Cyber Risks e a LGPD

Marcia Cicarelli

8º Encontro de Resseguro – Abril/2019

DEMAREST

Lei Geral de Proteção de Dados – LGPD

Lei nº 13.709, de 14 de agosto de 2018

Dispõe sobre a proteção do tratamento de **dados pessoais**, inclusive nos meios digitais, e altera a Lei nº 12.965/2014 (Marco Civil da Internet)

Inspirada na legislação europeia (*General Data Protection Regulation – GDPR*)

Recentemente modificada pela **Medida Provisória nº 869, de 27 de dezembro de 2018**

- Criação da Autoridade Nacional de Proteção de Dados (ANPD)
- Alteração do período de vacância da lei para 24 meses

Entrará em vigor a partir de **15 DE AGOSTO DE 2020**

Lei Geral de Proteção de Dados – LGPD

Lei nº 13.709, de 14 de agosto de 2018

- *Background* da proteção de dados no Brasil:

Normas esparsas: Constituição Federal, Código Civil, Código de Defesa do Consumidor, Lei nº 12.965/2014 (Marco Civil da Internet) e Decreto Regulamentador nº 8.771/2016

Portaria Normativa nº 539 do MP/DFT: Comissão de Proteção de Dados Pessoais (Novembro/2017)

MPF: Instauração de inquéritos civis e recomendações (*Netshoes*, *Uber*)

DEMAREST

Lei Geral de Proteção de Dados – LGPD

Lei nº 13.709, de 14 de agosto de 2018

- O que precisamos saber sobre a nova lei?

ABRANGÊNCIA	PROTEÇÃO	INFORMAÇÃO	SANÇÕES (Art. 52)
• Toda pessoa natural ou jurídica (direito público ou privado) que realize qualquer tratamento de dados pessoais (**Art. 1º**)	• O tratamento de dados pessoais deve observar 10 princípios **(Art. 6º)** • O tratamento de dados pessoais é autorizado	• Toda empresa deverá nomear o Encarregado (DPO – *Data Protection Officer*) **(Art. 41)** • Dever de notificação de	• Advertência • Multa de 2% sobre o faturamento do grupo no Brasil (máx. **R$ 50 milhões**) por infração

Lei Geral de Proteção de Dados – LGPD

Lei nº 13.709, de 14 de agosto de 2018

- Principais definições **(Art. 5º)**:

DADOS PESSOAIS	DADOS SENSÍVEIS	TRATAMENTO	AGENTES
• Qualquer informação relacionada à pessoa natural (identificada ou identificável) • "*Dado anonimizado*": relativo a um titular que não possa mais ser identificado, após o seu tratamento, em função do uso de meios para a anonimização de dados	• Dados pessoais que tenham relação com a origem racial ou étnica, credo, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político; que se referem à saúde ou vida sexual, e dados genéticos e biométricos	• Toda operação que seja realizada com os dados pessoais (incluindo: uso, coleta, produção, recepção, classificação, acesso, processamento, avaliação, distribuição, reprodução, difusão, extração, transmissão, armazenamento etc.)	• ***Controlador***: aquele a quem competem as decisões referentes ao tratamento de dados • ***Operador***: aquele que realiza o tratamento de dados pessoais em nome do Controlador • ***Encarregado (DPO)***: responsável frente à ANPD e aos titulares

Lei Geral de Proteção de Dados – LGPD

Lei nº 13.709, de 14 de agosto de 2018

- O que autoriza o tratamento de dados pessoais?

Consentimento do titular

Cumprimento de obrigação legal

Execução de políticas públicas

Estudos por órgãos de pesquisa

Execução de contratos

Exercício regular de direitos

Proteção da vida

Tutela da saúde

Interesse legítimo do Controlador

Proteção ao crédito

Lei Geral de Proteção de Dados – LGPD

Lei nº 13.709, de 14 de agosto de 2018

- O que fazer diante de um incidente de segurança ou vazamento de dados?

