Rede Paranaense de *Compliance*

4º Encontro

03/12/2018

Agenda

18:00 – 18:15 Boas vindas

18:15 – 18:20 Abertura

18:20 – 19:00 **Lei Geral de Proteção de Dados e seus aspectos práticos nas corporações**
Caroline Klamas

19:00 – 19:10 Intervalo

19:10 – 20:00 **Desafios para implementação da LGPD - a experiência da Phillip Morris**
Rogerio Moleiro, Vanessa Chrestani e Vinicius Gehlen

20:00 – 20:20 Perguntas e encerramento

20:20 – 21:00 Confraternização

Sistema Fiep FIEP SESI SENAI IEL programa de **Integridade**

Rede Paranaense de Compliance

O Sistema Fiep, signatário do Pacto Global, tem o compromisso de incentivar a gestão socialmente responsável das indústrias, estimulando a **transparência** e a **competitividade dos negócios**, por isso, lançou em março de 2018 a **Rede Paranaense de Compliance**, em parceria com o CIFAL Curitiba e o Unitar.

Trata-se de uma rede empresarial para debater sobre compliance e gestão de riscos, governança corporativa e integridade.

OBJETIVO:

Disseminar a cultura de compliance compartilhando informações alinhadas aos movimentos e novas práticas do mercado.

Como funciona

Serão encontros trimestrais para discutir o assunto, com especialistas na área e apresentação de cases. Esses eventos são abertos ao público.

Podem participar empresas interessadas na promoção de um mercado mais justo e uma sociedade mais desenvolvida.

Vantagens: Ser parte de uma rede de empresas comprometidas com boas práticas de governança corporativa, favorecendo a troca de experiências que promovam a ética social e empresarial.

Lei Geral de Proteção de Dados e seus aspectos práticos nas corporações

Caroline Cavassin Klamas

Advogada - Carvalho, Machado e Timm Advogados

CMT CARVALHO, MACHADO E TIMM ADVOGADOS

Proteção de Dados Pessoais

Caroline Cavassin Klamas
cklamas@cmtlaw.com.br

Graduada pela UPFR, LL.M. pela University of Miami School of Law, membro da New York State Bar Association

Rede Paranaense de Compliance - FIEP
Curitiba, 03/12/2018

CMT CARVALHO, MACHADO E TIMM ADVOGADOS

Lei geral de proteção de dados pessoais: nº 13.709, de 14 de agosto de 2018

Entrará em vigor em fevereiro de 2020

CMT CARVALHO, MACHADO E TIMM ADVOGADOS

leis estaduais

GPDR

LGPD

- privacidade como direito fundamental
- lei geral, aplicável a todos os tipos de dados pessoais
- escopo extraterritorial

- Liberdade de expressão e de imprensa (free speech - 1st Amendment)
- leis esparsas (por estado e por indústria)
- limitação territorial

aplicação territorial

- tratamento realizado no Brasil; ou
- cujo objetivo seja a oferta ou o fornecimento de bens e serviços no Brasil; ou
- de dados de indivíduos localizados no Brasil; ou
- de dados coletados no Brasil

CARVALHO, MACHADO E TIMM ADVOGADOS

penalidades

- advertência, com indicação de prazo para adoção de medidas corretivas;
- **multa** 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;
- multa diária;
- publicização da infração; e (**danos reputacionais**)
- Bloqueio/ eliminção dos dados referentes à infração.

+ Indenização do titular dos dados

CARVALHO, MACHADO E TIMM ADVOGADOS

princípios da LGPD

CMT CARVALHO, MACHADO E TIMM ADVOGADOS

dados pessoais

Todo dado relacionado a pessoas **identificadas** ou **identificáveis**.

- imagem
- dados locacionais (“GPS”)
- endereço de IP
- Identificadores eletrônicos
- CPF
- estado civil
- dados bancários

CARVALHO, MACHADO E TIMM ADVOGADOS

dados pessoais sensíveis

- 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

CARVALHO, MACHADO E TIMM ADVOGADOS

tratamento de dados:

toda operação realizada com dados pessoais, incluindo:

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

CMT CARVALHO, MACHADO E TIMM ADVOGADOS

direitos dos titulares

- confirmação do tratamento, acesso e correção aos dados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou em desconformidade com a lei;
- portabilidade a outro fornecedor;
- informação das entidades públicas e privadas com as quais o controlador compartilhou os dados;
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- revogação do consentimento ao tratamento.

CMT CARVALHO, MACHADO E TIMM ADVOGADOS

Titular dos Dados >>

Controlador >>
(Utiliza dados para seu propósito)

Operador >>
(Trata os dados p/ propósito do controlador)

CARVALHO, MACHADO E TIMM ADVOGADOS

principais hipóteses de processamento

1. consentimento expresso*

2. execução de contrato

3. cumprimento de dever legal ou regulatório*

4. defesa de direitos*

*Aplicáveis a dados sensíveis

CARVALHO, MACHADO E TIMM ADVOGADOS

principais hipóteses de processamento

5. proteção da vida ou da incolumidade física do titular ou de terceiro*

6. tutela da saúde (por profissionais da saúde ou entidades sanitárias)*

7. interesse legítimo do controlador

8. proteção ao crédito

É vedada a comunicação ou o uso compartilhado de dados sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.

