seusdados

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

2020

Conheça o nosso exclusivo serviço:

meudpo

DPO *as a service* CSC

SEGURANÇA DA INFORMAÇÃO

A informação é um ativo essencial para os negócios de uma organização e necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora cada vez mais exposta a ameaças e vulnerabilidades.

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos e maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

(extraído de ABNT NBR ISO/IEC 27002)

seusdados

LGPD / Lei Geral de Proteção de dados

CENÁRIO

Quando uma pessoa entrega seus dados pessoais a outrem ela precisa estar resguardada contra os riscos decorrentes da exposição indevida e da eventual má utilização desses dados.

Esses riscos decorrem da gestão incorreta do processo de tratamento de dados, e também de procedimentos equivocados adotados durante a sua coleta, compartilhamento, modo de tratar e armazenar, de comunicação e compliance, dentre outros.

Observando a prática atual, percebemos que a regulação é esparsa e não específica e a desinformação do cidadão coopera para que ocorram abusos. Existem indagações obrigatórias para a preservação da segurança e da privacidade:

Por quê? Para que? Por quanto tempo? Onde será armazenado? O que fazer em caso de uso indevido? A LGPD é de extrema importância para o mercado como um todo dada a ausência de providências práticas e efetivas por parte da grande maioria dos destinatários da LGPD.

É fundamental a adequação da sua política de tratamento de dados aos ditames da referida lei, o que demanda um tempo mais amplo para execução do processo (que deve estar *compliant*).

A Lei Geral de Proteção de Dados (LGPD) é de extrema importância para o mercado brasileiro. É fundamental que seja compreendido que a adequação da política de tratamento de dados pessoais aos ditames da referida lei demanda tempo considerável para que possa ser atingido o status de empresa adequada.

Todavia, o tempo para adaptação à lei não é única questão urgente. Existe uma defasagem competitiva que qualquer empresa brasileira tem, em termos globais, quanto a países que já possuem sua política de tratamento de dados baseados em boas práticas de segurança de dados pessoais e *compliance.*

Ao invés do enfrentamento da LGPD como "mais uma lei imposta para complicar a vida do empresariado brasileiro", como comumente se tratam as leis por aqui, ela deve ser enfrentada como uma oportunidade ímpar de nivelar a competitividade das empresas brasileiras no mercado global.

O processo de adequação das leis nacionais a uma política de segurança de dados já é uma realidade. O Regulamento Europeu de Proteção de Dados impõe que a circulação de dados pessoais com origem e destino em países não integrantes da União Europeia (UE), deve seguir os mesmos padrões e princípios de segurança definidos na sua lei, o que exigiu do Brasil e demais países do globo adaptação de suas leis para permitir que as empresas de fora do bloco que tenham interesse em tratar dados de europeus e empresas europeias possam realizar a troca de informações com referido bloco.

Resumindo:

