Série Proteção de Dados

12 COMO ME ADEQUAR?

VEIRANO ADVOGADOS



Este é o décimo segundo capítulo da Série Proteção de Dados. Clique aqui para acessar o cap. 11.



Em 2023, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou "LGPD") completa 5 anos de sua publicação – agora também com a possibilidade de aplicação das sanções administrativas pela ANPD, que se estende desde agosto de 2021. A Autoridade Nacional de Proteção de Dados ("ANPD") tem atuado ativamente para fomentar a discussão e disseminar os conceitos, práticas e princípios de privacidade e proteção de dados, com a publicação de diversos materiais para conscientização e regulamentação da LGPD desde a sua criação.

O Veirano Advogados tem acompanhado e participado das discussões relacionadas a estes temas. Por isso, nosso time de Proteção de Dados & Privacidade preparou a **Série Proteção de Dados**, na qual serão realizadas publicações periódicas sobre diferentes temas relacionados à privacidade, trazendo não somente os conceitos da LGPD, mas também publicações da ANPD sobre o tema, considerações relevantes, dentre outros conteúdos.

INTRODUÇÃO: O ATUAL CENÁRIO BRASILEIRO

Analisando o cenário brasileiro atual, apenas 36% das empresas afirmam estar totalmente adequadas, conforme mostram dados do estudo *IT Trends Snapshot 2023*, elaborado pela Logicalis. Por outro lado, grande parcela das empresas (43%) continua na fase de adoção, mas já apresenta iniciativas concretas de implementação.

Não obstante, o senso de urgência na corrida pela adequação se intensificou após a aplicação da 1ª multa pela Autoridade Nacional de Proteção de Dados (a "ANPD"), em decisão publicada em 06 de julho de 2023 (Processo nº 261.000489/2022-62). Contrariando a expectativa da maioria dos especialistas, a primeira multa foi aplicada contra uma microempresa que deixou de cumprir requisitos objetivos da lei, reforçando que a adequação à LGPD não deve ser uma preocupação apenas para as *Big Techs*.

Por este motivo, o Capítulo 12 do Privacy Series irá te auxiliar a entender como se adequar à LGPD, abordando os passos iniciais, as principais medidas para a adequação e os documentos que você pode precisar neste processo.





CHECKLIST DE PROTEÇÃO DE DADOS: POR ONDE COMEÇAR?

Antes de iniciar a jornada de adequação, você deverá analisar as medidas e práticas já adotadas pela sua empresa, assim você será capaz de verificar e mapear as mudanças que deverão ser feitas para garantir a adequação à legislação aplicável de proteção de dados, bem como identificar os próximos passos com relação à adequação da sua empresa.

Para te auxiliar, elaboramos abaixo um checklist para que você entenda o nível de maturidade da sua empresa:

- ☐ Você entende os conceitos básicos estabelecidos pela lei e está ciente que tem de se adequar?
- ☐ Os dados pessoais coletados durante a prestação dos serviços estão limitados ao necessário?
- ☐ O encarregado de dados (DPO) da sua empresa já foi nomeado?
- ☐ Sua empresa possui um prazo estabelecido para a retenção e exclusão dos dados?
- ☐ O “time de Privacy”, composto pela alta administração da empresa, já foi criado?
- ☐ Os titulares de dados possuem um meio de exercer seus direitos com relação ao tratamento dos dados?

- [ ] Sua empresa já adota medidas de segurança da informação como firewalls, antivírus, criptografia e dupla autenticação?
- [ ] Os principais riscos relacionados ao tratamento dos dados pessoais foram identificados e as medidas para sua mitigação já foram indicadas?
- [ ] Sua empresa já elaborou uma estratégia de privacidade? Já sabem quais são as prioridades no que se refere a proteção de dados?
- [ ] Os Termos de Uso e Políticas de Privacidade utilizados pela sua empresa já foram revisados e atualizados?
- [ ] Sua empresa já realizou um treinamento para contextualizar e dar conhecimento aos colaboradores sobre a lei e a adequação interna?
- [ ] Sua empresa já possui um procedimento de resposta às solicitações de titulares de dados e da ANPD?
- [ ] As atividades de tratamento realizadas pela sua empresa já foram mapeadas e o registro das atividades de tratamento já foi elaborado?
- [ ] O procedimento de resposta a incidentes de proteção de dados já foi criado?
- [ ] Os titulares de dados (colaboradores da empresa, clientes, fornecedores, prestadores de serviços, etc.) estão cientes do tratamento dos dados pela sua empresa? Eles sabem como e para que os seus dados são utilizados?
- [ ] Os contratos celebrados pela sua empresa com terceiros (colaboradores, prestadores de serviços, clientes, fornecedores, etc.) já contam com uma cláusula de proteção de dados aplicável? E os contratos anteriores à LGPD, já foram aditados?
- [ ] Você sabe suas responsabilidades com relação ao tratamento dos dados?
- [ ] Existe transferência internacional de dados no contexto da prestação dos serviços da sua empresa? As garantias aplicáveis já foram implementadas?

