o seguinte:

- a) respeito aos princípios da LGPD;
- b) a confirmação das bases legais para tratamento de dados;
- c) a garantia dos direitos dos titulares de dados;
- d) a implementação de medidas de segurança;
- e) a definição de procedimentos de retenção e eliminação de dados pessoais;
- f) as limitações de acesso e compartilhamento;
- g) as notificações sobre vazamento de dados.

Dentre as atividades supramencionadas, destaca-se aqui o conceito de "*privacy by design*", a ideia de que medidas técnicas e administrativas de privacidade e proteção de dados devem ser implementadas desde a concepção do desenvolvimento de um sistema, tendo a

DTI e o setor LGPD papéis preponderantes como garantidores de que os sistemas já no nascedouro terão privacidade e proteção de dados .

Esse paradigma ressalta ao menos três valores: (I) a proatividade, ao se incluir a privacidade como parte dos requisitos de engenharia do sistema; (II) a incorporação de controles de privacidade, que serão auditados e avaliados continuamente, e; (III) o respeito aos titulares de dados, a partir do uso de controles transparentes, permitindo que indivíduos exerçam seus direitos.

Alguns exemplos de medidas técnicas e organizacionais "*privacy by design*", que provavelmente serão incluídas no Programa de Governança a ser desenvolvido no RS (art. 6º, Decreto nº 55.987/2021), incluem:

- a) uso de criptografia para proteção de bases de dados e meios de comunicação;
- b) minimização e pseudonimização de bases de dados;
- c) controle de acesso baseado em funções;
- d) mecanismo de respostas a requisições e reclamações dos titulares de dados;
- e) plano de respostas a incidentes e remediação de segurança e privacidade;
- f) segurança física;
- g) políticas de privacidade para aquisição de produtos/serviços;
- h) políticas de gerenciamento da segurança da informação;
- i) política de retenção e eliminação de dados pessoais.

Duas práticas importantes a serem implementadas são os mecanismos de respostas a requisições e reclamações dos titulares de dados e a incidentes de segurança e privacidade, em canais de atendimento ao cidadão, com registro de log e respostas. Estes mecanismos têm como objetivo respeitar os direitos dos titulares de dados previstos na LGPD e preparar para cenários indesejados de vazamento de dados, identificando que áreas deverão ser envolvidas para conter o dano, informar as partes interessadas relevantes (ex. ANPD e titulares de dados) e lidar com responsabilizações judiciais.



GOVERNO DO ESTADO
RIO GRANDE DO SUL

III- ETAPA DE MONITORAMENTO

Este Programa de Governança em Privacidade não é estático. Ele deve evoluir com o tempo, acompanhando mudanças regulatórias, alterações estruturais do DETRAN, novos projetos que envolvam atividades de tratamento de dados, e aquisição de novas tecnologias, dentre outros.

O monitoramento deve ser conduzido pelo encarregado dos dados pessoais e os servidores responsáveis pelas ações sobre os dados pessoais, sempre sob orientação do Grupo de Trabalho que cuida da implantação da LGPD no Estado do Rio Grande do Sul.

A partir dessas informações trazidas, o Grupo de Trabalho poderá identificar lacunas e pontos de melhoria para aperfeiçoamento do Programa de Governança em Privacidade do DETRAN. No que diz respeito às atividades de monitoramento, cabe destacar o papel do gerenciamento de risco, dos indicadores de desempenho e da gestão de incidentes. Como o gerenciamento de riscos já foi abordado ao se comentar sobre o RIPD, destacam-se aqui os dois últimos elementos

A Etapa de Monitoramento compreende a definição dos indicadores de desempenho do Programa de Governança em Privacidade e a gestão de incidentes operacionais de violação de dados, a serem desenvolvidos pelo DPO do DETRANRS e setor da LGPD, se criado no organograma da Autarquia.

1. Indicadores de Desempenho

Os indicadores de desempenho fornecem evidências sobre o funcionamento do Programa de Governança em Privacidade, se ele cumpre o que foi projetado a realizar e se os controles estabelecidos são gerenciados corretamente.

