

# Registro de Operações de Tratamento

Como não fazer do artigo 37 um “log hell”

(Artigo 37 para desenvolvedores)



TDC Connections, 8 de Junho de 2021

# Sobre

---

## Público Alvo:

Desenvolvedores, Profissionais de TI e pessoas interessadas no tema LGPD

## Assunto:

Artigo 37 da LGPD e sua implementação

## Organização: 44 Slides (~30min) em 4 partes:

1. Introdução ao **Artigo 37**
2. **Tratamentos** de Dados Pessoais
3. Case **"Marketplace"**
4. **Registro** de Tratamentos

## DÉBORA MODESTO



Mestre em Informática pela Universidade Federal do Estado do Rio de Janeiro.

Atua desde 2010 no Serviço Federal de Processamento de Dados (SERPRO).

Gerente de um departamento de desenvolvimento, vivencia as dores e alegrias de equipes de desenvolvimento no contexto da empresa pública e agora, lidando com a proteção de dados em seus projetos.

Autora do blog [ArteSoftware.com.br](http://ArteSoftware.com.br)

## DOUGLAS SIVIOTTI



Analista de sistemas com especialização em engenharia de software pela Universidade Federal do Rio Grande do Sul, cursando especialização em Proteção e Uso de Dados pela PUC-MG.

Atua com desenvolvimento há mais de 20 anos e é arquiteto e software do SERPRO desde 2005. Nos últimos anos atua especialmente com arquitetura, qualidade de software, segurança e proteção de dados (LGPD), sendo um dos criadores do "guia de desenvolvimento confiável" do SERPRO.

Autor do blog [ArteSoftware.com.br](http://ArteSoftware.com.br)



# Aviso sobre o Conteúdo

## Conteúdo a Ser Regulamentado pela ANPD

---

1. Livre **interpretação** dos apresentadores sobre o artigo 37
2. Avaliação das experiência na **Europa** (GDPR)
3. Avaliação de práticas de **mercado** (ferramentas)
4. **Experiência** prévia dos apresentadores
5. Análise das **prováveis** definições sobre o tema

Regulamentação mais detalhada deve ser elaborada pela **Agência Nacional de Proteção de Dados (ANPD)**



LGPD **Artigo 37**: O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse

# Objetivo do Artigo 37

## Prestitação de Contas

---

A handwritten ledger on grid paper with columns for names and numerical values. The entries are written in cursive and include names and various numbers.

Nome	Valor 1	Valor 2	Valor 3	Valor 4
Pauline Bismarck	4464	883	143	2000
Pauline Bismarck	3534	143	1000	1000
Pauline Bismarck	8525	143	1000	1000
Pauline Bismarck	1132	143	1000	1000
Pauline Bismarck	6665	143	1000	1000
Pauline Bismarck	6789	143	1000	1000
Pauline Bismarck	3565	143	1000	1000
Pauline Bismarck	1271	143	1000	1000
Pauline Bismarck	4697	143	1000	1000
Pauline Bismarck	445	143	1000	1000
Pauline Bismarck	4030	143	1000	1000



# Objetivo do Artigo 37

Viabilizar Prestação de Contas

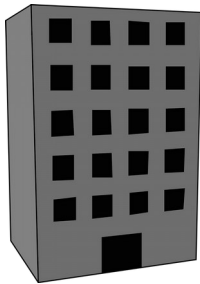


# Prestação de Contas

ANPD, Reguladores e Judiciário

---

- RIPD – Relatório de Impacto à Proteção de Dados
- Proteção do Operador frente ao Controlador
- Ônus da prova é do Controlador
- Demonstração de boa fé e adoção de medidas



ANPD  
(Regulador)

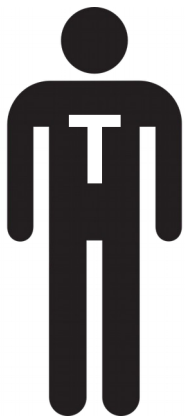


Judiciário

# Prestação de Contas

## Direitos do Titular

---



Titular

1 – Confirmação de existência

2 – Acesso aos dados

3 – Correção dos dados

4 – Decisão sobre desconformidades\*

5 – Portabilidade

6 – Eliminação se consentido

7 – Info. sobre compartilhamentos

8 – Consequências de não consentir

9 – Revogar consentimento

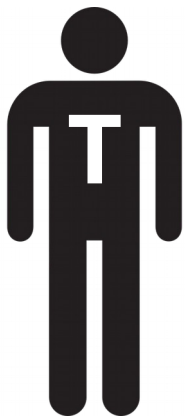
\* anonimizar, bloquear, eliminar dados desnecessários ou excessivos



# Prestação de Contas

## Direitos do Titular

---



Titular

1 – Confirmação de existência

2 – Acesso aos dados (tratados)

3 – Correção dos dados

4 – Decisão sobre desconformidades\*

5 – Portabilidade

6 – Eliminação se consentido

7 – Info. sobre compartilhamentos

8 – Consequências de não consentir

9 – Revogar consentimento

\* anonimizar, bloquear, eliminar dados desnecessários ou excessivos

# Escopo da Apresentação

## Produtos e Soluções Digitais

---



1

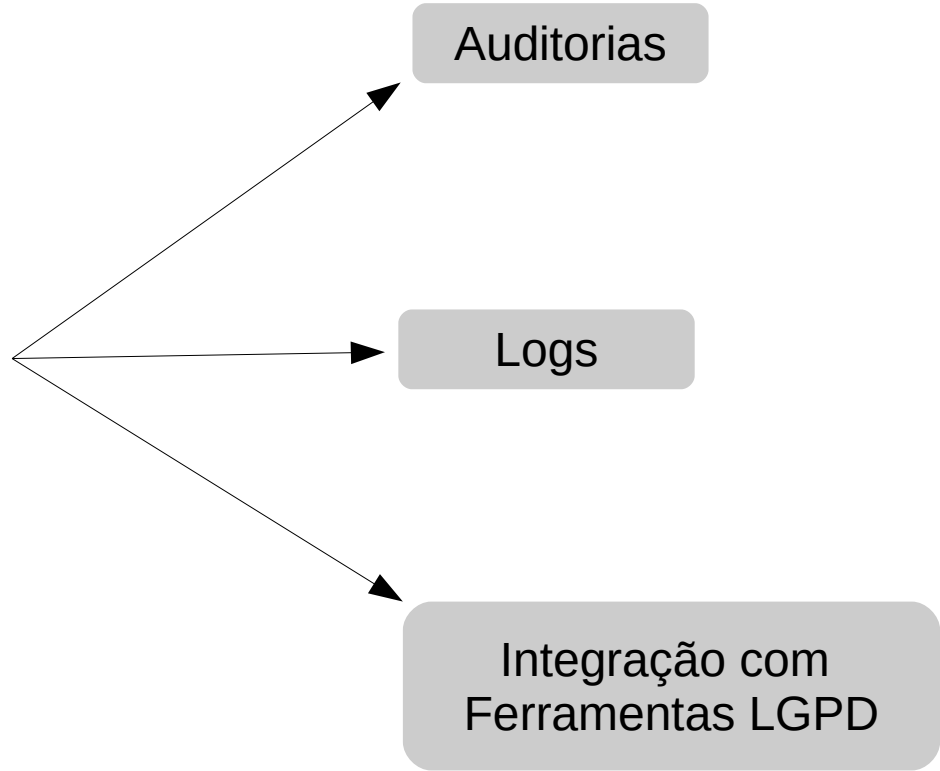


2

# Escopo da Apresentação

## Produtos e Soluções Digitais

---



LGPD Artigo 37: O controlador e o operador devem manter registro das **operações de tratamento** de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse

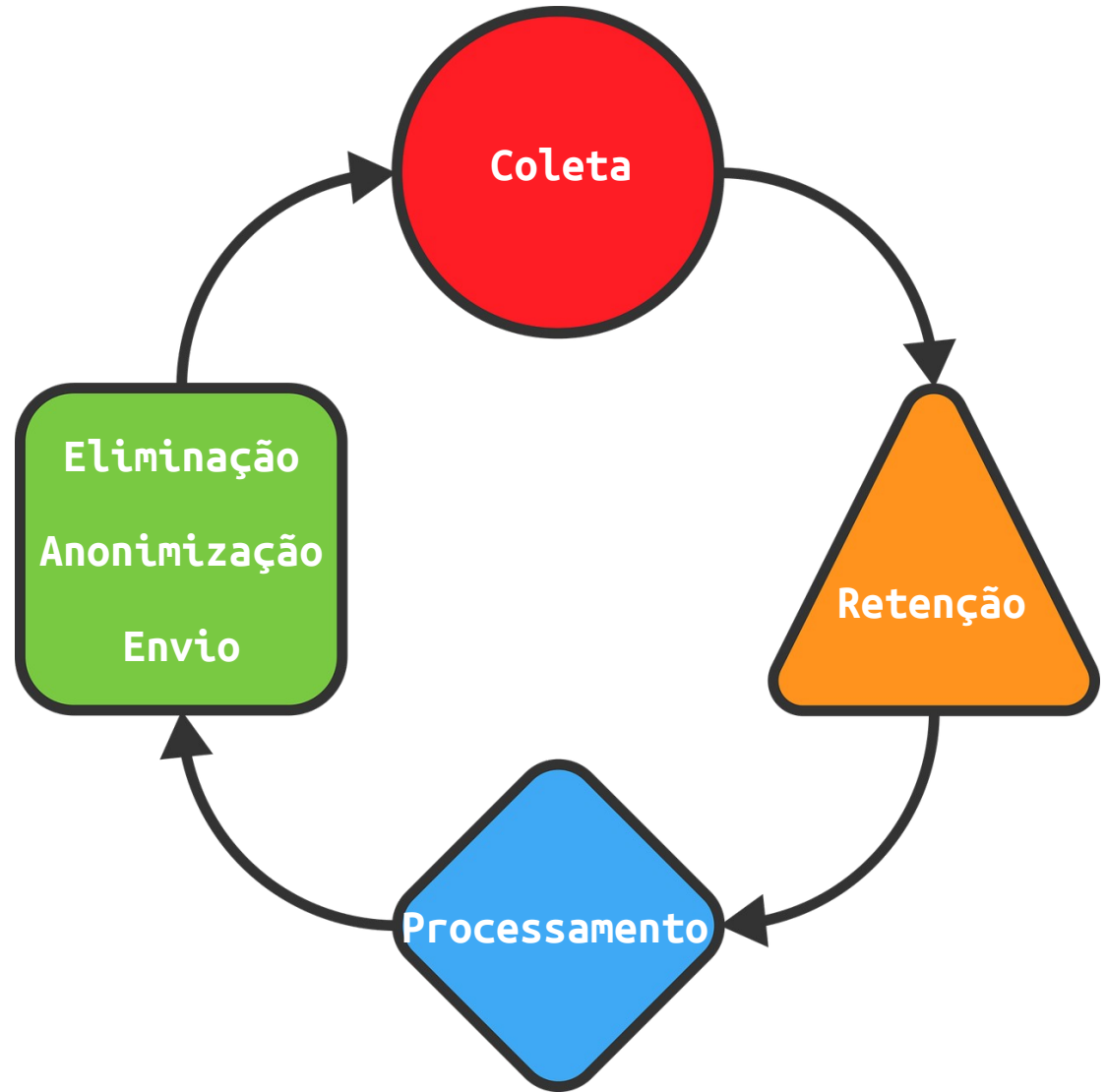
# Tratamento de Dados Pessoais

## Definição e Conceito

---

*“**toda operação** realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”*

*[LGPD: 20 Operações]*



o que sustenta  
um tratamento?



