XVII ENCONTRO NACIONAL
DE CONTROLE INTERNO

DESAFIOS DA LGPD AO PODER PÚBLICO E O PAPEL DAS CONTROLADORIAS

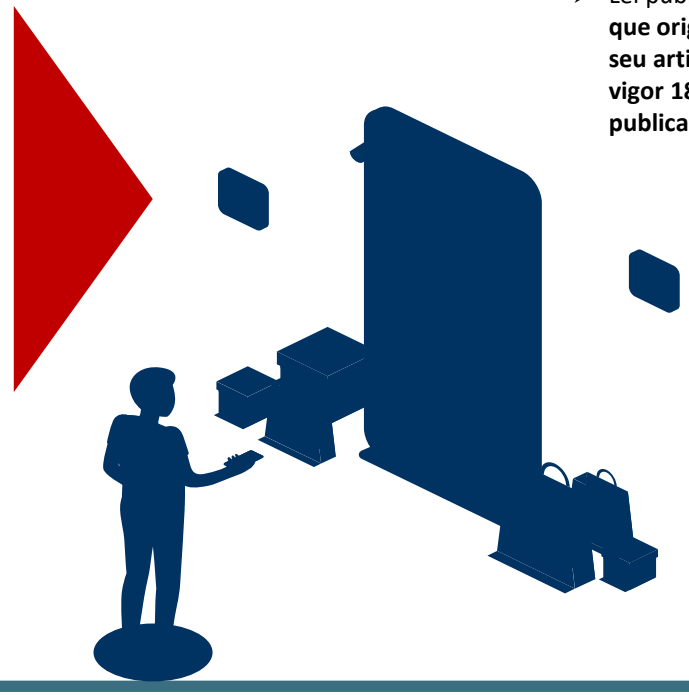
Rodrigo Pironti

Pós-Doutor em Direito Público – Complutense Madrid
Doutor e Mestre em Direito Econômico – PUCPR
Sócio do escritório Pironti Advogados

Google™

– Alô, é da pizzaria Gordon?
– Não, senhor, é da pizzaria Google.
– Desculpe, devo ter ligado para o número errado.
– Não o número está correto, o Google comprou a pizzaria.
– Ah, entendi. Pode anotar o meu pedido?
– Claro, o senhor quer a pizza de sempre?
– Como assim, você já trabalhava aí, me conhece?
– É que de acordo com nossos sistemas, nas últimas 12 vezes o senhor pediu pizza de salame com queijo, massa grossa e bordas recheadas.
– Isso, pode fazer essa mesma.
– No lugar dessa posso tomar a liberdade de sugerir uma de massa fina, farinha integral, de ricota e rúcula com tomate seco?
– Não, eu odeio vegetais!
– Mas o seu colesterol está muito alto.
– Quem te disse isso? Como você sabe?
– Nós acompanhamos os exames laboratoriais de nossos clientes e temos todos os seus resultados dos últimos 7 anos.
– Entendi, mas quero a pizza de sempre, eu tomo remédios para controlar o colesterol.
– O senhor não está tomando regularmente, porque nos últimos 4 meses só comprou uma caixa com 30 comprimidos, na farmácia do seu bairro.
– Comprei mais em outra farmácia.
– No seu cartão de crédito não aparece.
– Eu paguei em dinheiro.
– Mas de acordo com seu extrato bancário o senhor não fez saque no caixa automático nesse período.
– Eu tenho outra fonte de renda.
– Isso não está constando na sua Declaração de Imposto de Renda, a menos que seja uma fonte pagadora não declarada.
– Mas que inferno! Estou cansado de ter minha vida vigiada e vasculhada pelo Google, Facebook, Twitter, WhatsApp, essas porcarias todas! Vou mudar para uma ilha sem internet e sem telefone celular, onde ninguém possa me espionar.
– A decisão é sua, senhor, mas quero lhe avisar que seu passaporte venceu há 5 semanas...