Seu escopo deve incluir todas as unidades organizacionais do DETRANRS que tratam dados pessoais e, operadores de tratamento de dados credenciados. Um procedimento que deve incluir fases de planejamento/preparação, execução e produção do relatório.

Ela pode ser conduzida internamente (no âmbito da DETRANRS e sob coordenação do Encarregado). A auditoria interna é utilizada para realizar auto avaliações do Programa de Governança em Privacidade. Ela ajuda a verificar em que estado se encontra o programa e deficiências a serem corrigidas.

No caso da DETRANRS , em razão do grande volume de dados pessoais tratados, compete aos servidores, responsáveis pelo tratamento dos dados, assessorar o Encarregado na identificação de problemas diagnosticados e, conseqüentemente, no aprimoramento do programa de governança em privacidade, se não criado o setor LGPD, conforme solicitado pelo DPO a Direção do DETRAN.

Já a auditoria em operadores de dados, ocorre nas hipóteses em que o DETRANRS enquanto controlador de dados, necessita se certificar de que entidades credenciadas/conveniadas e/ou contratadas, como operadoras de tratamento de dados, cumprem suas obrigações frente a legislações de proteção de dados, no caso a LGPD.

Outro aspecto importante, para a análise de desempenho de um programa, é o estabelecimento de um modelo de maturidade da privacidade (*Privacy Maturity Model*), que permite identificar quão evoluído está este Programa. Para tanto, utilizam-se métricas específicas, que incluem:

- a) número de treinamentos realizados / percentual de equipe treinada;
 - b) percentual de treinamentos concluídos;
 - c) percentagem de conformidade de sistemas
 - d) número de requisições de titulares de dados;
 - e) número de reclamações de titulares de dados;
 - f) número de incidentes de segurança / vazamento de dados;
 - g) tempo médio entre incidentes;
 - h) tempo médio para recuperação;
 - i) percentagem de existência de planos de resposta;
2. Gestão de Incidentes

A gestão de incidentes a ser constituída no DETRANRS pelo setor LGPD visa identificar e

organizar uma ocorrência de vazamento de dados pessoais com rapidez, o que contribui para solução do incidente, permitindo que o órgão possa rastrear os dados relevantes.

Espera-se assim, que esse programa possa identificar quais dados foram afetados por uma violação ou vulnerabilidade, como são usados, quem tem acesso a eles e como se dá a fluência entre outras funcionalidades, e prontamente se consiga afastar a vulnerabilidade.

CONCLUSÃO

Embora este roteiro não aborde todas as minúcias referentes à estruturação do Programa de Governança em Privacidade, ele fornece etapas importantes que precisam ser cumpridas para garantir que o DETRANRS atenda as principais obrigações da LGPD. O PGP visa assegurar no DETRANRS a conformidade com os princípios básicos da segurança da informação – CID ou confidencialidade, integridade e disponibilidade.

Espera-se com isso, que o DETRANRS, composto por 652 servidores, milhares de credenciados nas mais diversos matizes, centenas de convênios e contratados, com um gigantesco volume de tratamento de dados pessoais e dados pessoais sensíveis possa contribuir para a implementação de um Programa de Governança em Privacidade no âmbito do Estado do Rio Grande do Sul, garantindo a observância à norma e o respeito aos titulares de dados.

O direito à privacidade é garantido pela Declaração Universal de Direitos Humanos. A LGPD veio garantir a privacidade no mundo real e digital, pois visa garantir o direito à vida privada e familiar das pessoas. Reportamos que a proteção de dados é o meio de proteger direitos e liberdade fundamentais, entre eles a privacidade, todo o esforço possível para bem implementarmos a LGPD no DETRANRS deve ser adotado.

Marcio Pires Berr

Analista-Direito-ID3044068

Encarregado pelo Tratamento de Dados Pessoais DPO da LGPD no DETRAN-RS