NOTIFICAÇÃO	DESCRIÇÃO	IDENTIFICAÇÃO	MITIGAÇÃO
• A ANPD deverá ser notificada em "prazo razoável" (que será definido por ela) • **ATENÇÃO**: eventuais demoras deverão ser justificadas!	• A comunicação do incidente/vazamento deverá descrever a natureza dos dados pessoais afetados	• Devem ser enviadas informações sobre os titulares dos dados envolvidos para se avaliar o alcance e o risco do incidente ou do vazamento	• Devem ser indicadas à ANPD todas as medidas técnicas e de segurança que foram adotadas para proteção dos dados / mitigação dos riscos

Lei Geral de Proteção de Dados – LGPD

Lei nº 13.709, de 14 de agosto de 2018

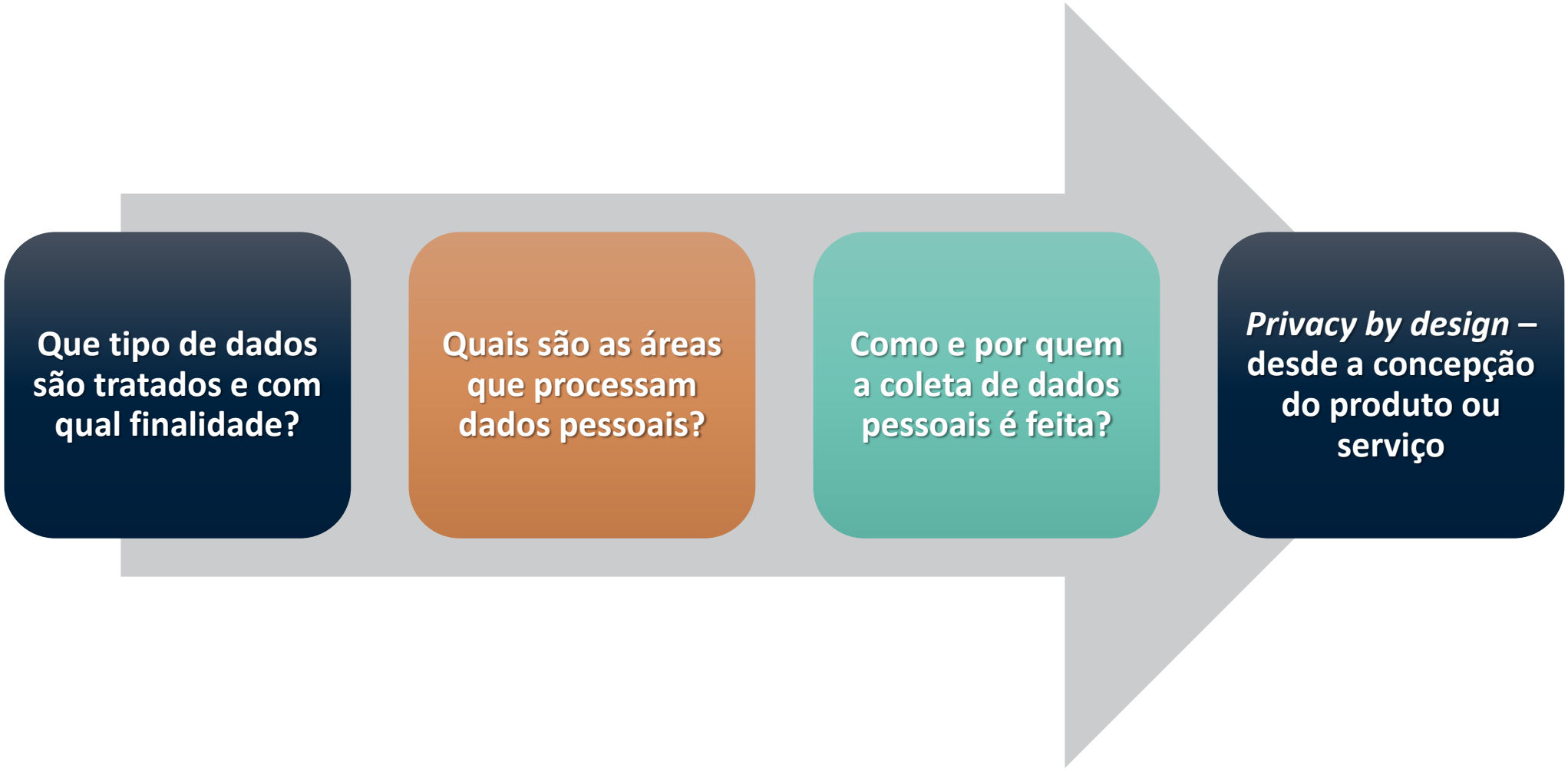
- **ANPD**: órgão da Presidência da República (receberá apoio da Casa Civil até sua estruturação)
- Estrutura: **Conselho Diretor** (5 membros com mandato de 2, 3, 4, 5 e 6 anos – conforme nomeação)
  + **Conselho Nacional de Proteção de Dados Pessoais e da Privacidade** (23 representantes ao todo)
- Competências da ANPD que afetarão o mercado segurador e ressegurador:

- Decidir reclamações dos titulares de dados
- Avaliar o nível de proteção de dados de países terceiros
- Autorizar a transferência internacional de dados
- Definir cláusulas-contratuais padrão
- Analisar as regras corporativas e de códigos de conduta
- Receber notificações de incidentes de segurança
- Definir os procedimentos a serem adotados para mitigação de um incidente de segurança ou de vazamento de dados
- Aplicar sanções aos agentes de tratamento
- Etc.

DEMAREST

Impactos no Mercado Segurador e Ressegurador

Fluxo de Dados

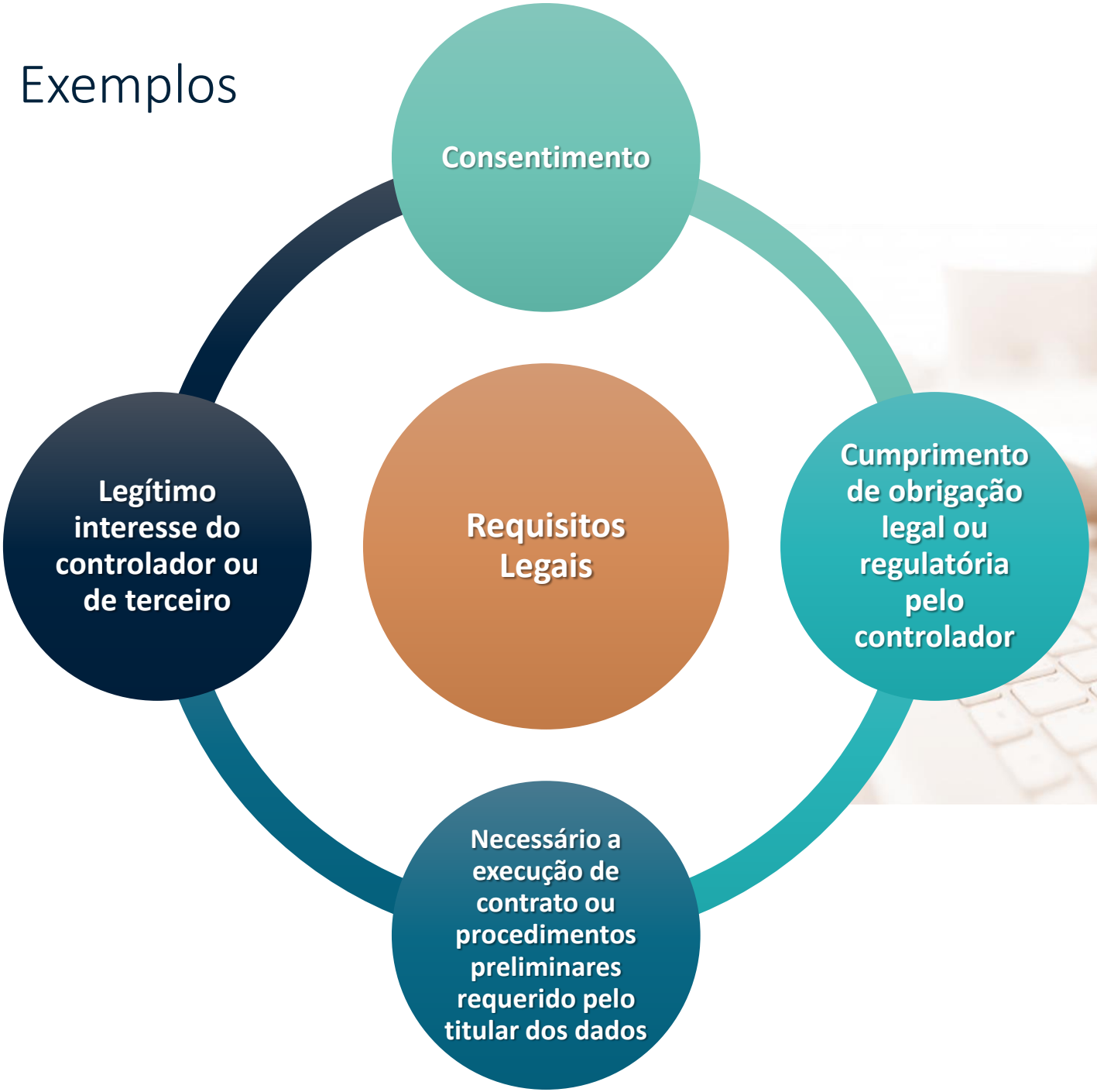


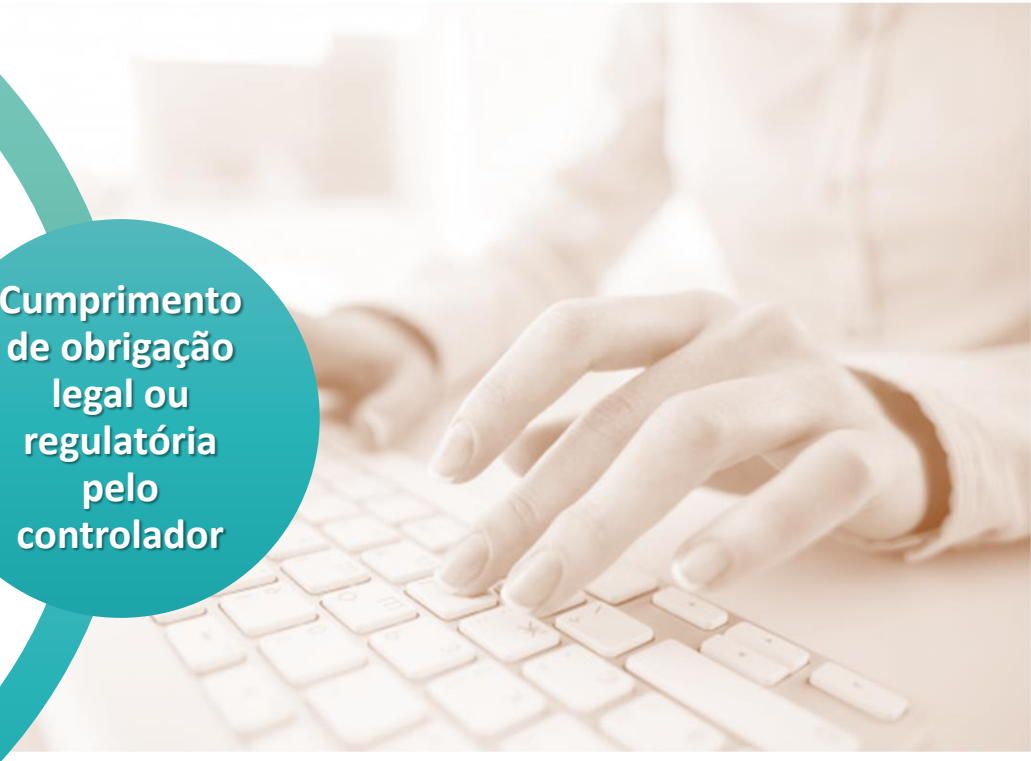
Exemplo de Áreas Envolvidas

- **JURÍDICO >> IDENTIFICAR A APLICABILIDADE DA LEI E AS CIRCUNSTÂNCIAS PARA TRATAMENTO:**
- **COMPLIANCE**
- **TI E SEGURANÇA CIBERNÉTICA>> TI INFRAESTRUTURA E OPERAÇÕES**
- **RECURSOS HUMANOS**
- **COMUNICAÇÃO E MARKETING**
- **P&D / ENGENHARIA / PRODUTO**

Tratamento de Dados

Exemplos


Consentimento
Legítimo interesse do controlador ou de terceiro
Requisitos Legais
Cumprimento de obrigação legal ou regulatória pelo controlador
Necessário a execução de contrato ou procedimentos preliminares requerido pelo titular dos dados



Lei Geral de Proteção de Dados – LGPD

Lei nº 13.709, de 14 de agosto de 2018

- Quais são os impactos para o mercado segurador e ressegurador?