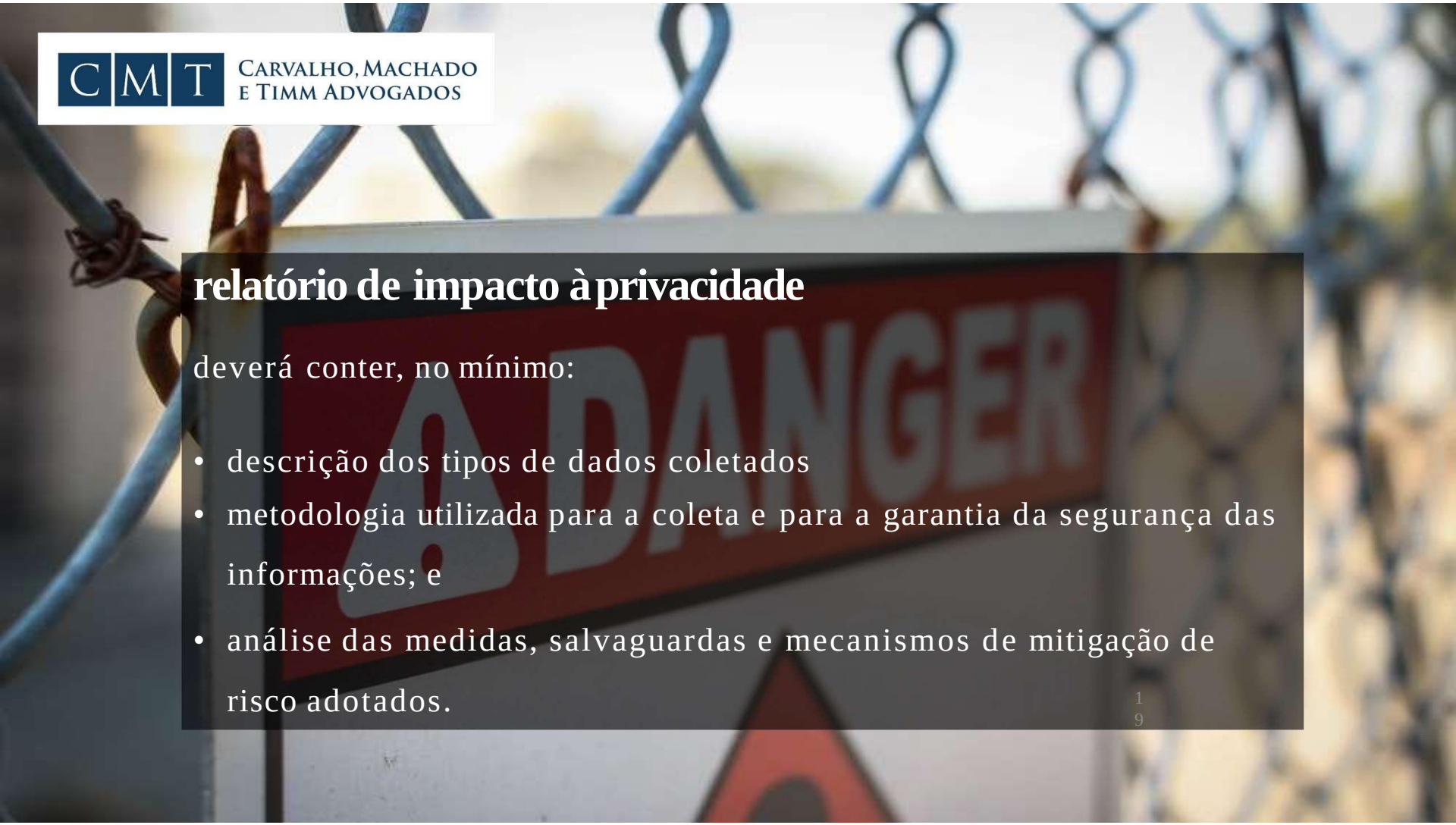
*Aplicáveis a dados sensíveis

CMT CARVALHO, MACHADO E TIMM ADVOGADOS

Incidente de segurança

dever de comunicar à autoridade nacional e ao titular:

- natureza dos dados afetados;
- informações sobre os titulares envolvidos;
- indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
- riscos relacionados ao incidente;
- motivos da demora, no caso de a comunicação não ter sido imediata; e
- medidas que foram ou que serão adotadas para reverter ou mitigar os danos.



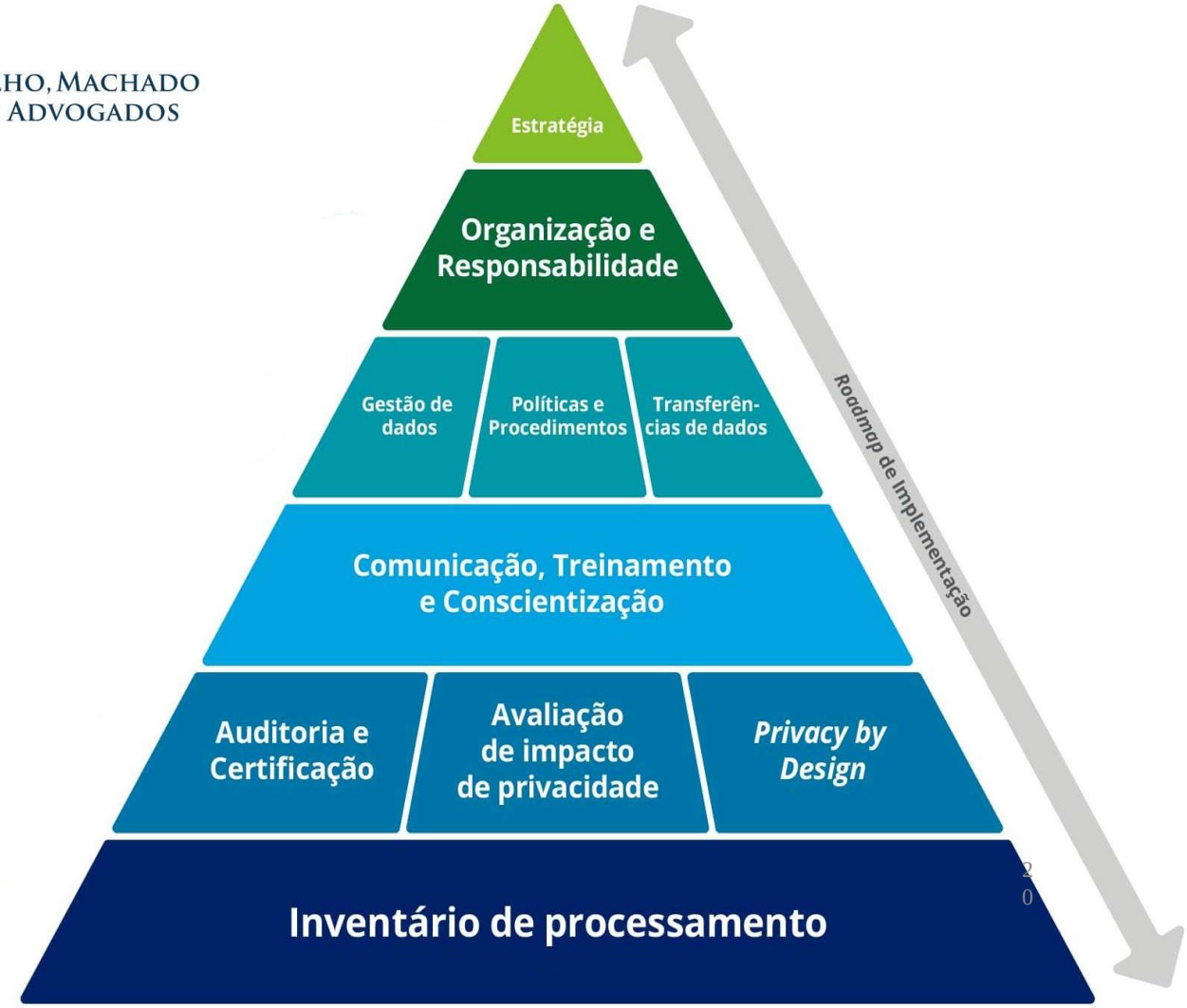
CMT CARVALHO, MACHADO E TIMM ADVOGADOS

relatório de impacto à privacidade

deverá conter, no mínimo:

- descrição dos tipos de dados coletados
- metodologia utilizada para a coleta e para a garantia da segurança das informações; e
- análise das medidas, salvaguardas e mecanismos de mitigação de risco adotados.

CARVALHO, MACHADO E TIMM ADVOGADOS



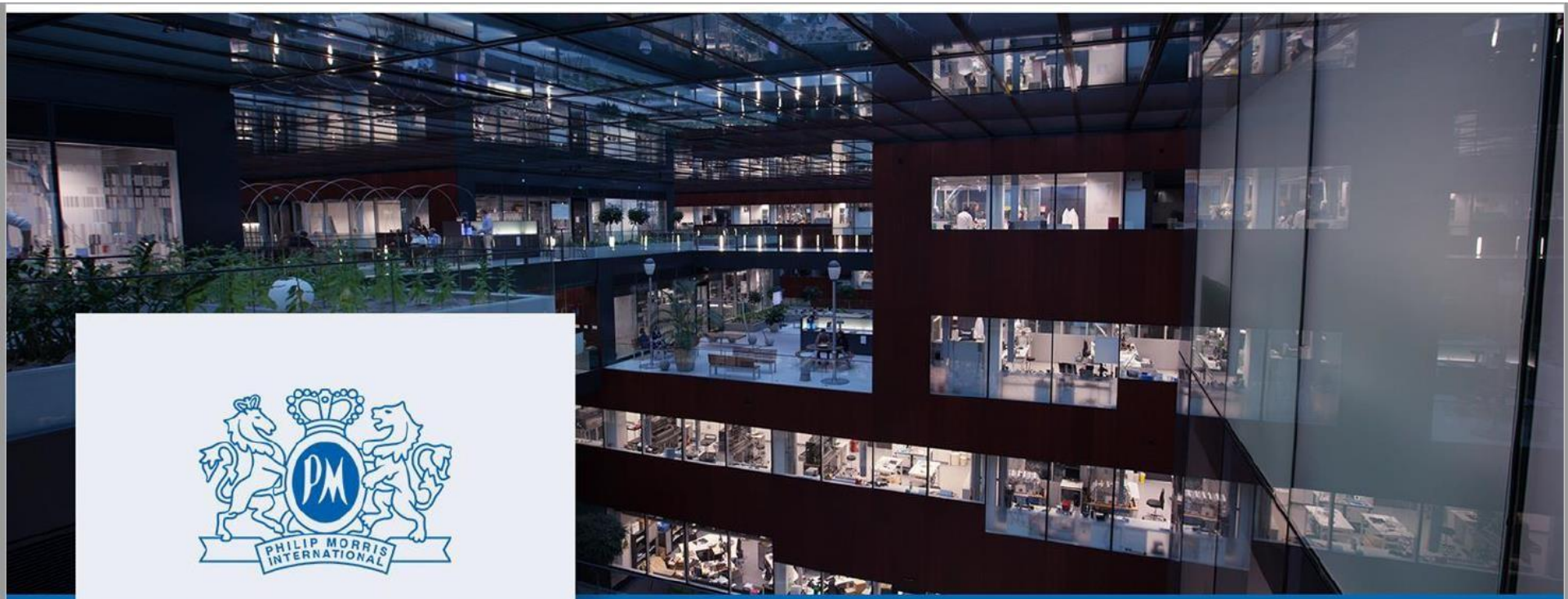
Dúvidas?

