CGE

CONTROLADORIA
E OUVIDORIA GERAL
DO ESTADO
GOVERNO DO ESTADO DO CEARÁ

LEI GERAL DE PROTEÇÃO DE DADOS

Rodrigo Pironti

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

– 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...

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.

DADOS PESSOAIS DIRETOS

Identificam diretamente uma pessoa natural, sem necessidade de outras informações: nome, CPF, RG, Título Eleitoral...

DADOS PESSOAIS INDIRETOS

Torna a pessoa natural identificável, isto é, necessita de outras informações para identifica-lo: profissão, sexo, idade, geolocalização...

DADO PSEUDOANONIMIZADO

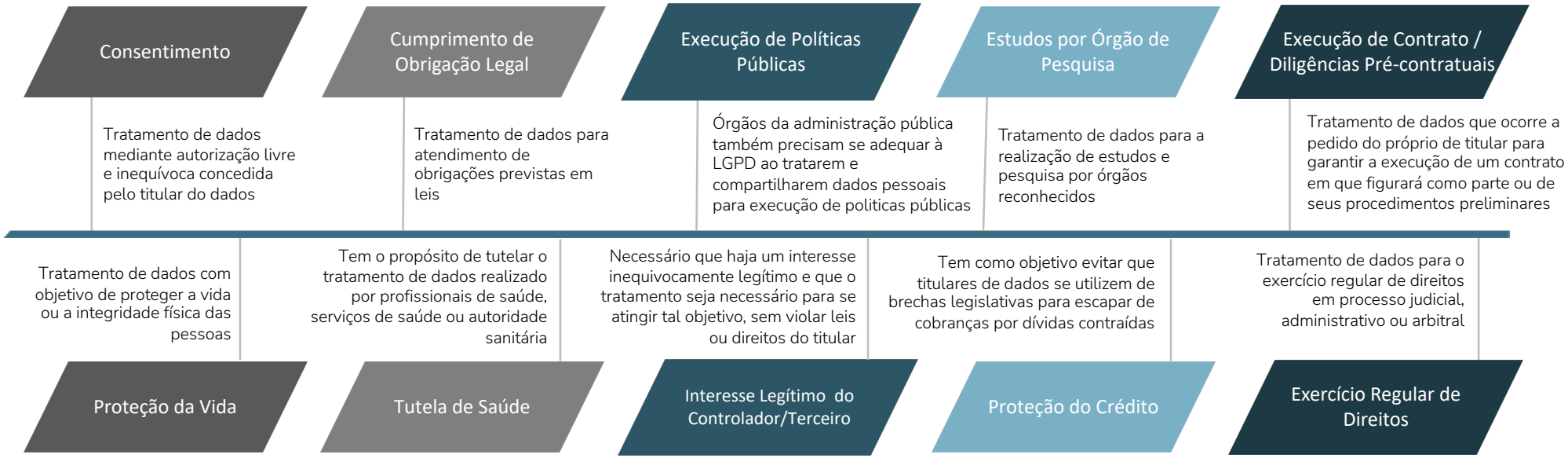
Dado do qual é retirada a possibilidade de associação direta ou indireta a um individuo

DADO ANONIMIZADO

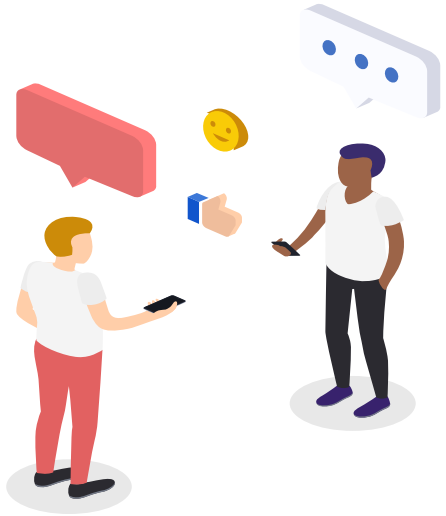
Dado relativo a titular que não possa ser identificado pelos meios técnicos razoáveis e disponíveis

