

Lei Geral de Proteção de Dados Pessoais

Rosana Muknicka

SCHMIDT, VALOIS, MIRANDA, FERREIRA & AGEL



MITOS E FATOS

LGPD

Lei 13.709/18

A lei vai
“pegar”?

Quem?

Todas as pessoas físicas e jurídicas? Nacionais e estrangeiras?.

Quando?

Já está em vigor? Entrará em vigor em fevereiro ou agosto de 2020? Posso aguardar até entrar em vigor?

Sanções

Se descumprir a norma, haverá alguma sanção?

O que fazer?

O que é relatório de impacto? Preciso contratar um encarregado?



QUAIS DADOS SÃO PROTEGIDOS?

Dados pessoais e dados sensíveis

Dados Pessoais:

qualquer informação **que identifique** ou **torne identificável** a pessoa natural, como seu nome, endereço, número de IP, localização, histórico escolar, entre outros.



QUAIS DADOS SÃO PROTEGIDOS?

Dados pessoais e dados sensíveis

Dados Sensíveis:

qualquer dado, on-line e/ou off-line, relacionado a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opiniões políticas, dados referentes a saúde ou vida sexual, dados genéticos/biométricos, além de informações sobre filiações a organizações por parte da pessoa natural.



GLOSSÁRIO

Tratamento - coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

Autoridade Nacional de Proteção de Dados: aplicar a LGPD, fiscalizar seu cumprimento e unificar a interpretação da lei.