Com base nos tópicos que você indicou como cumpridos, será possível identificar pendências e pontos a serem enfrentados para garantir a adequação.

Ressaltamos que o checklist acima visa a nortear as ações adotadas para a adequação de sua empresa e possui algumas das principais questões que deverão ser observadas, mas ele não esgota todas as temáticas relacionadas ao tratamento de dados pessoais.

PRINCIPAIS MEDIDAS PARA A ADEQUAÇÃO

Tendo em vista os pontos abordados no item anterior, estabelecemos, abaixo, algumas das principais ações a serem adotadas para adequação:



1. Nomeie o encarregado de dados (DPO) ou, se você se enquadrar como um Agente de Tratamento de Pequeno Porte, basta indicar um canal de comunicação com os titulares de dados (leia o Capítulo 3 do Privacy Series para saber mais);
2. Estabeleça os responsáveis pelas questões de proteção de dados em cada uma das áreas;
3. Entenda o fluxo dos dados pessoais dentro da empresa;
4. Documente os fluxos de cada área (coleta, compartilhamento, finalidade, etc.);
5. Identifique as bases legais para cada atividade de tratamento;
6. Identifique o que deve ser alterado em relação ao tratamento de dados;
7. Identifique os mecanismos apropriados para a transferência internacional de dados;
8. Estabeleça como as alterações serão realizadas;
9. Implemente as medidas identificadas e elabore um relatório para os processos de tratamento de dados pessoais de alto risco;
10. Revise os documentos relevantes;
11. Crie procedimentos e ferramentas para detectar violações ou vazamentos de dados;
12. Crie procedimentos e ferramentas para responder aos titulares de dados e as autoridades nacionais e garantir o exercício dos direitos;
13. Elabore uma política e cultura de governança de dados pessoais;
14. Dê aos seus colaboradores subsídios e informações para que eles possam tratar os dados pessoais de forma mais consciente e adequada.

DOCUMENTOS QUE VOCÊ PODE PRECISAR

A LGPD não estabelece um rol de documentos que deverão ser criados por todos os agentes de tratamento para estar de acordo com a lei. No entanto, para garantir *compliance* com a legislação aplicável de proteção de dados, será necessário implementar novas medidas e atualizar as normas corporativas para garantir que todos os princípios e requisitos estão sendo devidamente observados durante o tratamento dos dados dos indivíduos envolvidos nas atividades da empresa, sejam eles funcionários, clientes, fornecedores, etc.

A depender das atividades adotadas pela sua empresa, poderá ser necessário criar até 30 (trinta) documentos diferentes, dentre eles estão:

Políticas de Privacidade direcionadas aos titulares de dados	Modelos de cláusulas-padrão de proteção de dados pessoais	Termos de obtenção do consentimento
Procedimentos para atender a solicitações de titulares de Dados e da ANPD	Protocolos internos em caso de incidentes de segurança com dados pessoais	Códigos de Conduta e Guias de Boas Práticas



MONITORAMENTO E IMPORTÂNCIA DO CONCEITO DE *PRIVACY BY DESIGN*

Assim como a empresa em si, os processos internos são mutáveis e estão sendo aprimorados e modificados regularmente. Por isso, é importante levar em consideração que mesmo depois da realização do projeto de Adequação à LGPD, será necessário monitorar o tratamento dos dados pessoais pela empresa e atualizar as normas internas e, até mesmo, o inventário de dados pessoais, para garantir que as atividades adotadas pela companhia estão levando em conta os requisitos e diretrizes da legislação aplicável.

Além disso, é importante ressaltar que a mera atualização de políticas e documentos dentro da companhia não garante o cumprimento da lei.