Bases Legais para Tratamento de Dados

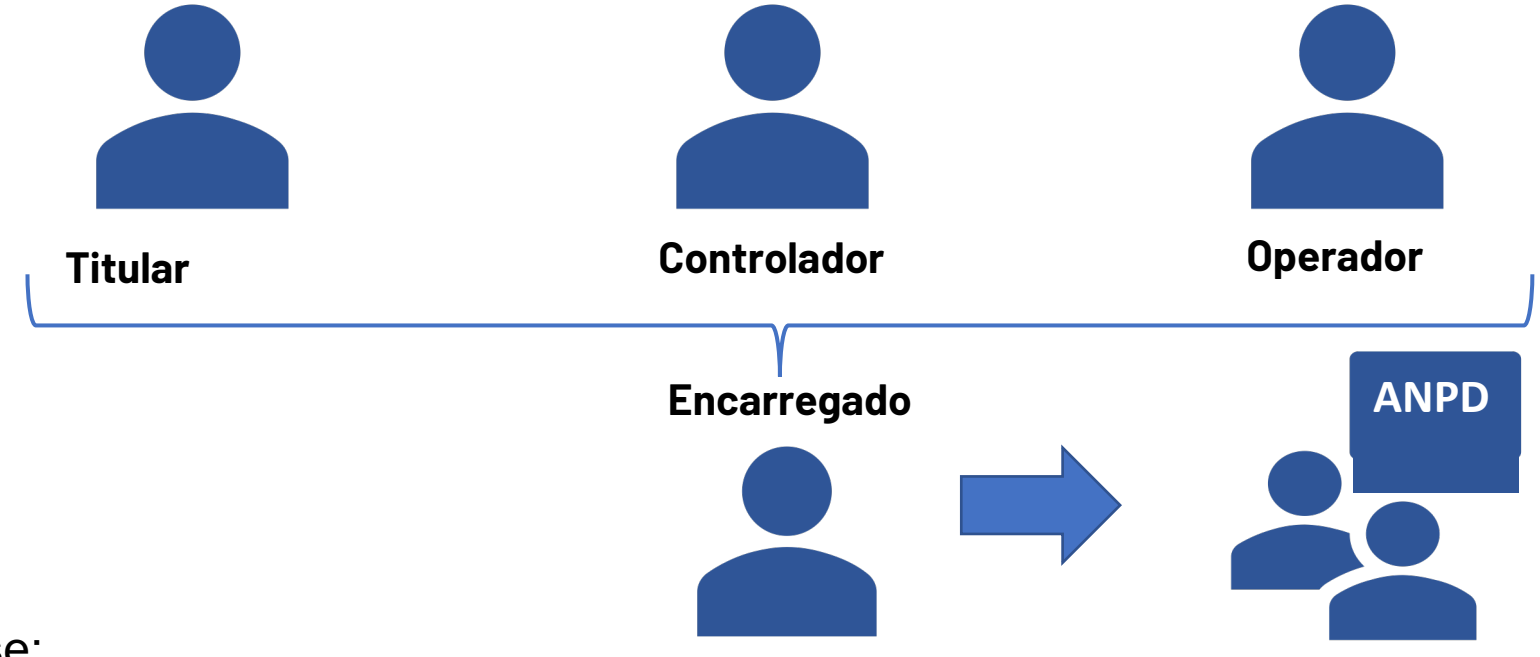
A LGPD não proíbe a coleta e tratamento de dados pessoais, desde que a finalidade esteja fundamentada em alguma das bases legais previstas no artigo 7º



ESTRUTURA DE GOVERNANÇA DE DADOS



Agentes da Relação no Tratamento de Dados



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

IX - agentes de tratamento: o controlador e o operador;

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;

18. Daí decorre que **não são controladoras as pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos.** É o caso de empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta. Nesse sentido, a definição legal de controlador não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades. De forma diversa, trata-se de comando legal que atribui obrigações específicas à pessoa jurídica, de modo que esta assume a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares e da ANPD.

22. Nesse sentido, a União, como controladora, é a responsável perante a LGPD, mas as atribuições de controlador, por força da desconcentração administrativa, **são exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte**, fenômeno que caracteriza a distribuição interna das competências. É o que se verifica nas hipóteses de uso compartilhado de dados pessoais (art. 26[10]), de atendimento às exigências da ANPD (art. 29[11]) e de aplicação de sanções administrativas (art. 52, § 3º[12]).