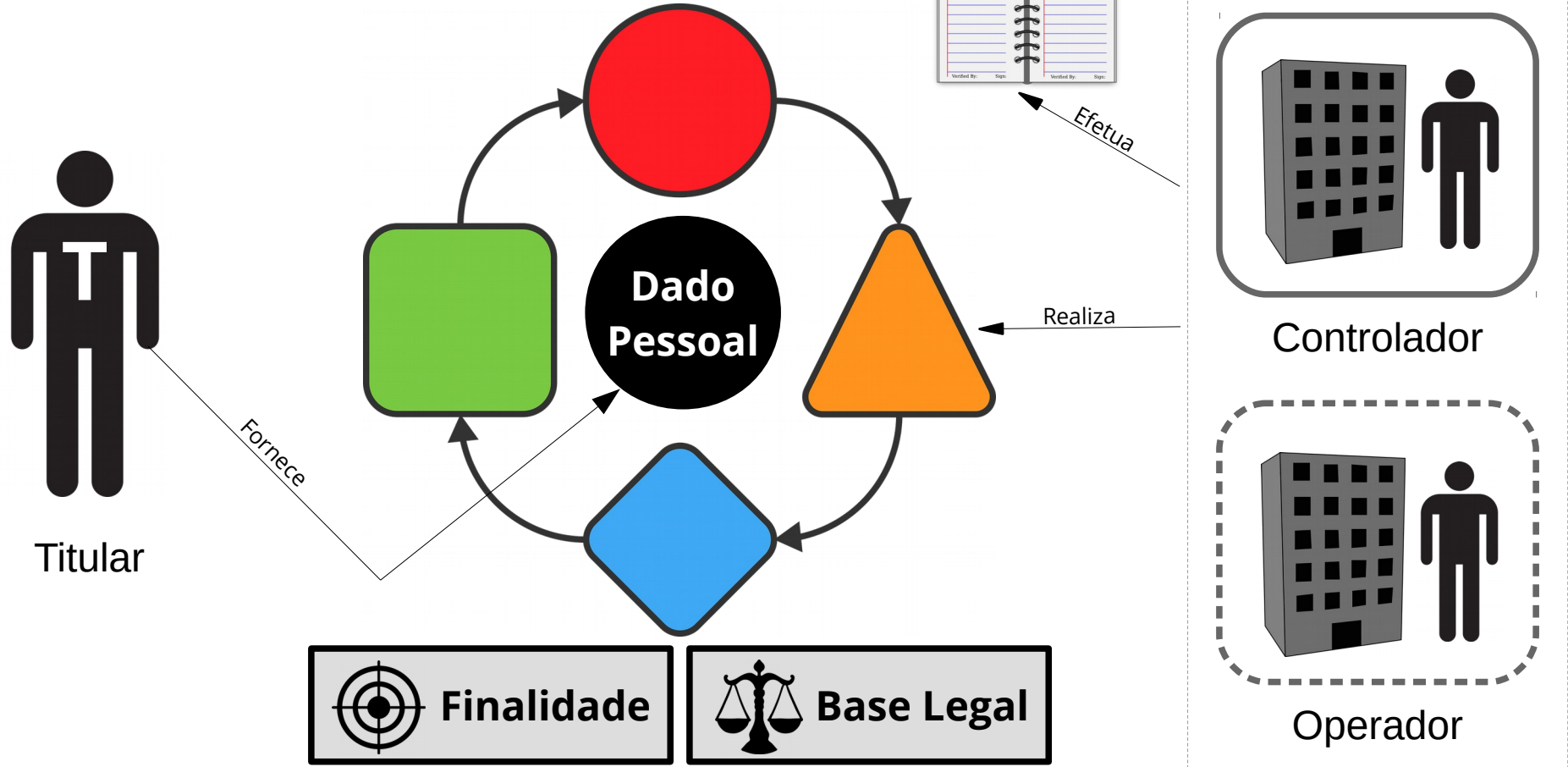
**Finalidade**



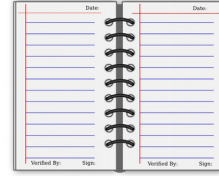
**Base Legal**

# O Tratamento

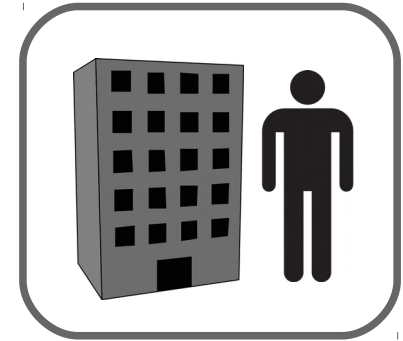
## Esquema Geral



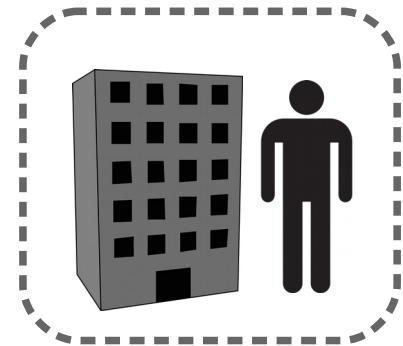
### Registro de Tratamentos



### Agentes de Tratamento



Controlador



Operador

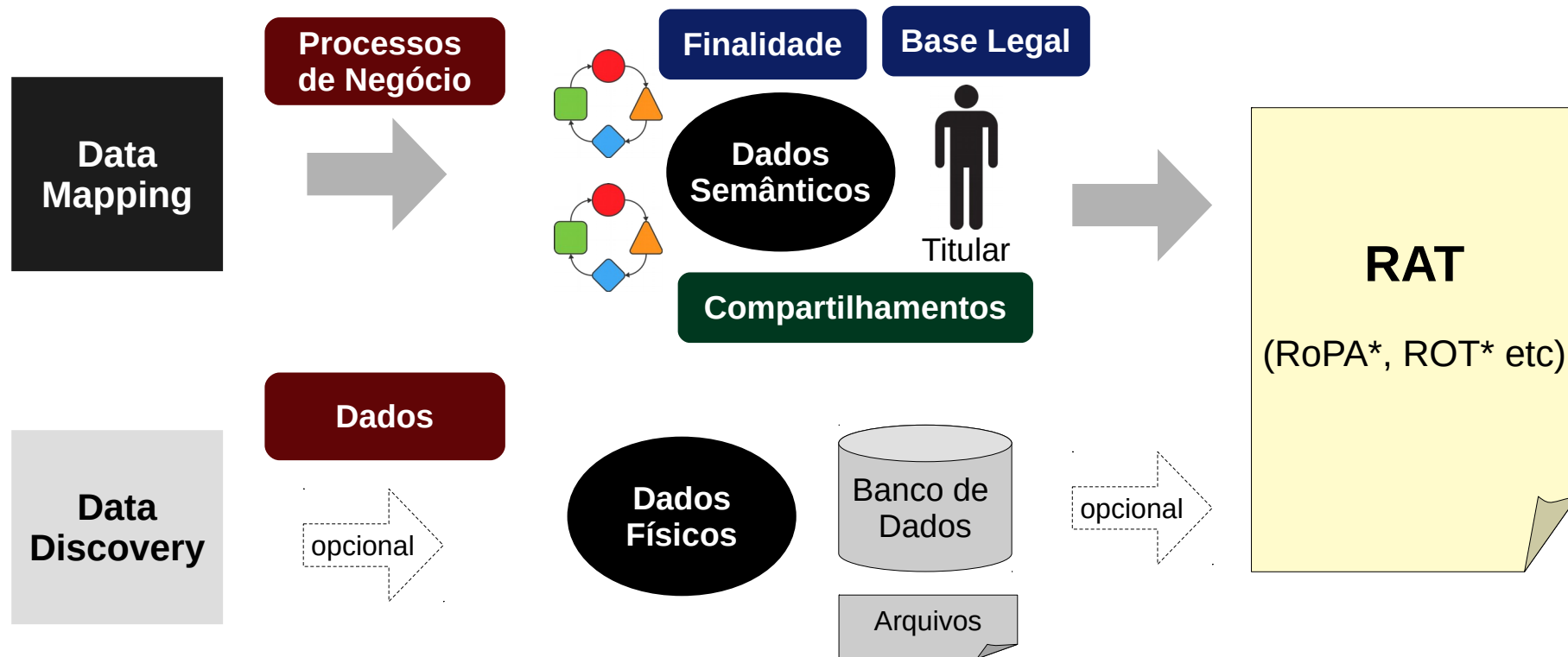
 Finalidade

 Base Legal



# RAT - Registro de Atividades de Tratamento

## Manifestação dos Tratamentos

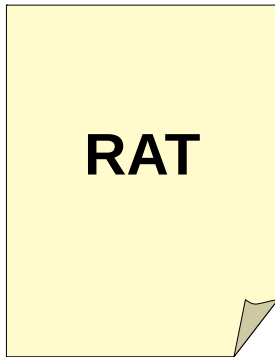


\* RoPA - Record of Processing Activities (Registro de Atividades de Processamento)

\* ROT – Registro das Operações de Tratamento

# Exemplo Hipotético

## 3 Manifestos



Itens da **GDPR** para cada Tratamento:  
Agentes / Contatos,  
Finalidades, Titulares,  
Dados Pessoais,  
Terceiros Retenção e  
Exclusão, Medidas  
Técnicas, Segurança

### Registro de Atividade de Tratamentos

<b>Controlador</b>	Rapitreco LTDA
<b>Operador</b>	não se aplica
<b>Titular (es)</b>	Clientes da Plataforma e Entregadores
<b>Análise Crítica</b>	O grau ponderado indica atenuantes em relação ao GAPD

#### Tratamentos

	<b>1</b>	<b>Descrição</b>	Entrega de trecos do remetente para o destinatário
		<b>Finalidade</b>	Prestar um serviço de entrega de um ponto a outro
		<b>Dados Pessoais</b>	Nome e endereço do remetente e do destinatário
		<b>Terceiros</b>	nenhum
		<b>Retenção</b>	Dados pessoais são excluídos, mas cliente pode salvar se quiser
	<b>2</b>	<b>Descrição</b>	Marketplace customer-to-customer: O destinatário (cliente) faz um pedido ao remetente (fornecedor)
		<b>Finalidade</b>	Prestar serviço de "marketplace"
		<b>Dados Pessoais</b>	Dados do cliente e do vendedor (nome, endereço, rating), dados do entregador e dados de compras dos clientes
		<b>Terceiros</b>	Empresas de cartão de crédito
		<b>Retenção</b>	Os pedidos são guardados indefinidamente. O cliente escolhe se salva os dados do cartão de crédito
	<b>3</b>	<b>Descrição</b>	Convênios com as Farmácias
		<b>Finalidade</b>	Prestar serviço de marketplace para farmácias
		<b>Dados Pessoais</b>	Dados do cliente e do vendedor (nome, endereço, rating), dados do entregador e dados de compras dos clientes. OBS: os dados de compra podem conter dados pessoais sensíveis
		<b>Terceiros</b>	Farmácias conveniadas e empresas de cartão de crédito
		<b>Retenção</b>	Os pedidos são guardados indefinidamente. O cliente escolhe se salva os dados do cartão de crédito



LGPD Artigo 37: O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse

# Case de Tratamentos

## O Marketplace

---

### O Marketplace

- Site de vendas online
- Vários produtos
- Vários fornecedores
- Realiza **entregas**
- Registra **preferências**
- **Sugere** produtos

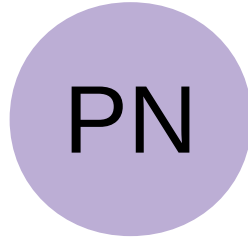


# Processo de Negócio

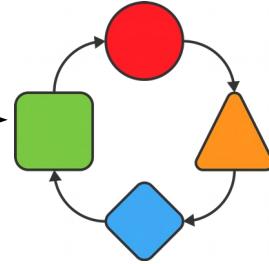
## Origem do Tratamento

---

Processo de Negócio



Tratamento (s)



- O processo de negócio é o que a organização faz como atividade
- Uma organização costuma ter vários processos de negócio
- Os processos de negócio podem tratar dados pessoais ou não
- Processo de Negócio do Marketplace: **Venda de produtos online**