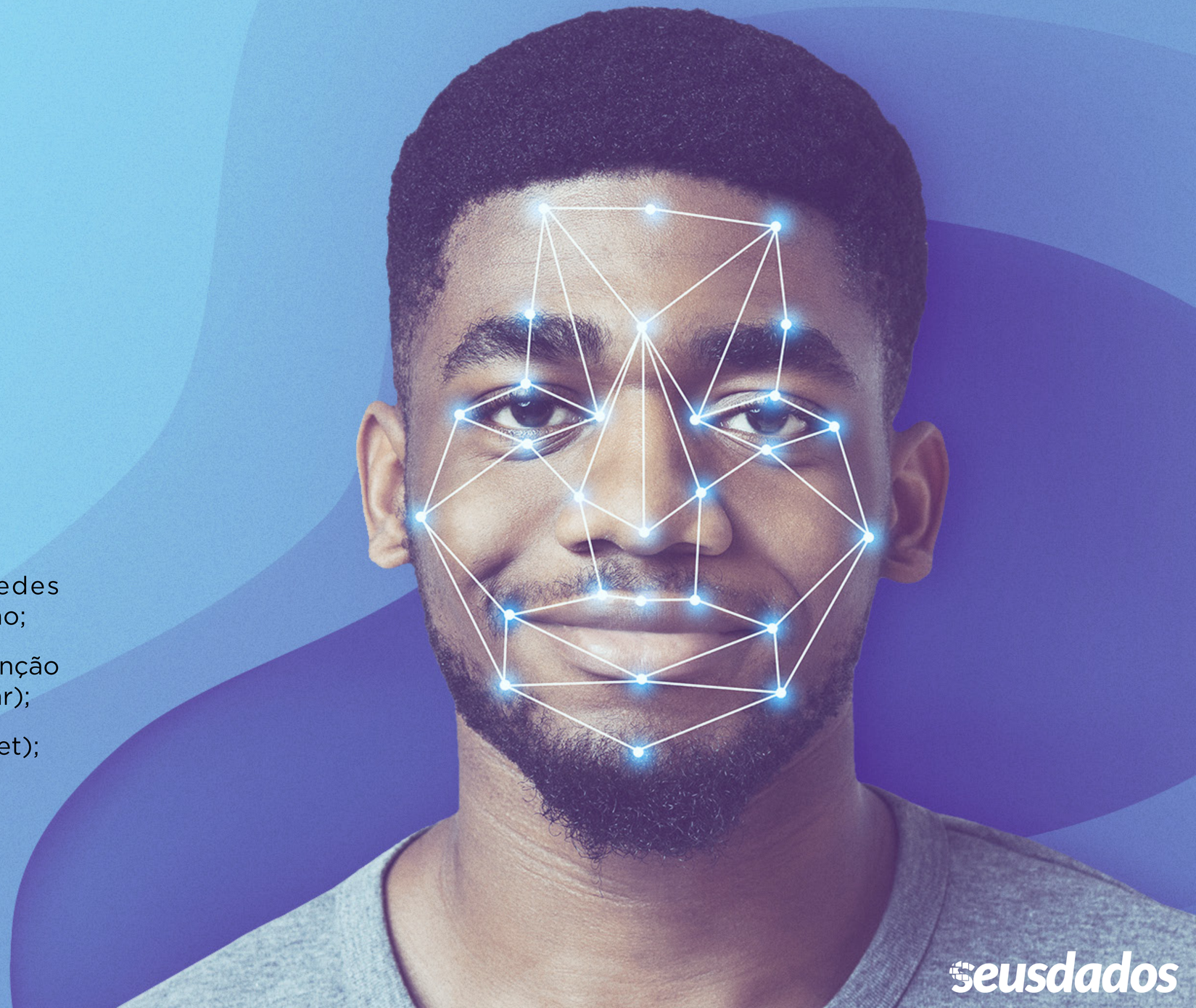
A Lei brasileira de proteção de dados pessoais (LGPD) está em período *vacatio legis.*

Sem a referida lei o cenário poderia apontar para uma situação em que se tornaria uma real possibilidade do Brasil ser classificado como um país não adequado e inseguro do ponto de vista da lei europeia de proteção de dados pessoais, o que implicaria na possibilidade de proibição pela UE de que empresas brasileiras não poderiam ofertar serviços e produtos para seus cidadãos porque estariam proibidas de tratar dados de europeus, o que sem dúvida alguma representaria grande defasagem competitiva no mercado global.

DADOS PESSOAIS

Exemplos:

- O nome e sobrenome;
- CPF, RG; o endereço da residência;
- O e-mail: nome@empresa.com.br;
- Dados de contas eletrônicas; de redes sociais, de aplicativos de comunicação;
- Dados de localização (por exemplo, a função de dados de localização em um celular);
- Um endereço IP (protocolo de Internet);
- Testemunhos de conexão (cookies).



seusdados

seusdados

CICLO DE VIDA
DOS DADOS PESSOAIS

O processo de tratamento de dados abrange todas essas fases:

meudpo
DPO as a service CSC

O **tratamento** de dados pessoais somente estará autorizado se encaixar-se em uma das seguintes bases legais:

- Bases Legais
  - Exercício regular de direitos em processo
  - Estudos por órgão de pesquisa
  - Políticas públicas pela administração
  - cumprimento de obrigação legal
  - Execução de contrato
  - legítimo interesse
  - Proteção da vida
  - Tutela da saúde
  - Proteção ao crédito
  - Consentimento do Titular

seusdados

PRINCÍPIOS QUE PERMITEM O TRATAMENTO DE DADOS

As bases legais de tratamento devem ser analisadas em conjunto e estarem adequadas aos princípios ao lado, sem exceção de nenhum deles

- **Finalidade;**
- **Adequação;**
- **Necessidade;**
- **Livre acesso;**
- **Qualidade dos dados;**
- **Transparência;**
- **Segurança;**
- **Prevenção;**
- **Não discriminação;**
- **Responsabilização e prestação de contas.**

FINALIDADE: Princípio mais relevante - propósitos legítimos, explícitos, específicos e informados. antes de tratar dados pessoais, há necessidade de transparência com o titular, em qualquer das bases legais utilizadas para tratar dados.