VIGÊNCIA DA LGPD:



- Lei publicada em **14/08/2018 que originalmente trazia em seu artigo 65 a entrada em vigor 18 meses após a publicação;**
- MP869/18, convertida na Lei 13,853/19, prorrogou a vacância por **mais 6 meses, para 08/2020;**
- PL1179/20, transformado na Lei 14.010/2020, **postergou somente a vigência das sanções para 08/21;**

SANÇÕES AGO/21

- MP 959/20 buscava prorrogar novamente a vigência da lei (para 05/21) mas o Senado declarou prejudicado ao art. 4° do projeto de lei de conversão.

VIGÊNCIA 18/09/20

O que se pretende proteger?

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.**

LGPD (LEI 13.709/18)

versus

LAI (LEI 12.527/11)

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

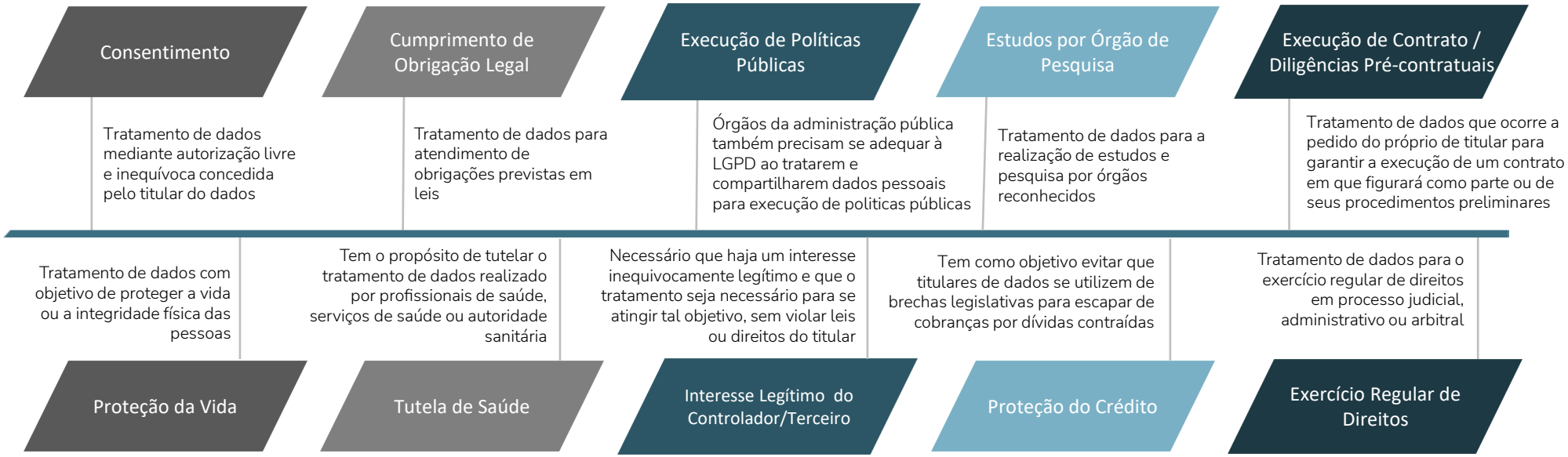
II - poderão ter autorizada sua divulgação ou acesso por terceiros **diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.**

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
III - ao cumprimento de ordem judicial;
IV - à defesa de direitos humanos; ou
V - à proteção do interesse público e geral preponderante.

Bases Legais para Tratamento de Dados

A LGPD não proíbe a coleta e tratamento de dados pessoais, desde que a finalidade esteja fundamentada em alguma das bases legais



Art. 7º O tratamento de dados pessoais **somente poderá ser realizado nas seguintes hipóteses**:

III - **pela administração pública**, para o tratamento e uso compartilhado de **dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres**, observadas as disposições do Capítulo IV desta Lei;

Art. 23. O tratamento de dados pessoais **pelas pessoas jurídicas de direito público** referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o **atendimento de sua finalidade pública**, na persecução do interesse público, com o **objetivo de executar as competências**

CONSENTIMENTO?

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

[...]

