


# Guia de preparação EXIN PDPF

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

| | | |
|---|---|---|
| **5** capítulos por domínio | **32** questões comentadas | **65%** nota de corte |
| **6** provas completas no curso | | |

ANTES DE COMEÇAR

# Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso EXIN PDPF: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

| Quando | O que fazer |
|---|---|
| **Semana 1** | Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame. |
| **Semana 2** | Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3. |
| **Semana 3** | Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação. |
| **Semana 4** | Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 65%). |

## Mapa do exame

Cada prova do curso tem 40 questões e 60 minutos, no formato do exame. Referência de aprovação: 65%.

| Domínio (capítulo) | Peso | Neste guia |
|---|---|---|
| 1. Avaliação e Mitigação de Riscos | 25% | 18 conceitos · 14 pegadinhas |
| 2. Escopo do GDPR | 12,5% | 18 conceitos · 14 pegadinhas |
| 3. Princípios do Tratamento de Dados | 37,5% | 18 conceitos · 14 pegadinhas |
| 4. Prática do Tratamento de Dados | 10% | 18 conceitos · 14 pegadinhas |
| 5. Transferências Internacionais de Dados Pessoais | 15% | 18 conceitos · 14 pegadinhas |

**Como ler os capítulos:** os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

## Estude um pouco todo dia, de graça

### Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o “não confunda” de cada certificação.

**Seguir no Instagram →**

### YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

**Inscrever-se no canal →**

DIAGNÓSTICO

# Você já sabe isso?

Responda às 12 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · Avaliação e Mitigação de Riscos

**Qual é o valor máximo da multa para violar obrigações do controlador e do operador, como as dos artigos 25 a 39?**

A. Até 50 milhões de euros ou 10% do faturamento anual
B. Até 1 milhão de euros, sem relação com o faturamento
C. Até 20 milhões de euros ou 4% do faturamento anual mundial
D. Até 10 milhões de euros ou 2% do faturamento anual mundial

D2 · Avaliação e Mitigação de Riscos

**Um funcionário perdeu um pendrive sem criptografia com a folha de pagamento da empresa. O que isso representa?**

A. Um incidente sem relevância, pois o pendrive era barato e antigo
B. Uma violação de dados pessoais que exige avaliação do risco
C. Um problema só de patrimônio, sem dados pessoais
D. Um evento que só importa se o pendrive for achado

D3 · Avaliação e Mitigação de Riscos

**Qual é o valor máximo de multa administrativa por violar os princípios básicos do tratamento, como os do artigo 5.º?**

A. 10 milhões de euros ou 2% do faturamento anual mundial
B. 1% do faturamento anual obtido na União Europeia
C. 20 milhões de euros ou 4% do faturamento anual mundial
D. 5 milhões de euros, sem relação com o faturamento

D4 · Escopo do GDPR

**Uma loja virtual sediada no Brasil, sem filial na Europa, vende produtos em euros e entrega para clientes na Itália. O GDPR se aplica a esse tratamento?**

A. Não, porque a empresa não tem estabelecimento na União
B. Sim, mas só se os clientes forem cidadãos italianos
C. Não, porque os pagamentos são feitos pela internet
D. Sim, porque oferece bens a pessoas que estão na União

D5 · Escopo do GDPR

**Como o GDPR trata os dados sobre condenações penais e infrações?**

A. Como dados livres para divulgação pela imprensa
B. Como dados anônimos, pois constam de processos públicos
C. Como dados comuns, tratados com qualquer base do artigo 6.º
D. Com regime próprio, sob controle de autoridade pública

D6 · Escopo do GDPR

**Uma companhia aérea registra os passageiros que pedem refeição kosher ou halal. Por que esse registro exige cuidado especial?**

A. Porque cardápios são protegidos por patente
B. Porque viagens aéreas estão fora do GDPR
C. Porque refeições são informações de saúde
D. Porque pode revelar convicções religiosas

D7 · Princípios do Tratamento de Dados

**Como o controlador pode demonstrar que cumpre a proteção de dados desde a concepção e por padrão?**

A. Pelo tamanho da equipe de marketing da empresa
B. Pela quantidade de dados que consegue coletar
C. Por um procedimento de certificação aprovado
D. Pelo número de clientes atendidos por dia

D8 · Princípios do Tratamento de Dados

**Qual princípio do GDPR exige que os dados coletados sejam adequados, pertinentes e limitados ao necessário para a finalidade?**

A. Exatidão
B. Transparência
C. Minimização dos dados
D. Limitação da conservação

D9 · Princípios do Tratamento de Dados

**O controlador havia tornado públicos certos dados e agora deve apagá-los. O que o artigo 17 exige além do apagamento?**

A. Publicar em jornal a lista dos dados que foram apagados
B. Adotar medidas razoáveis para avisar outros controladores
C. Retirar todos os dados da internet mundial em até 24 horas
D. Pagar uma indenização fixa ao titular pelo tempo de exposição

D10 · Prática do Tratamento de Dados

**Qual é a principal característica de um cookie persistente?**

A. Fica no dispositivo até expirar ou ser apagado
B. Só pode ser lido pelo sistema operacional
C. É apagado automaticamente ao fechar o navegador
D. Nunca contém dados pessoais nem identificadores

D11 · Prática do Tratamento de Dados

**Uma ONG passa a usar IA para analisar dados de doadores já coletados. O que é mais importante para cumprir o GDPR nessa mudança?**

A. Deixar de guardar os recibos para fins fiscais
B. Apagar todos os dados coletados até agora
C. Informar os doadores sobre o novo tratamento
D. Tornar os dados públicos para auditoria externa

D12 · Prática do Tratamento de Dados

**Quando um site deve obter o consentimento do visitante para cookies de análise de audiência que não são essenciais?**

A. Só quando o visitante fizer uma compra
B. Antes de gravar os cookies no navegador
C. Depois de trinta dias de navegação no site
D. Ao final de cada ano, em uma campanha

01

CAPÍTULO 1 · 25% DA PROVA

# Avaliação e Mitigação de Riscos

Segundo maior domínio: 25% da prova, cerca de 10 perguntas, com destaque para violações de dados pessoais (12,5%), seguido de DPIA e consulta prévia (7,5%) e autoridades de controle (5%). Preciso saber de cor quando notificar a autoridade (risco, 72 horas desde o conhecimento) e quando comunicar os titulares (alto risco), com as exceções; quando a DPIA é obrigatória e o que contém; e as faixas de multa. A prova adora cenários do tipo 'isso é violação?' (pendrive perdido, enfermeira curiosa, phishing bloqueado). Onde mais erro: trocar as faixas 10 mi/2% e 20 mi/4%, achar que sem acesso indevido não há violação e esquecer que toda violação precisa ser documentada.

**Neste capítulo**

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

## Tópicos-chave

### Violação de dados pessoais (art. 4.º, n.º 12)

Quebra de segurança que causa, de forma acidental ou ilícita, destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais. Inclui acesso interno por curiosidade, envio ao destinatário errado, perda de pendrive sem criptografia e perda irreversível de dados num backup que falhou.

### Incidente de segurança x violação de dados pessoais

Todo incidente com dados pessoais é violação de dados pessoais, mas nem todo incidente de segurança envolve dados pessoais. Phishing bloqueado sem acesso a dados, ou notebook perdido só com projetos de engenharia, é incidente, não violação de dados pessoais.

### Confidencialidade, integridade, disponibilidade

Planilha enviada por engano a outra empresa afeta a confidencialidade; atacante que altera dados bancários afeta a integridade; perda irreversível de dados afeta a disponibilidade. Minimização, anonimização e portabilidade não são aspectos de segurança.

### Notificação à autoridade (art. 33.º)

Sem demora injustificada e, se possível, em até 72 horas desde que o controlador toma conhecimento (certeza razoável de incidente que afetou dados pessoais). Depois disso, vem acompanhada dos motivos do atraso. Se faltam detalhes, notifica e envia as informações em fases. Dispensada só quando não for provável risco aos titulares.

### Conteúdo da notificação e documentação (art. 33.º, n.º 3 e 5)

Natureza da violação, categorias e número aproximado de titulares e de registros, contato do DPO, consequências prováveis e medidas adotadas ou propostas. Não se envia cópia dos dados, senhas nem lista nominal de titulares. Mesmo sem notificar, o controlador documenta a violação, seus efeitos e as medidas adotadas, para que a autoridade possa verificar o cumprimento, inclusive a decisão de não notificar.

### Operador diante de violação

Notifica o controlador sem demora injustificada (art. 33.º, n.º 2); quem avalia o risco e notifica autoridade e titulares é o controlador. O contrato do art. 28.º deve prever que o operador ajude nas obrigações dos arts. 32.º a 36.º.

### Comunicação aos titulares (art. 34.º) e outros interessados

Quando houver provável alto risco aos seus direitos, sem demora injustificada, em linguagem clara e simples: natureza da violação, contato do DPO, consequências prováveis e medidas adotadas. Conforme o caso: bancos emissores (para bloquear cartões vazados), polícia, seguradora, operador e DPO, além da autoridade e dos titulares. Imprensa, concorrentes e acionistas não são exigidos.

### Exceções à comunicação aos titulares (art. 34.º, n.º 3)

Dados ininteligíveis para terceiros (criptografia com chave segura e não comprometida); medidas posteriores fizeram o alto risco deixar de ser provável; ou esforço desproporcional, caso em que se faz comunicação pública ou medida de eficácia equivalente. A notificação à autoridade segue as regras do art. 33.º.

### DPIA: quando (art. 35.º)

Antes de iniciar tratamento que possa gerar alto risco aos direitos e liberdades. Exemplos do n.º 3: avaliação sistemática e extensiva com perfis e efeitos jurídicos (crédito automatizado); grande escala de categorias especiais ou dados penais (hospital); controle sistemático de zonas públicas em grande escala (câmeras nas praças). A autoridade publica lista do que exige DPIA e pode publicar a do que dispensa.

### DPIA: quem e como

Feita pelo controlador, com parecer do DPO; o operador auxilia; quando adequado, ouvem-se os titulares ou seus representantes. Uma única DPIA pode cobrir operações semelhantes com riscos semelhantes (mesmo sistema de câmeras em várias lojas). Deve ser revista quando o risco mudar.

### DPIA: conteúdo mínimo (art. 35.º, n.º 7)

Descrição do tratamento e das finalidades, avaliação da necessidade e da proporcionalidade, avaliação dos riscos e medidas previstas para tratá-los (garantias, controles de segurança, mecanismos para demonstrar conformidade). Não substitui o registro de atividades e não é para cálculo financeiro ou certificação ISO.

### Consulta prévia (art. 36.º)

Se a DPIA indica alto risco residual que o controlador não consegue reduzir, ele consulta a autoridade de controle antes de começar. A autoridade dá orientação por escrito em até 8 semanas, prorrogáveis por mais 6, e pode usar seus poderes do art. 58.º.

### Autoridade de controle

Independência total (art. 52.º): não pede nem recebe instruções externas e o Estado lhe dá recursos. Tarefas (art. 57.º): controlar a aplicação, tratar e investigar reclamações, promover a sensibilização, aconselhar, cooperar. Não aprova previamente todo tratamento, não redige políticas internas e não nomeia DPOs.

### Poderes do art. 58.º

Investigação: ordenar informações, realizar auditorias, acessar dados e instalações, notificar supostas infrações. Correção: advertências, repreensões, ordens para atender direitos, limitação temporária ou definitiva, proibição do tratamento e multas. Autorização/consultivos: pareceres, aprovar BCR e códigos de conduta, acreditar certificadoras, autorizar cláusulas ad hoc. Prisão e falência não são poderes da autoridade.

### Autoridade principal e cooperação

No tratamento transfronteiriço, a autoridade do país do estabelecimento principal é a principal (art. 56.º) e coordena com as demais pelo balcão único; em regra, a notificação de violação vai a ela. As autoridades cooperam por assistência mútua e operações conjuntas (art. 61.º). O titular pode reclamar na autoridade do próprio país (art. 77.º).

### EDPB e EDPS

EDPB (Comitê Europeu para a Proteção de Dados): assegura aplicação coerente do GDPR, reúne as autoridades e o EDPS, emite diretrizes e resolve litígios; não aplica multas nem substitui autoridades. EDPS (Autoridade Europeia para a Proteção de Dados): supervisiona as próprias instituições da UE.

### Multas (art. 83.º)

Art. 83.º, n.º 4: até 10 milhões de euros ou 2% do faturamento anual mundial para obrigações de controlador e operador (como as dos arts. 25.º a 39.º). Art. 83.º, n.º 5: até 20 milhões ou 4% para princípios, bases legais, direitos dos titulares e transferências. Vale o valor mais alto. Pesam natureza, gravidade, duração, intenção ou negligência, mitigação, cooperação, categorias de dados e infrações anteriores. Várias infrações na mesma operação: o total não passa o valor da mais grave. Multar órgãos públicos: cada Estado-membro decide.

### Outras sanções e indenização

Os Estados podem criar outras sanções, inclusive penais, que devem ser efetivas, proporcionadas e dissuasivas (art. 84.º). Quem sofre danos materiais ou imateriais tem direito a indenização do controlador ou do operador (art. 82.º); a multa não vai para o titular. Se a autoridade não trata a reclamação ou não informa em 3 meses, cabe recurso judicial contra ela (art. 78.º).

## Macetes para memorizar

### Notificar x comunicar

Risco: avisa a Autoridade. ALTO risco: avisa Autoridade e titulares. Sem risco: só documenta.

### Exceções à comunicação aos titulares

C-R-E: Criptografia, Risco eliminado depois, Esforço desproporcional (vira comunicação pública).

### Faixas de multa

Dobro para o essencial: 10/2 para obrigações (arts. 25 a 39); 20/4 para princípios, bases, direitos e transferências. Vale sempre o maior valor.

### Prazos de risco

72 horas para a violação; 8 + 6 semanas para a consulta prévia; 3 meses para a autoridade dar notícia da reclamação.

### Exemplos de DPIA obrigatória

P-E-V: Perfil com efeitos jurídicos, Especiais em grande escala, Vigilância pública em grande escala.

### Conteúdo da DPIA

D-N-R-M: Descrição, Necessidade/proporcionalidade, Riscos, Medidas.

### EDPB x EDPS

EDPB = Board que junta as autoridades (coerência). EDPS = Supervisor das instituições da UE.

