DIARIO OFICIAL ELETRONICO DPE/AM
nº 2632
Disponibilização: 15/04/2026
Publicação: 15/04/2026

GDPG - GABINETE DO DEFENSOR PÚBLICO GERAL

Avenida André Araújo, 679 |Manaus/AM| |

|CEP 69060-000|

ATO NORMATIVO Nº 12/2026/GDPG/DPE/AM

Dispõe sobre a obrigatoriedade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD/DPIA) para sistemas no âmbito da Defensoria Pública do Estado do Amazonas que envolvam tratamento de dados pessoais.

O DEFENSOR PÚBLICO GERAL DO ESTADO DO AMAZONAS , no uso das atribuições que lhe são conferidas pelo art. 9º da Lei Complementar n.º 01 de 30 de março de 1990, consolidada na forma do art. 9º da Lei Promulgada n.º 51, de 21 de julho de 2004;

CONSIDERANDO a atribuição do Defensor Público Geral. para praticar atos de gestão administrativa, na forma do art. 9º, inciso XII, da Lei Complementar Estadual n.º 01, de 30 de março de 1990;

CONSIDERANDO o disposto na Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), em especial seus artigos 5º, XVII, 6º, 37, 38, 46 e seguintes;

CONSIDERANDO a importância de adoção dos princípios de Privacy by Design e Privacy by Default, nos termos do artigo 46 da LGPD.

CONSIDERANDO a recomendação Agência Nacional de Proteção de Dados Pessoais, que orienta sobre a adoção de medidas de governança, segurança da informação e avaliação de riscos, inclusive por meio de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD);

CONSIDERANDO a natureza das atividades desenvolvidas pela Defensoria Pública do Estado do Amazonas, voltadas à defesa de direitos humanos e à assistência jurídica integral e gratuita a pessoas em situação de vulnerabilidade, envolvendo o tratamento de dados pessoais sensíveis e de dados de populações vulneráveis (pessoas de baixa renda, povos indígenas, comunidades quilombolas, vítimas de violência, população carcerária, crianças e adolescentes, dentre outros);

CONSIDERANDO a necessidade de estabelecer procedimento padronizado e obrigatório para a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD/DPIA) como instrumento de gestão de riscos e de efetiva implementação dos princípios de Privacy by Design e Privacy by Default em sistemas utilizados no âmbito da DPE/AM;

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Este Ato Normativo estabelece a obrigatoriedade de realização de Relatório de Impacto à Proteção de Dados Pessoais (RIPD/DPIA) para sistemas planejados, desenvolvidos, adquiridos ou utilizados pela Defensoria Pública do Estado do Amazonas – DPE/AM, que envolvam tratamento de dados pessoais, nos termos da LGPD.

Art. 2º Para fins deste Ato Normativo, considera-se:

I – Sistema: qualquer aplicação, solução tecnológica, base de dados, módulo, serviço em nuvem ou conjunto organizado de recursos de tecnologia da informação, própria ou de terceiros, que realize tratamento de dados pessoais no âmbito da DPE/AM, seja para atividade-fim, seja para atividade-meio;

II – Relatório de Impacto à Proteção de Dados Pessoais (RIPD/DPIA): documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação desses riscos, nos termos da LGPD e das orientações da ANPD;

III – Avaliação de Impacto Algorítmico (AIA): instrumento complementar ao RIPD, aplicável especialmente a sistemas que utilizem técnicas algorítmicas avançadas, inclusive de inteligência artificial, destinado a analisar riscos específicos, como vieses, discriminação, opacidade e impactos à autonomia dos titulares;

IV – Privacy by Design (PbD): incorporação de medidas de proteção de dados pessoais e de privacidade desde a concepção do sistema ou processo, considerando todo o seu ciclo de vida;

V – Privacy by Default (PbDf): adoção de configurações padrão que garantam o nível máximo de proteção de dados e privacidade, independentemente de ação do usuário, limitando por padrão a coleta, o uso e o compartilhamento de dados ao mínimo necessário.

CAPÍTULO II

DO ÂMBITO DE APLICAÇÃO

Art. 3º Estão sujeitos a este Ato Normativo todos os sistemas que:

I – estejam em fase de estudo, concepção, desenvolvimento, aquisição, contratação, homologação ou implantação;

II – encontrem-se em fase de testes (pilotos, provas de conceito, ambientes de homologação com dados reais ou de teste);

III – estejam em produção, ainda que implantados antes da vigência deste Ato Normativo.