III - seja indicado um encarregado quando realizarem operações de tratamento

COMPARTILHAMENTO

Art. 25. Os dados deverão ser mantidos em formato **interoperável e estruturado** para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O **uso compartilhado** de dados pessoais pelo Poder Público **deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas**, respeitados os princípios de proteção de dados pessoais elencados no art. 6o desta Lei.

VEDAÇÕES AO COMPARTILHAMENTO

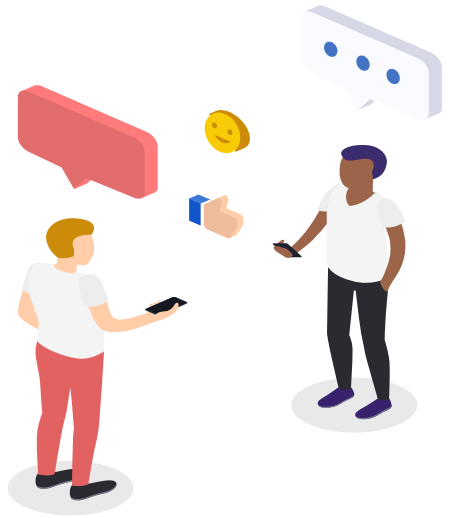
§ 1o É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: (...)

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei no 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;

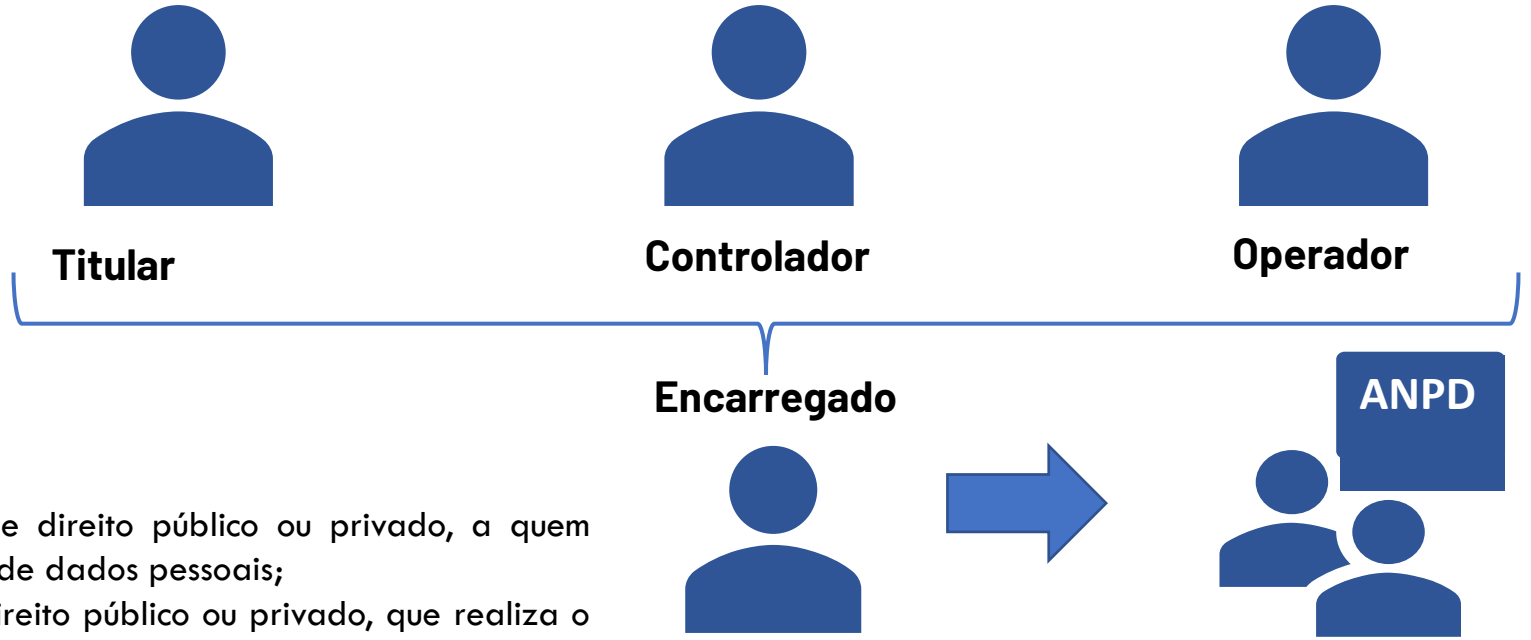
IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e

