KPMG

CAFÉ COM O CONTABILISTA - "A LGPD foi aprovada! E agora?"

Setembro de 2020

Agenda

01 **2 anos após a GDPR: como estamos?**

02 **LGPD em vigor: Como ficamos?**

03 **LGPD: 2 anos de projetos**

04 **E como podemos seguir?**

01

2 anos após a GDPR: como estamos?

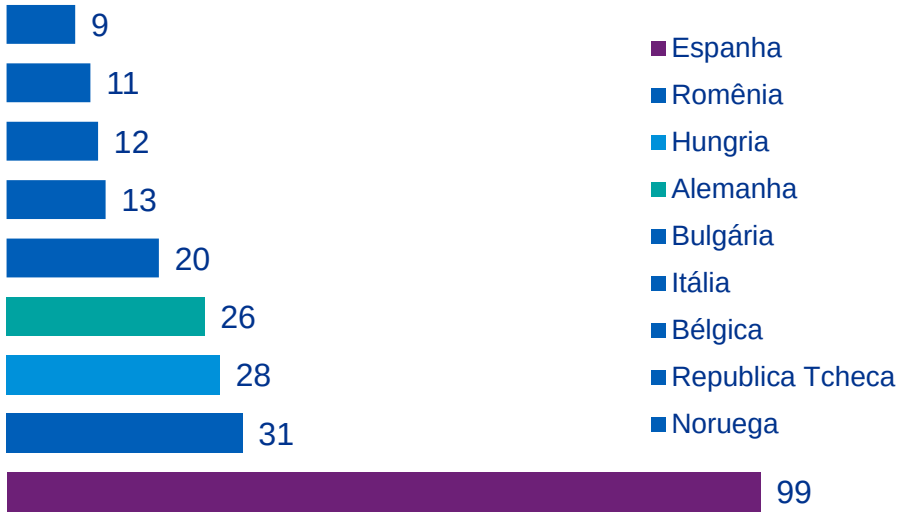
Algumas multas da GDPR

Multas mês a mês

Mês	Valor das multas	# de multas
2018		
Jul–2018	€ 400,000	1
Set-2018	€ 300	1
Out-2018	€ 388	1
Nov-2018	€ 20,000	1
Dez-2018	€ 15,700	5
2019		
Jan-2019	€ 50,000,888	3
Fev-2019	€ 65,108	12
Mar-2019	€ 462,004	8
Abr-2019	€ 312,135	7
Mai-2019	€ 557,240	6
Jun-2019	€ 1,076,000	6
Jul-2019	€ 315,349,200	7

Mês	Valor das multas	# de multas
2019		
Ago-2019	€ 3,246,630	6
Set-2019	€ 906,523	9
Out-2019	€ 34,409,514	27
Nov-2019	€ 1,114,800	20
Dez-2019	€ 21,757,530	23
2020		
Jan-2020	€ 28.116.160	16
Fev-2020	€ 886.090	29
Mar-2020	€ 7.873.600	36
Abr-2020	€ 802.200	7
Mai-2020	€ 766.400	12
Jun-2020	€ 2.042.140	29

Relação das Multas por países



País	# Multas	Média das Multas (em €)	Valor Multas (em €)
Espanha	99	28,646	2.835.910
Romênia	31	16,698	517.650
Hungria	28	18,471	517.197
Alemanha	26	1,014,536	26.377.925
Bulgária	20	160,535	3.210.690
Itália	13	3,035,308	39.459.000
Bélgica	12	13,000	156.000

Algumas multas da GDPR

Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação			Base legal inadequada para o processamento de dados				Cumprimento insuficiente dos direitos dos titulares de dados
British Airways (Reino Unido)	***Marriott International Inc (Reino Unido)***	***Telecoms provider (1&1 Telecom GmbH) (Alemanha)***	***Google Inc (França)***	***TIM (Itália)***	***Austrian Post (Austria)***	***Eni Gas e Luce (Itália)***	***Google Inc (SU)***
€204.600.000	***€110.390.200***	***€9.550.000***	***€50.000.0000***	***€27.800.000***	***€18.000.000***	***€18.500.000***	***€57.000.000***
08/jul/19	***09/jul/19***	***09/dez/19***	***21/jan/19***	***15/jan/20***	***23/out/19***	***11/dez/19***	***11/mar/20***

Algumas multas aplicadas na GDPR

Eslováquia

01 Multa

€ 40.000,00
Slovak Telekom

Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação.

Alemanha

01 Multa

€ 9.500.000,00
1&1 Telecom
Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação.

Romênia

01 Multa

€ 2.000,00
Telekom Romania Mobile

Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação.

