*Um guia elaborado para simplificar o **início** da sua jornada de estudos com a Lei Geral de Proteção de Dados.*

GPS LGPD

ALICE FERREIRA

PALAVRAS DA AUTORA

ALICE FERREIRA

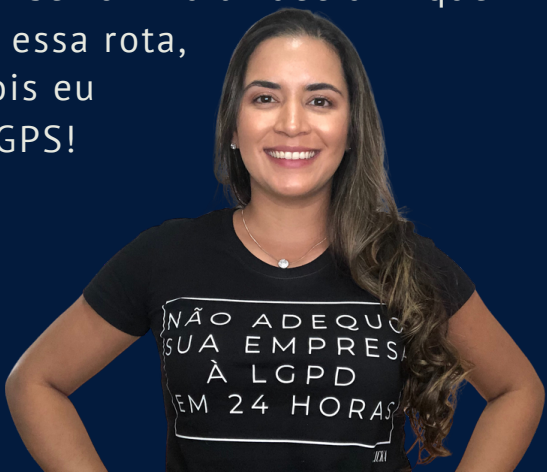
Não, esse EBook não possui a ambição de te dar uma solução mágica ou ditar verdades sobre a Lei Geral de Proteção de Dados e sua aplicabilidade. Apresento a você dicas, tópicos e pontos essenciais sobre um processo de adequação, pois quero instigar o seu interesse pelo tema e descobrir as oportunidades profissionais que a LGPD pode trazer para sua atividade profissional, seja você leitor da área jurídica ou de segurança da informação.

Reconheço que trabalhar com LGPD não é uma jornada solitária, pois precisamos aprender a conversar com diversas áreas, muitas vezes opostas de nossa expertise. Advogados precisam largar o juridiquês de lado e engenheiros de segurança da informação precisam dar ouvidos a essa gente que não entende nada de programação, mas no fim a missão é a mesma: Garantir a proteção de dados de pessoas como você e eu, e transformar a nossa sociedade da informação mais responsável e ética.

PALAVRAS DA AUTORA

ALICE FERREIRA

Aqui vou apresentar em linhas gerais pontos do roteiro de adequação, batizei o meu método de trabalho e ensino inclusive de GPS LGPD, pois é a analogia que mais gosto de usar durante as consultorias que gerencio. Temos como ponto de partida a situação atual da empresa, e como linha de chegada o respeito às disposições da LGPD - a conformidade. Para chegar cada vez mais perto da linha de chegada, precisamos analisar a distância, os obstáculos, traçar a rota e avaliar o tempo. Podem haver imprevistos na jornada, dificuldades de seguir o percurso ou até mesmo necessidade de recalcular a rota, mas ainda sim, sabemos qual é o destino final que buscamos. Aqui você vai poder observar o caminho por cima, e se um dia decidir que também quer percorrer essa rota, pode contar comigo, pois eu posso te ajudar com o GPS!



PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

CONTEXTUALIZANDO A **LEI GERAL DE PROTEÇÃO DE DADOS**

A Lei Geral de Proteção de Dados (nº 13.709/2018), ou simplesmente conhecida como LGPD, foi sancionada em agosto de 2018, primeiramente com um período de vacância e posteriormente prorrogações.

Sobre o cenário atual da LGPD, devo esclarecer que:
- A lei entrou em vigor, ou seja, está valendo desde 18 de setembro de 2020. Exceto as disposições sobre sanções administrativas.
- Os artigos referentes a sanções administrativas entrarão em vigor a partir de 1º de agosto de 2021.

A LGPD estabelece normas rigorosas para o tratamento e proteção de dados pessoais, com definições e disposições sobre o tratamento, direitos dos titulares, ações a serem adotadas para prevenção de riscos e como agir caso de ocorrências excepcionais.

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

CONTEXTUALIZANDO A **LEI GERAL DE PROTEÇÃO DE DADOS**

É muito importante ressaltar que a Lei Geral de Proteção de Dados ainda possui lacunas procedimentais e interpretativas de suas normas, e essas lacunas serão preenchidas com a edição de regulamentações e recomendações da Autoridade Nacional de Proteção de Dados - ANPD.

Por exemplo: O Art. 55-J da LGPD estabelece as competências da ANPD, e no inciso XVIII diz:

*"XVIII - editar normas, orientações e procedimentos simplificados e **diferenciados**, inclusive quanto aos prazos, para que **microempresas e empresas de pequeno porte**, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;"*

Ou seja, em breve teremos normas especiais para essa categoria de empresas que poderão prever prazos especiais, ou sobre a figura do Encarregado de Dados.