ESTRUTURA DE GOVERNANÇA DE DADOS



Agentes da Relação no Tratamento de Dados



Art. 5º Para os fins desta Lei, considera-se:
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

INSTRUÇÃO NORMATIVA SGD/ME Nº 117, DE 19 DE NOVEMBRO DE 2020

Art. 1. § 1º O Encarregado pelo Tratamento dos Dados Pessoais indicado:

I - deverá possuir conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente, os relativos aos temas de: privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público; e

II - não deverá se encontrar lotado nas unidades de Tecnologia da Informação ou ser gestor responsável de sistemas de informação do órgão ou da entidade.

Art. 42. O **controlador ou o operador** que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, **é obrigado a repará-lo**.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular **quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes**, entre as quais:

I - **o modo pelo qual é realizado**;

II - o resultado e os **riscos que razoavelmente dele se esperam**;

III - as **técnicas de tratamento** de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. **Responde pelos danos** decorrentes da violação da segurança dos dados o **controlador ou o operador que, ao deixar de adotar as medidas de segurança** previstas no art. 46 desta Lei, der causa ao dano.

COMO PROVAR?
COMO NÃO SE OMITIR?

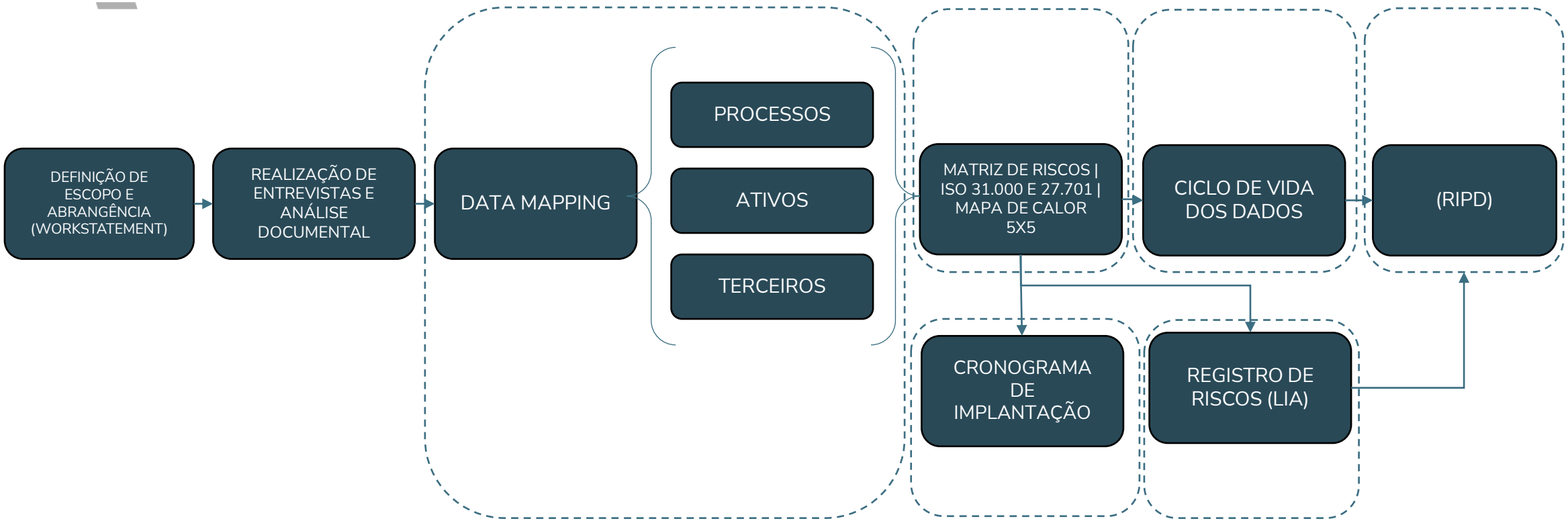
Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.