É indispensável que a companhia estabeleça também uma cultura de governança de dados, que adote todas as medidas operacionais e de segurança da informação para assegurar a integridade dos dados pessoais tratados durante a execução de suas atividades. Assim, também é essencial o envolvimento de todos os funcionários e prestadores de serviços, os quais deverão estar cientes de todas as práticas adotadas pela empresa para assegurar que a privacidade e os dados pessoais dos titulares de dados estão sendo devidamente tutelados.

O GDPR define os termos *Privacy by Design* e *Privacy by Default* e, apesar de a LGPD não adotá-los expressamente, são conceitos muito similares às determinações da lei brasileira e podem auxiliar no cumprimento da legislação aplicável de proteção de dados:

Privacy by Design
Considerar a natureza, os propósitos, o contexto e o escopo do processamento dos dados, no momento da criação de produtos e prestação de serviços, implementando medidas de segurança baseadas no risco.

Privacy by Default
Configurações-padrão de produtos ou serviços devem proteger o titular de dados na maior extensão possível, tanto em nível técnico quanto operacional, garantindo que o mínimo dos dados pessoais seja tratado.

O "*Privacy by Design*" consiste em aplicar os conceitos e princípios da proteção de dados desde a criação de uma tecnologia, de modo que esses estejam intrinsicamente integrados à sua funcionalidade.

Já o "*Privacy by Default*" exige que os controladores implementem medidas apropriadas, tanto em nível técnico quanto organizacional, para garantir que as tecnologias funcionem, natural e automaticamente, de forma a processar apenas o mínimo de dados pessoais necessário para cumprir seu propósito específico. Esse modelo de desenvolvimento visa a evitar o processamento excessivo, e auxiliar o controle sobre o armazenamento e a acessibilidade dos dados.

O principal diferencial dos referidos conceitos é que estes se baseiam em uma abordagem preventiva, e não reativa, como as empresas costumam adotar. Portanto, as companhias devem analisar toda a estrutura e os mecanismos de segurança inseridos no produto antes mesmo que ele seja lançado para o público, adotando todas as medidas possíveis para evitar que qualquer violação de dados venha a ocorrer.

Atenção!

O que é importante fazer após a conclusão do projeto?

- Estabelecer ou estruturar uma área responsável pelas questões relacionadas a proteção de dados;
- Monitorar e acompanhar os funcionários de perto, para verificar se as novas diretrizes estão sendo cumpridas;
- Atualizar o mapeamento regularmente;
- Aprimorar e implementar novos processos com relação às solicitações de titulares de dados e/ou da ANPD;
- Realizar treinamentos periódicos sobre os principais tópicos de proteção de dados (solicitação de titulares de dados; uso de dados de consumidores; obtenção do consentimento, etc.);
- Manter o Programa de Governança ativo, fornecendo a todos os colaboradores subsídios para garantir a proteção dos dados pessoais dos titulares de dados;
- Observar as novas diretrizes e/ou instruções normativas elaboradas pela ANPD para o tratamento de dados;
- Informar aos novos funcionários a importância da proteção dos dados para a empresa e instruí-los sobre o Programa de Governança de Dados implementado e adotado pela empresa, por meio de treinamentos, que poderão, inclusive ser gravados para essa finalidade exclusiva.



VEIRANO ADVOGADOS

A Experiência Veirano conta com uma abordagem holística, multidisciplinar e orientada para negócios. A fim de suprir todas as necessidades relacionadas à LGPD, nosso time de Proteção de Dados & Privacidade desenvolveu diversos formatos de projetos, que compreendem diferentes escopos de trabalho para atender demandas específicas de cada um dos nossos clientes:

1. Adequação completa

Com a atuação de uma equipe multidisciplinar, este projeto é destinado aos clientes que possuem como objetivo identificar e avaliar todas as atividades de Tratamento realizadas pela sua empresa e, a partir disso, identificar as vulnerabilidades e estruturar um plano de ação para criação de um programa de privacidade, proteção de dados embasado em pilares jurídico, processuais, de segurança da informação e governança corporativa.

2. *DPO as a service*

Neste modelo, assumimos a função de Encarregado (DPO) em nome do cliente. Para isso, alocamos um profissional para executar as atividades de gestão e monitoramento do programa de proteção de dados e privacidade do cliente.

3. Assessoria em M&A

Criado para assessorar clientes nos processos de auditoria legal de operações de fusão e aquisição, com o propósito de identificar questões de natureza jurídica relevantes (*red-flags*) e mitigar riscos relacionados à proteção e segurança de dados pessoais da empresa-alvo.

