POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS

DEFENSORIA PÚBLICA GERAL
DO ESTADO DO CEARÁ

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - SETIN

SUMÁRIO

1 SUMÁRIO

Controle do documento e histórico de atualização....2

Atualização, revisão e controle de vigência 2

Sumário....3

1. Apresentação....4

2. Objetivo....4

3. Escopo e abrangência....4

4. Referências normativas e técnicas....5

5. Definições essenciais....5

6. Princípios de proteção de dados pessoais....6

7. Diretrizes gerais de tratamento....7

8. Bases legais aplicáveis....7

9. Tratamento de dados pessoais na realidade da DPE-CE....8

9.1 Atividades finalísticas 8

9.2 Atividades administrativas e de apoio 9

10. Dados pessoais sensíveis e grupos vulneráveis....9

11. Direitos dos titulares....9

12. Atendimento aos titulares....10

13. Transparência, avisos de privacidade e linguagem acessível....11

14. Cookies, portais e serviços digitais....11

15. Compartilhamento de dados e interoperabilidade....11

16. Operadores, fornecedores e terceiros....12

17. Segurança da informação, confidencialidade e controle de acesso....12

18. Privacy by Design e Privacy by Default....13

19. Retenção, arquivamento e descarte....13

20. Relatório de Impacto à Proteção de Dados Pessoais - RIPD....14

21. Incidentes de segurança com dados pessoais....14

22. Transferência internacional de dados....15

23. Governança, papéis e responsabilidades....15

24. Capacitação e cultura de privacidade....16

25. Monitoramento, indicadores e melhoria contínua.....16

26. Descumprimento da política.....17

27. Disposições finais.....17

Anexo I - Matriz de responsabilidades.....19

Anexo II - Checklist mínimo de conformidade.....19

Anexo III - Modelo de registro de tratamento.....20

Anexo IV - Referências técnicas.....21

1. Apresentação

A Defensoria Pública-Geral do Estado do Ceará - DPGE-CE desempenha função essencial à justiça e realiza atividades voltadas à promoção do acesso à justiça, à orientação jurídica, à defesa de direitos e à proteção de pessoas em situação de vulnerabilidade. No exercício dessas competências, a instituição trata dados pessoais de assistidos(as), usuários de serviços, defensores(as), servidores(as), estagiários(as), colaboradores, fornecedores, parceiros, representantes legais e demais pessoas naturais relacionadas às suas atividades.

Esta Política de Privacidade e Proteção de Dados Pessoais estabelece diretrizes institucionais para assegurar que o tratamento de dados pessoais ocorra de forma legítima, necessária, transparente, segura, responsável e compatível com a finalidade pública da DPGE-CE. O documento orienta condutas internas, apoia a governança de dados, fortalece a cultura de privacidade e promove prestação de contas perante titulares, órgãos de controle e sociedade.

A política foi estruturada a partir da Lei Geral de Proteção de Dados Pessoais - LGPD, das orientações da Autoridade Nacional de Proteção de Dados - ANPD, de referências de governança e controle público do Tribunal de Contas da União - TCU, de práticas de transparência e proteção de dados adotadas pela Controladoria-Geral da União - CGU, e de boas práticas de segurança da informação e gestão de privacidade.

2. Objetivo

- Definir diretrizes para o tratamento de dados pessoais no âmbito da DPGE-CE.
- Promover proteção à privacidade dos titulares e respeito aos direitos fundamentais de liberdade, intimidade, privacidade e autodeterminação informativa.
- Orientar defensores(as), servidores(as), estagiários(as), colaboradores, prestadores, operadores e parceiros sobre responsabilidades relacionadas ao tratamento de dados pessoais.
- Estabelecer critérios para coleta, uso, acesso, compartilhamento, armazenamento, retenção, descarte, segurança e resposta a incidentes envolvendo dados pessoais.
- Integrar privacidade, proteção de dados, segurança da informação, transparência pública, gestão de riscos e governança institucional.
- Fortalecer a responsabilização, a prestação de contas e a capacidade da instituição de demonstrar conformidade com a LGPD e com boas práticas aplicáveis ao setor público.

3. Escopo e abrangência

Esta política aplica-se a todos os tratamentos de dados pessoais realizados pela DPGE-CE, em meio físico ou digital, em processos administrativos, judiciais, extrajudiciais, atendimentos presenciais, atendimentos remotos, sistemas institucionais, portais, aplicativos, canais de comunicação, bases de dados, contratações, convênios, termos de cooperação e demais atividades institucionais.

- defensores(as) públicos(as), servidores(as), empregados(as), cedidos(as), estagiários(as), residentes, voluntários(as), colaboradores(as) e terceirizados(as);
- assistidos(as), usuários(as) dos serviços, representantes legais, familiares, testemunhas, partes adversas, visitantes e demais titulares envolvidos nas atividades da DPGE-CE;
- fornecedores, operadores, prestadores de serviços, parceiros institucionais, entidades conveniadas e demais terceiros que tratem dados pessoais em nome da DPGE-CE ou em ambiente integrado aos seus serviços;
- dados pessoais tratados em sistemas próprios, sistemas compartilhados, soluções em nuvem, documentos físicos, documentos digitais, e-mails, processos, registros administrativos, arquivos e plataformas de atendimento.

