Gartner Security & Risk Management Summit

Privacy Program: LGPD Requires You to Have One

Ricardo M Machado
Executive Partner – Director – Executive Programs

Gartner®

LGPD

"Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de *proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.*"

Lei Nº 13.709/18.

Gartner®

Lei Geral de Proteção de Dados – 13.709/18

Sanções: **2% do faturamento da empresa** limitado em até **50 milhões de reais** por infração.... Entre outros prejuízos.

Escopo de Aplicação – Art. 1°
Qualquer atividade que envolva utilização de dados pessoais.

Autorização para o tratamento de dados – Art. 7°
Consentimento será uma das formas de legitimar o tratamento de dados pessoais.

Princípios de proteção de dados – Art. 6°
10 princípios da proteção de dados inclui demonstrar medidas adotadas para cumprir a lei (prestação de contas)

Direitos dos titulares de dados - art. 17 a 22
Titulares dos dados terão amplos direitos: informação, acesso, retificação, cancelamento, oposição, portabilidade, entre outros.

Notificações obrigatórias – Art. 48
Em caso de incidentes segurança envolvendo os dados.

Aplicação extraterritorial – Art. 3°
Aplica-se também a empresas que não possuem estabelecimento no Brasil.

Dados: Sensíveis, de menores e transferência internacional – Art. 11, 14 e 33
Regras específicas para tratar dados sensíveis, transferência internacional de dados e utilizar dados de crianças e adolescentes.

Verificação (assessment) sobre o tratamento de dados -- Art. 38
Avaliação de impacto à proteção de dados (DPIA – GDPR)

Mapeamento do tratamento de dados -- Art. 37
Atividades de tratamento de dados devem ser registrados em relatório.

Encarregado – DPO Data Protection Officer -- Art. 41
Toda empresa responsável pelo tratamento de dados deverá nomear um Encarregado da proteção de dados pessoais.

Autoridade – Vetado.
Previsão de Autoridade Nacional de proteção de Dados. Responsável por garantir o cumprimento da Lei .

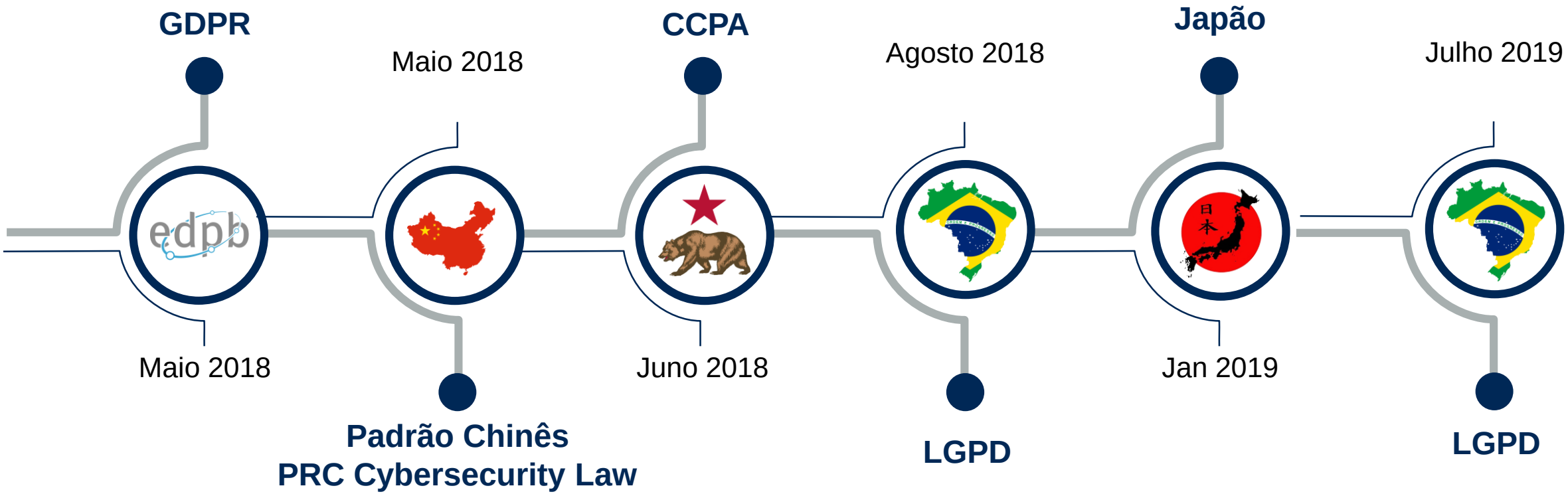
http://www.portaldaprivacidade.com.br/2018/07/17/redacao-final-do-projeto-de-lei-da-camara-no-53-de-2018-no-Origem: 4-060-de-2012-na-casa-de-origem/

Lei Geral de Proteção de Dados – 13.709/18

Gartner®

E nos últimos 12 meses

Com a introdução de novas leis de privacidade quase mensalmente, as organizações estão lutando para entender como elas são afetadas e, em caso afirmativo, o que elas podem fazer para se adaptar e continuar a fazer negócios globalmente.



Gartner

Por que a privacidade é importante para os negócios?

Gartner®

Os consumidores estão muito preocupados com a privacidade e a segurança no que se refere à tecnologia pessoal.

Gartner Survey: **Personal Technology Study December 11,2018**

No total, 12.081 foram entrevistados em idioma nativo nos EUA (25%); As porcentagens do Reino Unido (25%), Alemanha (25%) e China (25%) podem não somar em 100% devido a arredondamentos. Interpretar pequenos tamanhos de base (n <30) com cautela.

