RGM
TECNOLOGIA

# Workshop LGPD

As bases legais e hipóteses de tratamento de dados pessoais da LGPD

# Agenda

- Resumo sobre a LGPD e projetos de adequação
- Hipóteses de tratamento de dados pessoais da LGPD
- Como utilizar o LGPD Governance (PCP) para tratar as bases legais

RGM
TECNOLOGIA

# Adilson Taub Junior

CIO/CTO
DPO certified

20+ years of experience, helping companies solve problems with the right tools

## Contatos

/in/ataubjr/

adilsontj@rgm.com.br

## Acadêmico

**Master of Business Administration (MBA)**
Gestão Estratégica de Negócios

**Formação Executiva**
Compliance Empresarial (FGV)

**Pós-graduação**
Engenharia de Software

**Graduação**
Processamento de Dados

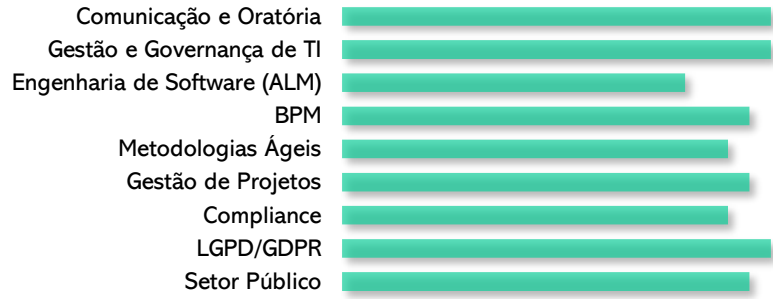
## Certificações

**Privacy & Security Management**
Data Protection Officer (DPO)
Privacy and Data Protection Practitioner
Privacy and Data Protection Foundation
Information Security (ISO/IEC 27.001)

**IT Governance and Service Management**
IT Service Management (ISO/IEC 20.000)
ITIL V3 Fdn. Certified
COBIT 4.1 Fdn. Certified
ITIL V2 Fdn. Certified

**Software Engineering**
Professional Scrum Product Owner (PSPO I)
Professional Scrum Master (PSM I)
Certified Scrum Professional
Certified ScrumMaster
Kanban Foundation KIKF
IBM Certified Solution Designer (RUP)
Certified Expert in BPM