4. Referências normativas e técnicas

- Constituição Federal, especialmente os direitos fundamentais à intimidade, vida privada, honra, imagem, acesso à informação e proteção de dados pessoais.
- Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD.
- Lei Federal nº 12.527/2011 - Lei de Acesso à Informação - LAI, naquilo que se relaciona à transparência, proteção de informações pessoais e restrições de acesso.
- Marco Civil da Internet e normas aplicáveis à segurança, guarda de registros e proteção de dados em ambientes digitais.
- Orientações da ANPD sobre tratamento de dados pessoais pelo Poder Público, agentes de tratamento, encarregado, cookies, incidentes e boas práticas de governança.
- Referências do TCU sobre LGPD, governança pública, accountability, controles internos, segurança da informação e gestão de riscos.
- Práticas da CGU sobre transparência, tratamento de dados pessoais, compartilhamento, registros institucionais, governança e integração entre LAI e LGPD.
- Boas práticas técnicas baseadas em normas ABNT NBR ISO/IEC 27001, 27002, 27005, 27701, 29100 e 29134, quando aplicáveis ao contexto institucional.

5. Definições essenciais

Termo	Definição operacional para esta política
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado pessoal sensível	Dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, saúde, vida sexual, dado genético ou biométrico, quando vinculado a pessoa natural.
Titular	Pessoa natural a quem se referem os dados pessoais tratados.
Tratamento	Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão,

Termo	Definição operacional para esta política
	distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.
Controlador	Agente a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito desta política, a DPE-CE será controladora quando definir finalidades, meios e decisões essenciais do tratamento.
Operador	Pessoa natural ou jurídica que realiza tratamento de dados pessoais em nome da DPE-CE, conforme contrato, convênio, termo de cooperação ou instrumento congênere.
Encarregado(a) ou EPD	Pessoa indicada para atuar como canal de comunicação entre a DPE-CE, titulares dos dados e a ANPD, além de orientar colaboradores e apoiar a governança de privacidade.
RIPD/DPIA	Relatório de Impacto à Proteção de Dados Pessoais, utilizado para avaliar riscos, necessidade, proporcionalidade, salvaguardas e medidas de mitigação em tratamentos de maior risco.
Incidente de segurança	Evento confirmado ou suspeito que comprometa confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais.
Privacy by Design	Integração da privacidade desde a concepção de projetos, processos, sistemas, contratações e serviços.
Privacy by Default	Configuração padrão mais protetiva à privacidade, limitando coleta, acesso, compartilhamento, retenção e exposição de dados ao mínimo necessário.

6. Princípios de proteção de dados pessoais

Todo tratamento de dados pessoais realizado pela DPE-CE deve observar a boa-fé, a finalidade pública e os princípios previstos na LGPD. A aplicação prática desses princípios deve orientar decisões cotidianas, desenho de processos, desenvolvimento de sistemas, contratação de serviços, compartilhamento de dados e atendimento aos titulares.

Princípio	Aplicação prática na DPE-CE
Finalidade	Tratar dados apenas para propósitos legítimos, específicos, explícitos e vinculados às atribuições institucionais da DPE-CE.
Adequação	Garantir compatibilidade entre o tratamento e a finalidade informada ou institucionalmente documentada.
Necessidade	Limitar dados ao mínimo necessário para atendimento, defesa de direitos, gestão administrativa, execução de políticas públicas ou

Princípio	Aplicação prática na DPE-CE
	cumprimento legal.
Livre acesso	Permitir consulta facilitada e gratuita, nos termos da LGPD e dos procedimentos institucionais, sobre tratamento de dados pessoais.
Qualidade dos dados	Manter dados exatos, claros, relevantes e atualizados, respeitada a finalidade do tratamento.
Transparência	Disponibilizar informações claras, precisas e acessíveis, observados sigilo profissional, segredo de justiça, LAI e proteção de terceiros.
Segurança	Adotar medidas técnicas e administrativas para proteger dados contra acessos não autorizados e eventos acidentais ou ilícitos.
Prevenção	Adotar medidas para evitar danos aos titulares e à instituição.
Não discriminação	Impedir tratamentos para fins discriminatórios ilícitos ou abusivos.
Responsabilização e prestação de contas	Registrar decisões, demonstrar controles, revisar processos e manter documentação que comprove a governança de privacidade.