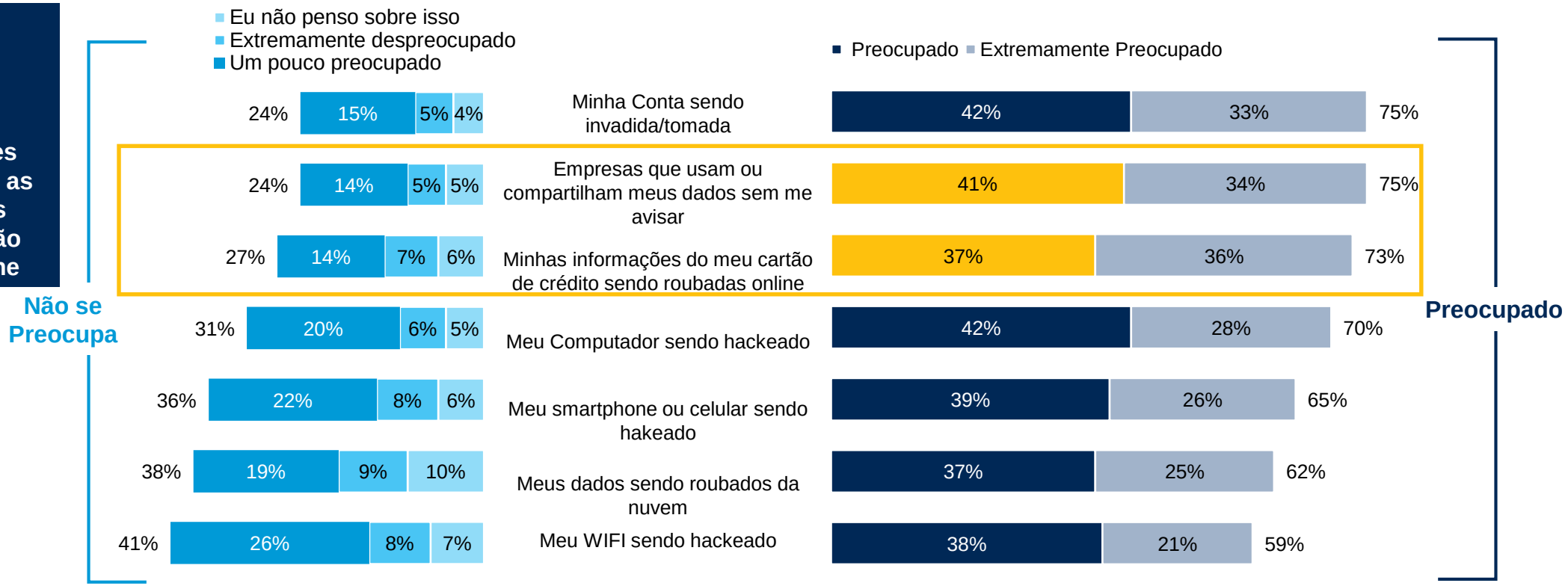
Gartner®

Percepção de segurança e principais preocupações

Percepções de segurança e principais preocupações
Porcentagem de entrevistados

6

Como os consumidores acreditam que as informações pessoais estão seguras online



Base: All respondents, n = 12,081
Q. On a scale from 1 to 10, indicate how secure you think your personal information is online, with 10 being completely secure, and 1 being completely vulnerable?
Q. How concerned are you about each of the following?

Gartner

Ações de Instituições na Preservação da Privacidade

MP DFT
Ministério Público do Distrito Federal e Territórios

Vivo é investigada por fornecer publicidade com dados pessoais de clientes

Mais uma empresa é investigada pelo possível uso e tratamento ilegal de dados pessoais de clientes. O Ministério Público do Distrito Federal e Territórios (MPDFT) instaurou inquérito civil público, nesta segunda-feira, 2 de abril, para apurar como a operadora Vivo tem utilizado as informações de cerca de 73 milhões de usuários para fins de publicidade. O serviço é oferecido aos anunciantes por meio do Vivo Ads, plataforma de marketing mobile da companhia.

A empresa promete fornecer publicidade usando dados qualificados dos clientes, como perfil, localização, comportamento de navegação, lugares frequentados e hábitos dos consumidores. A Vivo anuncia como vantagem que os espaços publicitários serão ocupados com propagandas e conteúdos segmentados. Para os anunciantes, é uma ótima opção de direcionamento de conteúdo para potenciais clientes.

Com o uso de dados pessoais, é possível identificar entre os clientes aqueles que estão passando por tratamento de saúde, a partir do mapeamento da circulação de usuários em clínicas e hospitais. Essas informações podem estar sendo usadas de maneira imprópria pela empresa para a venda de espaço publicitário. Vale destacar que o serviço Vivo Ads não permite que os clientes se oponham ao tratamento de seus dados pessoais para fins de publicidade.

Gartner

Ações de Instituições na Preservação da Privacidade

Idec notifica Dataprev por licitação para uso de reconhecimento facial – 30/Ago/2019

Instituto pede a suspensão imediata da licitação para aquisição de tecnologia de reconhecimento facial e impressão digital enquanto casos de vazamento de dados de beneficiários não forem solucionados

Para o Idec, o grave vazamento que ocorre há anos com as informações dos aposentados e pensionistas, usados para o cometimento de fraudes e assédio insistente para a oferta de crédito consignado, deixa explícita a vulnerabilidade da segurança das informações sob responsabilidade da Dataprev.

"Não é razoável que se implemente uma tecnologia que utilize dados sensíveis sem que o cidadão tenha segurança de que esses dados serão tratados de forma segura e não serão vazados para empresas que possuem práticas abusivas ou mesmo ilegais. É uma questão de responsabilidade com os dados dos consumidores que, tudo indica, está sendo desprezada", alerta Diogo Moyses, coordenador do programa de Telecomunicações e Direitos Digitais do Idec.

Ações de Instituições na Preservação da Privacidade

Congresso derruba vetos na LGPD

O Congresso Nacional derrubou em sessão realizada nesta terça-feira, 24/Set/2019, os vetos do governo às sanções administrativas aplicadas aos agentes de tratamento de dados pessoais que infringirem as regras previstas na lei 13.709 de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Trata-se do veto a respeito do direito do titular dos dados pessoais de pedir revisão por pessoa natural das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais no caso se sentir afetado ou prejudicado por tais decisões.

