



Aplicação da Lei Geral de Proteção de Dados – LGPD no Setor Público e no STJ

Lei 13.709, de 14/8/2018

Sumário Geral:

Aplicação da LGPD ao Setor Público e no STJ

- AULA 1: Revisão geral: princípios, fundamentos, conceitos, classificações e HL. Principais atores da LGPD e suas funções no Setor Público
- AULA 2: Direitos dos titulares de dados pessoais na prática
- AULA 3: Gestão de programa de privacidade em conformidade com a LGPD
- AULA 4: 10 passos para fazer adequação à LGPD no Setor Público.
- AULA 5: LGPD na prática do STJ e os principais entregáveis (relatórios e documentos).

Avaliação interativa e premiação!





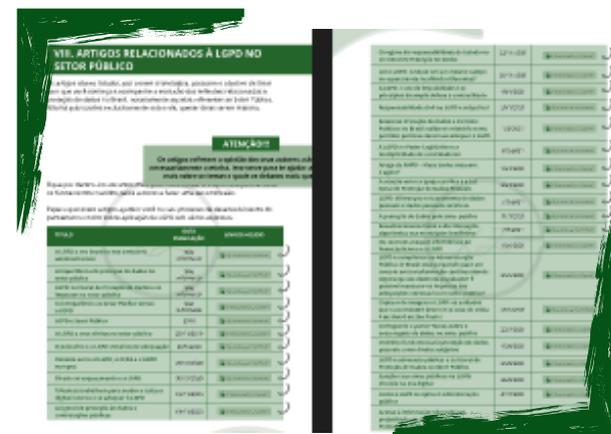
- ✓ O QUE É A LGPD
- ✓ A QUEM SE APLICA
- ✓ QUANDO NÃO INCIDE
- ✓ PORQUE ÓRGÃOS PÚBLICOS PRECISAM SE ADEQUAR
- ✓ QUAIS AS CONSEQUÊNCIAS DA NÃO ADEQUAÇÃO
- ✓ QUAIS AS MAIORES VANTAGENS
- ✓ UM BREVE HISTÓRICO DA LGPD
- ✓ NORMAS RELACIONADAS À PROTEÇÃO DE DADOS NO BRASIL.



Informações organizadas, todas com *links* de acesso direto para legislações, guias orientativos ANPD, pesquisas, artigos, vídeos e *sites* que tratam sobre a temática de privacidade e proteção de dados dentro do Setor Público.

O conteúdo para consultar, estudar ou simplesmente conhecer e saber TUDO sobre esse assunto, ainda em construção por doutrinadores, juristas e a própria ANPD.

Está tudo aqui!!



VAMOS NOS CONHECER MELHOR?

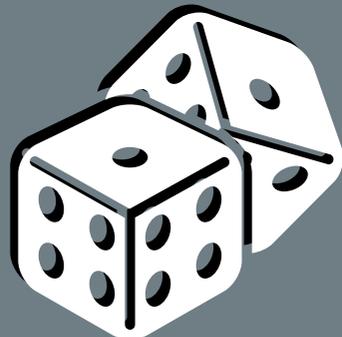
Digite o endereço abaixo:

www.menti.com



Insira o código na tela a seguir e siga as orientações.

Em seguida, vamos fazer uma dinâmica... continue lá!



Vazamento de dados do SUS

Em 2019, [uma matéria do UOL](#) relatou o vazamento de dados de cerca de 2,4 milhões de usuários do SUS (Sistema Único de Saúde), supostamente expostas no dia 11 de abril daquele ano.

Nesta sexta-feira (28/1) é celebrado o Dia Internacional da Proteção de Dados. Há uma semana (21/1), o Banco Central deu um exemplo de por que o tema está em alta: a autoridade monetária comunicou um incidente de segurança com vazamento de dados pessoais vinculados a chaves PIX sob responsabilidade de uma empresa de pagamentos (leia mais na lista abaixo).

Vazamento de dados na internet expõe servidores públicos

2 de junho de 2021

LGPD Brasil

Da Redação

Entenda como acontece o vazamento de dados públicos

Uma denúncia do jornal Folha de São Paulo apontou um comércio ilegal de cadastros do SUS, Receita e INSS. Entenda o vazamento de dados.

Compartilhamento ilegal de dados por órgão público gera direito a indenização

LGPD proíbe ao poder público transferir informações pessoais a entidades privadas sem o consentimento do segurado

Turma Recursal da Seção Judiciária de São Paulo/SP confirmou decisão que determinou ao Instituto Nacional do Seguro Social (INSS) indenizar os morais a segurada por compartilhamento ilegal de dados.

3) Vazamentos de dados no Ministério da Saúde

Em dezembro de 2020, reportagem do jornal O Estado de S. Paulo revelou que dados de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) ou como beneficiários de planos de saúde ficaram expostos na internet por falhas de segurança do Ministério da Saúde.

2) Operação Deepwater

Em janeiro do ano passado, a Autoridade Nacional de Proteção de Dados (ANPD) requisitou que a Polícia Federal abrisse uma investigação para apurar o vazamento de dados de mais de 223 milhões de brasileiros — número maior que a população do país, uma vez que a base de dados incluía até pessoas falecidas. O vazamento foi identificado pela empresa PSafe.

5) Vazamentos de dados da Enel em Osasco

Em novembro de 2020, cerca de 290 mil clientes da concessionária de energia Enel em Osasco, na Grande São Paulo, tiveram informações sensíveis vazadas após falha de segurança. Além de dados cadastrais, vazaram índices de leitura, nível de consumo e histórico de pagamentos.

Processos Administrativos Sancionadores instaurados pela ANPD:

Da lista de 8, apenas
1 era setor privado!!

• **Ministério da Saúde**. Setor Público. Instaurado em 07/03/2022. Com o intuito de investigar a ausência de encarregado de dados pessoais; ausência de comunicação a titulares de incidente de segurança processual. *Processo nº 00261.000456/2022-12.*

• **Telekall**. Setor Privado. Instaurado em 10/03/2022. Com o intuito de investigar a ausência de registro de operações; não envio de Relatório de Impacto de Proteção de Dados Pessoais; não requisição da ANPD. Atualmente se encontra na fase de instrução processual.

• **Instituto de Pesquisas Jardim Botânico**. Setor Público. Instaurado em 10/06/2022. Com o intuito de investigar a ausência de comunicação de incidente de segurança processual. Atualmente se encontra na fase de instrução processual. *Processo nº 00261.000574/2022-21.*

• **Secretaria de Educação do Distrito Federal**. Setor Público. Instaurado em 10/06/2022. Com o intuito de investigar a ausência de comunicação a titulares de incidente de segurança processual. Atualmente se encontra na fase de instrução processual. *Processo nº 00261.000574/2022-21.*

• **Instituto de Pesquisas Jardim Botânico**. Setor Público. Instaurado em 12/09/2022. Com o intuito de investigar a ausência de comunicação de incidente de segurança processual. Atualmente se encontra na fase de instrução processual. *Processo nº 00261.000574/2022-21.*

• **Secretaria de Estado da Saúde de Santa Catarina**. Setor Público. Instaurado em 14/09/2022. Com o intuito de investigar a ausência de comunicação a titulares de incidente de segurança processual. Atualmente se encontra na fase de instrução processual. *Processo nº 00261.001886/2022-51.*

Tinha o mesmo órgão
público 2X!!

• **Instituto de Assistência ao Servidor Público Estadual de São Paulo – IAMSPE**. Setor Público. Instaurado em 14/09/2022. Com o intuito de investigar as condutas: ausência de comunicação a titulares de incidente de segurança processual. Atualmente se encontra na fase de instrução processual. *Processo nº 00261.001969/2022-41.*

• **Secretaria de Desenvolvimento Social, Criança e Juventude-PE**. Setor Público. Instaurado em 14/09/2022. Com o intuito de investigar a ausência de comunicação a titulares de incidente de segurança processual. Atualmente se encontra na fase de instrução processual. *Processo nº 00261.001969/2022-41.*

AULA 1

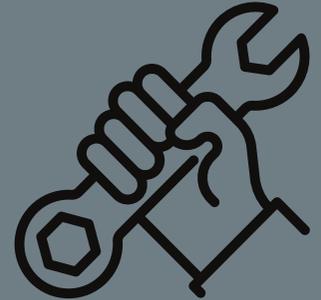
Revisão geral Principais atores da LGPD e suas funções no Setor Público

- Estrutura LGPD
 - Princípios ADM. Pública e da LGPD
 - Fragmentação legislativa e proteção de dados
 - Principais conceitos LGPD
 - Principais atores da LGPD:
 - Operador
 - Controlador
 - Encarregado de Dados
 - ANPD e CNPD
- (+ titular: Aula 2)



As principais “ferramentas de trabalho” com LGPD no Setor Público:

- Habilidade de comunicação clara, objetiva e assertiva.
- Autonomia gerencial e confiança da alta administração.
- Transparência e prestação de contas frequentes.
- Treinamento e conscientização como capacitação contínua.
- Conhecimentos mínimos ou habilidades com sistemas e ferramentas de TI/SI, direito e gestão administrativa.
- Noção de governança e gestão de processos e análise de riscos.
- Conhecimento de normas e regulamentos da atividade-fim ou das políticas públicas desenvolvidas pelo ente público.
- Vontade de aprender todo dia, de não ter medo do novo, de estudar e testar.
- Escrita inovadora aplicada a documentos e ideias criativas para soluções necessárias.



Norte: boa-fé.



Revisão Geral:

Aspectos jurídicos e técnicos da LGPD no Setor Público (escopo de atuação)



TRIPÉ ESTRUTURAL

Principiologia e conceitos básicos aplicados à LGPD no Setor Público

- Os princípios gerais aplicáveis à Administração Pública (legalidade, impessoalidade, moralidade, publicidade e eficiência) e a fragmentação legislativa
- Princípios da transparência (ativa e passiva) e do livre acesso.
- Princípios da finalidade e da adequação
- Princípios da necessidade, da qualidade dos dados e da segurança: a questão dos dados abertos e a sua relação com os princípios do Livre Acesso, da Qualidade, da Transparência e da Necessidade
- Princípios da prevenção e da não-discriminação
- Princípio da responsabilização e prestação de contas

Princípios da Legalidade, da Moralidade e da Eficiência



1. Legalidade X Legalidade estrita

2. Moralidade X Credibilidade

3. Eficiência X Eficácia X Efetividade



CUSTO



RESULTADO



IMPACTO

EFICIÊNCIA

CUSTO

fazer corretamente

utilizar produtivamente
os recursos

custo-benefício

mínimo de perdas e/ou
desperdícios

EFICÁCIA

RESULTADO

fazer o que deve ser feito

capacidade de atingir
objetivos

cumprir metas

realiza o que foi
proposto

EFETIVIDADE

IMPACTO

fazer corretamente o
que tem que ser feito

transformar a
situação existente

mudança e
desenvolvimento

relação entre a produção
e capacidade de produzir

Princípios da LGPD



1. **Finalidade:** propósito **LEGÍTIMO, ESPECÍFICO E EXPLÍCITO**. Informado ao titular. Não adicionar ou alterar sem comunicar ao titular. Sem possibilidade de tratamento posterior de forma incompatível com isso.
2. **Adequação:** tratamento **COMPATÍVEL** com a finalidade.

3. **Necessidade:** LIMITAÇÃO do tratamento ao que for estritamente necessário. Dados PERTINENTES, PROPORCIONAIS e NÃO EXCESSIVOS. (Evite ativos tóxicos!)

4. **Qualidade dos dados:** EXATIDÃO, CLAREZA, RELEVÂNCIA e atualização dos dados.

5. **Livre acesso:** garantia de consulta FACILITADA e GRATUITA. Forma e duração do tratamento: informados. Dados abertos e interoperabilidade.

6. **Transparência:** ATIVA X PASSIVA (LAI) - 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.

7. **Segurança:** (da informação, matriz do DNA da proteção de dados): medidas técnicas e administrativas. PROTEÇÃO DE ACESSOS não autorizados e de situações de perda, alteração, destruição e comunicação (indevida: acidental ou ilícita).

Capítulo VII da LGPD.

8. **Prevenção:** medidas PREVENTIVAS de danos em razão do tratamento de dados pessoais, salvaguardas. **Figura do pai zeloso, preocupado.**

Preocupação voltada a evitar e/ou minimizar riscos de incidentes de segurança, reduzir proporção do dano.

9. **Não discriminação:** mecanismos para evitar o tratamento para fins discriminatórios, ilícitos ou abusivos. **“Não usarás o santo dado do titular contra ele”.**

Tratamento igualitário, respeito ao titular (importante prática de *privacy by design*).

10. **Responsabilização e prestação de contas** (*accountability*): *Accountability* seria a **responsabilidade proativa, prospectiva e rastreável**. Mais que apenas responsabilização, portanto. CHECKS na conformidade.

OBSERVAÇÕES RELEVANTES PARA SETOR PÚBLICO:

- 1)** A questão dos dados abertos e os princípios do Livre Acesso, da Qualidade, da Transparência e da Necessidade: breves reflexões.
- 2)** Princípios da Transparência, do Livre Acesso e da Publicidade (perpassam LGPD e os gerais Setor Público)
 - Livre acesso** (~~≠~~ acesso irrestrito)
 - Publicidade** (transparência, boa-fé, legalidade, controle dos atos normativos Tribunais de Contas)
- 3)** Os princípios do livre acesso, da qualidade, da transparência e da necessidade estão focados, especialmente, em garantir DIREITOS DOS TITULARES DE DADOS.

Os Princípios Gerais LGPD e ADM. Pública

X

Autodeterminação informativa

O que deve ser protegido: porquê e como.
O que pode ser divulgado: porquê e como.



Ponderar:

Limitação da coleta de dados (ADM.PÚBLICA)

X

Escolha em fornecer dados (TITULAR DADOS)

GUIA ORIENTATIVO DA ANPD PARA O SETOR PÚBLICO

Conceito do termo “Poder Público” pela ANPD (Guia Orientativo ANPD):

O termo “**Poder Público**” é definido pela LGPD de forma ampla e inclui órgãos ou entidades dos entes federativos:

União, Estados, Distrito Federal e Municípios e dos três Poderes: **(Executivo, Legislativo e Judiciário + Cortes de Contas e Ministério Público** (art. 1º e 23, LGPD).

Assim, os tratamentos de dados pessoais realizados por essas entidades e órgãos públicos devem observar as disposições da LGPD, ressalvadas as exceções previstas no art. 4º da lei.



ENTIDADES + ÓRGÃOS PÚBLICOS = PODER PÚBLICO (ANPD)

Também se incluem no conceito de Poder Público:

- (i) os serviços notariais e de registro (art. 23, § 4º); e
- (ii) as empresas públicas e as sociedades de economia mista (art. 24),

OBS: No caso das entidades do item II, desde que

- 1) não estejam atuando em regime de concorrência; ou
- 2) operacionalizem políticas públicas, no âmbito da execução destas.

(Guia ANPD Poder Público, p.6)



LEI 14.534, de 11/1/2023

CPF seja adotado como único número do registro geral (RG) no Brasil.

A nova identificação só passará a valer integralmente, no entanto, após adequações feitas por órgãos públicos.

OBJETIVO: determinar um único número ao cidadão para que possa ter acesso a seus prontuários no SUS, aos sistemas de assistência e Previdência Social (Ex: Bolsa Família, o BPC [Benefício de Prestação Continuada] e os registros no INSS).

Também às informações fiscais e tributárias e ao exercício de obrigações políticas, como o alistamento eleitoral e o voto.

A numeração do CPF será protagonista, e os indivíduos não mais terão que se recordar ou valer-se de diferentes números para que os diversos órgãos públicos, bases de dados e cadastros os identifiquem.

LEI 14.534, de 11/1/2023

E qual é esse prazo para ADEQUAÇÃO?

Art. 9º Esta Lei entra em vigor na data de sua publicação e ficam fixados os seguintes prazos:

I – **12 (doze) meses**, para que os órgãos e as entidades realizem a adequação dos sistemas e dos procedimentos de atendimento aos cidadãos, para adoção do número de inscrição no CPF como número de identificação; e

II – **24 (vinte e quatro) meses**, para que os órgãos e as entidades tenham a interoperabilidade entre os cadastros e as bases de dados a partir do número de inscrição no CPF.