TRANSFERÊNCIA INTERNACIONAL	RESPONSABILIDADE	DADOS SENSÍVEIS	VANTAGEM ECONÔMICA
• Dados não podem ser enviados para países que não têm os mesmos níveis de segurança que o BR (ANPD = avaliação) • Consentimento específico?	• É possível haver a responsabilização por um vazamento ocorrido após envio dos dados para os parceiros comerciais (inclusive de forma solidária entre eles) • Definição de responsabilidades e ação de regresso	• A sua transmissão ao ressegurador precisa de consentimento do titular dos dados? • Contratação *vs*. Sinistro?	• A comunicação ou o uso compartilhado de dados pessoais sensíveis é vedada, exceto se houver *consentimento* do titular dos dados

Boas Práticas e Medidas Adicionais Sugeridas

Procedimentos para reclamações dos titulares de dados	**Ações educativas**	**Mecanismos internos de supervisão e de mitigação de riscos**	**Programas de governança em privacidade**
Política de Melhores Práticas e Governança	**Seguro**	**Contratos de tratamento de dados**	**Canal de comunicação**
Procedimentos e respostas a incidentes	**Revisão de cláusulas e contratos com terceiros (fornecedores/ clientes)**	**Aspectos trabalhistas**	**Sistemas de segurança**

DEMAREST

Seguro de *Cyber*: Riscos Cibernéticos

Seguro de Riscos Cibernéticos

Aspectos gerais

Cobertura de seguro compreensiva

FIRST-PARTY: danos sofridos pelo próprio segurado

+

THIRD-PARTY: responsabilidade civil do segurado por danos causados a terceiros

Seguro de Riscos Cibernéticos

Cobertura securitária

- Responsabilidade por dados pessoais e dados corporativos
- Responsabilidade por terceirizadas (Controlador *vs.* Operador)
- Responsabilidade por erro ou omissão na segurança de dados
- Custos de defesa

Seguro de Riscos Cibernéticos

Cobertura securitária

Custos de notificação, monitoramento e mitigação de um incidente

Custos de restituição de imagem corporativa ou pessoal

Proteção por interrupção de rede

Custos de extorsão na internet

Seguro de Riscos Cibernéticos

Principais exclusões

Atos ilícitos dolosos ou com culpa grave do Segurado

Danos Materiais e Danos Corporais causados a terceiros

Lucros cessantes em operações financeiras

Reconstrução de dados

Seguro de Riscos Cibernéticos

Tendências do mercado

- O que podemos aprender com a GDPR?

PRINCIPAIS SETORES-ALVO EM 2018

Saúde

41%

Instituições financeiras

20%

Educação

10%

Outros serviços profissionais

7%

PRINCIPAIS CAUSAS DE INCIDENTES EM 2018

Hackers ou *Malwares*

47%

Vazamentos acidentais

20%

Insiders

9%

Social engineering

8%

Dispositivos portáteis

6%

Perdas de documentos físicos

5%

Fonte: *Beazley Breach Briefing – 2019 (Março/2019)*

Seguro de Riscos Cibernéticos

Desafios e reflexões

- Desafios da subscrição / especificidades de cada indústria
- Questionários: informação *vs.* simplicidade
- Concorrência de apólices (E&O, D&O, etc.)
- Dever de notificação e demais obrigações da LGPD *vs.* agravamento de risco
- Apólice de serviços *vs*. responsabilidade da seguradora por prestadores?
- Incidente de segurança *vs*. sinistro
- Protocolos de resposta e sinistro

OBRIGADA!

Marcia Cicarelli Barbosa de Oliveira
mcicarelli@demarest.com.br
+55 (11) 3356-1825

demarest.com.br

DEMAREST