PROPOSTA DE ROTEIRO PARA ELABORAÇÃO DE PLANO DE ANÁLISE DE RISCOS RELATIVOS À PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA MUNICIPAL

versão 1 – 18/07/2022.

1 - Nome do serviço para o qual o **PLANO DE ANÁLISE DE RISCOS** será elaborado;

2 - Descrição do escopo do serviço e sua finalidade;

3 – Descrever os agentes de tratamento (controlador e operador) da prestação do serviço (aplicativo, programa ou sistema). Se houver Controladoria Conjunta[1], haverá a necessidade de deixar expressa tal situação;

4 – Descrever os encarregados de dados indicados pelos agentes de tratamento;

5 – Indicar expressamente quais as bases legais e finalidades específicas utilizadas no tratamento de dados pessoais do serviço;

6 - Identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais, independentemente de sua natureza (técnica, administrativa, de segurança da informação ou de privacidade). Alguns dos riscos à privacidade que devem ser elencados nesta análise, como exemplo:

a) Ausência de indicação de encarregado;
b) Acesso não autorizado;
c) Modificação não autorizada;
d) Tratamento sem consentimento do titular dos dados pessoais (Caso a base legal seja consentimento);
e) Compartilhar ou distribuir dados pessoais com terceiros fora das hipóteses de compartilhamento;
f) Perda;
g) Roubo;
h) Remoção não autorizada;
i) Utilização de dados em excesso;
j) Não especificação de quais as medidas de segurança adotadas;
k) Execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc;
l) Tratamento de dados pessoais de crianças e adolescentes sem o consentimento de pais ou responsáveis;
m) Retenção prolongada de dados pessoais sem necessidade;
n) O órgão/entidade não apresenta uma política de privacidade informando o tratamento realizado e dados pessoais tratados;
o) Compartilhamento de dados excessivos com órgãos públicos;
p) Informação insuficiente sobre a finalidade do tratamento;

[1]Conforme Guia da ANPD v 2.0: “Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente, as respectivas responsabilidades pelo cumprimento do presente regulamento”.

q) Falha em considerar os direitos do titular dos dados pessoais (Ex.: não possibilitar remoção do consentimento);
r) Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular;
s) Reidentificação de dados pseudonimizados.

7 – Mencionar a norma ou a boa prática não observada e que gerou o risco identificado, como por exemplo:

a) Ausência de indicação de encarregado: Art. 41, LGPD
b) Acesso não autorizado: princípio da segurança (art. 6, VII e art. 46, LGPD) + ISO / IEC 29134:2017;
c) Modificação não autorizada: princípio da segurança (art. 6, VII e art. 46, LGPD) + ISO / IEC 29134:2017;
d) Tratamento sem consentimento do titular dos dados pessoais (Caso a base legal seja consentimento): Art 5, inciso XII e art. 7, inciso I, LGPD;
e) Compartilhar ou distribuir dados pessoais com terceiros fora das hipóteses de compartilhamento: Art. 26 e 27 da LGPD;
f) Perda: princípio da segurança (art. 6, VII e art. 46, LGPD) + princípio da responsabilização (art. 6, X, LGPD);
g) Roubo: princípio da segurança (art. 6, VII e art. 46, LGPD) + princípio da responsabilização (art. 6, X, LGPD);
h) Remoção não autorizada: princípio da segurança (art. 6, VII e art. 46, LGPD) + princípio da responsabilização (art. 6, X, LGPD);
i) Utilização de dados em excesso: princípio da necessidade (art. 6, II e III, LGPD);
j) Não especificação de quais as medidas de segurança adotadas: princípio da segurança (art. 6, VII e art. 46, LGPD);
k) Execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.: princípio da qualidade dos dados (art. 6, V, LGPD);
l) Tratamento de dados pessoais de crianças e adolescentes sem o consentimento de pais ou responsáveis: princípio da segurança (art. 6, VII e art. 46) e princípio da responsabilização (art 6, X) e regras para tratamento de dados de crianças (art. 14, LGPD);
m) Retenção prolongada de dados pessoais sem necessidade: Art. 5, inc. XIV, LGPD + Art. 18, IV e VI, LGPD;
n) O órgão/entidade não apresenta uma política de privacidade informando o tratamento realizado e dados pessoais tratados: Art. 50, § 3º, LGPD + Princípio da transparência;
o) Compartilhamento de dados excessivos com órgãos públicos: Art. 18, VII, LGPD + princípio da necessidade;
p) Informação insuficiente sobre a finalidade do tratamento: Art. 6º, I; art. 9º, I; art. 23, LGPD;
q) Falha em considerar os direitos do titular dos dados pessoais (Ex.: não possibilitar remoção do consentimento): Art. 9º; art. 18º, LGPD;
r) Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular: Art 5º, I; art. 13, §4º, LGPD;
s) Reidentificação de dados pseudonimizados: Art 5º, I; art. 13, §4º, LGPD.

8 - Para cada risco identificado, define-se a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento. Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança (o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016);

9 – Após a identificação da probabilidade, do impacto e do nível, os riscos deverão ser classificados ((baixo (verde), médio (amarelo) ou alto (vermelho));

10 – Indicação de qual(is) ação(ões) são sugeridas para tratar ou minimizar a ocorrência dos riscos identificados;

11 – Por fim, identificar a classificação dos riscos residuais (baixo (verde), médio (amarelo) ou alto (vermelho)).