## Tabela de memorização: não confunda

| Quando é... | ...e quando é |
|---|---|

| | |
|---|---|
| **Notificar a autoridade (art. 33.º)**<br>Violação com risco provável: sem demora injustificada e, se possível, em até 72 horas desde o conhecimento. | **Comunicar os titulares (art. 34.º)**<br>Violação com provável ALTO risco: sem demora injustificada, salvo criptografia, risco eliminado ou esforço desproporcional (comunicação pública). |
| **Incidente de segurança**<br>Tentativa bloqueada ou perda de equipamento sem dados pessoais. | **Violação de dados pessoais**<br>Destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais, acidental ou ilícito. |
| **Multa de até 10 mi € ou 2%**<br>Obrigações do controlador e do operador (arts. 25.º a 39.º). | **Multa de até 20 mi € ou 4%**<br>Princípios (art. 5.º), bases legais, direitos dos titulares (arts. 12.º a 22.º) e transferências. |
| **DPIA**<br>Feita pelo controlador antes do tratamento de provável alto risco. | **Consulta prévia**<br>Quando a DPIA mostra alto risco residual não mitigado: autoridade responde em 8 semanas (+6). |
| **EDPB**<br>Coerência da aplicação do GDPR entre autoridades; diretrizes; litígios. | **EDPS**<br>Supervisão das instituições da própria UE. |
| **Confidencialidade**<br>Dados chegaram a quem não devia (e-mail errado). | **Integridade**<br>Dados foram alterados sem autorização (dados bancários modificados). |

## Números que caem

| Item | Valor |
|---|---|
| Peso do domínio na prova | **25% (10 de 40 perguntas): 5.1 DPIA e consulta prévia 7,5%; 5.2 Violações 12,5%; 5.3 Autoridades de controle 5%** |
| Notificação de violação à autoridade | **sem demora injustificada e, se possível, em até 72 horas desde o conhecimento** |
| Resposta à consulta prévia | **até 8 semanas, prorrogáveis por mais 6** |
| Multa do art. 83.º, n.º 4 | **até 10 milhões de euros ou 2% do faturamento anual mundial (o mais alto)** |
| Multa do art. 83.º, n.º 5 | **até 20 milhões de euros ou 4% do faturamento anual mundial (o mais alto)** |
| Recurso contra autoridade omissa | **se não tratar a reclamação ou não informar o titular em 3 meses (art. 78.º, n.º 2)** |

## Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** As 72 horas contam do início do ataque ou do fim da investigação interna.
**Como não cair:** Contam do momento em que o controlador toma conhecimento.

⚠ **Alerta de prova:** Sem todas as informações, esperar reuni-las ou deixar de notificar.
**Como não cair:** Notificar no prazo e completar em fases.

⚠ **Alerta de prova:** Violação sem risco não notificada não precisa de mais nada; até apagar os registros.
**Como não cair:** Toda violação é documentada (art. 33.º, n.º 5).

⚠ **Alerta de prova:** Operador que descobre a violação notifica direto os titulares ou resolve sozinho.
**Como não cair:** Avisa o controlador sem demora injustificada.

⚠ **Alerta de prova:** Notebook furtado com dados criptografados não é violação.
**Como não cair:** Pode ser violação; o que se dispensa é a comunicação aos titulares, porque os dados estão ininteligíveis.

⚠ **Alerta de prova:** Perda de dados num backup que falhou não é violação porque ninguém acessou ou porque não foi ataque.
**Como não cair:** Perda acidental afeta a disponibilidade e é violação, para qualquer dado pessoal.

⚠ **Alerta de prova:** Enfermeira do mesmo hospital que só olhou o prontuário não cometeu violação.
**Como não cair:** Acesso sem necessidade é acesso não autorizado, mesmo interno e sem cópia.

⚠ **Alerta de prova:** Phishing bloqueado ou notebook só com projetos é violação com notificação em 72 horas.
**Como não cair:** Sem dados pessoais afetados, é incidente, não violação de dados pessoais.

⚠ **Alerta de prova:** Violar princípios ou direitos dos titulares cai na faixa de 10 mi/2%.
**Como não cair:** Princípios e direitos estão na faixa de 20 mi/4% (art. 83.º, n.º 5).

⚠ **Alerta de prova:** O GDPR proíbe multar órgãos públicos, ou fixa 20 milhões para eles.
**Como não cair:** Cada Estado-membro decide.

⚠ **Alerta de prova:** DPIA é feita depois de uma violação, a pedido do titular ou pela autoridade.
**Como não cair:** Controlador faz antes de iniciar o tratamento de provável alto risco.

⚠ **Alerta de prova:** Loja que guarda e-mails para recibos precisa de DPIA porque e-mail é sensível.
**Como não cair:** Baixo risco não exige DPIA; e-mail não é categoria especial.

⚠ **Alerta de prova:** Alto risco residual: pedir autorização à Comissão Europeia ou publicar a DPIA.
**Como não cair:** Consulta prévia à autoridade de controle.

⚠ **Alerta de prova:** Reclamação de empresa com sede na Irlanda só pode ser feita na Irlanda, na Comissão ou no Tribunal de Justiça.
**Como não cair:** O titular pode reclamar na autoridade do seu país, que coopera com a principal.

## Como cai na prova

📝 **Como cai:** Cenário de incidente + 'isso é uma violação de dados pessoais?'
**Como resolver:** 1) Havia dados pessoais? Se não, é só incidente. 2) Houve destruição, perda, alteração, divulgação ou acesso não autorizado, acidental ou ilícito? Se sim, é violação, mesmo sem ataque e mesmo interno.

📝 **Como cai:** 'Quem deve ser informado e em quanto tempo?'
**Como resolver:** Avalie o risco: sem risco provável = documentar; risco = autoridade em até 72 horas desde o conhecimento; alto risco = também os titulares, salvo as três exceções. Operador só avisa o controlador.

📝 **Como cai:** Cenário de novo tratamento + 'o GDPR exige DPIA?'
**Como resolver:** Procure alto risco provável: perfis com efeitos jurídicos, categorias especiais em grande escala, vigilância de áreas públicas em grande escala, lista da autoridade. Tratamento simples e de baixo risco não exige. DPIA é sempre antes e feita pelo controlador.

📝 **Como cai:** 'Qual o valor máximo da multa?'
**Como resolver:** Identifique o que foi violado: obrigação de controlador/operador (DPO, registro, segurança, DPIA, notificação) = 10 mi/2%; princípios, bases legais, direitos ou transferências = 20 mi/4%. O maior valor entre fixo e percentual.

📝 **Como cai:** Tarefas e poderes da autoridade, EDPB e EDPS.
**Como resolver:** Autoridade: independente, trata reclamações, sensibiliza, audita, limita/proíbe, multa, aprova BCR. Descarte fixar preços, nomear diretores, prender ou decretar falência. EDPB = coerência; EDPS = instituições da UE.

## Gatilhos do enunciado

| Se o enunciado trouxer... | Pense em |
|---|---|

| | |
|---|---|
| '72 horas' | **Notificação à autoridade, contada do conhecimento.** |
| Notificou depois de 72 horas (ex.: 96 horas) | **Incluir os motivos do atraso.** |
| Ainda faltam detalhes | **Notificar em fases.** |
| Dados criptografados com chave segura | **Dispensa a comunicação aos titulares.** |
| Comunicar cada titular exigiria esforço desproporcional | **Comunicação pública ou medida equivalente.** |
| Cartões de pagamento vazados | **Avisar também os bancos emissores.** |
| E-mail enviado ao destinatário errado | **Confidencialidade.** |
| Dados perdidos para sempre | **Disponibilidade: é violação.** |
| Crédito automatizado com efeitos jurídicos, saúde em grande escala, câmeras em praças públicas | **DPIA obrigatória antes.** |
| Alto risco residual que não dá para reduzir | **Consulta prévia: 8 semanas (+6).** |
| Empresa com estabelecimento principal em outro país da UE | **Autoridade principal (balcão único).** |
| Instituições da própria UE | **EDPS.** |
| Aplicação coerente do GDPR entre países | **EDPB.** |
| Autoridade não respondeu em 3 meses | **Recurso judicial contra a autoridade (art. 78.º).** |

### 🎯 Se você lembrar de só uma coisa deste capítulo...

- 72 horas contam do conhecimento; atrasou, justifica; faltou informação, notifica em fases.
- Risco = autoridade; alto risco = autoridade + titulares; toda violação é documentada.
- Perda acidental, acesso interno por curiosidade e e-mail errado são violações; phishing bloqueado não.
- 10 mi/2% para obrigações de controlador e operador; 20 mi/4% para princípios, bases, direitos e transferências.
- DPIA antes do tratamento de alto risco; alto risco residual = consulta prévia à autoridade (8 + 6 semanas).

## Essenciais para a prova (checklist)

- ☐ Sei definir violação de dados pessoais e diferenciá-la de incidente de segurança.
- ☐ Sei classificar um caso como falha de confidencialidade, integridade ou disponibilidade.

- ☐ Sei o prazo, o marco inicial e o conteúdo da notificação à autoridade.
- ☐ Sei quando comunicar os titulares e as três exceções do art. 34.º, n.º 3.
- ☐ Sei o papel do operador numa violação.
- ☐ Sei quando a DPIA é obrigatória, quem a faz, quando e o que deve conter.
- ☐ Sei quando cabe consulta prévia e o prazo de resposta da autoridade.
- ☐ Sei as tarefas e os poderes da autoridade de controle e a regra da autoridade principal.
- ☐ Sei diferenciar EDPB e EDPS.
- ☐ Sei as duas faixas de multa, os fatores de dosimetria e as regras para várias infrações e órgãos públicos.

## Questões de revisão do capítulo

R1.1 · Avaliação e Mitigação de Riscos

**Além das multas administrativas, o GDPR permite que os Estados-membros criem outras sanções. Como elas devem ser?**

A. Simbólicas, sem efeito financeiro
B. Aplicadas só a órgãos públicos
C. Iguais para qualquer tipo de infração
D. Efetivas, proporcionadas e dissuasivas

R1.2 · Avaliação e Mitigação de Riscos

**Após identificar os riscos, o que a DPIA deve apresentar sobre eles?**

A. As medidas previstas para tratar os riscos
B. A lista de clientes que podem ser afetados
C. O nome dos atacantes mais prováveis
D. O valor de mercado dos dados tratados

R1.3 · Avaliação e Mitigação de Riscos

**Uma empresa já tinha sido multada pela mesma infração dois anos antes. Como isso pesa na nova multa?**

A. Obriga a autoridade a aplicar o valor mínimo
B. Infrações anteriores são fator a considerar no valor
C. Não pesa, pois cada caso é analisado sem olhar o histórico
D. Anula a nova multa, pois já houve punição

R1.4 · Avaliação e Mitigação de Riscos

**A partir de quando começa a contar o prazo de 72 horas para notificar uma violação à autoridade?**

A. Da data em que o ataque de fato começou nos sistemas
B. Da primeira reclamação de um titular
C. Do momento em que o controlador toma conhecimento
D. Do fim da investigação interna completa

## Respostas comentadas

### R1.1. D) Efetivas, proporcionadas e dissuasivas

Por quê: Os Estados podem prever sanções, inclusive penais, para infrações não sujeitas a multas administrativas.

✗ A) Incorreta. Devem ser efetivas.
✗ B) Incorreta. Valem para outros casos também.
✗ C) Incorreta. Devem ser proporcionadas.

> **Dica de prova:** Sanções: efetivas, proporcionadas, dissuasivas.

### R1.2. A) As medidas previstas para tratar os riscos

Por quê: As medidas incluem garantias, controles de segurança e mecanismos para proteger os dados e demonstrar conformidade.

✗ B) Incorreta. Não é o exigido.
✗ C) Incorreta. Não é o exigido.
✗ D) Incorreta. Não é o exigido.

> **Dica de prova:** DPIA: riscos + medidas para tratá-los.

### R1.3. B) Infrações anteriores são fator a considerar no valor

Por quê: A reincidência tende a agravar a multa, enquanto a cooperação e a mitigação de danos podem atenuá-la.

✗ A) Incorreta. Não há essa regra.
✗ C) Incorreta. O histórico é considerado.
✗ D) Incorreta. Não há anulação.

> **Dica de prova:** Reincidência pesa na multa.

**R1.4. C) Do momento em que o controlador toma conhecimento**

Por quê: O controlador toma conhecimento quando tem certeza razoável de que houve um incidente de segurança que afetou dados pessoais.

✗ A) Incorreta. Conta do conhecimento.

✗ B) Incorreta. Não depende de reclamação.

✗ D) Incorreta. Não se espera terminar.

> **Dica de prova:** 72 h: a partir do conhecimento.

02

CAPÍTULO 2 · 12,5% DA PROVA

# Escopo do GDPR

Aqui eu preciso separar com segurança o que é e o que não é dado pessoal, o que é tratamento e quando o GDPR se aplica (ou fica de fora). Vale 12,5% da prova, cerca de 5 perguntas, quase sempre em cenário curto: um IP, uma imagem de câmera, uma ficha de papel, um cargo único num relatório. Também caem a base jurídica europeia (regulamento x diretiva, Carta da UE, Convenção Europeia dos Direitos Humanos) e a diferença entre privacidade, proteção de dados e segurança. Onde mais erro: achar que sem nome não há dado pessoal, confundir pseudonimizado com anônimo e esquecer que o GDPR alcança empresas fora da UE que oferecem bens a quem está na União.

**Neste capítulo**
18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

# Tópicos-chave

### Privacidade

Ideia clássica: proteção contra interferência indevida na vida privada. É mais ampla que proteção de dados e envolve vida privada, família, domicílio e comunicações. Não é técnica de criptografia nem regra de preço de internet.

### Proteção de dados x privacidade

A proteção de dados é um meio de proteger a privacidade: o conjunto de regras e medidas que protege esse direito quando há tratamento de dados. Não são sinônimos, e a privacidade não é uma 'parte técnica' da proteção de dados; é o contrário.

### Segurança da informação x proteção de dados

A segurança (confidencialidade, integridade, disponibilidade) é só uma parte da proteção de dados. Um tratamento pode ser muito seguro e ainda assim ilícito, por exemplo sem base legal ou com finalidade incompatível. Criptografar não basta para cumprir o GDPR.

### Dado pessoal (art. 4.º, n.º 1)

Qualquer informação relativa a pessoa singular identificada ou identificável, direta ou indiretamente, por exemplo por um número de identificação ou identificador por via eletrônica. O formato não importa: texto, imagem, áudio ou vídeo. Não precisa conter o nome.

### Identificação indireta

Histórico de compras ligado ao número do cartão de fidelidade, ou 'a diretora financeira da empresa X' quando o cargo é ocupado por uma única pessoa, são dados pessoais. A combinação de elementos como cargo e empresa já aponta para alguém.

### Endereço IP

Um IP que o provedor consegue associar a um assinante é identificador por via eletrônica e, portanto, dado pessoal (considerando 30). Mesmo dinâmico pode identificar; não precisa mostrar o nome.

### Imagem de câmera

Imagem em que a pessoa pode ser reconhecida é dado pessoal, mesmo captada em local aberto ao público e mesmo sem som.

### Tratamento (art. 4.º, n.º 2)

Qualquer operação sobre dados pessoais, automatizada ou não: coleta, registro, organização, conservação, consulta, uso, divulgação, apagamento e destruição. Só visualizar um cadastro na tela já é tratamento; apagar também é.

### Sistema de arquivo (tratamento manual)

O GDPR vale para o tratamento automatizado e para o manual de dados contidos ou destinados a um sistema de arquivo (art. 2.º, n.º 1 e art. 4.º, n.º 6). Fichas de papel em ordem alfabética já estão no escopo, sem precisar digitalizar.

### Categorias especiais (art. 9.º)

Origem racial ou étnica, opiniões políticas, convicções religiosas, filiação sindical, dados genéticos, dados biométricos para identificar a pessoa de forma inequívoca, saúde e vida ou orientação sexual. Só podem ser tratadas nas exceções do art. 9.º, n.º 2. Número de passaporte NÃO está no art. 9.º (o art. 87.º permite regras nacionais sobre números de identificação).

### Dado que revela categoria especial

O art. 9.º protege também informação indireta: pedir refeição kosher ou halal pode revelar convicção religiosa. Diagnóstico em atestado é dado de saúde; impressão digital para ponto é dado biométrico.

### Dados penais (art. 10.º)

Condenações penais e infrações têm regime próprio: só podem ser tratadas sob controle de autoridade pública ou quando autorizado por lei com garantias adequadas. Não são dados comuns tratáveis com qualquer base do art. 6.º, nem viram anônimos por constarem de processos públicos.