23. No mesmo sentido, ressalta-se que **os órgãos públicos devem cumprir os deveres de transparência e de nomeação de encarregado (pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares de dados e a ANPD)**, pois além de atuarem em nome da pessoa jurídica da qual fazem parte, tais obrigações decorrem expressamente da LGPD (art. 23, I e III).[13]

Consultor Jurídico
conjur.com.br

OPINIÃO

O controlador e o operador de dados na Administração Pública: um risco iminente

23 de fevereiro de 2021, 10h39

Imprimir Enviar

Por Rodrigo Pironti

OPINIÃO

O controlador de dados e a ausência de personalidade dos órgãos de Estado

25 de abril de 2021, 7h12

Imprimir Enviar

Por Rodrigo Pironti

Exemplo 1:

Em uma contratação de uma solução de computação em nuvem de uma empresa por um determinado Ministério do Poder Executivo a controladora é a União, mas é o Ministério, na condição de órgão público federal, que exercerá as funções típicas do controlador. Por sua vez, o operador será a empresa contratada. Por exercer funções típicas de controlador, cabe ao Ministério designar um encarregado, bem como realizar notificações à ANPD em casos de incidentes de segurança, dentre outras obrigações previstas na LGPD. No entanto, caso um titular de dados decida ajuizar uma ação judicial, questionando o tratamento realizado, deverá ingressar contra o controlador, que é a União.

E o encarregado?

Art. 41. O **controlador** **deverá** **indicar encarregado pelo tratamento de dados pessoais**.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
§ 2º As atividades do encarregado consistem em:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

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. 2º A identidade e as informações de contato do Encarregado pelo Tratamento dos Dados Pessoais deverão ser divulgadas publicamente, de forma clara e objetiva, no sítio eletrônico institucional do órgão ou da entidade, nos termos do § 1º do art. 41 da Lei nº 13.709, de 2018.

Art. 3º A autoridade máxima do órgão ou da entidade deverá assegurar ao Encarregado pelo Tratamento dos Dados Pessoais:
I - acesso direto à alta administração;
II - pronto apoio das unidades administrativas no atendimento das solicitações de informações; e
III - contínuo aperfeiçoamento relacionado aos temas de privacidade e proteção de dados pessoais, de acordo com os conhecimentos elencados no inciso I do § 1º do art. 1º e observada a disponibilidade orçamentária e financeira do órgão ou entidade.

Direito dos titulares

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta

Direito dos titulares – prazo de resposta

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

Art. 15. O **término do tratamento de dados** pessoais ocorrerá nas seguintes hipóteses:
I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
II - fim do período de tratamento;
III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais **serão eliminados após o término de seu tratamento**, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

TRATAMENTO DE DADOS NA ADMINISTRAÇÃO PÚBLICA

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;

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 de dados pessoais, nos termos do art. 39 desta Lei;

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 a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

COMUNICAÇÃO À ANPD E CONSENTIMENTO NO COMPARTILHAMENTO

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.
Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação.

LGPD (LEI 13.709/18)

versus

LAI (LEI 12.527/11)

Diretrizes

Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:

I - observância da publicidade como preceito geral e do sigilo como exceção;

II - divulgação de informações de interesse público, independentemente de solicitações;

III - utilização de meios de comunicação viabilizados pela tecnologia da informação;

IV - fomento ao desenvolvimento da cultura de transparência na administração pública;

V - desenvolvimento do controle social da administração pública.

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.

Sanções

Advertência

Indicação de prazo para adoção de medidas corretivas

Multa simples

de até 2% do faturamento, limitada a R$ 50.000.000,00 por infração

Multa diária

Limitada aos valores da multa simples.

Publicização da infração

Após devidamente apurada e confirmada a sua ocorrência.

Bloqueio

dos dados pessoais a que se refere a infração até a sua regularização

Art. 52 - § 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

Sanções

Eliminação

Dos dados pessoais destacados na infração

Suspensão parcial

Do funcionamento do banco de dados, por no máximo de 6 (seis) meses, prorrogável por igual período, até a regularização.