7. Diretrizes gerais de tratamento

- Todo tratamento deve possuir finalidade determinada, base legal adequada, responsável definido e registro mínimo de sua execução.
- Dados pessoais devem ser coletados de forma proporcional, evitando exigências excessivas ou incompatíveis com o serviço prestado.
- O acesso a dados pessoais deve ser limitado às pessoas autorizadas e às necessidades funcionais do processo, sistema ou atividade.
- O compartilhamento deve ser precedido de análise de finalidade, base legal, necessidade, segurança, responsabilidades e registro institucional.
- Dados pessoais devem ser armazenados em ambientes controlados, com medidas proporcionais ao risco e à sensibilidade das informações.
- A retenção deve observar prazos legais, regulatórios, administrativos, judiciais, arquivísticos e de defesa de direitos.
- A eliminação ou descarte deve ser seguro, rastreável quando necessário e compatível com as normas de gestão documental.
- Tratamentos de maior risco devem ser submetidos à avaliação de privacidade, podendo exigir RIPD, parecer técnico ou deliberação do comitê competente.

8. Bases legais aplicáveis

As bases legais devem ser identificadas antes do tratamento ou, quando se tratar de processos já existentes, revisadas durante o mapeamento e a governança contínua. No setor público, a DPE-CE deve priorizar bases relacionadas ao cumprimento de obrigações legais, execução de políticas públicas, exercício de competências institucionais, proteção da vida, tutela da saúde, exercício regular de direitos e demais hipóteses aplicáveis.

Base legal	Exemplos de aplicação na DPE-CE	Cuidados mínimos
Cumprimento de obrigação legal ou regulatória	Registros funcionais, prestação de contas, obrigações administrativas, processamento de informações exigidas por lei.	Documentar a norma ou obrigação que justifica o tratamento.
Execução de políticas públicas / competências legais	Atendimento jurídico-assistencial, defesa de direitos, gestão de programas institucionais, execução de serviços públicos.	Registrar a finalidade pública e limitar dados ao necessário.
Exercício regular de direitos	Atuação em processos judiciais, administrativos ou arbitrais, defesa institucional e documentação de atos.	Observar sigilo, segredo de justiça e proteção de terceiros.
Proteção da vida ou da incolumidade física	Situações urgentes envolvendo risco à vida ou integridade de assistidos(as), usuários(as) ou terceiros.	Restringir o uso ao contexto emergencial e registrar a justificativa.
Tutela da saúde	Quando aplicável em procedimentos conduzidos por profissionais ou serviços de saúde, assistência ou apoio.	Limitar acesso e aplicar proteção reforçada.
Consentimento	Hipóteses residuais, quando não houver outra base legal mais adequada e o titular puder manifestar vontade livre, informada e inequívoca.	Evitar uso indevido no setor público; prever revogação e registro.
Legítimo interesse	Aplicação excepcional, quando juridicamente cabível e precedida de avaliação de necessidade, expectativa do titular e mitigação de riscos.	Não usar quando houver prevalência de direitos do titular ou finalidade pública específica mais adequada.

9. Tratamento de dados pessoais na realidade da DPGE-CE

A DPGE-CE trata dados pessoais em atividades finalísticas e administrativas. Em razão de sua missão institucional, muitos tratamentos envolvem pessoas em situação de vulnerabilidade, dados sensíveis, documentos de identificação, dados socioeconômicos, dados familiares, informações de saúde, dados processuais, dados de crianças e adolescentes, informações de violência, registros de atendimento, procurações, declarações, provas documentais e comunicações com órgãos públicos ou privados.

9.1 Atividades finalísticas

- atendimento inicial, triagem, orientação jurídica, assistência jurídica integral e gratuita;
- representação judicial e extrajudicial de assistidos(as);
- defesa de grupos vulneráveis, atuação coletiva e promoção de direitos humanos;
- gestão de processos, documentos, audiências, comunicações processuais e prazos;

- encaminhamentos a redes de atendimento, órgãos públicos, entidades parceiras e serviços especializados;
- registro e acompanhamento de demandas individuais, coletivas, extrajudiciais e administrativas.

9.2 Atividades administrativas e de apoio

- gestão de pessoas, folha, estágio, capacitação, saúde ocupacional, frequência e avaliação funcional;
- contratações públicas, gestão de fornecedores, contratos, pagamentos, fiscalização contratual e prestação de contas;
- segurança patrimonial, controle de acesso, gestão de visitantes e proteção de ambientes institucionais;
- tecnologia da informação, suporte, credenciais, logs, redes, e-mails e sistemas;
- comunicação institucional, eventos, ouvidoria, canais digitais e atendimento ao cidadão;
- auditoria, controle interno, integridade, gestão de riscos e governança institucional.

10. Dados pessoais sensíveis e grupos vulneráveis

Dados pessoais sensíveis exigem proteção reforçada. A DPGE-CE deve restringir seu uso ao necessário para cumprir finalidade institucional legítima, garantir direitos, prestar atendimento adequado, exercer atribuições legais ou cumprir decisões e procedimentos oficiais. O tratamento desses dados deve observar controles de acesso, sigilo funcional, registro adequado, comunicação limitada e maior cautela em compartilhamentos.