# Granularidade

## O Grande "Problema"

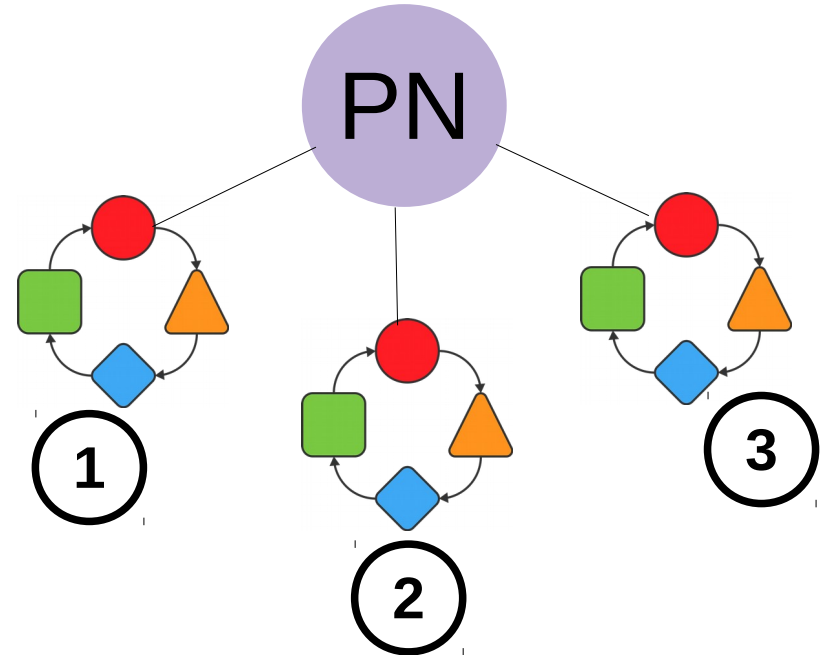
*Quantos tratamentos de dados pessoais existem em um único processo de negócio?*

Granularidade didática do marketplace:

3 Tratamentos de dados pessoais

- 1) **Vender e entregar produtos**
- 2) **Salvar preferências do usuário**
- 3) **Recomendar produtos**

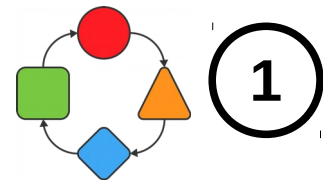
Processo de negócio:  
**Vender produtos online**





# Tratamento 1

## Vender e Entregar Produtos



O cliente se identifica, efetua um pedido com um ou vários itens (produtos) e informa um endereço de entrega. Também pode usar endereços salvos anteriormente na plataforma. O produto será entregue por uma transportadora contratada pela empresa do marketplace.



**Finalidade**

**Identificar** o cliente, oferecer interface de seleção de produtos e **entregar** os produtos escolhidos no endereço indicado.



**Base Legal**

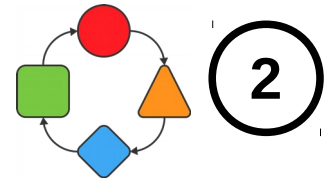
### “Execução de Contrato”

*Artigo 7, V - 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;*

## Tratamento 2

### Salvar Preferências do Usuário

---



O site do marketplace utiliza “cookies” para salvar escolhas e preferências do usuário. Dessa forma, a usabilidade do site torna-se muito melhor além de permitir que o usuário não precisa informar vários dados repetitivos toda vez que efetuar uma compra.



**Finalidade**

**Armazenar** dados de utilização e preferências do usuário para melhorar a usabilidade do site



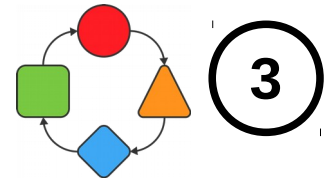
**Base Legal**

**“Consentimento”**

*Artigo 7, I - mediante o fornecimento de consentimento pelo titular*

## Tratamento 3

### Recomendação de Produtos



O site realiza milhões de vendas e por isso é capaz de “perceber” que alguns produtos costumam ser comprados junto com outros. É possível ainda fazer análise por cidade, bairro, idade entre outras características dos compradores. Dessa forma, o site é capaz de dar boas dicas de compras aos usuários.



