



Conselho Nacional de  
Proteção de Dados  
Pessoais e da Privacidade

Mecanismos,  
Instâncias e Práticas de  
Conformidade  
de Proteção de Dados

GTT 2

2025





## **Relatório Final do GT2 do CNPD**

### **Mecanismos, instâncias e práticas de conformidade de proteção de dados, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade<sup>1</sup>**

#### **Introdução**

O presente relatório apresenta os resultados dos trabalhos desenvolvidos pelo Grupo de Trabalho 2 (GT2) do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), constituído com o objetivo de fornecer subsídios para o desenvolvimento de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, especificamente no que tange aos mecanismos, instâncias e práticas de conformidade de proteção de dados pessoais.

O GT2 conduziu suas atividades entre outubro de 2024 e janeiro de 2025, realizando uma série de reuniões que contaram com a participação de especialistas nacionais e internacionais, representantes do setor público e privado, bem como acadêmicos e profissionais com reconhecida experiência na área de proteção de dados pessoais.

A metodologia adotada pelo grupo consistiu em:

---

<sup>1</sup>[Portaria CNPD nº 02, de 4 de outubro de 2024- Institui Grupo de Trabalho dedicado a fornecer subsídios, na temática de mecanismos, instâncias e práticas de conformidade de proteção de dados, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.](#)



1. Reuniões periódicas para discussão e alinhamento dos trabalhos;
2. Convite a especialistas para apresentação de diferentes perspectivas sobre o tema;
3. Análise de práticas nacionais e internacionais de conformidade em proteção de dados pessoais;
4. Identificação dos principais desafios enfrentados por organizações públicas e privadas;
5. Elaboração de propostas de diretrizes para a Política Nacional.

Entre os especialistas convidados, o GT2 contou com contribuições de:

- Marcel Leonardi (Advogado especialista em Direito Digital. Pós-Doutor em Direito pela University of California at Berkeley (2009). Doutor (2009), Mestre (2004) e Bacharel (1997) em Direito pela Universidade de São Paulo. Professor do Programa de Pós-Graduação Lato Sensu da FGV DIREITO SP. Assessor científico da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP). Diretor de Políticas Públicas do Google no Brasil. Foi advogado sócio de Leonardi Advogados e policy fellow na Electronic Frontier Foundation. Atua principalmente nos seguintes temas: Internet, direito, regulação, privacidade, segurança e proteção de dados pessoais, tutela e responsabilidade civil.)
- Andréia Saad (Legal Director and Data Protection Officer no Grupo Globo - Mídia e Conteúdo)



- Fabrício Guimarães Madruga Lopes (Coordenador-Geral de Fiscalização da ANPD. Especialização em Regulação de Serviços Públicos de Telecomunicações pela Universidade de Brasília.)
- Matthew Reisman (Centre for Information Policy Leadership – CIPL. Matthew Reisman is Director of Privacy and Data Policy in the Centre for Information Policy Leadership's Washington, DC office. In this role, Matthew is helping to advance responsible approaches to privacy, data protection, data governance, artificial intelligence, and other data-intensive domains in the U.S. and globally. Prior to joining CIPL, Matthew was a Director of Global Privacy Policy at Microsoft. In this role, he helped shape the company's advocacy on privacy and data policy, including intersections with security, digital safety, trade, data governance, and trustworthy cross-border data flows. Matthew previously led Microsoft's advocacy on international trade policy, including trade-related aspects of data protection, emerging technologies such as 5G and AI, export controls, supply chain security, and cybersecurity. He also led efforts to foster more economically inclusive approaches to trade. Across these roles, Matthew drove Microsoft's engagement with policymakers, the business community, and civil society and partnered closely with Microsoft field teams in the Asia-Pacific region, Latin America, the Middle East, Africa, and Europe. Matthew previously led research on the digital economy for Congress, the Executive Branch, and the public as a civil servant at the United States International Trade Commission. He also served as an advisor to emerging economies on international trade and investment policy through programs funded by the United States Agency for International Development and the World Bank. Matthew serves on the



Strategic Council of the Silverado Policy Accelerator and as a Visiting Scholar at the Digital Trade and Data Governance Hub at The George Washington University.)

- Mark Smith (Centre for Information Policy Leadership – CIPL. Mark is the Manager of Privacy and Data Policy at Hunton Andrews Kurth LLP's Centre for Information Policy Leadership (CIPL), a preeminent global privacy and security policy think tank with offices in Washington, London, and Brussels. Based in Washington, Mark works closely with team members to develop strategies and implement project plans that advance CIPL's U.S. and global policy agenda on a wide range of privacy and data protection issues. Prior to joining Hunton, Mark served for 11 years at Bloomberg Law. He covered federal, state, and international privacy law developments, and he created practical guidance pertaining to data collection practices and incident response management. Mark has written extensively on privacy law developments—including articles on consumer privacy rights, business obligations, consent protocols, data transfers. Mark is a graduate of Loyola University Maryland and the University of Maryland School of Law, and he holds three certifications (CIPP/US, CIPP/C, CIPM) from the International Association of Privacy Professionals. He currently serves as a co-chair of the IAPP Knowledge Net Chapter for Washington, D.C.)
- Fabrício da Mota Alves (Advogado especialista em Direito Digital. Tem vasta experiência na área, tendo participado ativamente no processo legislativo que levou à edição da Lei Geral de Proteção de Dados Pessoais brasileira. Foi assessor legislativo sênior do Senado Federal e



participou da Comissão de Juristas que elaborou o projeto de lei de regulação da Inteligência Artificial no Brasil. Coordenador jurídico da Frente Parlamentar de Proteção de Dados da Câmara dos Deputados. Foi representante do Senado Federal no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, órgão que compõe a Autoridade Nacional de Proteção de Dados. Professor de Proteção de Dados em São Paulo (Insper, LEC, Escola Paulista de Direito e Opice Blum Academy), Distrito Federal (IDP e ATAME), Paraná (PUC), Rio de Janeiro (FGV) e Recife.