CASOS DE CONFLITOS E DE COMPLEMENTARIEDADES com a LGPD:

Ponderação CASO A CASO

| CONFLITOS | COMPLEMENTARES |
|---------------------------|---------------------------------|
| - Liberdade de expressão | - Inviolabilidade da intimidade |
| - Acesso à informação | - Honra e imagem |
| - Interesse público | - Sigilo das comunicações |
| - Propriedade Intelectual | - Sigilo do negócio / de Estado |

QUADRO RESUMO:

Princípios Gerais LGPD e Escopos práticos (finalidades)

| PRINCÍPIOS | ESCOPOS |
|--|---|
| Finalidade Adequação Necessidade | LIMITAR UTILIZAÇÃO DOS DADOS PESSOAIS |
| Qualidade dos dados Transparência Livre acesso | GARANTIR DIREITOS DOS TITULARES DE DADOS |
| Segurança Prevenção Não discriminação | ASSEGURAR A PROTEÇÃO DOS DADOS PESSOAIS |
| Responsabilização e <i>Accountability</i> (prestação de contas) | GARANTIR A APLICAÇÃO DA LGPD E A DEMONSTRAÇÃO DE BOA-FÉ |

Principiologia da LGPD e da Administração Pública: interação com a prática das atividades públicas

Princípios gerais da Administração Pública
(art. 37, CF/88)

X

Fragmentação legislativa proteção de dados

- Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de **legalidade, impessoalidade, moralidade, publicidade e eficiência** [...]

Fundamentos da LGPD

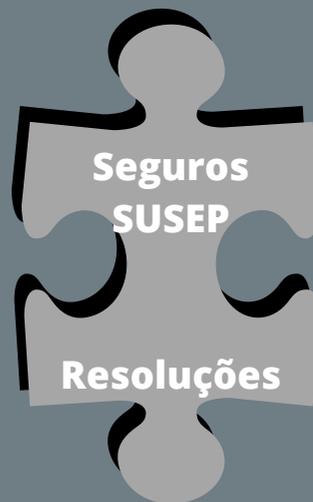
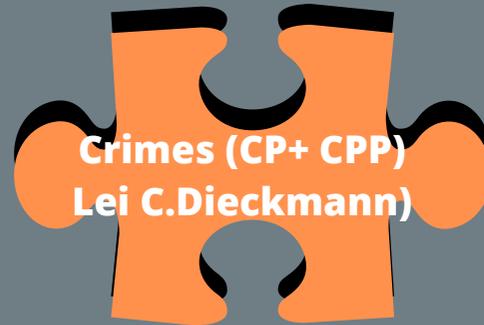
X

Fragmentação Legislativa

1. O respeito à privacidade.
2. A autodeterminação informativa.
3. A liberdade de expressão, de informação, de comunicação e de opinião.
4. A inviolabilidade da intimidade, da honra e da imagem.
5. O desenvolvimento econômico e tecnológico e a inovação.
6. A livre iniciativa, a livre concorrência e a defesa do consumidor.
7. Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

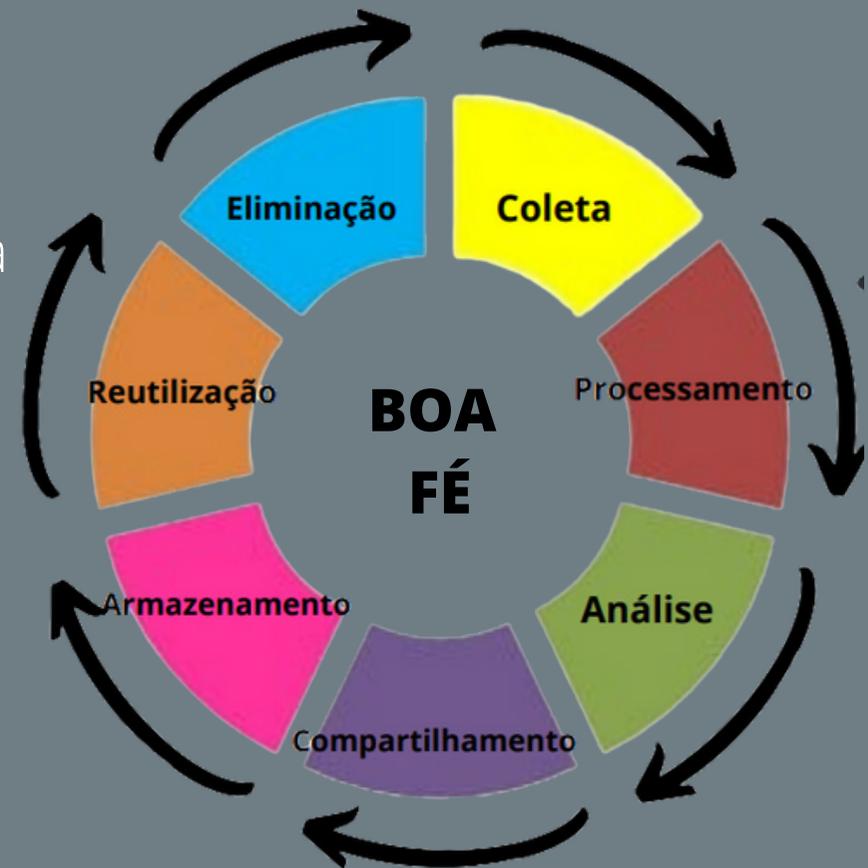
Dispositivo regulamentador: artigo 2º

Fragmentação legislativa X princípios gerais da Administração Pública (art. 37, CF/88)



Conceitos básicos importantes (sobre dados pessoais)

- 1. Importância da leitura atenta e consulta periódica aos dispositivos da norma, especialmente ao art. 5º.
- 2. Processo de adequação: etapas e demonstração de boa fé. Boa fé não está escrita de forma explícita no artigo que regulamenta os princípios mas ela é norteadora.
- 3. Se atentar ao ciclo de dados.



Conceito de tratamento de dados:

Qualquer operação ou conjunto de operações executadas em dados pessoais isoladamente ou em conjunto, independentemente de serem automatizadas. EXEMPLOS:

COLETA

REGISTRO

ESTRUTURAÇÃO

CONSULTA

RECUPERAÇÃO

UTILIZAÇÃO

DIVULGAÇÃO

DELEÇÃO

DISSEMINAÇÃO

Dispositivo regulamentador: art. 5º, X

SOBRE DADOS PESSOAIS:

CONCEITO. O que é dado pessoal?

ELEMENTOS. Identificadores diretos e indiretos. Teoria expansionista.

CLASSIFICAÇÃO dos dados pessoais e o tratamento diferenciado dado pela LGPD a alguns deles (dados comuns, dados sensíveis, dados de crianças e adolescentes, dados anonimizados e dados pseudonimizados).

Dispositivo regulamentador: art. 5º



Classificação dos Dados Pessoais

DADOS PESSOAIS x DADOS PESSOAIS SENSÍVEIS x DADOS DE CRIANÇAS E ADOLESCENTES

Art. 5º, I

Art. 5º, II



Titular de Dados

DADOS ANONIMIZADOS
Art. 5º, III

x
+

DADOS PSEUDONIMIZADOS
Art. 12, §4º

Dados Anonimizados e Pseudonimizados

ANONIMIZADO (art. 5º)

X

PSEUDONIMIZADO (art.12, §4º)

Elimina possibilidade de associação
Irreversível
Deixa de ser dado Pessoal

Elimina possibilidade de associação
Reversível
Continua sendo um dado pessoal



TESTE: É suficiente para identificar alguma pessoa?
O dado pode ser reidentificado?

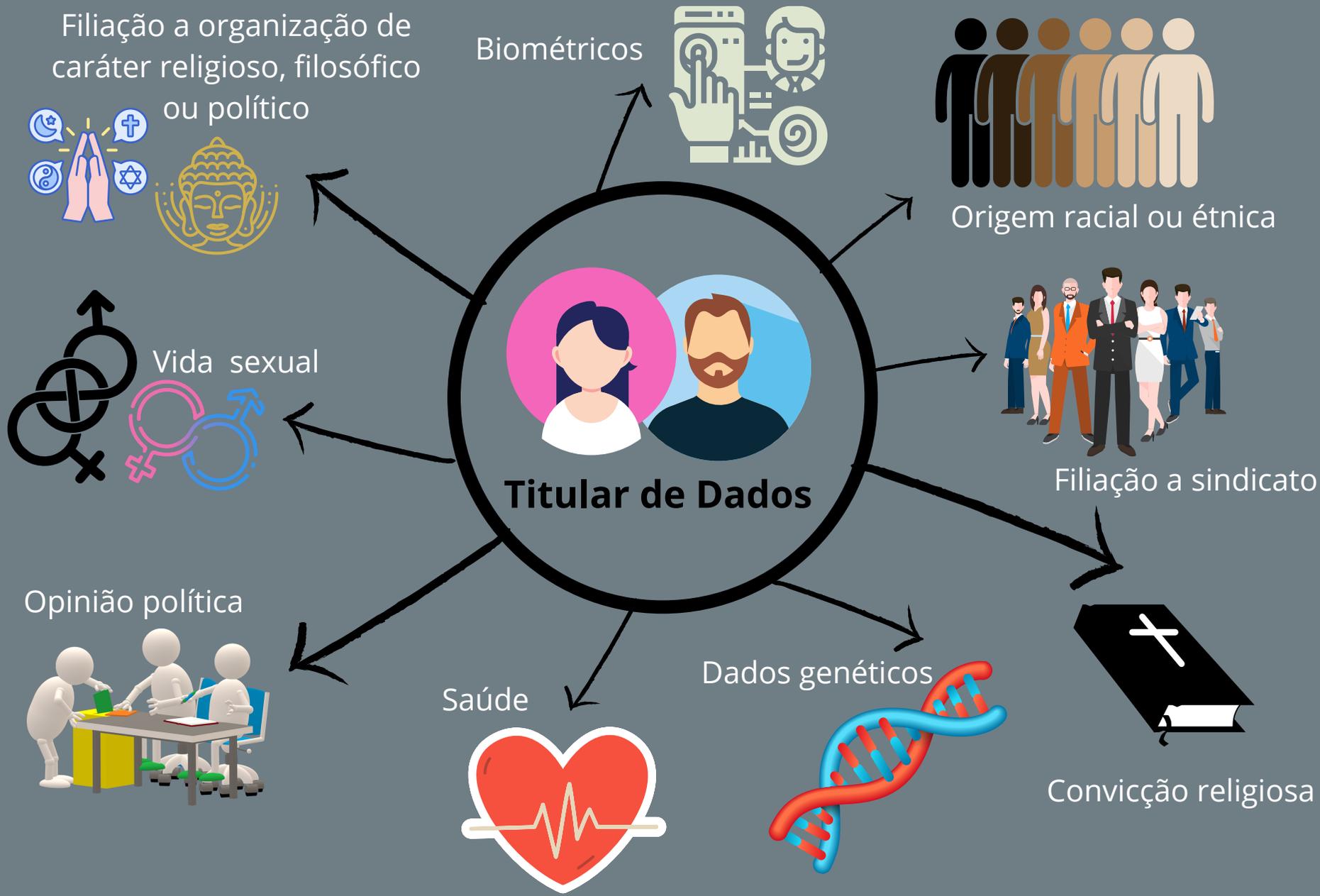
1 0 1 0 1
0 1 0 1 0
↓
1 1 1 0 0
0 1 0 0 1



TESTE: É possível reidentificar o titular do
dado com utilização de informações adicionais?

Dispositivos regulamentadores: arts. 5º e 12, §4º

Dados pessoais sensíveis



Hipóteses para tratamento de dados pessoais

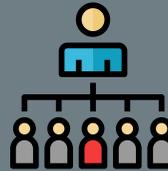
ART. 7º, LGPD



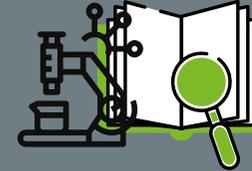
Consentimento do titular



Cumprimento de obrigação legal ou regulatória



Execução de políticas públicas pela Administração Pública



Realização de estudos por órgão de pesquisa



Execução de contrato



Exercício regular de direitos



Proteção da vida ou da incolumidade física



Tutela da Saúde



Legítimo interesse do controlador ou de terceiro



Proteção ao crédito

Execução de Políticas Públicas: hipótese legal EXCLUSIVA para uso da Administração Pública. Prevista para utilização do Poder Público quando for necessário tratamento de dados pessoais para realização de políticas públicas. EXCLUSIVIDADE DA ADMINISTRAÇÃO PÚBLICA.



Interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (LIMITADA PARA ADMINISTRAÇÃO PÚBLICA*).

Precisa fazer um teste (LIA).



Hipóteses para tratamento de dados pessoais sensíveis

ART. 11, LGPD



Consentimento
ESPECÍFICO E DESTACADO
do titular



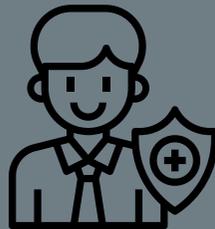
Cumprimento
de obrigação
legal ou
regulatória



Execução de políticas públicas
pela Administração Pública
(APENAS LEIS E REGULAMENTOS)



Exercício
regular de
direitos



Proteção da
vida ou da
incolumidade
física



Tutela da
Saúde



PREVENÇÃO À
FRAUDE E SEGURANÇA

OS ATORES DA LGPD

SUAS PRINCIPAIS FUNÇÕES E RELAÇÕES ENTRE SI

INTRODUÇÃO: Porque precisamos saber quem são e o que fazem? Importância prática.

O CONTROLADOR

Toma decisões referente ao tratamento de dados.
Aquele que decide sobre o tratamento de dados.
Contrato estabelece responsabilidades e seus limites.

Na Administração Pública?

O Ente Público (Ex.: União, Estado, Município, Autarquia, etc...).

Alta administração. Autoridade máxima.



Dispositivos regulamentadores: arts. 8º, §2º; 10, §2º; 42 e 48 da LGPD.

O OPERADOR:

Realiza tratamento de dados em nome do controlador e segundo instruções dele. Contrato estabelece limites. Não tem subordinação hierárquica com o controlador. Por isso, muito cuidado com o que está grifado acima. CNPJ do controlador \neq CNPJ do operador. Ausência de poder diretivo e hierarquia funcional entre operador e controlador.

SERVIDOR NÃO É OPERADOR.



Servidor = “colaboradores internos”, funcionários, empregados... todos que são contratados pelo controlador internamente, corpo funcional da organização.

É a pessoa física prestadora de serviço (contratado formalmente IN 116/2021) ou pessoa jurídica (diversa do controlador), que em seu nome, exerçam atividades de tratamento de dados, em razão de obrigações contratuais ou instrumentos congêneres.



Dispositivos regulamentadores: arts. 37; 39; 42, I; 44, §único e 50 da LGPD.

Destaque importante: **ATENÇÃO!**



QUEM PODE SER AGENTE DE TRATAMENTO:

São agentes de tratamento **o controlador e o operador** de dados pessoais, os quais podem ser pessoas naturais ou jurídicas, de direito público ou privado.

Ressalta-se que os agentes de tratamento devem ser definidos a partir de seu **caráter institucional**.

Não são considerados controladores (autônomos ou conjuntos) ou operadores, os indivíduos subordinados. Tais como: funcionários, servidores públicos ou equipes de trabalho de uma organização.

Motivo: atuam sob o poder diretivo do agente de tratamento.

(Guia ANPD – Agentes de Tratamento, p.5)

- Ou seja a **SUBORDINAÇÃO** retira a possibilidade de existência (co-existência) de operador e controlador dentro da mesma organização.

A responsabilidade dos agentes de tratamento e o ressarcimento de danos: aspectos extrajudiciais e judiciais

O titular de dados pessoais terá direito ao acesso facilitado de informações sobre o tratamento de seus dados pessoais, inclusive de saber sobre as RESPONSABILIDADES DOS AGENTES que realizarão o tratamento deles (art. 9º, VI, da LGPD).

Segundo o 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**.

MAS EM QUE MEDIDA CADA UM?

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.

Por isso sempre importante REGISTRAR EM CONTRATO o limite da responsabilidade de cada agente de tratamento.

Se ocorrer qualquer hipótese de violação do direito do titular no âmbito das **relações de consumo** a LGPD prevê que essas questões permanecerão sujeitas às regras de **responsabilidade previstas na legislação pertinente** (art. 45, da LGPD).

No **Setor Público**, aspecto precisa estar bastante "amarrado" em instrumentos de ajustes com **terceiros diversos do próprio órgão** (outro órgão, empresas privadas, fornecedores de serviços e produtos), seja por meio de contrato, TED, parcerias, convênios, etc... qualquer modalidade de contratação.



RESPONSABILIDADE acerca do COMPARTILHAMENTO DE DADOS PELO SETOR PÚBLICO (LGPD + Guia Orientativo ANPD)

X

Decisão STF ADI 6649/DF e ADPF 695/DF (julgamento conjunto)



As relações de Co-Controle e Suboperação:

Você sabe identificar as relações de:

CO-CONTROLE
X
SUB-OPERAÇÃO 

Art. 42, §1º, II, da LGPD (controladoria conjunta)

Suboperação: não está no texto da LGPD.

Mas segundo a ANPD: “a falta do conceito de suboperador na LGPD não impossibilita ou torna ilegal que ele exista ou que tenha funções, competências e responsabilidade no ambiente de proteção de dados pessoais brasileiro, principalmente porque pode desempenhar a função de operador em subordinação a outro operador”.

(Guia ANPD Agentes de Tratamento, p.19).