**Finalidade**

**Recomendar** produtos durante uma compra a partir de dados de **outras compras** já efetuadas.



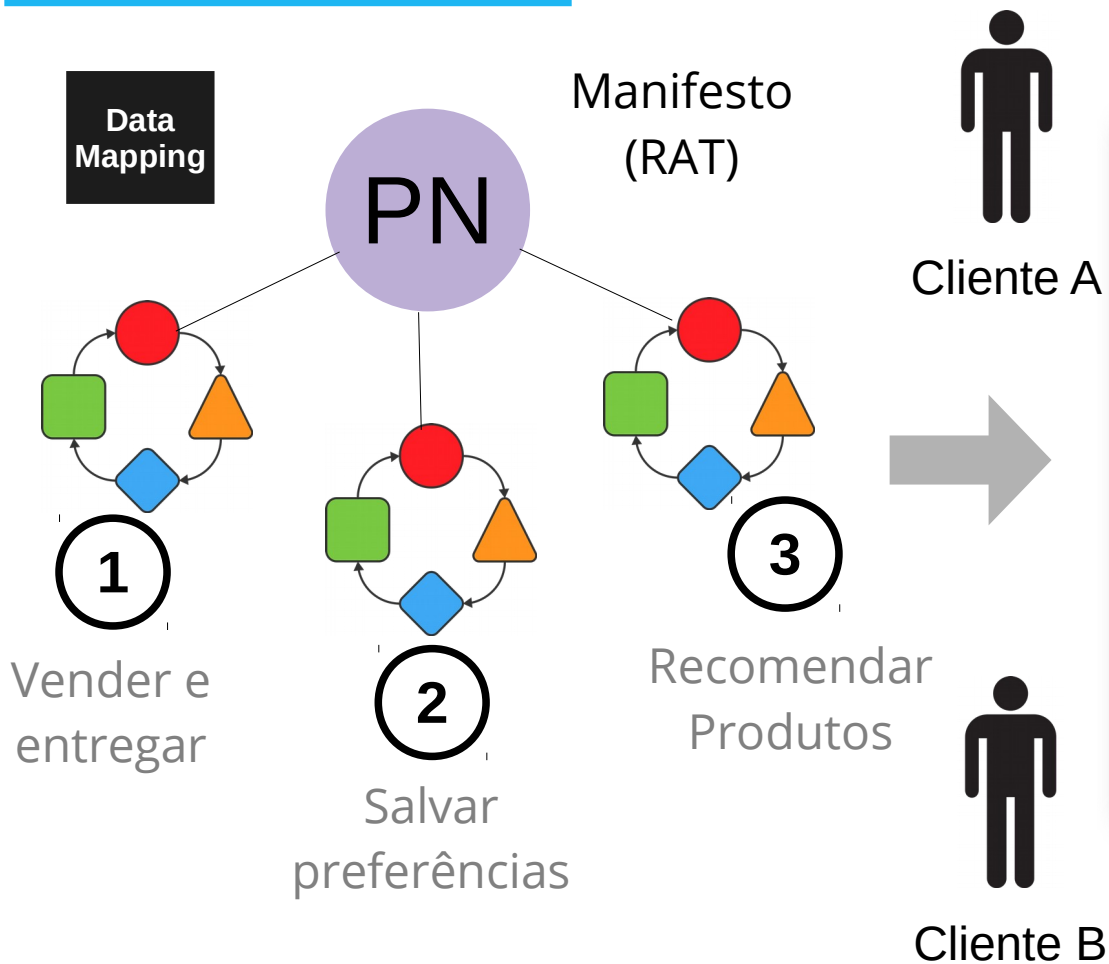
**Base Legal**

#### “Legítimo Interesse”

*Artigo 7, IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados p...;*

# Desafio Operacional do Marketplace

## Registrar Atividades de Tratamentos



## Registro de Ocorrências

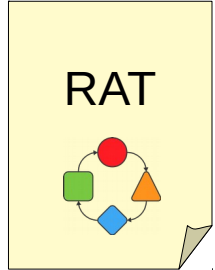
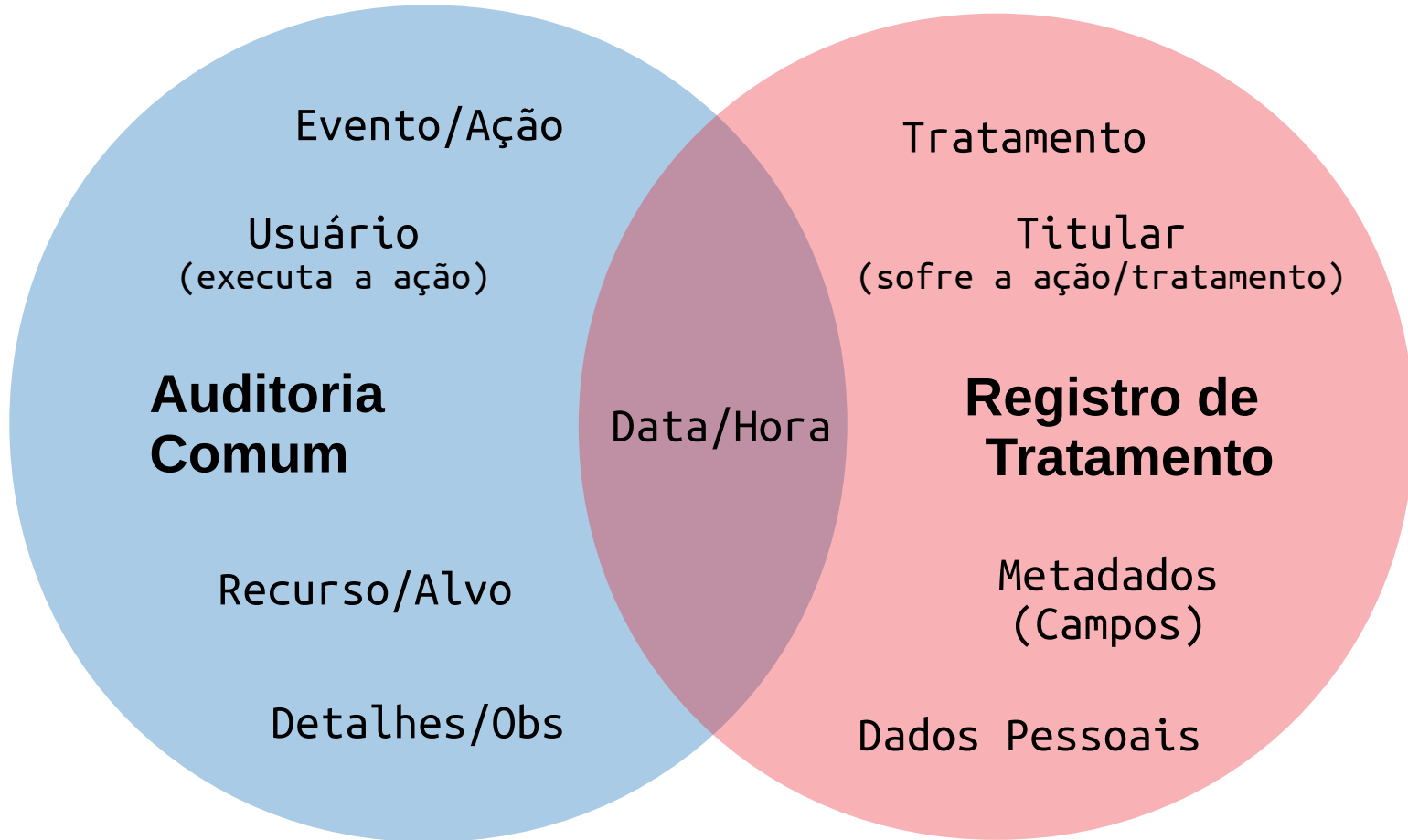
The notebook is open, showing two blank pages. Each page has a red vertical line on the left and right sides, and a red horizontal line at the top labeled "Date:". The pages are ruled with blue horizontal lines. At the bottom of each page, there are two fields: "Verified By:" and "Sign:". The notebook has a black spiral binding in the center.

LGPD Artigo 37: O controlador e o operador devem **manter registro** das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse

# Auditoria x Registro de Tratamento

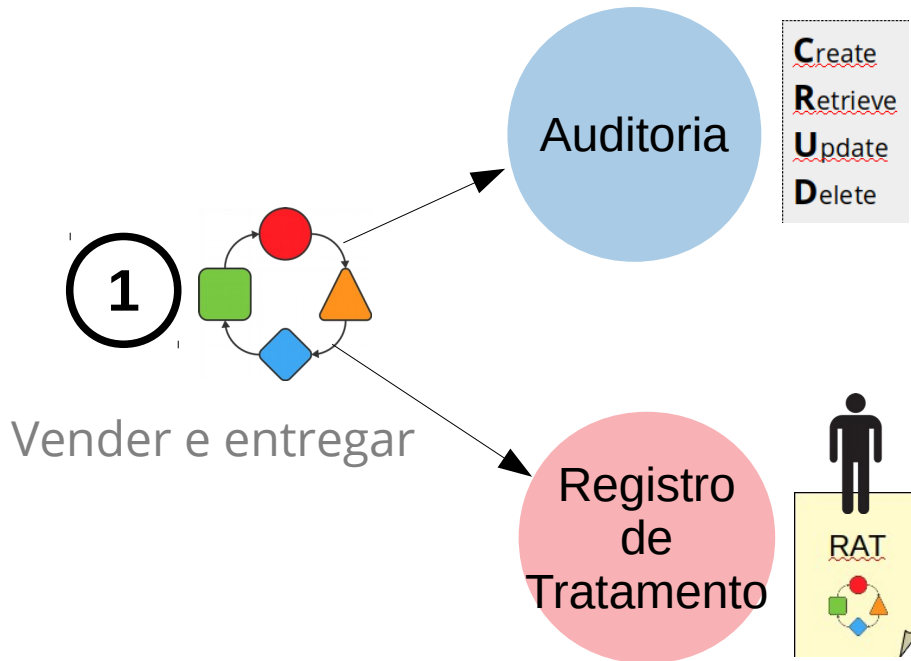
## Semelhanças e Diferenças

**C**reate  
**R**etrieve  
**U**pdete  
**D**elete



# Exemplo do Marketplace

## Tratamento 1: Vender e Entregar



05/05/2021 18:19 | Inserir | Pedido | P034

05/05/2021 18:19 | Inserir | Item | Prod 1

05/05/2021 18:19 | Inserir | Item | Prod 2

05/05/2021 18:19 | Alterar | Produto | Prod1

05/05/2021 18:19 | Alterar | Produto | Prod1

05/05/2021 18:19 | Tratamento 1 | Titular B

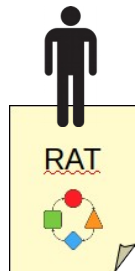


# Auditoria x Registro de Tratamento

## Semelhanças e Diferenças

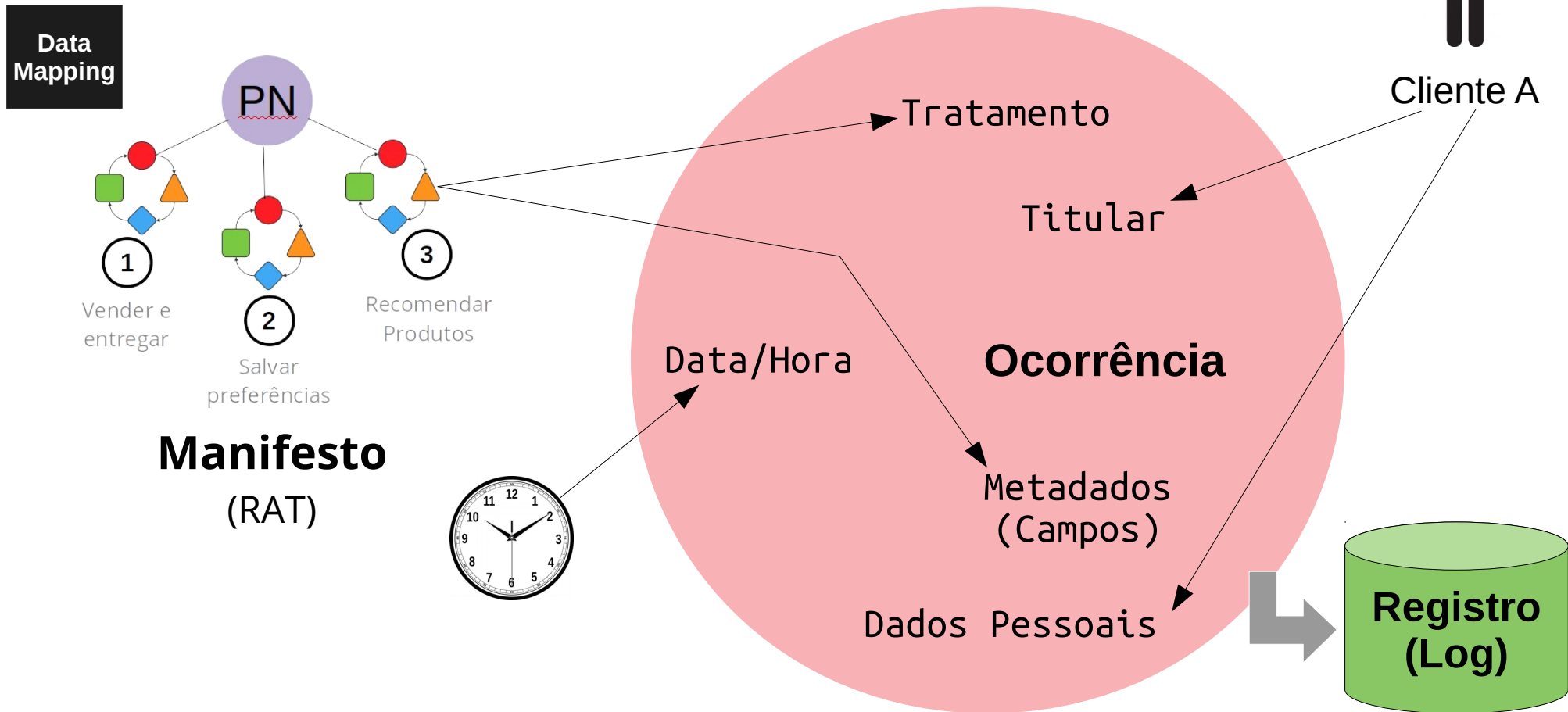
- Auditorias comuns não estão preparadas para registrar tratamentos
- Os **propósitos** e **estruturas** são diferentes
  - Auditoria: registro de **ações** de certos **usuários** e **eventos** do sistema
  - Registro de Tratamento: ocorrência de um **tratamento** para um certo **titular**
- É possível aproveitar a auditoria, mas ela precisa ser **adaptada** (trabalhoso)
- Muitos itens de auditoria não são tratamentos de dados pessoais
- Muitos itens de registro de tratamento não são auditáveis (sem usuário)

Create  
Retrieve  
Uppdate  
Delete



# O Registro de Tratamento

## Manifesto + Ocorrência



# Estratégias de Implementação

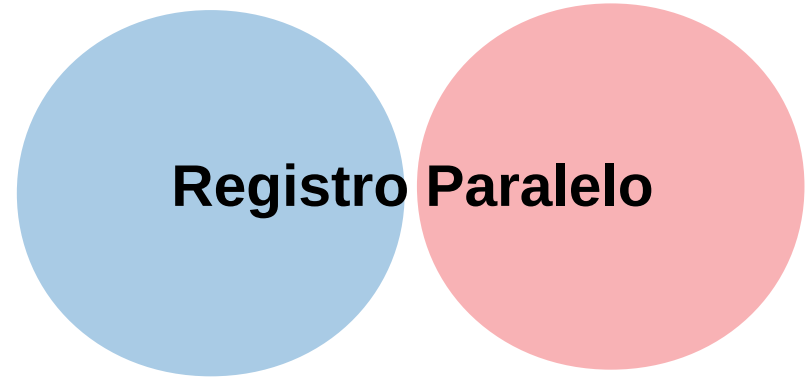
Adaptado ou Paralelo

---



A auditoria existente é adaptada e recebe os campos necessários para fazer o registro de tratamento.

Os eventos costumam mudar bastante, pois as **ações** estão relacionadas a **tratamentos**. O conteúdo precisa identificar o **titular**.




O registro de tratamentos é criado como **módulo separado** e faz os registros em função dos eventos de tratamento.

Os **pontos de log** dentro da aplicação são diferentes. Cada tratamento do **RAT** deve estar presente no log da aplicação.

# Adaptação da Auditoria

## Reaproveitamento de Campos



Auditoria Adaptada

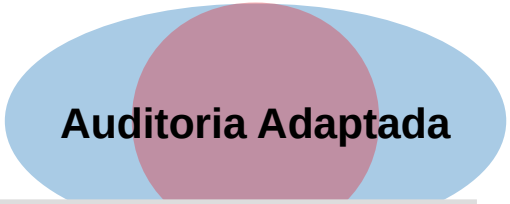
Data/Hora	Data/hora do evento de auditoria ou do tratamento de dado pessoal
Evento/Ação	Devem ser criados eventos para cada <b>tratamento</b> ou aproveitar os eventos que <b>são</b> os próprios tratamentos (evento = tratamento)
Usuário (executa a ação)	Não há alteração. A LGPD não pede “quem”, mas a informação é útil
Recurso/Alvo	Precisa fazer referência ao <b>titular</b> . Registro, ficha, cadastro ou qualquer Coisa que remeta diretamente ao titular afetado pelo tratamento
Detalhes/Obs	Precisa conter os <b>metadados</b> e os <b>dados*</b> tratados

\* cuidado com o Log Hell

# Adaptação da Auditoria

## Estrutura Híbrida

---



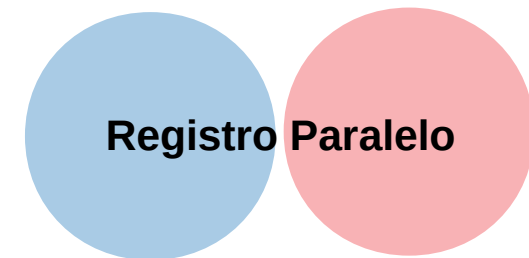
Auditoria Adaptada

Data/Hora	Data/hora do evento de auditoria ou do tratamento de dado pessoal
Evento/Ação	Identificação dos eventos ou ações do ponto de vista do sistema
Tratamento	Identificação dos tratamentos de dados associados aos eventos ou não
Usuário (executa a ação)	Não há alteração. A LGPD não pede “quem”, mas a informação é útil
Titular (executa a ação)	Identificação do Titular neste campo específico para isso
Recurso/Alvo	Continua apontando para tabelas, funcionalidades e outros recursos Que fazem sentido do ponto de vista do sistema/software
Detalhes/Obs	Precisa conter os <b>metadados</b> e os <b>dados</b> tratados

# Registro Paralelo

## Estrutura Especializada

---



Data/Hora	Data/hora da ocorrência do tratamento de dado pessoal
Tratamento	Código ou identificação do tratamento descrito no RAT
Titular	Identificação do titular. Preferencialmente pseudonimizado
Metadados	<b>[OPCIONAL]</b> No RAT já deve ter os metadados de um tratamento, mas Pode ser necessário em casos particulares
Dados Tratados	<b>[OPCIONAL]</b> Depende da estratégia de recuperação e da natureza dos dados
Detalhas/Obs	<b>[EVENTUAL]</b> Informações sobre compartilhamento e outros detalhes

# Objetivos de Qualquer Estratégia

Responder a Perguntas e Prestar Contas

---



1. Quais **tratamentos** definidos no **RAT** ocorreram e quando?  
(onde no registro está a ocorrência do que foi manifestado)
2. Quais tratamentos foram feitos para um certo **titular**?
3. Quais **metadados** (campos) foram tratados desse titular?
4. Quais **dados** pessoais foram tratados desse titular?
5. O que e com quem foi **compartilhado** desse titular?