Os incisos X, XI e XII do art. 52 da LGPD preveem sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados aos agentes de tratamento de dados que vão desde suspensão parcial do funcionamento do banco de dados por até seis meses, com possibilidade de prorrogação por igual período, até a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados no País.

Itaú, Quod e 99 são notificadas por Idec sobre uso de reconhecimento facial

Isabel Butcher | 3/06/19 19:49

Itaú, Quod e 99 foram notificadas pelo Instituto Brasileiro de Defesa do Consumidor (Idec) por não deixarem claras a seus clientes as regras de uso, consentimento e tratamento dos dados coletados por meio de reconhecimento facial. As três empresas informaram que vão começar a utilizar a tecnologia, mas, para o instituto, é preciso mais esclarecimentos para a segurança dos consumidores. O Idec reforça que o problema não está na tecnologia de reconhecimento facial em si, mas na falta de transparência das informações para o cliente.

US fines Facebook $5 billion for privacy violations

The US Federal Trade Commission has said it would also place new oversight and restrictions on Facebook. It is the largest fine that the FTC has ever imposed on a technology company.

© picture-alliance/AP Photo/R. Drew

Procon-SP notifica empresas para apurar possível violação de privacidade por aplicativo que envelhece fotos

Fundação de defesa do consumidor teme que o aplicativo FaceApp utilize as imagens dos usuários, o que seria indevido. Facebook diz que não foi formalmente notificado por distribuir o app. Google e Apple não responderam.

Por Léo Arcoverde, GloboNews

18/07/2019 18h49 · Atualizado há uma semana

Lei que cria Autoridade Nacional de Proteção de Dados é sancionada com vetos

Da Redação | 09/07/2019, 12h39


A MP foi aprovada em maio pelo Senado

Jefferson Rudy/Agência Senado

Gartner®

Oportunidade

Se você perde a **confiança** dos seus clientes, você quebra o seu negócio!

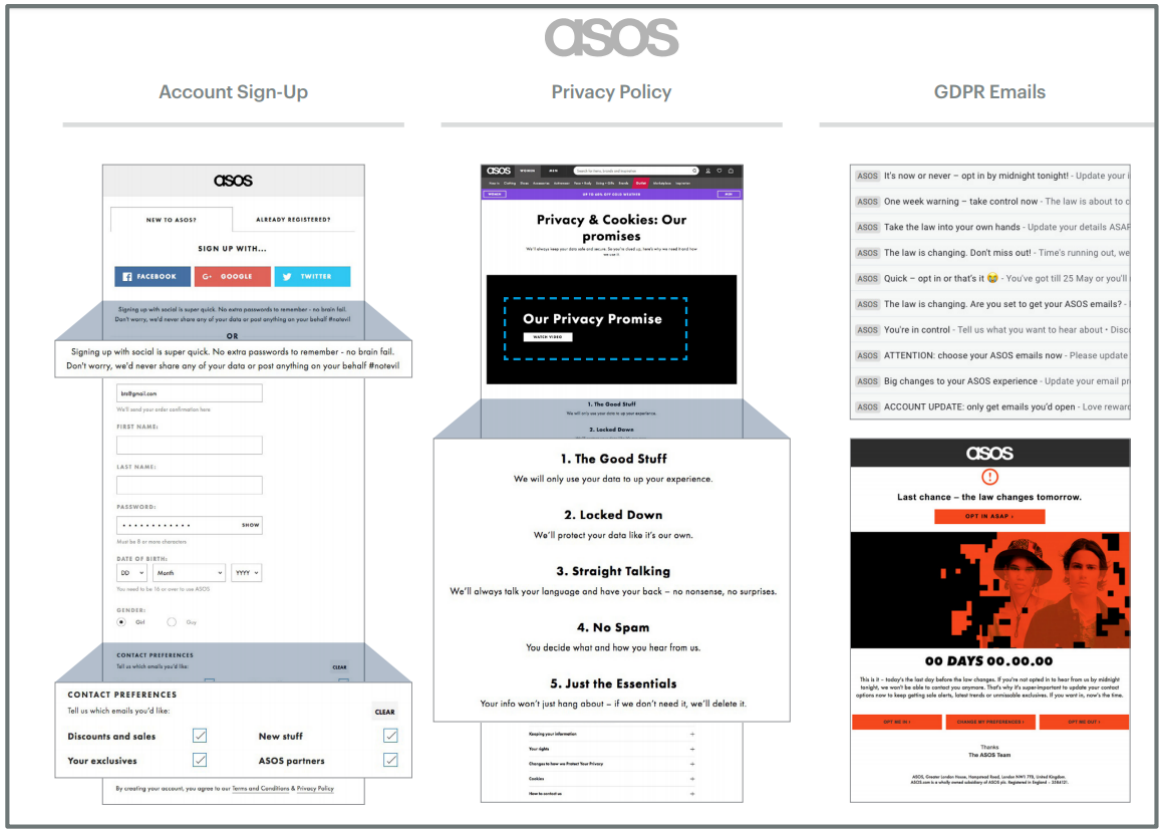
Confiança deve ser a fundação do seu negócio.