Grécia

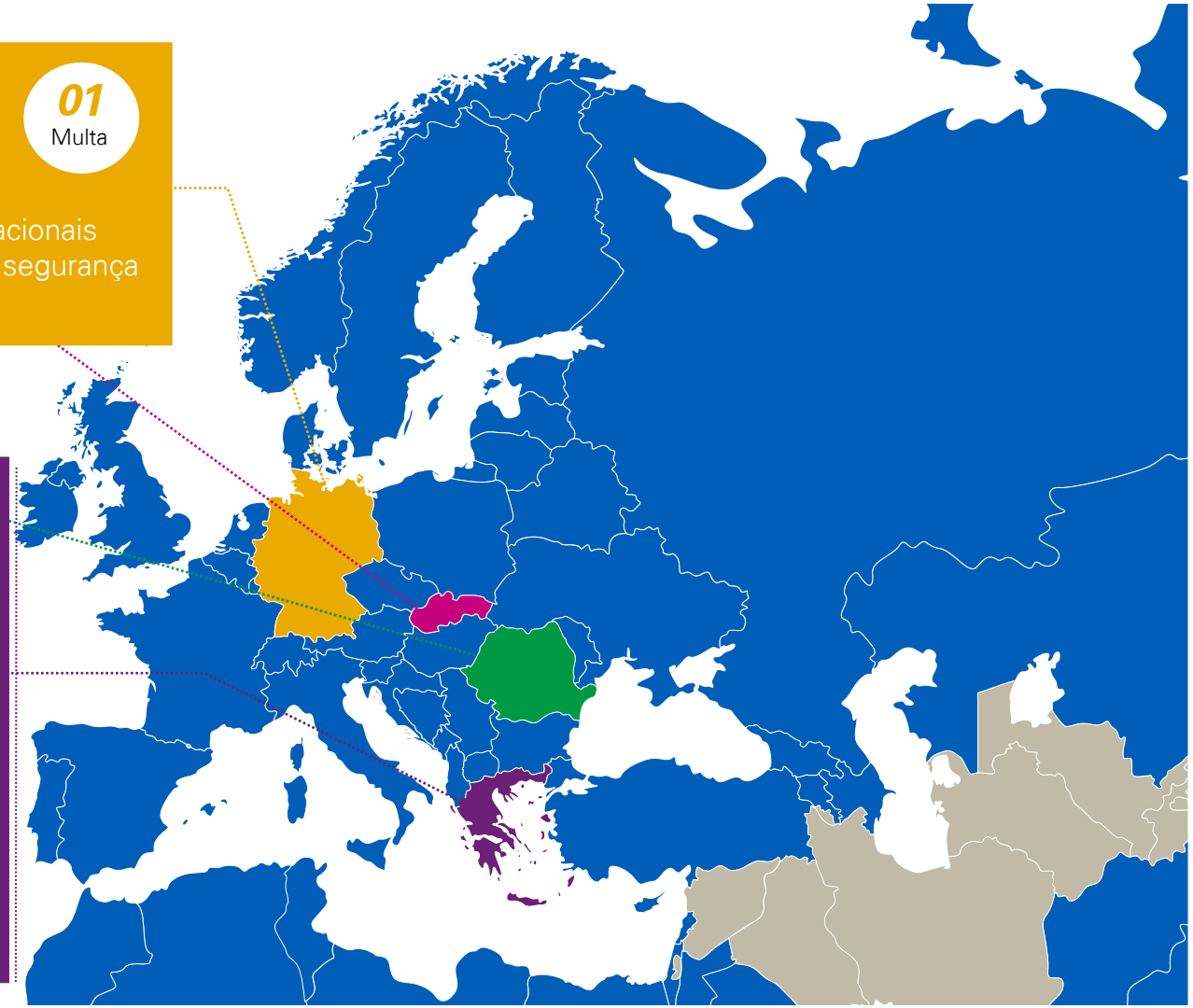
02 Multas

€ 200.000,00
Hellenic Telecommunications

Não conformidade com os princípios gerais de tratamento de dados.

€ 20.000,00
Wind Hellas Telecommunications

Não conformidade com os princípios gerais de tratamento de dados.



Algumas multas aplicadas na GDPR

Espanha

12
Multas

€ 60.000,00 - *Xfera Móviles S.A.*

Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação.

€ 60.000,00 - *Vodafone España*

Não conformidade com os princípios gerais de tratamento de dados.

€ 48.000,00 - *Telefonica Móviles*

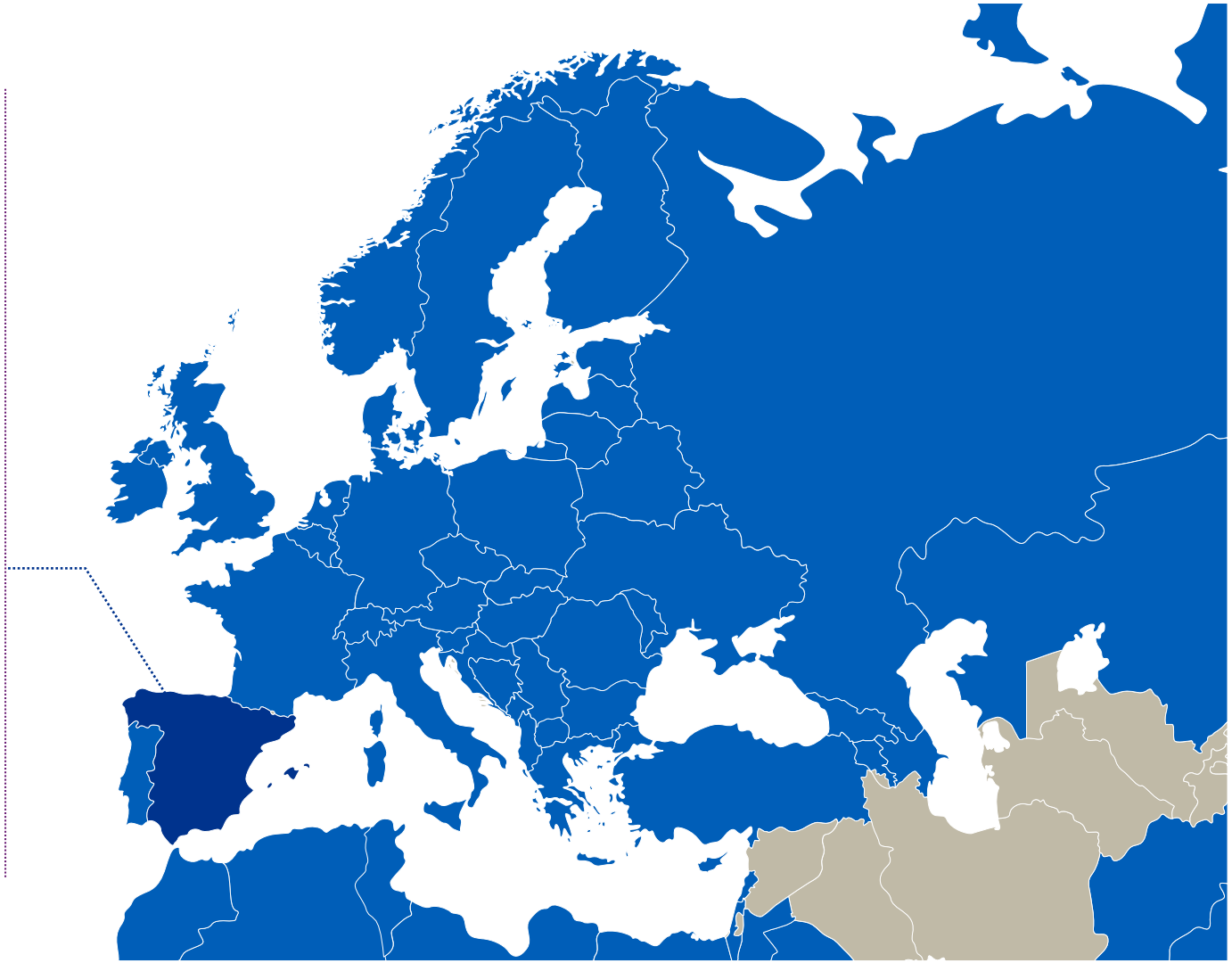
Não conformidade com os princípios gerais de tratamento de dados.

€ 40.000,00 - *Vodafone España*

Não foi utilizada base legal para o tratamento de dados.