- Marison Souza Gomes (COO e Co-Fundador da empresa Privacy Tools, profissional com mais de 25 anos de experiência em Tecnologia da Informação, especializado em Segurança da Informação, Proteção de Dados e Compliance Regulatória. Graduado em Sistemas de Informação pela Unisinos, com especializações em Privacy e Data Protection pela Universidade de Harvard e Compliance Regulatory pela Universidade da Pensilvânia, COO da Privacy Tools, que desenvolve soluções para proteção de dados e privacidade, e da MavenInventing, empresa focada em desenvolvimento de software e consultoria tecnológica. Tem como principais especialidades programação, análise de código-fonte, LGPD, privacidade e proteção de dados, contratos de TI, propriedade intelectual e marcas de software, blockchain, cibersegurança, pirataria, fraudes digitais, senhas, análises de áudio/vídeo e fotos, e licenciamento de software. Possui qualificações técnicas em blockchain, desenvolvimento de software e DevOps, atuando de maneira abrangente e aprofundada em casos que envolvem tecnologia avançada e conformidade regulatória.)



As discussões e análises realizadas pelo grupo buscaram contemplar diferentes perspectivas e realidades do cenário brasileiro, considerando desde pequenas e médias empresas até grandes corporações, bem como as especificidades do setor público. O objetivo foi desenvolver propostas que pudessem contribuir para uma política nacional efetiva e adequada à realidade do país, promovendo a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e, ao mesmo tempo, incentivando o desenvolvimento econômico e tecnológico e a inovação.

Este relatório está estruturado em três partes principais:

1. Histórico das atividades desenvolvidas
2. Produtos elaborados
3. Parecer conclusivo com recomendações para a Política Nacional de Proteção de Dados Pessoais e da Privacidade.



## **1 – Histórico das Atividades Desenvolvidas**

Conforme definido no Plano de Trabalho, os objetivos apresentados ao CNPD foram de fornecer subsídios, na temática de mecanismos, instâncias e práticas de conformidade de proteção de dados, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

O Trabalho foi realizado a partir da seguinte metodologia:

**1. Pesquisa e Análise Comparativa:**

- Levantamento e análise de legislações e boas práticas nacionais e internacionais em conformidade de proteção de dados pessoais.
- Revisão das diretrizes e regulamentações brasileiras existentes.

**2. Consultas e Entrevistas com Especialistas:**

- Reuniões e entrevistas com especialistas e stakeholders relevantes, como representantes de setores impactados e advogados especializados em proteção de dados pessoais e conformidade.

**3. Oficinas de Trabalho e Grupos de Discussão:**

- Realização de workshops com membros do GT para discutir propostas e identificar pontos críticos e lacunas na conformidade e privacidade de dados pessoais.

**4. Validação e Finalização do Relatório:**

- Consolidação dos dados coletados e elaboração do relatório final, com recomendações práticas e viáveis.



A partir destas diretrizes foram realizados 9 encontros, conforme cronograma das atividades apresentadas junto ao plano de trabalho, nos dias 31/10/2024; 07/11/2024; 14/11/2024; 28/11/2024; 05/12/2024; 12/12/2024; 19/12/2024, 16/01/2025 e 30/01/2025, cujos resumos seguem abaixo e as Atas das reuniões seguirão em documento apartado.

<b>Data</b>	<b>Resumo da Reunião</b>
31/10/2024	Os conselheiros discutiram sobre a necessidade de elaboração e entrega do cronograma dos trabalhos GT, bem como debateram sobre os possíveis especialistas a serem convidados para contribuições nas reuniões seguintes.
07/11/2024	<p><b>Especialista convidado: Marcel Leonardi</b></p> <p><b>Principais pontos abordados pelo convidado:</b></p> <ol style="list-style-type: none"> <li>1. Importância da Política Nacional de Proteção de Dados Pessoais <ul style="list-style-type: none"> <li>• Destacou que a política deve priorizar o "espírito da lei", buscando resultados efetivos na proteção de dados, em vez de focar apenas em conformidade burocrática ou checklists.</li> </ul> </li> </ol>



## 2. Compliance e Conformidade

- Observou que muitas empresas e órgãos públicos têm dificuldade em aplicar a LGPD, principalmente por falta de orientação clara.
- Alertou contra a visão de que "melhores práticas" ou checklists sejam suficientes para garantir a conformidade e que a ANPD deve ater-se menos à forma e mais ao conteúdo, de modo que distintos mecanismos e formas sejam considerados para fins de conformidade.
- Propôs o conceito de "melhores esforços" como alternativa prática para atender às exigências da lei, principalmente para empresas menores e órgãos públicos.

## 3. Diálogo Multissetorial

- Reforçou a importância do diálogo contínuo entre a ANPD, empresas, setor público, acadêmicos e ONGs para alinhar práticas e expectativas.
- Criticou a falta de articulação entre a ANPD e os regulados, sugerindo maior transparência nos processos e maior participação dos setores interessados.

## 4. Educação e Comunicação

- Ressaltou a necessidade de campanhas educativas e materiais didáticos com linguagem acessível.
- Exemplificou com iniciativas internacionais, como o site do ICO (*Information Commissioner's Office*, Autoridade de Proteção de Dados Pessoais do Reino Unido), que oferece guias específicos para diferentes públicos (empresas, cidadãos etc.).
- Citou a cartilha da Turma da Mônica como um exemplo inicial de material educativo no Brasil.