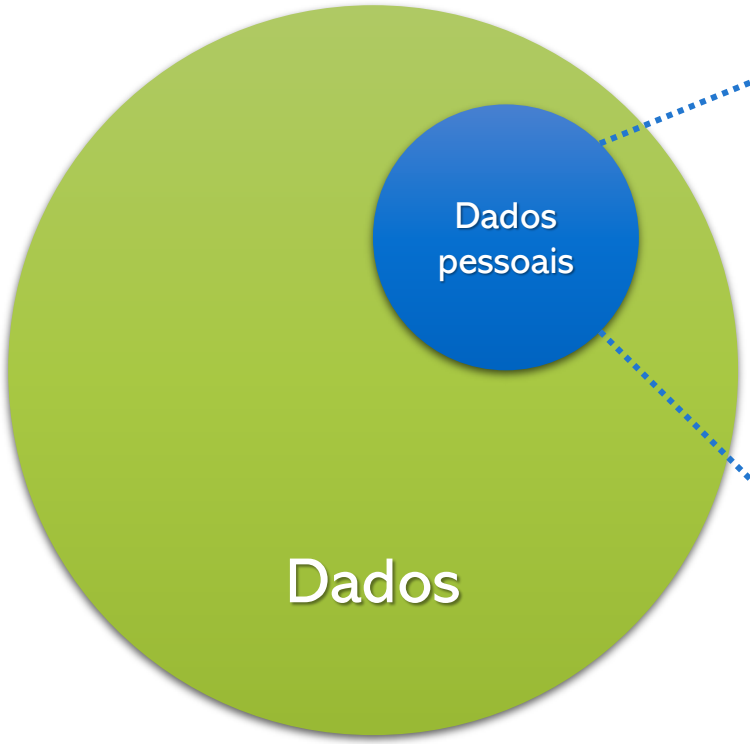
## Mapa de habilidades



# Resumo sobre a LGPD e projetos de adequação

RGM TECNOLOGIA

# Dados pessoais

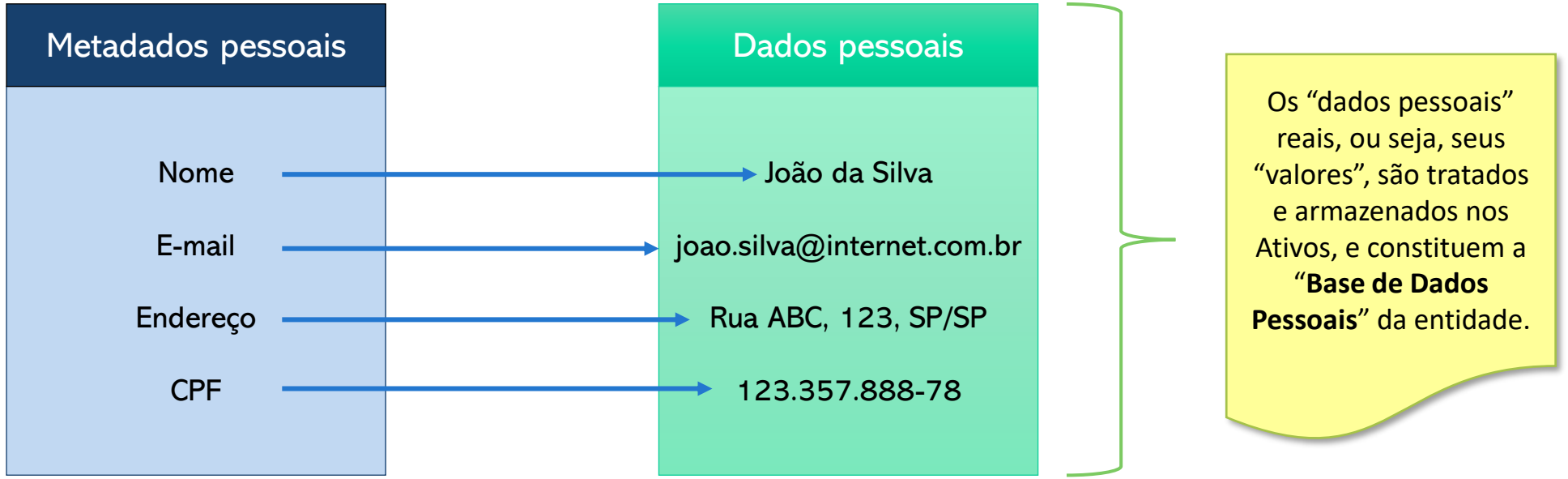



Nome
CPF
RG
Sexo
Data de nascimento
Endereço
E-mail
....

Dado pessoal: *informação relacionada a pessoa natural identificada ou identificável.*
(LGPD, Art. 5º)

# Dados e metadados pessoais

- Em um projeto de adequação à LGPD, inicialmente, o foco são os **metadados pessoais** e não o **valor** desses dados.



# Privacidade

*"São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."*

(Constituição Federal, Art. 5°, inciso X)

*"é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."*

(Constituição Federal, Art. 5°, inciso LXXIX – EC 115/22)

RGM TECNOLOGIA

# Histórico da LGPD

- Constituição Federal (Art. 5º)
- Lei de Acesso à Informação (Lei nº 12.527/2011)
- Lei de Crimes Cibernéticos (Lei Carolina Dieckmann - Lei nº 12.737/2012)
- Marco Civil da Internet (Lei nº 12.965/2014)
- *General Data Protection Regulation* - GDPR (União Europeia - 2016)
- *California Consumer Privacy Act of 2018* – CCPA (Estados Unidos - 2018)
- Lei da Desburocratização (Lei n.º 13.726/2018)
- Resolução 4658 BACEN (2018)

RGM TECNOLOGIA

# Objetivo da LGPD

- **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.