Co-controle ou controladoria conjunta, conforme termo utilizado pela ANPD, ocorre quando: “**duas ou mais entidades** possuem uma **intenção comum** sobre as **finalidades e meios de tratamento** e tomam **decisões em conjunto**.”

Em contrapartida, nas decisões convergentes existem decisões distintas sendo tomadas, porém elas se complementam de tal forma que o tratamento não seria possível sem a participação de ambos os controladores”

(Guia ANPD Agentes de Tratamento, p.13).

O suboperador é aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador.

A **relação direta do suboperador é com o operador** e não com controlador. Porém, independentemente dos arranjos institucionais entre operador e suboperador, para efeitos da LGPD, **ambos podem desempenhar**, a depender do caso concreto, **a função de operador e responder perante a ANPD.**

(Guia ANPD – Agentes de Tratamento, p. 19).

Requisitos para verificar a existência de **CONTROLADORIA CONJUNTA (casuística)**:

1. Mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais;
2. Há interesse mútuo de dois ou mais controladores, com base em finalidades próprias, sobre um mesmo tratamento; e
3. Dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades e elementos essenciais do tratamento.

- **NOTAS IMPORTANTES:**

- a. Esse instituto também existe no GDPR (art.26), onde sua existência se dá na medida da constatação da “participação conjunta” com relação às “finalidades e meios de tratamento”.
- b. Nas decisões comuns, duas ou mais entidades possuem uma intenção comum sobre as finalidades e meios de tratamento e tomam decisões em conjunto. Em contrapartida, nas decisões convergentes existem decisões distintas sendo tomadas, porém elas se complementam de tal forma que o tratamento não seria possível sem a participação de ambos os controladores.

SISTEMATIZAÇÃO das relações de Co-Controle e Suboperação

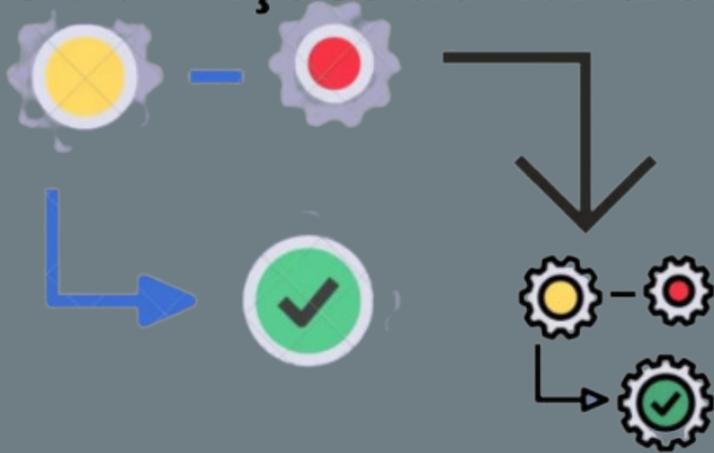
CONTROLADOR é a pessoa natural ou jurídica, de direito público ou privado, que determina como será feito o tratamento de dados pessoais.



OPERADOR é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, ou seja, não decide sobre como será realizado, apenas executa decisões do controlador.

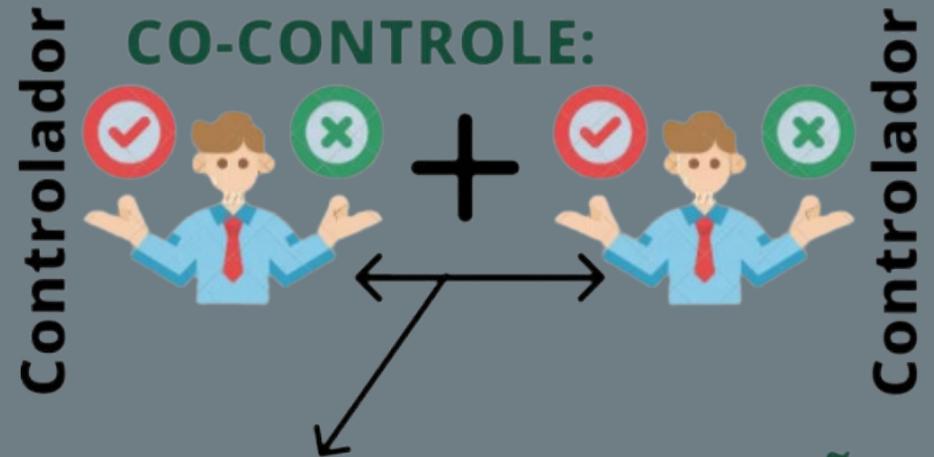


E a figura do **SUBOPERADOR**, surgirá, quando permitida pelo controlador na necessidade de o operador precisar delegar alguma atividade para atender às definições do controlador.



Portanto, nós teremos:

CO-CONTROLE:



SUB-OPERAÇÃO:



Segundo recomendações da ANPD, importante lembrar que, se o “operador realiza o tratamento de dados pessoais em nome do controlador, é de se supor que a relação entre eles esteja fundada na confiança. Nesse sentido, é recomendável que o operador, ao contratar o suboperador, obtenha autorização formal (genérica ou específica) do controlador, a qual pode inclusive constar do próprio contrato firmado entre as partes. Tal medida visa evitar que se entenda que, ao contratar o suboperador, o operador tenha executado o tratamento de dados descumprindo orientações do controlador, o que poderia atrair para o operador responsabilidades que normalmente são exclusivas do controlador”.

(Guia ANPD Agentes de Tratamento).

Exemplos práticos sobre agentes de tratamento (FIXAÇÃO):

Exemplo 1 - Médica profissional liberal.

Uma médica, profissional liberal, armazena os prontuários e os demais dados pessoais de seus pacientes no computador de seu consultório.

A médica, pessoa natural, é a controladora dos dados pessoais.

Exemplo 2 - Médica empregada de um hospital.

Uma médica é empregada de um hospital, constituído sob a forma de associação civil sem fins lucrativos.

Nessa condição, atua como principal representante do hospital junto a um serviço de armazenamento de dados de pacientes em nuvem, inclusive assinando os contratos correspondentes.

O hospital, isto é, a associação civil, pessoa jurídica de direito privado, é o controlador na hipótese.

A médica, por atuar sob o poder diretivo da organização, não se caracteriza como agente de tratamento.

Exemplo 3 - Órgão público contratante de um serviço de inteligência artificial.

Um órgão público, vinculado à União, contrata uma solução de inteligência artificial fornecida por uma sociedade empresária com a finalidade específica de realizar o tratamento automatizado de decisões com base em um banco de dados gerido pelo órgão.

Seguindo as instruções fornecidas pelo gestor público responsável e estabelecidas em contrato, a sociedade empresária realiza as operações necessárias para viabilizar o tratamento dos dados em questão.

A União, pessoa jurídica de direito público, é a controladora na hipótese. Não obstante, o órgão público responsável detém obrigações legais específicas em face dos titulares e da ANPD, conforme previsto na LGPD.

A sociedade empresária é a operadora, uma vez que realiza o tratamento dos dados conforme as instruções fornecidas pelo controlador.

Por fim, o gestor público responsável, por atuar como servidor público subordinado à União, não se caracteriza como agente de tratamento.

Exemplo 4 – Uso de dados abertos disponibilizados por Agência Reguladora.

Agência Reguladora disponibiliza acesso público aos dados relativos às outorgas dos serviços regulados, incluindo informações de pessoas naturais sócias de prestadoras.

A base de dados é armazenada pela própria Agência e utilizada para subsidiar decisões administrativas.

Organização da Sociedade Civil tem acesso aos dados disponibilizados pela Agência e efetua, com base em solução de inteligência artificial, cruzamento com outras bases de dados visando à realização de ações de controle social de entidades e agentes públicos.

Sociedade Empresária também trata os dados em questão, visando, porém, fornecer serviços de consultoria aos agentes do setor regulado.

Embora a mesma base de dados seja utilizada pelas três entidades (Agência Reguladora, Organização da Sociedade Civil e Sociedade Empresária), cada uma dessas organizações é responsável e responde pelos respectivos tratamentos realizados.

Neste contexto, não há controladoria conjunta pois o tratamento de dados ocorre no âmbito das atividades e das finalidades definidas por cada organização.

O ENCARREGADO DE DADOS

Não é agente de tratamento, é ator do Sistema LGPD de proteção de dados

Indicado pelo controlador. Canal de comunicação entre titular e a ANPD e autoridades supervisoras (Procon, MP, TCU...). Gerir atendimento aos titulares. Orientar internamente colaboradores. Crítica e análise de conformidade. Atender às determinações e encargos que a ANPD lhe determinar.

Como ele é responsável pela supervisão da conformidade em proteção de dados, é recomendado que ele não faça a análise de impacto. Porque cabe a ele a crítica, controle e supervisão disso. Como um fiscal.

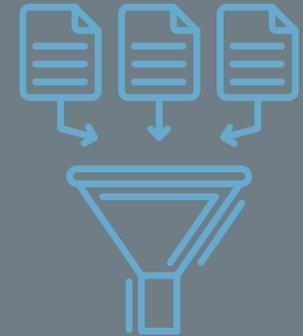
Portanto, para evitar “conflito de interesses” é que há essa orientação.

A LGPD não dispõe expressamente sobre isso, nem há manifestação da ANPD ainda sobre esse ponto específico. Mas há no Gov.br.



QUEM PODE SER? HÁ RESTRIÇÕES? HABILIDADES? RESPONSABILIDADES?

Modalidades: interno / *as a service* / híbrido



**Diferença entre:
Encarregado de dados e gestor de dados.**

IN 117/2020 (SGD/ME): sobre o encarregado de dados Setor Público.

Encarregado de dados (Atenção: DPO no GDPR: mesma coisa?)

**SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO
E GOVERNO DIGITAL**

SECRETARIA DE GOVERNO DIGITAL

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

Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.



DPO na GDPR

Diretiva 95/46/CE  artigo 24 do Regulamento (CE) 45/2001

Previa que cada instituição/órgão nomeasse pelo menos um Oficial de Proteção de Dados (DPO), para garantir de forma independente a aplicação interna das diretrizes (arts. 37 a 39).

Já na lei alemã, considerada uma das primeiras leis sobre o assunto, chamada de BDSG de 1977, o seu § 29 definia algumas tarefas do DPO como por exemplo:

“manter uma visão geral do tipo de dados pessoais armazenados e das finalidades e objetivos comerciais, cujo cumprimento requer o conhecimento desses dados, de seus destinatários regulares e do tipo de sistemas automatizados de processamento de dados utilizados”.

Report on the Status of Data Protection Officers, realizado em 2012 pela Autoridade Europeia de Proteção de Dados (AEPD): dados de DPOs de todas as instituições e órgãos da UE (nome, duração do mandato, status, recursos, posição e outros): visão geral nas instituições e avaliar funções e atribuições.

RESPONSABILIDADES



1. Interação com a ANPD: ponto de contato com o órgão pela Autoridade Nacional, devendo receber suas notificações e adotar as providências necessárias.
2. Atendimento ao titular de dados.
3. Execução de todas as atribuições que lhe forem conferidas pela legislação, pela ANPD e internamente pelo seu órgão.
4. Orientação e instruções sobre LGPD a membros, servidores, estagiários e terceirizados sobre as melhores práticas e posturas relacionadas à privacidade proteção de dados dentro daquele órgão.
5. Recomendar, auxiliar e subsidiar a elaboração do RIPD com o apoio de áreas técnicas.
6. Monitoramento da conformidade das atividades de tratamento de dados pessoais nos termos das legislações e normas vigentes.
7. Opinar sobre privacidade e proteção de dados pessoais em processos internos do órgão quando for demandado.
8. Oferecer suporte ao Comitê ou Comissão de Dados pessoais quando solicitado, ou ainda, diretamente à Alta Administração, em processos de trabalho, ou fluxo de atividades, quando relacionado à privacidade e proteção de dados pessoais.

PERFIL E COMPETÊNCIAS:



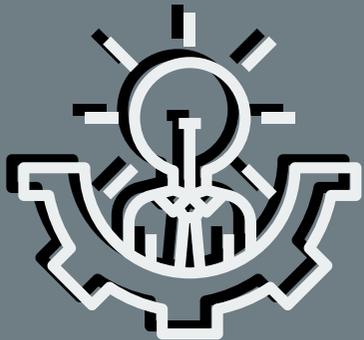
1. Nomeação deverá ser feita pela autoridade máxima do órgão.

2. Deverá ter acesso direto à alta Administração (atendimento a requisito da LGPD de "não subordinação").



3. Deverá prestar pronto apoio às unidades administrativas no atendimento às solicitações de informações.

4. Deverá servir de suporte para atender às dúvidas apresentadas pelo Comitê ou Comissão de dados Pessoais do órgão.



5. Deverá desenvolver habilidades complementares que permitam a efetiva execução das responsabilidades que lhe forem delegadas.

PRINCIPAIS HABILIDADES:



1. Ter conhecimentos multidisciplinares relacionados às áreas de conhecimento sobre: gestão de risco, Direito, TI e SI, compliance e governança de dados, acesso à informação no Setor Público, gestão de pessoal e fluxos de trabalho e de processos, dentre outras.



2. Habilidade de comunicação e interação com pessoas é fundamental e fará toda a diferença na atuação e resultados de seu trabalho.



3. Organização e metodologia de trabalho bem estabelecida facilitará a vida desse profissional que terá demandas e prazos de atendimento muito diversificados.

IMPORTANTE:

A IN que regulamenta esse assunto dentro do Setor Público orienta que não deve ser pessoa lotada em unidade de TI ou ser gestor de sistemas de informação.

Possível conflito de interesses.

Sobre o Encarregado de Dados na CBO

CBO 1435-21: Classificação Brasileira de Ocupações reconheceu a profissão de encarregado de dados pessoais como “Oficial de Proteção de Dados”.

1421-35 - Oficial de proteção de dados pessoais (dpo)

Encarregado de proteção de dados pessoais



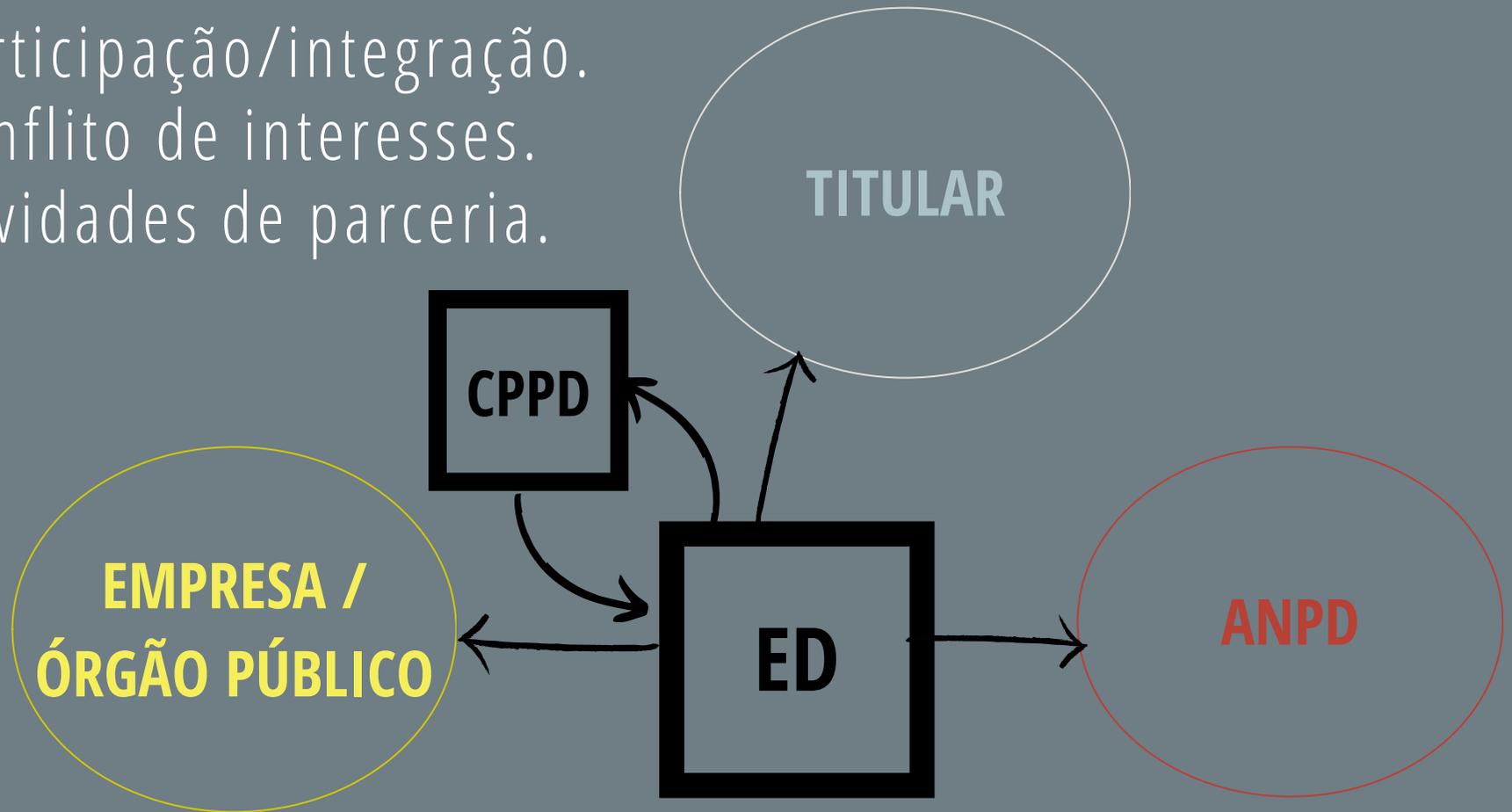
DPO

Descrição Sumária

Planejam processos administrativos, financeiros, de Compliance, de riscos e de proteção de dados pessoais e privacidade. Gerenciam pessoas, rotinas administrativas e financeiras. Administram riscos, recursos materiais, serviços terceirizados e canal de denúncia. Participam da implementação do programa de compliance e/ou de governança em privacidade. Monitoram e avaliam o cumprimento das políticas do programa, normativas, código de ética, procedimentos internos e parceiros de negócios. Participam da identificação de situações de riscos e propõem ações para mitigação dos mesmos. Prestam atendimento ao cliente e/ou cooperado e/ou titular de dados pessoais.