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

CONTEXTUALIZANDO A **LEI GERAL DE PROTEÇÃO DE DADOS**

Mas isso significa que devemos esperar essas regulamentações para começar a trabalhar de fato com a LGPD?

Absolutamente não! Já estamos vivendo um contexto social onde a interação das pessoas com tecnologia é um caminho sem volta, e é em razão dessa nova realidade que a legislação se faz necessária.

O desafio de criar um equilíbrio entre o tratamento de dados pessoais com interesse econômico e o respeito a personalidade da pessoa natural, não começou com a LGPD. Podemos destacar o Art. 12 da Declaração Universal dos Direitos Humanos - *a nossa Pátria foi uma das primeiras nações a rattificar o documento em 1948* - que reconhece valores de proteção e privacidade individual e familiar, assim como o Art. 19 que menciona a liberdade de informação, opinião e expressão.

Alguma similaridade com a nossa tão recente Lei para você?

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

CONTEXTUALIZANDO A **LEI GERAL DE PROTEÇÃO DE DADOS**

Então qual seria o nosso momento de "maturação" sobre a LGPD que estamos vivendo agora?

Atualmente estamos no ponto onde:
- A lei já está valendo, principalmente em relação aos direitos dos titulares, que já começaram a questionar abusos e falta de transparência dos controladores.
- Órgãos como PROCON e Ministério Público já trabalham ativamente na fiscalização e defesa de direitos dos titulares.
- Enquanto a sociedade começa a descobrir a existência da lei, as empresas passam a entender a importância de buscar conhecimento especializado e integrar procedimentos internos de proteção de dados pessoais, para evitar passivos financeiros.
- Os profissionais devem iniciar a execução de projetos de *compliance* em proteção de dados, transmitindo conhecimento, gerando consciência e adotando medidas técnicas com reavaliação contínua nos próximos meses.

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

CONTEXTUALIZANDO A **LEI GERAL DE PROTEÇÃO DE DADOS**

E por onde podemos começar?

Existem dois ditados que eu gosto de usar para ilustrar esse momento atual: "Antes tarde do que nunca" e "Feito é melhor que perfeito". Sim, estamos atrasados no mundo perfeito de conformidade, se considerarmos que as sanções começarão em agosto, e sim, ainda haverão regulamentações a serem publicadas.

Mas agora é o momento de COMEÇAR o quanto antes e com os instrumentos que temos nas mãos. Seja analisando as bases legais, respeito aos princípios, medidas de segurança disponíveis e o mais importante de tudo: consolidação de cultura e entendimento sobre Proteção de Dados Pessoais.

E são esses passos fundamentais que vou apresentar para você em um conjuto de check lists!

Lembrete: Você pode acrescentar ou reduzir ações de acordo com as especificidades do seu cliente.

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GPS LGPD

QUEM É QUEM NA
LEI GERAL DE PROTEÇÃO DE DADOS

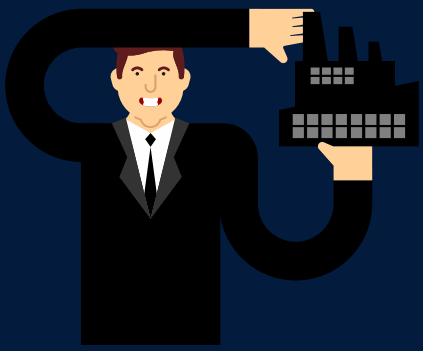
Vamos começar identificando as figuras descritas pela LGPD e seus diferentes papéis:

TITULAR

Pessoa natural a quem se referem os dados objeto de tratamento.

CONTROLADOR

Pode ser pessoa natural ou jurídica e possui poder de comando e decisão sobre como os dados pessoais deverão ser tratados.



PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GPS LGPD

QUEM É QUEM NA
LEI GERAL DE PROTEÇÃO DE DADOS

OPERADOR

Aquele que realiza o tratamento de dados pessoais em nome do controlador, acatando suas diretrizes.

ENCARREGADO

Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD

Orgão da administração pública direta federal com atribuições relacionadas a regulamentação e fiscalização do cumprimento da LGPD.