€ 21.000,00 - *Vodafone España*

Não foi utilizada base legal para o tratamento de dados.



02

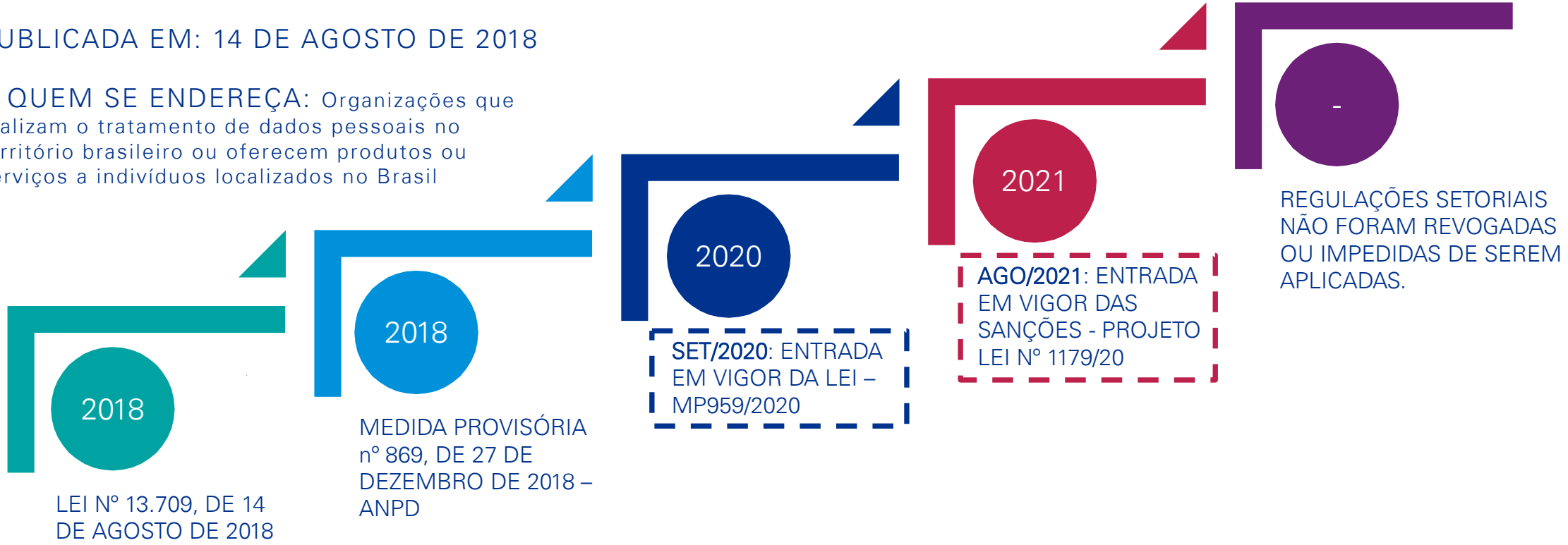
LGPD em vigor: Como ficamos?

A Lei Geral de Proteção de Dados (LGPD)

Lei 13.709

PUBLICADA EM: 14 DE AGOSTO DE 2018

A QUEM SE ENDEREÇA: Organizações que realizam o tratamento de dados pessoais no território brasileiro ou oferecem produtos ou serviços a indivíduos localizados no Brasil



SANÇÕES

Multas de 2% do faturamento anual da empresa, até o limite de R$ 50.000.000,00.
Publicitação da infração após devidamente apurada e confirmada a sua ocorrência.
Suspensão parcial do funcionamento do banco de dados pelo período máximo de 6 (seis) meses, prorrogável por igual período.

A Lei Geral de Proteção de Dados (LGPD)

Autoridade Nacional de Proteção de Dados (ANPD)

- Decreto nº 10.474 que aprova a estrutura regimental e o quadro demonstrativo de cargos da ANPD, o que **oficialmente estabelece a criação do órgão;**
- **Sanções somente poderão ser aplicadas em ago/2021;**
- Possui como principal ação **regular aspectos específicos da Lei;**
- **Aplicação de Penalidades e Sanções;**

X

Ministério Publico (MP)

- Ações específicas já acontecendo antes da entrada da Lei em vigor;
- **LGPD em vigor: ações futuras são esperadas;**
- LGPD em vigor: **primeira ação civil pública** pelo MP do Distrito Federal contra site que **comercializava dados pessoais online** (ação foi extinta);
- **Atuação do MP deve compreender suspeitas de violações,** bem como violações verificadas em atividades de entes públicos e privados.

A Lei Geral de Proteção de Dados (LGPD): Ações do MP

MP já tem fiscalizado utilização de dados pessoais, para fins econômicos, mesmo antes da **LGPD – Lei Geral de Proteção de Dados** entrar em vigor.

Hering terá que explicar o que faz com dados de reconhecimento facial de clientes

Empresa foi notificada pelo Idec que teme que prática para direcionamento de ofertas viole direitos como liberdade de escolha e informação adequada

Liminar obriga Via Quatro a suspender coleta de emoções de usuários na Linha 4-Amarela

Publicado em 15 de setembro de 2018 por blogpontodeonibus em Brasil, Destaque 2, Metrô, Notícia, Outros destaques, Tecnologia // 1 comentário

Desde de abril a Linha Amarela conta com recurso de reconhecimento facial em portas interativas que conseguem identificar emoções dos usuários. Ação do Idec sustentou que passageiro não tem direito de escolha

MP_DFT Ministério Público do Distrito Federal e Territórios

Unidade Especial de Proteção de Dados e Inteligência Artificial - ESPEC

Despacho Ministerial

Inquérito Civil Público n. *08190.005366/18-16* **Vivo Ads**

O **Ministério Público do Distrito Federal e Territórios**, por sua **Unidade Especial de Proteção de Dados e Inteligência Artificial**, requisita à **Telefônica Brasil S.A.** (**Vivo**) que elabore Relatório de Impacto à Proteção de Dados Pessoais (*Data Protection Impact Assessment – DPIA*), no prazo de 60 (sessenta) dias, em relação ao tratamento dos dados usados para o produto Mídia Geolocalizada do serviço **Vivo Ads**.