	<p><b>5. Exemplos Práticos e Referências Internacionais</b></p> <ul style="list-style-type: none"> <li>Mencionou o ICO e a CNIL (<i>Commission Nationale de l'informatique et des Libertés</i>, Autoridade de Proteção de Dados Pessoais da França) como referências de boas práticas.             <ul style="list-style-type: none"> <li>ICO: Auditorias “educacionais”, mediante solicitação das próprias empresas, a fim de verificar a conformidade de processos.</li> <li>CNIL: Abordagem prática para desafios técnicos como blockchain e retenção de dados em backups.</li> </ul> </li> <li>Destacou a necessidade de adaptar as melhores práticas internacionais à realidade brasileira.</li> </ul> <p><b>6. Recomendações para a Política Nacional</b></p> <ul style="list-style-type: none"> <li>Incluir mecanismos que incentivem boas práticas, mas sem torná-las obrigatórias ou inviáveis para agentes de tratamento, especialmente os de pequeno porte.</li> <li>Garantir revisões periódicas do entendimento sobre a LGPD (assim como GDPR), a fim de sua eficácia e propor ajustes.</li> <li>Encorajar associações setoriais a criarem guias, orientações e autorregulações específicas para seus membros.</li> </ul>
14/11/2024	<p><b>Especialistas convidados: Andréia Saad e Fabrício Guimarães Madruga Lopes</b></p> <p><b>Principais pontos abordados por Andréia Saad (DPO Globo):</b></p>



1. Implementação do Programa de Conformidade da Globo:

- Falou sobre o programa de conformidade da Globo, criado em 2019 com base na LGPD e práticas de mercado internacional.

2. Desafios Operacionais:

- Incertezas sobre a regulamentação e interpretação da LGPD.
- Necessidade de revisar constantemente políticas e processos com base nos direcionamentos da ANPD.

3. Soluções Propostas:

- Criação de guias concretos pela ANPD para ajudar as empresas a comprovar esforços de conformidade.
- Definir indicadores claros (ex.: porcentagem de treinados e número de iniciativas de conscientização).

**Principais pontos abordados por Fabrício Guimarães Madruga Lopes  
(Coordenador-Geral de Fiscalização da ANPD)**

1. Visão da Fiscalização:

- Foco em educar e orientar, priorizando mudança de comportamentos em vez de punições.
- Incentivo à resolução ágil de problemas pelas empresas para evitar sanções.



2. Desafios da Política Nacional:

- Necessidade de abranger tanto o setor público quanto o privado, reconhecendo diferenças estruturais.
- Enfatizar valores como proteção de crianças no ambiente digital e segurança de transações.

3. Critérios para Conformidade:

- Importância de criar estímulos positivos, como reconhecimento público para empresas em conformidade.
- Considerar esforços de monitoramento e treinamento nas análises de conformidade.

4. Prioridades Identificadas pela ANPD:

- Direitos dos titulares, dados de crianças e adolescentes, e regulação de inteligência artificial.
- Preocupações com o uso indevido e compartilhamento de dados pessoais sensíveis.

5. Recomendações para a Política:

- Trazer exemplos concretos de boas práticas e indicadores.
- Usar a política para direcionar a ANPD a criar guias práticos e ouvir a sociedade antes de publicar regulamentos.
- Incentivar uma melhor articulação entre a ANPD e outros órgãos reguladores para aumentar a eficácia da fiscalização.



28/11/2024	<p>Discutiu-se sobre o formato e conteúdo do relatório a ser entregue à ANPD pelo GT, retomando o material que o grupo possui até o momento, constituído das contribuições do próprio grupo e das reuniões com os especialistas e passando, também, sobre possíveis pontos que ainda podem ser cobertos por especialistas nas próximas reuniões.</p>
05/12/2024	<p><b>Especialistas convidados: Matthew Reisman e Mark Smith (CIPL).</b></p> <p><b>Principais pontos abordados pelos convidados:</b></p> <ol style="list-style-type: none"> <li>1. Introdução ao tema de governança de dados pessoais e privacidade: <ul style="list-style-type: none"> <li>• Explicaram a importância de práticas globais e melhores práticas para a conformidade com leis de privacidade.</li> <li>• Diferenciaram conformidade (compliance) de responsabilização (accountability), enfatizando que accountability vai além de cumprir regras, englobando uma abordagem ética e proativa na gestão de dados pessoais, e que a conformidade é apenas um elemento da responsabilização.</li> <li>• O accountability não é processo único, é um processo contínuo de mudança interna, à medida que os negócios, o mundo e a tecnologia evoluem.</li> </ul> </li> </ol>



- Muitas empresas utilizam padrões ISO ou outros modelos para gestão de programas de privacidade, e os especialistas destacaram a importância de que as empresas possuam uma estrutura bem definida.

#### 2. Modelo de Responsabilização Organizacional:

- Introduziram framework com sete pilares para accountability: liderança e supervisão, avaliação de riscos, políticas e procedimentos, transparência, treinamento e conscientização, monitoramento e verificação, e resposta e aplicação.

#### 3. Alinhamento da LGPD com práticas internacionais:

- Destacaram como a Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil já incorpora conceitos de responsabilização e como essas práticas podem ser operacionalizadas para maior eficiência.

- Discutiram a relevância de uma possível adesão do Brasil ao CBPR (Cross-Border PrivacyRules), para apoiar transferências internacionais de dados e demonstrar accountability.

#### 4. Experiência global e lições aprendidas:

- Compartilharam estudos de caso de organizações globais, destacando práticas como o envolvimento de equipes multifuncionais e a importância de integrar avaliação de riscos de privacidade com avaliações de risco mais amplas.