Caroline Klamas
cklamas@cmtlaw.com.br

CMTLAW.COM.BR

Desafios para implementação da Lei Geral de Proteção de Dados (LGPD) - a experiência da Phillip Morris

Rogerio Moleiro - Diretor de Ética & Compliance
Valeska Chrestani - Advogada
Vinicius Gehlen - Especialista em Segurança da Informação



PHILIP MORRIS BRASIL

FIEP, Dec'18

AGENDA

1. A PMI E NOSSO PROGRAMA DE CONFORMIDADE
2. O AMBIENTE REGULATÓRIO DE PRIVACIDADE DE DADOS
3. NOSSO PROGRAMA GLOBAL DE PRIVACIDADE (GPP)
4. EQUÍVOCOS COMUNS E APRENDIZADOS

Presença

no Brasil

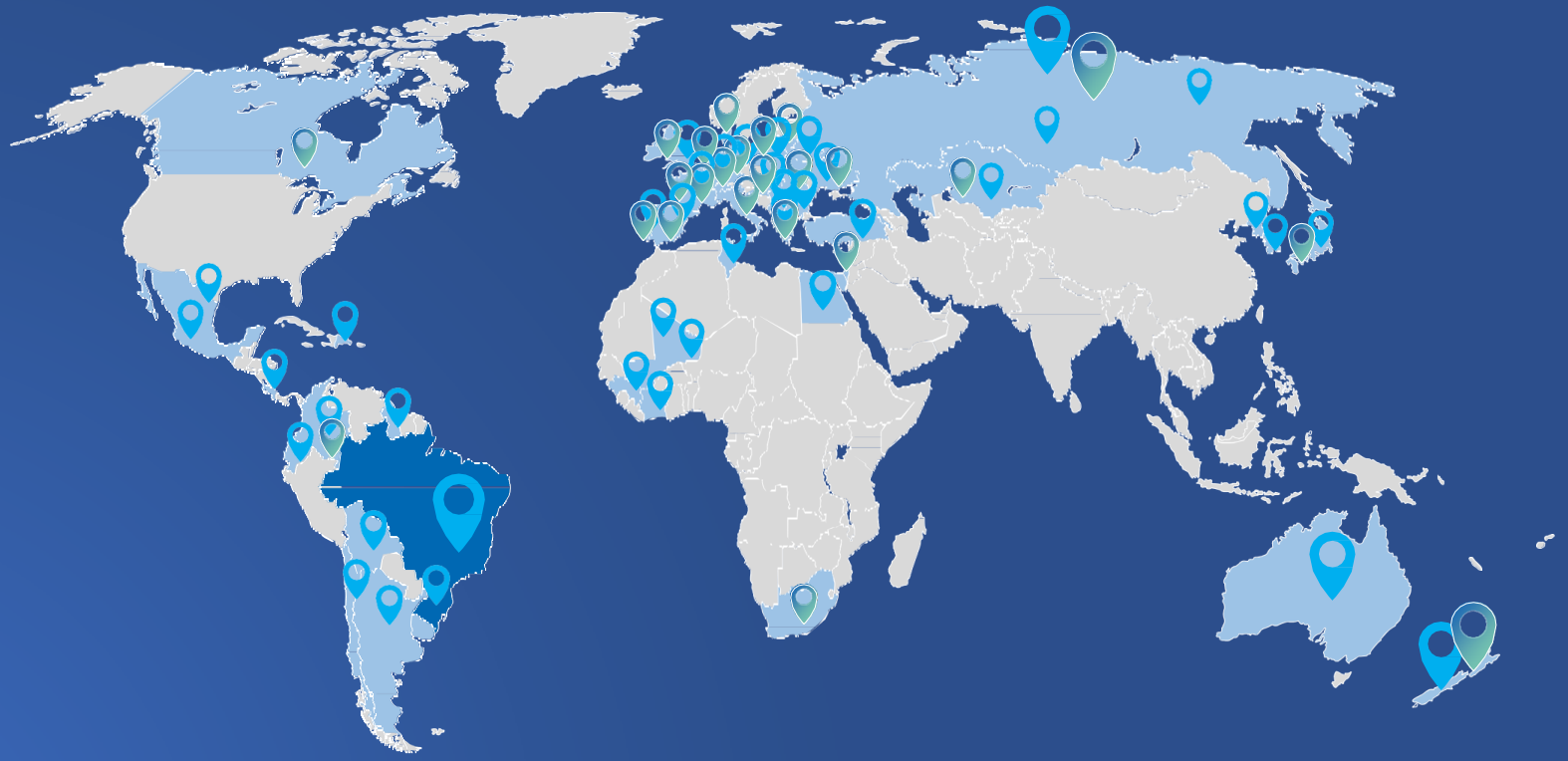
Cerca de 3 mil colaboradores
2ª maior fabricante de cigarros do País

Fábrica

Centros de distribuição

Escritório central

Presença no Mundo



Produtos em **180** mercados

27,9% de participação

GUIA PARA O SUCESSO

CÓDIGO DE CONDUTA PMI

Plataformas

Programas de Compliance

Responsáveis

PHILIP MORRIS BRASIL

Ética & Compliance	Violações Conflitos de Interesse
Marketing	Marketing e Venda de Produtos
Finanças	Fiscal e Comércio Informações da Companhia Tributação
RH	Integridade no Local de Trabalho
Jurídico	Concorrencia Direitos de Propriedade Intelectual Anticorrupção Abuso de Informação Privilegiada
IT	Uso de Tecnologia de Informática Proteção de Dados Pessoais
Assuntos Externos	Contribuições de Caridade Comunicações Externas e Declarações Públicas
Operações	Meio Ambiente, Saúde, Segurança e Proteção Regulamentação, Desenvolvimento e Fabricação de Produtos

Nossa visão de futuro

Deixar de comercializar cigarros.
Proporcionar produtos de risco reduzido, sem a combustão do tabaco, a adultos que tem a intenção de continuar fumando.