(Lei nº 13.709/18)

- Promulgada em 14 de agosto de 2018
- Em vigor desde 18 de setembro de 2020
- Sanções começaram a ser aplicadas em 01 de agosto de 2021

RGM TECNOLOGIA

# Escopo da LGPD


É necessário **justificar** todos os tratamentos de Dados Pessoais que você realiza e encontrar **bases legais** que sustentem as rotinas de coleta, processamento, armazenamento e distribuição desses dados

Deverá se implementar medidas administrativas e técnicas de **segurança da informação**, para garantir a **Confidencialidade**, **Integridade** e **Disponibilidade** dos Dados Pessoais que você usa

Por fim, é preciso implantar **novos procedimentos** operacionais obrigatórios segundo a LGPD e **modificar suas rotinas** atuais visando atender a todos os novos parâmetros legais em vigor, incluindo gerenciar os **Direitos dos Titulares**

RGM TECNOLOGIA

# Pilares de adequação à LGPD

# Hipóteses de tratamento de dados pessoais na LGPD

RGM TECNOLOGIA

# Princípios
## do tratamento de dados pessoais

- **Art. 6º** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

  I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

  II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

  III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

  IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

  V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

  VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

  VII - **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

  VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

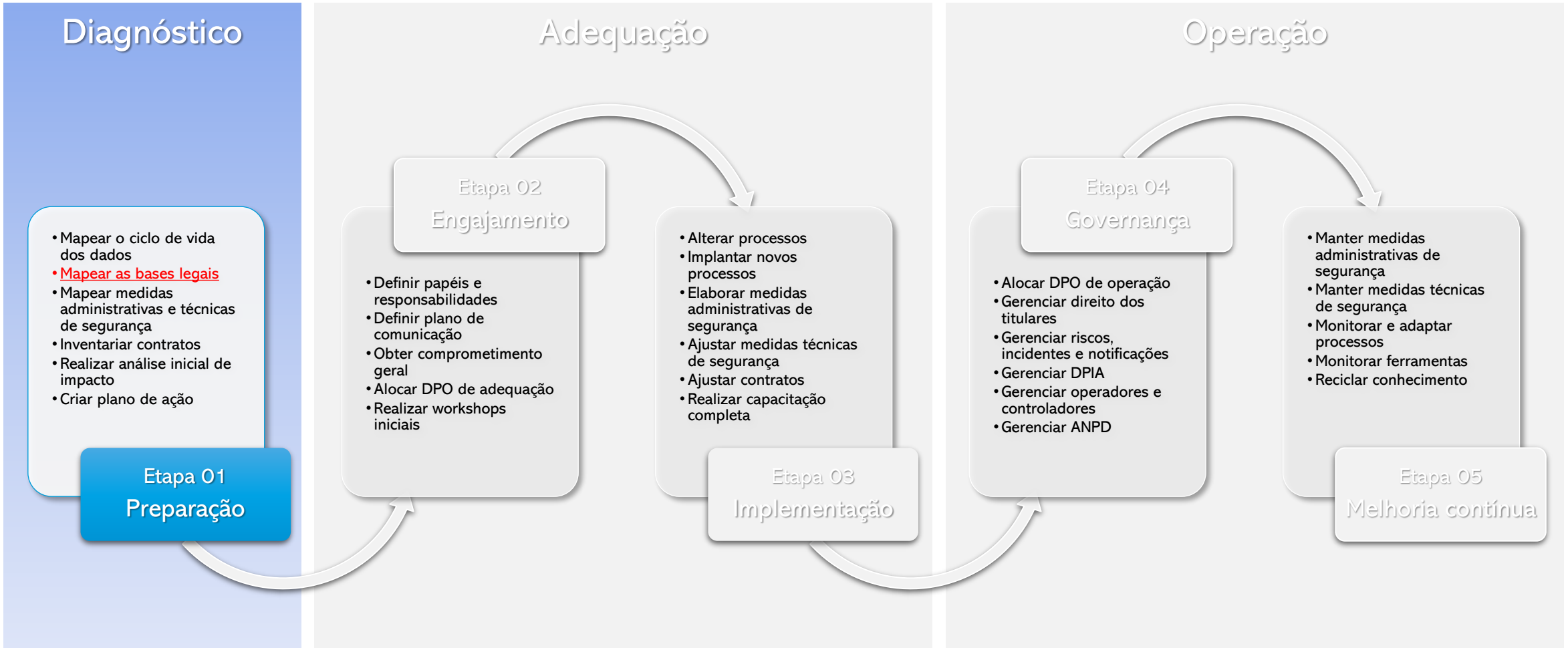
  IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

  X - **responsabilização** e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

RGM TECNOLOGIA

# Como implementar um SGPD

# Como implementar um SGPD



# Diagnóstico
## 1. Preparação

- **Principal objetivo da etapa:**
  - Elaborar *o Plano de Ação* com atividades claras e objetivas que deverão ser executadas posteriormente para garantir a adequação do controlador à LGPD.