#### 5. Certificação de terceiros:

- Discutiram a utilidade de certificações de terceiros para que as empresas possam demonstrar conformidade e, ao mesmo tempo, seja incentivada a implementação de processos e práticas mais eficientes. Ao mesmo tempo,



	<p>organização certificadora poderia ter alguns “poderes limitados”, a fim de não sobrecarregar a ANPD.</p>
12/12/2024	<p><b>Especialistas convidados: Fabrício Mota e Marison Souza</b></p> <p><b>Principais pontos abordados por Fabrício da Mota Alves:</b></p> <p>1. Política Nacional de Proteção de Dados Pessoais:</p> <ul style="list-style-type: none"> <li>• Importância: A política deve ser abrangente e não se limitar à atuação da ANPD. Deve orientar todo o Estado brasileiro em conformidade com os direitos constitucionais.</li> <li>• Crítica ao Estado Atual: Falta uma política nacional de proteção de dados eficaz, o que prejudica o amadurecimento do tema no país.</li> <li>• Recomendação: A política deve: <ul style="list-style-type: none"> <li>◦ Estimular campanhas públicas de educação e conscientização sobre proteção de dados.</li> <li>◦ Garantir maior coordenação regulatória, por meio da articulação entre reguladores.</li> <li>◦ Encorajar boas práticas e auto-organização da sociedade para reduzir a dependência de regulamentação estatal.</li> </ul> </li> </ul> <p>2. Críticas à ANPD:</p> <ul style="list-style-type: none"> <li>• Limitações estruturais: A ANPD enfrenta restrições financeiras e operacionais, dificultando sua atuação.</li> </ul>



- Atuação fiscalizatória prematura: Processos sancionatórios iniciados antes de regulamentações claras enfraquecem a atuação da ANPD e geram insegurança jurídica.

- Exemplo citado: Caso em que a ANPD negou Termos de Ajustamento de Conduta (TACs) por ausência de regulamentação própria, inviabilizando um dos instrumentos garantidos pela LGPD aos agentes de tratamento para a solução de litígios e conformidade com a LGPD.

#### 3. Necessidade de coordenação regulatória:

- Problemas identificados: Falta de diálogo e alinhamento entre diferentes órgãos reguladores, como Banco Central e ANPD, o que gera conflitos e esforços duplicados.
- Impacto: Insegurança jurídica e aumento de judicializações.

#### 4. Auto-organização e práticas de conformidade:

- Proposta: Estimular boas práticas voluntárias por parte das empresas, com selos, certificações e auditorias que fortaleçam a confiança do mercado.
- Benefícios:
  - Reduzir a pressão sobre a ANPD.
  - Criar ambientes mais maduros e especializados, com menor dependência de regulação detalhada.

#### 5. Necessidade de clareza regulatória:

- Necessidade de priorizar regulamentação antes de avançar com fiscalizações e sanções.



### **Principais pontos abordados por Marison Souza (Privacy Tools):**

#### **1. Experiência prática com empresas:**

- Perfil dos clientes atendidos pela Privacy Tools:
  - Pequenas empresas: Demandam soluções completas (DPO terceirizado), com baixa maturidade no tema.
  - Médias empresas: Orçamento limitado, com DPO acumulando múltiplas funções.
  - Grandes empresas: Envolve equipes robustas, mas enfrentam alta rotatividade de profissionais e desafios com regulamentações internacionais.
  - Órgãos públicos: Muitos iniciam programas de privacidade sem estrutura interna adequada.

#### **2. Problemas recorrentes nas empresas:**

- Direitos dos titulares:
  - Falta de clareza técnica para atender pedidos, como portabilidade e cópia de dados pessoais.
  - Necessidade de padrões seguros para autenticação, criptografia e rastreabilidade.
- Transferência internacional de dados pessoais:
  - Incerteza sobre permissões, especialmente relacionadas aos Estados Unidos.
  - Preferência por manter dados pessoais no Brasil devido à insegurança jurídica.



	<ul style="list-style-type: none"> <li>• Cálculo de alto risco:           <ul style="list-style-type: none"> <li>◦ Empresas têm dificuldade para identificar e medir o grau de risco em tratamentos de dados pessoais.</li> </ul> </li> </ul> <p>3. Propostas de soluções práticas:</p> <ul style="list-style-type: none"> <li>• Direitos dos titulares:           <ul style="list-style-type: none"> <li>◦ Criação de critérios técnicos claros para entrega de dados pessoais e autenticação segura.</li> <li>◦ Desenvolvimento de protocolos padronizados para interoperabilidade e portabilidade.</li> </ul> </li> <li>• Transferência internacional de dados pessoais:           <ul style="list-style-type: none"> <li>◦ Lista objetiva de países autorizados para armazenamento de dados pessoais.</li> <li>◦ Guias e FAQs simplificados para orientar empresas.</li> </ul> </li> <li>• Cálculo de risco:           <ul style="list-style-type: none"> <li>◦ Ferramentas práticas, como calculadoras ou guias exemplificadas para auxiliar empresas a determinar riscos.</li> </ul> </li> </ul>
19/12/2024	Vitor destacou que irá elaborar e enviar aos demais membros as atas e um documento com os principais pontos discutidos até o momento. Enfatizou que, na sua visão, é necessário selecionar poucos pontos principais para a temática de conformidade, com foco na política nacional de proteção de dados pessoais. Foi proposto que cada membro contribua com três pontos principais, baseados em sua experiência e nas discussões realizadas, para alinhar as ideias do grupo. Após



	alinhar os pontos, o trabalho será dividido entre os membros, com foco na redação final do documento em janeiro de 2025.
16/01/2025	O Grupo discutiu sobre o formato e conteúdo deste Relatório final, definindo que nas próximas semanas os participantes fariam suas contribuições para elaboração da versão final.
30/01/2025	O Grupo discutiu sobre o formato e conteúdo deste Relatório final, especialmente em reação aos “Produtos Elaborados” e “Parecer conclusivo com recomendações finais para a Política Nacional”.



## **2 – Produtos Elaborados**

Inicialmente, destacamos a importância da Política Nacional de Proteção de Dados Pessoais e da Privacidade como instrumento para fortalecimento do ambiente de proteção de dados e da privacidade no país.