4. LGPD Pocket

Uma assessoria "pocket" para a adequação das atividades e/ou dos produtos desenvolvidos pela empresa, independentemente de seu porte ou linha de negócios, com um número reduzido de entregáveis.

5. LGPD on Demand

O LGPD on Demand é direcionado às organizações que desejam contar com uma assessoria multidisciplinar jurídica, de segurança da informação e governança corporativa, com atuação pontual e específica, relacionada a proteção de dados pessoais.

6. LGPD Legal Helpdesk

O Helpdesk foi criado para assessorar clientes em consultas e demandas sobre proteção de dados dentro de um pacote mensal de horas, seja antes, durante ou após o processo de adequação inicial.

7. Task Force para avaliação e comunicação de incidentes de segurança (VA Cybersecurity)

Assessoria jurídica específica e multidisciplinar para aspectos relacionados à suspeita ou ocorrência de um Incidente de Segurança, de acordo com as instruções mais atualizadas da ANPD e demais leis e regulamentos aplicáveis ao tema.

8. Representação em ações administrativas e judiciais envolvendo proteção de dados

Representação de clientes em ações ou potenciais ações administrativas e/ou judiciais em matéria de proteção de dados.

9. Análise de decisões administrativas e judiciais sobre proteção de dados

Monitoramento periódico de decisões proferidas em processos judiciais e administrativos, a fim de apresentar o entendimento das autoridades e os impactos para a empresa ou setor econômico ao cliente de forma resumida.

10. Elaboração e atualização de relatório de impacto à proteção de dados

A ANPD poderá solicitar ao Controlador o Relatório de Impacto à Proteção de Dados Pessoais (“RIPD” ou, em inglês, “DPIA”). Nossa equipe possui expertise no tema, e pode auxiliar com a elaboração e atualização do RIPD.

11. Desenvolvimento de workshops

Elaboração e aplicação de treinamentos sobre os principais conceitos de privacidade e proteção de dados para capacitação de seus colaboradores.

12. Playbook para negociação de contratos comerciais

Elaboração de *playbooks* para negociação e contratos comerciais, para facilitar e agilizar processos internos de equipes comerciais, técnicas e jurídicas.

13. Handbook para resposta aos titulares

Elaboração de materiais para auxiliar as empresas no atendimento tempestivo das solicitações dos titulares, bem como no procedimento a ser seguido pela empresa na resposta ao titular, conforme o modelo de negócio da companhia.

14. Transferência internacional de dados

Ajudamos clientes a entender o contexto da transferência internacional, adequá-la ao fundamento legal aplicável, avaliar requisitos de localização de dados, aditar contratos, elaborar e revisar acordos intragrupo e, de forma geral, responder consultas relacionadas à harmonização da legislação estrangeira com a brasileira.

15. Auditoria de privacidade e proteção de dados

Realizamos auditorias para avaliação do nível de maturidade da companhia, apresentando recomendações para mitigação de risco.

16. Elaboração e revisão de documentos pertinentes ao setor financeiro

Nosso time tem expertise em elaborar políticas de segurança em conformidade com as regulamentações específicas de segurança da informação do Banco Central, além de responder consultas sobre o tema.

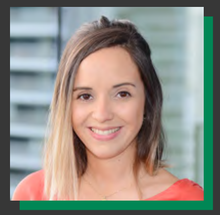
Estamos à disposição caso tenha dúvidas ou precise de informações adicionais



FÁBIO PEREIRA
+55 11 2313 5906
fabio.pereira@veirano.com.br



CINTIA ANDRADE
+55 21 3824 4655
cintia.andrade@veirano.com.br



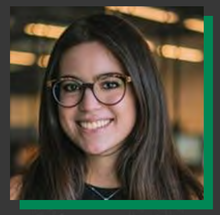
DENISE LOUZANO
+55 11 2313 5912
denise.louzano@veirano.com.br



ISABEL HERING
+55 11 2313 5726
isabel.hering@veirano.com.br



PAOLA LORENZETTI
+55 11 99976 8480
paola.lorenzetti@veirano.com.br



HELOISA HELENA DE PAULA CUNHA
+55 11 2313-3830
heloisa.cunha@veirano.com.br

Disclaimer: Este material foi atualizado pela última vez em 20 de julho de 2023 e publicado em 21 de julho de 2023. Para informações mais atualizadas, entre em contato conosco.