idp CEDIS Centro de Direito, Internet e Sociedade

CIPL Centre for Information Policy Leadership HUNTON ANDREWS KURTH

12 PRIORIDADES PARA ADEQUAÇÃO À LGPD

CHECKLIST

O *Centre for Information Policy Leadership* (CIPL) e o Centro de Direito, Internet e Sociedade of the Instituto Brasiliense de Direito Público (CEDIS-IDP) concluíram um novo relatório para ajudar organizações públicas e privadas navegarem as diversas prioridades para adequação às regras da Lei Geral de Proteção de Dados Pessoais (LGPD).

Acesse aqui o conteúdo completo do relatório do CIPL e do CEDIS-IDP entitulado "Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD)".

PRIORIDADE 1

Entender o impacto da LGPD na organização e obter a adesão da alta administração

- ☐ Compreender o impacto das regras da LGPD na organização e o uso de dados pessoais como controlador e/ou operador.
- ☐ Explicar e demonstrar à alta administração a importância da adequação às regras de privacidade e os benefícios da prestação de contas.
- ☐ Solicitar apoio da alta administração, incluindo para orçamento e recursos.

PRIORIDADE 2

Designar o encarregado pelo tratamento de dados pessoais, e identificar e envolver os principais stakeholders

- [ ] Designar o encarregado, documentar e comunicar internamente seu papel e suas responsabilidades.

- [ ] Identificar e envolver os principais stakeholders internos e líderes sêniores que patrocinarão o programa de governança de privacidade e proteção de dados pessoais e terão responsabilidade pela implementação do programa.

- [ ] Identificar e envolver os principais stakeholders externos.

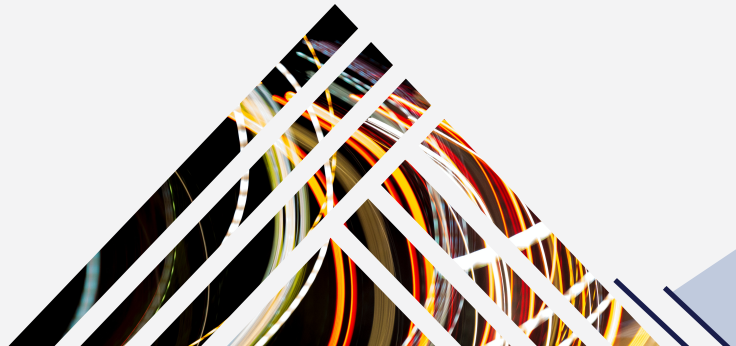
PRIORIDADE 3

Identificar as atividades de tratamento e os dados utilizados pela organização

- [ ] Definir a metodologia para mapear e registrar as atividades de tratamento de dados pessoais efetuadas pela organização (como controladora e/ou operadora) e revisar periodicamente o ciclo de vida dos dados.

- [ ] Mapear os dados pessoais e as respectivas atividades de tratamento o mais rápido possível.

- [ ] Considerar a anonimização e minimização de dados para reduzir os riscos e o ônus decorrente da obrigação de conformidade da organização.



PRIORIDADE 4

Determinar o papel e as obrigações da organização ao atuar como controladora ou operadora

- [ ] Determinar o papel e as obrigações da organização como controladora ou operadora.

- [ ] Comunicar essas obrigações aos indivíduos e às equipes relevantes dentro da organização.

- [ ] Considerar atualizações necessárias aos contratos dos clientes para refletir o papel da organização.

PRIORIDADE 5

Avaliar os riscos associados ao tratamento de dados pessoais

- [ ] Implementar processo de avaliação de riscos aos indivíduos relacionados ao tratamento de dados pessoais.

- [ ] Priorizar as medidas de conformidade relacionadas ao tratamento de dados pessoais que implicam maiores riscos para os indivíduos e para a organização.

PRIORIDADE 6

Elaborar e implementar um programa de governança de privacidade e proteção de dados pessoais que cubra as exigências da LGPD

- [ ] Elaborar um programa de governança de privacidade e proteção de dados pessoais e um plano de ação para implementá-lo com base nos riscos identificados.

- [ ] Identificar quais são as ações mais simples e implementá-las o mais rápido possível.

- [ ] Manter e revisar o programa de governança de privacidade e proteção de dados pessoais de forma contínua.