Especificamente no que tange a mecanismos, instâncias e práticas de conformidade, objeto de estudos por parte deste Grupo de Trabalho, entendemos que as disposições da Política Nacional de Proteção de Dados Pessoais e da Privacidade devem ser mais principiológicas, abrangentes e alinhadas à LGPD, fornecendo ferramentas e incentivando a atuação da ANPD, bem como de toda a sociedade, na promoção da proteção de dados pessoais, também garantindo a necessária segurança jurídica aos agentes de tratamento.

A promoção da conformidade com a LGPD é uma forma de concretizar os princípios previstos no art. 6, da LGPD, inclusive os indicados abaixo:

- Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Nesse sentido, sugerimos abaixo direcionamentos gerais a serem levados em consideração na elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade.



Aproveitamos para mencionar que o GT 4 do CNPD debruçou-se sobre Governança de Dados no Setor Público, indicando em seu relatório algumas iniciativas voltadas aos mecanismos, instâncias e práticas de conformidade adotadas por entes públicos.

## **1. Fomentar a adoção e a orientação acerca de mecanismos, instâncias e práticas de conformidade**

- **1.1 - Privilegiar os mecanismos de conformidade já previstos na LGPD:** A LGPD já prevê mecanismos e critérios de conformidade e recomendamos que a Política Nacional incentive a orientação e a regulamentação pela ANPD, quando necessário, tanto de forma geral sobre a LGPD, como a respeito de tais mecanismos. Citamos, exemplificativamente, os seguintes mecanismos já previstos na LGPD: a manutenção de registro das operações de tratamento (art. 37, da LGPD); a elaboração de relatório de impacto à proteção de dados pessoais (art. 38, da LGPD); a indicação de encarregado pelo tratamento de dados pessoais (art. 41, da LGPD); e a adoção de medidas de segurança para proteção de dados (art. 46, da LGPD). Além disso, a ANPD deve privilegiar a regulamentação ou orientação de temas subjacentes essenciais aos mecanismos de conformidade, tais como a avaliação de alto risco e larga escala nas atividades de tratamento de dados pessoais, trazendo mais clareza, efetividade e segurança jurídica à sociedade.
  
- **1.2 - Fomentar a adoção de mecanismos, instâncias e práticas de conformidade:** A Política Nacional deve incentivar a adoção de



mecanismos, instâncias e práticas de conformidade pelos agentes de tratamento, reconhecendo a sua adoção de forma benéfica aos agentes de tratamento e aos titulares. Nesse sentido, a Política Nacional deve, também, orientar a ANPD a considerar todas as práticas positivas, as quais devem levar em conta mais o conteúdo e propósito, do que a forma específica. A ANPD deve ter uma visão aberta e abrangente, reconhecendo as diferentes e mais diversas práticas de conformidade.

- **1.3 - Orientação e regulamentação equilibradas:** A Política Nacional deve reconhecer que a regulamentação pela ANPD deve ser orientada pela estrita necessidade de regulamentação e/ou de orientação, sem a criação de ônus excessivos ou de obstáculos indevidos ao tratamento de dados pessoais, dada a sua crucial importância em praticamente todas as atividades da sociedade, de forma a garantir a proteção de dados pessoais e da privacidade e promovendo o necessário equilíbrio com o desenvolvimento social, econômico, tecnológico e a inovação.
  
- **1.4 - Privilegiar a sinergia com outras normas e mecanismos de conformidade já existentes:** A ANPD deve ser incentivada a realizar a atividade de regulamentação e de orientação de forma eficiente, reconhecendo mecanismos de conformidade já previstos em outras normas, especialmente no caso de setores regulados. Dessa forma, evita-se a sobreposição e potenciais contradições regulatórias, sem criar ônus de observância desarrazoados ou impraticáveis para os agentes de tratamento. Da mesma forma, práticas já consolidadas nos mercados



também devem ser positivamente consideradas pela ANPD, quando adotadas pelos agentes de tratamento.

- **1.5 - Proteção do segredo empresarial:** A Política Nacional deve reafirmar a proteção do segredo empresarial dos agentes de tratamento, não apenas no tocante às práticas e mecanismos de conformidade, mas de forma geral. A proteção do segredo empresarial é também amplamente prevista na LGPD, de modo que a Política Nacional também deve reforçar a necessidade e importância de sua proteção.
- 2. Incentivar o diálogo da ANPD com a sociedade em todas as suas esferas de atuação**

- **2.1 - Prioridade na Atuação responsiva:** A Política Nacional deve reafirmar a necessidade de atuação responsiva por parte da ANPD, promovendo sempre o diálogo entre a Autoridade e os titulares e agentes de tratamento, em todas as suas esferas de atuação, especialmente, no que tange à atividade fiscalizatória. A proximidade da ANPD com a sociedade é crucial para compreender a realidade das situações de tratamento de dados pessoais e dos agentes de tratamento, devendo essas serem levadas em conta pela Autoridade nas atividades de fiscalização, de modo a promover a conformidade dos agentes e a proteção de dados pessoais de forma equilibrada, factível e eficiente. A priorização do diálogo e da adoção de medidas de conformidade que



atendam aos propósitos de proteção de dados pessoais, sem ônus desnecessário, devem ser privilegiadas.

- **2.2 –Autocomposição de Conflitos:** A Política Nacional deve reafirmar e incentivar a adoção de mecanismos amigáveis de resolução de disputas e litígios, seja por meio da mediação como meio de solução de controvérsias entre particulares e a autocomposição de conflitos no âmbito da administração pública. São vários os instrumentos jurídicos que podem ser utilizados, como é o caso do Termo de Ajustamento de Conduta previsto desde 1985 na Lei da Ação Civil Pública (artigo 5º da Lei 7.347/85) e no artigo 55-J, inciso XVII, da LGPD e nos artigos 43 e seguintes da Resolução CD/ANPD nº 1, de 28 de outubro de 2021 que aprovou o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados Pessoais.