ADEQUAÇÃO: Tratamento tem que ser compatível com a finalidade informada ao titular para o tratamento de dados.

NECESSIDADE: Utilizar o mínimo necessário para atingir a minha finalidade de tratamento de dados.

Seusdados

Dados sensíveis:

Todo e qualquer dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como aqueles referentes à saúde ou à vida sexual, genéticos ou biométricos, quando vinculado a uma pessoa natural.

Os dados sensíveis não podem ter como base legal para o tratamento o legítimo interesse e a execução de contratos

seusdados

AUTO DETERMINAÇÃO INFORMACIONAL

O mais relevante dos direitos da LGPD

“Eu, por mim mesmo, ter o poder de determinar o que será feito com os meus dados pessoais”.

Há um questionamento que sempre deve ser feito:

O tratamento vai facilitar o acesso aos dados pelo seu titular? Se a resposta for positiva pode-se dizer que se está no caminho certo de adequação.

seusdados

APLICABILIDADE TRANSNACIONAL

O que irá definir qual a lei de proteção de dados pessoais aplicável não é a nacionalidade ou o local onde o dado está armazenado:

1

Será aplicada a lei brasileira (LGPD):

- Se o tratamento é realizado no Brasil;
- Se o tratamento presta-se para comercialização de bens ou serviços;
- Ou se refere a indivíduos localizados no Brasil, mesmo que sejam estrangeiros e não residentes;

2

Será aplicada ainda a LGPD, por exemplo:
Na hipótese de uma empresa de cloud estrangeira que colete dados no Brasil e os armazene fora do país, quanto a estes dados coletados no Brasil.

3

Será aplicável a GDPR (lei européia):
Para o tratamento de dados pessoais, por exemplo, se realizado em razão de ofertas de produtos e serviços por empresa Brasileira para cidadãos que estejam no referido continente.

Seusdados

ENCARREGADO DE PROTEÇÃO DE DADOS

DPO (Data Protection Officer)

Na dinâmica de gestão e proteção de dados, aparece a figura do encarregado (DPO), que deve ser alguém com conhecimentos jurídicos e regulatórios, cuja identidade deverá ser tornada pública, de forma clara, para que o cidadão tenha acesso a elas.

São algumas das obrigações do DPO:

- Receber reclamações e comunicações;
- Prestar esclarecimentos;
- Adotar providências;
- Orientar funcionários;
- Se reportar a Autoridade Nacional de Dados.

Conheça o nosso exclusivo serviço:

meudpo

DPO *as a service* CSC

PRESERVAÇÃO DA ATIVIDADE EMPRESARIAL:

A condução do processo de adequação da empresa à legislação não pode travar o negócio.

Apesar da complexidade, a elaboração e implementação do plano de estruturação jurídica da política de proteção de dados pessoais, bem como do plano de ações e do código de conduta, deverão se pautar em buscar incessantemente a adequação da empresa a LGPD/GDPR, sem se olvidar do propósito não menos importante de **garantir o desenvolvimento da atividade econômica.**

seusdados

BOAS PRÁTICAS E GOVERNANÇA

Recomenda-se:

1 - Implementar programa de governança em privacidade que, no mínimo:

a) Demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento da lei;

b) Seja aplicável a todo o conjunto de dados pessoais;

c) Seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) Tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

e) Conte com planos de resposta a incidentes e remediação;

f) Seja atualizado constantemente;

2 - Demonstrar a efetividade do programa de governança em privacidade quando apropriado e, em especial, a pedido da ANPD.

Seusdados

Independentemente de ter ou não ocorrido um evento de vazamento de dados, o tão só fato de não estar seguro e adequado aos termos da LGPD, poderá gerar a imposição de diversas penalidades dentre elas:

MULTA DE 2% DO FATURAMENTO

ATÉ R$50 MILHÕES.

Outras penalidades:

(i) Advertência;

(ii) Bloqueio do uso de dados pessoais;

(iii) Publicização do ato de insegurança, o que vai gerar grande perda de reputação da empresa

Seusdados

seusdados

Conheça o nosso exclusivo serviço:

meudpo

DPO *as a service* CSC

Representação e Parceria:

www.seusdados.com
+55 11 4587 2900