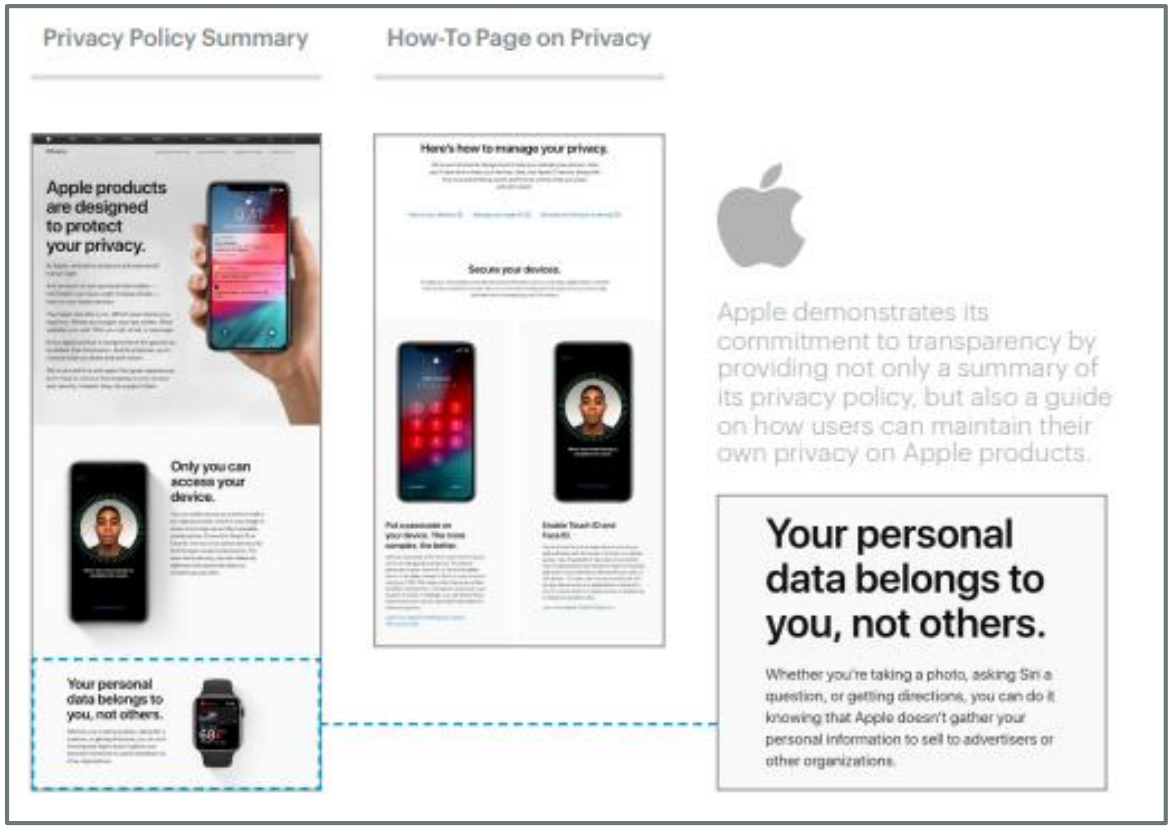
Privacidade:
Políticas e processos que governam a coleta, processamento, compartilhamento e eliminação de dados pessoais em conformidade com leis de proteção e regulamentações.

Segurança:
Políticas administrativas, técnicas e físicas, processos e controles que protegem a informação em conformidade com padrões, leis e regulamentações.

Gartner®

Exemplo de Marcas que constroem confiança





Gartner®

Criando um programa de gestão de privacidade

Gartner®

10 Princípios para Tratamento de Dados Pessoais

Finalidade
Propósitos Legítimos, Específicos, Explícitos e Informados

Adequação
Compatível com as Finalidades

Necessidade
Utilização (apenas) de Dados Estritamente Necessários

Livre Acesso
Acesso ao Tratamento e à Integridade dos Dados

Qualidade dos Dados
Dados Exatos, Claros, Relevantes e Atualizados

Transparência
Informações Claras e Precisas aos Titulares dos Dados

Segurança
Medidas Técnicas e Administrativas aptas a Proteger os Dados Pessoais

Prevenção
Adoção de Medidas para evitar danos aos titulares dos dados

Não discriminação
Não utilização para fins discriminatórios, ilícitos ou abusivos

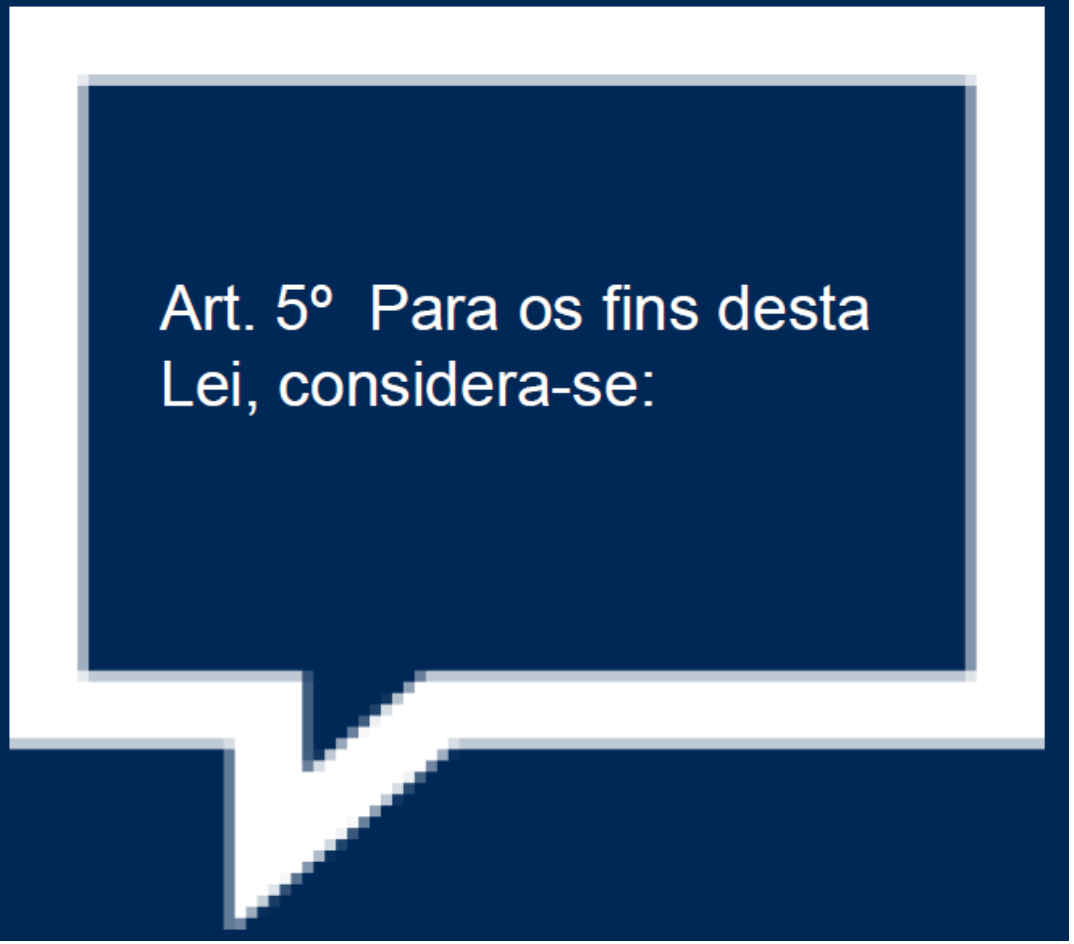
Responsabilidade e Prestação de Contas
Demonstração de adoção de medidas eficazes ao cumprimento das normas