A Lei Geral de Proteção de Dados (LGPD): Riscos inerentes

- Dados Pessoais com base de tratamento inadequado:
- Atender Solicitação do Titular de Dados Pessoais
- Exposição inadequada de privacidade: sites, politicas de privacidade
- Vazamento de Dados Pessoais / Segurança da Informação
- Risco de imagem / marca;

A Lei Geral de Proteção de Dados (LGPD): Riscos inerentes

Encarregado

- Definição do profissional;
- Definição da estrutura para apoiar na implementação de ações e tocar o "dia a dia";
- Papeis e responsabilidades definidos de forma inconsistente
- Implementar ferramentas para apoiar na execução das atividades;

03

LGPD: 2 anos de projetos

Jornada da LGPD

FASE I: ASSESSMENT

- Definição do escopo
- Fluxos de Dados
- Gap Assessment
- Roadmap estratégico

FASE II: DESENHO

- Gestão de Riscos de Terceiros e Contratos
- Avaliações de impacto de privacidade (PIA) e privacidade por design (PbD)
- Política e Definição de Procedimentos
- Mapeamento e Inventário de Dados
- Governança de Privacidade & Modelo Operacional

FASE III: IMPLEMENTAR E MONITORAR

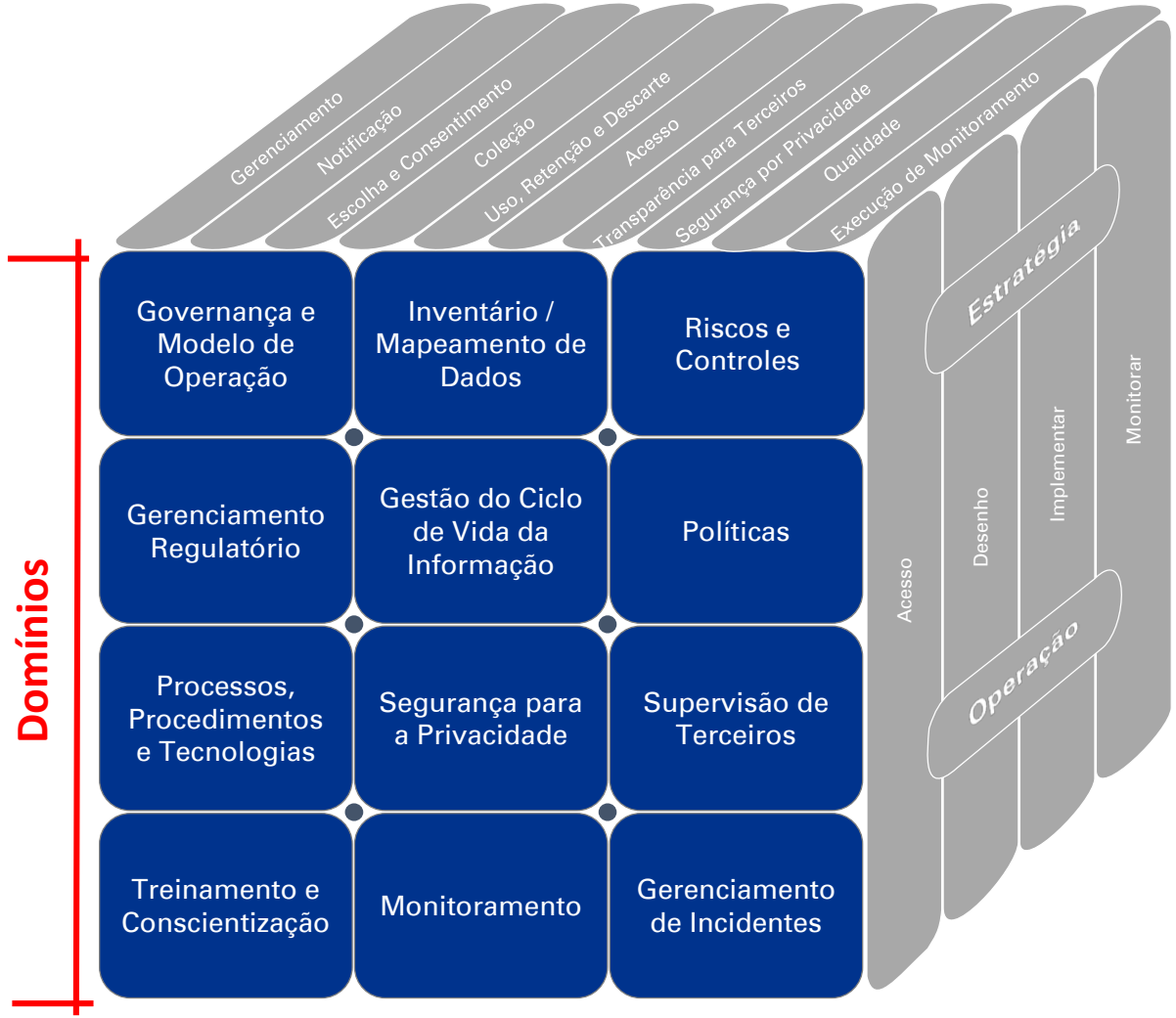
- Iterações de Implementação do Programa de Privacidade
- Treinamento de Privacidade & Consciência
- Melhoria Contínua dos Processos
- Testes de Controle/ Auditoria

LGPD - Data Privacy Assessment (DPA)

O *framework* de Gestão de Privacidade é um *framework* modular composto dos Princípios de Privacidade Geralmente Aceitos (GAPP), e dos Elementos e Subcomponentes do *Framework* de Gestão de Privacidade que **definem os fundamentos para as atividades** de gestão de risco de privacidade que acontecem em uma organização, **contemplados na metodologia de gestão de privacidade**.

Com o **advento das Leis e Regulamentos** que passaram a ser publicadas para reger a privacidade e proteção de dados ao redor do mundo**, a metodologia foi atualizada** para contemplar os **requisitos específicos da GDPR**, na Europa, e mais recentemente, **para a LGPD**, no Brasil.

Como resultado, a metodologia oferece uma **linguagem clara e consistente** e um entendimento compartilhado de privacidade e dos **diferentes requisitos** da legislação local, abrangendo também **princípios intrínsecos à gestão de privacidade**, além do atualmente requerido.