- **Crianças e adolescentes:** o tratamento deve observar o melhor interesse, a proteção integral, a necessidade e a restrição de acesso.
- **Pessoas em situação de violência ou vulnerabilidade:** o tratamento deve preservar segurança, dignidade, sigilo e não exposição indevida.
- **Dados de saúde, orientação, condição social ou familiar:** devem ser tratados apenas quando necessários para o atendimento, defesa de direitos ou cumprimento de obrigação legal.
- **Dados biométricos ou genéticos:** somente devem ser utilizados quando houver necessidade comprovada, base legal adequada, controles reforçados e avaliação de impacto quando aplicável.
- **Dados processuais sigilosos:** devem observar segredo de justiça, sigilo profissional, regras processuais e acesso restrito.

11. Direitos dos titulares

A DPGE-CE deve disponibilizar canal e procedimento para atendimento aos direitos dos titulares, observadas as limitações legais, o sigilo profissional, o segredo de justiça, a proteção de terceiros, a segurança institucional e as competências públicas da Defensoria.

Direito do titular	Tratamento institucional
Confirmação e acesso	Informar, quando cabível, se há tratamento de dados pessoais e permitir acesso conforme procedimento interno.
Correção	Permitir correção de dados incompletos, inexatos ou desatualizados, quando cabível e tecnicamente possível.
Anonimização, bloqueio ou eliminação	Avaliar pedidos relacionados a dados desnecessários, excessivos ou tratados em desconformidade.

Direito do titular	Tratamento institucional
Portabilidade	Avaliar conforme regulamentação aplicável, viabilidade técnica e restrições do setor público.
Informação sobre compartilhamento	Informar entidades públicas e privadas com as quais houve compartilhamento, quando cabível.
Revogação do consentimento	Permitir revogação quando o consentimento for a base legal do tratamento.
Revisão de decisões automatizadas	Disponibilizar revisão quando houver decisão tomada unicamente com base em tratamento automatizado que afete interesses do titular.
Peticionamento à ANPD	Orientar o titular sobre a possibilidade de peticionar à ANPD, preferencialmente após manifestação da DPE-CE.

12. Atendimento aos titulares

- O atendimento aos titulares deve possuir fluxo próprio, canal identificado, registro da solicitação, controle de prazo, análise de identidade e resposta formal.
- A DPGE-CE deve adotar linguagem clara, acessível e compatível com o perfil do solicitante, evitando excesso de termos técnicos.
- A resposta poderá ser limitada ou negada quando houver fundamento legal, segredo de justiça, sigilo profissional, proteção de terceiro, segurança institucional ou impossibilidade técnica justificada.
- Pedidos que envolvam dados de terceiros, processos sigilosos ou informações sensíveis devem ser analisados com cautela e, quando necessário, submetidos ao Encarregado(a), à unidade jurídica ou à autoridade competente.
- As solicitações e respostas devem ser registradas para fins de controle, rastreabilidade, melhoria contínua e prestação de contas.

Etapa	Descrição	Responsável sugerido	Registro mínimo
Recebimento	Receber demanda por canal oficial e classificar o pedido.	Unidade de atendimento / EPD	Protocolo, data, titular, descrição.
Validação	Confirmar identidade, legitimidade e escopo do pedido.	Unidade responsável / EPD	Documentos de validação e análise de legitimidade.
Análise	Verificar dados envolvidos, base legal, restrições e providências possíveis.	Área gestora / EPD / jurídico quando necessário	Parecer ou despacho de análise.
Resposta	Responder ao titular de modo claro, fundamentado e acessível.	EPD ou unidade designada	Resposta enviada, data e meio

Etapa	Descrição	Responsável sugerido	Registro mínimo
			utilizado.
Encerramento	Registrar resultado e arquivar a solicitação.	EPD / área gestora	Status, providências e lições aprendidas.

13. Transparência, avisos de privacidade e linguagem acessível

A DPGE-CE deve disponibilizar informações claras sobre o tratamento de dados pessoais, respeitando a Lei de Acesso à Informação, a LGPD, o sigilo profissional, o segredo de justiça, a segurança da informação e a proteção de dados de terceiros. A transparência deve ser proporcional ao contexto do tratamento, sem expor dados pessoais ou informações protegidas.

- Publicar, quando aplicável, aviso de privacidade em páginas, formulários, sistemas e canais digitais que coletem dados pessoais.
- Informar a finalidade, a base legal, as categorias de dados, os titulares afetados, os compartilhamentos relevantes, os canais de atendimento e os direitos dos titulares.
- Utilizar linguagem simples para assistidos(as), usuários(as) e público externo, especialmente em serviços de grande alcance social.
- Disponibilizar versões resumidas ou avisos por camadas em canais digitais, mantendo documentação completa em repositório institucional.
- Evitar a divulgação pública de dados pessoais, documentos, imagens, áudios, vídeos ou informações processuais sem base legal, finalidade legítima e controle adequado.