PRIORIDADE 7

Definir as bases legais para as atividades de tratamento de dados da organização

- [ ] Identificar os indivíduos ou equipes que serão responsáveis por determinar as bases legais para o tratamento de dados pessoais—esses indivíduos deverão, como prioridade, definir em quais bases legais a organização se baseará.

- [ ] Considerar quais processos devem ser implementados e/ou adaptados para a manutenção contínua das bases legais.

PRIORIDADE 8

Definir medidas técnicas e administrativas para garantir a segurança dos dados pessoais, assim como para elaborar relatórios internos e gerenciamento efetivos de incidentes de segurança

- ☐ Trabalhar com as equipes de segurança da informação e de arquitetura de sistemas/dados para determinar as mudanças necessárias para implementar as medidas apropriadas de segurança.

- ☐ Estabelecer um processo para a elaboração de relatórios internos, gerenciamento de incidentes de segurança, violações de dados pessoais e notificação da ANPD, se necessário.

PRIORIDADE 9

Identificar os terceiros com os quais a organização compartilha dados pessoais e estabelecer um processo de gestão de terceiros

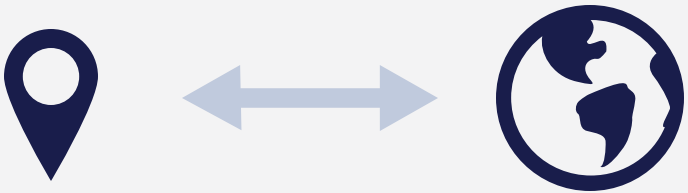
- [ ] Identificar os terceiros que realizam tratamento de dados pessoais em nome da organização e determinar se a organização trata dados pessoais em nome de terceiros.

- [ ] Avaliar e adotar mecanismos de gerenciamento de terceiros, incluindo processos de due diligence e a celebração de contratos relacionados ao tratamento de dados.

PRIORIDADE 10

Identificar os fluxos internacionais de dados da organização (entrada e saída) e estabelecer os mecanismos apropriados para permitir tal transferência de dados

- [ ] Identificar se a organização transfere dados pessoais para outros países e, se o faz, para quais finalidades e em qual capacidade (como controlador ou como operador).
- [ ] Avaliar e implementar os mecanismos de transferência de dados mais apropriados.



PRIORIDADE 11

Construir processos eficazes para transparência e gerenciamento dos direitos dos titulares de dados pessoais

- ☐ Preparar avisos de privacidade e outros recursos para fornecer informações facilmente acessíveis aos titulares de dados sobre o tratamento realizado pela organização.
- ☐ Mapear os possíveis casos de exercícios de direitos pelos titulares relacionados aos seus dados pessoais, avaliar o tempo que a organização precisaria para responder e para desenvolver os processos relevantes.
- ☐ Desenvolver processos para responder a tais solicitações.

PRIORIDADE 12

Treinar funcionários sobre as regras da LGPD e criar um programa de conscientização

- [ ] Implementar treinamento contínuo para todos os funcionários, incluindo os terceirizados e os recém-chegados.

- [ ] Planejar atividades de treinamento e comunicação tanto no início do programa de governança de privacidade e proteção de dados pessoais quanto de forma contínua.

Bojana Bellamy
Presidente, CIPL

Giovanna Carloni
Gerente Global de Políticas de Privacidade, CIPL

Laura Schertel
Advogada e professora, Diretora do CEDIS-IDP

Danilo Doneda
Advogado e professor, Diretor do CEDIS-IDP

O que é o CIPL

O CIPL é um *think tank* global de privacidade e segurança de dados, sediado em Washington, DC, Bruxelas e Londres. O CIPL trabalha com líderes do setor industrial, autoridades reguladoras e gestores de políticas públicas para desenvolver soluções globais e boas práticas para a era da informação.

O que é o CEDIS-IDP

O CEDIS-IDP é uma instituição brasileira focada na promoção de pesquisas e debates sobre a implementação de novas leis e regulamentos que impactam a sociedade da informação, tais como os relativos à privacidade e proteção de dados, concorrência e inovação, e governança da internet.

Clique aqui para mais informações sobre o projeto LGPD do CIPL e do CEDIS-IDP.

Clique aqui para o conteúdo completo do relatório do CIPL e do CEDIS-IDP sobre "Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a (LGPD)".