Art. 5º Para os fins desta Lei, considera-se:

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

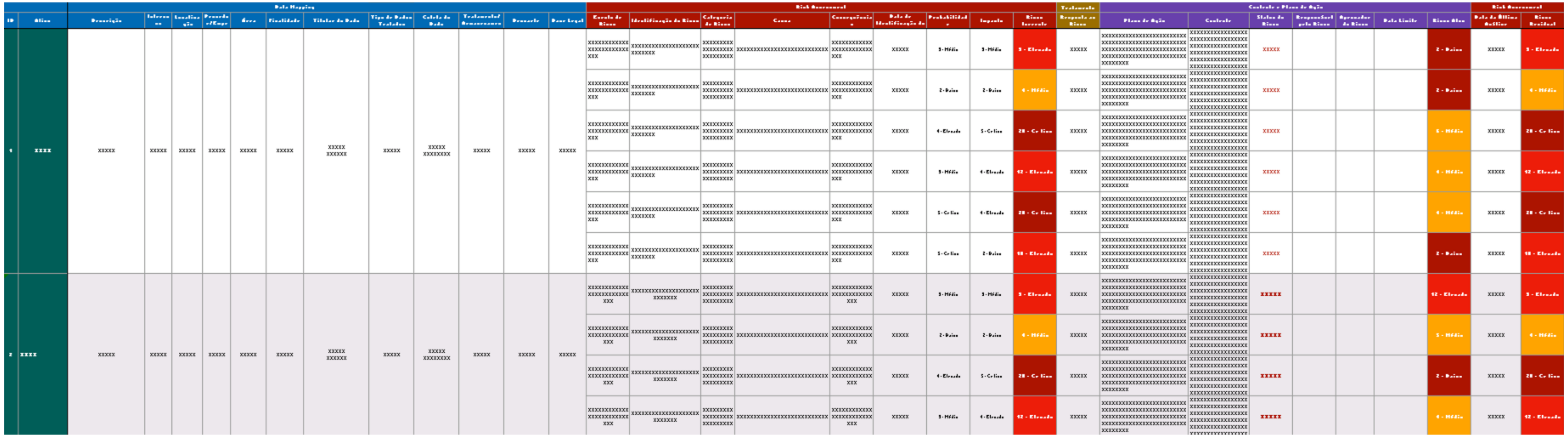
ASPECTOS PRÁTICOS DE IMPLANTAÇÃO
FRAMEWORK MÍNIMO

Fluxo de Trabalho para elaboração do RIPD

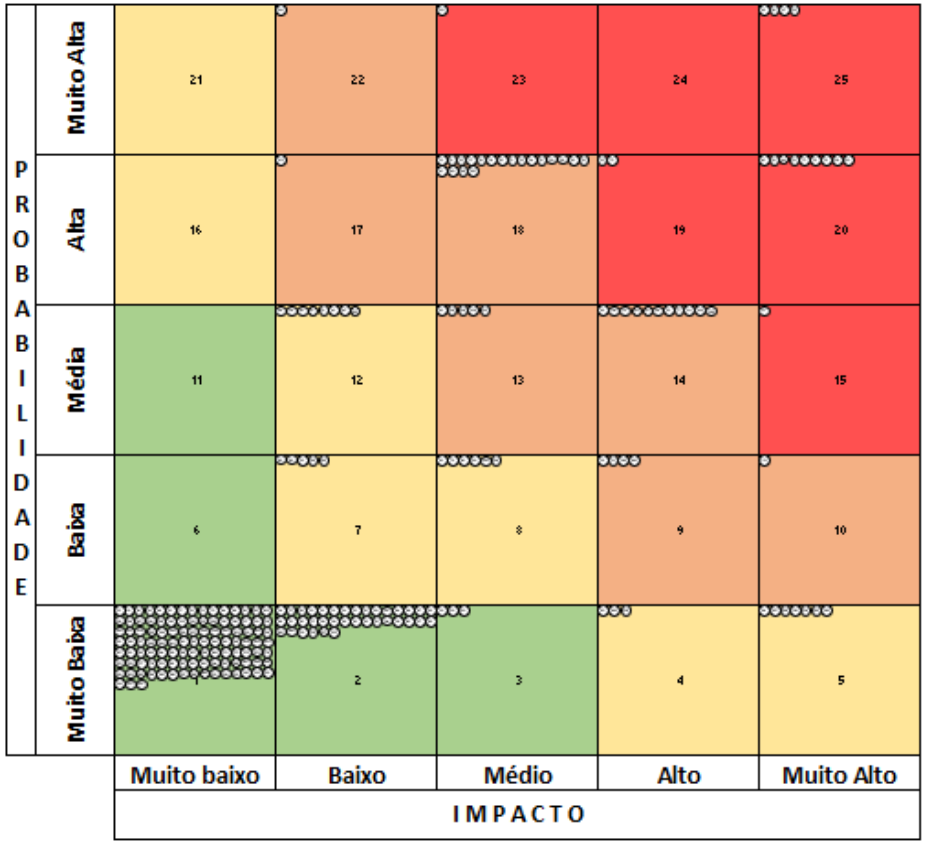


Matriz de Riscos de LGPD

Data mapping + Matriz de Riscos ISO 31.000, 27.001 e 27.701

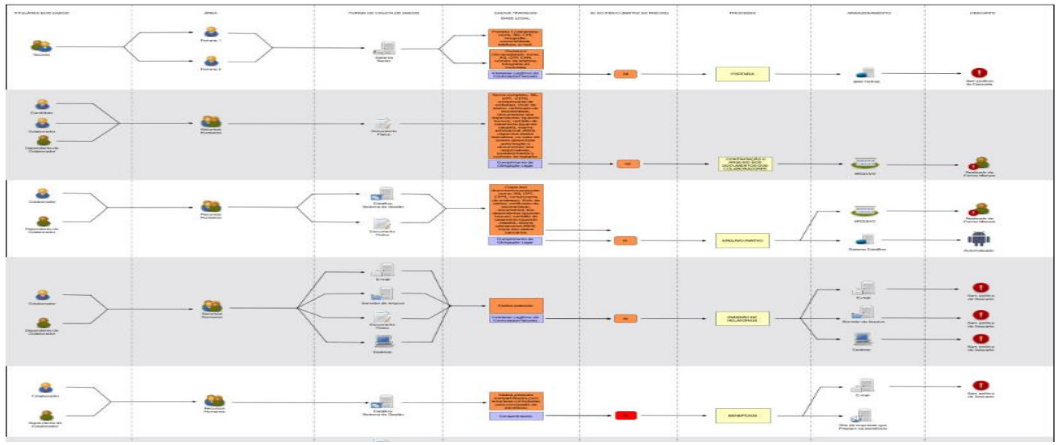


Heat Map (Mapa de calor 5x5)



International Organization for Standardization
ISO
31000
Risk-Management

Ciclo de Vida dos Dados



Privacy by Design - qualquer projeto que envolva o processamento de dados pessoais deve ser realizado mantendo a proteção e a privacidade dos dados a cada passo. Isso inclui o desenvolvimento de produtos, desenvolvimento de software, sistemas de TI etc. Na prática, significa que a organização deve garantir que a privacidade seja incorporada ao sistema durante todo o ciclo de vida.

Privacy by Default - significa que, assim que um produto ou serviço for lançado ao público, as configurações mais seguras de privacidade deverão ser aplicadas por padrão, sem nenhuma entrada manual do usuário final. Além disso, todos os dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto devem ser mantidos apenas pelo tempo necessário para fornecer o produto ou serviço. Se mais informações do que o necessário para fornecer o serviço forem divulgadas, esse conceito será violado.

Obrigado!

Rodrigo Pironti

Rodrigo Pironti A. de Castro

+55 41 3209.7200 | +55 41 3209.7300

pirontiadvogados.com.br