O ENCARREGADO DE DADOS X Comitê de Privacidade de Dados

Participação/integração.
Conflito de interesses.
Atividades de parceria.



O ANPD e o CNPD :

| QUEM | Nat. Jurídica | Provimento cargos | Composição | Mandato | OBS: |
|------------------------------------|---|--|--|---------------------------------|---|
| ANPD Lei 13.853/2019 | Ex Órgão da Adm. Publ Federal – Presid. República (<u>natureza transitória</u>). Atualmente Autarquia Especial (Lei 14.460, de 25/10/2022) | Condicionado à expressa autorização física e financeira LOA e LDO. Cessão de servidores no momento. REMUNERADO | .Cons. Diretor (5) .CNPD .Corregedoria .Ouvidoria .Órgão de Assessoramento Jurídico próprio .Unidades adm. e especializadas | 4 anos (*) | .Cons. Diretor escolhidos e nomeados pelo Pres. Repub, após aprovação Senado (DAS 5). .PAD: Ministro Casa Civil .Afastamento: Pres. Rep. .Quarentena |
| CNPD | Parte integrante da ANPD (abaixo do Conselho Diretor) | SEM REMUNERAÇÃO (prestação de serviço público relevante) | 23 representantes (art. 58-A) | 2 anos (permitida 1 recondução) | .Indicados Pres. Rep (mas é permitida delegação) |

Atribuições da ANPD: art. 55-J da LGPD.

Autonomia técnica e decisória. Gestão administrativa e financeira descentralizadas.

Atribuições CNPD: art. 58-B.

Por hoje é isso!
Até amanhã!

thank you



AVALIAÇÃO INTERATIVA DA AULA 1:

Acesse:

www.kahoot.it

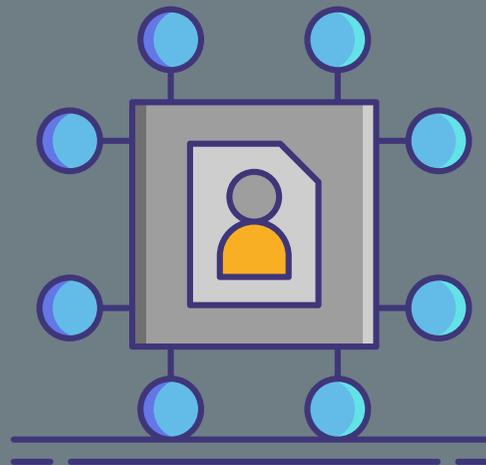


Ao entrar digite o PIN que vai aparecer na tela.

AULA 2

O TITULAR DE DADOS: Exercício de direitos na prática

- Direitos do titular de dados pessoais
- Jornada do titular
- Sistematização e controle de respostas BD
- Governança corporativa – controles internos e externos
- Treinamento de PMO's,
- Gestão e controle de processo de mapeamento



Conceito, direitos dos titulares de dados pessoais e o seu exercício (arts. 17 ao 22 – Capítulo III)

- • Liberdade, intimidade e privacidade
- • Acesso
- • Oposição
- • Informação
- • Portabilidade
- • Peticionar para a garantia dos seus direitos
- • Explicação e revisão de decisões automatizadas
- • Anonimização, bloqueio ou eliminação
- • Direitos do titular
- • Confirmação do tratamento
- • Correção
- • Eliminação
- • Revogação do consentimento

QUEM É O TITULAR DE DADOS? **Pessoa física**, sempre!

(art. 5º, V, da LGPD - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento).

DIREITOS BASE:
Art. 17, LGPD.



ACESSO
RETIFICAÇÃO
CANCELAMENTO
OPOSIÇÃO

MODO DE EXERCÍCIO:
Art. 18, LGPD.

ACESSO

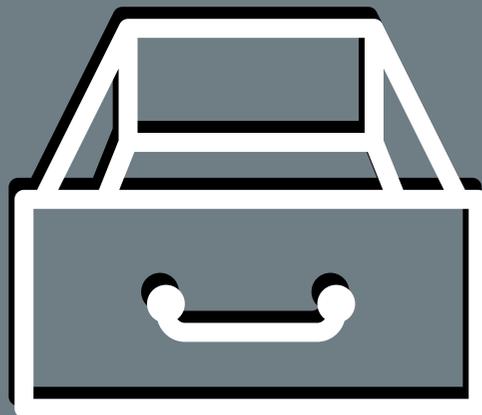
Nessa gaveta estão guardados os seguintes direitos garantidos aos titulares de dados pessoais:

ACESSO

INFORMAÇÃO

CONFIRMAÇÃO

PETICIONAMENTO



LAI: compatibilização. INFORMAÇÃO x DADOS PESSOAIS
Enunciado 4, de 10/3/2022, CGU.
Acesso ativo. Acesso passivo.
Categorização e segmentação de acesso (interno e externo).

Acesso

Art. 18, II, da LGPD:
O titular dos dados pessoais tem direito de acesso aos dados.

Informação

Art. 18, VII e VIII, da LGPD:
O titular dos dados pessoais tem direito a:

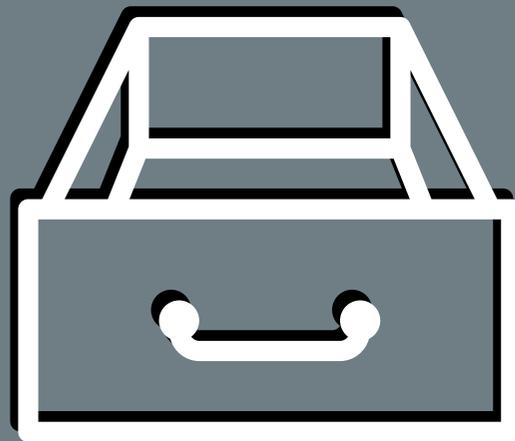
- informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

Confirmação

Art. 18, I, da LGPD:
O titular dos dados pessoais tem direito a confirmar a existência de tratamento.

RETIFICAÇÃO

Já nessa gaveta estão guardados os direitos dos titulares relativos ao PRINCÍPIO DA QUALIDADE, especialmente:



CORREÇÃO

CONFIRMAÇÃO DO TRATAMENTO

Modo de exercício

Art. 18, da LGPD:

O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição.

Confirmação

Art. 18, I, da LGPD:

O titular dos dados pessoais tem direito a confirmar a existência de tratamento.

Acesso para correção

Art. 18, II, da LGPD:

O titular dos dados pessoais tem direito de acesso aos dados.

CANCELAMENTO

Nessa outra aqui estão guardados os direitos dos titulares relativos à AUTODETERMINAÇÃO INFORMATIVA, especialmente.



**ANONIMIZAÇÃO, BLOQUEIO OU
ELIMINAÇÃO
REVOGAÇÃO DO CONSENTIMENTO**

Anonimização, bloqueio e eliminação

Art. 18, IV, da LGPD:

O titular dos dados pessoais tem direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.

Revogação do Consentimento

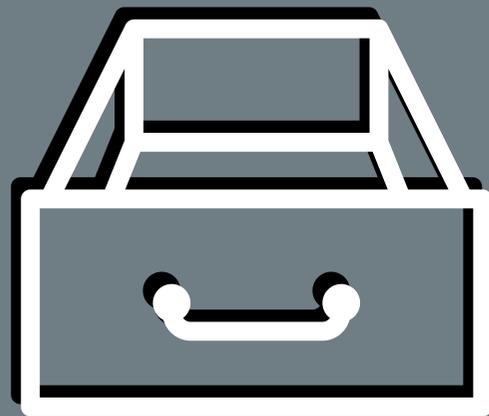
Art. 18, VI, da LGPD:

O titular dos dados pessoais tem direito de eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei.

Art. 18, IX, da LGPD
revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

OPOSIÇÃO

NESSA ÚLTIMA ESTÃO GUARDADOS OS DIREITOS DOS TITULARES RELATIVOS A:



OPOSIÇÃO
EXPLICAÇÃO E REVISÃO
(decisões automatizadas)
PORTABILIDADE

Oposição

Art. 18, §2º, da LGPD:

O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento à LGPD.

Explicação e Revisão

Art. 20, da LGPD:

O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Portabilidade

Art. 18, V, da LGPD:

O titular dos dados pessoais tem direito à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.

ARCO

É um conjunto BASE.

Reúne o que a LGPD explicitou em seu texto sobre o conjunto de direitos garantidos aos titulares de dados pessoais.

Arts. 17 a 22, LGPD.



Revogação do Consentimento



Art. 18, IX, da LGPD
revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Art. 8º, § 5º, da LGPD:
O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18 desta Lei.

Petição perante Autoridade

Art. 18, § 1º § 3º, da LGPD: Modo de exercício?
O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

Art. 18, § 3º, da LGPD: Quem pode peticionar?
Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento

Art. 18, § 5º, da LGPD: Gratuito?
O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

Art. 18, § 8º, da LGPD: Onde mais?
O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Denúncias ou Petições de titular



Informações essenciais para o envio de requerimentos à ANPD

ANPD apresenta nova página para envio de requerimentos

Fluxograma



Identifiquei uma situação de possível descumprimento da LGPD?

SIM

NÃO

É uma situação que afeta direta e especificamente meus dados pessoais de forma individualizada?

Não é competência da ANPD

SIM

NÃO

E tenho o comprovante da solicitação não atendida ou de resposta insatisfatória.

Já entrei em contato com o controlador?

É uma situação que pode afetar/afeta um conjunto de titulares?

Ex.: vazamentos ou descumprimento do dever de controlador publicar seus dados de contato.

SIM

NÃO

SIM

NÃO


Envio de petição.

Entro em contato com o controlador


Envio de denúncia.

Sua situação pode não estar relacionada à LGPD e à atuação da ANPD.

Acompanhada dos comprovantes do contato previamente estabelecido com o controlador.

Por meio de seus canais oficiais (ex.: canais ou contatos disponíveis em páginas de políticas de privacidade).

Sobre possível descumprimento à LGPD.

Em caso de dúvida, consulte nossa seção de perguntas frequentes ou entre em contato por meio de nossos canais de atendimento.

Prazos que a organização terá para responder ao titular:

Art. 19, da LGPD:

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.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento **tiver origem no consentimento do titular ou em contrato**, o titular **poderá solicitar cópia eletrônica integral de seus dados pessoais**, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.



(VIDE RESOLUÇÃO 2/2022, ANPD: prazo em dobro para ME e EPP)

PRAZOS DE RESPOSTA PARA O TITULAR PELO SETOR PÚBLICO

Tem diferença com o setor privado? **SIM!**



IMPORTANTE: ART. 23, §3º, LGPD:

Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da [Lei nº 9.507, de 12 de novembro de 1997 \(Lei do Habeas Data\)](#), da [Lei nº 9.784, de 29 de janeiro de 1999 \(Lei Geral do Processo Administrativo\)](#), e da [Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#).

Como está regulamentado esse assunto nessas legislações?

LHD: art. 1º, parágrafo único e art. 2º: Considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações. O requerimento será apresentado ao órgão ou entidade depositária do registro ou banco de dados e será deferido ou indeferido no prazo de quarenta e oito horas.

A decisão será comunicada ao requerente em vinte e quatro horas.

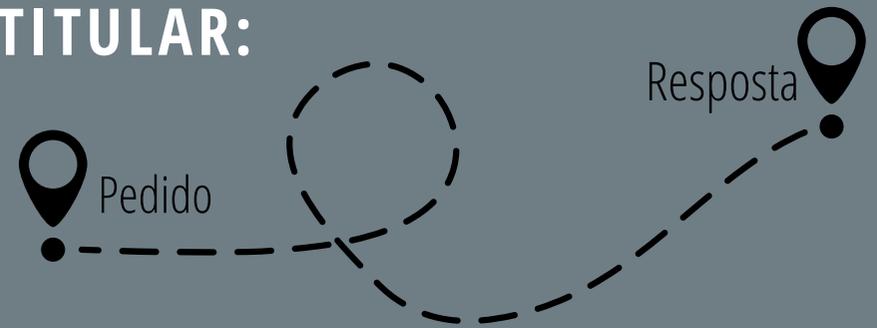
LPA: Art. 39 e seguintes: Quando for necessária a prestação de informações ou a apresentação de provas pelos interessados ou terceiros, serão expedidas intimações para esse fim, mencionando-se data, prazo, forma e condições de atendimento.

Não sendo atendida a intimação, poderá o órgão competente, se entender relevante a matéria, suprir de ofício a omissão, não se eximindo de proferir a decisão. Quando dados, atuações ou documentos solicitados ao interessado forem necessários à apreciação de pedido formulado, o não atendimento no prazo fixado pela Administração para a respectiva apresentação implicará arquivamento do processo.

Quando deva ser obrigatoriamente ouvido um órgão consultivo, o parecer deverá ser emitido no prazo máximo de quinze dias, salvo norma especial ou comprovada necessidade de maior prazo. Encerrada a instrução, o interessado terá o direito de manifestar-se no prazo máximo de dez dias, salvo se outro prazo for legalmente fixado.

LAI: Art. 11. O órgão ou entidade pública deverá autorizar ou conceder o acesso imediato à informação disponível. Não sendo possível conceder o acesso imediato, na forma disposta no caput, o órgão ou entidade que receber o pedido deverá, em prazo não superior a 20 (vinte) dias. O prazo referido podará ser prorrogado por mais 10 (dez) dias, mediante justificativa expressa, da qual será cientificado o requerente.

JORNADA DO TITULAR:



Como estruturar? Fluxo.

Quais são os principais elementos que devem constar das respostas?

- titulares internos (Fluxo 1)
- titulares externos (Fluxo 2)

Sistematização e acompanhamento das respostas (acessos a BD, modelos de respostas por categorias de assuntos, casos que deverão ir para Comitê, etc...).

Definição de norma interna (para controles diretos e indiretos da sistematização).

Treinamento e capacitação da cadeia de PMO's.

Gestão e controle do processo de atividade por meio do mapeamento de dados adequado e estabilizado. Controles interno e externo (indicadores).

JORNADA DO TITULAR:



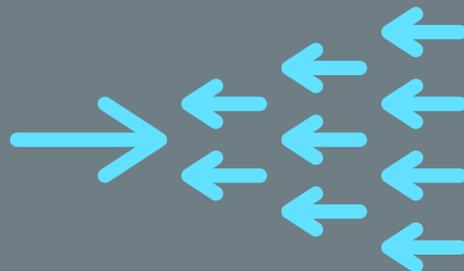
CHECK LIST (básico) de estruturação para ED:

1. Identificar origem da demanda (interna ou externa)
2. Selecionar o fluxo de jornada correspondente (1 ou 2)
3. Verificar se há resposta geral/genérica ou já cadastrada no Banco de Dados de Respostas. Se sim, utilizar. Se não, prosseguir.
4. Identificar área responsável por prestar informações sobre o pedido.
(*)
5. Enviar demanda ao PMO assinalando prazo interno de retorno.
6. Acompanhar prazo interno e cobrar unidade se preciso.
7. Receber informação unidade.
8. Analisar necessidade de complemento por outra unidade ou de remessa ao Comitê Gestor de Dados Pessoais (CGDP).
9. Se não precisar: elaborar resposta ao titular e enviar. Se precisar: remeter ao CGDP, assinalando prazo interno de retorno.
10. Acompanhar prazo interno e cobrar se preciso.
11. Receber informação do CGDP, elaborar resposta ao titular e enviar.

(*)

Se ao receber a demanda, o ED perceber que precisa consultar previamente o CGDP, ele pode optar por fazê-lo, fundamentadamente e remeter primeiramente a ele para os devidos esclarecimentos ou orientações.