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GPS LGPD

O NORTE QUE DEVEMOS SEGUIR
PRINCÍPIOS DA LGPD

Não importa sua expertise, advogado ou engenheiro, todos nós devemos ter como o norte de nossas bússulas os Princípios da LGPD.

Princípios são o alicerce sólido de uma norma, portanto, caso uma ação não respeite um dos princípios, poderá ser considerada em vão. Eis a importancia de masterizar esses preceitos e engloba-los em todas as nuances de um projeto de adequação. Os princípios da LGPD são:

FINALIDADE	ADEQUAÇÃO
NECESSIDADE	QUALIDADE DOS DADOS
TRANSPARÊNCIA	LIVRE ACESSO
SEGURANÇA	PREVENÇÃO
NÃO DISCRIMINAÇÃO	PRESTAÇÃO DE CONTAS

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GPS LGPD

DIGA-ME UM PORQUÊ

BASES LEGAIS DA LGPD

As Bases Legais da LGPD são as hipóteses/ fundamentos/justificativas, que legitimam a coleta e tratamento de dados pessoais.

Importante reforçar que para cada finalidade, é necessário indicar qual a base legal. Não existe uma base mais forte ou melhor que a outra, ou uma bala de prata que irá garantir poderes ilimitados. Lembre-se que qualquer uma das Bases Legais abaixo deverá obedecer todos os Princípios.

CONSENTIMENTO	■	■	CUMPRIMENTO DE OBRIGAÇÃO LEGAL
EXEUCUÇÃO DE POLÍTICAS PÚBLICAS	■	■	ESTUDOS POR ÓRGÃO DE PESQUISA
DILIGÊNCIA/EXECUÇÃO DE CONTRATO	■	■	EXERCÍCIO REGULAR DE DIREITO
PROTEÇÃO DA VIDA	■	■	TUTELA DA SAÚDE
LEGÍTIMO INTERESSE	■	■	PROTEÇÃO AO CRÉDITO

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

ATENÇÃO ESPECIAL PARA OS **DIREITOS DOS TITULARES**

Quando a LGPD entrou em vigor, ainda que parcialmente, em setembro de 2020, de imediato afirmei: Os Direitos dos Titulares precisam ser respeitados imediatamente para evitar problemas maiores! E há quem tenha relativizado dizendo que não era hora para alarmes.

Em janeiro de 2021 já era possível ler em diversas manchetes: Aumento de reclamações, ações judiciais fundamentadas na LGPD, notificações do PROCON e Ministério Público, e a pressão social por transparência só aumenta.

O fato das sanções administrativas estarem em vacância até agosto de 2021, significa que a ANPD não poderá autuar as empresas, mas os Direitos dos Titulares não estão em vacância. Além de já estarem valendo, também já é possível observar seus reflexos, seja por iniciativa popular ou pelos órgãos responsáveis por verificar se tais disposições da lei estão sendo respeitadas ou não.

Mas afinal, quais direitos são esses?

ATENÇÃO ESPECIAL PARA OS

DIREITOS DOS TITULARES

O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

- CONFIRMAÇÃO DA EXISTÊNCIA DO TRATAMENTO
- ACESSO AOS DADOS
- CORREÇÃO, ATUALIZAÇÃO OU COMPLEMENTAÇÃO
- ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO
- PORTABILIDADE MEDIANTE REQUISIÇÃO
- ELIMINAÇÃO DE DADOS CONSENTIDOS
- INFORMAÇÃO SOBRE COMPARTILHAMENTO
- INFORMAÇÃO SOBRE POSSIBILIDADE DE NÃO CONSENTIR E CONSEQUÊNCIAS
- REVOGAÇÃO DO CONSENTIMENTO

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GPS LGPD

CALMA! EXISTEM EXCEÇÕES!

QUANDO A LGPD NÃO SE APLICA

Toda Lei que se preze, apresenta suas próprias excessões. Brincadeiras a parte, destaquei abaixo situações que dispensam a observância da LGPD.
Lembrando que as exceções também merecem uma análise dedicada no caso concreto, quando eventualmente, o titular se sentir lesado pelo tratamento de dados.