### Pseudonimização (art. 4.º, n.º 5)

Trocar nomes por códigos e guardar a tabela de ligação em outro sistema reduz riscos, mas os dados continuam pessoais, porque podem ser atribuídos à pessoa com informação adicional. Pseudonimizar não muda a categoria do dado.

### Anonimização (considerando 26)

Dados anônimos, sem reidentificação por meios razoáveis, ficam fora do GDPR, mesmo que tenham vindo de dados pessoais. O processo de anonimizar em si é tratamento.

### Exclusões do escopo

Atividade exclusivamente pessoal ou doméstica (agenda de contatos para uso próprio) fica fora (art. 2.º, n.º 2, alínea c). Polícia investigando crimes segue a Diretiva (UE) 2016/680, não o GDPR. Dados de pessoas falecidas ficam fora (considerando 27), mas cada Estado-membro pode criar regras.

### Alcance territorial (art. 3.º)

N.º 1: aplica-se ao tratamento no contexto de um estabelecimento na União, esteja o servidor onde estiver. N.º 2: alcança controladores fora da UE que oferecem bens ou serviços a pessoas que estão na União ou monitoram o comportamento delas. O critério é estar na União, não a cidadania.

### Regulamento x diretiva e atos da UE

O GDPR (Regulamento 2016/679) substituiu a Diretiva 95/46/CE e é obrigatório e diretamente aplicável, com cláusulas de abertura para leis nacionais (ex.: art. 88.º, trabalho). Pelo art. 288.º do TFUE: regulamento, diretiva, decisão, recomendação e parecer; só recomendação e parecer não vinculam.

### Base de direitos fundamentais

Convenção Europeia dos Direitos Humanos (Conselho da Europa), art. 8.º: respeito pela vida privada e familiar. Carta dos Direitos Fundamentais da UE: art. 7.º privacidade e art. 8.º proteção de dados como direito fundamental próprio. O art. 1.º do GDPR protege em primeiro lugar os direitos e liberdades das pessoas, e garante a livre circulação dos dados na União.

## Macetes para memorizar

### 💡 Regulamento x diretiva

Regulamento é Reto (aplica direto); Diretiva Depende de lei nacional.

### 💡 Atos não vinculativos

Recomendação e Parecer não Prendem (R-P).

### Carta da UE

Sete é a vida privada, oito são os dados. Na CEDH, o 8 é vida privada e familiar.

### Pseudônimo x anônimo

Tem chave? É pessoal. Sem volta? Está fora.

### Categorias especiais

Oito sensíveis: Raça, Política (opiniões), Fé, Sindicato, DNA (genéticos), Digital (biometria para identificar), Saúde, Sexualidade.

### Tratamento

Do berço ao túmulo: coletar, olhar, guardar, usar, apagar, destruir. Tocou no dado, tratou.

### Alcance territorial

Sede na UE ou alvo na UE: GDPR em qualquer dos dois.

## Tabela de memorização: não confunda

| Quando é... | ...e quando é |
|---|---|
| **Dado pseudonimizado**<br>Há chave ou tabela que permite religar o código à pessoa: continua dado pessoal e sob o GDPR. | **Dado anônimo**<br>Ninguém consegue reidentificar por meios razoáveis: deixa de ser dado pessoal e sai do GDPR. |
| **Regulamento**<br>Obrigatório em todos os elementos e diretamente aplicável em todos os Estados-membros (é o caso do GDPR). | **Diretiva**<br>Fixa um resultado a alcançar e precisa ser transposta por lei nacional (ex.: Diretiva ePrivacy). |
| **Dado pessoal comum**<br>Endereço, e-mail corporativo, histórico de compras, número do passaporte. | **Categoria especial (art. 9.º)**<br>Saúde, biometria para identificar, genética, religião, opinião política (filiação a partido), filiação sindical, origem racial ou étnica, vida ou orientação sexual. |
| **Art. 3.º, n.º 1 (estabelecimento)**<br>Empresa com sede na UE: GDPR se aplica mesmo com servidores no Brasil. | **Art. 3.º, n.º 2 (alvo)**<br>Empresa sem filial na UE que vende em euros e entrega na Itália, ou monitora usuários na União: GDPR se aplica. |
| **Diretiva (UE) 2016/680**<br>Tratamento por polícia e autoridades judiciárias para prevenir, investigar e reprimir infrações penais. | **Diretiva ePrivacy**<br>Cookies e comunicações eletrônicas; não é a norma da investigação criminal. |
| **CEDH, art. 8.º**<br>Tratado do Conselho da Europa: respeito pela vida privada e familiar; base histórica da privacidade. | **Carta da UE, arts. 7.º e 8.º**<br>Carta da UE separa privacidade (art. 7.º) e proteção de dados como direito fundamental próprio (art. 8.º). |

## Números que caem

| Item | Valor |
|---|---|
| Peso do domínio na prova | **12,5% (5 de 40 perguntas): 1.1 Privacidade e proteção de dados 5%; 1.2 Escopo do GDPR 7,5%** |
| GDPR | **Regulamento (UE) 2016/679, que substituiu a Diretiva 95/46/CE** |
| Polícia e infrações penais | **Diretiva (UE) 2016/680** |
| Carta dos Direitos Fundamentais da UE | **art. 7.º privacidade; art. 8.º proteção de dados** |
| Convenção Europeia dos Direitos Humanos | **art. 8.º: vida privada e familiar** |
| Atos jurídicos da UE | **art. 288.º do TFUE: 5 tipos; 2 não vinculativos (recomendação e parecer)** |

## Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Não é dado pessoal porque o nome não aparece no registro.
**Como não cair:** Basta a pessoa ser identificável, direta ou indiretamente: cartão de fidelidade, cargo único ou IP já identificam.

⚠ **Alerta de prova:** Fichas de papel não são dados pessoais, ou só entram no GDPR depois de digitalizadas.
**Como não cair:** O suporte não importa: papel organizado em sistema de arquivo já está no escopo.

⚠ **Alerta de prova:** Apagar não é tratamento, porque o dado deixa de existir.
**Como não cair:** Qualquer operação é tratamento, inclusive apagamento e destruição, automatizados ou manuais.

⚠ **Alerta de prova:** Só olhar o cadastro na tela, sem alterar ou imprimir, não é tratamento.
**Como não cair:** Consulta e visualização estão na definição; tratamento não exige alteração nem envio a terceiros.

⚠ **Alerta de prova:** Empresa sem estabelecimento na União está fora do GDPR.
**Como não cair:** Pelo art. 3.º, n.º 2, oferecer bens ou serviços a quem está na União (ou monitorar comportamento) já atrai o GDPR.

⚠ **Alerta de prova:** O GDPR só vale se os clientes forem cidadãos italianos.
**Como não cair:** No art. 3.º, n.º 2, o critério é a pessoa estar na União, não a cidadania. A residência também não define se o dado é pessoal.

⚠ **Alerta de prova:** Servidores fora da UE (ou a lei brasileira) afastam o GDPR de uma empresa com sede na Espanha.
**Como não cair:** Tratamento no contexto de estabelecimento na União segue o GDPR, onde quer que o tratamento ocorra.

⚠ **Alerta de prova:** Dados pseudonimizados são anônimos e saem do regulamento.
**Como não cair:** Se existe informação adicional que reidentifica, o dado continua pessoal.

⚠ **Alerta de prova:** Estatística anonimizada continua sob o GDPR porque veio de dados pessoais.
**Como não cair:** Após anonimizar de verdade (sem reidentificação razoável), o resultado fica fora do GDPR.

⚠ **Alerta de prova:** IP não é dado pessoal por ser número técnico ou por mudar de tempos em tempos.
**Como não cair:** IP associável a um assinante é identificador por via eletrônica; mesmo dinâmico pode identificar.

⚠ **Alerta de prova:** Atestado é documento oficial, então o diagnóstico é dado público (ou comum).
**Como não cair:** Diagnóstico é dado de saúde, categoria especial do art. 9.º.

⚠ **Alerta de prova:** Número do passaporte é categoria especial.
**Como não cair:** Merece cuidado, mas não está no art. 9.º; é dado pessoal comum.

⚠ **Alerta de prova:** Agenda no celular está no GDPR porque o celular é sistema automatizado.
**Como não cair:** Atividade exclusivamente pessoal ou doméstica fica fora, qualquer que seja o meio.

⚠ **Alerta de prova:** O GDPR é uma diretiva que exige lei nacional de transposição.
**Como não cair:** É regulamento: obrigatório e diretamente aplicável, com algumas cláusulas de abertura.

## Como cai na prova

📝 **Como cai:** 'Essa informação é dado pessoal?' com um cenário em que falta o nome.
**Como resolver:** Pergunte: dá para chegar à pessoa, direta ou indiretamente? Se sim, é dado pessoal. Descarte alternativas que exigem nome, publicação, residência ou som.

📝 **Como cai:** 'O GDPR se aplica a esse tratamento?' com empresa fora da UE ou servidor fora da UE.
**Como resolver:** Verifique art. 3.º: há estabelecimento na União (n.º 1)? Oferece bens/serviços ou monitora quem está na União (n.º 2)? Qualquer sim = aplica. Descarte cidadania e meio de pagamento.

📝 **Como cai:** 'Como o GDPR classifica esse dado?' (atestado, digital, refeição, passaporte).
**Como resolver:** Confira a lista do art. 9.º e se a informação revela algo da lista, mesmo indiretamente. Penal vai para o art. 10.º. Passaporte é comum.

📝 **Como cai:** 'Isso é tratamento?' para operações passivas (ver, apagar).
**Como resolver:** Lembre que qualquer operação é tratamento; a alternativa que restringe o conceito (só coleta, só se imprimir, só automatizado) está errada.

📝 **Como cai:** Questões de base jurídica: tipo de ato, Carta, CEDH, relação privacidade x proteção x segurança.
**Como resolver:** Regulamento direto; diretiva transposta; recomendação/parecer não vinculam. Proteção de dados é meio para a privacidade; segurança é só uma parte.

## Gatilhos do enunciado

| Se o enunciado trouxer... | Pense em |
|---|---|
| 'nome não aparece', 'só um código', 'número do cartão', 'cargo ocupado por uma única pessoa' | **Identificável indiretamente: é dado pessoal.** |
| Tabela de ligação guardada em outro sistema | **Pseudonimização: continua dado pessoal.** |
| 'ninguém pode ser reidentificado por meios razoáveis', estatísticas agregadas | **Anônimo: fora do GDPR.** |
| Fichas de papel em ordem alfabética, arquivo | **Sistema de arquivo: GDPR se aplica.** |
| Apenas visualiza, consulta, apaga, destrói | **Tudo é tratamento.** |
| Empresa fora da UE vende em euros, entrega na UE ou monitora usuários europeus | **Art. 3.º, n.º 2: GDPR se aplica.** |
| Sede na UE e servidores em outro país | **Art. 3.º, n.º 1: GDPR se aplica.** |
| Diagnóstico, impressão digital, partido político, sindicato, refeição religiosa | **Categoria especial do art. 9.º.** |
| Condenações penais, infrações | **Art. 10.º: regime próprio, controle de autoridade pública.** |
| Polícia investigando crimes | **Diretiva (UE) 2016/680, não o GDPR.** |
| Agenda pessoal, contatos e aniversários de amigos | **Exceção doméstica: fora do GDPR.** |
| Pessoa falecida | **Fora do GDPR; Estado-membro pode legislar.** |

| | |
|---|---|
| 'ato que não vincula' | **Recomendação ou parecer (art. 288.º do TFUE).** |
| 'tratado do Conselho da Europa', 'vida privada e familiar' | **Convenção Europeia dos Direitos Humanos, art. 8.º.** |

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Identificável basta: sem nome ainda é dado pessoal.
- Pseudonimizado continua pessoal; só o anônimo de verdade sai do GDPR.
- Oferecer bens ou monitorar quem está na União atrai o GDPR para empresa de fora.
- Passaporte não é categoria especial; refeição religiosa revela religião.
- Polícia investigando crime: Diretiva 2016/680; uso doméstico e falecidos: fora do GDPR.

## Essenciais para a prova (checklist)

- ☐ Sei definir dado pessoal e dar exemplos de identificação indireta (IP, cargo único, cartão de fidelidade).
- ☐ Sei que qualquer operação, inclusive consultar e apagar, é tratamento.
- ☐ Sei que fichas de papel em sistema de arquivo estão no escopo do GDPR.
- ☐ Sei listar as categorias especiais do art. 9.º e reconhecer que passaporte não está nelas.
- ☐ Sei que dados penais seguem o art. 10.º.
- ☐ Sei diferenciar pseudonimização de anonimização e o efeito de cada uma no escopo.
- ☐ Sei aplicar o art. 3.º, n.º 1 e n.º 2 a empresas e servidores fora da UE.
- ☐ Sei as exclusões: uso doméstico, polícia (Diretiva 2016/680) e falecidos.
- ☐ Sei diferenciar regulamento, diretiva, decisão, recomendação e parecer.
- ☐ Sei situar a CEDH art. 8.º e a Carta da UE arts. 7.º e 8.º.

## Questões de revisão do capítulo

R2.1 · Escopo do GDPR

**Um endereço IP que o provedor consegue associar a um assinante pode ser considerado dado pessoal?**

A. Não, pois é só um número técnico da rede
B. Não, pois muda de tempos em tempos
C. Sim, mas só quando mostra o nome da pessoa
D. Sim, é um identificador por via eletrônica

R2.2 · Escopo do GDPR

**A imagem de uma câmera de segurança em que um cliente pode ser reconhecido é dado pessoal?**

A. Não, pois foi captada em local aberto ao público
B. Não, pois imagens não são informações escritas
C. Sim, mas só quando a gravação tem som
D. Sim, pois permite identificar a pessoa

R2.3 · Escopo do GDPR

**No sistema jurídico da União Europeia, o GDPR é classificado como qual tipo de ato?**

A. Regulamento, obrigatório e diretamente aplicável
B. Recomendação, que não gera obrigações legais
C. Diretiva, que exige lei nacional de transposição
D. Decisão, vinculante só para destinatários específicos

R2.4 · Escopo do GDPR

**Uma pessoa guarda no celular os telefones e aniversários dos amigos para uso próprio. O GDPR se aplica a esse tratamento?**

A. Não, pois é atividade exclusivamente pessoal ou doméstica
B. Sim, pois qualquer lista de contatos exige consentimento prévio
C. Não, pois números de telefone não são dados pessoais
D. Sim, pois o celular é um sistema automatizado

## Respostas comentadas

**R2.1. D) Sim, é um identificador por via eletrônica**

Por quê: Dado pessoal é qualquer informação relativa a pessoa identificada ou identificável, direta ou indiretamente, inclusive por identificadores por via eletrônica.

✗ A) Incorreta. Pode levar à identificação.
✗ B) Incorreta. Mesmo dinâmico pode identificar.
✗ C) Incorreta. Não precisa conter o nome.

> **Dica de prova:** IP identificável: dado pessoal.

**R2.2. D) Sim, pois permite identificar a pessoa**

Por quê: Qualquer informação relativa a pessoa identificável é dado pessoal, seja texto, imagem, áudio ou vídeo.

✗ A) Incorreta. O local não afasta o GDPR.
✗ B) Incorreta. O formato não importa.
✗ C) Incorreta. O som não é necessário.

> **Dica de prova:** Imagem reconhecível: dado pessoal.