É procedimento de exceção.



Deve ser usado com cautela, pois como demanda resposta do CGDP e ele para isso, precisa se reunir, pode haver maior demora na resposta ao interessado.

Desenhar em fluxograma e determinar prazos e regras do fluxo em norma interna são **procedimentos recomendados** para maior compreensão de todos acerca do funcionamento dessa atividade e dá maior clareza ao titular.

Instrumento de governança aliado a fatores de maturidade (diagnóstico em proteção de dados pessoais) e **mecanismo de controle direto e indireto por meio de indicadores específicos.**

EXEMPLO DE FLUXOS:

Cidadão (formulário/*email site*) OU (servidor/público interno)

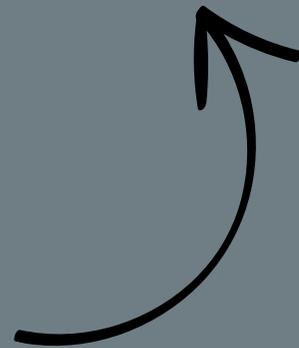
FLUXO 2

FLUXO 1

Ouvidoria (Geral ou LGPD)

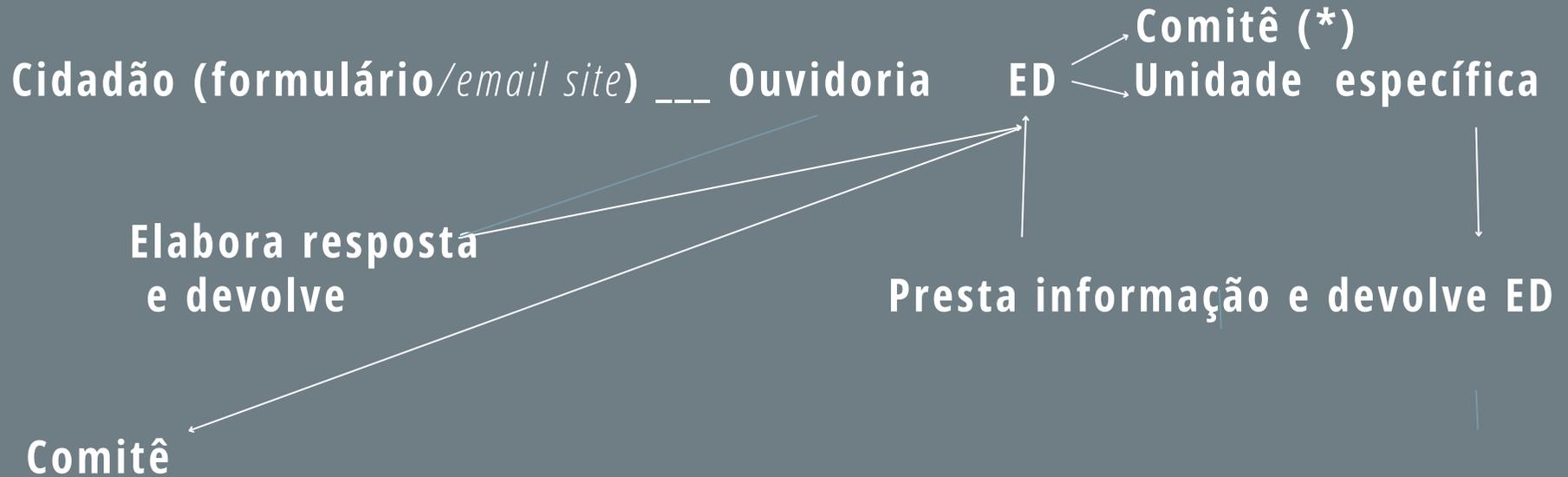
ED

Unidade específica



Comitê (*)

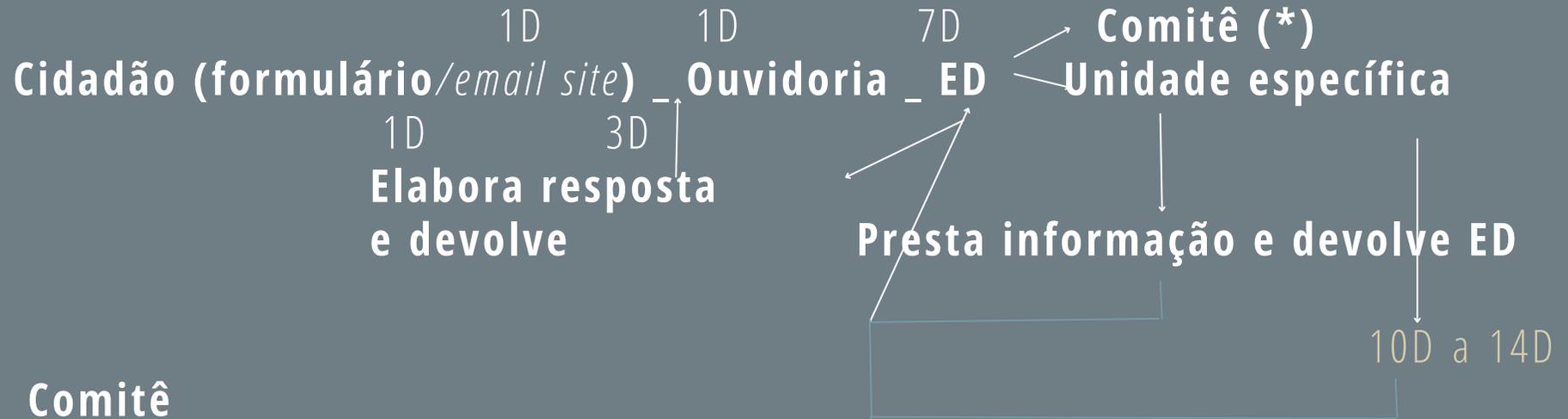
EXEMPLO DE FLUXO 2:



O que está faltando?

**O que mais poderia ter aqui
para auxiliar nosso follow up?**

EXEMPLO DE FLUXO 2:



**Prazos! Isso mesmo.
Precisamos estabelecer prazos internos
por etapas de circulação.**

ATIVIDADE PRÁTICA:

Por hoje é isso!
Até amanhã!

AVALIAÇÃO INTERATIVA DA AULA 2:

Acesse:

www.kahoot.it



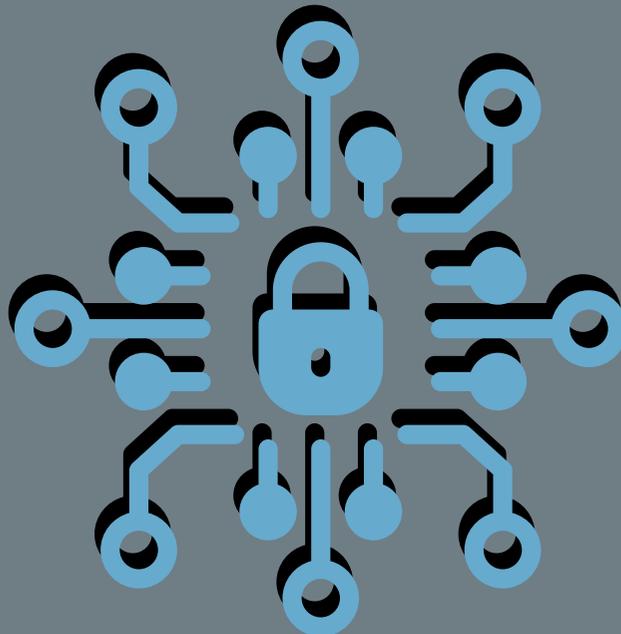
Ao entrar digite o PIN que vai aparecer na tela.



AULA 3

Gestão de programa de privacidade em conformidade com a LGPD

- Aspectos formais e materiais da implementação
- A implementação no Setor Público
- Informações e direcionamentos do Guia Orientativo ANPD
- Boas Práticas recomendáveis



GESTÃO DE PROGRAMA DE PRIVACIDADE

Guia Orientativo ANPD

X

Boas Práticas recomendáveis

- 1. Formalização e registro
- 2. Objeto e finalidade
- 3. Base legal
- 4. Duração do tratamento
- 5. Transparência e direitos dos titulares
- 6. Prevenção e segurança
- 7. Outros requisitos



1. Formalização e registro

- A partir do art. 23, a LGPD dispõe sobre o tratamento de dados pelo Poder Público. E o art. 37 prevê a formalização e o registro das operações de tratamento de dados.
- Para isso, recomenda-se a instauração de processo administrativo para registro e acompanhamento dessas atividades, juntada de documentos técnicos, planilhas, pareceres, relatórios e tudo mais que estiver a elas relacionadas. Afinal, é esse controle de registros que orientará a necessidade da elaboração de normativos internos que sejam necessários para regulamentar determinadas ações que precisarem ser tomadas no âmbito da adequação à LGPD.

Exemplos e recomendações de formalizações e registros importantes:

1) Análise de compartilhamentos.

Registrar se: há compartilhamento de dados com terceiros?

A política de compartilhamento de dados está vigente?

Os dados podem ser exportados para planilhas, arquivos editáveis, pdf...?

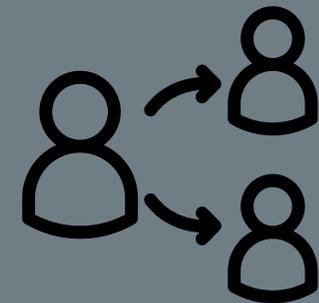
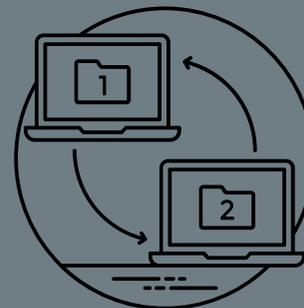
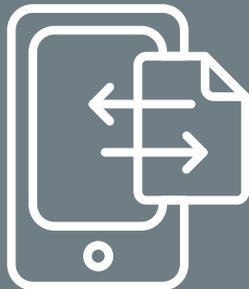
Os computadores aceitam pen drives?

A empresa tem *email* corporativo?

Quais os sistemas operacionais e administrativos que são utilizados? Estão seguros?

Há backup? Com que frequência?

E outros aspectos dessa mesma natureza e relevância deverão ser observados.



Exemplos e recomendações de formalizações e registros importantes:

2) Análise do armazenamento de dados: registros importantes.

- - Estabelecer **finalidade** comercial e qual **base legal** (hipótese de tratamento) que justifica o armazenamento.
- - Estabelecer o **período de guarda** e respectiva justificativa legal. Indicar o **local de armazenamento** (físico ou digital) e se digital, informar se o servidor é interno ou externo; se é próprio ou alugado, e nesse caso, se a empresa terceira tem sede no Brasil ou exterior.
- - Informar sobre o **acesso interno** aos dados armazenados: dizer quem tem acesso, se há controle e restrições (biometria/senha/token) e se há registro de acesso (níveis de acesso – segmentação, e gestão de acessos).



Recomendações:

- * Editar atos normativos internos (portarias, instruções normativas ou resoluções) para regulamentar, especialmente:
 - competências de cada unidade;
 - fluxo de respostas ao titular de dados;
 - prazos de respostas (interno e externo);
 - requisitos essenciais que deverão ser observados pelas unidades (relacionados às suas atividades que envolvam tratamento de dados pessoais);
 - requisitos para o compartilhamento externo;
 - metodologias de organização e gestão dos dados a serem compartilhados;
 - categorização dos dados que podem e não podem ser compartilhados e as situações em que isso se dará.
- Essas são **sugestões de hipóteses mínimas** de regulamentação pelos órgãos públicos, que deverão ser definidas com a equipe de trabalho e comitê de privacidade e proteção de dados e encarregado de dados.

2. Objeto e finalidade

Independente da opção que o órgão adotar como forma de registrar o tratamento e o compartilhamento de dados, importante ressaltar que ele deverá ser o mais DETALHADO E CLARO possível.

Ser objetivo e bem desenhado facilitará a compreensão pelas pessoas e minimizará chances de má interpretação e erros.

IMPORTANTE: atentar para as finalidades específicas que são permitidas pela LGPD para os casos de compartilhamento pelo Poder Público (art. 26), sempre voltadas à execução de políticas públicas realizadas por determinado órgão.



O que diz a norma?

Vejamos:

- § 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);
- II - (VETADO);
- III - nos casos em que os dados forem **acessíveis publicamente**, observadas as disposições desta Lei.
- IV - quando houver **previsão legal ou a transferência for respaldada** em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019).
- 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. (Incluído pela Lei nº 13.853, de 2019). Vigência
- § 2º Os contratos e convênios de que trata o § 1º deste artigo **deverão ser comunicados à autoridade nacional**.

Sobre a Decisão STF na ADI 6649/DF e ADPF 695/DF em julgamento conjunto, sobre compartilhamento de dados pelo Setor Público (Decreto 10.046/2019)

Relator Min. Gilmar Mendes

Autores: Conselho Federal da OAB e o Partido Socialista Brasileiro (respectivamente)

Objeto: Validade do DECRETO 10.046/2019 da Presidência da República que prevê:

- compartilhamento de dados **biométricos, genéticos e biográficos** + “de forma mais ampla possível”
- institui o CBC (Cadastro Base do Cidadão): interoperabilidade necessária ao intercâmbio facilitado dos dados dessa base, servirá como base de referência de informações sobre cidadãos para órgãos e entidades do Poder Executivo Federal.

Questionado o convênio, por exemplo, entre a ABIN e o DENATRAN, com informações da CNH. Após essas 2 ações, esse **convênio foi revogado pelo governo federal**, após alegação dos autores de que o decreto permitia uma espécie de “vigilância massiva do cidadão”.

As ações ainda **alegavam que** a interligação de informações, as lacunas e algumas “falhas estruturais” geravam “insegurança ao cidadão” em relação ao potencial uso indevido de seus dados pessoais e portanto, deixaria de confiar nos atuais mecanismos de proteção de dados da Administração Pública.

PGR entendeu que não haveria riscos pois prevê compartilhamento dentro dos parâmetros legais.

AGU entendeu que isso facilitaria atividades que hoje são muito burocráticas, como por exemplo a “prova de vida” junto ao INSS e bancos para recebimentos de aposentadorias e benefícios e sua inconstitucionalidade significaria um “retrocesso”.

Entidades interessadas da ADI* alegaram, em geral, que o decreto possui “salvaguardas pobres”. Como por exemplo, armazenamento de dados em elevado volume e de forma indiscriminada, de forma a ferir princípio da separação de poderes e também da legalidade, e ainda, desrespeitaria os direitos fundamentais de intimidade e vida privada.

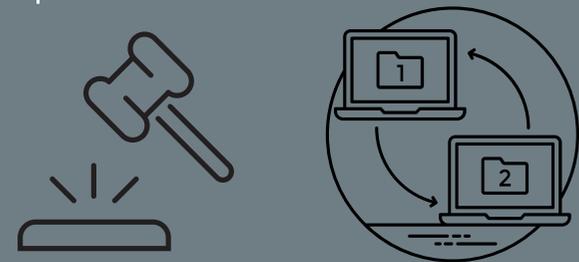


() Instituto Mais Cidadania, Associação Data Privacy Brasil de Pesquisa e Laboratório de Políticas Públicas e internet LAPIN) e da ADPF (Laboratório de Políticas Públicas e Internet – LAPIN, Associação dos Servidores da Agência Brasileira de Inteligência – ASBIN, Associação Lawgorithm de Pesquisa em Inteligência Artificial e o Instituto Beta para Democracia e Internet – IBIDEM.*

Resultado do julgamento:

Interpretação conforme a CF ao decreto para estabelecer que o compartilhamento de dados entre os órgãos públicos pressupõe propósitos legítimos e específicos e que procedimentos devem atender a LGPD. Que o Comitê Central de Governança de Dados deveria ser reestruturado de modo a contar com uma composição mais plural, estabelecendo prazo de até 60 dias para isso.

No caso de desobediência à LGPD, o Estado responderá OBJETIVAMENTE pelos danos que vier a causar às pessoas e o funcionário ou servidor que não atender à publicidade prevista no art. 23, I, da LGPD será responsabilizado por ato de improbidade administrativa. Assim, além da previsão na LGPD, essa importante decisão judicial deixa expressa a responsabilidade do Estado e de seus agentes no caso de uso indevido de dados dos cidadãos.

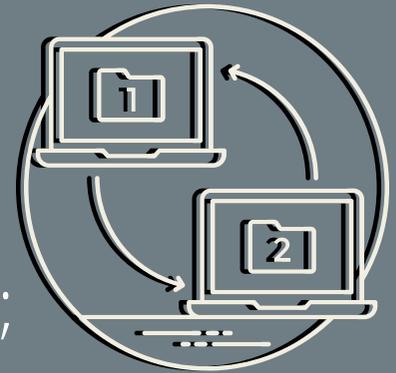


Sobre os **órgãos de inteligência**, deverá haver procedimento formal instaurado para utilização dos dados pessoais, no qual deverão ser utilizados sistemas de segurança e controle de acessos para evitar abusos ou acessos indevidos ou não autorizados.