14. Cookies, portais e serviços digitais

Os portais, sites, formulários eletrônicos, aplicativos e demais serviços digitais utilizados pela DPGE-CE devem observar práticas de transparência e minimização no uso de cookies, tecnologias de rastreamento, registros de acesso e dados de navegação. Cookies essenciais à prestação do serviço podem ser utilizados conforme necessidade técnica, enquanto cookies analíticos, de desempenho ou de terceiros devem ser avaliados quanto à finalidade, necessidade, transparência e possibilidade de escolha do usuário.

- Manter aviso de cookies claro, acessível e compatível com as funcionalidades utilizadas.
- Evitar coleta excessiva de dados de navegação ou uso de tecnologias incompatíveis com a finalidade pública do serviço.
- Documentar ferramentas de terceiros utilizadas em canais digitais e avaliar riscos de compartilhamento indevido.
- Permitir gestão de preferências quando houver cookies não essenciais.
- Revisar periodicamente scripts, plugins, ferramentas analíticas, formulários e integrações externas.

15. Compartilhamento de dados e interoperabilidade

O compartilhamento de dados pessoais pela DPGE-CE deve ocorrer apenas quando houver finalidade institucional legítima, base legal adequada, necessidade demonstrada, segurança compatível e registro mínimo da operação. O compartilhamento pode ocorrer com órgãos do sistema de justiça, órgãos

públicos, entidades da rede de atendimento, parceiros institucionais, operadores e fornecedores, respeitados sigilo profissional, segredo de justiça, proteção de terceiros e demais restrições legais.

Situação de compartilhamento	Requisitos mínimos
Órgãos públicos e sistema de justiça	Finalidade pública, competência legal, necessidade, registro e proteção de dados sensíveis.
Rede de atendimento e políticas públicas	Encaminhamento necessário, minimização, proteção da pessoa atendida e controle de acesso.
Fornecedores e operadores	Contrato ou instrumento formal, cláusulas de privacidade, segurança, confidencialidade e responsabilidade.
Pesquisas, estatísticas e transparência	Preferir anonimização ou agregação; avaliar risco de reidentificação.
Publicação de informações	Observar LAI, LGPD, sigilos legais, anonimização quando cabível e proteção de terceiros.

16. Operadores, fornecedores e terceiros

- Contratos, convênios e instrumentos congêneres que envolvam dados pessoais devem conter cláusulas de privacidade, confidencialidade, segurança da informação, comunicação de incidentes, subcontratação, auditoria, eliminação ou devolução de dados e responsabilização.
- Operadores devem tratar dados apenas conforme instruções documentadas da DPGE-CE e não podem utilizar dados para finalidades próprias incompatíveis.
- Antes da contratação de serviços relevantes, especialmente tecnologia, nuvem, atendimento, suporte, gestão documental ou sistemas, a unidade demandante deve avaliar riscos de privacidade e segurança.
- Fornecedores devem comunicar incidentes, vulnerabilidades ou acessos indevidos em prazo compatível com os procedimentos da DPGE-CE.
- A DPGE-CE deve manter inventário ou registro de operadores relevantes e dos tratamentos realizados por terceiros.

17. Segurança da informação, confidencialidade e controle de acesso

A proteção de dados pessoais depende de medidas técnicas e administrativas compatíveis com risco, sensibilidade e volume dos dados tratados. A Política de Segurança da Informação da DPGE-CE deve ser aplicada de forma integrada a esta política, especialmente em temas de controle de acesso, senhas, registro de logs, backup, criptografia quando aplicável, classificação da informação, gestão de vulnerabilidades, monitoramento, resposta a incidentes e continuidade de serviços.

- Aplicar privilégio mínimo e necessidade de saber no acesso a dados pessoais.
- Revisar periodicamente perfis de acesso, especialmente em desligamentos, mudanças de lotação, afastamentos e mudanças de função.
- Proteger credenciais, dispositivos, e-mails, mídias removíveis, arquivos físicos e digitais.

- Registrar acessos e operações críticas quando tecnicamente possível e proporcional.
- Evitar envio de dados pessoais sensíveis por canais não seguros ou sem necessidade comprovada.
- Utilizar anonimização, pseudonimização, mascaramento ou agregação sempre que tais medidas reduzirem riscos sem comprometer a finalidade institucional.
- Realizar backup, testes de restauração e controles de continuidade para serviços críticos.

18. Privacy by Design e Privacy by Default

A DPE-CE deve incorporar privacidade desde a concepção e por padrão em projetos, processos, serviços, sistemas, contratações e alterações relevantes. Nenhum novo projeto que envolva dados pessoais deve ser implantado sem avaliação mínima de finalidade, necessidade, base legal, riscos, controles, responsáveis e impacto sobre titulares.

Fase	Diretriz de privacidade	Registro recomendado
Abertura da demanda	Definir finalidade, público, dados necessários e unidade responsável.	Termo de abertura ou registro da demanda.
Avaliação preliminar	Identificar dados pessoais, sensíveis, titulares, bases legais, compartilhamentos e riscos.	Checklist de privacidade ou triagem preliminar.
Desenho da solução	Aplicar minimização, controle de acesso, retenção limitada, transparência e segurança.	Requisitos de privacidade e segurança.
Contratação/desenvolvimento	Incluir cláusulas, controles, testes e requisitos de operadores.	Termo de referência, contrato, matriz de riscos.
Implantação	Validar configurações padrão mais protetivas e orientar usuários.	Homologação, checklist, comunicado.
Monitoramento	Revisar riscos, incidentes, métricas, reclamações e oportunidades de melhoria.	Relatórios, atas, indicadores, plano de ação.