**R2.3. A) Regulamento, obrigatório e diretamente aplicável**

Por quê: O GDPR (Regulamento 2016/679) substituiu a Diretiva 95/46/CE e se aplica diretamente em toda a UE, com algumas cláusulas de abertura para leis nacionais.

✗ B) Incorreta. Recomendações não são vinculantes.
✗ C) Incorreta. Diretivas fixam objetivos; o GDPR não é diretiva.
✗ D) Incorreta. Decisões obrigam apenas quem é destinatário.

> **Dica de prova:** GDPR = regulamento: direto e uniforme na UE.

**R2.4. A) Não, pois é atividade exclusivamente pessoal ou doméstica**

Por quê: A exceção vale para atividades sem ligação com atividade profissional ou comercial, como correspondência e agendas pessoais.

✗ B) Incorreta. A exceção doméstica afasta o GDPR.
✗ C) Incorreta. São dados pessoais.
✗ D) Incorreta. O meio não afasta a exceção.

> **Dica de prova:** Uso pessoal ou doméstico: fora do GDPR.

03

CAPÍTULO 3 · 37,5% DA PROVA

# Princípios do Tratamento de Dados

Este é o domínio mais pesado: 37,5% da prova, cerca de 15 perguntas. Preciso dominar os papéis (controlador, operador, responsáveis conjuntos, DPO), as seis bases legais, os princípios do art. 5.º, os sete princípios de privacy by design, o by default e todos os direitos do titular com seus prazos e exceções. As perguntas quase sempre trazem um cenário e pedem 'qual princípio', 'qual base legal' ou 'qual direito'. Onde mais erro: misturar minimização com limitação da conservação, proporcionalidade com subsidiariedade, limitação com apagamento, e trocar o prazo de 1 mês do titular pelas 72 horas de violação.

**Neste capítulo**

18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

## Tópicos-chave

### Controlador (art. 4.º, n.º 7)

Quem determina as finalidades e os meios do tratamento, sozinho ou com outros. É quem cumpre os princípios e deve demonstrar isso (art. 5.º, n.º 2), quem prova o consentimento e quem responde pela conformidade; não transfere essa responsabilidade ao operador ou ao fornecedor de TI.

### Operador (art. 4.º, n.º 8)

Trata dados por conta do controlador e segue instruções, como a nuvem que só armazena. O mesmo provedor pode ser controlador de outros dados (faturamento dos próprios clientes). Se usa os dados para finalidades próprias, passa a ser tratado como controlador desse tratamento (art. 28.º, n.º 10).

### Responsáveis conjuntos (art. 26.º)

Duas ou mais empresas que decidem juntas finalidades e meios (ex.: programa de fidelidade comum). O acordo entre elas deve deixar claro quem cumpre cada obrigação, e sua essência deve ser disponibilizada ao titular.

### Destinatário (art. 4.º, n.º 9)

Quem recebe os dados, seja ou não terceiro. Autoridades públicas que recebem dados numa investigação específica, segundo o direito da União ou nacional, não são consideradas destinatárias.

### Contrato do art. 28.º

Escrito, antes do início: objeto, duração, natureza, finalidade, tipos de dados e obrigações do operador. O operador só trata mediante instruções documentadas; garante confidencialidade do pessoal e segurança, apoia os direitos dos titulares, devolve ou elimina os dados ao final e permite auditorias. Suboperador exige autorização prévia por escrito do controlador; com autorização geral, o operador informa mudanças e o controlador pode se opor.

### Registro das atividades e dispensa (art. 30.º)

Controlador registra finalidades, categorias de titulares e de dados, destinatários, transferências internacionais, prazos de eliminação e, quando possível, medidas de segurança. O operador também mantém registro das categorias de tratamento feitas para cada controlador. É por escrito, inclusive eletrônico, e fica disponível à autoridade quando pedir; registra categorias, não nomes de titulares. Empresas com menos de 250 pessoas ficam dispensadas, salvo se o tratamento gerar risco, não for ocasional ou envolver categorias especiais ou dados penais. Empresa de 80 funcionários que trata dados de saúde dos empregados regularmente NÃO está dispensada.

### Encarregado (DPO): quando, tarefas e independência

Obrigatório (art. 37.º, n.º 1) quando o tratamento é feito por organismo público, ou a atividade principal envolve monitoramento regular e sistemático em grande escala ou categorias especiais em grande escala. Pode ser funcionário ou externo por contrato de serviços, com conhecimento especializado. Tarefas: informar e aconselhar, controlar a conformidade, orientar sobre a DPIA e cooperar com a autoridade (art. 39.º). Não recebe instruções sobre suas tarefas, não pode ser punido por exercê-las e responde à direção ao mais alto nível. Pode ter outras funções sem conflito de interesses: quem decide finalidades e meios (ex.: diretor de TI) não pode fiscalizar a si mesmo. Não precisa ser advogado nem trabalhar em outro país.

### Representante na União (art. 27.º)

Empresa sem estabelecimento na UE que monitora pessoas na União designa por escrito um representante num Estado-membro onde estão os titulares, como ponto de contato de autoridades e titulares. Não afasta a responsabilidade do controlador.

### Princípios do art. 5.º

Licitude, lealdade e transparência; limitação da finalidade (determinada, explícita, legítima); minimização (adequados, pertinentes e limitados ao necessário); exatidão (corrigir ou apagar sem demora); limitação da conservação (tempo); integridade e confidencialidade (segurança); e responsabilização (cumprir e demonstrar). Portabilidade e retificação são direitos, não princípios.

### Proporcionalidade e subsidiariedade

Proporcionalidade: a interferência na privacidade deve ser proporcional ao objetivo (registrar cada tecla para medir pausas é excessivo). Subsidiariedade: a finalidade não pode ser atingida de forma razoável por meio menos invasivo (câmera no banheiro quando um monitor no corredor resolveria).

### Seis bases legais (art. 6.º, n.º 1)

Consentimento, execução de contrato, obrigação legal, interesses vitais, interesse público e interesse legítimo. Basta uma base válida por finalidade. Interesse legítimo exige ponderação com os direitos do titular (que prevalecem, sobretudo se for criança); autoridades públicas no exercício das funções não o usam. Considerando 47: o tratamento estritamente necessário para prevenir fraudes é interesse legítimo, e o marketing direto pode ser baseado nele. Mesmo assim o titular pode se opor a qualquer momento, e as regras de ePrivacy para e-mails continuam valendo.

### Consentimento válido e crianças (arts. 7.º e 8.º)

Livre, específico, informado e inequívoco, por ato positivo; silêncio, inatividade ou caixa pré-marcada não valem. O pedido deve se distinguir dos outros assuntos (não escondido nos termos). Não é livre se condicionado a tratamento desnecessário ao contrato (art. 7.º, n.º 4). Retirar deve ser tão fácil quanto dar, sem justificativa, e não torna ilícito o tratamento anterior. Para categorias especiais, quando a base é o consentimento (sem outra exceção aplicável), ele precisa ser explícito. Em serviços da sociedade da informação oferecidos diretamente a crianças, a idade padrão para consentir é 16 anos, e cada país pode reduzir até 13. Abaixo dela, o consentimento é dado ou autorizado pelo responsável parental, com esforços razoáveis de verificação.

### Compatibilidade de finalidade (art. 6.º, n.º 4)

Para avaliar um novo uso: ligação entre a finalidade antiga e a nova, contexto da coleta, natureza dos dados, consequências para o titular e salvaguardas como criptografia ou pseudonimização. Arquivo de interesse público, pesquisa científica ou histórica e estatística, com as garantias do art. 89.º, não são considerados incompatíveis.

### Privacy by design: sete princípios

Proativo, não reativo (preventivo, não corretivo); privacidade como configuração padrão; privacidade incorporada ao projeto; funcionalidade total (soma positiva, não soma zero); segurança de ponta a ponta (da coleta à destruição segura); visibilidade e transparência; respeito pela privacidade do usuário. Benefício: evitar correções caras depois da implantação.

### Proteção por padrão (art. 25.º, n.º 2)

Por padrão, só os dados necessários a cada finalidade: abrange quantidade de dados, extensão do tratamento, prazo de conservação e acessibilidade. Dados não ficam acessíveis a número indeterminado de pessoas sem intervenção do titular (perfil restrito aos amigos). Certificação aprovada (art. 42.º) pode ajudar a demonstrar o art. 25.º.

### Transparência e prazos (arts. 12.º a 14.º)

Informação concisa, transparente, inteligível, em linguagem clara, em regra gratuita. Prazo de resposta: 1 mês, prorrogável por mais 2 (avisando dentro do primeiro mês). Recusa: informar motivos e possibilidade de reclamação e recurso judicial em até 1 mês. Dúvida sobre identidade: pedir informações adicionais. Coleta direta (art. 13.º) inclui prazo de conservação e, se houver decisão automatizada, a lógica envolvida; dados de terceiros (art. 14.º) incluem a origem, em até 1 mês após a obtenção ou no primeiro contato.

### Direitos do titular (arts. 15.º a 22.º)

Acesso (cópia + finalidades, destinatários, prazo, origem; primeira cópia grátis, extras com taxa razoável; sem prejudicar terceiros). Retificação (corrigir e completar). Apagamento (com exceções, como obrigação legal e defesa em processo). Limitação (guardar sem usar). Portabilidade (tratamento automatizado com base em consentimento ou contrato; envio direto se tecnicamente possível). Oposição (para marketing direto é absoluta). Não ficar sujeito a decisão exclusivamente automatizada com efeitos significativos.

### Reclamação e tutela

O titular pode reclamar à autoridade de controle (art. 77.º), sobretudo no Estado de residência habitual, de trabalho ou onde ocorreu a infração; propor ação judicial contra o controlador onde ele tem estabelecimento ou onde o titular reside (art. 79.º); e mandatar entidade sem fins lucrativos da área de proteção de dados (art. 80.º). Multas cabem à autoridade, não ao titular.

## Macetes para memorizar

### Princípios do art. 5.º

LI-FI-MI-EX-CO-IN-RE: Licitude/lealdade/transparência, Finalidade, Minimização, Exatidão, Conservação, Integridade/confidencialidade, Responsabilização.

### Seis bases legais

C-C-L-V-P-L: Consentimento, Contrato, Lei, Vital, Público, Legítimo. 'Interesse comercial do setor' não existe.

### Prazos que se confundem

Titular espera 1 mês (+2); autoridade espera 72 horas pela violação.

### Quanto x quanto tempo

Minimização = quanto; Conservação = quanto tempo; By default = quanto, quanto tempo e quem acessa.

### Proporcionalidade x subsidiariedade

Proporcionalidade: pesou demais? Subsidiariedade: tinha algo mais leve por baixo?

### Sete princípios de privacy by design

PRO-PA-PRO-SO-PON-VI-U: Proativo, Padrão, Projeto (incorporada), Soma positiva, Ponta a ponta, Visibilidade, Usuário.

### DPO obrigatório

P-M-S: Público, Monitoramento em grande escala, Sensíveis em grande escala.

### Direitos pelo verbo

Copiar = acesso; corrigir/completar = retificação; apagar = apagamento; congelar = limitação; levar = portabilidade; parar = oposição; 'máquina decidiu' = art. 22.

## Tabela de memorização: não confunda

| Quando é... | ...e quando é |
|---|---|
| **Minimização dos dados**<br>O problema é QUANTO e QUAL dado: newsletter que pede estado civil, renda e filhos. | **Limitação da conservação**<br>O problema é POR QUANTO TEMPO: placas de carro guardadas por anos só para planejar vagas. |
| **Proporcionalidade**<br>A medida é exagerada para o fim (registrar cada tecla para controlar pausas de café). | **Subsidiariedade**<br>Existe meio menos invasivo que atinge o mesmo fim (monitor no corredor em vez de câmera no banheiro). |
| **Direito à limitação**<br>Guardar mas não usar: titular contesta a exatidão enquanto se verifica, ou tratamento ilícito em que ele prefere não apagar. | **Direito ao apagamento**<br>Dados não são mais necessários, consentimento retirado sem outra base, oposição sem interesse prevalecente, tratamento ilícito, obrigação legal de apagar. |
| **Controlador**<br>Decide finalidades e meios; prova consentimento; responde pela conformidade. | **Operador**<br>Segue instruções documentadas; se decidir finalidade própria vira controlador desse tratamento. |

| | |
|---|---|
| **Proteção desde a concepção (by design)**<br>Privacidade embutida na arquitetura e pensada antes, evitando correções caras depois. | **Proteção por padrão (by default)**<br>Configuração de fábrica mais protetora: só o necessário em quantidade, extensão, prazo e acessibilidade. |
| **Interesse legítimo**<br>Empresa privada ponderando seu interesse com os direitos do titular (fraude, marketing direto). | **Interesse público**<br>Autoridade pública no exercício de funções (prefeitura organizando matrícula escolar). |
| **Direito de acesso**<br>Obter cópia dos dados e saber finalidades, destinatários, prazo; vale em geral. | **Direito à portabilidade**<br>Levar os dados que forneceu, em formato estruturado e de leitura automática, para outro controlador; só com tratamento automatizado baseado em consentimento ou contrato. |

## Números que caem

| Item | Valor |
|---|---|
| Peso do domínio na prova | **37,5% (15 de 40 perguntas): 2.1 Papéis 7,5%; 2.2 By design/by default 5%; 2.3 Bases legais 5%; 2.4 Direitos 12,5%; 2.5 Princípios 7,5%** |
| Bases legais do art. 6.º | **6** |
| Princípios de privacy by design | **7** |
| Prazo de resposta ao titular | **1 mês, prorrogável por mais 2 meses** |
| Informar dados obtidos de terceiros (art. 14.º) | **prazo razoável, no máximo 1 mês após a obtenção, ou no primeiro contato** |
| Idade para consentir em serviços da sociedade da informação | **16 anos; Estados podem reduzir até 13** |
| Dispensa do registro do art. 30.º | **menos de 250 pessoas, salvo risco, tratamento não ocasional, categorias especiais ou dados penais** |
| Cópia no direito de acesso | **primeira gratuita; adicionais com taxa razoável** |

## Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Prazo para responder ao titular é 72 horas sem prorrogação.
**Como não cair:** É 1 mês, prorrogável por mais 2. As 72 horas são da notificação de violação à autoridade.

⚠ **Alerta de prova:** Retirar o consentimento anula os tratamentos feitos antes.
**Como não cair:** O tratamento anterior continua lícito; o controlador para daí em diante e, sem outra base, apaga.

⚠ **Alerta de prova:** Caixa pré-marcada vale, porque o titular pode desmarcar.
**Como não cair:** Consentimento exige ato positivo e inequívoco; silêncio e caixa pré-marcada não valem, nem com política de privacidade.

⚠ **Alerta de prova:** Consentimento é livre porque o app é gratuito ou pode ser desinstalado.
**Como não cair:** Se o serviço depende de consentir com tratamento desnecessário a ele, o consentimento não é livre (art. 7.º, n.º 4).

⚠ **Alerta de prova:** Cabe portabilidade de dados tratados por interesse legítimo, obrigação legal ou interesse público, ou em papel.
**Como não cair:** Portabilidade exige tratamento automatizado com base em consentimento ou contrato.

⚠ **Alerta de prova:** Empresa com menos de 250 funcionários está sempre dispensada do registro do art. 30.º; tratar só dados de funcionários também dispensa.
**Como não cair:** A dispensa cai se houver risco, tratamento não ocasional, categorias especiais ou dados penais. Funcionários também são titulares.