Além disso, mecanismos de autocomposição de conflitos são incentivados e regulamentados pela Lei 13.140/2015, que dispõe sobre a mediação entre particulares como meio de solução de controvérsias e sobre a autocomposição de conflitos no âmbito da administração pública. Importante, ainda, o disposto na Lei 13.874/19, que institui a Declaração de Direitos da Liberdade Econômica e tem como princípio a intervenção subsidiária e excepcional do Estado sobre o exercício de atividades econômicas, dentre outras regras.

- **2.3 - Orientação e regulamentação com ampla participação social:** A ampla participação social deve ser garantida e incentivada na Política



Nacional, promovendo instrumentos tanto para a ANPD, quanto para a sociedade em geral para efetivar essa participação de forma ampla e abrangente. A participação contínua da sociedade na gestão pública é um direito assegurado pela Constituição Federal que possibilita a todos os cidadãos a fiscalização quanto a aplicação dos recursos públicos, como também a participação ativa nos processos de formulação de políticas públicas.

A participação social pode se dar de diversas maneiras, já garantidas pela ANPD, que já garante aos cidadãos múltiplas formas de engajamento. Os canais da Ouvidoria permitem o envio de reclamações, dúvidas e sugestões. Há, ainda, a possibilidade de participação por meio dos editais públicos que possibilitam participação direta. Cidadãos podem acompanhar órgãos consultivos vinculados à Autoridade e contribuir ativamente na regulamentação através de consultas, audiências públicas e outros mecanismos de participação social. Existem ainda outros mecanismos como os importantes guias orientativos, que são elemento central para as práticas de conformidade com a LGPD.

Essa ampla participação social promove o diálogo entre a Autoridade e os diversos setores da sociedade, garantindo que a Autoridade escute e considere as diferentes visões em seu processo de regulamentação e orientação.

### **3. Incentivar a adoção de boas práticas e de governança de dados pessoais, selos e certificações**



- **3.1 - Boas Práticas e Governança de Dados Pessoais:** A LGPD incentiva a adoção de boas práticas e governança de dados pessoais. É importante que a Política Nacional reconheça as diversas boas práticas e que essas podem ser implementadas de forma ampla, e não apenas como previsto no art. 50, da LGPD, de modo a incentivar a sua adoção de forma mais facilitada e abrangente pela sociedade. A Política Nacional pode reforçar a possibilidade de adoção de tais práticas, de forma não obrigatória, em linha com o previsto na LGPD.
  
- **3.2 - Incentivar a criação e reconhecimento de selos, certificações e autorregulações setoriais:** Os selos, certificações e autorregulações setoriais são uma das principais ferramentas de conformidade com a legislação de proteção de dados. A Política Nacional deve incentivar a ANPD a priorizar a viabilização e reconhecimento de tais instrumentos, para que possam ser mais amplamente adotados pela sociedade e promover um ambiente de proteção de dados pessoais mais robusto.

#### **4. Incentivar a promoção de ações educacionais**

- **Ações educacionais:** A Política Nacional deve incentivar a implementação de ações educacionais, não apenas, mas especialmente pela ANPD. O fortalecimento do ambiente de proteção de dados pessoais e da privacidade, inclusive no que tange a práticas e mecanismos de conformidade, tem como um dos pilares a educação, tanto dos titulares



quanto dos agentes de tratamento, de modo que deve ser amplamente incentivada pela Política Nacional.

## 5. Implementação de Programas de Compliance em Proteção de Dados Pessoais

- **5.1 - Fomentar a adoção de Diretrizes de Compliance:** Propor que a Política Nacional facilite o reconhecimento da implementação de programas de compliance em proteção de dados pessoais nas organizações públicas e privadas. Essas diretrizes devem alinhar-se com a LGPD e podem reconhecer como boa prática de conformidade a adoção de padrões internacionais, como o GDPR europeu, sempre considerando que padrões internacionais devem ser adequados à realidade fática e normativa brasileira, bem como que padrões nacionais e outros usados pelos agentes de tratamento devem ser também dessa reconhecidos.
- **5.2 - Fomento à Cultura Organizacional de Privacidade:** Recomendar que a política incentive a incorporação da proteção de dados pessoais na cultura organizacional, inclusive por meio da adoção de ações educacionais, promovendo a conscientização de todos os níveis hierárquicos e não apenas dos setores específicos das organizações.
- **5.3 - Orientação para Pequenas e Médias Empresas (PMEs):** Destacar a necessidade de diretrizes específicas para PMEs, facilitando a implementação de programas de compliance adequados ao seu porte e capacidade, evitando sobrecarga regulatória.



- **5.4 - Parcerias Público-Privadas para Desenvolvimento de Recursos:**  
Sugerir a formação de parcerias entre governo, empresas e academia para o desenvolvimento de ferramentas, treinamentos e recursos que auxiliem na implementação eficaz de programas de compliance em proteção de dados pessoais.

## 6. Mecanismos de Monitoramento e Auditoria Interna

- **6.1 - Auditorias Periódicas:** Propor que a política nacional incentive e reconheça como boa prática não obrigatória a realização pelas organizações de auditorias internas e, se os agentes de tratamento entenderem necessário, externas periódicas para avaliar a conformidade com a LGPD e outras normas relacionadas. Como mencionado, a realização de auditorias não é obrigatória e deve continuar dessa forma, mas é um importante instrumento que pode ser incentivado e reconhecido como boa prática pela Política Nacional.
- **6.2 - Reconhecimento de Padrões de Auditoria:** Em linha com o item 6.1 anterior, os padrões e metodologias nacionais e internacionais, assim como padrões e metodologias próprios adotados pelos agentes de tratamento para auditorias não obrigatórias em proteção de dados pessoais, podem ser reconhecidos como boas práticas, garantindo consistência e confiabilidade nos processos de avaliação.
- **6.3 - Implementação de Sistemas de Monitoramento Contínuo:** Recomendar que a política incentive o uso de tecnologias e sistemas que permitam o monitoramento contínuo do tratamento de dados pessoais, facilitando a detecção precoce de irregularidades ou vulnerabilidades.



