

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

- (viii) tutela da saúde;
- (ix) atender aos interesses legítimos do controlador ou de terceiros;
- (x) proteção do crédito; e
- (xi) garantia da prevenção à fraude e à segurança do titular.>

<Cumprir 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 o tratamento de dados pessoais, mesmo que essa finalidade não conste nos citados exemplos, mas que tenha relação às hipóteses de tratamento de dados pessoais previstas pelos arts. 7º e 11, da LGPD.

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

- (i) Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais e a sua importância;
- (ii) Informar os benefícios esperados para o órgão ou para a entidade ou mesmo para a sociedade como um todo.>

<Neste momento, deve-se atentar para o caso de a **finalidade** ser para atender ao legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado o 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.>

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

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

4 – PARTES INTERESSADAS CONSULTADAS

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

<Neste subitem, é importante identificar:

- (i) quais partes foram consultadas – como, por exemplo, o operador (art. 5º, inc. VII, LGPD), o Encarregado pela Proteção de Dados Pessoais competente (art. 5º, inc. VIII, LGPD), consultores jurídicos e especialistas em segurança da informação, privacidade e proteção de dados pessoais; e
- (ii) o que cada parte consultada indicou como necessário à salvaguarda dos direitos à privacidade e à proteção e dados pessoais.>

<Caso não seja conveniente registrar o que foi consultado, é importante apresentar o motivo de não se ter realizado esse registro – como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes comprometeria segredo comercial ou industrial ou mesmo reduziria a segurança da informação.>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

5 – NECESSIDADE E PROPORCIONALIDADE

<Descrever como o órgão ou a entidade avalia a necessidade e a proporcionalidade do tratamento de dados pessoais. É necessário demonstrar que as operações realizadas limitam o tratamento ao mínimo necessário para a realização de suas finalidades (art. 6º, inc. III, LGPD).>

<Nesse sentido, destacar:

- (i) a fundamentação legal para o tratamento dos dados pessoais;
- (ii) caso o fundamento legal seja embasado no legítimo interesse do controlador (art. 10, LGPD), demonstrar que:
 - a. esse tratamento de dados pessoais é indispensável;
 - b. não há outra hipótese de tratamento possível de ser utilizada para alcançar a mesma finalidade; e
 - c. esse tratamento de dados pessoais de fato auxilia na finalidade almejada.
- (iii) Quais medidas são adotadas a fim de assegurar que o operador (art. 5º, inc. VII, LGPD) realize o tratamento de dados pessoais em conformidade ao sistema normativo protetivo à privacidade e aos dados pessoais e respeite os critérios estabelecidos pela organização que exerça o papel de controlador (art. 5º, inc. VI, LGPD);
- (iv) Como estão implementadas as medidas que asseguram a efetivação do exercício dos direitos dos titulares de dados pessoais (arts. 9º e 17 a 22, LGPD); e
- (v) Quais são as salvaguardas para as transferências internacionais de dados pessoais.>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

6 – GESTÃO DE RISCOS

<O art. 5º, inc. XVII, da LGPD, preconiza que o Relatório de Impacto à Proteção de Dados Pessoais deve descrever as “medidas, salvaguardas e mecanismos de mitigação de risco” implementados no âmbito da organização.>

<Para a realização da Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais de seu órgão ou de sua entidade, recomenda-se a consulta à metodologia, orientada pela Controladoria Geral do Município de São Paulo (CGM/SP), presente no “Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública Municipal”.>