WWW.PERICIACOMPUTACIONAL.COM
(54)99645-0777

"Sem segurança não há privacidade"

LGPD

GUIA DE IMPLEMENTAÇÃO PARA SUA EMPRESA

Material elaborado para facilitar o início do seu trabalho de adequação à LGPD.

28 passos para você começar.

PETTER ANDERSON LOPES

Petter Anderson Lopes
DPO (LGPD e GDPR)
Perito em Forense Digital (Judicial, Ad Hoc e Consultoria)
Hacker Ético
Árbitro (Juiz Arbitral)

P +55 (54)99645-0777
E petter@periciacomputacional.com

W www.periciacomputacional.com

Skype petter.lopes

Guia para implementação da LGPD na sua empresa

A LGPD (LEI GERAL DE PROTEÇÃO DE DADOS) é aplicada para qualquer operação de tratamento de dados pessoais realizada por pessoa natural ou por pessoa jurídica. Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I. A operação de tratamento seja realizada no território nacional; ou
II. A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III. Os dados pessoais objeto do tratamento, tenham sido coletados no território nacional.

Consideramos dados coletados quando o titular se encontra no País no momento da coleta.

Por exemplo, quando um estrangeiro estiver em férias no Brasil, e seus dados forem coletados por um hotel, então esse dado está submetido à LGPD.

A exceção se dá nos dados de origem internacional em passagem pelo Brasil, sem processamento.

Para facilitar o início da implementação da conformidade da empresa com a Lei Geral de Proteção de Dados, elaborei este pequeno guia em 28 passos.

Importante

O sucesso da implementação da LGPD na sua empresa vai depender exclusivamente de você e sua equipe. Para que o projeto seja executado com sucesso será necessário a leitura completa da lei bem como a sua compreensão, além de adoção e compreensão de normas já reconhecidas e amplamente difundidas internacionalmente.

Os 28 passos para a implementação

1. Crie um **comitê da LGPD**, para a implementação da **LGPD** na organização. Delegue responsabilidades para pessoas "chave" que possam repassar o conhecimento e informar sobre o projeto para as demais áreas da empresa. Recomenda-se que pelo menos uma pessoa de cada área faça parte do grupo.

2. Nomeie um **encarregado de proteção de dados DPO**, de preferência alguém com conhecimento em Segurança da Informação e a **LGPD**, conhecer a **ISO27001** fará uma grande diferença.

3. Procure seguir alguma norma, a **ISO27001** será de grande ajuda, podemos perceber sua importância na certificação para DPO (Data Protection Officer) da Exin.

4. **Mapeie os dados**, ou seja, estabeleça os dados que sua empresa coleta, onde coleta, como e onde armazena.

5. Não obtenha dados que não são relevantes para a sua finalidade, não guarde dados que você não precisa, guarde os dados

relevantes somente pelo tempo determinado e possibilite sua fácil atualização e exclusão.

6. Separe os dados em **categorias**, se a sua empresa desenvolve sistemas, também será necessário avaliar a conformidade do seu produto.

7. Identifique a **base legal** para processar cada categoria de dados. É importante lembrar que a **LGPD** não irá se sobrepor a outras regras, sendo assim, é importante entender bem a sua regra de negócios e implementar a **LGPD** de acordo com **CDC**, **CPC**, **Marco Civil da Internet**, **Lei Carolina Dieckmann**, etc...

8. **Verifique os sistemas de terceiros**, tenha conhecimento de como processadores e controladores de dados estão agindo perante os dados de seus clientes, como por exemplo, Zoho, Intercom, Mailchimp, sistemas de Gestão de RH, Gestão de Saúde, etc ... Este cuidado é necessário pois você **poderá** estar **violando a lei indiretamente**.

9. Implementar uma política para identificar e manipular quaisquer **solicitações de acesso de assunto de dados**.

10. Implemente uma política para identificar e manipular qualquer **solicitação de correção ou eliminação de dados**.

11. Crie um documento de **problemas** de **não conformidade** para mostrar a conscientização sobre omissões de conformidade e para planejar a conformidade total ou, pelo menos, a mitigação de riscos completa.