Houve manifestação do Min. Edson Fachin, no sentido de que novo decreto fosse redigido, pois, no seu entender “o decreto adota conceitos que são incompatíveis com a LGPD”.

O compartilhamento **deve** CUMULATIVAMENTE:

1. Atender ao restrito cumprimento da finalidade pública;
2. Ter propósitos lícitos e compatíveis com a finalidade pública;
3. Ter persecução do interesse público;
4. Utilizar o mínimo de informações possíveis para atender aos itens 1 a 3;
5. Ter o objetivo de executar competências legais ou cumprir atribuições legais do serviço público;
6. Informar obrigatoriamente as hipóteses legais (bases legais) que autorizam o tratamento de cada dado pessoal;
7. Dever de publicidade clara e atualizada sobre as previsões legais, assim como a finalidade, os procedimentos e as práticas utilizadas para essas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.



3. Base Legal

(Hipóteses de tratamento)

- Deve-se sempre registrar a base legal que justifica, que ampara o compartilhamento do dado pessoal pelo Poder Público (ver art. 11 para dados pessoais comuns e art. 7º para dados pessoais sensíveis).
- O ato formal que autorizar esse compartilhamento deverá apontar expressamente qual é a base legal utilizada naquele caso.

4. Duração do Tratamento

- É parte do que chamamos de “ciclo de dados”.
- Todo tratamento de dados pessoais deve ter duração definida, e após sua conclusão os dados deverão ser descartados (observadas as regras de gestão de documentos e arquivos).
- O art. 16, da LGPD estabelece hipóteses genéricas sobre permissão para manutenção dos dados pessoais:

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.

Importante registrar que a **delimitação desse período** é relevante para a **reavaliação das condições** impostas inicialmente, se suficientes, razoáveis ou ainda persistentes.

Pois pode haver **alterações ao longo do tempo** e isso precisa estar constantemente monitorado para ajustes, especialmente sobre as **hipóteses autorizativas do compartilhamento**, que podem ser alteradas. Ou até mesmo **inovações que podem ser desenvolvidas** (medidas de segurança a partir de novas tecnologias, por exemplo).

É necessário **delimitar o objeto do compartilhamento, a finalidade específica e a sua amplitude.**

5. Transparência e direitos dos titulares

Deve-se lembrar que o Princípio da Transparência deve estar presente nos atos que regem e autorizam o compartilhamento de dados pessoais pelo Poder Público (art. 6º, VI e art. 23, I da LGPD).

Dicas:

- Registrar o compartilhamento existente na página do órgão na parte que fala sobre LGPD;
- Delimitar a divulgação das informações exigidas pela LGPD;
- Estabelecer responsabilidades e atribuir competências;
- Estabelecer fluxos das atividades relacionadas às solicitações apresentadas pelos titulares de dados (internos e externos).
- Respostas ao titulares dentro do prazo

(+ detalhes: ADI 6.649/DF e ADPF 695/DF).

6. Prevenção e Segurança



Sobre os compartilhamentos que serão feitos pelo órgão.
Registrar as medidas de segurança, medidas administrativa e medidas técnicas que serão tomadas para proteger os dados compartilhados.

Exemplos: segmentação de acesso, autorização de acesso limitada, e o que acontecerá em caso de perda, alteração, comunicação indevida, compartilhamento acidental ou ilícito, destruição indevida, etc.

IMPORTANTE:

- Medidas devem guardar proporcionalidade com fato ocorrido, e aos riscos as liberdades civis e direitos dos titulares envolvidos em cada caso;
- Devem estar previstas nos atos que regulamentam e autorizam o compartilhamento de dados de forma antecipada, preventiva e informativa; e
- Deve haver o gerenciamento proativo de riscos.



7. Outros requisitos

- A LGPD dispõe de outras **situações peculiares** em que será necessário observar outros requisitos que são provenientes de outras normas específicas já em vigor quando da sua publicação.

Exemplo é o caso de eventual **novo compartilhamento ou transferência posterior de dados a serem efetuados pelo recebedor dos dados no âmbito do próprio setor público ou para entes do setor privado.**

Segundo a ANPD:

“Entre outras possibilidades, o instrumento que rege o uso compartilhado dos dados pode vedar a realização de novo compartilhamento ou, ainda, autorizá-lo sob determinadas condições, observadas as normas aplicáveis.

Por exemplo, no caso de dados pessoais disponibilizados para a realização de estudos em saúde pública, a LGPD veda que o órgão de pesquisa responsável transfira os dados a terceiro (art. 13, § 2º)”.



- Importante registrar também quando o compartilhamento irá gerar algum **ônus financeiro**, e quem irá suportá-lo, como se dará a remuneração, ou não havendo transferências de recursos financeiros, também registrar essa informação.
- Questão delicada e que precisa ser considerada é quando houver **compartilhamento de dados pessoais entre ente público e empresas privadas**. A LGPD dispõe expressamente essa possibilidade sob as seguintes, e restritas, hipóteses (art. 26):
 - (i) nos casos de execução descentralizada da atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado;
 - (ii) nos casos de dados acessíveis publicamente;
 - (iii) quando houver previsão legal ou a transferência for respaldada em contratos e instrumentos congêneres; ou
 - (iv) na hipótese de a transferência 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.

E seguem os dispositivos seguintes da LGPD que regulamentam assuntos restantes sobre esse tema:

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. [\(Incluído pela Lei nº 13.853, de 2019\).](#) [Vigência](#)

Art. 28. (VETADO).

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. [\(Redação dada pela Lei nº 13.853, de 2019\).](#) [Vigência](#)

Art. 30. A autoridade nacional **poderá** estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

QUADRO RESUMO:

| <u>Requisito</u> | <u>Recomendação</u> |
|---|--|
| Formalização e registro | <ul style="list-style-type: none">• Instauração de processo administrativo;• Análise técnica e jurídica;• Decisão administrativa ou celebração de contrato, convênio ou instrumento congêneres;• Edição de ato normativo interno. |
| Objeto e finalidade | <ul style="list-style-type: none">• Descrição dos dados pessoais de forma objetiva e detalhada;• Indicação de finalidade específica;• Avaliação da compatibilidade entre a finalidade original e a finalidade do compartilhamento. |
| Base legal | <ul style="list-style-type: none">• Indicação da base legal utilizada. |
| Duração do tratamento | <ul style="list-style-type: none">• Definição do período (duração) do uso compartilhado dos dados, de forma fundamentada, e esclarecimento sobre a possibilidade de conservação ou a necessidade de eliminação após o término do tratamento. |
| Transparência e direitos dos titulares | <ul style="list-style-type: none">• Divulgação das informações pertinentes na página eletrônica dos órgãos e das entidades responsáveis;• Divulgação de maneira que as informações sobre dados pessoais tratados pela entidade sejam de fácil compreensão;• Definição de responsabilidades e de procedimentos relativos ao atendimento de solicitações de titulares. |
| Prevenção e segurança | <ul style="list-style-type: none">• Descrição das medidas técnicas e administrativas adotadas para proteger os dados pessoais de incidentes de segurança. |
| Outros requisitos (avaliação conforme o caso concreto) | <ul style="list-style-type: none">• Autorização ou vedação para novo compartilhamento ou transferência posterior dos dados pessoais;• Ônus financeiro;• Requisitos específicos para compartilhamento de dados pessoais com entidades privadas (art. 26, § 1º e art. 27, LGPD);• Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário;• Identificar as funções e responsabilidades dos agentes de tratamento. |

O papel da ANPD sobre Compartilhamento de Dados no Setor Público

| <u>Parâmetro</u> | <u>Recomendação</u> |
|---|---|
| A coleta do dado pessoal é necessária e adequada para a finalidade do tratamento? | <ul style="list-style-type: none">• Verificar a possibilidade de dispensa da coleta ou de eliminação dos dados pessoais, tendo em vista a sua efetiva necessidade para o alcance das finalidades do tratamento;• Verificar se há formas de atingir a finalidade almejada sem o tratamento de dados pessoais e de maneira menos gravosa para o titular de dados. |
| A divulgação envolve dados pessoais sensíveis? | <ul style="list-style-type: none">• Em caso afirmativo, o tratamento deve ser efetuado com maior cautela, observando-se normas específicas, como os dispositivos da LGPD relativos a estudos em saúde pública. |
| Quais medidas de mitigação de risco para o titular de dados podem ser adotadas? | <ul style="list-style-type: none">• Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário;• Medidas de prevenção e segurança, a exemplo de anonimização ou pseudonimização dos dados pessoais sempre que isso não comprometa o exercício do controle social;• Limitação da divulgação àqueles dados necessários para alcançar a finalidade pretendida, observados o contexto, a finalidade e as expectativas legítimas dos titulares;• Transparência do tratamento; e• Garantia de direitos dos titulares. |

Mais alguns pontos a serem considerados:

Para além do compartilhamento, é importante atentar para:



**SEGURANÇA E
BOAS PRÁTICAS!!**



Vejamos a seguir algumas recomendadas pela LGPD:

Segurança e Boas Práticas

1. Atentar ao cumprimento dos princípios norteadores previstos na LGPD.
1. Enquadrar de forma correta o tratamento de dados pessoais nas bases legais previstas pela LGPD.
1. Estabelecer um plano de ação para resposta aos titulares quando questionarem sobre o tratamento de seus dados pessoais pelo ÓRGÃO PÚBLICO.
1. Definir medidas de segurança (técnicas e administrativas) para proteção dos dados pessoais (*softwares*, treinamentos, cartilhas, sistemas...).
1. Definir Plano para Incidentes de Segurança.
1. Estabelecer, a partir da análise de riscos, em quais processos ou tratamentos de dados será necessário realizar RIPD.
1. Elaborar cartilhas de conscientização com periodicidade.
1. Elaborar *workshops* temáticos com as áreas que mais tratam dados pessoais, portanto, mais vulneráveis, para apoio.

9. Plano de aprimoramento e capacitação profissional anual.
10. Atualização e proteção de banco de dados: periodicidade.
11. Garantir o registro das atividades durante o processo de adequação bem como o tratamento de dados conforme diretrizes controlador e Comitê.
12. Estabelecer o gerenciamento proativo de riscos como garantia da segurança de dados.
13. Contribuir com práticas, projetos e iniciativas internas que garantam a alteração gradual de cultura da proteção e privacidade de dados pessoais no ambiente de trabalho (*mindset*).
14. Gerar constante conscientização e importância do assunto dentro do órgão público, colocando o servidor também como destinatário da norma.
15. Promover a conscientização de colaboradores, empresas prestadoras de serviço, fornecedores de produtos e serviços como destinatários da norma e a necessidade de também se adequarem.

Onde a LGPD menciona e pede pelas boas práticas (notadamente aos órgãos públicos)?

Art. 13: quando menciona o uso de dados de saúde em ambiente controlado e que possua boas práticas de segurança.

Art. 23, I: com relação ao tratamento de dados pelo setor público, realizado para o atendimento de sua finalidade pública, na busca do interesse público e com o objetivo de executar as competências legais ou cumprir com as atribuições estatutárias ou legais do serviço público, desde 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.

Art. 32: que fala que a ANPD poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Art. 41, III: quando fala sobre a obrigação do controlador em indicar o encarregado de dados e **orientar os funcionários e os contratados da entidade a respeito das práticas** a serem tomadas em relação à proteção de dados pessoais.

Todo o **Capítulo VII** (art. 46 a 49) que está voltado especialmente para a abordagem sobre Segurança e Boas Práticas (cuja leitura complementar se faz recomendável).

- Inclusive o art. 46, §1º menciona que a **ANPD poderá dispor sobre padrões técnicos mínimos** para tornar aplicável a adoção de medidas de segurança (técnicas e administrativas), levando em consideração a **natureza** das informações tratadas, as **características específicas** do tratamento e o **estado atual da tecnologia**, especialmente no caso de dados pessoais sensíveis.

Art. 49: informa que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos **requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais** previstos nesta Lei e às demais normas regulamentares

Art. 50 Os **controladores e operadores**, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão **formular regras de boas práticas e de governança** que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as **normas de segurança**, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as **ações educativas**, os mecanismos internos de **supervisão e de mitigação de riscos** e outros aspectos relacionados ao tratamento de dados pessoais.

O **art. 50, §1º** dispõe que, ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, **a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios** decorrentes de tratamento de dados do titular.

Ainda com relação ao **Programa de Governança em Privacidade**, o mesmo artigo fala da importância de ser demonstrado o **comprometimento do controlador** em adotar processos e políticas internas que **assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais**.

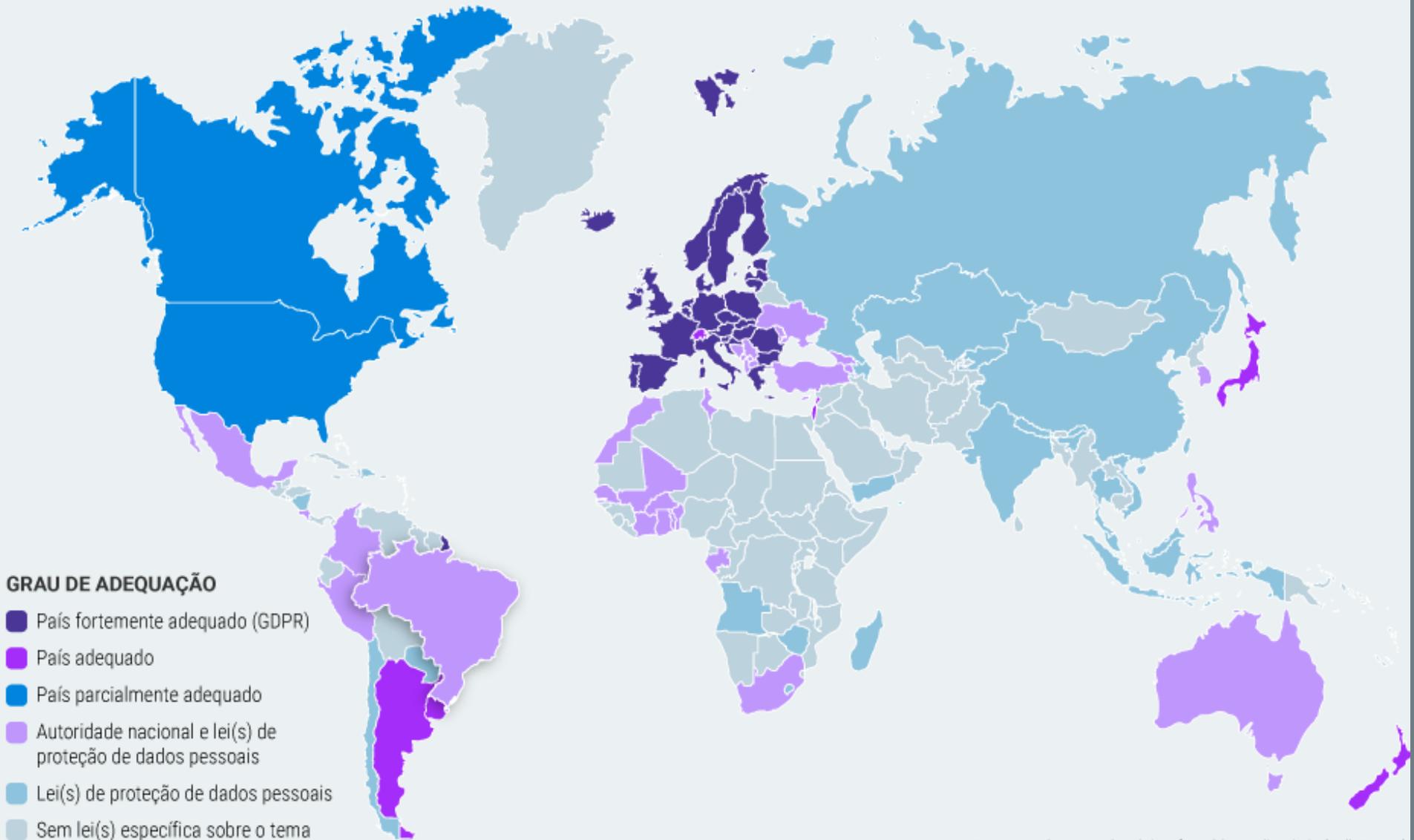
E ainda dentro desse mesmo art. 50, a LGPD especifica que as regras de boas práticas e de governança **deverão ser publicadas e atualizadas periodicamente** e poderão ser reconhecidas e divulgadas pela autoridade nacional.

No art. 52, que fala sobre as penalidades, no inciso IX, a LGPD informa que a **adoção de política de boas práticas e governança será observada para aplicação gradativa e proporcional da sanção**. Ou seja, poderá ainda, auxiliar na diminuição da gravidade da penalidade considerada inicialmente como **demonstração de boa fé e medida de segurança voltada à mitigação de riscos**.