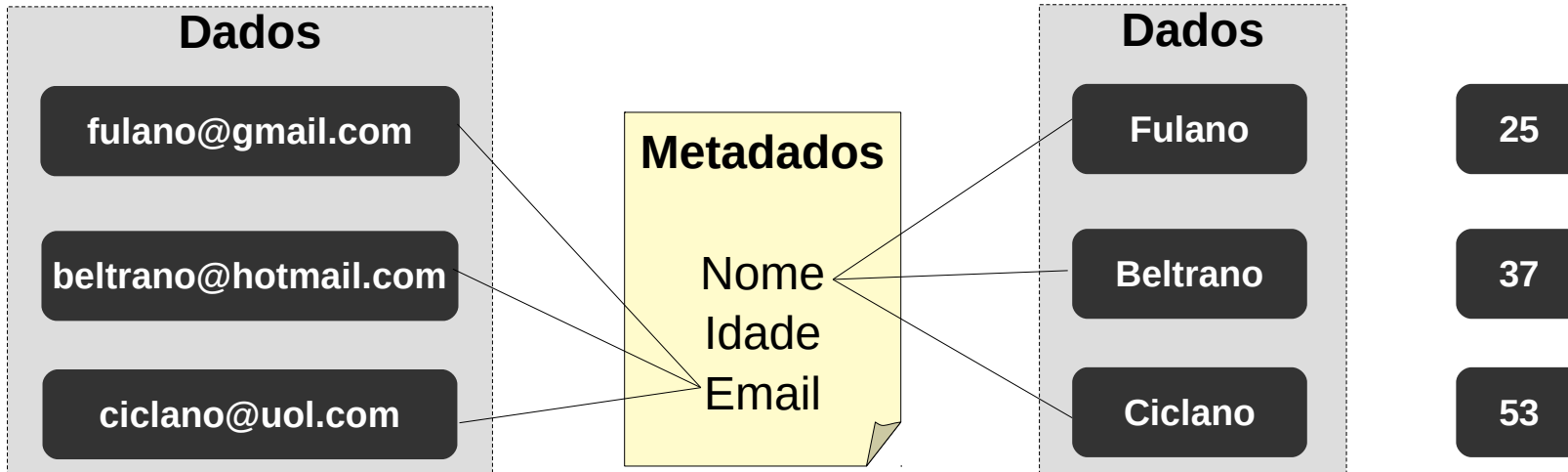
A blank ledger page with a central spiral binding. The page is divided into two columns by a vertical line. Each column has a header 'Date:' at the top. At the bottom of each column, there are labels 'Verified By:' and 'Sign:'. The page contains several horizontal lines for writing.

# Questões Chave

## Análise Caso a Caso



1. Onde colocar os **gatilhos** de log/registo de tratamentos?
2. Quais **Metadados** devem estar no log/registo?
3. Quais **Dados** devem estar no log/registo?





# Pontos de Log

## Onde Colocar os Gatilhos?

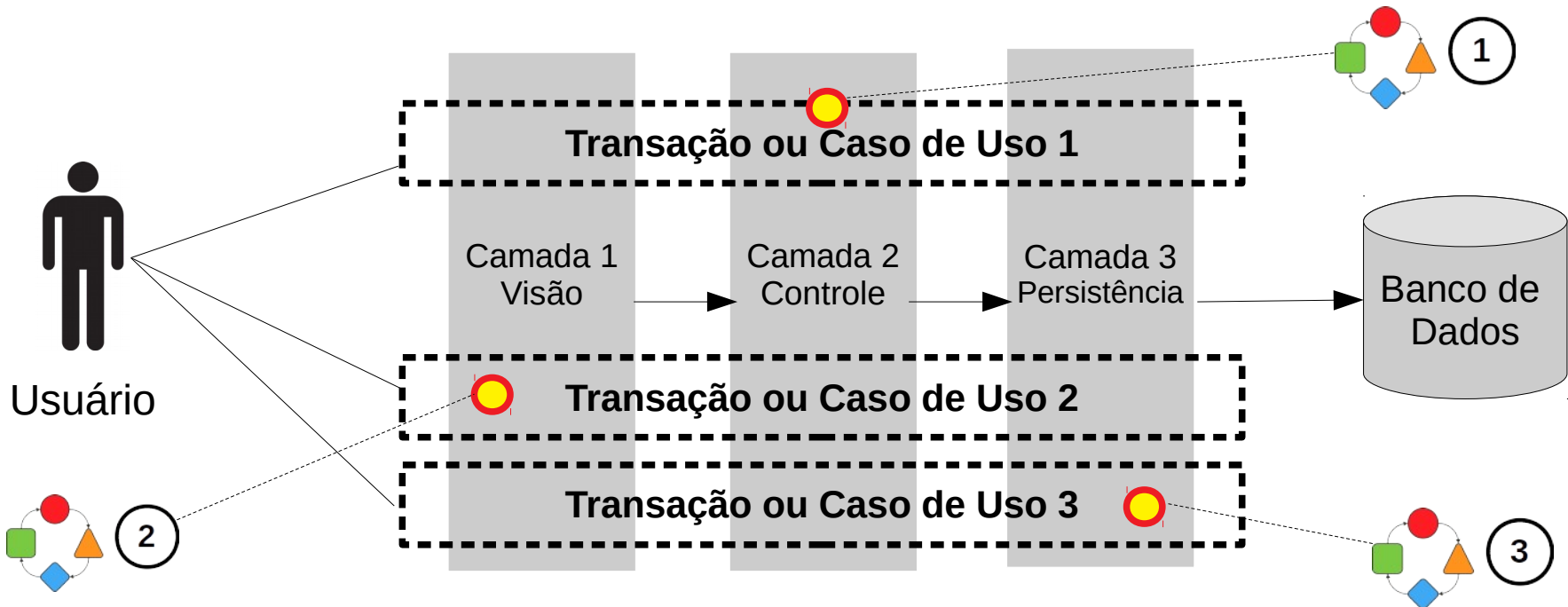
Pontos de Log



na aplicação

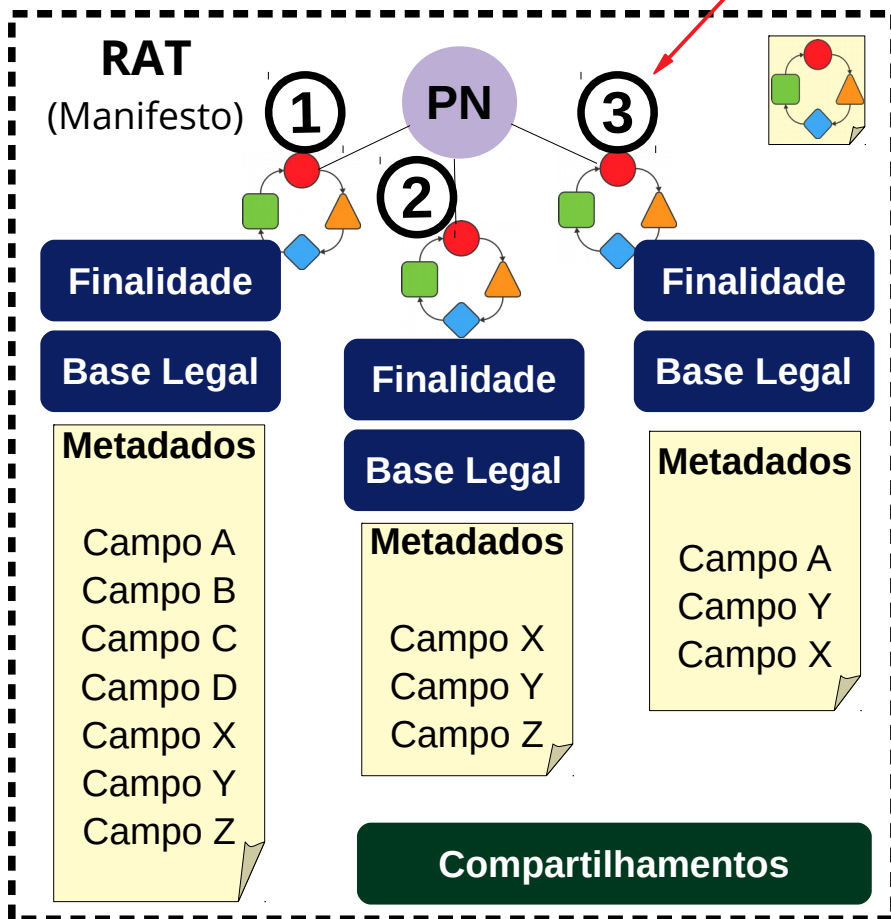
Cada **tratamento** descrito no RAT deve gerar **um ponto de log** na aplicação

