<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

difusão ou extração".>

<O objetivo principal dessa descrição é fornecer um cenário institucional relativo aos processos que envolvam o tratamento dos dados pessoais, fornecendo subsídios para a avaliação e o tratamento de riscos.>

3.1 – NATUREZA DO TRATAMENTO

<A **natureza** representa como o órgão ou entidade pretende tratar ou trata o dado pessoal.>

<Importante descrever, por exemplo:

• como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;

• fonte de dados (por exemplo: titular de dados, planilha eletrônica, arquivo .xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais;

• com quais órgãos, entidades ou empresas dados pessoais são compartilhados e quais são esses dados;

• quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador (agente de tratamento) e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;

• se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e

• medidas de segurança atualmente adotadas.>

<Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados do órgão ou entidade.>

3.2 – ESCOPO DO TRATAMENTO

<O **escopo** representa a abrangência do tratamento de dados.>

<Nesse sentido, considere destacar:

• as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis;

• o volume dos dados pessoais coletados e tratados;

• a extensão e frequência em que os dados são tratados;

• o período de retenção, que é a informação sobre quanto tempo os dados pessoais são mantidos, retidos ou armazenados;

• o número de titulares de dados afetados pelo tratamento; e

• a abrangência da área geográfica do tratamento.>

<O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.>

3.3 – CONTEXTO DO TRATAMENTO

<Nesta seção, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas dos titulares dos dados pessoais ou o impacto sobre o tratamento dos dados.>

<O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares dos dados:

• natureza do relacionamento do órgão ou entidade com os indivíduos;

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

• nível ou método de controle que os indivíduos exercem sobre os dados pessoais;

• destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;

• destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, se o dado pessoal não é tratado de maneira diversa do que é determinado em normas e regulamentos e se é comunicado pelo órgão ou entidade ao titular de dados;

• destaque de qualquer experiência anterior com esse tipo de tratamento de dados;

• destaque de avanços relevantes do órgão ou entidade em tecnologia ou segurança que contribuam para a proteção dos dados pessoais.>

3.4 – FINALIDADE DO TRATAMENTO

<A **finalidade** é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É imprescindível estabelecer claramente a finalidade, pois é o que justifica o tratamento e fornece os elementos para informar o titular dos dados.>

<Nesta seção, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com as hipóteses elencadas abaixo, que se referem àquelas presentes nos arts. 7º e 11 da LGPD, no que for aplicável:

• cumprimento de obrigação legal ou regulatória pelo controlador;

• execução de políticas públicas;

• alguma espécie de estudo realizado por órgão de pesquisa;

• execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

• exercício regular de direitos em processo judicial, administrativo ou arbitral;

• proteção da vida ou da incolumidade física do titular ou de terceiro;

• tutela da saúde;

• atender aos interesses legítimos do controlador ou de terceiro;

• proteção do crédito; e

• garantia da prevenção à fraude e à segurança do titular.>

<Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que essa finalidade não conste nos citados exemplos.

Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

• Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados;

• Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.>

<Neste momento, deve-se atentar para o caso de a **finalidade** ser para atender o legítimo interesse do controlador (agente de tratamento). Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD.

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> **I - apoio e promoção de atividades do controlador; e**
> **II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.**
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os
> dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.>

<Cumpre ressaltar que devem ser equilibrados os interesses do controlador de dados pessoais com os dos indivíduos com os quais se tem relacionamento.>

4 – PARTES INTERESSADAS CONSULTADAS

<Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.>

<Nessa seção, é importante identificar:

• quais partes foram consultadas, como, por exemplo: operador (art. 5º, inc. VII, LGPD), Encarregado pela Proteção de Dados Pessoais (art. 5º, inc. VIII, LGPD), gestores, especialistas em segurança da informação, consultores jurídicos, etc.; e

• o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve se observar os riscos de não-conformidade ante a LGPD e demais normas relativas à proteção de dados pessoais, bem como ante aos instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados pessoais e privacidade).>

<Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não se ter realizado tal registro, como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial, fragilizaria a segurança da informação, ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.>

5 – NECESSIDADE E PROPORCIONALIDADE

<Descrever como o órgão ou entidade avalia a necessidade e a proporcionalidade de dados pessoais. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos com relação às finalidades do tratamento de dados pessoais (art. 6º, inc. III, LGPD).>

<Nesse sentido, destacar:

• A fundamentação legal para o tratamento dos dados pessoais;

• Caso o fundamento legal seja embasado no legítimo interesse do controlador (art. 10, LGPD), demonstrar que:

- esse tratamento de dados pessoais é indispensável;
- não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
- esse processamento de fato auxilia no propósito almejado.

• Como será garantida a qualidade (exatidão, clareza, relevância e atualização de dados pessoais) e a minimização de dados pessoais;

• Quais medidas são adotadas a fim de assegurar que o operador (art. 5º, inc. VII, LGPD) realize o

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pelo órgão ou entidade que exerça o papel de controlador (art. 5º, inc. VI, LGPD);

• Como estão implementadas as medidas que asseguram o direito do titular de dados pessoais de obter do controlador (agente de tratamento) o previsto pelo art. 18 da LGPD;

• Como o órgão ou entidade pretende fornecer informações de proteção de dados pessoais para os titulares;

• Quais são as salvaguardas para as transferências internacionais de dados pessoais.>

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

<O art. 5º, inc. XVII, da LGPD, preconiza que o Relatório de Impacto à Proteção de Dados Pessoais deve descrever *"medidas, salvaguardas e mecanismos de mitigação de risco".*>

<Antes de definir essas medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular de dados pessoais.>

<Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco e o possível impacto na eventualidade da ocorrência do risco, a fim de avaliar o nível potencial de risco para cada evento.>

<Parâmetros escalares podem ser utilizados para representar os níveis de **probabilidade** e **impacto** que, após a multiplicação, resultarão em níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:>

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

<A figura a seguir apresenta a **Matriz Probabilidade x Impacto**, instrumento de apoio para a definição dos critérios de classificação do nível de risco.>

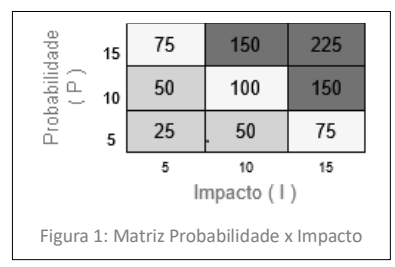

Figura 1: Matriz Probabilidade x Impacto

<O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.

Risco enquadrado na região:

- verde, é entendido como baixo;