§ 1º Incluem-se no disposto neste artigo os sistemas utilizados:

I – na **atividade-fim**, para atendimento a assistidos, registro e gestão de atendimento, análise de processos, elaboração de peças, emissão de pareceres, gestão de prazos judiciais e correlatos;

II – na **atividade-meio**, para gestão de pessoas, gestão documental, gestão administrativa e financeira, comunicação institucional, gestão de contratos, infraestrutura de TI e outros.

§ 2º Aplica-se igualmente a sistemas **desenvolvidos internamente** ou **contratados de terceiros**, incluindo soluções em nuvem (SaaS, PaaS, IaaS) e integrações com sistemas externos.

CAPÍTULO III

DA OBRIGATORIEDADE DO RIPD/DPIA

Art. 4º É **obrigatória** a elaboração de **RIPD/DPIA**, na forma deste Ato Normativo, para sistemas que:

I – tratem **dados pessoais sensíveis**;

II – tratem dados de pessoas em situação de vulnerabilidade;

III – sejam utilizados em contexto de **atividade-fim** da DPE/AM;

IV – envolvam decisões automatizadas ou semiautomatizadas com impacto relevante sobre os direitos dos titulares;

V – utilizem dados em larga escala ou com potencial de monitoramento sistemático de pessoas;
VI – sejam classificados como de **risco médio, alto ou excessivo** para os direitos dos titulares, a juízo da Assessoria de Proteção de Dados Pessoais (APDP).

§ 1º Para sistemas que não se enquadrem nas hipóteses dos incisos I a VI, a APDP poderá, mediante justificativa, dispensar o RIPD ou admitir um **RIPD simplificado**, sem prejuízo da avaliação de risco.

§ 2º Nos casos em que o sistema utilize técnicas algorítmicas avançadas, inclusive de inteligência artificial, a APDP poderá requerer, adicionalmente, a realização de **Avaliação de Impacto Algorítmico (AIA)**, a ser anexada ao RIPD/DPIA.

CAPÍTULO IV

DO MOMENTO E DO PROCEDIMENTO DE REALIZAÇÃO

Art. 5º O RIPD/DPIA deverá ser:

I – elaborado na fase de **concepção ou planejamento** do sistema, antes da aprovação final do projeto ou da contratação;

II – revisado e atualizado sempre que houver:

a) alteração relevante da finalidade, das categorias de dados tratados ou das bases legais;
b) mudança significativa de arquitetura tecnológica ou de provedores (ex.: migração para nova plataforma ou nuvem);

c) expansão de uso para novas unidades, núcleos ou públicos-alvo;
d) identificação de incidentes de segurança ou de riscos relevantes não previstos inicialmente.

Art. 6º Nenhum sistema abrangido por este Ato Normativo poderá entrar em **produção**, ou ter seu uso ampliado de forma significativa, sem que:

I – o respectivo RIPD/DPIA tenha sido **elaborado, analisado e aprovado** pela APDP; e
II – no caso de sistemas que requeiram AIA, essa avaliação tenha sido realizada e apreciada pela APDP.

Parágrafo único. Em situação excepcional, devidamente fundamentada, o Defensor Público-Geral poderá autorizar a utilização experimental de sistema por prazo determinado, condicionada à apresentação, em cronograma definido, do RIPD/DPIA e, se cabível, da AIA.

CAPÍTULO V

DO CONTEÚDO MÍNIMO DO RIPD/DPIA

Art. 7º O RIPD/DPIA deverá conter, no mínimo:

I – identificação do sistema, do órgão responsável, da unidade gestora e dos principais atores envolvidos (TI, núcleos, fornecedores, etc.);

II – descrição detalhada do tratamento de dados pessoais, incluindo:

a) tipos de dados pessoais e sensíveis tratados;

b) fontes e fluxos de dados (internos e externos);

c) volume estimado de dados;

d) ciclo de vida dos dados (coleta, uso, armazenamento, compartilhamento e descarte);
e) medidas de segurança da informação existentes;

III – identificação da(s) base(s) legal(is) e das finalidades específicas do tratamento, com destaque para dados sensíveis e dados de grupos vulneráveis;

IV – análise de **necessidade** e **proporcionalidade**, indicando se a finalidade pode ser atingida com menor coleta de dados ou com menor impacto à privacidade;

V – identificação e classificação dos riscos aos direitos dos titulares (privacidade, não discriminação, segurança, integridade, honra, imagem, entre outros), considerando o contexto da atuação da DPE/AM;

VI – descrição das medidas de mitigação, salvaguardas e mecanismos de governança adotados ou planejados, incluindo aquelas que implementem **Privacy by Design** e **Privacy by Default** (minimização de dados, limitação de acessos, configurações padrão protetivas, etc.);

VII – definição de prazos de retenção, critérios de descarte, níveis de acesso por perfil e configurações padrão de privacidade do sistema;

VIII – plano de monitoramento, revisão e auditoria do sistema, especificando periodicidade, indicadores e responsáveis;

IX – conclusão com avaliação do risco residual, recomendações da APDP e manifestação do gestor responsável pelo sistema.