- REALIZADO POR PESSOA NATURAL SEM FINALIDADE ECONÔMICA
- REALIZADO PARA FINS EXCLUSIVAMENTE JORNALÍSTICO, ARTÍSTICO E ACADÊMICO
- REALIZADO PARA FINS EXCLUSIVOS DE SEGURANÇA PÚBLICA; DEFESA NACIONAL; SEGURANÇA DO ESTADO; ATIVIDADES DE INVESTIGAÇÃO E REPRESSÃO DE INFRAÇÕES PENAIS;
- PROVENIENTES DE FORA DO TERRITÓRIO NACIONAL E QUE NÃO SEJAM OBJETO DE COMUNICAÇÃO, COMPARTILHAMENTO COM AGENTES DE TRATAMENTO BRASILEIROS OU OBJETO DE TRANSFERÊNCIA INTERNACIONAL DE DADOS COM OUTRO PAÍS QUE NÃO O DE PROVENIÊNCIA, **DESDE QUE O PAÍS DE PROVENIÊNCIA PROPORCIONE GRAU DE PROTEÇÃO DE DADOS PESSOAIS ADEQUADO**

GPS LGPD

DICAS QUE VOCÊ VAI ENCONTRAR NESSE CHECK LIST

- IDENTIFICANDO O CLIENTE
- ANÁLISE ESPECÍFICA
- LEVANTAMENTO REGULATÓRIO
- ANÁLISE DE LACUNAS
- PLANO DE AÇÃO
- POLÍTICA DE PRIVACIDADE
- CONSCIENTIZAÇÃO DA EQUIPE
- COMITÊ DE SEGURANÇA
- MAPEAMENTO DE DADOS
- PRIVACY BY DESIGN
- RELATÓRIO DE IMPACTO
- MONITORAMENTO

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

AS FASES DE UM **PROJETO DE ADEQUAÇÃO**

Primeiramente, preciso ressaltar que o processo de estar em conformidade é cíclico. Começamos identificando os principais pontos da empresa, mas é necessário monitoramento e nova análise, afinal, os colaboradores mudam, as tecnologias utilizadas mudam, assim como as próprias demandas e processos internos da empresa também podem mudar. Resumidamente, temos as fases que você, profissional em proteção de dados, irá seguir é:

- IDENTIFICAR O CLIENTE
- CONSCIENTIZAR A EQUIPE
- ANÁLISE ESPECÍFICA PARA PLANEJAMENTO
- CRIAR UM COMITÊ MULTIDISCIPLINAR
- LEVANTAR REGULAMENTAÇÕES ADICIONAIS
- MAPEAR OS DADOS
- IDENTIFICAR LACUNAS
- PLANEJAR AS SOLUÇÕES E EXECUÇÃO
- MONITORAR O DESEMPENHO E NOVAS DEMANDAS SOBRE PPD

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

IDENTIFICANDO O CLIENTE

Informações essenciais para mensurar o tempo a ser investido no projeto e apresentação de orçamento:

- NOME DA EMPRESA
- SEGMENTO (Ex. Saúde, Educação, Bancos)
- TIPO DE NEGÓCIO (B2B, B2C, B2G)
- TOTAL DE CLIENTES
- GRUPO ECONÔMICO, MATRIZ, FILIAL
- QUANTIDADE DE DEPARTAMENTOS
- QUANTIDADE DE COLABORADORES
- QUANTIDADE E TIPOS DE CONTRATOS

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

CONSCIENTIZAÇÃO DA EQUIPE

Quem vai acompanhado, chega mais rápido! Prepare os colaboradores com conhecimento e poderá contar com o engajamento de todos no projeto.

- [ ] AGENDAMENTO DE WORKSHOP
- [ ] O QUE É A LGPD?
- [ ] QUAL O OBJETIVO DA LGPD?
- [ ] VERDADES E MITOS
- [ ] ACESSO CONSCIENTE
- [ ] RESPONSABILIZAÇÃO
- [ ] PRINCÍPIOS DA LGPD
- [ ] BASES LEGAIS DA LGPD
- [ ] QUAIS SÃO OS DIREITOS DOS TITULARES?
- [ ] ENTREGA DE INFORMATIVO COM RESUMO

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

ANÁLISE ESPECÍFICA

Entender detalhamente a estrutura da empresa.

Quais departamentos a empresa possui?

- [ ] RECURSOS HUMANOS
- [ ] COMERCIAL/VENDAS/CONTRATOS
- [ ] FINANCEIRO
- [ ] PÓS VENDA/SAC/ASSISTÊNCIA TÉCNICA
- [ ] MARKETING E RELACIONAMENTO
- [ ] TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO
- [ ] PESQUISA E DESENVOLVIMENTO
- [ ] JURÍDICO
- [ ] CONTÁBIL
- [ ] DIRETORIA

ANÁLISE ESPECÍFICA

Entender detalhamente a estrutura da empresa.