Configurações padrão mínimas

Novos sistemas ou serviços devem iniciar com coleta mínima, acesso restrito, compartilhamento desativado quando não necessário, retenção limitada, logs proporcionais, comunicação clara ao titular e revisão periódica de permissões.

19. Retenção, arquivamento e descarte

Dados pessoais devem ser mantidos apenas pelo tempo necessário ao cumprimento de finalidades institucionais, obrigações legais, prazos administrativos, prazos judiciais, gestão documental, controle

interno, prestação de contas e exercício regular de direitos. A retenção deve ser compatível com tabela de temporalidade, normas arquivísticas, regras processuais e diretrizes internas.

- Definir prazos de guarda por categoria de documento, processo, sistema ou finalidade.
- Evitar manutenção indefinida de bases sem finalidade atual ou obrigação de guarda.
- Eliminar, anonimizar ou bloquear dados quando cessada a finalidade e inexistir obrigação de retenção.
- Realizar descarte seguro de documentos físicos e mídias digitais.
- Registrar descartes relevantes e manter trilha de auditoria quando exigido por norma interna ou risco do tratamento.

20. Relatório de Impacto à Proteção de Dados Pessoais - RIPD

O RIPD deve ser utilizado como instrumento de governança para tratamentos que possam gerar riscos relevantes aos titulares, especialmente quando envolverem dados sensíveis, crianças e adolescentes, pessoas vulneráveis, grande volume de dados, monitoramento sistemático, decisões automatizadas, novas tecnologias, compartilhamentos amplos, tratamento de dados de acesso restrito ou operações que possam impactar direitos fundamentais.

- O RIPD deve descrever o tratamento, finalidades, bases legais, dados envolvidos, titulares, agentes, compartilhamentos, medidas de segurança, riscos e salvaguardas.
- A atualização do RIPD deve ocorrer quando novos riscos forem mapeados, quando houver mudança relevante no tratamento ou quando ocorrer incidente significativo.
- A elaboração ou revisão do RIPD deve contar com a participação da área demandante, Encarregado(a), TI, segurança da informação, área jurídica e outras unidades envolvidas, conforme o caso.
- As recomendações do RIPD devem gerar plano de ação, responsáveis, prazos e acompanhamento periódico.

21. Incidentes de segurança com dados pessoais

Incidentes de segurança envolvendo dados pessoais devem ser tratados conforme plano institucional de resposta a incidentes, com registro, triagem, classificação, contenção, investigação, avaliação de risco, comunicação interna, comunicação aos titulares e à ANPD quando cabível, recuperação e lições aprendidas. A comunicação à ANPD deve observar o regulamento vigente e os prazos aplicáveis, incluindo a comunicação em até 3 dias úteis quando o incidente puder acarretar risco ou dano relevante aos titulares.

Etapa	Providência mínima	Responsável principal
Identificação	Registrar suspeita ou confirmação de incidente, data, origem, sistemas afetados e dados envolvidos.	Usuário, área gestora, TI ou segurança.
Triagem	Classificar severidade, risco aos titulares, abrangência, sensibilidade e necessidade de contenção.	TI, Segurança da Informação, EPD.

Etapa	Providência mínima	Responsável principal
Contenção	Reduzir exposição, bloquear acesso indevido, preservar registros e estabilizar ambiente.	TI e Segurança da Informação.
Análise jurídica e de privacidade	Avaliar risco ou dano relevante, titulares afetados, comunicação e medidas de mitigação.	EPD, jurídico, área gestora.
Comunicação	Comunicar ANPD e titulares quando cabível, com linguagem clara e orientações práticas.	Autoridade competente / EPD.
Encerramento	Documentar causa, medidas corretivas, lições aprendidas e atualização de controles.	EPD, TI, Segurança, área gestora.

22. Transferência internacional de dados

Transferências internacionais de dados pessoais somente devem ocorrer quando houver fundamento legal, necessidade institucional, controle contratual, avaliação de risco e salvaguardas adequadas. O uso de serviços em nuvem, ferramentas de colaboração, suporte técnico internacional, armazenamento fora do Brasil ou fornecedores globais deve ser analisado sob a perspectiva de transferência internacional, segurança, contrato, suboperadores e transparência.

- Identificar países, fornecedores, suboperadores e bases de transferência.
- Verificar cláusulas contratuais, medidas técnicas e responsabilidades.
- Garantir que dados sejam tratados apenas para finalidade definida pela DPE-CE.
- Registrar a avaliação e submeter casos relevantes ao Encarregado(a), jurídico e TI.