- **Perguntas que devemos responder nessa etapa:**
  - Quais Dados Pessoais utilizamos e como eles trafegam por nossas rotinas?
  - Por que utilizamos esses Dados Pessoais e como justificamos isso?
  - Utilizamos apenas os Dados Pessoais minimamente necessários para cumprir nossos objetivos?
  - Quais são os compromissos que nossa empresa assume em relação à privacidade e segurança de dados?
  - Quais os níveis de Confidencialidade, Integridade e Disponibilidade dos nossos Ativos de Informação?
  - Como está nosso website corporativos em relação à LGPD?
  - Temos um DPO?
  - Sob quais riscos de privacidade estamos atuando hoje? Como tratá-los?
  - O que temos que fazer para cobrirmos as lacunas em relação à LGPD?

RGM TECNOLOGIA

# Etapa de Preparação

## Passo 1.1 Encontrar os Dados Pessoais

### Mapear os processos de negócio

- Usar modelagem BPMN
- Identificar atores
- Determinar objetivo e responsável de cada processo

### Inventariar seus Ativos

- Classificar o tipo (físico ou eletrônico)
- Detalhar quem mantém o Ativo
- Associar aos processos de negócio
- *Envolvimento do time de TI*

### Inventariar seus Artefatos e Dados

- Artefatos são documentos (físicos ou eletrônicos) que circulam pelos Ativos (devem ser associados)
- Dados pessoais estão dentro de Artefatos e podem ser reutilizados em vários artefatos

### Classificar seus Dados Pessoais

- A LGPD classifica os dados pessoais em “normais” ou “sensíveis”
- O Decreto Federal 10.046 estende essa classificação e pode ser utilizado em conjunto

RGM TECNOLOGIA

# Etapa de Preparação

## Passo 1.2 Justificar os Tratamentos de Dados Pessoais

### Elencar cada tratamento de dado

- Um processo pode ter “n” tratamentos em execução
- Identificar os detalhes sobre o ciclo de vida dos dados para cada tratamento
- Identificar parâmetros adicionais (como o uso de operadores, dados de crianças, compartilhamento e rotinas automatizadas)

### Classificar as hipóteses

- Utilizar os incisos definidos no Art. 7° para dados normais
- Utilizar os incisos definidos no Art. 11° para dados sensíveis
- *Envolvimento do time jurídico*