Suspensão

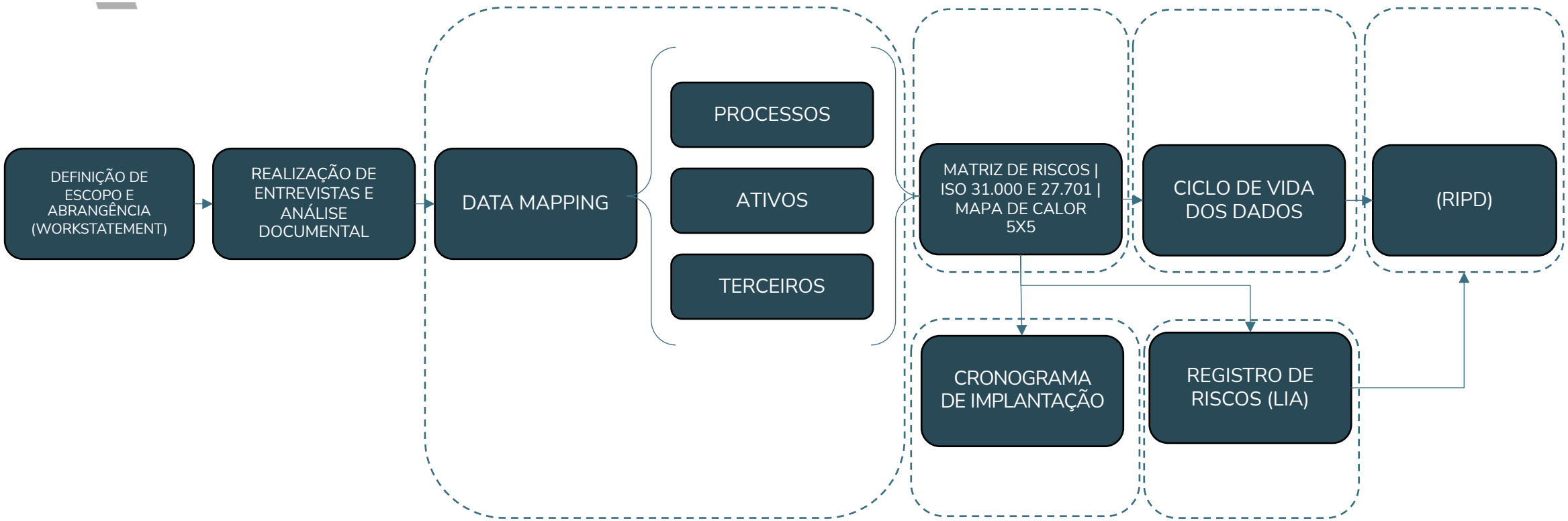
Do exercício da atividade de tratamento dos dados pessoais pelo período máximo de 6 (seis) meses, prorrogável por igual período.

Proibição

Parcial ou total do exercício de atividades relacionadas a tratamento de dados.

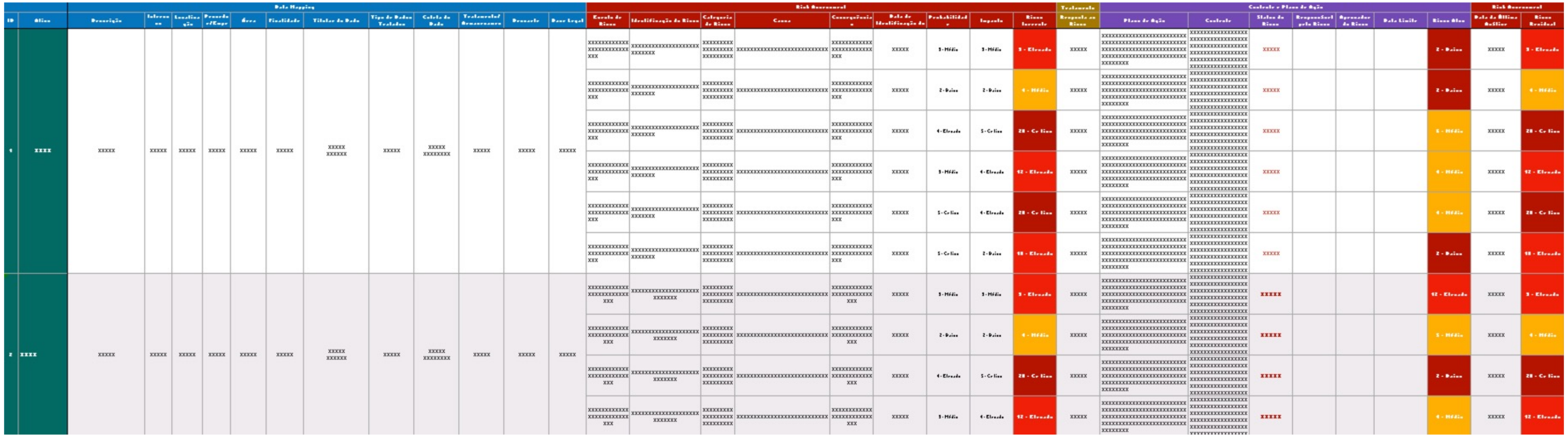
ASPECTOS PRÁTICOS DE IMPLANTAÇÃO
FRAMEWORK MÍNIMO