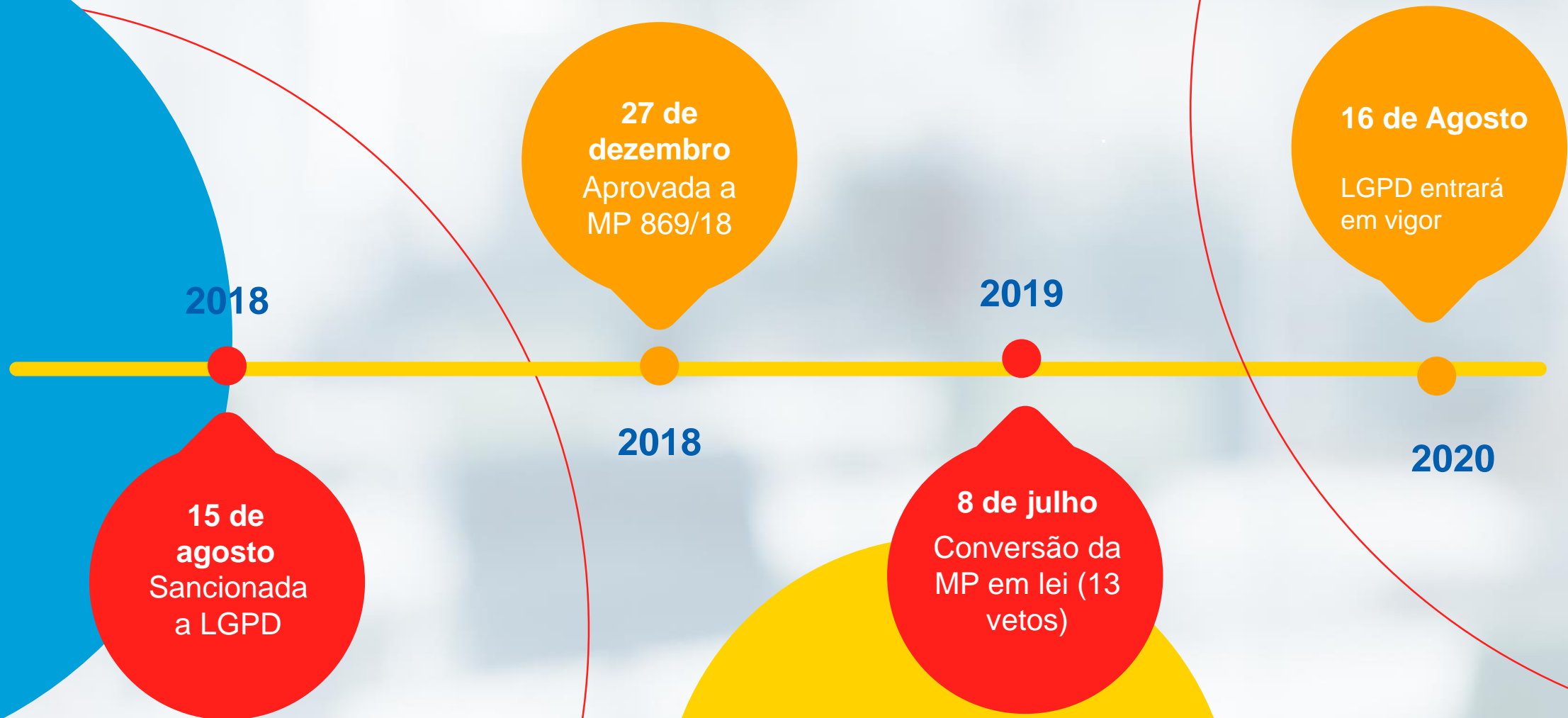
Encarregado

Dados digitais e físicos

Vazamento x violação



Quando?



A man and a woman in business attire are looking at a tablet together. The man is holding the tablet and pointing at the screen, while the woman looks on attentively. The background is a bright, modern office setting.

Quem?

Todas as **peçoas jurídicas de direito público e privado** serão afetadas pela nova lei.

Com relação à **peçoas natural**, esta somente não estará sujeita à LGPD se utilizar os dados pessoais para fins exclusivamente particulares e não econômicos.

EXCLUSÕES

Pessoa Natural

Pessoa Natural para fins exclusivamente **particulares** e **não econômicos**

Notícias e estudo

Fins exclusivamente **artísticos e jornalísticos** ou **acadêmicos**

Segurança

Fins exclusivos de **segurança pública, defesa nacional, segurança do Estado**, ou atividades de **investigação e repressão de infrações penais**

Internacional

Provenientes de fora do território nacional e que **não sejam objeto** de comunicação, uso compartilhado de dados 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 ao previsto nesta Lei

Quando haverá exclusão da aplicação da LGPD?

Fins Acadêmicos (GDPR)

A isenção somente se aplicará se o controlador do tratamento dos dados pessoais acreditar que a pesquisa ou estudo poderiam sofrer prejuízos caso houvesse a observância das limitações impostas pela LGPD, se o tratamento estiver sendo realizado com o propósito de publicação do material e este seja de interesse público, no qual há a necessidade de preservação da liberdade de expressão.



A world map is centered on the page, rendered in a bright yellow color. The background is a gradient of orange and yellow, with a large yellow sun in the top right corner. A thin red line curves across the map. The title 'EXTRATERRITORIALIDADE' is written in large, bold, white capital letters across the middle of the map.

EXTRATERRITORIALIDADE

A LGPD **deverá ser aplicada, inclusive, a empresas sediadas no exterior, caso o tratamento de dados pessoais ou dados sensíveis tenha sido realizado em território brasileiro.**

A lei também gerará impactos sobre as empresas que oferecem bens e/ou serviços no mercado brasileiro e que realizam o tratamento de dados de indivíduos localizados no Brasil.

Sanções



Advertência

Com prazo para adoção de medidas corretivas.



Multa

Multa simples de **até 2% do faturamento** da pessoa jurídica, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada a **R\$50 milhões por infração ou multa diária**.



Bloqueio

Bloqueio dos dados pessoais a que se refere a infração até a sua regularização



Remoção

Eliminação dos dados pessoais a que se refere a infração



Publicização

Publicização da infração.

PRINCÍPIOS APLICÁVEIS

NECESSIDADE
ou
MINIMIZAÇÃO

LIVRE
ACESSO

PREVENÇÃO
(Australian National
University junho/19)

FINALIDADE
propósitos legítimos,
específicos e explícit
os

QUALIDADE

NÃO
DISCRIMINAÇÃO

TRANSPARÊNCIA

SEGURANÇA
(Universidade de
Greenwich
£120.000,00
Maio/18)

ADEQUAÇÃO

PRESTAÇÃO
DE CONTAS

Vazamentos

Junho 2019

Graceland University, Oregon State University and Missouri Southern State University – hackers

USP, UDESC (Santa Catarina), UFG (Goiás) e IFSP (Guarulhos), UNESP, Faculdade Oswaldo Cruz

Março 2019

Oberlin College in Ohio, Grinnell College in Iowa and Hamilton College in New York – formulário inscrição

University of Washington – erro configuração – 1 milhão de pacientes

UCLA Health – acordo de US\$7,5 milhões por vazamento de dados



BASES LEGAIS



Direitos do Titular

Portabilidade dos Dados

Confirmação da existência dos dados

Direito de acesso, correção e “apagamento” dos dados

Anonimização dos Dados

Informação sobre o compartilhamento de dados com entidades

Informação sobre as consequências do não consentimento

Revogação do Consentimento

O que fazer?