### Associar fundamentos legais

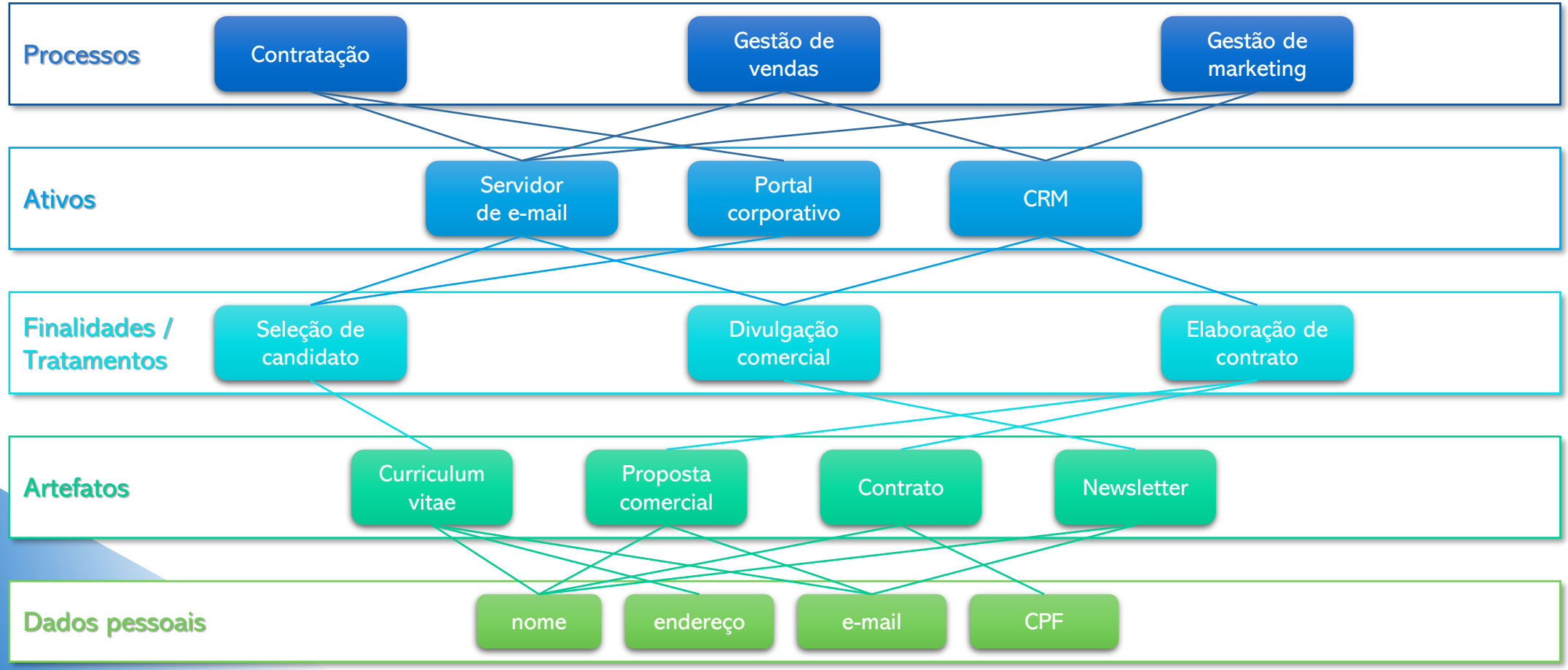
- Algumas hipóteses de tratamento podem exigir a indicação de fundamentos legais adicionais para justificar cada tratamento de dados
- *Envolvimento do time jurídico*

### Analisar o princípio da Necessidade

- Para cada tratamento inventariado, é necessário indicar quais artefatos são utilizados e, dentro desses artefatos, quais dados pessoais são REALMENTE necessários para cumprir a finalidade do tratamento de dados
- *Envolvimento do time jurídico*

RGM TECNOLOGIA

# Hierarquia da informação pessoal



# Finalidades de Tratamento de Dados

- Cada processamento de um Dado Pessoal (que ocorre por um motivo específico), pode ser considerado uma **Finalidade de Tratamento de Dados Pessoais**, que deve ser detalhada corretamente, especificando:
  - Quais artefatos e dados pessoais são utilizados na rotina e em quais ativos de informação
  - Origem e destino da informação
  - Se é executado por um Operador (e quem é o Operador)
  - Se realiza Dados Pessoais (e com quem se compartilha)
  - Se é uma rotina automatizada (sem intervenção humana)
  - Se trata dados de crianças e adolescentes
  - Se os dados são descartados ao final, e qual o período de retenção
  - Qual a base legal que justifica/sustenta o tratamento de dados

RGM TECNOLOGIA

# Exemplo de inventário de dados pessoais
(1/2)

- **Processo de Negócio**: Admissão de Colaborador
- **Objetivo do processo**: Realizar a contratação de um novo colaborador para o quadro da entidade, disponibilizando mais força de trabalho a um determinado time de trabalho
- **Ativos de Informação envolvidos**: e-mail, ERP, WhatsApp
- **Artefatos envolvidos**: Curriculum, e-mail de agendamento de entrevista, contrato de prestação de serviços, crachá, carteirinha de plano de saúde
- **Dados pessoais envolvidos**: Nome, data de nascimento, endereço de e-mail, endereço residencial, telefone, dados bancários, tipo sanguíneo, histórico médico

RGM TECNOLOGIA

# Exemplo de inventário de dados pessoais
(2/2)

## Finalidade #01

### Seleção de candidato

- **Ativo utilizado**: e-mail
- **Artefato utilizado**: Curriculum
- **Dados pessoais tratados**: Nome, data de nascimento, telefone, e-mail, endereço residencial
- **Hipótese de tratamento**: Legítimo interesse do Controlador (Art. 7º, inciso IX)
- **Tempo de armazenamento**: 12 meses
- **Compartilha dados com terceiros**: Não
- **Usa operador**: Não
- **Trata dados de crianças ou adolescentes**: Não