23. Governança, papéis e responsabilidades

A governança de privacidade deve ser integrada às instâncias de governança, integridade, conformidade, segurança da informação, gestão de riscos, tecnologia da informação, contratação pública e gestão administrativa da DPE-CE. A responsabilização e a prestação de contas exigem papéis claros, registros, ritos de acompanhamento e revisão contínua.

Ator	Responsabilidades principais
Alta Administração	Aprovar diretrizes, prover apoio institucional, priorizar recursos e promover cultura de privacidade.
CGIC ou instância equivalente	Acompanhar diretrizes estruturantes, deliberar temas críticos, monitorar planos e integrar privacidade à governança institucional.
Encarregado(a) / EPD	Atuar como canal de comunicação, orientar unidades, apoiar titulares, acompanhar incidentes, revisar riscos e promover boas práticas.
Unidades gestoras	Identificar tratamentos, manter registros, cumprir diretrizes, proteger dados sob sua responsabilidade e implementar planos de

Ator	Responsabilidades principais
	ação.
TI e Segurança da Informação	Implementar controles técnicos, gerir acessos, monitorar riscos, apoiar incidentes, backups, logs e segurança dos sistemas.
Jurídico / Assessoria técnica	Apoiar interpretação legal, bases jurídicas, contratos, compartilhamentos, restrições de acesso e respostas complexas.
Gestão de Pessoas	Aplicar diretrizes em registros funcionais, capacitação, ciência dos colaboradores e desligamentos.
Contratações e fiscalização contratual	Incluir cláusulas, exigir controles de operadores, monitorar obrigações e registrar conformidade contratual.
Colaboradores e usuários internos	Cumprir a política, proteger credenciais, comunicar incidentes e tratar dados apenas para finalidades autorizadas.
Operadores e fornecedores	Tratar dados conforme contrato, manter segurança, comunicar incidentes e não usar dados para finalidades próprias incompatíveis.

24. Capacitação e cultura de privacidade

- A DPGE-CE deve promover capacitações periódicas sobre LGPD, privacidade, segurança da informação, atendimento aos titulares, incidentes e condutas esperadas.
- Novos colaboradores devem receber orientação básica sobre privacidade e proteção de dados no processo de integração.
- Unidades que tratam dados sensíveis ou de alto risco devem receber orientações específicas.
- Campanhas internas devem reforçar sigilo, cuidado com documentos, uso adequado de e-mails, controle de acesso, descarte seguro e comunicação de incidentes.
- Registros de capacitação, comunicados e materiais de orientação devem ser mantidos para controle e melhoria contínua.

25. Monitoramento, indicadores e melhoria contínua

A implementação desta política deve ser monitorada por meio de registros, indicadores e revisões periódicas. O acompanhamento deve permitir identificação de fragilidades, priorização de ações, atualização de controles e prestação de contas.

Indicador sugerido	Periodicidade	Finalidade
Solicitações de titulares recebidas e respondidas	Mensal ou trimestral	Avaliar demanda, prazos e qualidade das respostas.
Tratamentos mapeados e atualizados	Trimestral	Monitorar maturidade do inventário e governança.

Indicador sugerido	Periodicidade	Finalidade
RIPDs elaborados ou revisados	Trimestral	Acompanhar tratamentos de maior risco.
Incidentes registrados e tratados	Mensal ou por ocorrência	Aprimorar segurança e resposta a incidentes.
Revisões de acesso realizadas	Trimestral ou semestral	Reduzir riscos de acesso indevido.
Contratos com cláusulas de privacidade	Trimestral	Monitorar conformidade de operadores e fornecedores.
Capacitações realizadas e participantes	Semestral	Fortalecer cultura institucional.
Planos de ação concluídos	Trimestral	Acompanhar evolução das medidas corretivas.

26. Descumprimento da política

O descumprimento desta política, de normas internas de segurança, de obrigações contratuais ou de regras de confidencialidade poderá ensejar medidas administrativas, contratuais, disciplinares ou outras providências cabíveis, respeitados o devido processo, a legislação aplicável, a natureza da ocorrência, a gravidade, a reincidência e a existência de dano ou risco aos titulares e à instituição.

- A utilização indevida de dados pessoais deve ser comunicada aos canais internos competentes.
- Colaboradores devem cooperar com apurações, preservar registros e não ocultar incidentes.
- Fornecedores e operadores podem estar sujeitos a sanções contratuais, suspensão de acesso, rescisão e responsabilização por danos.
- Medidas corretivas devem priorizar proteção dos titulares, recuperação dos controles e prevenção de reincidência.

27. Disposições finais

Esta política entra em vigor após aprovação pela autoridade competente ou instância institucional designada pela DPGE-CE, devendo ser divulgada aos públicos internos e, quando aplicável, disponibilizada em formato público, simplificado e acessível aos titulares. Casos omissos devem ser avaliados pelo Encarregado(a), pelas unidades competentes e pelas instâncias de governança, observadas a LGPD, as orientações da ANPD, a legislação aplicável e as boas práticas de administração pública.