⚠ **Alerta de prova:** O registro do art. 30.º é exclusivo do controlador, ou o contrato do art. 28.º dispensa o operador.
**Como não cair:** O operador também mantém registro das categorias de tratamento por controlador.

⚠ **Alerta de prova:** O registro lista nominalmente os titulares, é publicado no site ou enviado todo mês ao EDPB.
**Como não cair:** Registra categorias, por escrito, e fica disponível à autoridade quando ela pedir.

⚠ **Alerta de prova:** O DPO é obrigatório pelo número de funcionários ou por contratar operador de TI.
**Como não cair:** Critérios: organismo público, monitoramento regular e sistemático em grande escala, ou categorias especiais em grande escala.

⚠ **Alerta de prova:** O diretor de TI que decide os sistemas pode ser o DPO; ou o DPO precisa ser advogado.
**Como não cair:** O problema é conflito de interesses; não há exigência de ser advogado.

⚠ **Alerta de prova:** Prefeitura pode usar interesse legítimo, ou o consentimento das famílias, para a matrícula escolar.
**Como não cair:** Autoridade pública no exercício de funções usa interesse público (ou obrigação legal).

⚠ **Alerta de prova:** Paciente inconsciente: base é consentimento, contrato ou interesse legítimo do hospital.
**Como não cair:** Proteger a vida do titular ou de outra pessoa é interesse vital.

⚠ **Alerta de prova:** Pedido de apagamento com notas fiscais obrigatórias: recusar tudo ou apagar tudo.
**Como não cair:** Apaga o que não é exigido por lei e mantém as notas fiscais; a obrigação legal é exceção parcial.

⚠ **Alerta de prova:** Segunda cópia no acesso pode ser negada, ou cobrada com valor livre.
**Como não cair:** Primeira cópia é gratuita; cópias extras admitem taxa razoável pelos custos administrativos.

## Como cai na prova

📝 **Como cai:** Cenário de uso de dados + 'qual princípio é mais afetado/violado?'
**Como resolver:** Ache o defeito: pedir demais (minimização), guardar demais (conservação), esconder (lealdade e transparência), mudar a finalidade (limitação da finalidade), proteger mal (integridade e confidencialidade), dado errado (exatidão). Elimine 'exatidão' quando os dados podem estar corretos e elimine direitos (portabilidade, retificação), que não são princípios.

📝 **Como cai:** Cenário + 'qual base legal é a mais adequada?'
**Como resolver:** Procure a base mais específica: a lei obriga? (obrigação legal) É necessário para o contrato pedido pelo titular? (contrato) Há vida em risco? (interesses vitais) É autoridade pública em sua função? (interesse público) Senão, interesse legítimo com ponderação ou consentimento. Consentimento raramente é a resposta quando há base mais específica.

📝 **Como cai:** Titular pede algo + 'qual direito ele exerce?'
**Como resolver:** Traduza o verbo do pedido (copiar, corrigir, apagar, congelar, levar, parar, não ser decidido por máquina) e confira as condições: portabilidade só automatizado + consentimento/contrato; limitação quando quer guardar sem usar.

📝 **Como cai:** Papéis: quem é controlador, operador, conjunto, destinatário, DPO.
**Como resolver:** Pergunte quem decide finalidades e meios. Seguir instruções = operador; decidir junto = responsáveis conjuntos; usar para si = controlador. DPO aconselha e controla, nunca decide finalidades nem paga multas.

📝 **Como cai:** Qual princípio de privacy by design o cenário aplica.
**Como resolver:** Palavra-chave: antecipar falhas = proativo; ativado de fábrica = padrão; embutido na arquitetura = incorporado ao projeto; sem sacrificar usabilidade = soma positiva; da coleta à destruição = ponta a ponta; verificável = visibilidade; centrado no usuário = respeito ao usuário.

📝 **Como cai:** Prazos, gratuidade e procedimento de resposta ao titular.
**Como resolver:** 1 mês (+2), gratuito em regra, taxa razoável para cópias extras ou pedidos manifestamente infundados/excessivos, pedir confirmação de identidade em caso de dúvida, recusa com motivos e indicação de reclamação.

## Gatilhos do enunciado

| Se o enunciado trouxer... | Pense em |
|---|---|
| Formulário pede dados além do necessário | **Minimização.** |
| Guarda por anos o que só precisava contar | **Limitação da conservação.** |
| Notebook sem senha nem criptografia | **Integridade e confidencialidade.** |
| Coleta em segundo plano, sem informar ninguém | **Licitude, lealdade e transparência.** |
| Dados coletados para X usados para Y incompatível | **Limitação da finalidade.** |
| 'um meio menos invasivo resolveria' | **Subsidiariedade.** |
| Empresas decidem juntas finalidades e meios | **Responsáveis conjuntos (art. 26.º).** |
| Provedor que só armazena seguindo instruções | **Operador; se usar para si, vira controlador.** |
| 'como exige a lei', envio à receita | **Obrigação legal.** |
| Prevenção de fraude, marketing direto (considerando 47) | **Interesse legítimo.** |
| Titular contesta exatidão e pede que parem de usar | **Limitação do tratamento.** |
| 'não quero mais receber ofertas' | **Oposição ao marketing direto: absoluta, inclusive os perfis ligados a ele.** |
| IA decide sozinha, sem intervenção humana | **Art. 22.º: intervenção humana, ponto de vista, contestação.** |
| Perfil novo restrito aos amigos, usuário decide abrir | **Proteção por padrão (by default).** |

### 🎯 Se você lembrar de só uma coisa deste capítulo...

- Controlador decide finalidades e meios e precisa cumprir E demonstrar (accountability).
- Consentimento: ato positivo, destacado, livre (não condicionado), retirável tão fácil quanto dado, sem efeito retroativo.
- Titular: 1 mês (+2), gratuito em regra; 72 horas é só para violação.
- Portabilidade só com tratamento automatizado e base em consentimento ou contrato.
- Oposição ao marketing direto é absoluta; para interesse legítimo, o controlador só continua com razões imperiosas e legítimas ou para defender direitos em processo.

## Essenciais para a prova (checklist)

☐ Sei distinguir controlador, operador, responsáveis conjuntos e destinatário em um cenário.

☐ Sei o conteúdo do contrato do art. 28.º e a regra do suboperador.

☐ Sei o que entra no registro do art. 30.º, que o operador também registra e quando a dispensa de menos de 250 não vale.

☐ Sei quando o DPO é obrigatório, suas tarefas e as garantias de independência.

☐ Sei listar os princípios do art. 5.º e apontar qual é violado em um cenário.

☐ Sei diferenciar proporcionalidade de subsidiariedade.

☐ Sei listar as seis bases legais e escolher a mais adequada em cada cenário.

☐ Sei os requisitos do consentimento válido, a idade de 16 (até 13) e o consentimento explícito para dados especiais.

☐ Sei os sete princípios de privacy by design e os quatro aspectos do by default.

☐ Sei cada direito do titular, suas condições, exceções e o prazo de 1 mês (+2).

## Questões de revisão do capítulo

R3.1 · Princípios do Tratamento de Dados

**Uma pessoa não quer mais receber ofertas de uma loja em que comprou há anos. Qual direito garante que o marketing direto pare?**

A. Direito à portabilidade
B. Direito de oposição
C. Direito de acesso
D. Direito de retificação

R3.2 · Princípios do Tratamento de Dados

**Um adulto pede o apagamento de dados que forneceu a uma rede social quando era criança. O que o GDPR prevê?**

A. Os dados passam a ser públicos quando ele faz 18 anos
B. Nada, pois os dados foram fornecidos de forma voluntária
C. Os dados só podem ser apagados com autorização dos pais
D. Ele pode pedir o apagamento, com proteção reforçada

R3.3 · Princípios do Tratamento de Dados

**Uma empresa quer registrar cada tecla digitada pelos funcionários apenas para controlar as pausas para café. Qual princípio questiona essa medida?**

A. Exatidão
B. Portabilidade dos dados
C. Retificação
D. Proporcionalidade

R3.4 · Princípios do Tratamento de Dados

**Uma pessoa liga pedindo acesso a dados de um cliente, mas o controlador tem dúvidas sobre quem ela é. O que o GDPR permite?**

A. Recusar o pedido sem responder à pessoa
B. Pedir informações adicionais para confirmar a identidade
C. Cobrar uma taxa alta para desencorajar o pedido
D. Entregar os dados imediatamente para evitar reclamação

## Respostas comentadas

### R3.1. B) Direito de oposição

Por quê: Quando o titular se opõe ao marketing direto, inclusive a perfis ligados a ele, os dados deixam de ser tratados para essa finalidade.

✗ A) Incorreta. Serve para levar os dados.
✗ C) Incorreta. Serve para obter os dados.
✗ D) Incorreta. Serve para corrigir dados.

> **Dica de prova:** Parar marketing direto: oposição.

### R3.2. D) Ele pode pedir o apagamento, com proteção reforçada

Por quê: O considerando 65 destaca esse direito quando o consentimento foi dado em criança, sem plena consciência dos riscos.

✗ A) Incorreta. Não é o previsto.
✗ B) Incorreta. Há direito ao apagamento.
✗ C) Incorreta. Ele já é adulto.

> **Dica de prova:** Dados dados na infância: apagamento reforçado.

### R3.3. D) Proporcionalidade

Por quê: A interferência na privacidade deve ser proporcional à finalidade; registrar teclas para medir pausas é excessivo.

✗ A) Incorreta. Os registros podem ser exatos.
✗ B) Incorreta. Não é princípio do tratamento.
✗ C) Incorreta. É um direito, não o princípio em jogo.

> **Dica de prova:** Medida exagerada para o fim: proporcionalidade.

### R3.4. B) Pedir informações adicionais para confirmar a identidade

Por quê: Verificar a identidade evita entregar dados a quem não é o titular, o que seria uma violação de confidencialidade.

✗ A) Incorreta. Deve responder.
✗ C) Incorreta. Não é o previsto.
✗ D) Incorreta. Pode gerar violação de dados.

> **Dica de prova:** Dúvida sobre identidade: pedir confirmação.

04

CAPÍTULO 4 · 10% DA PROVA

# Prática do Tratamento de Dados

Domínio pequeno (10%, cerca de 4 perguntas), mas com perguntas bem previsíveis: cookies e Diretiva ePrivacy, ciclo de vida dos dados (DLM) e governança, definição de perfis e uso de inteligência artificial com dados pessoais. Na prova, o cenário costuma trazer um site, um banner de cookies, uma empresa treinando IA ou um dado no fim do prazo de retenção. Onde mais erro: achar que todo cookie exige consentimento, que dados públicos na internet estão livres para treinar IA, e que a oposição ao marketing não alcança a definição de perfis.

**Neste capítulo**

18 tópicos-chave · 14 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

## Tópicos-chave

### Definição de perfis (profiling, art. 4.º, n.º 4)

Tratamento automatizado para avaliar aspectos pessoais: analisar ou prever desempenho, situação econômica, saúde, preferências, comportamento ou localização. Cadastro manual em fichas, backup ou eliminação não são profiling.

### Cookie

Pequeno arquivo que o site guarda no navegador do usuário. Pode lembrar login e carrinho, medir audiência ou rastrear para publicidade. Não é senha, antivírus nem contrato.

### Cookie de sessão x persistente

O de sessão é apagado ao fechar o navegador. O persistente fica no dispositivo até expirar ou ser apagado, servindo para lembrar preferências ou login; pode conter identificadores pessoais.

### Cookie primário x de terceiros

Primário é do próprio site visitado. De terceiros vem de outro domínio, como uma rede de anúncios, e permite rastrear o usuário entre sites; por isso exige consentimento pela Diretiva ePrivacy. 'Sessão' e 'persistente' falam de duração, não de origem.

### Cookie estritamente necessário

Cookie indispensável ao serviço pedido pelo usuário, como o que guarda o carrinho de compras, dispensa consentimento. Cookies de publicidade e de análise de audiência, em regra, exigem.

### Consentimento prévio para cookies

Cookies não essenciais só podem ser gravados depois do consentimento. Carregá-los antes viola a Diretiva ePrivacy, mesmo que o banner apareça em seguida. Aviso no rodapé não substitui consentimento, e não é preciso autorização da autoridade.

### Recusar tão fácil quanto aceitar

Pela orientação do EDPB, a opção de recusar cookies não essenciais deve ser tão fácil quanto aceitar. Se aceitar é um clique e recusar exige vários (ou fica escondido numa segunda página), o consentimento não é livre.

### E-mail de marketing para clientes atuais (ePrivacy)

Para quem já comprou e para produtos semelhantes, o envio pode ser feito se o cliente puder se opor de forma fácil e gratuita, na coleta e em cada mensagem. Não exige carta registrada nem registro na autoridade.

### Oposição ao marketing direto

É absoluta e abrange a definição de perfis ligada a esse marketing (art. 21.º, n.º 2 e 3). O direito deve ser apresentado de forma explícita, clara e separada de outras informações, no máximo na primeira comunicação (art. 21.º, n.º 4).

### Gestão do ciclo de vida dos dados (DLM)

Gerir os dados fase a fase: coleta, armazenamento, uso, compartilhamento, arquivamento e destruição, com controles e responsáveis em cada uma. Ajuda a saber onde estão os dados, quem usa, por quanto tempo guardar e como eliminar. Não dispensa base legal, não substitui a DPIA e não transfere a responsabilidade do controlador para a TI.

### Arquivamento

Guarda dados que não são mais usados no dia a dia, mas precisam ser mantidos por obrigação legal ou outra razão legítima, com acesso restrito até o fim do prazo. Arquivo não é para consulta livre nem para novas campanhas.

### Fim do prazo de retenção

Quando o prazo termina, o dado deve ser destruído com segurança ou anonimizado. Mandar para pasta compartilhada, fazer backup extra 'por precaução' ou vender a parceiros contraria o DLM.

### Classificação dos dados (governança)

Classificar conforme a sensibilidade permite definir quem acessa, como proteger, por quanto tempo guardar e como eliminar cada tipo de dado. Pasta aberta, pendrives e apagar logs prejudicam a governança.

### IA: novo uso = nova atividade de tratamento

Usar IA sobre dados já coletados costuma ser nova atividade: exige base legal, transparência (informar os titulares) e, conforme o risco, DPIA. Não é preciso apagar tudo o que foi coletado.

### IA generativa pública com dados de clientes

Colar dados de clientes numa ferramenta pública cria risco de divulgação a terceiros sem base legal. Resposta organizacional: política de uso de IA, ferramentas aprovadas com contrato de operador e treinamento dos funcionários.

### Dados públicos no treino de IA

Estar disponível na internet não torna o dado livre: o treino precisa de base legal, transparência e respeito aos direitos. Treinar 'por ser pesquisa interna' também exige base legal.

### Boas práticas no treino de IA

Minimizar e pseudonimizar os dados de treino; definir finalidade e base legal; informar os titulares; fazer DPIA quando houver alto risco (avaliação de candidatos em grande escala); revisar vieses. Usar todos os campos 'por garantia' ou guardar por tempo indeterminado viola minimização e conservação.

### Viés, explicabilidade e revisão humana

Modelo que recusa crédito a um bairro sem justificativa indica tratamento desleal que pode gerar discriminação. Modelos opacos dificultam explicar a lógica da decisão, que o titular tem direito de conhecer. A intervenção humana deve ser real, com autoridade e competência para mudar a decisão, e não mera confirmação.