A Estrutura de Gerenciamento de Privacidade da KPMG e a LGPD

Artigo da LGPD	
22	Representantes de Controlador
23-32	Tratamento de dados de Direito Público
13	Estudos de saúde pública
51	Adoção de padrões estimulados pela Autoridade Nacional

Governance and Operating Model

Artigo da LGPD	
37	Registro de operações de tratamento pelo Controlador e Operador

Inventory/ Data Mapping

Artigo da LGPD	
5	Conceitos e gestão de riscos
49	Estruturação de sistemas de forma a atender aos requisitos de Segurança
50	Estabelecer associações e formular regras e boas práticas e de governança

Risk and Control

Artigo da LGPD	
33-36	Transferência de dados

Regulatory Management

Artigo da LGPD	
50	Estabelecer associações e formular regras e boas práticas e de governança

Policies

Artigo da LGPD	
1-4	Conceitos e aplicação
52-65	Infrações e penalidades definidas

Governance and Operating Model | Inventory/ Data Mapping | Risk and Control

Regulatory Management | Information Lifecycle Management | Policies

Processes, Procedures and Technology | Security for Privacy | Third Party Oversight

Training and Awareness | Monitoring | Incident Management

Artigo da LGPD	
46	Proteção dos dados
47	Segurança no processamento dos dados

Security for Privacy

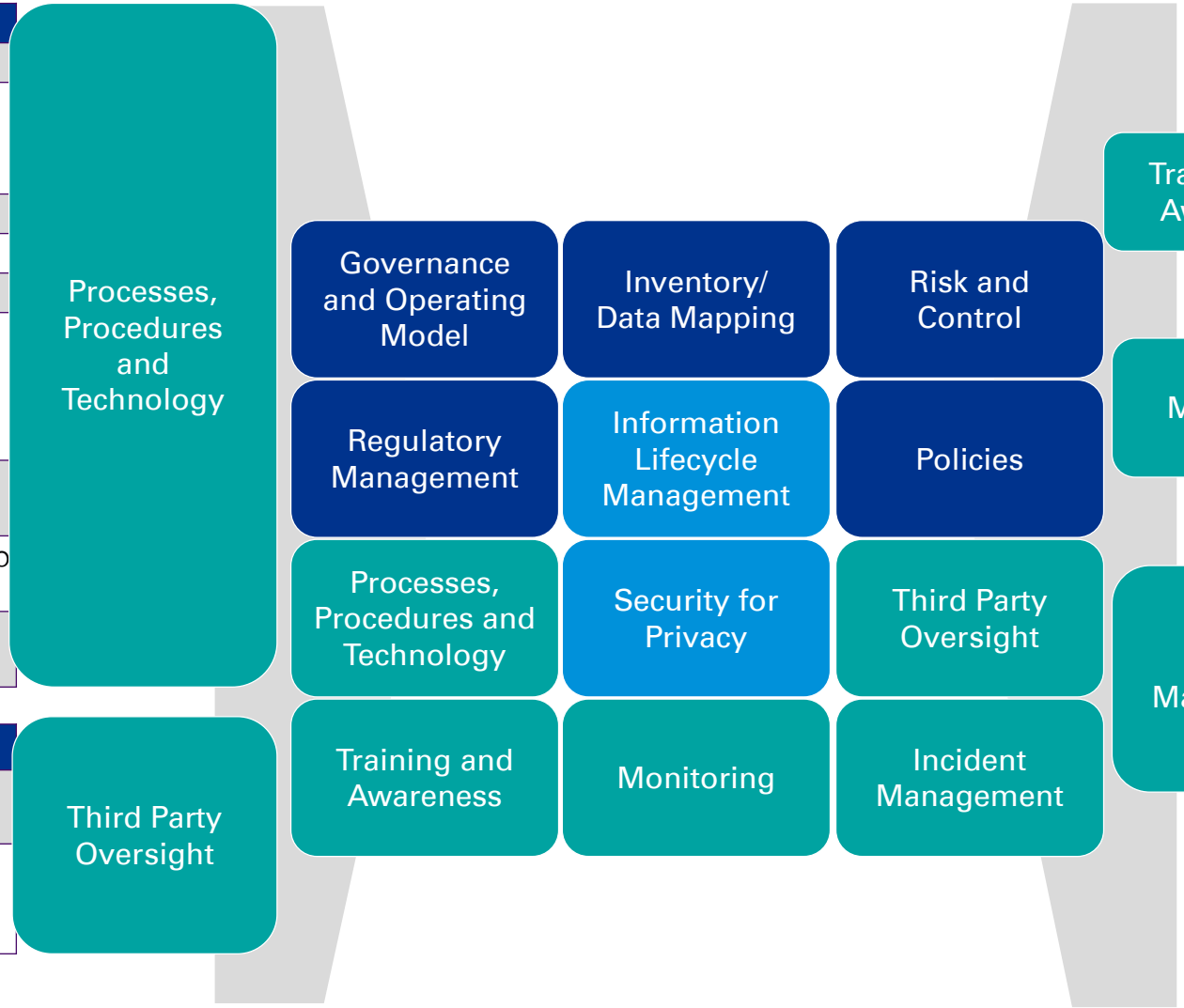
Information Lifecycle Management

Artigo da LGPD	
6	Princípios de tratamento de dados pessoais
7	Tratamento de dados pessoais e hipóteses
8	Princípios de Consentimento
14	Tratamento de dados de crianças e adolescentes
9	Informações sobre o tratamento de dados
10	Interesse do Controlador e tratamento dos dados
11	Tratamento de dados sensíveis
20	Tratamento automatizado dados
21	Utilizar dados para prejuízo da pessoa
44	Irregularidade do tratamento dos dados
45	Violação de direitos nas relações de consumo

A Estrutura de Gerenciamento de Privacidade da KPMG e a LGPD

Artigo da LGPD	
12	Dados anonimizados
40	Padrões de interoperabilidade para portabilidade, acesso aos dados, guarda de dados e transparência
15	Término do tratamento dos dados
16	Eliminação dos dados
17	Garantia do direito de liberdade
18	Relação dos dados tratados pelo controlador, eliminação, compartilhamento, revogação, petição
19	Confirmação de existência e requisição dos dados
42	Reparação de danos causados pelo Controlador e Operador
43	Isenção de responsabilidades dos agentes de tratamento

Artigo da LGPD	
39	Execução pelo Operador a partir de orientação do Controlador
38	Autoridade solicitar relatório ao Controlador sobre impacto á Proteção de Dados