Os tratamentos costumam estar associados às **transações** de negócio



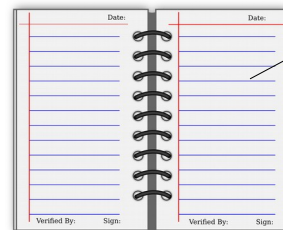
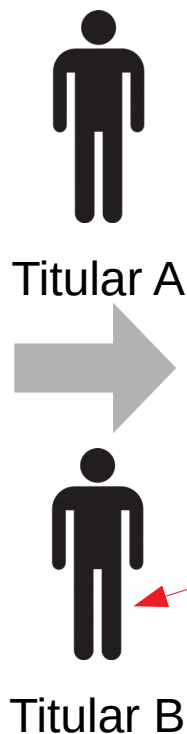
# Metadados

O que deve ir pro Log?



## Referência

Se o RAT já descreve os campos, não é necessário logar metadados para prestar contas do que foi tratado



**05/05/2021 18:19**  
**Tratamento 3**  
**Titular B**

**Referência**  
(pseudonimizado)

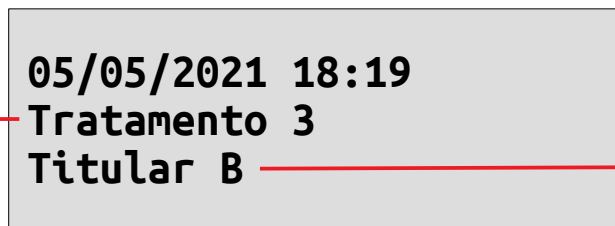
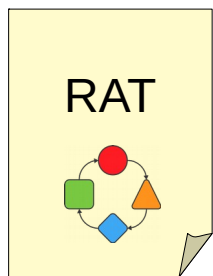
Os compartilhamentos devem ser logados um por um independente do RAT pra saber quando, o que, com quem e de quem foi compartilhado

# Dados Tratados: Nível de Log 1

O que deve ir pro Log?

1

- **Nível 1:** Registra somente o essencial da ocorrência e referencia o resto
- Melhor cenário: Usar “Referência” para metadados e dados do titular



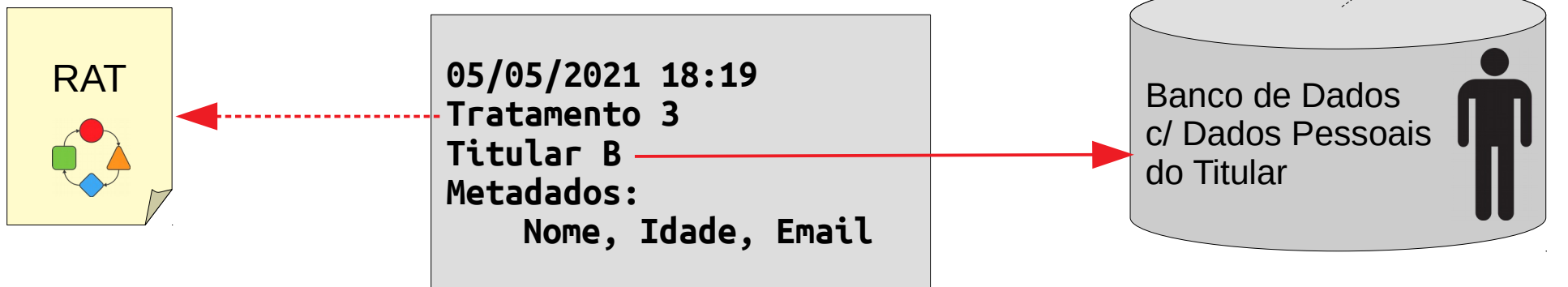
Lembre-se: Log com os dados tratados também é dado pessoal e requer cuidados

## Dados Tratados: Nível de Log 2

O que deve ir pro Log?

2

- **Nível 2:** Registra os metadados tratados e **referencia** os dados
- Cenário: Metadados mudam com frequência ou há subconjuntos



Salvar os parâmetros de uma consulta sem o resultado é uma espécie de nível 2

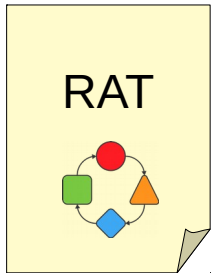
Para consultas em massa (muitos registros) pode ser a melhor escolha

# Dados Tratados: Nível de Log 3



## O que deve ir pro Log?

- **Nível 3:** Registra os metadados e os dados tratados
- Cenário: Metadados e **dados** mudam com frequência ou há subconjuntos



05/05/2021 18:19  
Tratamento 3  
Titular B  
Metadados e Dados:  
Nome : Fulano  
Idade: 25  
Email: fulano@gmail.com

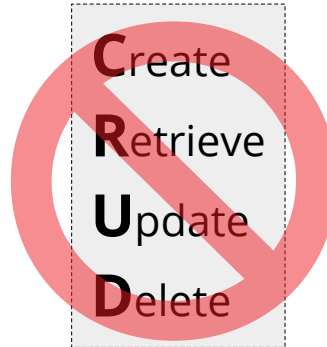
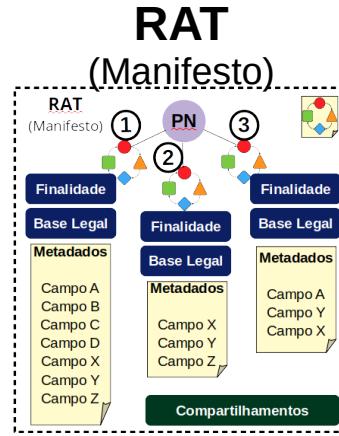
Consultas em massa de titulares é recomendado guardar apenas os **parâmetros** (query/nível 2) e não todos os dados obtidos (Log Hell)

Nos casos de **compartilhamento** é recomendado log nível 3 com registro detalhado (foto) do que foi enviado para outro controlador

# O Que Fazer Agora?

## Ações Imediatas

1. Elaborar um **RAT** ou similar
  - Data Mapping, Catálogo de Tratamentos
  - Evite usar operações "CRUD"
2. Criar um Log para **tratamentos** e outro para **compartilhamentos**
3. Identificar **pontos de Log** na App
4. **Implementar** gravação dos Logs
5. **Gerenciar** o conteúdos dos Logs (Guarda, backup, leitura, recuperação)



Usuário A  
(Titular)



Usuário B  
(Titular)



# Nossos Contatos

---

DÉBORA MODESTO



 deb.modesto@gmail.com

 /modestodebora

DOUGLAS SIVIOTTI



 douglas.siviotti@gmail.com

 /douglas-siviotti



[instagram.com/  
artessoftware](https://www.instagram.com/artessoftware)



[artessoftware.com.br](https://artessoftware.com.br)



[facebook.com/  
artessoftware.com.br](https://www.facebook.com/artessoftware.com.br)