FASES DE IMPLEMENTAÇÃO DA LGPD



Atividades preparatórias

identificação e entendimento sobre o negócio realizado pela empresa e formação de equipes multidisciplinares de compliance



Mapeamento

Dos dados pessoais tratados, políticas e códigos internamente adotados bem como dos contratos celebrados e das práticas preventivas de vazamento de dados



Adequação

Elaboração de novos documentos ou adequação dos já existentes à LGPD (e GDPR se cabível, assessoria na escolha do Encarregado (DPO)



Documentação

Elaboração do Relatório de impacto e do Plano de Crise



O que fazer?

Nomeação do Encarregado ou Data Protection Officer (“DPO”)

Armazenamento de dados, backup e cloud.

Revisão de **contratos** celebrados com terceiros

Verificação de **conveniência** na obtenção de **certificação dos sistemas de segurança**

Revisão dos procedimentos dos dados armazenados **fisicamente**

Criptografia dos documentos **confidenciais**

Elaboração de **Relatório de Impacto (“DPIA”)** e do **Plano de Crise**

O que fazer?



Adoção de Políticas internas

BYOD, home office, uso dos meios eletrônicos, wifi, e-mail, confidencialidade e ética.



Descarte Seguro de dados

Candidatos a vagas de emprego. Documentos relativos ao INSS. Demais documentos.



Realização de Treinamentos

Engajamento dos empregados. Questão dos “Millenials”. Utilização de redes sociais



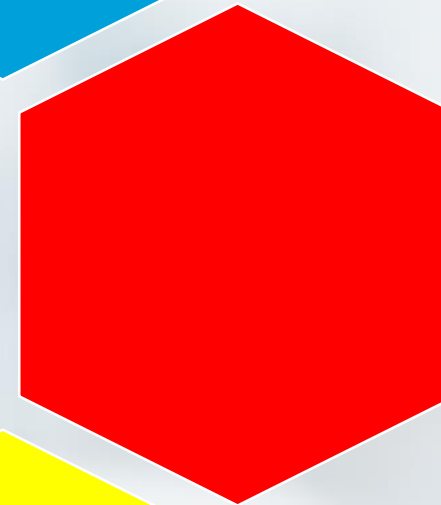
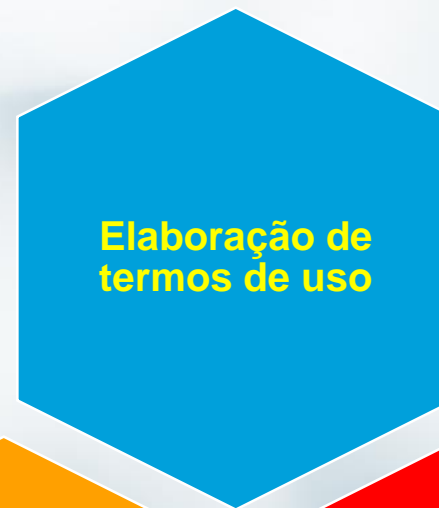
Compartilhamento de dados pessoais

Transferência para órgãos públicos e privados. Transferências internacionais. Terceirização de serviços.



O que fazer?

Campanhas de conscientização interna sobre o uso dos dados



Revisão das campanhas para o público



Redes Sociais, website e aplicativos



Consentimento dos titulares



Verificação de acesso por crianças e adolescentes



Relatório de Impacto

✓ Recomenda-se a elaboração do **Relatório de Impacto**, um documento que poderá ser exigido pela autoridade nacional e será útil em eventual operação de fusão ou aquisição da empresa ("M&A").

✓ Este relatório deverá conter, no mínimo:

A descrição dos tipos de dados coletados;

A metodologia utilizada para a coleta e para a garantia da segurança das informações e

A análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

PLANO DE CRISE



A descrição da natureza dos dados pessoais afetados



As informações sobre os titulares envolvidos



Quais as medidas técnicas e de segurança que foram utilizadas



Riscos relacionados ao incidente e as medidas que foram ou que serão adotadas.



Motivos da demora, no caso da comunicação não ter sido imediata