Construir um Futuro sem Fumaça

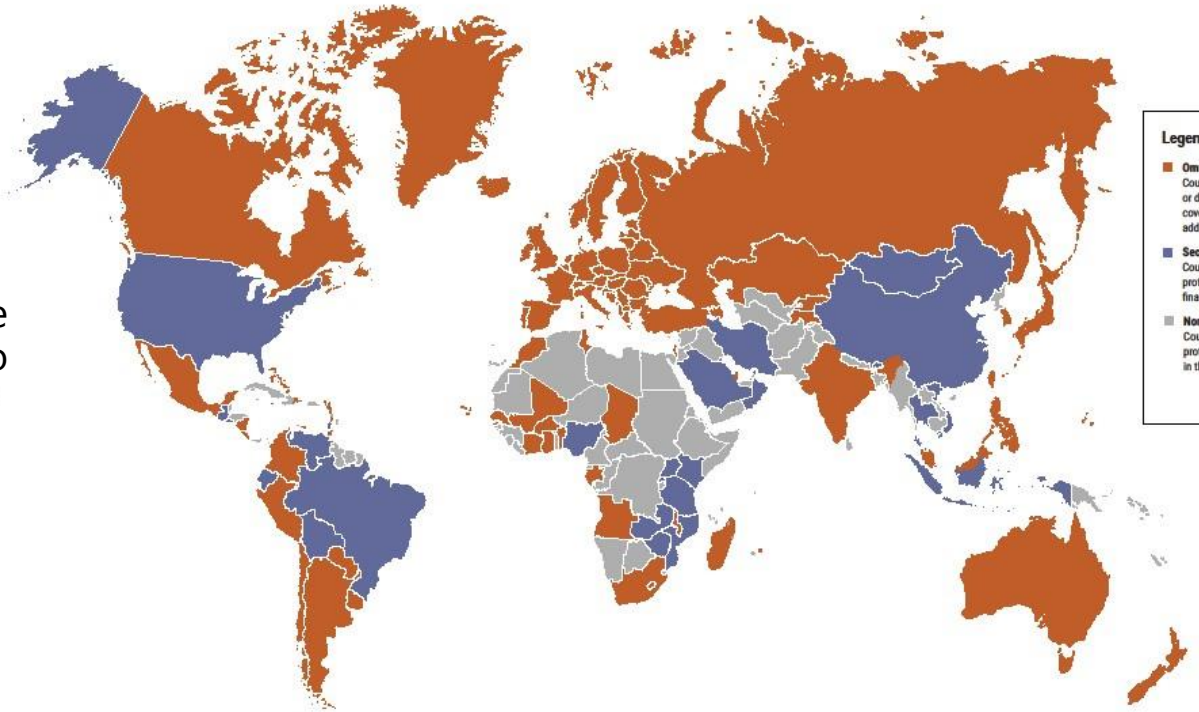
- Empresa líder e de sucesso
- Demanda da Sociedade
- Inovação, ciência e tecnologia
- Responsabilidade Moral

O PROGRAMA GLOBAL DE PRIVACIDADE DA PMI

Regulação

>100 leis no mundo regulamentando o que pode (ou não) ser feito com dados pessoais.

Sectoral and Omnibus Privacy and Data Protection Laws



Legend

- **Omnibus Coverage**
  Countries that have a single or multiple national privacy or data protection laws that result in comprehensive coverage. These laws do not exclude the possibility of additional sector-specific privacy regulation.
- **Sectoral Coverage**
  Countries that have sectoral privacy or data protection laws, for example in the public sector, financial sector, telecommunication sector.
- **None**
  Countries that do not have privacy or data protection laws but may have some coverage in their constitution or other laws.

Updated November 2017.

NYMITY RESEARCH™

Copyright © 2017 NYMITY Inc. All rights reserved. All text, images, logos, trademarks and information contained in this document are the intellectual property of Nymity Inc. unless otherwise indicated. Reproduction, modification, transmission, use or quotation of any content, including text, images, photographs etc., requires the prior written permission of Nymity Inc. Requests may be sent to info@nymity.com.

Omnibus Law Countries

Albania, Andorra, Angola, Antigua & Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, Bahamas, Belarus, Belgium, Benin, Bermuda, Bonaire/St. Eustatius/Saba, Bosnia & Herzegovina, Bulgaria, Burkina Faso, Canada, Cape Verde, Chad, Chile, Colombia, Costa Rica, Cote D'Ivoire, Croatia, Curacao, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Faroe Islands, Finland, France, Gabon, Germany, Georgia, Ghana, Gibraltar, Greece, Greenland, Guam, Guernsey, Hong Kong, Hungary, Iceland, India, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Kazakhstan, Kosovo, Kyrgyz Republic, Latvia, Lesotho, Liechtenstein, Lithuania, Luxembourg, Macao SAR, Macedonia, Madagascar, Malawi, Malaysia, Mali, Malta, Mauritius, Mexico, Moldova, Monaco, Montenegro, Morocco, Netherlands, New Zealand, Nicaragua, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, San Marino, Sao Tome and Principe, Senegal, Serbia, Seychelles, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, St. Lucia, St. Maarten, Sweden, Switzerland, Taiwan, Trinidad & Tobago, Tunisia, Turkey, Ukraine, United Kingdom, Uruguay

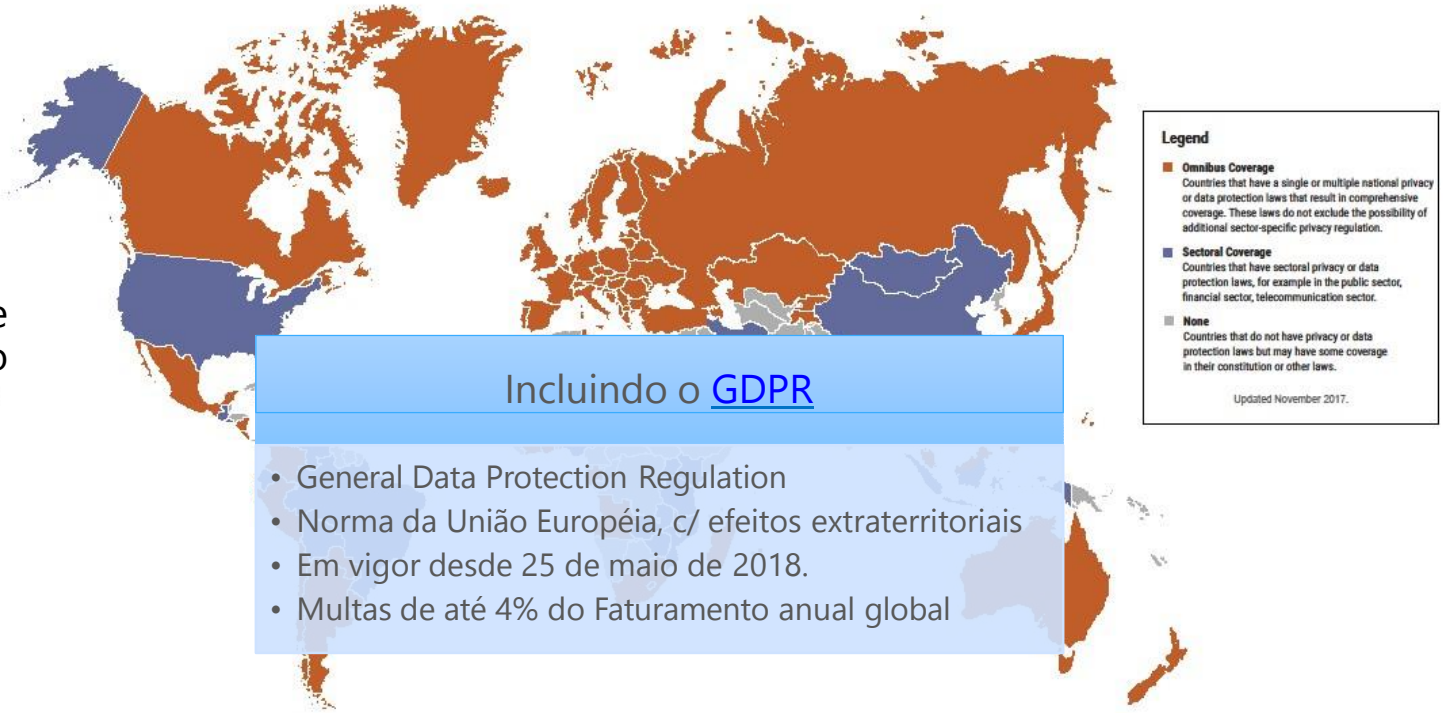
Sectoral Law Countries

Bahrain, Barbados, Bolivia, Bhutan, China, Ecuador, Guatemala, Indonesia, Iran, El Salvador, Jamaica, Kenya, Kuwait, Mongolia, Montserrat, Mozambique, Nigeria, Oman, Rwanda, Saudi Arabia, Tanzania, Uganda, Vanuatu, Venezuela, Vietnam, Zambia

Regulação

>100 leis no mundo regulamentando o que pode (ou não) ser feito com dados pessoais.