Artigo da LGPD	
39	Tasks of DPO

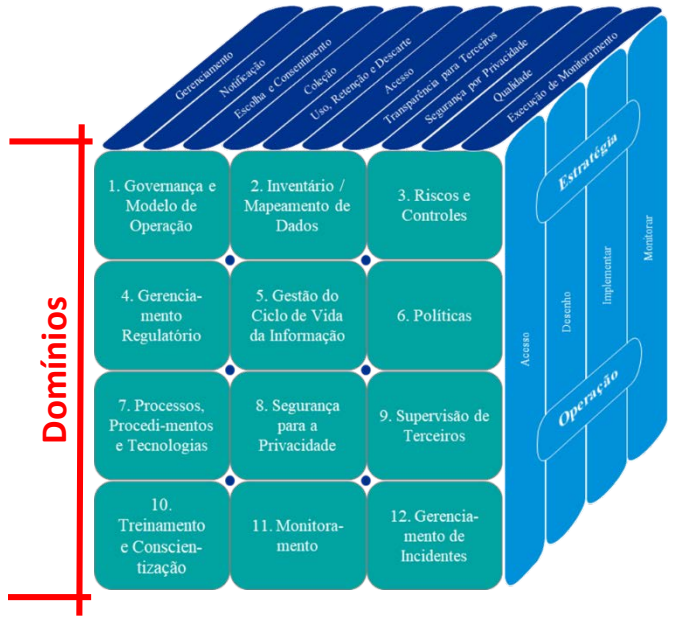
Artigo da LGPD	
41	Controlador indicar o DPO

Artigo da LGPD	
48	Comunicação em caso de Incidentes
34	Notificação de falhas individuais

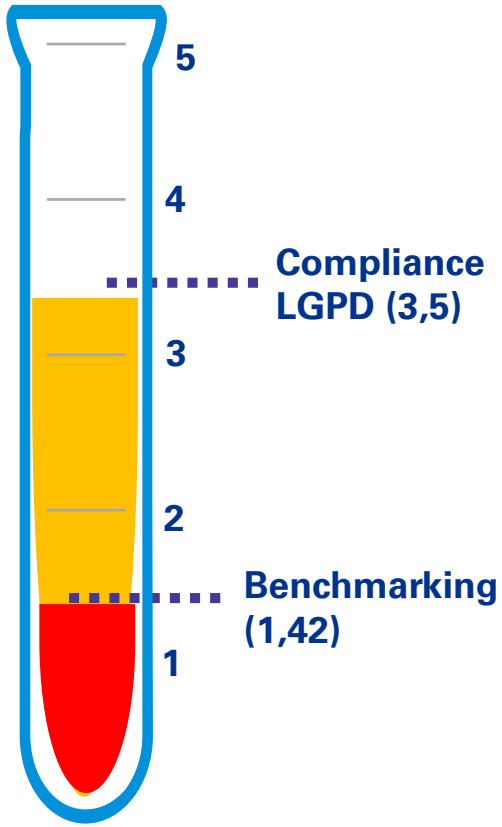
Metodologia para Análise de Maturidade

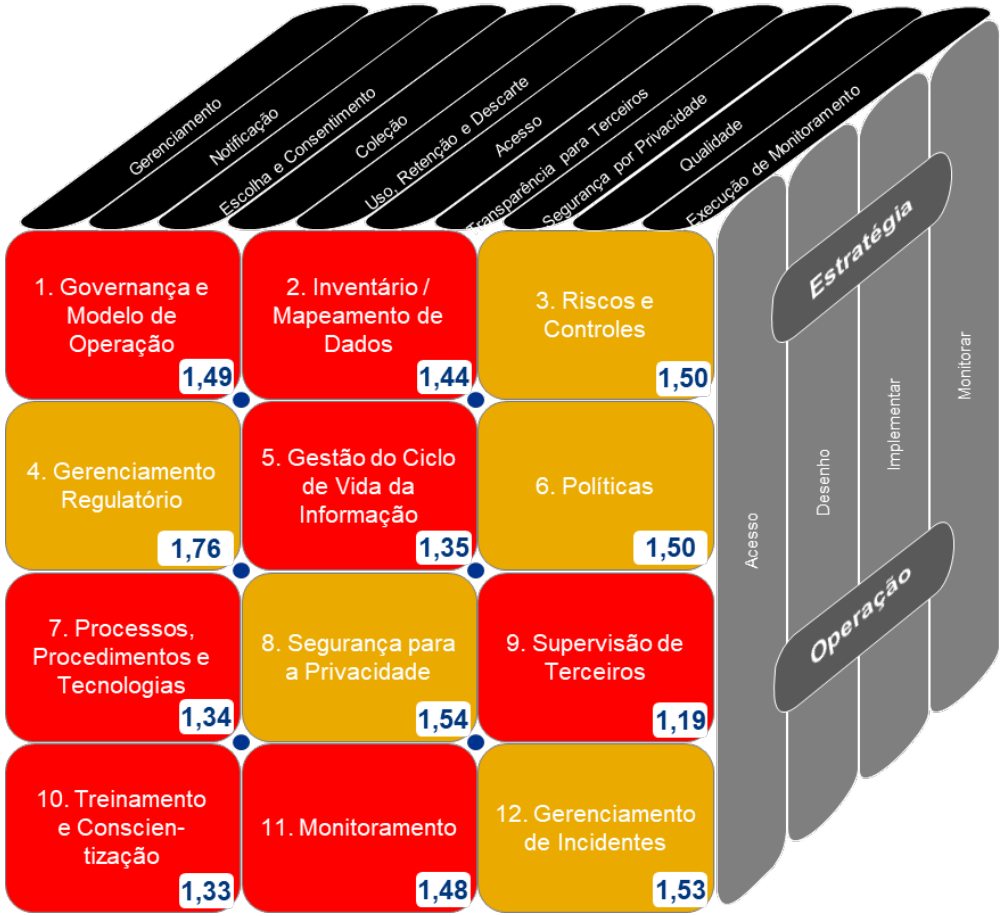
Apresentamos ao abaixo a tabela contendo o nível de Classificação de Maturidade de Privacidade de Dados, considerando os critérios levados em consideração e o descritivo das situações identificadas.