E por fim, estabelece como uma das **competências da ANPD**, elencadas no art. 55, a **promoção e elaboração de estudos sobre as práticas nacionais e internacionais** de proteção de dados pessoais e privacidade.

Mapa da Proteção de Dados ao redor do Mundo: grau de adequação (SERPRO)

PROTEÇÃO DE DADOS PESSOAIS AO REDOR DO MUNDO



Fonte: Comissão Nacional de Informática e Liberdade (Cnil/França)

CASOS PRÁTICOS COMENTADOS

sobre compartilhamento de dados pelo Poder Público



1) Perfil Socioeconômico de SERVIDORES PÚBLICOS

Formulários que contenham dados sensíveis (racial, religião, filiação a sindicato, etc...): atentar para necessidade, segmentação de acessos. Não divulgar nome (pseudonimizar).

Evitar coletar dados socioeconômicos (necessidade e finalidade); eliminar os atuais existentes e desnecessários.

2) CURRÍCULO de candidato a órgão consultivo (representação social)

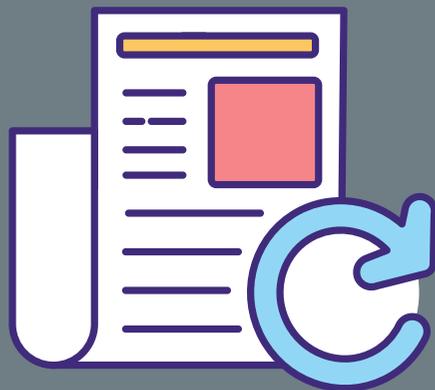
Atentar para a disponibilização dos CV na internet. Adotar prática de eliminação após escolha, assim como limitar a divulgação dos CVs mesmo durante o processo seletivo, para evitar exposição pública. Desnecessária manutenção do armazenamento posterior.

3) RECEPÇÃO dos órgãos públicos

A LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) exige transparência de vários atos administrativos, inclusive o da agenda da autoridade máxima do órgão. É obrigatória a divulgação dos compromissos oficiais agendados. Portanto, ao chegar a pessoa que possui agendamento deverá ser informada que dados pessoais seus poderão ser compartilhados para atender essa obrigação da agenda pública. Informar finalidades coleta e compartilhamento, que podem inclusive, constar do Aviso de Privacidade.

4) Dados para CONTRATOS ADMINISTRATIVOS

Seja para adquirir merenda, material de escritório, etc... É preciso celebrar contratos. Contudo é recomendado limitar o tratamento ao mínimo necessário para a realização de suas finalidades, dispensando, por exemplo, tratar dados de estado civil e endereço.



5) Política pública de VACINAÇÃO e campanha controle do TABAGISMO

A implementação e monitoramento de políticas públicas relacionadas à saúde da população vai tratar dados sensíveis. Assim, o tratamento dos dados pessoais é realizado com base no art. 11, II, b, da LGPD e seu compartilhamento com um órgão de pesquisa atende a finalidade específica de realização de estudos em saúde pública ou de execução de política pública (ver caso a caso). Neste caso, o tratamento posterior dos dados é compatível com a finalidade original da coleta, em conformidade com o princípio da finalidade.

Por se tratar de dados sensíveis, relativos à saúde, o órgão deve ter cautela ao compartilhá-los ou divulgá-los, sempre observando o art. 13 e o Capítulo IV da LGPD. Nesse sentido, é preferível que o compartilhamento dessas informações inclua, sempre que possível, a pseudonimização ou a anonimização dos dados.

6) Processo legislativo (ATAS REUNIÕES, dados dos parlamentares, etc...)

Comum durante o processo legislativo é o tratamento de dados pessoais de parlamentares, servidores, cidadãos, etc... envolvidos nos atos relacionados às normas de organização da Assembleia Legislativa.

Portanto, o tratamento dos dados pessoais é legítimo, na medida em que diretamente vinculado ao cumprimento de obrigações e à execução de competências típicas do órgão legislativo, que decorrem de normas de organização previstas na Constituição Estadual, em conformidade com a base legal prevista no art. 7º, II, e com o disposto no art. 23, da LGPD.

7) Criação e uso de CANAL TV próprio por Assembleia Legislativa

Assembleia Legislativa pretende lançar canal de TV próprio. Para tanto, entre outros requisitos, o órgão regulador determinou a apresentação de dados pessoais de parlamentares e servidores responsáveis pela direção do canal, sob pena de ter o pedido de outorga indeferido.

O tratamento dos dados pessoais pela Assembleia Legislativa é legítimo, uma vez que, nos termos do art. 7º, II, da LGPD, vincula-se diretamente ao cumprimento de normas de conduta, no caso, obrigações regulatórias definidas pelo órgão regulador competente, em conformidade com a legislação aplicável.

8) Agências reguladoras (hipóteses legais iguais e finalidades distintas)

Uma agência reguladora trata dados pessoais de seus servidores públicos com a finalidade específica de realizar o pagamento de salários e benefícios previdenciários, como pensões e aposentadorias. Essas obrigações estão expressamente previstas na legislação que dispõe sobre o regime jurídico dos servidores.

A mesma agência reguladora tem a atribuição legal de fiscalizar prestadoras de um determinado serviço público. Para cumprir essa competência geral de fiscalização, conforme estipulado na lei que dispõe sobre a sua estrutura e funcionamento, a agência reguladora trata dados pessoais, como, por exemplo, aqueles provenientes de reclamações de usuários do serviço.

Embora atendam a finalidades distintas, em ambos os casos o tratamento dos dados pessoais pela agência reguladora se fundamenta na hipótese de cumprimento de obrigação legal, nos termos do art. 7º, II, da LGPD.

Exemplo para fixação:

Uma autarquia federal trata dados pessoais de seus servidores, como nome, telefone e e-mail para fins de gestão de pessoas.

Uma entidade financeira privada solicita ao setor de recursos humanos dessa autarquia os dados de contato dos servidores para oferecer empréstimo consignado.

O pedido foi negado pela autoridade competente, com base em análise técnica e jurídica, que concluiu pela impossibilidade de realização do compartilhamento dos dados, tendo em vista:

- (i) a incompatibilidade entre a finalidade original da coleta e a finalidade proposta para o compartilhamento;
- (ii) a inexistência de base legal válida a amparar o uso compartilhado dos dados, em particular a inexistência de consentimentos dos titulares, de obrigação legal ou de qualquer vínculo com a execução de políticas públicas na hipótese; e
- (iii) a vedação prevista no art. 26, § 1º, da LGPD e o não enquadramento do caso em uma das exceções previstas nos incisos do mesmo dispositivo.

Por hoje é isso!
Até amanhã!

**THANKS
FOR YOUR
PATIENCE**

AVALIAÇÃO INTERATIVA DA AULA 3:

Acesse:

www.kahoot.it



Ao entrar digite o PIN que vai aparecer na tela.

AULA 4

AULA 4 – A prática da LGPD no Setor Público

- Como iniciar um projeto de adequação
- O passo a passo para adequação no Setor Público
- Fases principais



LGPD

MÉTODO
10
PASSOS





1. Plano de Ação. Registro no SEI.

2. Indicação encarregado de dados e formação de Comitê de Proteção de dados.

3. A Conscientização. O que é, qual finalidade e importância. Método da conscientização "P a P".



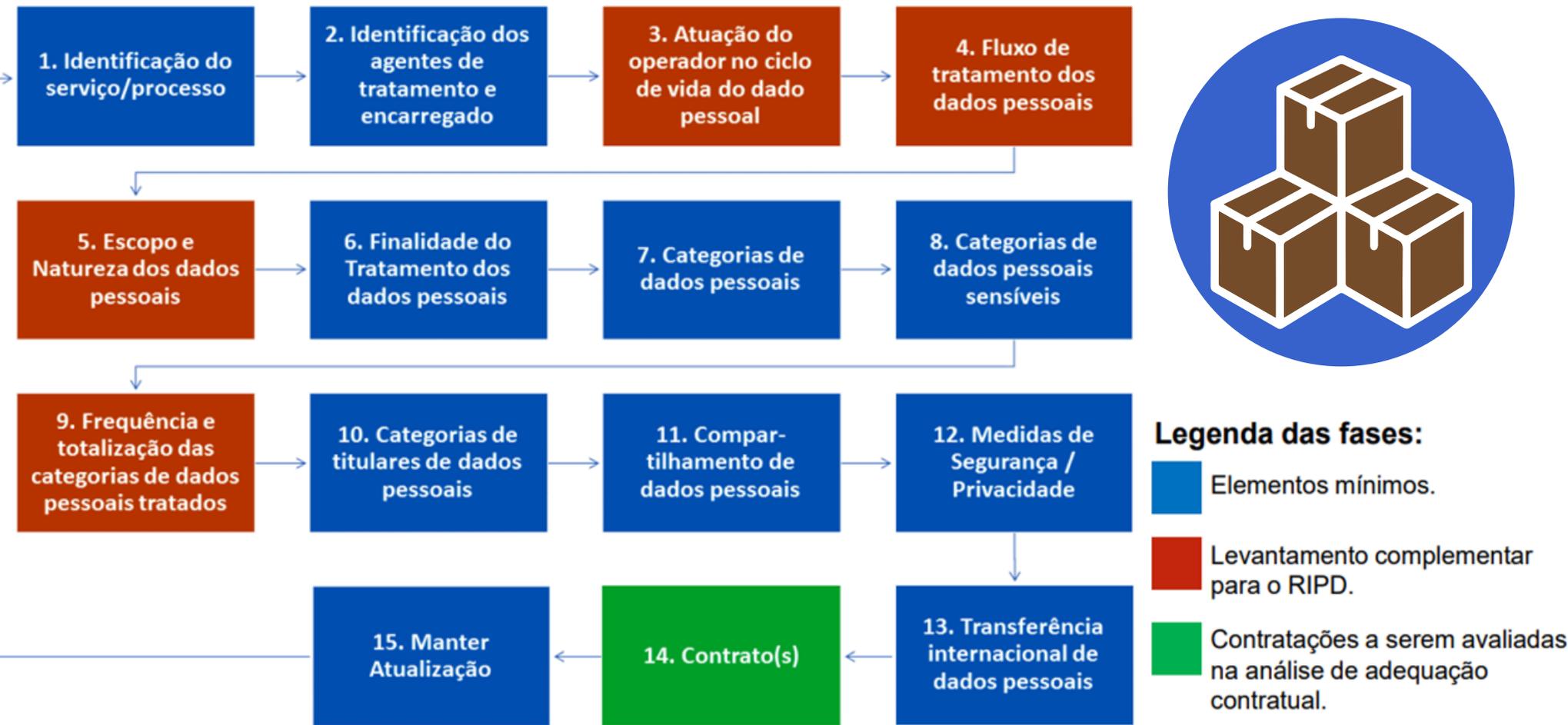
4. Entrevistas e informativos para iniciar o mapeamento de dados.

Fase de coleta e planilhamento/inventário dos dados: Importância acerca da origem do dado. Quais dados serão coletados? De que forma? Para quê? Houve excesso na coleta? Por quanto serão mantidos? Em que local serão armazenados? Serão compartilhados? Haverá transferência internacional? Como serão eliminados?

5. Fase de registrar os processos completos dos ciclos de dados: coleta – processamento – análise – armazenamento – reutilização - descarte. Inventário de dados.

O Inventário de Dados Pessoais no Setor Público

Segundo o art. 37, da LGPD, o inventário de dados pessoais representa entrada para o processo de elaboração do RIPD. A Secretaria Digital, assim distribuiu, com base nisso, as fases de elaboração do inventário de dados pessoais:



6. Análise de gaps e riscos. Relatório de Impacto à Proteção de Dados (RIPD).

MODELO DE MATRIZ DE RISCO:

| | | | CONSEQUÊNCIAS | | | | |
|------------------------|-------------|------------------|----------------|--|----------|-------|--------------|
| | | | Insignificante | Menor | Moderada | Maior | Catastrófica |
| | | | 1 | 2 | 4 | 8 | 16 |
| PROBABILIDADE | Raro | 1 | 1 | 2 | 4 | 8 | 16 |
| | Improvável | 2 | 2 | 4 | 8 | 16 | 32 |
| | Possível | 3 | 3 | 6 | 12 | 24 | 48 |
| | Provável | 4 | 4 | 8 | 16 | 32 | 64 |
| | Quase certo | 5 | 5 | 10 | 20 | 40 | 80 |
| Nível do Risco (P x C) | | Zonas de Decisão | | Tratamento | | | |
| NR ≤ 4 | | Tolerável | | Manter controles existentes | | | |
| 4 < NR ≤ 8 | | Significativo | | Avaliar necessidade de novos controles | | | |
| 8 < NR ≤ 16 | | Sério | | Implementar novos controles | | | |
| NR >16 | | Intolerável | | Paralisar a atividade | | | |

A estrutura do RIPD no Setor Público

A estrutura do RIPD, segundo o *template* da Secretaria Digital deve conter capa, controle de versões, objeto e 8 seções assim denominadas:



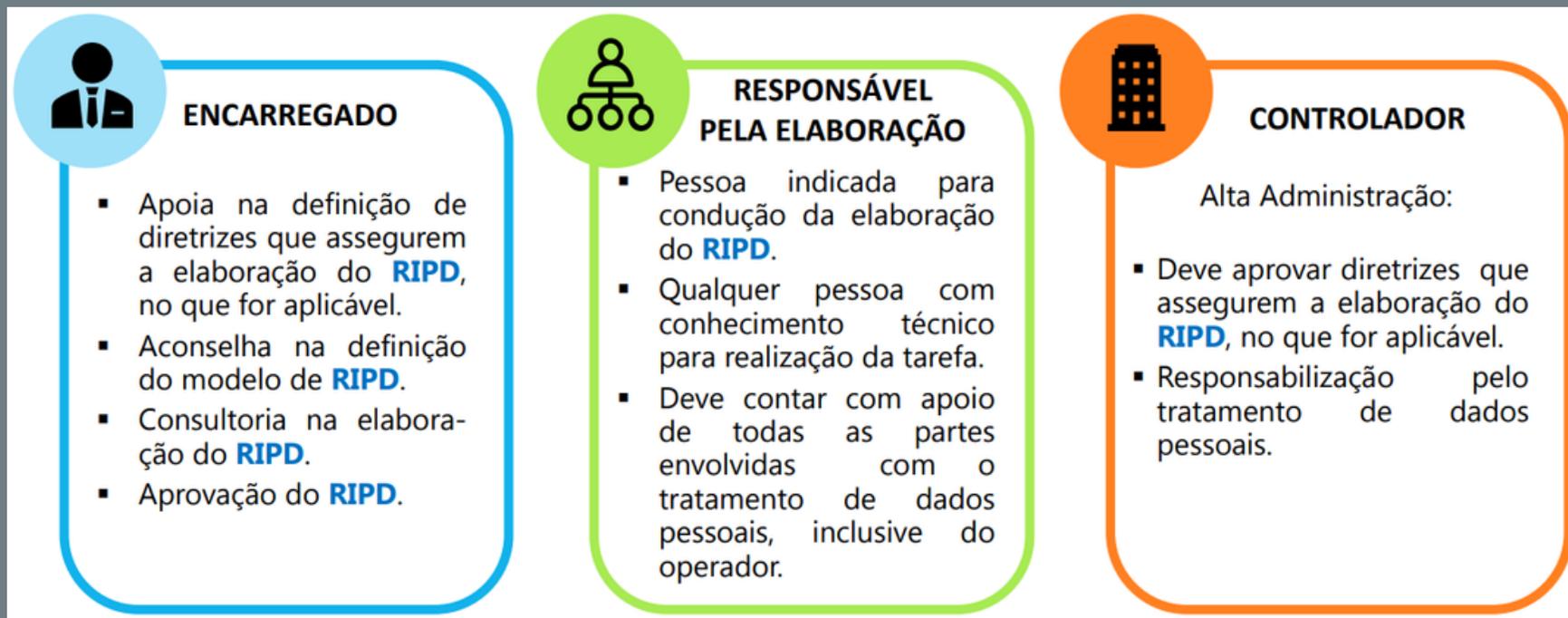
Para saber mais detalhes sobre como elaborar o RIPD no Setor Público, segundo as orientações da Sec. Digital, verificar Seção 2.5, do Guia de Boas Práticas LGPD no *link* abaixo (p.20)

FONTE: Secretaria Digital (gov.br): https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-dados/apresentacoes/apresentacao_ripd.pdf

O Guia de Preenchimento do RIPD da Secretaria de Governo Digital do Ministério da Economia (gov.br)

A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público (art. 32, LGPD).

Com base nisso, a Secretaria Digital resumiu as orientações da LGPD sobre o assunto considerando os seguintes pontos atores, quanto às suas atribuições quanto ao RIPD:



FONTE : Secretaria Digital (gov.br): https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/apresentacoes/apresentacao_ripd.pdf



7. Planejamento para implementação dos ajustes necessários à proteção de dados.

8. Fase da revisão de contratos e documentação, revisão de sistemas e processos de gestão, bem como dos processos de trabalho mapeados: governança de dados. Realização de relatórios, relatório final, entregáveis e fluxogramas. Auxílio ao diagnóstico, verificação de procedimentos, prestação de contas, entrega da documentação.