## Macetes para memorizar

### 💡 Tipos de cookie

Sessão x persistente = QUANTO TEMPO; primário x terceiros = DE QUEM; necessário x não essencial = PRECISA DE CONSENTIMENTO?

### 💡 Banner de cookies

Antes, livre e simétrico: pergunta antes de gravar, recusar com o mesmo esforço de aceitar.

### 💡 Fases do DLM

Coleta, Armazena, Usa, Compartilha, Arquiva, Destrói: 'CAUCAD'.

### 💡 Fim da retenção

Prazo acabou: tritura ou anonimiza, nunca 'guarda por precaução'.

**IA e GDPR**

IA BOA: Base legal, Oriente o titular (transparência), Avalie impacto (DPIA); e no treino, menos campos e pseudônimos.

**Oposição ao marketing**

Disse não ao marketing, morreu também o perfil.

## Tabela de memorização: não confunda

| Quando é... | ...e quando é |
|---|---|
| **Cookie de sessão**<br>Some ao fechar o navegador. | **Cookie persistente**<br>Fica até expirar ou ser apagado; lembra preferências ou login. |
| **Cookie primário**<br>Gravado pelo próprio site visitado. | **Cookie de terceiros**<br>Vem de outro domínio (rede de anúncios) e rastreia entre sites; exige consentimento. |
| **Cookie estritamente necessário**<br>Carrinho de compras pedido pelo usuário: dispensa consentimento. | **Cookie de publicidade ou análise**<br>Exige consentimento prévio, antes de gravar, com recusa tão fácil quanto aceitar. |
| **Arquivamento**<br>Dado fora do uso diário que ainda deve ser mantido: acesso restrito até o fim do prazo. | **Destruição ou anonimização**<br>Prazo de retenção encerrado: eliminar com segurança ou anonimizar. |
| **Oposição ao marketing direto**<br>Absoluta: para o envio e o profiling ligado ao marketing, sem decisão judicial. | **Oposição a tratamento por interesse legítimo em geral**<br>O controlador para, salvo razões imperiosas e legítimas que prevaleçam ou defesa de direitos em processo. |

## Números que caem

| Item | Valor |
|---|---|
| Peso do domínio na prova | **10% (4 de 40 perguntas): 3.1 Governança de dados 2,5%; 3.2 Tratamento online 2,5%; 3.3 Uso de IA 5%** |

## Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Todo cookie exige consentimento prévio.
**Como não cair:** Os estritamente necessários ao serviço pedido (carrinho) são exceção.

⚠ **Alerta de prova:** Cookies de sessão nunca guardam dados.
**Como não cair:** Podem guardar dados; 'sessão' fala só de duração.

⚠ **Alerta de prova:** Cookie persistente é apagado ao fechar o navegador.
**Como não cair:** Esse é o de sessão; o persistente sobrevive até expirar ou ser apagado.

⚠ **Alerta de prova:** Basta um aviso no rodapé para cookies de publicidade.
**Como não cair:** Aviso não substitui consentimento prévio.

⚠ **Alerta de prova:** O consentimento para cookies pode vir depois da compra, de 30 dias ou em campanha anual.
**Como não cair:** Deve vir antes de gravar os cookies no navegador.

⚠ **Alerta de prova:** A recusa pode ficar numa segunda página de configurações ou só para cadastrados.
**Como não cair:** Recusar deve ser tão fácil quanto aceitar.

⚠ **Alerta de prova:** Após a oposição, o profiling pode continuar porque só o envio de ofertas é afetado.
**Como não cair:** A oposição ao marketing direto inclui a definição de perfis ligada a ele.

⚠ **Alerta de prova:** O direito de oposição pode ser informado quando o titular perguntar, em letras miúdas ou na décima mensagem.
**Como não cair:** Explícito, separado e, no máximo, no primeiro contato.

⚠ **Alerta de prova:** Dados publicados na internet estão livres do GDPR para treinar IA.
**Como não cair:** Continuam sendo dados pessoais: exigem base legal e transparência.

⚠ **Alerta de prova:** Treinar IA com todos os campos, por garantia, e guardar os dados de treino indefinidamente.
**Como não cair:** Minimizar e pseudonimizar; respeitar a limitação da conservação.

⚠ **Alerta de prova:** No fim do prazo, fazer um backup extra por precaução.
**Como não cair:** Fim do prazo = destruição segura ou anonimização; backup extra prolonga a retenção sem motivo.

⚠ **Alerta de prova:** DLM dispensa base legal, substitui a DPIA ou passa a responsabilidade para a TI.
**Como não cair:** DLM organiza fases e controles; base legal, DPIA e responsabilidade do controlador continuam.

⚠ **Alerta de prova:** Para cumprir o GDPR com IA, esconder do cliente que há IA ou retirar o direito de contestar.
**Como não cair:** Transparência, revisão humana real e direito de contestar são exigidos.

⚠ **Alerta de prova:** Para usar IA sobre doadores, a ONG deve apagar tudo ou parar de guardar recibos fiscais.
**Como não cair:** O essencial é informar os titulares sobre o novo tratamento; a obrigação fiscal continua.

## Como cai na prova

📝 **Como cai:** Descrição de um cookie + 'como se chama?' ou 'precisa de consentimento?'
**Como resolver:** Classifique por duração (sessão/persistente), origem (primário/terceiros) e necessidade. Só o estritamente necessário ao serviço pedido dispensa consentimento.

📝 **Como cai:** 'Quando/como o site deve obter o consentimento para cookies?'
**Como resolver:** Antes de gravar, com recusa tão fácil quanto aceitar. Descarte aviso no rodapé, consentimento posterior e recusa escondida.

📝 **Como cai:** Empresa usa ou treina IA com dados pessoais + 'qual o desafio/medida mais importante?'
**Como resolver:** Procure a alternativa de proteção de dados (base legal, transparência, DPIA, minimizar/pseudonimizar, revisão humana real, viés). Descarte custos, energia, licenças, velocidade ou tradução, que não são temas do GDPR.

📝 **Como cai:** Fase do ciclo de vida + 'o que se espera da organização?'
**Como resolver:** Arquivamento = acesso restrito até o fim do prazo; fim do prazo = destruir ou anonimizar; governança = classificar por sensibilidade.

📝 **Como cai:** Marketing direto + oposição ou e-mail para clientes.
**Como resolver:** Oposição absoluta e inclui profiling; informar no primeiro contato de forma separada; para clientes atuais, recusa fácil e gratuita em cada mensagem.

## Gatilhos do enunciado

| Se o enunciado trouxer... | Pense em |
|---|---|
| Cookie que só guarda o carrinho de compras | **Estritamente necessário: sem consentimento.** |
| Cookie de rede de anúncios de outro domínio | **Cookie de terceiros: consentimento.** |
| 'fica no dispositivo até expirar' | **Cookie persistente.** |

| | |
|---|---|
| Banner aparece depois que os cookies já foram carregados | **Violação: consentimento tem de ser antes.** |
| Aceitar com um clique, recusar com vários | **Consentimento não livre: recusar tão fácil quanto aceitar.** |
| E-mail de ofertas de produtos semelhantes a quem já comprou | **Opção simples de recusar em cada mensagem (ePrivacy).** |
| 'avaliar aspectos pessoais automaticamente', prever comportamento | **Definição de perfis.** |
| Titular se opõe a perfis de consumo para ofertas | **Oposição absoluta: param o marketing e o profiling ligado a ele.** |
| 'da coleta à eliminação, fase a fase' | **DLM.** |
| Prazo de retenção terminou | **Destruir com segurança ou anonimizar.** |
| Funcionários colam dados em ferramenta pública de IA | **Divulgação a terceiros sem base legal; política de IA, ferramenta aprovada, treinamento.** |
| IA avalia candidatos em grande escala | **DPIA antes do lançamento.** |
| IA recusa mais pedidos de um grupo sem justificativa | **Tratamento desleal, discriminação, viés.** |
| IA sugere decisões que afetam o cliente | **Revisão humana real antes da decisão final.** |

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Só o cookie estritamente necessário dispensa consentimento; os demais exigem consentimento antes de gravar.
- Recusar cookies deve ser tão fácil quanto aceitar.
- Dado público na internet não é livre para treinar IA: precisa de base legal e transparência.
- Fim do prazo de retenção: destruir com segurança ou anonimizar.
- Oposição ao marketing direto derruba também o profiling ligado a ele.

## Essenciais para a prova (checklist)

- ☐ Sei definir profiling e diferenciá-lo de cadastro manual, backup e eliminação.
- ☐ Sei classificar cookies por duração, origem e necessidade.
- ☐ Sei quando o cookie exige consentimento e que ele deve ser prévio.
- ☐ Sei a regra de recusa tão fácil quanto aceitar.
- ☐ Sei a regra de e-mail de ofertas para clientes atuais na Diretiva ePrivacy.
- ☐ Sei as fases do DLM e o que fazer no arquivamento e no fim do prazo.

- ☐ Sei os riscos de colar dados em IA pública e as medidas organizacionais.
- ☐ Sei as boas práticas de treino de IA (base legal, transparência, minimizar, pseudonimizar, DPIA, viés, revisão humana real).

## Questões de revisão do capítulo

R4.1 · Prática do Tratamento de Dados

**Uma empresa cria perfis de consumo para personalizar ofertas. O titular se opõe. O que acontece com a definição de perfis?**

A. Deve parar, pois a oposição ao marketing inclui o profiling
B. Deve parar só depois de uma decisão judicial definitiva
C. Pode continuar, pois só o envio de ofertas é afetado
D. Pode continuar se a empresa pagar uma taxa ao titular

R4.2 · Prática do Tratamento de Dados

**Qual é o objetivo da gestão do ciclo de vida dos dados (DLM)?**

A. Eliminar a necessidade de base legal para tratar dados
B. Guardar todos os dados pelo maior tempo possível
C. Gerir os dados da coleta à eliminação, fase a fase
D. Substituir a avaliação de impacto sobre a proteção de dados

R4.3 · Prática do Tratamento de Dados

**Na fase de arquivamento do ciclo de vida dos dados, o que se espera da organização?**

A. Liberar o arquivo para consulta livre dos funcionários
B. Manter o arquivo sem prazo, sem revisar a retenção
C. Usar os dados arquivados em novas campanhas de vendas
D. Guardar os dados com acesso restrito até o fim do prazo

R4.4 · Prática do Tratamento de Dados

**Funcionários colam dados de clientes em uma ferramenta pública de IA generativa para resumir casos. Qual risco de GDPR isso cria?**

A. Aumento do tempo de resposta aos clientes
B. Redução do custo das licenças de software
C. Melhoria da qualidade dos resumos
D. Divulgação de dados a terceiros sem base legal

### Respostas comentadas

### R4.1. A) Deve parar, pois a oposição ao marketing inclui o profiling

Por quê: Para marketing direto, a oposição é absoluta e abrange a definição de perfis relacionada a esse marketing.

✗ B) Incorreta. A oposição tem efeito direto.
✗ C) Incorreta. O profiling ligado ao marketing também para.
✗ D) Incorreta. Não é o previsto.

> **Dica de prova:** Oposição ao marketing inclui profiling.

### R4.2. C) Gerir os dados da coleta à eliminação, fase a fase

Por quê: O DLM mapeia as fases (coleta, armazenamento, uso, compartilhamento, arquivamento e destruição) e define controles e responsáveis em cada uma.

✗ A) Incorreta. A base legal continua obrigatória.
✗ B) Incorreta. Contraria a limitação da conservação.
✗ D) Incorreta. Não substitui a DPIA.

> **Dica de prova:** DLM: gerir o dado da coleta ao descarte.

### R4.3. D) Guardar os dados com acesso restrito até o fim do prazo

Por quê: O arquivamento guarda dados que não são mais usados no dia a dia, mas que precisam ser mantidos por obrigação legal ou outra razão legítima.

✗ A) Incorreta. Aumenta o risco.
✗ B) Incorreta. Contraria a conservação.
✗ C) Incorreta. Seria nova finalidade.

> **Dica de prova:** Arquivar: acesso restrito até eliminar.

### R4.4. D) Divulgação de dados a terceiros sem base legal

Por quê: A empresa deve ter política de uso de IA, ferramentas aprovadas com contrato de operador e treinamento dos funcionários.

✗ A) Incorreta. Não é risco de proteção de dados.
✗ B) Incorreta. Não é risco.
✗ C) Incorreta. Não é risco.

> **Dica de prova:** IA pública com dados de clientes: divulgação indevida.

05

CAPÍTULO 5 · 15% DA PROVA

# Transferências Internacionais de Dados Pessoais

Vale 15% da prova, cerca de 6 perguntas. Preciso saber o mapa completo: dentro do EEE os dados circulam livremente; para fora (países terceiros e organizações internacionais) vale o capítulo V, na ordem adequação (art. 45.º), garantias adequadas (art. 46.º: SCC, BCR, códigos, certificações) e, por último, derrogações (art. 49.º). Caem muito a linha do tempo UE-EUA (Safe Harbor, Privacy Shield, Data Privacy Framework), quem adota as SCC e quem aprova as BCR. Onde mais erro: achar que Reino Unido ou Suíça estão no EEE, que o DPF cobre qualquer empresa americana e que Schrems II proibiu as SCC.

**Neste capítulo**

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

## Tópicos-chave

### Espaço Econômico Europeu (EEE)

UE + Islândia, Liechtenstein e Noruega. Todos aplicam o GDPR, então os dados circulam livremente: enviar de Portugal para a filial na Alemanha não exige nada além do cumprimento normal do GDPR. Reino Unido, Suíça e Turquia não integram o EEE.

### Livre circulação na União (art. 1.º, n.º 3)

Um Estado-membro não pode restringir o envio de dados para outro Estado-membro por motivos de proteção de dados, porque todos aplicam o mesmo regulamento.

### Capítulo V (art. 44.º)

As regras de transferência valem para países terceiros e organizações internacionais (como uma agência da ONU), inclusive transferências ulteriores. Não se aplicam a envio para operador em outro país do EEE, filial no mesmo país ou servidor no mesmo prédio.

### Decisão de adequação (art. 45.º)

A Comissão Europeia reconhece que o país oferece proteção essencialmente equivalente; as transferências passam a dispensar garantias adicionais e autorização específica, como se fosse dentro do EEE. Não muda o status do país nem se presume.

### Critérios da adequação (art. 45.º, n.º 2)

Estado de direito e autoridade de controle independente, respeito aos direitos humanos, legislação sobre acesso de autoridades públicas e compromissos internacionais. Idioma, tamanho do mercado ou número de empresas europeias não contam.

### Revisão da adequação (art. 45.º, n.º 3)

Pelo menos a cada quatro anos. A Comissão acompanha a evolução no país e pode revogar, alterar ou suspender a decisão.

### Países com adequação

Exemplos: Japão, Suíça, Canadá (organizações comerciais), Israel, Nova Zelândia, Coreia do Sul e Reino Unido (após o Brexit, por decisão de adequação). Rússia, Índia e China não têm.

### Cláusulas contratuais-padrão (SCC)

Garantia adequada do art. 46.º, n.º 2, adotada pela Comissão Europeia (uma autoridade de controle também pode adotar, depois aprovadas pela Comissão). Dispensam autorização específica. É o caminho típico para fornecedor fora do EEE, inclusive empresa americana não certificada no DPF. Pode acrescentar cláusulas que não contradigam as padrão; alterar o texto tira a validade (considerando 109).