## Finalidade #02

### Contratação

- **Ativo utilizado**: Folha de Pagamento, eSocial, ERP
- **Artefato utilizado**: Contrato de Trabalho
- **Dados pessoais tratados**: Nome, data de nascimento, telefone, e-mail, endereço residencial, dados bancários, CPF, PIS
- **Hipótese de tratamento**: Execução de Contratos (Art. 7º, inciso V)
- **Tempo de armazenamento**: 5 anos após demissão
- **Compartilha dados com terceiros**: SIM: Receita Federal, via eSocial
- **Usa operador**: SIM: Terceirizado da Contabilidade
- **Trata dados de crianças ou adolescentes**: Não

## Finalidade #03

### Convite para festas

- **Ativo utilizado**: e-mail, Whatsapp
- **Artefato utilizado**: Convite
- **Dados pessoais tratados**: Nome, telefone, e-mail
- **Hipótese de tratamento**: Consentimento do Titular (Art. 7º, inciso I)
- **Tempo de armazenamento**: N/A
- **Compartilha dados com terceiros**: Não
- **Usa operador**: Não
- **Processo de consentimento**: XPTO
- **Trata dados de crianças ou adolescentes**: Não

RGM TECNOLOGIA

# Quando usar cada hipótese

RGM
TECNOLOGIA

# Hipóteses de Tratamento de Dados

- Cada Finalidade de Tratamento de Dados Pessoais deve ter uma **Hipótese de Tratamento** associada, de acordo com os Artigos 7° e 11° da LGPD:
  - Cumprimento de obrigação legal ou regulatória
  - Execução de políticas públicas
  - Realização de estudos e pesquisas
  - Execução de contrato
  - Processos judiciais, administrativos ou arbitrais
  - Proteção da vida
  - Tutela de saúde
  - Proteção de crédito
  - Proteção contra fraudes
  - Legítimo interesse do controlador
  - Consentimento explícito

RGM TECNOLOGIA

# Cumprimento de obrigação legal ou regulatória

- Utilizada quando há um dispositivo legal externo (fundamento legal) que obriga o Controlador a executar a rotina de tratamento de dado pessoal associado
- **Exemplo**:
  - Processo de negócio: Realizar pagamentos
  - Finalidade de tratamento: Pagar salário de colaborador
  - Artefatos utilizados:
    - Ordem bancária: Nome | CPF | Dados bancários | Valor do salário
    - Comprovante de pagamento: Nome | Dados bancários | Valor do salário
    - Registro de evento no eSocial: Nome | CPF | Valor pago
  - Hipótese associada: Art. 7° inciso II ou Art. 11° inciso II, alínea "a"
  - Fundamento legal associado: Decreto-Lei n° 5.452/43 (CLT), Art. 465

    "*O pagamento dos salários será efetuado em dia útil e no local do trabalho, dentro do horário do serviço ou imediatamente após o encerramento deste, salvo quando efetuado por depósito em conta bancária, observado o disposto no artigo anterior.*"
- **Regras**:
  - Requer, obrigatoriamente, o apontamento de qual **Fundamento Legal** está associado (Lei, Decreto, Portaria etc.)
  - Permite o tratamento de dados pessoais sensíveis
  - Pode ser utilizado por entes públicos ou privados

# Execução de políticas públicas

- Utilizada 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
- **Exemplo**:
  - Processo de negócio: Implementar programa "Internet para todos"
  - Finalidade de tratamento: Cadastrar usuário rural
  - Artefatos utilizados:
    - Cadastro de usuário: Nome | CPF | Endereço
    - Login de usuário: e-mail| senha
  - Hipótese associada: Art. 7° inciso III ou Art. 11° inciso II, alínea "b"
  - Fundamento legal associado: Portaria Estadual 999/25, Art. 3°