Maturidade	Descrição	Status
1,0 a 1,4	**Ad Hoc -** Ambiente de controle imprevisível, onde as atividades de controle não são projetadas ou não estão em vigor.	**Não-conformidade**
1,5 a 2,4	**Inicial** • Atividades e processos existem, mas não estão adequadamente documentados; • Controles dependem principalmente de pessoas (e de sua boa vontade); • Não existe treinamento formal ou comunicação da atividade de controle; e • Desvios das atividades de controle provavelmente não serão detectados;	**Não-conformidade** Existe uma base na atual Legislação aplicável. No entanto, são necessárias modificações para atingir a conformidade.
2,5 a 3,4	**Controlado** • Atividades de controle são projetadas e implementadas; • Atividades de controle foram documentadas e comunicadas aos funcionários; e • Não há revisão gerenciada e estruturada da eficácia operacional do controle.	**Parcialmente em conformidade**
3,5 a 4,5	**Gerenciado** • Controles padronizados com testes periódicos em design e operação eficazes; • Automação e ferramentas podem ser usadas de forma limitada para suportar atividades de controle;	**Em conformidade**
4,6 a 5,0	**Otimizado** • Existe uma estrutura integrada de controle interno com monitoramento em tempo real pelo gerenciamento com melhoria contínua (gerenciamento de risco em toda a empresa); e • Automação e ferramentas são usadas para apoiar as atividades de controle e permitir que a Organização faça mudanças rápidas nas atividades de controle, caso necessário.	**Em conformidade**
-	**Não Aplicável -** Caso o controle não seja aplicável, um comentário deve será adicionado para explicar os motivos.	**Não Aplicável**



Avaliação de Maturidade de Privacidade





1,0 a 1,4	Ad Hoc	1,5 a 2,4	Inicial	2,5 a 3,4	Controlada	3,5 a 4,4	Gerenciado	4,5 a 5,0	Otimizado

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	**1,49**
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

1

Governança e Modelo de Operação

- **Encarregado definido;**
- **Ausência de uma definição de uma estrutura** para apoiar o Encarregado;
- Ausência de d**efinição de papeis e responsabilidades de privacidade** nas Organizações;

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	**1,44**
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

2

Inventário / Mapeamento de Dados

- Ausência de um **mapeamento contendo uma visão formal sobre os processos de negócios e atividades de tratamento de dados pessoais, bem como o fluxo de tráfego entre sistemas, fornecedores, parceiros**, outros;
- Ausência de **um processo formal para sustentação de mapeamento de dados pessoais realizados**, em linha com exigência com aspectos da Lei;
- Ausência **de ferramentas para apoiar no processo de mapeamento e atualização** do registro de dados pessoais;

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	**1,50**
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

3

Riscos e Controles

- **Ausência de um processo formal que visa identificar, avaliar e gerenciar os riscos de privacidade** atual e/ou desejado na organização com base na estratégia geral de negócios.
- **Ausência de matriz de riscos e controles de privacidade**, formalmente definida, bem como de uma linha de base dos riscos de privacidade de dados tolerados pela organização.
- **Os controles de privacidade de dados não são formalmente definidos** ou documentados, bem como os **riscos de privacidade que devem ser endereçados;**

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	**1,76**
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

4

Gerenciamento Regulatório

- Ausência de processo formal de identificação, avaliação e **gerenciamento de identificação de leis/regulamentações e mudanças regulatórias** no que diz respeito a **privacidade de dados;**
- Ausência de definição de diretrizes para **mitigar as mudanças regulatórias identificadas;**
- Ausência de processos formais que visam **reconhecer e responder as solicitações de informações sobre atividades de tratamento de dados perante a Autoridade Nacional de Proteção de Dados (ANPD).**

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	**1,35**
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

5

Gestão do Ciclo de Vida da Informação

- Ausência de **processo de minimização de** informações pessoais estabelecido;
- Nenhum processo formal foi estabelecido para fornecer **notificação e/ou obter o consentimento dos titulares de dados** pessoais para processar suas Informações;
- Não existe **políticas e processos formalizados**, em vigor, sobre: (a) **classificação das Informações** de dados pessoais coletadas, usadas, retidas e divulgadas; (b) **retenção de dados pessoais**; e (c) **destruição de dados pessoais** após a data de retenção;
- Ausência de um **processo de anonimização / Pseudonomização de dados pessoais;**

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	**1,50**
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

6

Políticas

- Ausência de **Politica/Normativa Internas de Privacidade** e outras tais como: retenção e exclusão segura de dados; avisos de privacidade ao empregado; tratamento de dados recebidos por e-mail; outras.
- Ausência de **Políticas Externas de Privacidade** e outras, tais como: Política de Cookies; Política de privacidade direcionada a terceiros e fornecedores; Política para o atendimento às solicitações dos titulares;

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	**1,50**
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

6

Políticas (continuação)

- Ausência de uma Estrutura de Políticas e Gerenciamento de Mudanças, considerando: (a) **processo formal para avaliação das políticas e alterações**; (b) procedimentos formais para agenda da divulgação e **aceite das políticas e armazenamento de evidências**; e (c) **inventário e repositório de políticas** relacionadas ao tema **de privacidade.**

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	**1,34**
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

7

Processos, Procedimentos e Tecnologias

- Não existem processos formalmente estabelecidos para avaliar os **riscos de privacidade, no conceito de Pbd – Privacy by Design e PIA – Privacy Impact Assessment;**
- Tratamento de dados pessoais para **titulares de dados são feitos de forma manual**, sem considerar todos os **aspectos exigidos pela Lei e sem ferramenta suporte;**
- Ausência de avaliação de **transferência de dados internacionais** antes do compartilhamento de informações;
- Aspectos de **segurança da informação não contemplam privacidade de dados pessoais**, tanto na suporte de ferramentas (ex.: DLP) ou autenticação de usuários;

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	**1,54**
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

8

Segurança para a Privacidade

- Não há um processo formal de comunicação entre o Time de Privacidade e a área de Segurança da Informação
- Existência de controles que dão suporte à segurança lógica sobre as Informações Pessoais, entretanto, esses controles não são efetivamente projetados em linha com o risco de Privacidade imposto a Informações Pessoais.

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	**1,07**
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

9

Supervisão de Terceiros

- **Ausência de processos de Due Diligence (com foco em privacidade),** considerando uma avaliação baseada em risco dos processos e controles de privacidade em vigor em um provedor terceirizado (operador);
- Ausência de **cláusulas contratuais de privacidade na totalidade de contratos** identificados;
- Ausência de **Garantia de Terceiros**, considerando uma **abordagem baseada em riscos para conduzir revisões** periódicas do desenho e eficácia operacional **dos controles de Privacidade de terceiros;**

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	**1,33**
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

10

Treinamento e Conscientização

- **Ausência de treinamentos e reciclagens periódicos** às áreas responsáveis pela privacidade de dados;
- Ausência **de treinamentos de forma ampla dos requisitos da Lei Geral de Proteção de Dados para todos os colaboradores (incluindo terceiros)** que façam interação com alguma parte do ciclo de vida do tratamento da informação;
- **Ausencia de um proceso de Conscientização continuo para aspectos de provacidade**, bem como **comunicações contantes** com definições de obrigações em relação ao processamento de Informações Pessoais para funcionários e terceiros;.

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	**1,33**
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

10

Treinamento e Conscientização (continuação)

- Não há mecanismos **de acompanhamento das atividades de treinamento e conscientização**, como avaliações e medições para verificar a aceitação do público alvo.