Quais são as operações externas ou terceirizadas?

- [ ] CONTABILIDADE
- [ ] JURÍDICO
- [ ] SEGURANÇA/CONTROLE DE ACESSO
- [ ] LIMPEZA
- [ ] TRANSPORTE

- [ ] FORNECEDORES
- [ ] PARCEIROS COMERCIAIS
- [ ] VENDEDORES EXTERNOS
- [ ] OUTROS

COMITÊ DE SEGURANCA MULTIDISCIPLINAR

Para empresas de médio e grande porte é necessário a criação de um comitê de trabalho. Um representante que irá guiar a condução das ações estipuladas pelo consultor, e verificar o progresso de sua equipe e apresentar demandas ou dificuldades.

- REPRESENTANTE DA DIREÇÃO
- CONSULTIVO: ENCARREGADO OU CONSULTOR
- REPRESENTANTE DO RECURSOS HUMANOS
- REPRESENTANTE DO COMERCIAL
- REPRESENTANTE DO MARKETING
- REPRESENTANTE DA SEG DA INFORMAÇÃO

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

LEVANTAMENTO REGULATÓRIO ADICIONAL

Existem outras legislações que precisamos observar em paralelo a LGPD com esse cliente? Exemplos:

- CÓDIGO DE DEFESA DO CONSUMIDOR
- BACEN
- ANVISA
- GPDR
- ISOS
- LEI DE ACESSO A INFORMAÇÃO
- MARCO CIVIL DA INTERNET

Antes de iniciar os trabalhos com LGPD, é necessário considerar legislações que já eram observadas pela empresa para integrar mais medidas de conformidade legal e não sobrepor uma legislação sobre a outra. É necessário buscar uma sinergia entre todas essas frentes.

MAPEAMENTO DE DADOS

Agora vamos identificar quais dados pessoais estão armazenados na empresa, fluxo e possíveis exposições. O mapeamento identificar pontos como:

- DEPARTAMENTO - ATIVIDADE - PROCESSO
- ORIGEM DO DADO
- RESPONSÁVEL PELO PROCESSO
- DESCRIÇÃO DOS DADOS SOLICITADOS
- TIPO DE DADO: COMUM, SENSÍVEL, CRIANÇA
- FINALIDADE INTERNA
- BASE LEGAL
- AUTORIZAÇÃO E CONTROLE DE ACESSO
- RESPONSÁVEL HIERÁRQUICO
- SOFTWARE UTILIZADO
- lOCAL DE ARMAZENAMENTO
- COMPARTILHAMENTO COM TERCEIROS
- COMPARTILHAMENTO INTERNACIONAL
- SEGURANÇA APLICADA
- PRAZO PARA DESCARTE

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

ANÁLISE DE LACUNAS

Depois de fazer o levantamento de quais dados pessoais você possui na sua mão, vamos olhar para esse mapeamento e identificar quais pontos estão em desacordo com a LGPD e quais medidas administrativas e técnicas podemos adotar para aprimorar a segurança do armazenamento e tratamento de dados, mitigando ou minimizando os riscos da empresa. Considere na Análise de Lacunas:

- OS DIREITOS DOS TITULARES ESTÃO SENDO OBSERVADOS?
- OS PRINCÍPIOS DA LGPD ESTÃO SENDO OBSERVADOS?
- FRAGILIDADES NOS SISTEMAS
- GESTÃO DE CONTRATOS E PARCEIROS
- NECESSIDADE DO RELATÓRIO DE IMPACTO
- REVISÃO OU CRIAÇÃO DE POLÍTICAS

Lembre-se: Analisar apenas do ponto de vista técnico é tão ineficaz quanto analisar apenas do ponto de vista legal. As fases de mapeamento e lacunas são atividades multidisciplinares e as propostas de soluções também deverão ser feitas considerando essas duas faces disciplinares.

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

PRIVACY BY DESIGN

O privacy by design é um conceito que nasceu na década de 1990, e foi idealizado primeiramente para setores da tecnologia, entretanto vem ganhando peso como medida de compliance para proteção de dados e privacida após a generosa menção do conceito pelo Regulamento Europeu (GDPR) usando a estratégia como um importante direcionamento de ações necessárias.