Fonte extra-Gartner:http://www.portaldaprivacidade.com.br/2018/07/19/infografico-04-os-10-principios-para-o-tratamento-de-dados-pessoais

Gartner

Quem são os atores envolvidos

- **O titular:** é a pessoa física a quem se referem os dados pessoais.
- **O controlador:** é a empresa ou pessoa física que coleta dados pessoais e toma todas as decisões em relação a forma e finalidade do tratamento dos dados. O controlador é responsável por como os dados são coletados, para que estão sendo utilizados e por quanto tempo serão armazenados.
- **O operador:** é a empresa ou pessoa física que realiza o tratamento e processamento de dados pessoais sob as ordens do controlador.
- **O encarregado:** é a pessoa física indicada pelo controlador e que atua como canal de comunicação entre as partes (controlador, os titulares e a autoridade nacional), além de orientar os funcionários do controlador sobre práticas de tratamento de dados.



Data Protection Officer (DPO) - Atividades

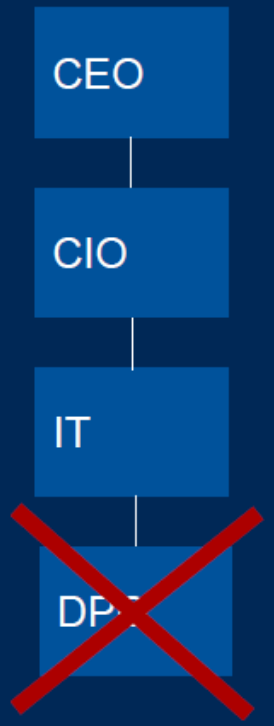
- Receber e responder às solicitações de assunto de dados
- Interagir com a autoridade nacional de proteção de dados
- Fornecer orientação para funcionários e contratados sobre práticas de proteção de dados
- Coordenar orientação geral das políticas e práticas de privacidade e garantir a adesão à elas
- Realizar treinamento relacionado à privacidade em toda a empresa
- Conduzir a resposta da empresa a emergências relacionadas à privacidade e outros eventos potencialmente prejudiciais
- Trabalhar com partes interessadas de terceiros (incluindo parceiros de negócios, fornecedores, provedores de serviços e fornecedores de produtos de TI) para garantir que eles entendam claramente e cumpram os requisitos básicos de privacidade da empresa

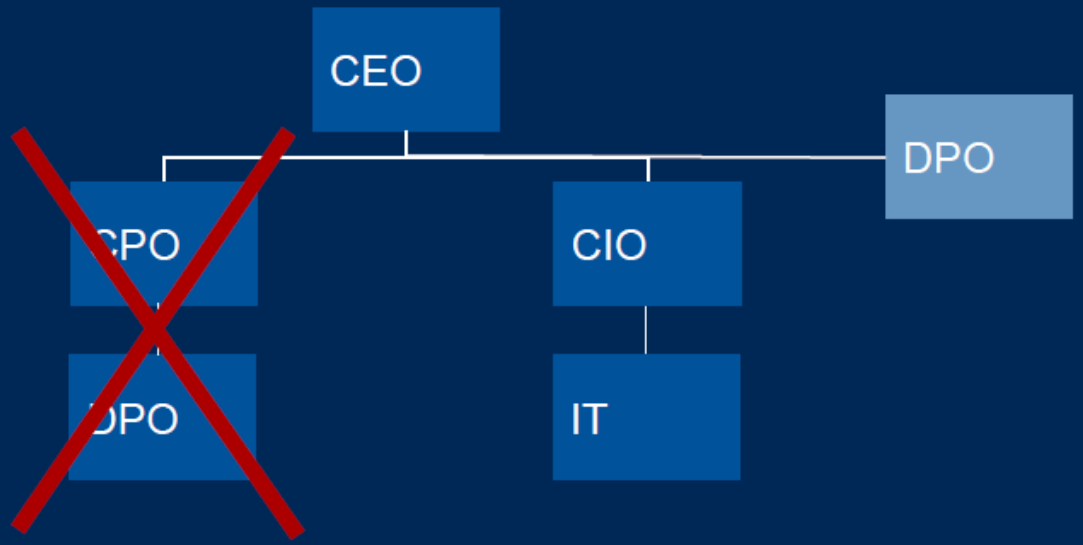
Gartner®

Um único ponto de contato: O Encarregado (DPO)

Características:

- Reporta diretamente ao CEO ou conselho diretor ou similar
- Deve ter autonomia e estabilidade
- Independência de orçamento
- Obrigatório para todas as empresas que atuam como controladores





Caminho de maturidade sobre privacidade

Descoberta de dados pessoais mantidos pela organização

Mapeamento e visualização (ciclo de vida dos dados)

Conexão com **base legal**, incluindo gerenciamento de consentimento

Data loss prevention, **classificação** (incluindo rotulagem ou marcação de metadados)

Autorização e gestão de acesso

Demonstração de uso **(Linhagem de dados)**

Retenção e controle diário (incluindo offline)

Pseudo-anonimização onde possível, e **atomização** onde necessário

Gestão de risco regular e demonstração de conformidade

"A evolução de **criptografia"** **versus** "risco de **reidentificação"**

Desenvolvendo Capacidades de Gerenciamento de Privacidade

ESTABELECER

Os recursos fundamentais necessários para avaliar a maturidade e impulsionar um programa de gerenciamento de privacidade eficaz e sustentável

MANTER

Recursos focados em administração contínua, gerenciamento de recursos e escalabilidade de tarefas recorrentes. Isso permite que as organizações alinhem a prática de privacidade com as metas de negócios.