12. Crie uma **política** de **Segurança da Informação**, pois "*sem segurança não há privacidade*".

13. Entre em contato com seu banco de dados inteiro, você irá precisar adequar seu armazenamento de dados de modo que fique fluído. Neste momento será necessário pensar também em como fazer a transferência dos dados, pois há a necessidade de garantir a portabilidade.

14. Mantenha um **registro dos consentimentos** para aqueles que já optaram por participar e aqueles que ainda estão optando por fazê-lo.

15. Crie uma **agenda de retenção** para dados. Quando os dados chegaram ao final do seu período de retenção, destrua-os de acordo com uma **política de destruição de dados** (minimize os dados que você guarda).

16. Treine sua equipe para que **TODOS** entendam o **que constitui dados pessoais**, de início explique e exemplifique os papeis do controlador, processador, **DPO**, também é de extrema importância ficar claro o que significa cada um dos 10 princípios da LGPD.

17. Treine sua equipe para **identificar violação** de dados e mantenha um registro dos eventos.

18. Opte por Segurança por Design, ou seja, desde sua concepção, quando possível.

DPO

PETTER LOPES

WWW.PERICIACOMPUTACIONAL.COM
(54)99645-0777

Relatório de Impacto à Proteção de Dados
RIPD ou DPIA (para a GDPR)

De acordo com o inciso XVII do artigo 5º, que faz alusão a esse relatório como sendo a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco"

19. Implemente uma política de **Resposta à Incidentes**, neste momento pode aproveitar para alinhar com seu **Relatório de Impacto à Proteção de Dados RIPD**.

20. Faça o devido inventário de seus equipamentos, verifique se os **computadores estão criptografados**, crie regras bem definidas para o transporte dos equipamentos para fora da empresa,

também crie regras para **BYOD**. Manter sempre um registro de ativos atualizado.

21. Revise e documente a **segurança física** dos dados (discos USB, sistemas de arquivamento de papel atrás de trava e chave, etc.)
22. Bloqueie com segurança **todos os dados pessoais** incluindo dados sensíveis.

23. Considere quais indivíduos devem ter **acesso aos dados em cada dispositivo**.

24. Atualize a **política de privacidade** do seu site (para incluir a identidade do responsável pelo processamento e a base legal, o interesse legítimo, qualquer destinatário ou categorias de destinatários dos dados pessoais, o direito de retirar o consentimento a qualquer momento e o período de retenção de dados). Verifique o uso de **cookies do seu website**.

25. Realize auditorias internas para verificar a conformidade com a **LGPD** e também quanto a norma de segurança adotada (pode ser a **ISO27001**).

26. Realize periodicamente testes de intrusão (**Pentest** ou Penetration Tests), tenha em seus contatos o nome de um **Hacker Ético** (ou **Pentester)**.

27. Use os relatórios de Pentest a seu favor, tanto para identificar as vulnerabilidades e potenciais invasões afim de corrigir e aumentar a segurança da sua organização, quanto para passar ao seu cliente como forma e confiança, demonstrando que a sua empresa tem preocupação com a segurança e privacidade dos dados.

28. Contate um **Perito em Computação Forense** que **tenha conhecimento** sobre a **LGPD** para lhe ajudar a produzir provas quando necessário.

DOS REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

LGPD

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses

I
Mediante o fornecimento de consentimento pelo titular, não pode ser utilizado mecanismos de aceite automático.

II
Para o cumprimento de obrigação legal ou regulatória pelo controlador. Vale lembrar que a LGPD não sobrepõe outras leis.

III
Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

IV
Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais

V
Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

VI
Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

VII
Para a proteção da vida ou da incolumidade física do titular ou de terceiro.

VIII
Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

IX
Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X
Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Fonte: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Petter Anderson Lopes
DPO (LGPD e GDPR)
Perito em Forense Digital (Judicial, Ad Hoc e Consultoria)
Hacker Ético
Árbitro (Juiz Arbitral)

P +55 (54)99645-0777
E petter@periciacomputacional.com
W www.periciacomputacional.com
Skype petter.lopes