9. Treinamento Final. Apresentação de fluxogramas informativos com resumo dos ciclos de dados por processo mapeado. Boas práticas (cartilhas, códigos, informativos, etc...)

10. Monitoramento. PDCA.

Objetivos do Programa de conformidade à LGPD

- Precisa estar adequado ao modelo de negócio da organização (+ : valores, missão, visão, objetivos e Ética).

Desenho de soluções alinhadas.

No Setor Público: atos normativos, política de governança, programa de integridade. Orientações gerais para o Poder e esfera federativa.

- Precisa estar alinhado e atender às necessidades e em compatibilidade com as demais normas já vigentes.

Conviver com a aplicabilidade das demais legislações.

No Setor Público: alinhamento com as políticas públicas e atividade-fim realizadas pelo órgão. Foco no cidadão.





- Gestão de riscos deve identificar vulnerabilidades relacionadas à proteção de dados, que deverão ser consideradas no programa e terem prioridade sobre as demais.

No Setor Público: utilizar tabela disponibilizada pela Secretaria Digital e ferramenta eletrônica com questionário auto-aplicável já padronizado com os riscos mais comuns sobre privacidade proteção de dados, que pode ser solicitada para o *email*: cgsin@economia.gov.br.

Na solicitação de acesso é preciso se identificar com nome, instituição a que pertence e o *email* institucional para que o *token* de acesso à ferramenta possa ser encaminhado.

Entregáveis devem estar alinhados e deve ser feito um cronograma de trabalho dentro de um plano de ação coordenado.

Esse cronograma deve conter, basicamente: a atividade que será realizada, quanto tempo (estimado), desdobramentos (qual setor, qual processo de trabalho, medida X quantidade, etc...), locais (onde), responsabilidades (quem), relatório parcial (*reports*), cronograma em datas para assinalar avanço da adequação como se fosse uma “obra de construção”, estimativa da duração das atividades e realizar acompanhamento (data início/duração em dias/data término).

Assim ficará visivelmente possível para qualquer pessoa acompanhar a evolução e entender as etapas de trabalho.



Por hoje é isso!
Até 3f da semana que vem!

AVALIAÇÃO INTERATIVA DA AULA 4:

Acesse:

www.kahoot.it



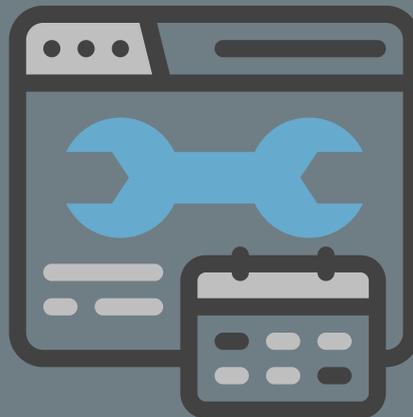
Ao entrar digite o PIN que vai aparecer na tela.



AULA 5

LGPD na prática do STJ e os principais entregáveis (relatórios e documentos)

- Os principais entregáveis da LGPD
- Sobre elaboração de documentos: regras importantes
- A prática da LGPD dentro do Tribunal, como está?
- Tira-dúvidas geral
- Avaliação final e premiação



Principais entregáveis de um Projeto de Adequação à LGPD

INTRODUÇÃO:

- - Linguagem clara (sem juridiquês/tecniquês)
- - Qual a importância?
- - *Legal Design ou Visual Law* (pode usar?)
- - Amparo legal e normas existentes: para Setor Público (“considerandos”).

Obs: considerar normativos internos também.

- - Publicação/publicização: obrigatória para Setor Público.



ESTRUTURA:

- - Objetivos (finalidade/necessidade)
- - Destinatários
- - Responsabilidades



Pode unificar mais de um documento na mesma estrutura?

Regra da unificação:

Exemplos:

1) Política de Privacidade X Política de Cookies:

| | PP | PC |
|------------------------|--|--|
| Objetivos = | Contar ao titular sobre ciclo tratamento de dados. | Contar ao titular sobre coleta de cookies. |
| Destinatários = | Titular de dados | Titular de dados |



2) Código de Conduta X Termos de Uso

| | CC | TU |
|------------------------|--|--|
| Objetivos ≠ | Manual sobre cultura de dados dentro da organização. | Explica regras de utilização daquele determinado ambiente. |
| Destinatários ≠ | Usuários Internos: servidores, colaboradores... | Usuários externos |



Elementos a observar para Elaboração de Documentos



- Quem é o titular? CHD ou adolescente? RESPONSÁVEL
- Com quem / Para quem (para definir a linguagem e o foco da comunicação): titular
- Finalidade e base legal: 7º, e 11.
- Porquê: motivo dele existir: tratamento de dados pessoais para atividade "X"
- Objetivo do documento: transparência e atender LGPD
- Se vai compartilhar com alguém? Transferência internacional (art. 33, VIII): tem que ser específico. Regras do compartilhamento S. Público.
- Vai armazenar dados? Qual finalidade e HL? Quanto tempo?
- Informar sobre os direitos de titular envolvidos: revogação, acesso (cópia) e meios de como fazer isso (acesso gratuito e mediante manifestação - link, formulário).
- Informações do encarregado de dados para contato.
- Controlador é órgão público ou empresa privada?
- Como será feito descarte? Após quanto tempo de findo o armazenamento?



Lista entregáveis (mais comuns)

Política de Privacidade (aviso de privacidade/declaração de privacidade)

Termos de uso

Política de Cookies (Cardápio e orientações ANPD – Guia)

Política de armazenamento e descarte de dados

Termo de consentimento

Termo de confidencialidade

Relatório final e relatórios parciais

Avisos e informativos

Contratos e aditivos contratuais trabalhistas (Controlador-controlador. Controlador-operador. Operador-operador).

Termo de autorização para guarda e armazenamento de currículos em banco de dados.

Código de boas práticas

Código de Conduta

Política de segurança da informação



Política de tela e mesa limpa

Política de BYOD (*Bring Your Own Devices*)

Jornada do titular

Atestado de comparecimento em eventos de capacitação e treinamento

Cronograma de atividades (para realização da adequação)

Relatório de Impacto à Proteção de Dados (RIPD) (modelo específico ANPD)

Contrato de fornecimento de serviços (capítulo com cláusulas sobre LGPD) para novos contratos e aditivos dos atuais em vigência. EDITAIS DE LICITAÇÃO*.

Política de segmentação de acessos

Política de ação em caso de incidentes de segurança



COMO SABER QUAIS DOCUMENTOS ALÉM DESSES EU VOU PRECISAR?

Analise a rotina da organização, avalie suas necessidades e identifique suas vulnerabilidades. Pense que você deve considerar mecanismos para proteger ao máximo os dados pessoas, em todos os níveis de tratamento. Criatividade, atenção, muita observação e estudo.

MERECEM ESPECIAL ATENÇÃO E NÃO PODEM SER ESQUECIDOS:

Política de Cookies pela ANPD (principais aspectos). E outros que ela atualizar.

Normas ABNT da família ISO (27.000, 31.000):

(governança de dados, segurança da informação, análise de riscos...)

Contratos e editais de licitação: pontos de atenção.

Programa contínuo de aperfeiçoamento: treinamentos e ciclo de monitoramento: periodicidade.

Jurisprudência de aplicação LGPD e GDPR.

A prática da LGPD no Tribunal, como está?

A adequação do STJ à LGPD

- Normativos
- Política de Privacidade
- Política de Cookies
- Contratos

Obrigada!



@kassiazinato



YouTube



kassiazinato



HOJE TEM PREMIAÇÃO!!!!

AVALIAÇÃO INTERATIVA DA AULA 5:



Acesse:

www.kahoot.it

Ao entrar digite o PIN que vai aparecer na tela.





EXTRA

BONUS



MATERIAL EXTRA:



TESTE DO LEGÍTIMO INTERESSE (LIA) (*Legitimate Interests Assessment*)

Fase 1 – Avaliação da PONDERAÇÃO: (art. 6, I + 10)

LEGITIMIDADE DO INTERESSE DO CONTROLADOR:

(situação concreta + finalidade legítima)

- a) A finalidade para uso dessa base legal é legítima e lícita?
- b) O interesse da organização é adequado e proporcional?
- c) A situação concreta está definida e articulada?

Fase 2 – Avaliação da NECESSIDADE: (art. 10, §1º)

- a. Existe outra base legal na LGPD que poderia ser mais adequada?
- b. Estão sendo utilizados os dados estritamente necessários a esse tratamento para atingir a finalidade pretendida?



TESTE DO LEGÍTIMO INTERESSE (LIA)

(*Legitimate Interests Assessment*)

CONTINUAÇÃO (...)

- Fase 3 – Regra do BALANCEAMENTO** (medir compatibilidade de interesses da organização X expectativas do titular de dados): (art. 10, I e II)
- Há legítima expectativa sobre o uso dos dados pelo seu titular?
(Teoria do Susto)
 - Os direitos e liberdades fundamentais estão sendo respeitados?

- Fase 4 – SALVAGUARDAS:** (art. 10, §§2º e 3º)
- Há necessidade de elaborar RIPD (Relatório de Impacto à Proteção de Dados) /DPIA (*Data Protection Impact Assessment*)?
 - Foram estabelecidas medidas técnicas e administrativas para mitigar riscos?
 - Há transparência e mecanismos de oposição (*opt out*)?

TESTE DOS 4 PASSOS

TESTE DO LEGÍTIMO INTERESSE

PODE USAR

1 Finalidades Legítimas

OK

2 Necessidade

OK

3 Balanceamento

OK

4 Salvaguardas

OK

Deve atender cumulativamente a todos eles.

<https://www.observatorioprivacidade.com.br/jogo-da-lia/>

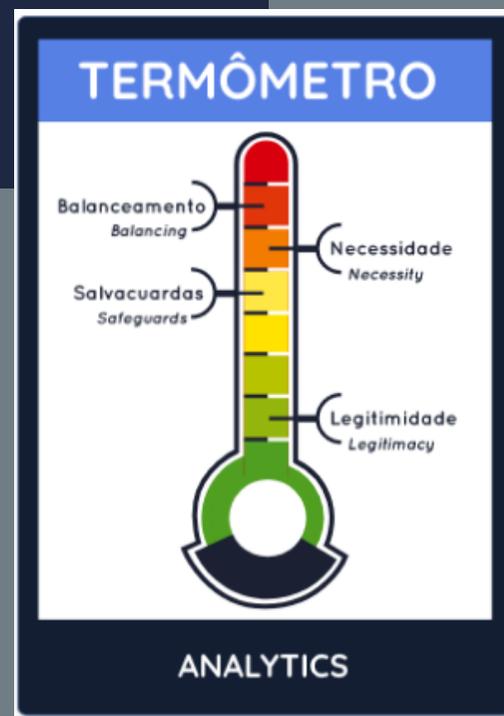


Jogo do Legítimo Interesse

A aplicação das bases legais da LGPD na prática pode ser um desafio, especialmente enquanto as práticas e interpretações sobre o tema ainda estão sendo construídas. Nessa página, você poderá navegar por casos práticos que discutem o emprego da base legal do Legítimo Interesse e a sensibilidade de cada etapa da avaliação que deve ser feita antes de aplicá-la. Confira as instruções e vamos jogar!

instruções

A partir do nível de criticidade identificado nas cartas de análise, o termômetro serve como visão geral e ilustrativa dos pontos de atenção das fases do LIA para cada tema. Assim como se observará em relação às análises, o termômetro utiliza-se de colorações que medem a “temperatura” (grau de sensibilidade) do legítimo interesse para aquela temática: (i) vermelho: alta; (ii) amarelo: média e; (iii) verde: baixa. Aqui, cabe novamente a ressalva de que o termômetro não tem como objetivo afirmar se um caso “passa” ou não no teste de legítimo interesse, mas sim, indicar quais os pontos sensíveis que merecem maior atenção por parte dos agentes de tratamento, titulares e autoridades sobre determinado tema.





Dados pessoais de acesso público e dados tornados manifestamente públicos pelo titular.

O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização (art. 7º, §3º, LGPD).

Será dispensado o consentimento para dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na Lei (art. 7º, §4º, LGPD).

O tratamento posterior dos dados pessoais a que se referem essas duas situações anteriores poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei (art. 7º, §7º, LGPD).

Nesse ponto, importante lembrar sobre os dados pessoais de acesso público.
Exemplos:

- a) Dado pessoal que esteja disponível à consulta pública gratuita por obrigação legal;
- b) Dados de cartórios públicos;
- c) Diários Oficiais;
- d) Dados de servidores públicos.

E também existem os dados pessoais tornados manifestamente públicos pelo titular, cuja iniciativa é do próprio titular de tornar o dado de conhecimento público. (art. 7º, § 4º, LGPD) .

Exemplos:

- a) Dado pessoal publicado em perfis de redes sociais; e
- b) Dado pessoal publicado em *sites* e blogs do próprio titular.

Portanto, se já são de acesso público, não precisam de consentimento para serem tratados pelo Poder Público. Contudo, continuam sendo dados pessoais e devem seguir as regras da LGPD.

ATIVIDADE FISCAL E REGULATÓRIA DOS TC's

Sobre a atuação do TCU e TCE's:

Os tribunais de contas, em geral, têm poder de fiscalização acerca da conformidade à LGPD, com relação ao *compliance* da proteção de dados pessoais nos órgãos públicos (governança, conformidade, previsibilidade de riscos, medidas administrativas e técnicas, dentre outros).

A fiscalização TCU, em auditoria a 382 órgãos públicos: resultados do relatório publicado em 2022:

17,8% estão no nível inexpressivo;

58,9% estão no nível inicial;

20,4% estão no nível intermediário e

2,9% estão no nível aprimorado.



Segundo o Portal do TCU:

“a conclusão do diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD apresentou, portanto, situação de alto risco à privacidade dos cidadãos que têm dados pessoais coletados e tratados pela Administração Pública Federal”.

Isso levou o TCU a expedir recomendação de conformidade á LGPD aos órgãos com baixa conformidade. Inclusive determinando *“implementação de procedimentos internos mais céleres (fast track) e controles simplificados para o uso compartilhado de dados pessoais no âmbito dos órgãos da Administração Direta, considerando o disposto nos arts. 7º, inciso III; 11, inciso II, “b” e “g”; 23; 25; 26 e 27, inciso II, da Lei 13.709/2018 e as diretrizes estabelecidas no item 7.5 da ABNT NBR ISO/IEC 27701:2019”*.

- E porque esta informação está aqui no meio de um curso sobre LGPD no Setor Público?

Para te mostrar que os órgãos de fiscalização estão de olho na LGPD, na conformidade dos órgãos públicos.

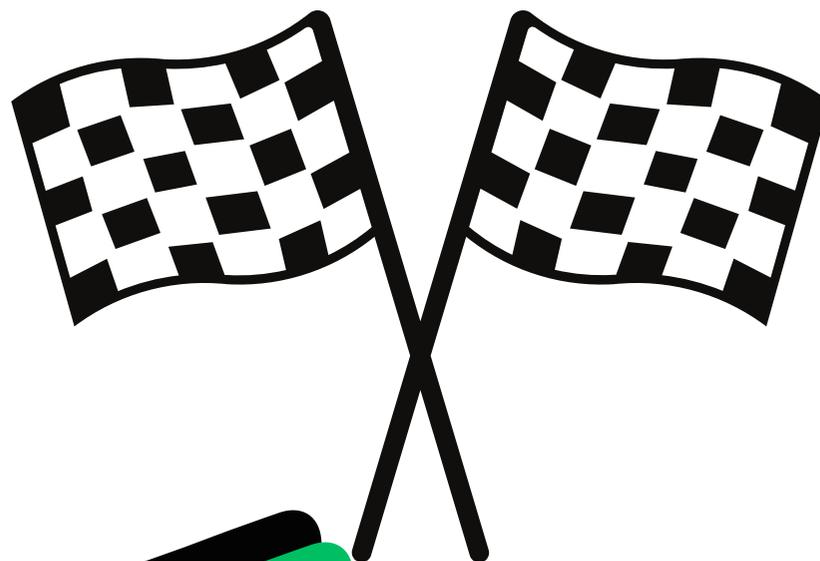
O TCU já publicou seu relatório, mas neste momento há outros tribunais de contas pelo país, a própria ANPD e outros órgãos fiscalizatórios prontos para chegar a qualquer momento e cobrar isso de outros órgãos, inclusive estaduais e municipais.

Atribuições da ANPD: art. 55-J da LGPD.

Atribuições CNPD: art. 58-B.

TCU: tem poder de fiscalização da proteção de dados pessoais nos órgãos públicos (governança, conformidade, previsibilidade de riscos, medidas administrativas e técnicas, dentre outros).





**The
End**



LGPD
no Setor Público