Essas ações não obrigatórias também podem ser incentivadas como boas práticas pela Política Nacional.

- **6.4 - Relatórios de Conformidade:** Propor que organizações sejam incentivadas a elaborar relatórios de conformidade, evidenciando as medidas adotadas para proteger dados pessoais e os resultados das auditorias realizadas. Essas medidas não obrigatórias também podem ser reconhecidas como boas práticas.
- **6.5 - Capacitação de Auditores Internos:** Sugerir programas de capacitação e certificação para profissionais responsáveis por auditorias internas, assegurando que possuam conhecimentos atualizados em proteção de dados e segurança da informação.

## 7. Gestão de Incidentes e Planos de Resposta a Vazamentos de Dados Pessoais

- **7.1 - Elaboração de Planos de Resposta a Incidentes:** A Lei Geral de Proteção de Dados Pessoais determina aos agentes de tratamento de dados pessoais a adoção de medidas para prevenir a ocorrência de danos aos titulares em virtude de suas atividades e na eventualidade de um incidente de segurança, é necessário a mitigação de danos aos titulares por meio de uma série de ações, que passam pela comunicação da ocorrência até a elaboração de planos de mitigação de dano em razão da exposição dos dados em razão do incidente.

Como o cumprimento dessa obrigação é elemento fundamental para proteção de dados dos titulares, a Comunicação de Incidente de Segurança (CIS) deve ter sua base principiológica como elemento da



Política Nacional de Proteção de Dados Pessoais. Por isso tal Política Nacional deve prever o desenvolvimento e manutenção de planos formais de resposta a incidentes de segurança atualizados envolvendo dados pessoais.

- **7.2. Diretrizes para Notificação de Incidentes:** Sugerir a definição pela ANPD de prazos claros e procedimentos padronizados para notificação de incidentes à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados, alinhando-se com as melhores práticas internacionais.
- **7.3. Estabelecimento de Equipes de Resposta a Incidentes:** Reconhecer como boa prática a designação pelas organizações de equipes ou indivíduos responsáveis pela gestão de incidentes de segurança, garantindo uma resposta rápida e coordenada.
- **7.4. Realização de Testes e Simulações:** Reconhecer como boa prática a realização de testes e simulações de incidentes (ex.: exercícios de mesa, testes de invasão), permitindo que organizações avaliem e melhorem seus planos de resposta. A realização de testes e simulações não é medida obrigatória que também pode ser reconhecida como boa prática.
- **7.5. Comunicação Transparente com Titulares de Dados:** Sugerir que sejam estabelecidas orientações sobre como comunicar incidentes aos titulares de dados afetados de forma clara, transparente e útil, incluindo informações sobre as medidas tomadas e recomendações para mitigar possíveis danos.

## 8. Transferência Internacional de Dados Pessoais



- **Viabilizar mecanismos de transferência internacional de dados pessoais:** A Política Nacional deve direcionar a ANPD a priorizar a viabilização dos mecanismos de transferência internacional de dados pessoais previstos na LGPD. A transferência internacional de dados pessoais é crucial para o fluxo internacional de dados, que ocorre em muitas atividades de tratamento e, até o momento, apenas as cláusulas padrão foram regulamentadas pela ANPD. Existem outros instrumentos de transferência previstos na LGPD que também devem ser priorizados pela ANPD, além da devida orientação aos agentes de tratamento sobre a implementação de tais mecanismos.



### **3 – Parecer conclusivo com recomendações para a Política Nacional**

#### **3.1 - A Importância de Mecanismos, Instâncias e Práticas de Conformidade para a Política Nacional de Proteção de Dados Pessoais e da Privacidade**

A implementação efetiva da Lei Geral de Proteção de Dados Pessoais (LGPD) representa um dos maiores desafios enfrentados por organizações públicas e privadas no Brasil. A conformidade com a legislação de proteção de dados pessoais vai além do mero cumprimento formal de requisitos legais, demandando uma abordagem holística que envolve mudanças culturais, implementação de processos robustos e adoção de práticas que efetivamente protejam os dados pessoais e os direitos fundamentais dos titulares.

Neste contexto, o reconhecimento de mecanismos, instâncias e práticas de conformidade torna-se elemento central para o sucesso da Política Nacional de Proteção de Dados Pessoais e da Privacidade. Tais elementos são essenciais não apenas para garantir o cumprimento legal, mas principalmente para criar um ambiente de confiança e responsabilidade no tratamento de dados pessoais, estimulando a adoção de boas práticas de conformidade e promovendo o desenvolvimento econômico e tecnológico e a inovação de forma ética e sustentável.



A experiência internacional e as práticas já adotadas por organizações brasileiras demonstram que **a conformidade efetiva requer uma combinação de diferentes elementos:**

1. Mecanismos de governança e prestação de contas;
2. Instâncias adequadas para supervisão e implementação de programas de privacidade;
3. Materiais informativos e Guias de Boas Práticas;
4. Práticas que traduzam os princípios legais em ações concretas e mensuráveis;
5. Ferramentas e processos que permitam demonstrar a conformidade.

A definição desses elementos na Política Nacional é fundamental por diversas razões:

1. Promover segurança jurídica ao estabelecer parâmetros claros para avaliação da conformidade;
2. Facilitar a adoção de boas práticas por organizações de diferentes portes e setores;
3. Incentivar a autorregulação e o desenvolvimento de padrões setoriais;
4. Permitir uma fiscalização mais eficiente e focada em resultados concretos;
5. Contribuir para a construção de uma cultura de proteção de dados pessoais no país.