- Ausência de **campanhas de promoção do tema de conscientização e compreensão do público sobre os riscos**, regras, salvaguardas e direitos em relação ao processamento de informações pessoais.

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	**1,48**
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

11

Monitoramento

- Ausência de um processo formal ou orientação para **avaliação de desempenho e monitoramento (indicadores estabelecidos) contínuo focado em privacidade dos dados** e controles de segurança de privacidade;
- Ausência de um processo formal ou orientação para **avaliações independentes dos controles de Privacidade de Dados implantados;**

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

12

Gerenciamento de Incidentes

- Ausência de **normativos/manuais específicos para tratar vazamentos de dados pessoais** – existem mas não que contemplem dados pessoais;
- Ausência de procedimento de **notificação à órgãos reguladores e partes interessadas em caso de incidente de vazamento de dados;**
- Ausência de um processo / procedimento específico de segurança de dados pessoais e/ou sensíveis coletados durante uma **investigação de incidente ou denúncias**;

.

Avaliação de Maturidade de Privacidade

Domínio	Benchmark
1. Governança e Modelo de Operação	1,49
2. Inventário / Mapeamento de Dados	1,44
3. Riscos e Controles	1,50
4. Gerenciamento Regulatório	1,76
5. Gestão do Ciclo de Vida da Informação	1,35
6. Políticas	1,50
7. Processos, Procedimentos e Tecnologias	1,34
8. Segurança para a Privacidade	1,54
9. Supervisão de Terceiros	1,07
10. Treinamento e Conscientização	1,33
11. Monitoramento	1,48
12. Gerenciamento de Incidentes	1,53
Maturidade Média	**1,42**

12

Gerenciamento de Incidentes (continuação)

- **Papeis e responsabilidades não estão claramente definidos de como comunicar o vazamento de informações**, incluindo dados pessoais;
- **Ausência de prazos estabelecidos para resposta à incidentes** que inclua dados pessoais – requisito da Lei pode não ser atendido (prazo razoável);

04

E como podemos seguir?

Os desafios de Mapeamento de Dados Pessoais devem ser considerados

Identificar os dados pessoais

Os dados pessoais podem residir em vários locais e ser armazenados em vários formatos, como papel, eletrônico e até áudio. O **primeiro desafio é decidir quais informações você precisa registrar e em que formato.**

Identificar salvaguardas técnicas e organizacionais apropriadas

O segundo desafio é identificar a tecnologia apropriada - e as política e os procedimentos para o seu uso - para proteger as informações, **além de determinar quem controla o acesso a elas.**

Compreender as obrigações legais e regulamentares

Determinar quais **são as obrigações legais e regulamentares de sua organização.** Assim como a LGPD ou GDPR, isso pode incluir outros padrões de conformidade, como o Padrão de Segurança de Dados do Setor de (por exemplo, PCI DSS).

Menosprezar os volumes

Muitos projetos de **mapeamento de dados falham no menosprezo dos dados que nem sempre estão aparentes nos principais processos de negócio** e o seu volume distribuído na Empresa.

Aspectos importantes a serem trabalhados

Governança, inventário e risco — estão todos Ligados

É necessário entender **quais dados você possui, como você está indo para gerenciá-lo**, e quais são os riscos envolvidos, assim você pode **avaliar o seu apetite de risco e aplicar o nível de controle apropriado.**

.

Direitos do Titular de Dados — já podem ser exercidos

Direitos dos indivíduos — **o "direito à eliminação", e a questão da retenção de dados são fortemente ligada.** Se você **não sabe que dados você tem, e se você está armazenando mais do que é necessário, como você pode esperar para ser capaz de identificar o que deve ser removido tal pedido?**

Gerenciamento de Incidentes

Gerenciamento de incidentes — há uma nova regra e exigente para relatar violações ao regulador dentro de um "prazo definido". **Sem um processo de gestão de incidentes robustos, você poderia mobilizar uma investigação e ser capaz de relatar dentro do prazo estabelecido?**

Aspectos importantes a serem trabalhados

Treinamento e Conscientização

Treinamento — você precisa **garantir que sua equipe esteja ciente do impacto do LGPD** e ter uma decente compreensão de como se aplica a eles. Todos vão precisar de treinamento básico, **mas áreas de alto risco como RH ou marketing vão precisar de treinamento focado em como gerenciar categoria especiais de privacidade de informações (PI).**

Diligência e contratos de terceiros

Diligência e contratos de terceiros — dados pessoais de **Controladores serão obrigados a ter um entendimento de como sua cadeia de suprimentos lida com sua privacidade de Informações (PI).** Você será obrigado a ter explícito **cláusulas de privacidade em contratos, um período de retenção e o direito de auditar**. Os **Processadores (operadores) de dados serão exigidos para ter as mesmas proteções** no lugar que os dados dos Controladores.

Garantia de terceiros

Garantia de terceiros — muitas **organizações têm melhorado os seus processos de gestão de terceiros** nos últimos anos, mas poucas desenvolveram um **processo que satisfaz as necessidades especificas do LGPD.** Contratação de terceiro requerem atenção urgente; No entanto, **as atividades em curso de garantia podem ser postas em primeiro lugar como diligência e o processo de recontratação.**

Aspectos importantes a serem trabalhados

Encarregado

Encarregado – a **definição de um profissional para o cargo** e a **criação de papeis e responsabilidades, bem como criação de um modelo de Governança** para suporte o processo de privacidade nas Organizações devem ter prioridade nesse momento. **Questionamentos Legais já podem ser uma realidade nas Organizações;**

Modelo de Compliance

Modelo de Compliance - Nunca se esqueça que a **LGPD é como qualquer outro processo de Compliance,** esta é uma **atividade que fará parte da rotina das Organizações** preocupadas com os dados pessoais de seus clientes / funcionários / parceiros;

Como começar?

Como começar? - **Não existem modelos corretos ou incorretos.** Existem modelos que melhor se adaptarão à sua Organização, mas comece logo!

Não perca tempo, **independentemente da abordagem comece sua trajetória.**

Contatos

Rodrigo Milo

SÓCIO
CYBER SECURITY & PRIVACY
T: +55 (21) 2207-9462 / +55 (21) 98306-5132
E: rodrigomilo@kpmg.com.br

Henrique Sirot

GERENTE
CYBER SECURITY & PRIVACY
T: +55 (31) 99297-4714
E: hsirot@kpmg.com.br

Obrigado!

home.kpmg/socialmedia