Fluxo de Trabalho para elaboração do RIPD

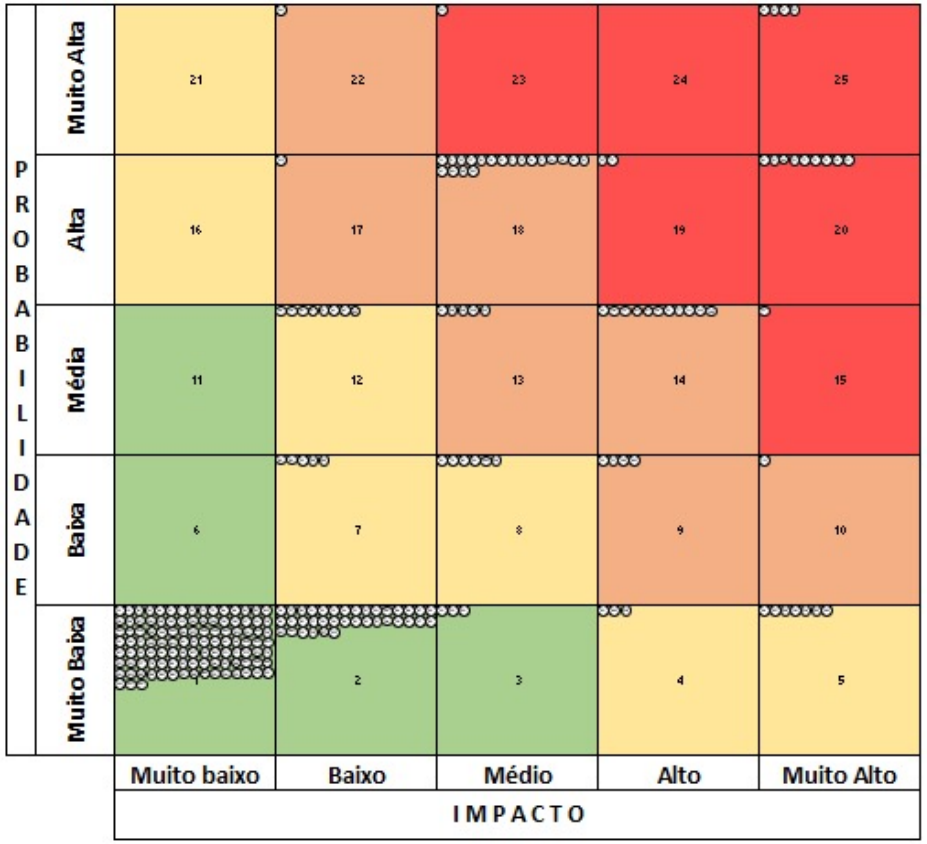


Matriz de Riscos de LGPD

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

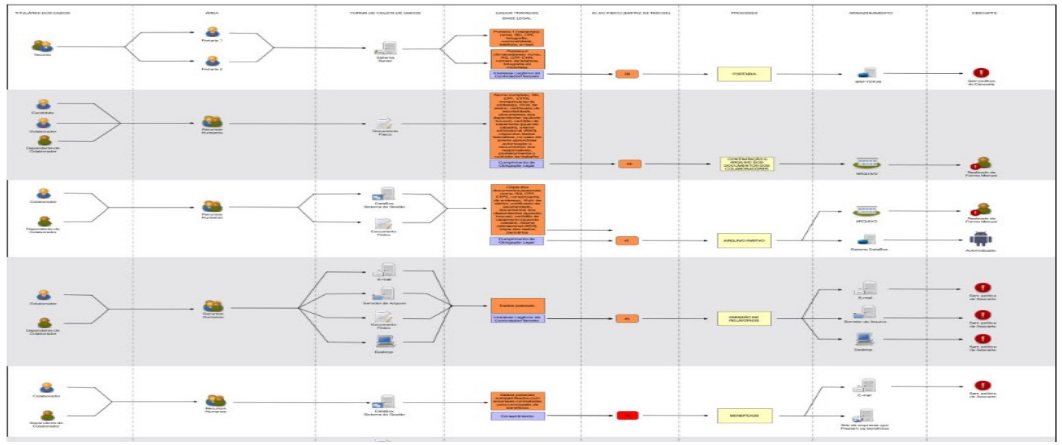


Heat Map (Mapa de calor 5x5)



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 A. de Castro

+55 41 3209.7200 | +55 41 3209.7300

pirontiadvogados.com.br

Rodrigo Pironti