Exame simulado

Edição 202308

Conteúdo

Introdução

Este é o exame simulado EXIN Privacy & Data Protection Foundation (PDPF.PR). As regras e regulamentos do exame do EXIN se aplicam a este exame.

Este exame consiste de 40 questões de múltipla escolha. Cada questão de múltipla escolha possui um certo número de alternativas de resposta, entre as quais apenas uma resposta é a correta.

O número máximo de pontos que pode ser obtido neste exame é 40. Cada resposta correta vale 1 ponto. Você precisa de 26 pontos ou mais para passar no exame.

O tempo permitido para este exame é de 60 minutos.

Boa Sorte!

Exame simulado

1 / 40
Um lojista deseja registrar quantos visitantes entram em sua loja todos os dias. Um sistema detecta o endereço MAC do smartphone de cada visitante. É impossível o lojista identificar o proprietário do telefone a partir deste sinal, mas os provedores de serviços de telefonia podem relacionar o endereço MAC ao proprietário do telefone.

De acordo com o GDPR, é permitido que o lojista utilize este método?

A) Sim, porque o lojista não pode identificar o proprietário do telefone.
B) Sim, porque o visitante consentiu automaticamente quando se conectou ao Wi-Fi.
C) Não, porque o endereço MAC do telefone deve ser considerado como um dado pessoal.
D) Não, porque os provedores de serviços de telefonia são os proprietários dos endereços MAC.

2 / 40
Os dados pessoais, de acordo com a definição no GDPR, podem ser divididos em vários tipos. Um desses tipos é descrito do seguinte modo:

Dados que revelem direta ou indiretamente as origens raciais ou étnicas de uma pessoa, suas visões políticas, filosóficas ou religiosas, afiliação sindical e dados relacionados à saúde, vida sexual ou orientação sexual.

Que categoria de dados pessoais é esta?

A) Dados pessoais diretos
B) Dados pessoais indiretos
C) Dados pseudonimizados
D) Dados pessoais de categoria especial

3 / 40
Uma pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, isoladamente ou em conjunto com outras partes, determina os objetivos e os meios de processamento de dados pessoais.

Que papel na proteção de dados é definido aqui?

A) Controlador
B) Processador
C) Autoridade supervisora
D) Terceiro

4 / 40
Ocorreu uma violação de segurança em um sistema de informação que também contém dados pessoais.

De acordo com o GDPR, qual é a **primeira** coisa que o controlador deve fazer?

A) Verificar se a violação pode ter provocado a perda ou o processamento ilegal de dados pessoais
B) Avaliar o risco de efeitos adversos para os titulares dos dados usando uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)
C) Determinar se dados pessoais de caráter sensível foram ou possam ter sido processados ilegalmente
D) Relatar a violação imediatamente a todos os titulares dos dados e à autoridade supervisora relevante

5 / 40
Uma violação da segurança que provoque a destruição, perda, alteração, divulgação não autorizada ou acesso acidental ou ilegal de dados pessoais transmitidos, armazenados ou processados de outro modo.

Qual é o termo **exato** associado a esta definição no GDPR?

A) Violação da confidencialidade
B) Violação de dados pessoais
C) Violação de segurança
D) Incidente de segurança

6 / 40
Que direito do titular dos dados é definido explicitamente pelo GDPR?

A) Uma cópia dos dados pessoais deve ser fornecida no formato solicitado pelo titular dos dados.
B) O acesso aos dados pessoais deve ser fornecido sem custo para o titular dos dados.
C) Os dados pessoais sempre devem ser alterados mediante solicitação do titular dos dados.
D) Os dados pessoais devem ser apagados sempre que isso for solicitado pelo titular dos dados.

7 / 40
Quando dados pessoais são processados, quem é o responsável final por demonstrar conformidade com o GDPR?

A) O controlador
B) O Data Protection Officer (DPO)
C) O processador
D) A autoridade supervisora

8 / 40
De acordo com o princípio de limitação de finalidade, os dados não devem ser processados além do objetivo legítimo definido. Contudo, o processamento adicional é permitido em alguns casos específicos, desde que sejam adotadas salvaguardas apropriadas aos direitos e liberdades dos titulares dos dados.

Para qual finalidade o processamento adicional **não** é permitido?

A) Para fins de arquivamento por interesse público
B) Para fins comerciais e de marketing direto
C) Para fins estatísticos em geral
D) Para fins de pesquisa histórica ou científica

9 / 40
De acordo com o GDPR, em que situação os titulares dos dados devem ser **sempre** notificados de uma violação de dados pessoais?