Sectoral and Omnibus Privacy and Data Protection Laws



Incluindo o GDPR

- General Data Protection Regulation
- Norma da União Européia, c/ efeitos extraterritoriais
- Em vigor desde 25 de maio de 2018.
- Multas de até 4% do Faturamento anual global

NYMITY RESEARCH™

Copyright © 2017 NYMITY Inc. All rights reserved. All text, images, logos, trademarks and information contained in this document are the intellectual property of Nymity Inc. unless otherwise indicated. Reproduction, modification, transmission, use or quotation of any content, including text, images, photographs etc., requires the prior written permission of Nymity Inc. Requests may be sent to info@nymity.com.

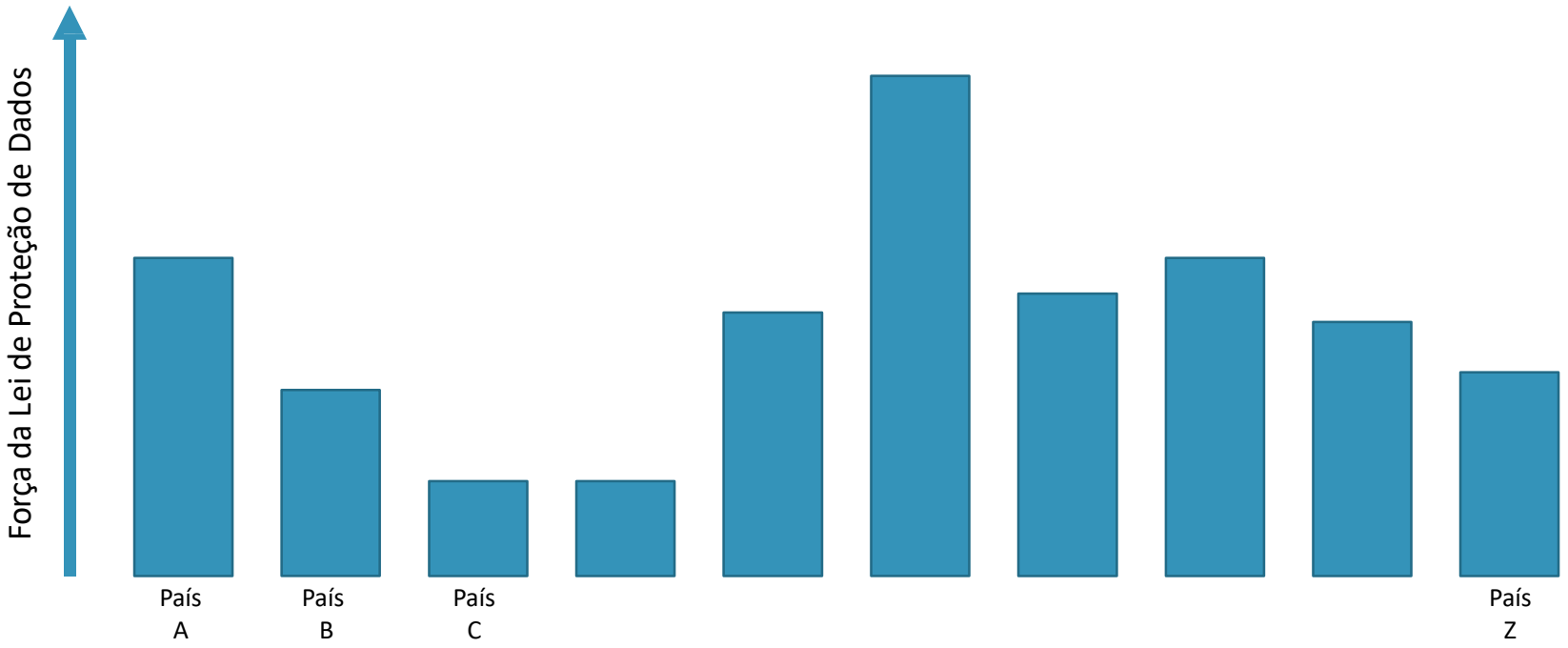
Omnibus Law Countries

Albania, Andorra, Angola, Antigua & Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, Bahamas, Belarus, Belgium, Benin, Bermuda, Bonaire/St. Eustatius/Saba, Bosnia & Herzegovina, Bulgaria, Burkina Faso, Canada, Cape Verde, Chad, Chile, Colombia, Costa Rica, Cote D'Ivoire, Croatia, Curacao, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Faroe Islands, Finland, France, Gabon, Germany, Georgia, Ghana, Gibraltar, Greece, Greenland, Guam, Guernsey, Hong Kong, Hungary, Iceland, India, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Kazakhstan, Kosovo, Kyrgyz Republic, Latvia, Lesotho, Liechtenstein, Lithuania, Luxembourg, Macao SAR, Macedonia, Madagascar, Malawi, Malaysia, Mali, Malta, Mauritius, Mexico, Moldova, Monaco, Montenegro, Morocco, Netherlands, New Zealand, Nicaragua, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, San Marino, Sao Tome and Principe, Senegal, Serbia, Seychelles, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, St. Lucia, St. Maarten, Sweden, Switzerland, Taiwan, Trinidad & Tobago, Tunisia, Turkey, Ukraine, United Kingdom, Uruguay

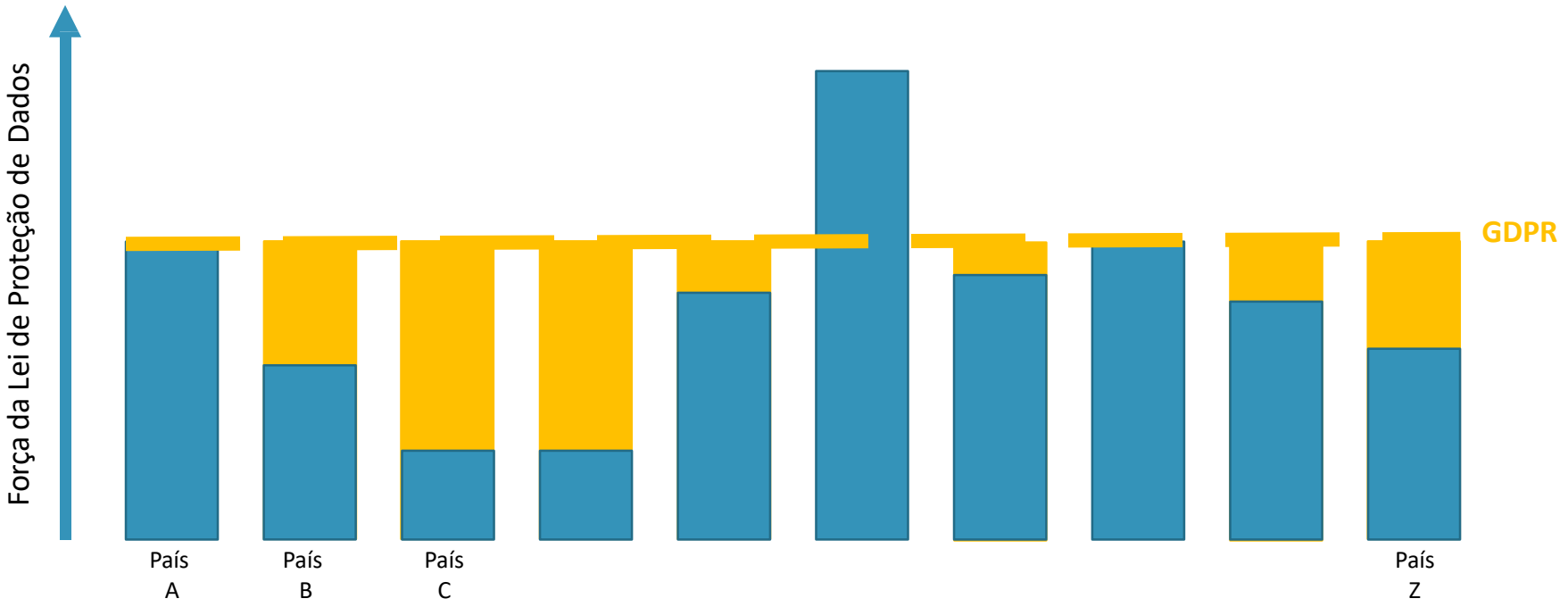
Sectoral Law Countries

Bahrain, Barbados, Bolivia, Bhutan, China, Ecuador, Guatemala, Indonesia, Iran, El Salvador, Jamaica, Kenya, Kuwait, Mongolia, Montserrat, Mozambique, Nigeria, Oman, Rwanda, Saudi Arabia, Tanzania, Uganda, Vanuatu, Venezuela, Vietnam, Zambia