Portanto, ao propor, na seção 2 deste Relatório, os subsídios para as diretrizes na elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, o Grupo de Trabalho pautou-se pelos elementos acima, apresentando 8 (oito) temáticas a serem levadas em consideração na elaboração da PNDP, no que tange ao reconhecimento de mecanismos, instâncias e práticas de conformidade adequadas, especialmente no que tange ao seu reconhecimento positivo como boas práticas, as quais estão abaixo sintetizadas:

- 1.** Incentivo à adoção e à orientação de mecanismos, instâncias e práticas de conformidade, especialmente por meio de mecanismos já previstos na LGPD e sinergia com outras normas já existentes. Além disso, a PNDP pode fomentar o equilíbrio entre as atividades de orientação e regulamentação pela ANPD, a fim de evitar a criação de ônus excessivos ou de obstáculos indevidos ao tratamento de dados pessoais.
- 2.** Estímulo ao diálogo da ANPD com a sociedade em todas as suas esferas de atuação, promovendo a participação social por meio de consultas, audiências públicas e outros mecanismos. Estímulo, também, à atuação responsável da ANPD, especialmente, no que tange à atividade fiscalizatória, promovendo sempre o diálogo entre a Autoridade e os titulares e agentes de tratamento.
- 3.** Fomento à adoção de boas práticas de governança de dados pessoais de forma ampla, e não apenas como previsto no art. 50, da LGPD, bem como incentivo à criação selos e certificações de conformidade.



4. Incentivo à promoção de ações educacionais, pela ANPD e outros órgãos, voltadas não só aos titulares, como também aos agentes de tratamento.
5. Estímulo e incentivo a adoção de mecanismos amigáveis de resolução de disputas e litígios, seja por meio da mediação como meio de solução de controvérsias entre particulares e a autocomposição de conflitos no âmbito da administração pública.
6. Estímulo à promoção de diretrizes claras para incentivar a implementação de programas de compliance em organizações públicas e privadas, por meio do fomento à Cultura Organizacional de Privacidade, bem como de orientações específicas para Pequenas e Médias Empresas e estímulo à formação de Parcerias Público-Privadas para desenvolvimento de recursos que auxiliem na implementação eficaz de programas de compliance em proteção de dados pessoais.
7. Incentivo ao reconhecimento de Padrões de Auditoria, Implementação de Sistemas de Monitoramento Contínuo e programas de capacitação e certificação para profissionais responsáveis por auditorias internas, além do incentivo à realização de auditorias internas pelas próprias organizações. Essas práticas não obrigatórias podem ser reconhecidas como boas práticas pela PNPD.
8. Incentivo ao desenvolvimento e manutenção, pela ANPD, de planos formais de resposta à incidentes de segurança, bem como a definição de prazos claros e procedimentos padronizados para notificação de incidentes à Autoridade e aos titulares afetados, além do reconhecimento



de boas práticas não obrigatórias das organizações, como a designação pelas de equipes ou indivíduos responsáveis pela gestão de incidentes de segurança e a realização de testes e simulações.

9. Direcionamento à priorização, pela ANPD, da viabilização dos mecanismos de transferência internacional de dados pessoais, conforme previsto na LGPD.

Dessa forma, nota-se que as diretrizes propostas pelo Grupo de Trabalho, que podem ser adotadas na Política Nacional de Proteção de Dados Pessoais e da Privacidade, estão voltadas, precipuamente, à uma atuação responsável da ANPD, à ampla participação e engajamento social, à orientação sobre práticas de conformidade já previstas na LGPD e ao incentivo ao reconhecimento como boas práticas de outros mecanismos e práticas de conformidade, de forma equilibrada e positiva para os titulares e os agentes de tratamento.

A Política Nacional de Proteção de Dados Pessoais e da Privacidade desempenhará um papel essencial na construção de um ambiente regulatório sólido, equilibrado e eficaz para o tratamento de dados pessoais no Brasil. Ao estabelecer diretrizes e incentivar a adoção de boas práticas, a PNPD fortalecerá a segurança jurídica e impulsionará a conformidade com a LGPD, garantindo, também, um cenário de maior maturidade sobre o tema em organizações públicas e privadas e, por consequência, maior confiança da sociedade no uso responsável de informações pessoais. O incentivo à implementação de mecanismos de compliance, a valorização do diálogo entre a ANPD e a sociedade, o incentivo à capacitação e a criação de incentivos regulatórios são pilares fundamentais para consolidar uma cultura nacional de proteção de dados pessoais que beneficie tanto os titulares quanto os agentes de tratamento.



Além disso, a fim de concretizar seus objetivos, é essencial que, após sua elaboração, a PNPD seja continuamente aprimorada para acompanhar os avanços tecnológicos e as demandas sociais, assegurando, assim, que o Brasil se mantenha alinhado às melhores práticas globais. Dessa forma, a Política Nacional não apenas fortalecerá a proteção dos dados pessoais, mas também impulsionará a competitividade global do país ao promover a privacidade como um valor central para o desenvolvimento econômico, tecnológico e inovação.

Brasília, 19 de fevereiro de 2025

Vitor Moraes de Andrade

Conselheiro Titular do CNPD e Coordenador do GT 2

Annette Martinelli de Mattos Pereira

Conselheira Suplente do CNPD e Vice Coordenadora do GT2

Tiago Lopes de Aguiar

Conselheiro Titular do CNPD e membro do GT2

Claudio Eduardo L. de Abreu Rocha

Conselheiro Suplente do CNPD e membro do GT2

Ana Paula Moraes Canto de Lima

Conselheira Suplente do CNPD e membro do GT2