### Regras corporativas vinculantes (BCR, art. 47.º)

Regras de proteção de dados de um grupo empresarial ou de empresas em atividade econômica conjunta, juridicamente vinculantes para todas as entidades e funcionários, aprovadas pela autoridade de controle competente pelo mecanismo de coerência. Vantagem: transferências dentro do grupo sem contrato para cada envio. Não valem para empresas independentes nem para vender dados fora do grupo.

### Conteúdo das BCR (art. 47.º, n.º 2)

Estrutura do grupo, transferências, princípios aplicados, direitos dos titulares e meios de exercê-los, procedimentos de reclamação, verificação da conformidade, formação do pessoal, cooperação com a autoridade, papel do DPO e responsabilidade: a entidade estabelecida num Estado-membro responde por violações de entidade do grupo fora da União, salvo se provar que o fato não lhe é imputável.

### BCR para operadores + contrato

Existem BCR para controladores e para operadores. Um operador com BCR aprovadas ainda precisa de contrato do art. 28.º com o controlador, que define instruções e obrigações e torna as BCR vinculativas no serviço.

### Códigos de conduta e certificações

Aprovados, podem servir de garantia adequada, desde que acompanhados de compromisso vinculante do importador de aplicar as garantias (art. 46.º, n.º 2, alínea e).

### Cláusulas ad hoc (art. 46.º, n.º 3)

Cláusulas contratuais negociadas entre as partes exigem autorização específica da autoridade de controle. SCC, BCR já aprovadas, códigos, certificações e adequação não exigem.

### Derrogações (art. 49.º)

Sem adequação nem garantias, exceções para situações específicas, usadas de forma restritiva: consentimento explícito do titular após informado dos riscos; necessidade para executar contrato com o titular (reserva de hotel na Tailândia, transferência ocasional); importantes razões de interesse público (troca entre autoridades fiscais, aduaneiras, de saúde pública); defesa de um direito em processo judicial. Custo, porte da empresa ou interesse comercial não são derrogações.

### Ordens de autoridades de país terceiro (art. 48.º)

Decisão de tribunal ou autoridade estrangeira só fundamenta transferência se baseada em acordo internacional, como tratado de assistência jurídica mútua. Não é reconhecida automaticamente.

### Linha do tempo UE-EUA

Safe Harbor invalidado em 2015 (Schrems I); Privacy Shield invalidado em julho de 2020 (Schrems II); EU-U.S. Data Privacy Framework em 2023, vigente. O GDPR continua em vigor; Schrems II não revogou nada além do Privacy Shield.

### EU-U.S. Data Privacy Framework (DPF)

A empresa americana adere por autocertificação junto ao Departamento de Comércio dos EUA, comprometendo-se com os princípios do DPF; a lista é pública. A decisão de adequação vale só para organizações certificadas. O DPF limitou o acesso de agências de inteligência ao necessário e proporcional e criou o Tribunal de Revisão de Proteção de Dados (Data Protection Review Court).

### SCC depois de Schrems II

As SCC seguiram válidas, mas o exportador deve avaliar a legislação do país de destino e, se preciso, adotar medidas complementares: criptografia forte com chaves mantidas no EEE, pseudonimização e controles contratuais adicionais. Assinar e deixar de acompanhar não basta.

## Macetes para memorizar

### 💡 Ordem dos mecanismos

A-G-D: Adequação (45), Garantias (46), Derrogações (49). Tenta na ordem; derrogação é o último recurso.

### 💡 Países do EEE fora da UE

I-L-N: Islândia, Liechtenstein, Noruega. 'Reino Unido saiu, Suíça nunca entrou.'

### 💡 SCC x BCR

SCC: Standard da Comissão (Comissão adota). BCR: Bloco do grupo, autoridade aprova.

### 💡 Linha do tempo UE-EUA

Safe (2015) cai com Schrems I; Shield (2020) cai com Schrems II; Framework (2023) está de pé. S-S-F, em ordem cronológica.

### 💡 Revisão da adequação

Adequação tem 'Copa do Mundo': revisão a cada 4 anos.

### 💡 Cláusulas-padrão

Pode somar, não pode mexer.

### 💡 DPF

No DPF a empresa se inscreve sozinha: autocertificação no Departamento de Comércio, e só quem está na lista é coberto.

## Tabela de memorização: não confunda

| Quando é... | ...e quando é |
|---|---|
| **Cláusulas contratuais-padrão (SCC)**<br>Contrato com qualquer importador fora do EEE; adotadas pela Comissão; texto não pode ser alterado. | **Regras corporativas vinculantes (BCR)**<br>Transferências dentro do mesmo grupo empresarial; aprovadas pela autoridade de controle competente pelo mecanismo de coerência. |

| | |
|---|---|
| **Decisão de adequação (art. 45.º)**<br>O país de destino (ou o DPF, para empresas certificadas) foi reconhecido pela Comissão: sem garantias extras. | **Garantias adequadas (art. 46.º)**<br>Destino sem adequação: SCC, BCR, códigos ou certificações com compromisso vinculante. |
| **Garantias adequadas (art. 46.º)**<br>Base estável e regular para transferências. | **Derrogações (art. 49.º)**<br>Exceção restritiva quando não há adequação nem garantias: consentimento explícito informado, contrato com o titular, interesse público importante, defesa em processo. |
| **Schrems I (2015)**<br>Invalidou o Safe Harbor. | **Schrems II (julho de 2020)**<br>Invalidou o Privacy Shield e exigiu avaliação do destino para quem usa SCC. |
| **Empresa dos EUA certificada no DPF**<br>Transferência apoiada na decisão de adequação do DPF. | **Empresa dos EUA não certificada**<br>Precisa de garantia do art. 46.º (como SCC) ou derrogação do art. 49.º. |
| **SCC da Comissão**<br>Não exigem autorização específica; pode acrescentar cláusulas sem contradizer. | **Cláusulas ad hoc**<br>Negociadas entre as partes: exigem autorização específica da autoridade de controle. |
| **Envio dentro do EEE**<br>Nada além do cumprimento normal do GDPR. | **Envio para país terceiro ou organização internacional**<br>Capítulo V: adequação, garantias adequadas ou derrogação. |

## Números que caem

| Item | Valor |
|---|---|
| Peso do domínio na prova | **15% (6 de 40 perguntas): 4.1 Transferências dentro do EEE 10%; 4.2 Transferências para fora do EEE 5%** |
| Revisão da decisão de adequação | **pelo menos a cada 4 anos (art. 45.º, n.º 3)** |
| Schrems I | **2015, invalidou o Safe Harbor** |
| Schrems II | **julho de 2020, invalidou o Privacy Shield** |
| EU-U.S. Data Privacy Framework | **2023, vigente** |
| Países do EEE fora da UE | **3: Islândia, Liechtenstein, Noruega** |

## Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Depois do Brexit, o Reino Unido continua no EEE.
**Como não cair:** Não integra o EEE; as transferências se apoiam numa decisão de adequação.

⚠ **Alerta de prova:** Suíça (ou Turquia) integra o EEE.
**Como não cair:** EEE não-UE = só Islândia, Liechtenstein e Noruega. A Suíça tem adequação, mas não é EEE.

⚠ **Alerta de prova:** O DPF vale para todas as empresas dos EUA.
**Como não cair:** Só para organizações autocertificadas no Departamento de Comércio.

⚠ **Alerta de prova:** O Privacy Shield ainda está em vigor.
**Como não cair:** Foi invalidado em 2020 (Schrems II); o vigente é o DPF, de 2023.

⚠ **Alerta de prova:** Schrems II proibiu as SCC em todo o mundo, ou criou o DPF.
**Como não cair:** As SCC seguiram válidas com avaliação do destino; o DPF veio depois, em 2023.

⚠ **Alerta de prova:** BCR são contratos-padrão publicados pela Comissão para uso geral.
**Como não cair:** Isso são as SCC. BCR são regras internas do grupo aprovadas pela autoridade.

⚠ **Alerta de prova:** BCR são aprovadas pela Comissão por decisão de adequação, ou pelo próprio conselho do grupo.
**Como não cair:** Aprovação da autoridade de controle competente, pelo mecanismo de coerência.

⚠ **Alerta de prova:** BCR servem para empresas independentes mandarem dados a parceiros eventuais.
**Como não cair:** Valem dentro de um grupo empresarial ou de empresas em atividade econômica conjunta.

⚠ **Alerta de prova:** O contrato só pode ter as cláusulas-padrão, ou pode alterar o texto delas.
**Como não cair:** Pode acrescentar cláusulas que não contradigam; alterar o texto tira a validade.

⚠ **Alerta de prova:** Código de conduta aprovado dispensa qualquer outra medida.
**Como não cair:** Exige compromisso vinculante do importador.

⚠ **Alerta de prova:** A adequação da Tailândia é presumida, ou o interesse comercial do site justifica o envio da reserva.
**Como não cair:** Adequação não se presume; a base é a derrogação de necessidade para o contrato com o titular.

⚠ **Alerta de prova:** Consentimento implícito dos contribuintes ou consentimento presumido da parte contrária.
**Como não cair:** Não existe; as derrogações são interesse público importante e defesa de direito em processo.

⚠ **Alerta de prova:** Ordem de tribunal estrangeiro deve ser cumprida sem demora.
**Como não cair:** Só vale com base em acordo internacional (art. 48.º).

⚠ **Alerta de prova:** Com adequação, cada transferência precisa de autorização prévia; ou a decisão é revisada a cada vinte anos.
**Como não cair:** Adequação dispensa autorização; revisão pelo menos a cada quatro anos.

## Como cai na prova

📝 **Como cai:** 'Em que se baseia/qual mecanismo torna lícita a transferência para o país X?'
**Como resolver:** 1) Destino está no EEE? Nada extra. 2) Tem adequação (ou empresa certificada no DPF)? Adequação. 3) Não tem? Garantias do art. 46.º (SCC para fornecedor; BCR para o próprio grupo). 4) Só em situação específica, derrogação do art. 49.º.

📝 **Como cai:** 'Quem adota/aprova/autoriza?'
**Como resolver:** SCC: Comissão adota. BCR: autoridade competente aprova pelo mecanismo de coerência. Cláusulas ad hoc: autoridade autoriza. Adequação: Comissão decide, e revisa a cada 4 anos.

📝 **Como cai:** Histórico Schrems e DPF.
**Como resolver:** Associe o caso ao acordo derrubado: I = Safe Harbor (2015); II = Privacy Shield (2020). DPF (2023) é adequação só para autocertificados e criou o Data Protection Review Court.

📝 **Como cai:** Cenário sem adequação e sem garantia + 'qual derrogação se aplica?'
**Como resolver:** Identifique a necessidade: contrato pedido pelo titular, interesse público importante, defesa em processo ou consentimento explícito após informar os riscos. Descarte custo, porte, interesse comercial e consentimento implícito ou presumido.

📝 **Como cai:** Detalhes das BCR (conteúdo, quem pode usar, quem responde).
**Como resolver:** Grupo ou atividade econômica conjunta; vinculantes para todos; direitos dos titulares, reclamações, verificação, formação, cooperação; a entidade na UE responde pelas falhas de entidade fora da União.

## Gatilhos do enunciado

| Se o enunciado trouxer... | Pense em |
|---|---|
| Envio entre países da UE ou para Noruega, Islândia, Liechtenstein | **Dentro do EEE: livre circulação.** |
| Agência da ONU ou outra organização internacional | **Capítulo V se aplica.** |
| Reino Unido pós-Brexit, Japão | **Decisão de adequação.** |
| Empresa americana certificada / 'autocertificação' | **DPF, Departamento de Comércio, adequação.** |
| Fornecedor fora do EEE sem DPF | **SCC (garantia adequada).** |
| Grupo multinacional, filiais, 'sem contrato para cada envio' | **BCR.** |
| 'quem aprova' as BCR | **Autoridade de controle competente, mecanismo de coerência.** |
| Cláusulas negociadas entre as partes | **Ad hoc: autorização específica da autoridade.** |
| Safe Harbor / 2015 | **Schrems I.** |
| Privacy Shield / julho de 2020 | **Schrems II: avaliar destino e medidas complementares.** |
| Europeu contesta acesso de agências de inteligência dos EUA | **Data Protection Review Court do DPF.** |
| Reserva de hotel em país sem adequação | **Derrogação: necessária ao contrato com o titular.** |
| Autoridades fiscais trocando dados contra fraude | **Derrogação: importantes razões de interesse público.** |
| Tribunal estrangeiro ordena envio de dados | **Art. 48.º: só com acordo internacional.** |

### 🎯 Se você lembrar de só uma coisa deste capítulo...

- Ordem: adequação (45), garantias adequadas (46), derrogações (49).
- SCC: Comissão adota; BCR: autoridade competente aprova; ad hoc: autoridade autoriza.
- DPF cobre só empresas americanas autocertificadas; as demais usam SCC.
- Schrems I derrubou o Safe Harbor (2015); Schrems II derrubou o Privacy Shield (2020), mas não as SCC.
- EEE = UE + Islândia, Liechtenstein, Noruega; Reino Unido e Suíça têm adequação, mas não são EEE.

## Essenciais para a prova (checklist)

- ☐ Sei quais países formam o EEE e que dentro dele não há requisito extra de transferência.

- ☐ Sei que o capítulo V cobre países terceiros e organizações internacionais.
- ☐ Sei o efeito, os critérios e a periodicidade de revisão da decisão de adequação.
- ☐ Sei citar países com adequação e reconhecer os que não têm.
- ☐ Sei quem adota as SCC e as regras sobre cláusulas adicionais.
- ☐ Sei quem aprova as BCR, quem pode usá-las, o que devem conter e quem responde por violações.
- ☐ Sei quando uma garantia exige autorização específica da autoridade (cláusulas ad hoc).
- ☐ Sei as derrogações do art. 49.º e aplicá-las a cenários.
- ☐ Sei a linha do tempo Safe Harbor, Privacy Shield, DPF e o que mudou após Schrems II.
- ☐ Sei a regra do art. 48.º para ordens de autoridades de país terceiro.

## Questões de revisão do capítulo

R5.1 · Transferências Internacionais de Dados Pessoais

**Qual elemento a Comissão Europeia avalia ao decidir sobre a adequação de um país terceiro?**

A. O idioma oficial falado no país
B. O Estado de direito e a autoridade independente
C. O tamanho do mercado consumidor do país terceiro
D. O número de empresas europeias instaladas no país

R5.2 · Transferências Internacionais de Dados Pessoais

**Em 2015, a decisão Schrems I do Tribunal de Justiça da UE invalidou qual acordo de transferência entre a UE e os EUA?**

A. O Safe Harbor
B. O Privacy Shield
C. O Data Privacy Framework
D. O Acordo de Schengen

R5.3 · Transferências Internacionais de Dados Pessoais

**Uma empresa na França quer transferir dados de clientes para um fornecedor nos Estados Unidos que não participa do Data Privacy Framework. Qual mecanismo pode tornar a transferência lícita?**

A. Cláusulas contratuais-padrão aprovadas pela Comissão
B. As regras corporativas da empresa francesa
C. Um aviso de privacidade publicado no site da empresa
D. Uma declaração do fornecedor sem nenhum contrato

R5.4 · Transferências Internacionais de Dados Pessoais

**Sem decisão de adequação nem garantias adequadas, em qual situação o GDPR ainda permite uma transferência para fora do EEE?**

A. Sempre que o destino tiver custos de armazenamento menores
B. Com consentimento explícito do titular, após informado dos riscos
C. Quando a empresa receptora for de grande porte
D. Quando os dados forem enviados por e-mail

## Respostas comentadas

### R5.1. B) O Estado de direito e a autoridade independente

Por quê: Também contam o respeito aos direitos humanos, a legislação sobre acesso de autoridades públicas e os compromissos internacionais do país.