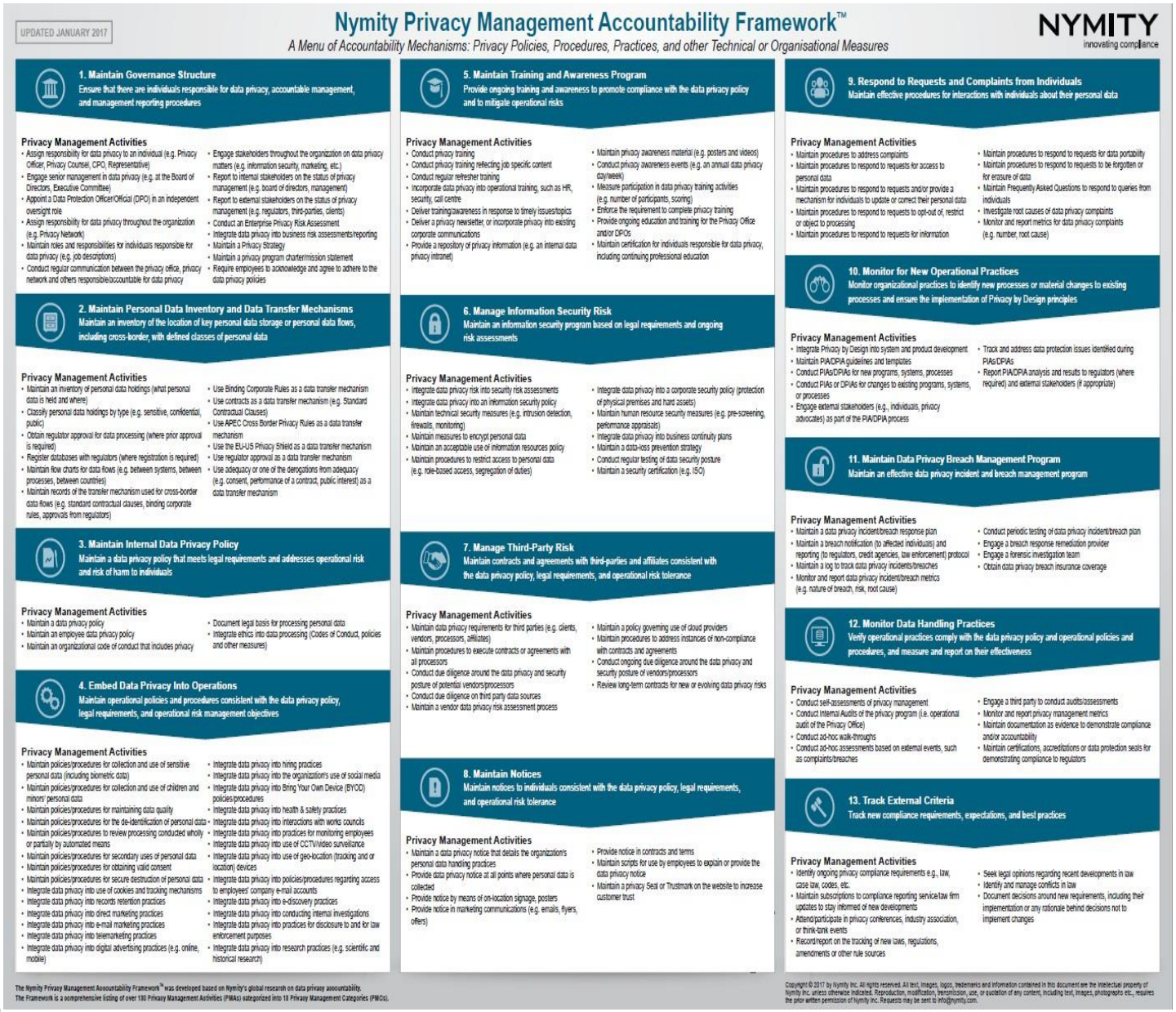
Abordagem Global



Abordagem Global



Estruturado conforme o Nymity Privacy Framework



UPDATED JANUARY 2017

Nymity Privacy Management Accountability Framework™

A Menu of Accountability Mechanisms: Privacy Policies, Procedures, Practices, and other Technical or Organisational Measures

NYMITY
innovating compliance

1. Maintain Governance Structure

Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

Privacy Management Activities

- Assign responsibility for data privacy to an individual (e.g. Privacy Officer, Privacy Counsel, CPO, Representative)
- Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)
- Appoint a Data Protection Officer/Official (DPO) in an independent oversight role
- Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)
- Maintain roles and responsibilities for individuals responsible for data privacy (e.g. job descriptions)
- Conduct regular communication between the privacy office, privacy network and others responsible/accountable for data privacy
- Engage stakeholders throughout the organization on data privacy matters (e.g. information security, marketing, etc.)
- Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)
- Report to external stakeholders on the status of privacy management (e.g. regulators, third-parties, clients)
- Conduct an Enterprise Privacy Risk Assessment
- Integrate data privacy into business risk assessments/reporting
- Maintain a Privacy Strategy
- Maintain a privacy program charter/mission statement
- Require employees to acknowledge and agree to adhere to the data privacy policies

2. Maintain Personal Data Inventory and Data Transfer Mechanisms

Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

Privacy Management Activities

- Maintain an inventory of personal data holdings (what personal data is held and where)
- Classify personal data holdings by type (e.g. sensitive, confidential, public)
- Obtain regulator approval for data processing (where prior approval is required)
- Register databases with regulators (where registration is required)
- Maintain flow charts for data flows (e.g. between systems, between processes, between countries)
- Maintain records of the transfer mechanism used for cross-border data flows (e.g. standard contractual clauses, binding corporate rules, approvals from regulators)
- Use Binding Corporate Rules as a data transfer mechanism
- Use contracts as a data transfer mechanism (e.g. Standard Contractual Clauses)
- Use APEC Cross Border Privacy Rules as a data transfer mechanism
- Use the EU-US Privacy Shield as a data transfer mechanism
- Use regulator approval as a data transfer mechanism
- Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism

3. Maintain Internal Data Privacy Policy

Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals

Privacy Management Activities

- Maintain a data privacy policy
- Maintain an employee data privacy policy
- Maintain an organizational code of conduct that includes privacy
- Document legal basis for processing personal data
- Integrate ethics into data processing (Codes of Conduct, policies and other measures)

4. Embed Data Privacy Into Operations

Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

Privacy Management Activities

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for collection and use of children and minors' personal data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into direct marketing practices
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into digital advertising practices (e.g. online, mobile)
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into practices for disclosure to and for law enforcement purposes
- Integrate data privacy into research practices (e.g. scientific and historical research)

5. Maintain Training and Awareness Program

Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

Privacy Management Activities

- Conduct privacy training
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training, such as HR, security, call centre
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information (e.g. an internal data privacy intranet)
- Maintain privacy awareness material (e.g. posters and videos)
- Conduct privacy awareness events (e.g. an annual data privacy day/week)
- Measure participation in data privacy training activities (e.g. number of participants, scoring)
- Enforce the requirement to complete privacy training
- Provide ongoing education and training for the Privacy Office and/or DPOs
- Maintain certification for individuals responsible for data privacy, including continuing professional education