EVOLUIR

Capacidades especializadas focadas na redução do risco de privacidade com pouco ou nenhum impacto na utilidade da organização.

Gartner®

Programa de Privacidade Orientado por Tecnologia

ESTABELECER

- Descoberta
- Classificação
- Avaliação de Risco & acompanhamento
- Manutenção de registro (RoPA)
- Minimização do dado
- Notificação e política
- Gestão de Consentimento e preferencias(Consent and Preference Management (CPM))
- Gestão de cookies
- Gestão do direito do titular

Experiência do Usuário/Privacidade

MANTER

- Métricas & Reporting
- Mapeamento do dado e ciclo de vida
- Automação de PIA (Privacy Impact Assessment)
- Ampliação de resposta a incidentes
- Centro de Privacidade(Portal self-service)

EVOLUIR

- Anonimização e Pseudo-anonimização
- Ferramentas analíticas e inteligencia de negócios (ABI)
- Controle de dados fim-a-fim

Gartner®

Experiência do Usuário

UX

A experiência do usuário é um termo que engloba toda a gama de funções centradas no manuseio das informações pessoais de um indivíduo ao interagir com uma organização. Estas tendem a ser as áreas em que as organizações investem **primeiro** à medida que são expostas ao mundo.

Notificação & Política

Gestão de consentimento e Preferência

Gestão de Cookies

Gestão do direito do Titular

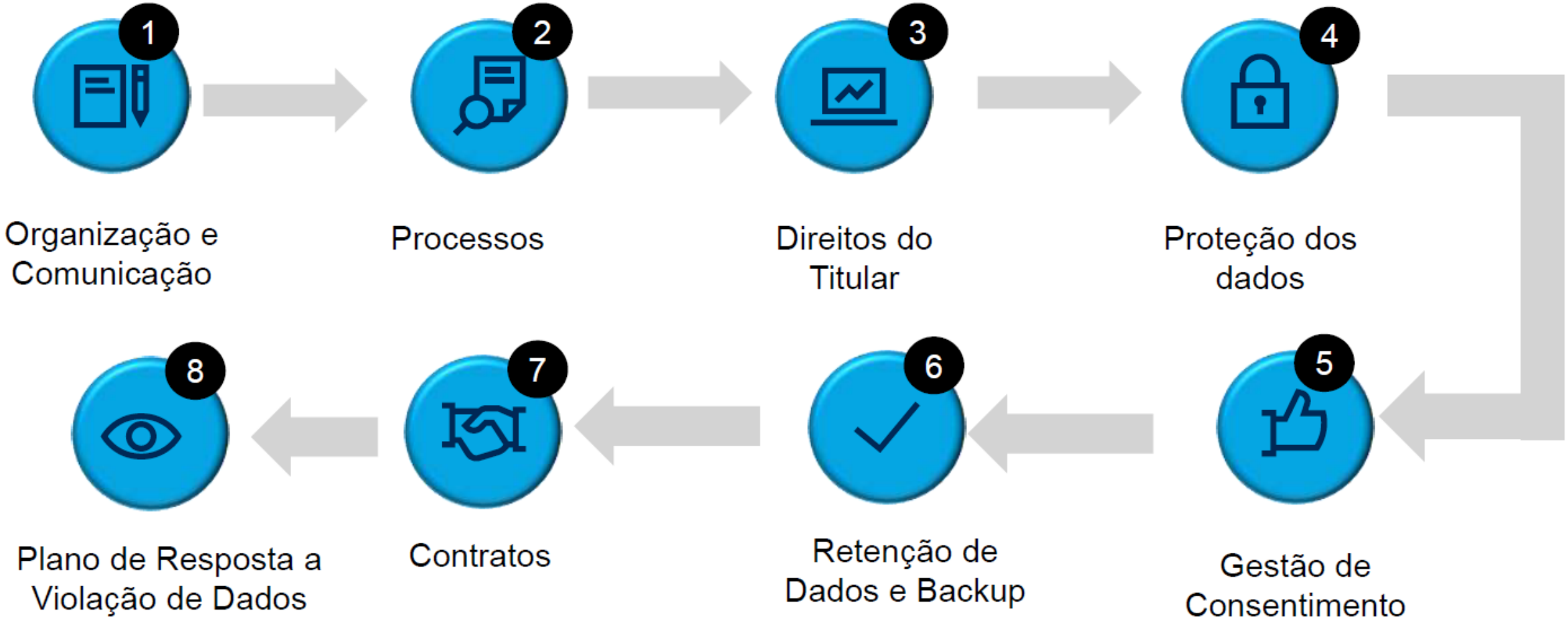
Gartner

Informe o titular do dado:

- Atualize os avisos de privacidade e os formulários de consentimento, conforme necessário, com as seguintes informações:
- Defina finalidade específica do processamento, incluindo se o processamento é uma condição para receber produtos ou serviços.
- Informe a forma e a duração do processamento.
- Identifique o controlador de dados, incluindo detalhes de contato.
- Informe se terceiros receberão os dados pessoais e por quais motivos e as responsabilidades de terceiros que processam dados em nome do controlador.
- Demonstre como os titulares de dados podem exercer seus direitos.

Gartner®

Nada melhor que um plano a ser seguido ...