    "*O acesso ao programa Internet para Todos ocorrerá mediante cadastro pessoal e intransferível de um representante adulto da moradia rural, onde se identifique, individualmente, a pessoa natural responsável por guardar o login e senha de acesso ao programa.*"
- **Regras**:
  - Requer, obrigatoriamente, o apontamento de qual **Fundamento Legal** está associado (Lei, Decreto, Portaria etc.)
  - Requer que o tratamento ainda cumpra todos os requisitos estabelecidos nos Artigos 23 a 30 da LGPD
  - Permite o tratamento de dados pessoais sensíveis
  - Pode ser utilizado apenas por entes públicos

RGM TECNOLOGIA

# Realização de estudos e pesquisas

- Utilizada por órgãos de pesquisa para a realização de estudos
- **Exemplo**:
  - Processo de negócio: Realizar pesquisa de intenção eleitoral
  - Finalidade de tratamento: Compilar respostas de entrevistados
  - Artefatos utilizados:
    - Formulário de resposta: Nome* | Idade | Candidato | Gênero/Sexo*

    (*) Dados devem ser anonimizado antes da publicação dos resultados
  - Hipótese associada: Art. 7° inciso IV ou Art. 11° inciso II, alínea “c”
- **Regras**:
  - Só pode ser utilizada por órgãos de pesquisa (públicos ou privados)
  - Permite o tratamento de dados pessoais sensíveis
  - Define que, sempre que possível, deve-se anonimizar os dados pessoais tratados, principalmente os sensíveis

RGM TECNOLOGIA

# Execução de contrato

- Utilizada quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados
- **Exemplo**:
  - Processo de negócio: Realizar venda
  - Finalidade de tratamento: Elaborar proposta comercial
  - Artefatos utilizados:
    - Proposta comercial: Nome do cliente | e-mail do cliente | Nome do vendedor | e-mail do vendedor | assinatura do vendedor
  - Hipótese associada: Art. 7º inciso V
- **Regras**:
  - Não permite o tratamento de dados pessoais sensíveis
  - Deve ser utilizado sempre observando os interesses do Titular de Dados
  - Pode ser utilizado por ente público ou privado

RGM TECNOLOGIA

# Processos judiciais, administrativos ou arbitrais

- Utilizada para o exercício regular de direitos em processo judicial, administrativo ou arbitral
- **Exemplo**:
  - Processo de negócio: Gerenciar reclamações na ouvidoria
  - Finalidade de tratamento: Segmentar reclamações e dar primeiro atendimento
  - Artefatos utilizados:
    - Formulário de reclamação: Nome do reclamante| e-mail do reclamante| Nome do colaborador envolvido
  - Hipótese associada: Art. 7° inciso VI ou Art. 11° inciso II, alínea "c"
- **Regras**:
  - Permite o tratamento de dados pessoais sensíveis
  - Pode ser utilizado por ente público ou privado
  - Quando se tratar de processo arbitral, deve-se observar os dispostos na Lei n° 9.307/96

RGM TECNOLOGIA

# Proteção da vida

- Utilizada para a proteção da vida ou da incolumidade física do titular ou de terceiro
- **Exemplo**:
  - Processo de negócio: Gerenciar incidente de trabalho
  - Finalidade de tratamento: Abrir ocorrência de acidente de trabalho
  - Artefatos utilizados:
    - Formulário de ocorrência: Nome do colaborador| idade do colaborador
  - Hipótese associada: Art. 7° inciso VII ou Art. 11° inciso II, alínea “e”
- **Regras**:
  - Permite o tratamento de dados pessoais sensíveis
  - Pode ser utilizado por ente público ou privado

RGM TECNOLOGIA

# Tutela de saúde

- Utilizada para a tutela da saúde, considerando todas as etapas de atendimento, pronto atendimento, exames, procedimentos cirúrgicos ou farmacêuticos e odontológicos
- **Exemplo**:
  - Processo de negócio: Realizar pronto atendimento
  - Finalidade de tratamento: Atualizar prontuário de triagem do paciente
  - Artefatos utilizados:
    - Prontuário médico: Nome do paciente | idade do paciente | gênero/sexo do paciente | temperatura corporal | dados PCD | pressão arterial
  - Hipótese associada: Art. 7° inciso VIII ou Art. 11° inciso II, alínea "f"
- **Regras**:
  - Permite o tratamento de dados pessoais sensíveis
  - Pode ser utilizado por ente público ou privado
  - Só pode ser utilizada em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
  - Quando os dados forem compartilhados com outros agendes que não sejam profissionais de saúde, deve-se utilizar o consentimento do Titular de Dados