6. Manage Information Security Risk

Maintain an information security program based on legal requirements and ongoing risk assessments

Privacy Management Activities

- Integrate data privacy risk into security risk assessments
- Integrate data privacy into an information security policy
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain measures to encrypt personal data
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)
- Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Integrate data privacy into business continuity plans
- Maintain a data-loss prevention strategy
- Conduct regular testing of data security posture
- Maintain a security certification (e.g. ISO)

7. Manage Third-Party Risk

Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)
- Maintain procedures to execute contracts or agreements with all processors
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Conduct due diligence on third party data sources
- Maintain a vendor data privacy risk assessment process
- Maintain a policy governing use of cloud providers
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct ongoing due diligence around the data privacy and security posture of vendors/processors
- Review long-term contracts for new or evolving data privacy risks

8. Maintain Notices

Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain a data privacy notice that details the organization's personal data handling practices
- Provide data privacy notice at all points where personal data is collected
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. emails, flyers, offers)
- Provide notice in contracts and terms
- Maintain scripts for use by employees to explain or provide the data privacy notice
- Maintain a privacy Seal or Trustmark on the website to increase customer trust

9. Respond to Requests and Complaints from Individuals

Maintain effective procedures for interactions with individuals about their personal data

Privacy Management Activities

- Maintain procedures to address complaints
- Maintain procedures to respond to requests for access to personal data
- Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data
- Maintain procedures to respond to requests to opt-out of, restrict or object to processing
- Maintain procedures to respond to requests for information
- Maintain procedures to respond to requests for data portability
- Maintain procedures to respond to requests to be forgotten or for erasure of data
- Maintain Frequently Asked Questions to respond to queries from individuals
- Investigate root causes of data privacy complaints
- Monitor and report metrics for data privacy complaints (e.g. number, root cause)

10. Monitor for New Operational Practices

Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

Privacy Management Activities

- Integrate Privacy by Design into system and product development
- Maintain PIA/DPIA guidelines and templates
- Conduct PIAs/DPIAs for new programs, systems, processes
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes
- Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process
- Track and address data protection issues identified during PIAs/DPIAs
- Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)

11. Maintain Data Privacy Breach Management Program

Maintain an effective data privacy incident and breach management program

Privacy Management Activities

- Maintain a data privacy incident/breach response plan
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol
- Maintain a log to track data privacy incidents/breaches
- Monitor and report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage

12. Monitor Data Handling Practices

Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness

Privacy Management Activities

- Conduct self-assessments of privacy management
- Conduct Internal Audits of the privacy program (i.e. operational audit of the Privacy Office)
- Conduct ad-hoc walk-throughs
- Conduct ad-hoc assessments based on external events, such as complaints/breaches
- Engage a third party to conduct audits/assessments
- Monitor and report privacy management metrics
- Maintain documentation as evidence to demonstrate compliance and/or accountability
- Maintain certifications, accreditations or data protection seals for demonstrating compliance to regulators

13. Track External Criteria

Track new compliance requirements, expectations, and best practices

Privacy Management Activities

- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments
- Attend/participate in privacy conferences, industry association, or think-tank events
- Record/report on the tracking of new laws, regulations, amendments or other rule sources
- Seek legal opinions regarding recent developments in law
- Identify and manage conflicts in law
- Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes

The Nymity Privacy Management Accountability Framework™ was developed based on Nymity's global research on data privacy accountability.
The Framework is a comprehensive listing of over 130 Privacy Management Activities (PMAs) categorized into 13 Privacy Management Categories (PMCs).

Copyright © 2017 by Nymity Inc. All rights reserved. All text, images, logos, trademarks and information contained in this document are the intellectual property of Nymity Inc. unless otherwise indicated. Reproduction, modification, transmission, use, or quotation of any content, including text, images, photographs etc., requires the prior written permission of Nymity Inc. Requests may be sent to info@nymity.com.

Dividido em
13 categorias

O que é o GPP?

O GPP é o Programa Global de Privacidade da PMI

- Busca garantir conformidade com as legislações de proteção de dados pessoais.
- GDPR é a régua de análise.
- Liderado conjuntamente por IS e Jurídico.

O papel do Líder de Privacidade de Dados (DPL)

Qual é o papel do DPL?

- **Lidera a implementação local** do Programa Global de Privacidade (GPP), o que inclui:
  - Garantir que os colaboradores **conheçam** as normas aplicáveis.
  - Manter o **inventário** de atividades de processamento de dados.
  - Monitorar o **compliance** com as diretrizes de proteção.
  - Oferecer **orientação** em relação às obrigações relacionadas ao processamento de dados pessoais.
- **É um papel, uma responsabilidade – não uma função.**

NOSSO PROGRAMA GLOBAL DE PRIVACIDADE (GPP)

Promoção de uma Cultura de Privacidade

- PMI 03-C – Política de Proteção de Dados Pessoais da PMI.
- Plano de comunicação.
- Treinamentos presenciais para funções chave. Vídeos e e-learning para as demais.
- Comunicação do CIO e CEO para a liderança.

Inventário de Dados Pessoais

O ponto de partida de diversas outras atividades dentro do GPP. É também uma obrigação prevista na GDPR.

O Inventário serve para mapear todos os dados pessoais aos quais a empresa tem acesso, seja por meio de:

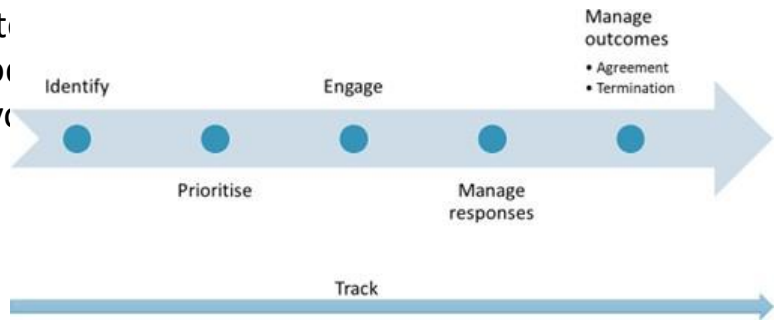
- Processos
- Sistemas
- Terceiros
- Informação não estruturada
- Arquivos físicos

CLASSE	DESCRIÇÃO	EXEMPLO
A	Dados declarados como "sensíveis" pela legislação.	• Opiniões políticas
	Outros dados pessoais que poderiam acarretar sérias consequências se perdidos ou revelados para terceiros	• Cartões de crédito • Dados Bancários • CPF
B	Dados pessoais gerais que não sejam do tipo "A" ou "B"	• Pedidos do consumidor • "Grade" do empregado
C	Contatos de negócio e dados de acesso a sistemas necessários para interações padrão com a PMI e seus parceiros de negócio aprovados.	• Cargo, e-mail de trabalho e centro de custo.

Nenhum tipo de processamento de dados deve ser feito sem sua inclusão no inventário!

Ajustes de Contrato

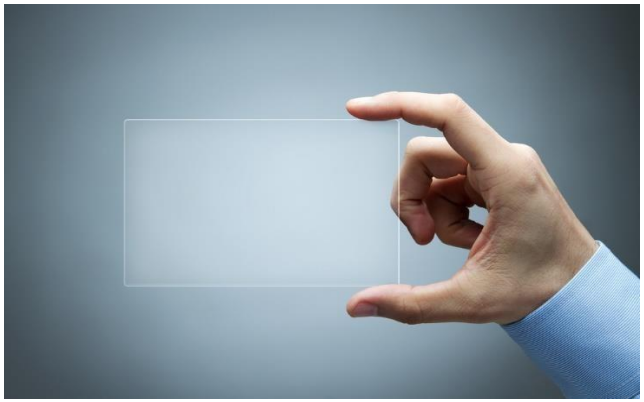
- Desenvolvimento de cláusulas padrão.
- Definição de prioridades para o aditamento de contratos existentes.
- Inclusão de cláusulas padrão de prot
  to
  env



Acordo de Confidencialidade <> Cláusula de Proteção de Dados <> Acordos de Transferência de Dados <> Security Schedule

Políticas e Avisos de Privacidade

A transparência é **conceito-chave** de compreensão da GDPR.