O que é privacy by design?
O privacy by design é uma abordagem à engenharia de sistemas que, basicamente, diz que um produto ou sistema precisa ser pensado, projetado e desenvolvido para proteger os dados dos usuários desde sua concepção.

Diferente da GDPR, a nossa LGPD não destaca um capítulo ou menciona o conceito em seu texto, mas o profissional que entende os princípios de PBD e os expressa em seu projeto de adequação, sem dúvidas estará mais próximo do ideal de conformidade e buscando garantir de fato, não apenas a obediência da lei, mas a efetivação da proteção à privacidade do titular.

PRIVACY BY DESIGN

OS SETE PRINCÍPIOS

- PROATIVO NÃO REATIVO / PREVENTIVO NÃO CORRETIVO
- PRIVACIDADE INCORPORADA AO DESIGN DA SOLUÇÃO
- FUNCIONALIDADE COMPLETA
- SEGURANÇA DE PONTA A PONTA (END-TO-END)
- VISIBILIDADE E TRANSPARÊNCIA
- RESPEITO PELA PRIVACIDADE DO USUÁRIO
- PRIVACIDADE COMO CONFIGURAÇÃO PADRÃO

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

PLANO DE AÇÃO
IMPLEMENTANDO SOLUÇÕES

Se você chegou aqui, posso interpretar que você já conhece a fundo a empresa e atividade do seu cliente, educou os colaboradores para que tivessem conhecimento sobre a LGPD, montou uma equipe com diversas frentes representativas, verificou os ativos de dados que a empresa possui e também analisou quais são os pontos delicados que precisam ser sanados, agora que temos um diagnóstico completo e uma equipe amadurecida, vamos executar as soluções! Agora é necessário:

- APRESENTAR CADA AÇÃO PARA SANAR OU REDUZIR O RISCO ANTERIORMENTE VERIFICADO
- INDICAR QUEM SERÃO OS EXECUTORES DE CADA AÇÃO
- ESTIPULAR UM CRONOGRAMA

Importante considerar:

- SEPARAÇÃO DE FRENTES: PROCESSOS, INFORMAÇÃO
- ENTREGAS PARCIAIS PARA VALIDAÇÃO DE APLICABILIDADE
- ATIVIDADES QUE DEPENDEM DE TERCEIROS EXTERNOS PODEM DISPOR DE MAIS ATENÇÃO

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

PLANO DE AÇÃO
O QUE NÃO FAZER

- NÃO PRIORIZAR AS AÇÕES QUE BUSQUEM SANAR OS MAIORES RISCOS
- IGNORAR AS DIFICULDADES DOS OPERADORES NA EXECUÇÃO DAS ATIVIDADES ESTIPULADAS
- DESCONSIDERAR A NECESSIDADE DE UMA NOVA ESTRATÉGIA
- DEIXAR DE REGISTRAR AS AÇÕES, PROGRESSO E REANÁLISES - CRIE PROVAS DE SUAS ATIVIDADES
- IGNORAR NOVOS RISCOS APÓS A ESTIPULAÇÃO DO PROJETO
- NÃO ATENDER OS DIREITOS DO TITULAR DURANTE A EXECUÇÃO DO PROJETO - A LEI JÁ ESTÁ VALENDO!

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

O Relatório de impacto à Proteção de Dados Pessoais - RIPD, é um documento elaborado pelo controlador para apresentar o estudo prévio dos riscos existentes no tratamento de determinados dados pessoais que sua atividade executa, e quais providências estão previstas como Controle de Risco e Gestão de Crise.

A princípio, o RIPD não é obrigatório em todos os casos, conforme breve leitura do Art. 38 da LGPD, são pontuados como exemplo, o tratamento de dados sensíveis, sem grandes detalhes.

Sua exigência será melhor definida pela ANPD. Entretanto, já se observa que o Relatório de Impacto é um excelente documento de *compliance*, além de se alinhar com os fundamentos do *privacy-by-design*.