RGM TECNOLOGIA

# Proteção de crédito

- Utilizada para a análise de crédito de consumidores, como consulta de cadastro negativo de consumidores que é previsto no Código de Defesa do Consumidor (CDC)
- **Exemplo**:
  - Processo de negócio: Realizar empréstimo
  - Finalidade de tratamento: Verificar solvência e risco de crédito para empréstimo
  - Artefatos utilizados:
    - Cadastro negativo: Nome do cliente | cpf do cliente | nível de solvência do cliente
  - Hipótese associada: Art. 7° inciso X
- **Regras**:
  - Não permite o tratamento de dados pessoais sensíveis
  - Pode ser utilizado por ente público ou privado
  - Geralmente utilizada por entidades financeiras
  - Deve ser utilizada ainda se observando os demais direitos do Titular de Dados

RGM TECNOLOGIA

# Proteção contra fraudes

- Utilizada para identificação e autenticação de cadastro de sistemas eletrônicos visando a proteção dos interesses do Titular de Dados contra fraudes
- **Exemplo**:
  - Processo de negócio: Consultar extrato bancário
  - Finalidade de tratamento: Verificar autenticidade de login de usuário
  - Artefatos utilizados:
    - Cadastro do usuário: Nome do cliente| chave de acesso do cliente | biometria facial do cliente
  - Hipótese associada: Art. 11° inciso II, alínea “g”
- **Regras**:
  - Exclusivo para o tratamento de dados pessoais sensíveis (biométricos)
  - Pode ser utilizado por ente público ou privado
  - Deve ser utilizada ainda se observando os demais direitos do Titular de Dados

RGM TECNOLOGIA

# Legítimo interesse do controlador

- Utilizada para casos onde o tratamento de dados visa atender aos interesses do controlador, em especial sobre a promoção de suas atividades
- **Exemplo**:
  - Processo de negócio: Admissão de novo colaborador
  - Finalidade de tratamento: Análise de *curriculum vitae*
  - Artefatos utilizados:
    - Curriculum vitae: Nome | cpf | idade | e-mail | endereço | histórico profissional | conhecimentos técnicos
  - Hipótese associada: Art. 7º inciso IX

    "*A triagem de CV visa dar agilidade ao processo de admissão buscando encontrar candidatos compatíveis com a descrição da vaga. O Titular de Dados se beneficia com esse tratamento uma vez que se candidatou por vontade própria e também não quer perder tempo em entrevistas improdutivas, onde ele não tem chances reais de prosseguir no processo de contratação.*"
- **Regras**:
  - Não permite o tratamento de dados pessoais sensíveis
  - Pode ser utilizado por ente público ou privado
  - Deve ser utilizada ainda se observando os interesses do Titular de Dados e eventuais riscos
  - Deve ser sempre acompanhado de uma descrição do interesse do Controlador e dos benefícios obtidos pelo Titular de Dados
  - O uso dessa hipótese não está regulamentado pela ANPD

# Consentimento explícito do titular de dados

- Utilizada quando não há outra hipótese que sustente ou justifique o tratamento de dados pessoal
- **Exemplo**:
  - Processo de negócio: Cadastro de cliente
  - Finalidade de tratamento: Atualização da lista de convites de evento beneficente
  - Artefatos utilizados:
    - Cadastro do usuário: Nome do cliente| e-mail do cliente
  - Hipótese associada: Art. 7°, inciso I ou Art. 11° inciso I
- **Regras**:
  - Permite o tratamento de dados pessoais sensíveis
  - Pode ser utilizado por ente público ou privado
  - Obrigatório quando há compartilhamento de dados pessoais entre entes públicos e privados
  - Deve ser específico, claro, preciso, datado e com prazo pré-definido
  - Quando for solicitado, deve ser destacado de outras cláusulas e ser acompanhado com uma descrição dos impactos na não aceitação do consentimento
  - Pode ser revogado como um dos direitos dos Titulares de Dados previstos na LGPD

RGM TECNOLOGIA

# Demonstração prática

RGM TECNOLOGIA

# Obrigado!

Adilson Taub Jr.

https://www.linkedin.com/in/ataubjr/

RGM Tecnologia

www.rgm.com.br

SCAN ME