Gartner

Organização e Comunicação

- Nomear o Oficial de Proteção de Dados (DPO)
- Apontar e documentar proprietários do processo de negócios;
- Identificar contatos em consultoria jurídica, RH e outros grupos de partes interessadas
- Identificar as funções da própria organização e dos parceiros: Controladores de Dados / Processadores de dados
- Comunicar a campanha a todos os grupos de partes interessadas relevantes
- Criar novo aviso de privacidade e publicar (externamente)
- Criar uma nova Política de Privacidade e publique (internamente)

Gartner®

Processos

- Criar um inventário de todos os processos de negócios que envolvem dados pessoalmente indentificáveis
- Identificar quais dados pessoais são processados em qual processo de negócio
- Motivar processos de dados pessoais (“propósito de processamento”) para cada processo de negócio
- Determinar e documentar fundamentos legais para processamento
- Identificar os processadores de dados envolvidos nos processos de negócios
- Identificar por quais meios os dados são processados para cada processo
- Identificar qualquer subprocesso onde aplicável
- Alterar os processos de negócios existentes para garantir a minimização dos dados

- Remover quaisquer dados pessoais que não atendam aos critérios de finalidade de processamento (incluindo backups)
- Registrar as assinaturas dos proprietários dos processos de negócios, indicando que seu processo é totalmente compatível
- Criar ou alterar o processo de avaliação de impacto da privacidade
- Criar ou alterar o processo de avaliação de ricos
- Implementar a repetição periódica e orientada ao gerenciamento de mudanças / projeto de varreduras rápidas da PIA
- Implementar a repetição periódica e controlada por gerenciamento de mudança / projeto de varreduras rápidas da DPIA

Gartner®

Direitos do Titular

- Criar processo para tratar o direito de acesso por pessoa de dados
- Criar processo para tratar o direito de retificação
- Criar processo para tratar o direito de apagar
- Crie um processo para tratar direito a restrição do processo
- Criar processo para tratar a notificação
- Criar processo para tratar o direito à portabilidade de dados
- Crie processo para tratar direito para objetar
- Criar processo para tratar o direito de não estar sujeito a uma decisão baseada em perfis, etc.
- OPCIONAL: Criar portal de autoatendimento onde os sujeitos de dados podem executar ações para executar seus direitos
- Garantir que os detalhes de contato do DPO estejam disponíveis para todos os assuntos de dados

Gartner®

Proteção de Dados

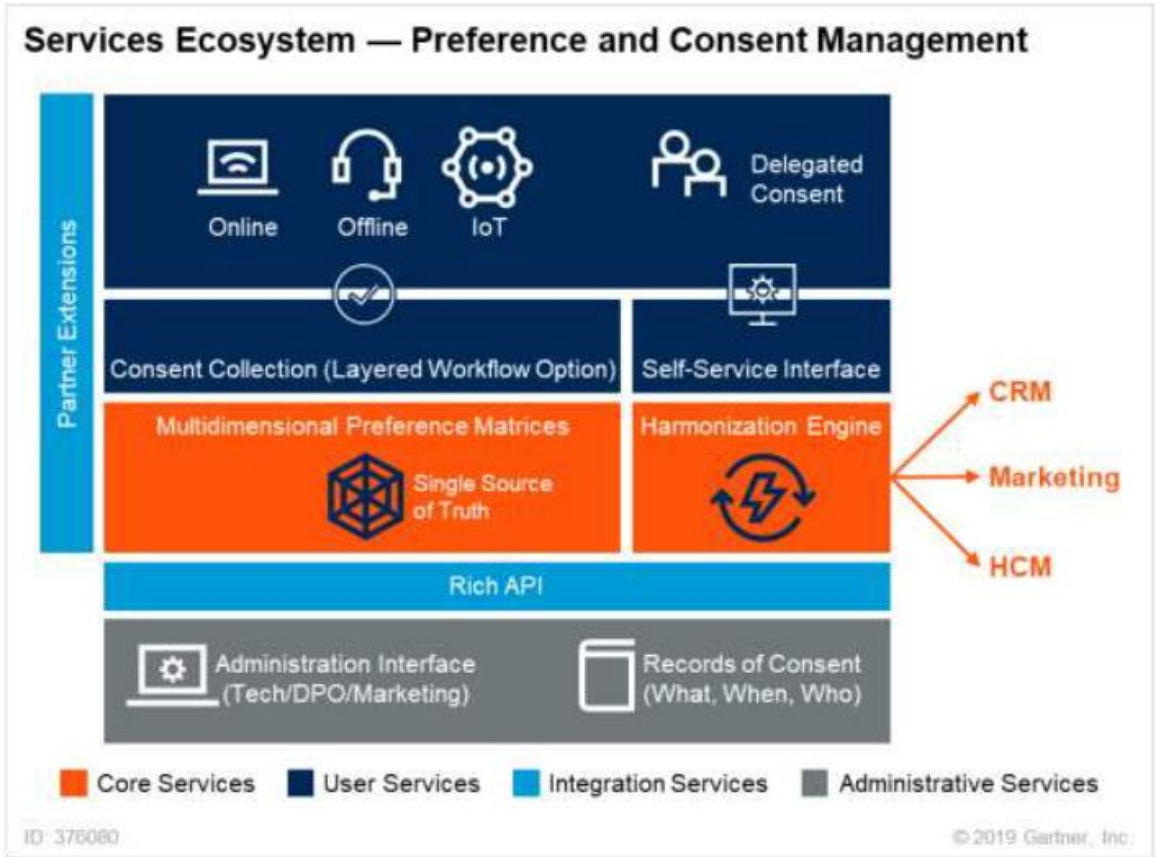
- Rever o armazenamento atual de dados pessoais
- Realizar uma avaliação de risco quando apropriado
- Identificar medidas técnicas e organizacionais adequadas para proteger dados pessoais
- Implementar medidas técnicas e organizacionais adequadas para proteger dados pessoais
- Revisar a solução MDM atual para verificar se fornece medidas adequadas para proteger dados pessoais