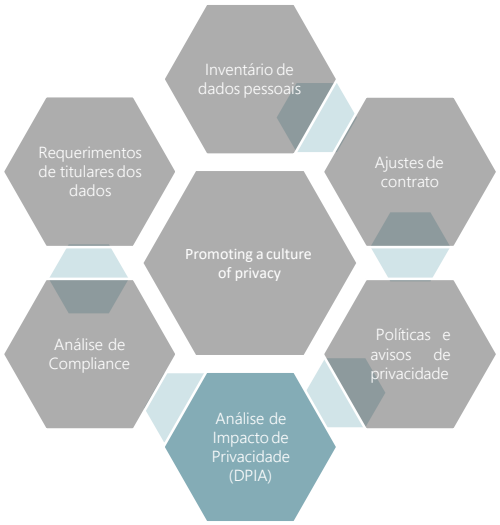


Devemos informar quando coletamos informações pessoais, para que fim e por quanto tempo iremos armazená-las.

Esta informação deve estar disponível em um formato que seja **acessível**, de **fácil compreensão** e que use **linguagem simples e direta**.

E nada de políticas gerais – elas sempre devem ser específicas à situação e ao interlocutor pretendido.

Análise de Impacto de Privacidade (DPIA)



DPIA é uma análise de risco

- Na perspectiva do indivíduo.

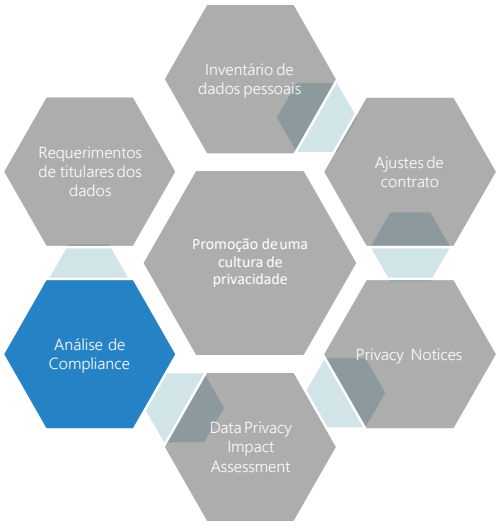
DPIA ajuda a identificar:

- Quais são os riscos a um indivíduo de determinado processamento de dados pessoais?
- A atividade atinge um equilíbrio entre proteger a privacidade de dados pessoais e o legítimo interesse de negócio?

DPIA é necessário <u>antes</u>:

- Iniciar uma nova atividade que envolva o processamento de dados pessoais.
- Modificar substancialmente uma atividade existente que envolva o processamento de dados pessoais.

Análise de Compliance



Análise de Compliance de Privacidade

- Como nós analisamos que estamos em conformidade e garantimos que iremos permanecer em conformidade.
- Capturar evidências.
- Endereçar eventuais oportunidades.

3 dimensões

- **Atividade:** questões relacionadas à minimização dos dados necessários e à sua manutenção apenas pelo tempo estritamente necessário.
- **Sistema:** questões relacionadas à acesso e criptografia.
- **Terceiros:** questões relacionadas à contrato e *due diligence* do fornecedor/prestador.

Análise continua baseada em risco

Requerimentos de Titulares dos Dados

- Mapear pontos de contato com titulares de dados para processar requerimentos de titulares (ex: acesso, retificação, exclusão).
- Estabelecer fluxos. Manter evidências.
- Treinar os envolvidos.
- Ter procedimentos claros para gerenciamento de crise.

HANDLING A POTENTIAL PERSONAL DATA BREACH?

WHAT IS A PERSONAL DATA BREACH?

It is when someone, internal or external, gets unauthorized access to personal data

It could for example be the result of a hacking attempt but equally it could be an e-mail sent to an unintended person or documents forgotten in a photocopier

WHY IS THIS IMPORTANT?

A personal data breach can have serious impacts on the individuals whose data has been exposed

It can have also serious consequences for PMI in terms of for example fines and reputational harm

In case of a potential data breach it is important to act quickly to protect individuals and PMI

Laws impose strict timelines on how quickly a company must respond, including potentially informing authorities and the individual concerned with 72 hours

WHAT MUST YOU TO DO IF YOU SUSPECT A POTENTIAL PERSONAL DATA BREACH?

EQUÍVOCOS COMUNS

- Dado pessoal = Dado pessoalmente identificável.
- O significado de processamento.
- Aplicabilidade do GDPR fora da União Europeia.
- A privacidade de dados como um problema de IS, Jurídico ou Compliance.
- O GDPR como ato contínuo.

...E ALGUMAS DICAS FINAIS

- Comece cedo!
- Engaje a liderança.
- Trabalhe com um time multifuncional.
- Abrace a incerteza – e discuta.
- Priorize, priorize, priorize.

Obrigado!

Vinicius Gehlen (Especialista Segurança da Informação na Phillip Morris) - Vinicius.Gehlen@pmi.com
Valeska Chrestani (Advogada na Phillip Morris) - Valeska.Chrestani@pmi.com
Rogério Moleiro (Diretor de Ética e *Compliance* na Phillip Morris)

Reuniões em 2018

1º Encontro

- ✓Criação e objetivos da Rede (Sistema Fiep).
- ✓Resultados Pesquisa Maturidade Compliance (KPMG).
- ✓36 participantes.

2º Encontro

- ✓Palestra Lei Anticorrupção (VG&P Advogados).
- ✓*Case* de implementação da área de *Compliance* (Itaipu Binacional).
- ✓33 participantes.

3º Encontro

- ✓Palestra Inovações Tecnológicas no *Compliance* (Gerência Inovação Sistema Fiep).
- ✓*Case* Grupo Marista (Diretoria de Auditoria, Riscos e *Compliance*).
- ✓50 participantes.

4º Encontro – *86 confirmados

* Dados do dia 30/11

Entregas de 2018

REDE PARANAENSE DE COMPLIANCE EM 2018

Planejamento de Temas com base nas solicitações do 1º encontro

Definição de Comitê Técnico

Regulamento

Site da Rede

Avaliação em Grupo

1. O QUE FOI BOM?

Que coisas ocorreram durante este ano na Rede Paranaense de Compliance e que merecem destaque?

2. O QUE DEVEMOS MELHORAR?

Quais os aspectos construídos que poderiam ser melhores ou diferentes para o próximo ano?

3. SOBRE O QUE DEVEMOS FALAR?

Quais os temas você julga importante debatermos em 2019?

Avaliação Individual

3. Por favor, classifique as seguintes afirmações utilizando a escala numérica de concordo plenamente (5) para discordo totalmente (1).

	Concordo plenamente 5	Concordo 4	Neutro 3	Discordo 2	Discordo plenamente 1
As informações apresentadas neste evento eram novas para mim.	○	○	○	○	○
O conteúdo do evento é relevante para o meu trabalho.	○	○	○	○	○
É provável que eu use as informações adquiridas.	○	○	○	○	○
No geral, o evento foi muito útil.	○	○	○	○	○
Eu vou recomendar este evento para um colega.	○	○	○	○	○
O palestrante demonstrou domínio do conteúdo.	○	○	○	○	○

4. Por favor, deixe seus comentários adicionais a respeito desse seminário e, se quiser, sugira temas para futuros eventos.

Próxima Reunião

Primeira quinzena de março
(a confirmar)

Campus da Indústria

8:30 às 11:00

Sistema Fiep

FIEP
SESI
SENAI
IEL

nosso i é de indústria.