Uma das chaves para estar e conformidade com a LGPD é a boa-fé. Prepara um Relatório de Impacto, ainda que o responsável pelo tratamento não tenha sido formalmente exigido, demontra uma conduta diligente e prepara todos os envolvidos para qualquer cenário. Pecar pelo excesso não é um problema para a LGPD.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Seguindo a leitura do Art. 38 da LGPD, verificamos que precisa constar no Relatório de Impacto:

- DESCRIÇÃO DOS TIPOS DE DADOS COLETADOS
- METODOLOGIA UTILIZADA PARA COLETA
- METODOLOGIA UTILIZADA PARA GARANTIA DA SEGURANÇA
- MEDIDAS, SALVAGUARDAS E MECANISMOS DE MITIGAÇÃO DE RISCOS ADOTADOS

Acrescente também:

- A BASE LEGAL E RESUMO DO FLUXO
- QUALIFICAÇÃO DE GRAU DE RISCO

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

POLÍTICAS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O número de Políticas a serem estipuladas pelo controlador é o menos relevante para a Adequação à LGPD, pois a mera elaboração para documentação não é o que garantirá a conformidade.

As políticas precisam ser absorvidas pela cultura da empresa e efetivamente transmitidas aos seus destinatários: colaboradores, fornecedores, parceiros, clientes, e principalmente, ser seguida por seus gestores, pois o exemplo hierárquico é indispensável.

Algumas Políticas que poderão ser desenhadas pelo controlador e posteriormente adotadas por todos são:

- POLÍTICA CORPORATIVA DE PROTEÇÃO DE DADOS
- POLÍTICA DE PRIVACIDADE
- POLÍTICA DE USO DO SITE, E DEMAIS CANAIS
- POLÍTICA DE COOKIES

COMPONENTES GERAIS DE UMA POLÍTICA DE PRIVACIDADE

- IDENTIFICAÇÃO DO RESPONSÁVEL
- QUAIS DADOS SÃO COLETADOS E TRATADOS
- FINALIDADE DO TRATAMENTO
- INFORMAR OS DIREITOS DOS TITULARES
- BASE(S) LEGAL DO TRATAMENTO
- COMPARTILHAMENTO DOS DADOS
- AUTOMATICAÇÃO, SISTEMAS
- USO DE COOKIES
- DADOS DE CRIANÇAS E ADOLESCENTES
- CANAL DE ATENDIMENTO - ENCARREGADO/DPO
- PRAZO DE RETENÇÃO - SOLICITAÇÃO DE EXCLUSÃO
- DISPOSIÇÕES SOBRE SEGURANÇA DA INFORMAÇÃO

MONITORAMENTO

A consultoria para adequação à LGPD, não é um trabalho fim, mas o início de uma nova cultura empresarial. Algumas métricas e pontos de monitoramento para se adotar:

- NÚMERO DE CLIENTES VERSUS NÚMERO DE REQUISIÇÕES, EXCLUSÕES E RECLAMAÇÕES
- QUANTIDADE DE RECUSA DE CONCESSÃO OU REVOGAÇÃO DE CONSENTIMENTO
- QUAIS AÇÕES DEIXARAM DE SER EXECUTADAS PELA EQUIPE
- QUANTIDADE DE AMEAÇAS DE INCIDENTES
- SUBSTITUIÇÃO E CONTRATAÇÃO DE NOVOS FUNCIONÁRIOS
- ALTERAÇÃO DE SOFTWARES
- ELABORAÇÃO DE NOVOS PRODUTOS
- DADOS DE CRIANÇAS E ADOLESCENTES
- AUMENTO SIGNIFICATIVO NO VOLUME DE DADOS

O programa de governança também é levado em consideração pela ANPD no momento de avaliar a autuação ou não após a ocorrência de um incidente de segurança.

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GLOSSÁRIO BÁSICO DO DIREITO DIGITAL

- LGPD ou LGPDP - Lei Geral de Proteção de Dados ou Lei Geral de Proteção de dados Pessoais
- GDPR - General Data Protection Regulation - ou em Português RGPD: Regulamento Geral de Proteção de Dados (União Europeia)
- TITULAR - Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
- CONTROLADOR - Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
- OPERADOR - Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GLOSSÁRIO BÁSICO DO DIREITO DIGITAL

- ANPD - Autoridade Nacional de Proteção de Dados: quem irá fiscalizar, regulamentar e promover o conhecimento a toda população sobre a lei
- DPO - Data Protection Officer - EM PORTUGUÊS - Encarregado de Dados: O PROFISSIONAL que fará a ponte entre o titular-empresa, autoridade-empresa.
- DADOS PESSOAIS- Informação relacionada a pessoa natural identificada ou identificável
- DADOS PESSOAIS SENSÍVEIS - Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GLOSSÁRIO BÁSICO DO DIREITO DIGITAL