Gartner®

Gestão de Consentimentos

5

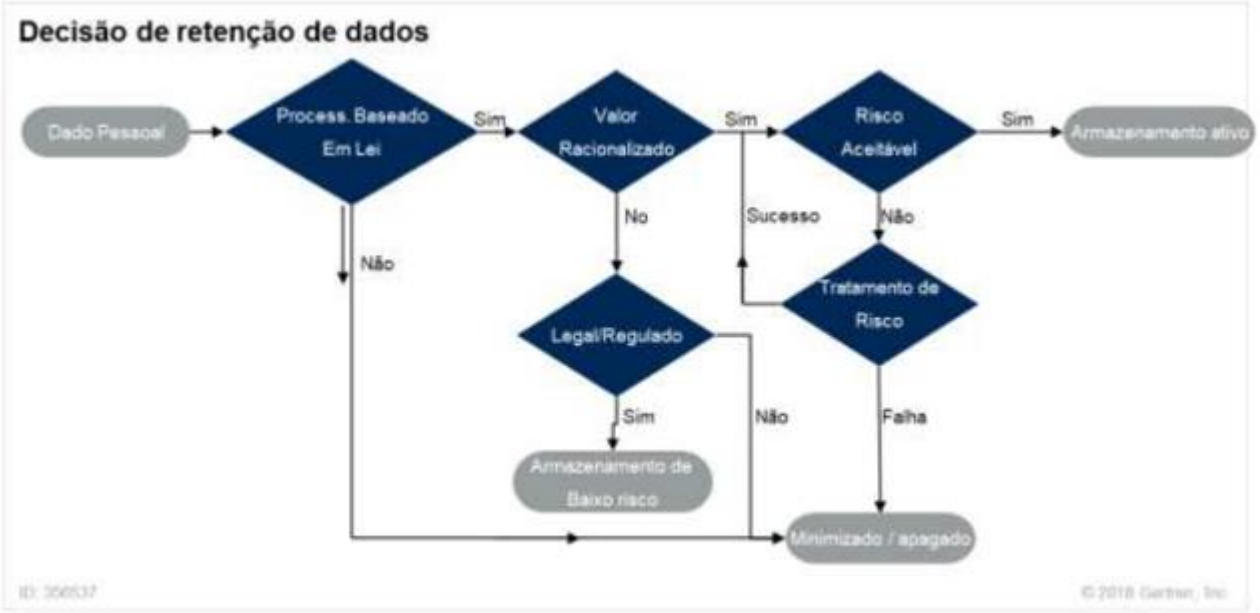
- Identificar todos os pontos de contato em que o consentimento do assunto dos dados é obtido
- Identificar processos para os quais é necessário o consentimento
- Identificar controladores de dados e processadores envolvidos com dados para os quais é necessário o consentimento
- Revisar o gerenciamento de consentimento existente no site e altere para LGPD
- Revisar a gestão de consentimento existente em formulários em papel e altere para LGPD
- Desenvolver o processo para obter o consentimento dos pais, caso os dados sobre menores sejam coletados
- Criar repositório para gerenciamento de consentimento para garantir que o ônus da prova possa ser facilitado



Gartner

Retenção de Dados e Backup

- Revisar os requisitos de retenção de dados existentes
- Revisar os processos de backup existentes
- Alterar as políticas de retenção de dados e os processos de backup
- Remover todos os dados pessoais em backups existentes



Gartner®

Revisão de Contratos

- Criar acordos controlador-processador onde ainda não estejam em vigor
- Atualizar os acordos do controlador-processador (uso intencional e requisitos de segurança)
- Atualizar outros acordos existentes, quando aplicárvel
- Atualizar o processo de aquisição (critérios de seleção para novos serviços)
- Atualizar o processo de aquisição (novos requisitos incluídos em novos contratos)

Gartner®

Resposta a Incidentes/Violação de dados

8

- Identificar detalhes de contato da Autoridade Nacional de Proteção de Dados (DPA)
- Identificar representante da UE para lidar com a notificação de violação (apenas para organizações não pertencentes à UE)
- Desenvolver playbook para o cenário de violação de dados, realizar exercício de mesa (*tabletop exercise*) para prep. treinamento (repita periodicamente)
- Desenvolver processo de gerenciamento de violações para permitir a notificação dentro de 72 horas
- Processo de gerenciamento de violações de teste (anualmente)

Gartner

Recommended Gartner Research

- **Beyond GDPR: 5 Best Practices for LGPD Compliance**
  Claudio Neiva and Bart Willemsen (G00381480)
- **The State of Privacy and Personal Data Protection, 2019-2020**
  Nader Henein and Bart Willemsen (G00376084)
- **Practical Privacy — Executing Subject Rights Requests**
  Nader Henein (G00356536)
- **Practical Privacy — Managing Data Retention and Backups**
  Nader Henein (G00356537)
- **The Four Do's and Don'ts of Implementing Your Privacy Program**
  Bart Willemsen and Prateek Bhajanka (G00319945)
- **Use These Privacy Deliverables in Every IT Development Project**
  Bart Willemsen (G00342056)
- **Toolkt: Assess Your Personal Data Processing Activities**
  Bart Willemsen and Prateek Bhajanka (G00319945)

For information, please contact your Gartner representative.

Gartner®

Obrigado!

Gartner®

LGPD – Bases Legais – Tratamento dos Dados Pessoais

1.mediante consentimento;
2.para cumprimento de obrigação legal ou regulatória pelo controlador;
3.pela administração pública, para tratamento de dados necessários a políticas públicas;
4.para realização de estudos por órgão de pesquisa, sendo garantida a anonimização dos dados;
5.quando necessário para a execução de contrato;
6.exercício regular de direitos em processo judicial, administrativo ou arbitral;
7.para a proteção da vida ou incolumidade física do titular ou terceiros;
8.para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
9.interesses legítimos do controlador ou de terceiro;
10.proteção do crédito.

Lei Nº 13.709 , de 14 de Agosto de 2018.