Esta política deve ser interpretada em conjunto com a Política de Segurança da Informação, o Plano de Resposta a Incidentes, o Plano de Contingência, o Inventário de Dados Pessoais, os Relatórios de Impacto à Proteção de Dados Pessoais, as normas de gestão documental, as políticas de contratação de terceiros e demais instrumentos internos de governança, integridade, conformidade e controle.

Anexo I - Matriz de responsabilidades

Atividade	Área demandante	EPD	TI/Segurança	Jurídico	CGIC	Operador/Fornecedor
Identificar novo tratamento de dados	R	C	C	C	I	I
Definir finalidade e necessidade	R	C	C	C	I	I
Indicar base legal	C	R	I	C	I	I
Realizar triagem de privacidade	C	R	C	C	I	I
Elaborar ou atualizar RIPD	C	R	C	C	A	I
Implementar controles técnicos	C	C	R	I	I	C
Incluir cláusulas de privacidade	C	C	C	R	I	C
Atender solicitação de titular	C	R	C	C	I	I
Gerir incidente de segurança	C	R	R	C	I/A	C
Monitorar indicadores	C	R	C	I	A	I

Legenda: R = responsável pela execução; A = aprovador ou autoridade de decisão; C = consultado; I = informado. A matriz pode ser ajustada conforme estrutura interna, complexidade do tratamento e rito decisório aplicável.

Anexo II - Checklist mínimo de conformidade

Nº	Pergunta de controle	Sim/Não/Parcial	Observação
1	A finalidade do tratamento está documentada?		
2	A base legal foi definida e validada?		
3	Os dados coletados são necessários e proporcionais?		
4	Há tratamento de dados sensíveis ou de pessoas		

Nº	Pergunta de controle	Sim/Não/Parcial	Observação
	vulneráveis?		
5	Foi avaliada a necessidade de RIPD?		
6	Foram definidos responsáveis e controles de acesso?		
7	Há compartilhamento com órgãos, parceiros, fornecedores ou operadores?		
8	Existem cláusulas contratuais de privacidade e segurança quando aplicável?		
9	O titular recebeu informação clara sobre o tratamento quando cabível?		
10	Há prazo de retenção e regra de descarte definidos?		
11	Foram avaliados riscos de segurança e privacidade?		
12	Há procedimento para atendimento de titulares e incidentes?		

Anexo III - Modelo de registro de tratamento

Campo	Descrição a preencher
Nome do processo ou atividade	Identificação do processo, sistema, serviço, formulário ou base de dados.
Unidade responsável	Área gestora do tratamento.
Finalidade	Propósito específico e institucional do tratamento.
Base legal	Hipótese legal aplicável, com referência normativa quando necessário.
Categorias de titulares	Assistidos(as), usuários, servidores, defensores, fornecedores, visitantes, terceiros etc.
Categorias de dados	Dados cadastrais, processuais, documentos, dados sensíveis, dados de acesso, imagens, áudios etc.
Dados sensíveis	Indicar se há e qual o cuidado adicional.
Compartilhamentos	Órgãos, entidades, fornecedores, operadores ou parceiros envolvidos.
Sistemas e repositórios	Local onde os dados são armazenados ou processados.
Controles de segurança	Acesso restrito, autenticação, logs, backup, criptografia,

Campo	Descrição a preencher
	segregação etc.
Prazo de retenção	Prazo ou critério de guarda e descarte.
Riscos identificados	Riscos aos titulares e à instituição.
Medidas de mitigação	Controles existentes e ações planejadas.
Responsável pela revisão	Nome ou função responsável pela atualização do registro.
Data da última revisão	Data de revisão mais recente.

Anexo IV - Referências técnicas

BRASIL. Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD.

BRASIL. Lei nº 12.527/2011 - Lei de Acesso à Informação - LAI.

ANPD. Guia orientativo: tratamento de dados pessoais pelo Poder Público.

ANPD. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.

ANPD. Guia orientativo: cookies e proteção de dados pessoais.

ANPD. Resolução CD/ANPD nº 18/2024 - Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.

ANPD. Resolução CD/ANPD nº 15/2024 - Regulamento de comunicação de incidente de segurança.

TCU. Materiais institucionais sobre LGPD, governança, accountability, segurança da informação e controle público.

CGU. Orientações e práticas institucionais sobre tratamento de dados pessoais, transparência pública e compartilhamento de dados.

ABNT NBR ISO/IEC 29100 - Estrutura de privacidade.

ABNT NBR ISO/IEC 27001 - Sistema de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002 - Controles de segurança da informação.

ABNT NBR ISO/IEC 27005 - Gestão de riscos de segurança da informação.

ABNT NBR ISO/IEC 27701 - Sistema de gestão de privacidade da informação.

ABNT NBR ISO/IEC 29134 - Avaliação de impacto à privacidade.

Cláusula de controle documental

A versão oficial desta política deve ser mantida em repositório institucional controlado. Cópias impressas ou arquivos locais devem ser considerados cópias não controladas, salvo quando expressamente validados pela unidade responsável.