- TRATAMENTO - Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração
- CONSENTIMENTO - Manifestação de vontade livre, informada e inequívoca
- CONSENTIMENTO GENÉRICO - Sem possibilidade de escolha do indivíduo ou com lacuna de informações
- CONSENTIMENTO GRANULARIZADO - Consentimento por etapas e sempre bem informado

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GLOSSÁRIO BÁSICO DO DIREITO DIGITAL

- ANPD - Autoridade Nacional de Proteção de Dados: quem irá fiscalizar, regulamentar e promover o conhecimento a toda população sobre a lei
- DPO - Data Protection Officer - EM PORTUGUÊS - Encarregado de Dados: O PROFISSIONAL que fará a ponte entre o titular-empresa, autoridade-empresa.
- ROPA - Records of Processing Activities - Registro dAS Operações de tratamento DOS DADOS PESSOAIS - PRÁTICA DE accountability
- ACCOUNTABILITY - Pode ser traduzido para o português como responsabilidade ética - remete à obrigaçãO DE transparência, prestaÇÃO DE contas (um dos princípios da LGPD)
- PIA - Privacy Impact Assessment - Avaliação de Impacto de Privacidade E relação custo-benefício

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GLOSSÁRIO BÁSICO DO DIREITO DIGITAL

- DPIA - Data Protection Impact Assessment OU RIPD - Relatório de Impacto de Proteção de Dados: análise de riscos no tratamento de dados
- LIA - Legitimate Interests Assessment - Avaliação de Legítimo Interesse: Relatório para atribuir e justificar a base legal do Legítimo Interesse do Controlador
- DSAR - Data Subject Access Request - Requisições dos titulares: são os pedidos realizados pelos titulares ao Controlador
- BYOD - Bring Your Own Device - Traga seu próprio equipamento: política empresarial que permite o colaborador levar e usar o seu próprio dispositivo de trabalho
- ANONIMIZAÇÃO - Procedimento para impossibilitar a identificação do titular dos dados

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

GLOSSÁRIO BÁSICO DO DIREITO DIGITAL

- PSEUDOANONIMIZAÇÃO - Estratégia que busca reduzir a identificação do titular, mas ainda há um interesse em manter os identificadores diretos do titular
- CRIPTOGRAFIA - Prática na qual um dado é codificado por meio de um algoritmo e descodificado por uma chave de acesso
- COOKIES - Armazenamento de histórico de busca, preferências e informações de navegação em um site.

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

QUADRO COMPARATIVO

GDPR	LGPD
REGISTRO DE ATIVIDADE DE PROCESSAMENTO	
Não obrigatório para empresas com menos de 250 funcionários	Obrigatório para todas as empresas
MULTAS	
Até 4% do faturamento / € 20 Milhões	Até 2% do faturamento / R$ 50 Milhões
REQUISIÇÃO DE INFORMAÇÕES	
Até 30 dias, gratuidade opcional	Até 15 dias a contar do requerimento, gratuita
NOTIFICAÇÃO OBRIGATÓRIA DE INCIDENTES	
72 horas	Tempo razoável (a ser definido)

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

QUADRO COMPARATIVO

GDPR	LGPD
AGÊNCIA REGULADORA	
EDPB e DPA de cada Estado Membro	ANPD (Cooperação PROCON, MP, outros)
DPO / ENCARREGADO	
Pessoa Natural ou Jurídica	Pessoa Natural ou Jurídica
LEGÍTIMO INTERESSE	
MAIS RESTRITO	MAIS FLEXÍVEL
DADOS ANONIMIZADOS	
Não são considerados pessoais em perfis	Podem ser considerados pessoais em perfis

PARTICIPE DA NOSSA COMUNIDADE LGPD NO TELEGRAM - QRCODE

QUADRO COMPARATIVO

GDPR	LGPD
PERFIS COMPORTAMENTAIS	
Necessário causar impacto no titular dos dados	Sempre considera a possibilidade de causar impactos no titular dos dados
TRANSFERÊNCIA INTERNACIONAL DE DADOS	
Possibilidade, com base no legítimo interesse, caso não seja frequente	Com consentimento específico, mesmo sem legítimo interesse
DADOS SENSÍVEIS SOBRE SAÚDE	
Não podem ser tratados mediante contrato	Podem ser tratados mediante contrato de prestação de serviço

GOSTOU DESSE EBOOK?

ACOMPANHE MINHAS REDES SOCIAIS PARA MAIS CONTEÚDOS

/gpslgpd

www.lgpdparaque.com