✗ A) Incorreta. Não é critério.
✗ C) Incorreta. Não é critério.
✗ D) Incorreta. Não é critério.

> **Dica de prova:** Adequação: Estado de direito e autoridade independente.

### R5.2. A) O Safe Harbor

Por quê: A sequência histórica: Safe Harbor (invalidado em 2015), Privacy Shield (invalidado em 2020) e Data Privacy Framework (2023).

✗ B) Incorreta. Foi invalidado em 2020.
✗ C) Incorreta. É de 2023 e está vigente.
✗ D) Incorreta. Não trata de transferências.

> **Dica de prova:** Schrems I: Safe Harbor. Schrems II: Privacy Shield.

### R5.3. A) Cláusulas contratuais-padrão aprovadas pela Comissão

Por quê: As cláusulas contratuais-padrão (SCC) são uma das garantias adequadas; a avaliação do risco da transferência também é recomendada.

✗ B) Incorreta. BCR valem dentro do próprio grupo.
✗ C) Incorreta. Não é mecanismo de transferência.
✗ D) Incorreta. Não oferece garantias adequadas.

> **Dica de prova:** Fornecedor fora do EEE: SCC.

**R5.4. B) Com consentimento explícito do titular, após informado dos riscos**

Por quê: As derrogações do artigo 49 são exceções para situações específicas, como contrato com o titular ou interesse público importante, e não devem ser a regra.

✗ A) Incorreta. Custo não é derrogação.

✗ C) Incorreta. Porte não é derrogação.

✗ D) Incorreta. O meio não muda a regra.

> **Dica de prova:** Sem adequação nem garantias: derrogações do art. 49.

DIA DA PROVA

# Estratégia de prova

A prova tem 40 perguntas de múltipla escolha em 60 minutos, sem consulta, e aprova com 65% (26 acertos). Ela cobra os níveis 1 e 2 de Bloom: lembrar (prazos, faixas de multa, quem adota ou aprova) e entender (interpretar, comparar e escolher a descrição correta de um fato ou cenário curto). A maioria das perguntas traz uma situação do dia a dia e pede o princípio, a base legal, o direito, o papel ou o mecanismo correto. As alternativas erradas costumam ser absurdas (fixar preços, prisão, idioma), trocar um conceito vizinho (minimização x conservação, SCC x BCR, 10/2 x 20/4) ou exagerar a regra com 'sempre', 'nunca', 'todo'.

## Como responder

✓ Tenho cerca de 1 minuto e meio por pergunta: faço uma primeira passada respondendo o que sei e marco as dúvidas para voltar.

✓ Distribuo o estudo pelo peso: Princípios (37,5%) e Avaliação e Mitigação de Riscos (25%) somam quase dois terços da prova.

✓ Leio o verbo do cenário antes das alternativas: pedir demais, guardar demais, esconder, mudar de finalidade, decidir junto, seguir instruções. Cada verbo aponta um conceito.

✓ Elimino primeiro as alternativas sem relação com proteção de dados (custo, porte, idioma, preço, energia, imprensa); em geral sobram duas.

✓ Entre as duas finais, procuro o detalhe do enunciado que decide: 'alto risco' x 'risco', 'certificada no DPF' x 'não certificada', 'dentro do grupo' x 'fornecedor', 'dados especiais' x 'menos de 250'.

✓ Desconfio de absolutos ('todo cookie', 'toda violação', 'sempre', 'nenhum'): o GDPR quase sempre tem exceção.

✓ Para números, confiro o par certo: 72 horas (violação), 1 mês + 2 (titular), 8 + 6 semanas (consulta prévia), 4 anos (adequação), 16 a 13 anos (crianças), 10/2 e 20/4 (multas).

✓ Na revisão final, confiro se marquei todas as 40 respostas e volto às dúvidas marcadas usando a eliminação por conceito vizinho.

## Erros que derrubam candidatos

✗ Achar que sem nome não há dado pessoal, ou que pseudonimizado é anônimo.

✗ Confundir o prazo de 1 mês do titular com as 72 horas da notificação de violação.

✗ Trocar as faixas de multa: princípios e direitos dos titulares são 20 milhões/4%, não 10 milhões/2%.

✗ Escolher consentimento como base legal quando existe base mais específica (lei, contrato, interesse vital, interesse público).

✗ Achar que o DPF cobre qualquer empresa americana, que o Privacy Shield vale ou que Schrems II proibiu as SCC.

✗ Pensar que só há violação com ataque ou acesso externo, esquecendo perda acidental e acesso interno.

✗ Confundir quem adota (Comissão: SCC) com quem aprova (autoridade competente: BCR).

## Na semana da prova

- ☐ Refazer as provas simuladas cronometrando 60 minutos e revisar cada erro pelo motivo da alternativa errada.
- ☐ Reler as tabelas de comparação de cada capítulo e os macetes até recitar sem olhar.
- ☐ Montar uma folha de números (72 h, 1 mês + 2, 8 + 6 semanas, 4 anos, 16/13 anos, 250 pessoas, 10/2 e 20/4) e revisar todo dia.
- ☐ Repassar com atenção extra Princípios e Riscos, que valem 62,5% da prova.
- ☐ Na véspera, só revisão leve dos itens 'lembrar' de cada capítulo e descanso.

REVISÃO FINAL

# Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

## 1. Avaliação e Mitigação de Riscos

‣ '72 horas' → **Notificação à autoridade, contada do conhecimento.**

‣ Notificou depois de 72 horas (ex.: 96 horas) → **Incluir os motivos do atraso.**

‣ Ainda faltam detalhes → **Notificar em fases.**

‣ Dados criptografados com chave segura → **Dispensa a comunicação aos titulares.**

‣ Comunicar cada titular exigiria esforço desproporcional → **Comunicação pública ou medida equivalente.**

⚠ Contam do momento em que o controlador toma conhecimento.

⚠ Notificar no prazo e completar em fases.

⚠ Toda violação é documentada (art. 33.º, n.º 5).

## 2. Escopo do GDPR

‣ 'nome não aparece', 'só um código', 'número do cartão', 'cargo ocupado por uma única pessoa' → **Identificável indiretamente: é dado pessoal.**

‣ Tabela de ligação guardada em outro sistema → **Pseudonimização: continua dado pessoal.**

‣ 'ninguém pode ser reidentificado por meios razoáveis', estatísticas agregadas → **Anônimo: fora do GDPR.**

‣ Fichas de papel em ordem alfabética, arquivo → **Sistema de arquivo: GDPR se aplica.**

‣ Apenas visualiza, consulta, apaga, destrói → **Tudo é tratamento.**

⚠ Basta a pessoa ser identificável, direta ou indiretamente: cartão de fidelidade, cargo único ou IP já identificam.

⚠ O suporte não importa: papel organizado em sistema de arquivo já está no escopo.

⚠ Qualquer operação é tratamento, inclusive apagamento e destruição, automatizados ou manuais.

## 3. Princípios do Tratamento de Dados

‣ Formulário pede dados além do necessário → **Minimização.**

‣ Guarda por anos o que só precisava contar → **Limitação da conservação.**

‣ Notebook sem senha nem criptografia → **Integridade e confidencialidade.**

‣ Coleta em segundo plano, sem informar ninguém → **Licitude, lealdade e transparência.**

‣ Dados coletados para X usados para Y incompatível → **Limitação da finalidade.**

⚠ É 1 mês, prorrogável por mais 2. As 72 horas são da notificação de violação à autoridade.

⚠ O tratamento anterior continua lícito; o controlador para daí em diante e, sem outra base, apaga.

⚠ Consentimento exige ato positivo e inequívoco; silêncio e caixa pré-marcada não valem, nem com política de privacidade.

## 4. Prática do Tratamento de Dados

‣ Cookie que só guarda o carrinho de compras → **Estritamente necessário: sem consentimento.**

‣ Cookie de rede de anúncios de outro domínio → **Cookie de terceiros: consentimento.**

‣ 'fica no dispositivo até expirar' → **Cookie persistente.**

‣ Banner aparece depois que os cookies já foram carregados → **Violação: consentimento tem de ser antes.**

‣ Aceitar com um clique, recusar com vários → **Consentimento não livre: recusar tão fácil quanto aceitar.**

⚠ Os estritamente necessários ao serviço pedido (carrinho) são exceção.

⚠ Podem guardar dados; 'sessão' fala só de duração.

⚠ Esse é o de sessão; o persistente sobrevive até expirar ou ser apagado.

## 5. Transferências Internacionais de Dados Pessoais

‣ Envio entre países da UE ou para Noruega, Islândia, Liechtenstein → **Dentro do EEE: livre circulação.**

‣ Agência da ONU ou outra organização internacional → **Capítulo V se aplica.**

‣ Reino Unido pós-Brexit, Japão → **Decisão de adequação.**

‣ Empresa americana certificada / 'autocertificação' → **DPF, Departamento de Comércio, adequação.**

‣ Fornecedor fora do EEE sem DPF → **SCC (garantia adequada).**

⚠ Não integra o EEE; as transferências se apoiam numa decisão de adequação.

⚠ EEE não-UE = só Islândia, Liechtenstein e Noruega. A Suíça tem adequação, mas não é EEE.

⚠ Só para organizações autocertificadas no Departamento de Comércio.

GABARITO

# Respostas do diagnóstico

**D1. D) Até 10 milhões de euros ou 2% do faturamento anual mundial** → revise o capítulo 1

Por quê: Aplica-se o valor mais alto entre o fixo e o percentual; a faixa maior vale para princípios, bases legais, direitos e transferências.

✗ A) Incorreta. Não é o limite previsto.

✗ B) Incorreta. Não é o limite previsto.

✗ C) Incorreta. Faixa do artigo 83.º, n.º 5.

> **Dica de prova:** Obrigações do controlador/operador: 10 mi ou 2%.

**D2. B) Uma violação de dados pessoais que exige avaliação do risco** → revise o capítulo 1

Por quê: Salários e dados bancários podem gerar risco relevante; sem criptografia, a notificação à autoridade e aos titulares tende a ser necessária.

✗ A) Incorreta. O valor do dispositivo não importa.

✗ C) Incorreta. A folha tem dados pessoais.

✗ D) Incorreta. A perda já é violação.

> **Dica de prova:** Pendrive sem criptografia perdido: violação.

**D3. C) 20 milhões de euros ou 4% do faturamento anual mundial** → revise o capítulo 1

Por quê: As multas devem ser efetivas, proporcionais e dissuasivas; o nível de 10 milhões ou 2% vale, por exemplo, para obrigações de controlador e operador.

✗ A) Incorreta. Esse é o teto do nível inferior.

✗ B) Incorreta. Não é o critério do GDPR.

✗ D) Incorreta. Não é o teto do GDPR.

> **Dica de prova:** Teto máximo: 20 milhões ou 4%.

**D4. D) Sim, porque oferece bens a pessoas que estão na União** → revise o capítulo 2

Por quê: O GDPR alcança controladores de fora da UE que oferecem bens ou serviços a titulares que estão na União ou monitoram o comportamento deles.

✗ A) Incorreta. O alcance vai além do estabelecimento.

✗ B) Incorreta. O critério é estar na União, não a cidadania.

✗ C) Incorreta. O meio de pagamento não importa.

> **Dica de prova:** Oferta a quem está na UE: GDPR se aplica.

**D5. D) Com regime próprio, sob controle de autoridade pública** → revise o capítulo 2

Por quê: O tratamento só pode ocorrer sob controle de autoridade pública ou quando autorizado por lei com garantias adequadas.

✗ A) Incorreta. Não é o regime do GDPR.
✗ B) Incorreta. Continuam sendo dados pessoais.
✗ C) Incorreta. Há regras específicas no artigo 10.

> **Dica de prova:** Dados penais: artigo 10, regime próprio.

**D6. D) Porque pode revelar convicções religiosas** → revise o capítulo 2

Por quê: O artigo 9.º protege dados que revelem crenças religiosas, mesmo quando a informação é indireta.

✗ A) Incorreta. Não tem relação com o GDPR.
✗ B) Incorreta. O GDPR se aplica.
✗ C) Incorreta. Não é o motivo.

> **Dica de prova:** Dado que revela religião: categoria especial.

**D7. C) Por um procedimento de certificação aprovado** → revise o capítulo 3

Por quê: A certificação do artigo 42 pode ser usada como elemento para demonstrar o cumprimento do artigo 25.

✗ A) Incorreta. Não demonstra conformidade.
✗ B) Incorreta. Não demonstra conformidade.
✗ D) Incorreta. Não demonstra conformidade.

> **Dica de prova:** Demonstrar by design: certificação.

**D8. C) Minimização dos dados** → revise o capítulo 3

Por quê: Minimização se refere à quantidade e ao tipo de dados; limitação da conservação se refere ao tempo em que ficam guardados.

✗ A) Incorreta. Trata de dados corretos e atualizados.
✗ B) Incorreta. Trata da informação ao titular.
✗ D) Incorreta. Trata do tempo de guarda.

> **Dica de prova:** Só o necessário: minimização.

**D9. B) Adotar medidas razoáveis para avisar outros controladores** → revise o capítulo 3

Por quê: Considerando a tecnologia e os custos, o controlador informa os outros que o titular pediu o apagamento de links, cópias ou reproduções.

✗ A) Incorreta. Exporia de novo o titular.
✗ C) Incorreta. Exige medidas razoáveis, não impossíveis.
✗ D) Incorreta. Não é exigência do artigo 17.

> **Dica de prova:** Dados públicos: avisar os outros controladores.

**D10. A) Fica no dispositivo até expirar ou ser apagado** → revise o capítulo 4

Por quê: Cookies persistentes servem, por exemplo, para lembrar preferências ou login; cookies não essenciais exigem consentimento pela Diretiva ePrivacy.

✗ B) Incorreta. Cookies são lidos por sites.
✗ C) Incorreta. Esse é o cookie de sessão.
✗ D) Incorreta. Pode conter identificadores pessoais.

> **Dica de prova:** Persistente: sobrevive ao fechamento do navegador.

**D11. C) Informar os doadores sobre o novo tratamento** → revise o capítulo 4

Por quê: O uso de IA costuma ser uma nova atividade de tratamento: exige base legal, transparência e, conforme o risco, uma DPIA.

✗ A) Incorreta. A obrigação fiscal continua.
✗ B) Incorreta. Não é necessário.
✗ D) Incorreta. Violaria a confidencialidade.

> **Dica de prova:** Novo uso com IA: informar os titulares.

**D12. B) Antes de gravar os cookies no navegador** → revise o capítulo 4

Por quê: Carregar cookies não essenciais antes do consentimento viola a Diretiva ePrivacy, mesmo que o banner apareça em seguida.

✗ A) Incorreta. Não depende de compra.
✗ C) Incorreta. Seria tarde demais.
✗ D) Incorreta. Deve ser antes.

> **Dica de prova:** Cookies não essenciais: consentimento antes.


## Agora, treine no formato real

Faça as 6 provas completas do curso EXIN PDPF: 240 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

**Ver as 6 provas completas e o cupom do mês →**


## Até o dia da prova, uma revisão por dia no seu feed

### Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

**Seguir no Instagram →**

### YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

**Inscrever-se no canal →**

Material independente de preparação, sem afiliação ou endosso de EXIN. As questões são inéditas e não reproduzem a prova real.