CAPÍTULO VI

DAS RESPONSABILIDADES

Art. 8º Compete à **Assessoria de Proteção de Dados Pessoais (APDP)** :

I – elaborar e manter atualizados os **modelos padrão** de RIPD/DPIA e, quando cabível, de AIA;

II – orientar gestores, a Diretoria de Tecnologia da Informação (DTI) e demais unidades na correta elaboração dos relatórios;

III – analisar e emitir parecer sobre os RIPD/DPIA apresentados, podendo aprová-los, aprová-los com recomendações ou solicitar complementações;

IV – propor medidas de mitigação de riscos e ajustes em sistemas e processos, especialmente no que se refere à implementação de PbD e PbDf;

V – acompanhar, em conjunto com a DTI e as unidades gestoras, a implementação dos planos de ação e recomendações constantes dos relatórios.

Art. 9º Compete à **Diretoria de Tecnologia da Informação (DTI)** :

I – assegurar que todo sistema sob sua responsabilidade técnica ou operacional seja submetido à APDP para avaliação, quando aplicável;

II – fornecer informações técnicas completas e atualizadas para subsidiar a elaboração do RIPD/DPIA;

III – implementar as medidas técnicas de segurança e de PbD/PbDf recomendadas pela APDP, na medida de sua viabilidade;

IV – garantir que sistemas não sejam colocados em produção, ou tenham seu escopo ampliado, em desacordo com este Ato Normativo.

Art. 10. Compete aos **gestores das unidades demandantes** (núcleos, diretorias, coordenações):

I – identificar projetos e iniciativas em suas áreas que envolvam sistemas com tratamento de dados pessoais e informá-los à APDP e à DTI, desde a fase de concepção;

II – cooperar na elaboração do RIPD/DPIA, fornecendo informações sobre fluxos de trabalho, perfis de usuários, contextos de uso e impactos esperados;

III – zelar para que servidores, membros, estagiários e colaboradores utilizem os sistemas em conformidade com a LGPD, com este Ato Normativo e com as orientações da APDP.

CAPÍTULO VII

DA IMPLEMENTAÇÃO GRADUAL E DISPOSIÇÕES TRANSITÓRIAS

Art. 11. Os sistemas em produção na data de publicação deste Ato Normativo que se enquadrem nas hipóteses do art. 4º deverão:

I – ser mapeados em relatório consolidado pela DTI, com apoio da APDP, no prazo de até **30 (trinta***) dias; II – ter os respectivos RIPD/DPIA elaborados e submetidos à APDP no prazo de até* 60 **(sessenta)** dias, contados da conclusão do mapeamento.

§ 1º A APDP poderá estabelecer **critérios de priorização**, considerando volume de dados, sensibilidade, impacto sobre direitos dos titulares e criticidade do sistema.

§ 2º Enquanto não concluídos os relatórios, a APDP poderá emitir **recomendações provisórias** de mitigação de riscos, a serem implementadas pela DTI e pelas unidades gestoras, sem prejuízo da elaboração posterior do RIPD/DPIA.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 12. Os casos omissos e as dúvidas na aplicação deste Ato Normativo serão dirimidos pelo Defensor Público-Geral, ouvido, quando necessário, a APDP, a DTI e demais unidades competentes.

Art. 13. Este Ato Normativo entra em vigor na data de sua publicação.

Cientifique-se. Publique-se. Cumpra-se.

GABINETE DO DEFENSOR PÚBLICO GERAL DO ESTADO DO AMAZONAS , em Manaus, 14 de abril de 2026.

Documento assinado eletronicamente por **RAFAEL VINHEIRO MONTEIRO BARBOSA**, **Defensor Público Geral**, em 14/04/2026, às 17:51, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site *Conferência de Autenticidade de Documentos - SEI DPE AM* informando o código verificador **0622698** e o código CRC **BA593698**.