A) Quando os dados pessoais forem processados em uma unidade do processador que não esteja localizada dentro das fronteiras da Área Econômica Euopeia (AEE)
B) Quando os dados pessoais forem processados por uma parte que concordou com o contrato de processamento, mas ainda não o assinou
C) Quando o sistema no qual os dados pessoais são processados for atacado, causando uma avaria em seus dispositivos de armazenamento
D) Quando houver uma probabilidade considerável de que a violação provoque um alto risco à privacidade dos titulares dos dados

10 / 40
Alguns processamentos de dados estão fora do escopo material do GDPR.

Que tipo de processamento **não** está sujeito ao GDPR?

A) Coleta de informações de nome e endereço para um clube de ginástica
B) Criação de um backup de dados biométricos para fins de segurança dos dados
C) Edição de fotografias pessoais antes de imprimi-las em casa

11 / 40
O GDPR não define privacidade como um termo, mas emprega o conceito de modo implícito em todo o seu texto.

Qual seria uma definição correta de privacidade, conforme implicitamente utilizado por todo o GDPR?

A) O direito fundamental à proteção de dados pessoais, independentemente do modo como foram obtidos
B) O direito de não ser incomodado por pessoas não convidadas, não ser seguido, vigiado ou monitorado
C) O direito ao respeito pela vida privada e familiar de uma pessoa, seu lar e sua correspondência pessoal
D) O direito à liberdade de opinião e expressão e o direito a buscar, receber e divulgar informações

12 / 40
Qual é a relação entre privacidade e proteção de dados?

A) Proteção de dados e privacidade são sinônimos e têm o mesmo significado.
B) Proteção de dados é a parte da privacidade que protege a integridade física de um indivíduo.
C) Proteção de dados refere-se às medidas necessárias para proteger a privacidade de um indivíduo.

13 / 40
Qual é a situação jurídica do GDPR?

A) O GDPR é uma lei funcional em todos os estados membros da Área Econômica Europeia (AEE). Alguns artigos permitem que a legislação dos estados membros forneça regras mais específicas.
B) O GDPR é uma recomendação da Comissão Europeia para que as autoridades legais dos países da AEE melhorem suas leis sobre proteção de dados pessoais.
C) O GDPR estabelece condições e requisitos mínimos. Os estados membros devem aprovar leis nacionais que atendam a estes requisitos mínimos.

14 / 40
No GDPR, alguns tipos de dados pessoais são considerados como dados pessoais de categoria especial.

Quais dados pessoais são considerados como dados pessoais de categoria especial?

A) Uma lista de pagamentos efetuados usando um cartão de crédito
B) Uma lista de endereços dos membros de um partido político
C) Um registro genealógico dos ancestrais de uma pessoa

15 / 40
Para planejar o tamanho da área de estacionamento necessária, um governo local monitora e salva o número da placa de cada carro que entra e sai do centro da cidade. Foi obtida uma permissão para coletar dados sobre o número de carros presentes no centro da cidade.

Pela comparação dos horários de entrada e saída para as placas, é calculado o número de carros presentes a cada momento de cada dia. A cada mês é gerado um relatório detalhando o número médio de carros presentes no centro da cidade em momentos específicos para cada dia da semana. Em todas as entradas no centro da cidade, um cartaz explica com clareza quais dados são coletados por quem, a finalidade do processamento e o fato de que os números das placas serão armazenados em segurança por até dois anos, porque as medidas serão repetidas no ano seguinte.

Que princípio básico do processamento legítimo de dados pessoais está sendo **violado** neste caso?

A) Os dados pessoais devem ser coletados para finalidades especificadas, explícitas e legítimas e não devem ser processados adicionalmente.
B) Os dados pessoais devem ser mantidos de modo que permita a identificação dos titulares dos dados por um período não maior que o necessário.
C) Os dados pessoais devem ser processados de modo que garanta a segurança apropriada dos dados pessoais.
D) Os dados pessoais devem ser processados de modo transparente em relação ao titular dos dados.

16 / 40
Os dados pessoais devem ser adequados, relevantes e limitados ao que for necessário em relação às finalidades para as quais são processados.

Que princípio do processamento de dados é descrito aqui?

A) Exatidão
B) Minimização de dados
C) Equidade e transparência
D) Limitação de finalidade

17 / 40
Um indivíduo está se mudando da cidade A para a cidade B, em um estado membro da Área Econômica Europeia (AEE). Na cidade A, ele era um paciente do hospital local A. Na cidade B, passa a ser um paciente do hospital B. O paciente optou pela não inclusão no sistema nacional de prontuários eletrônicos de pacientes.

O paciente solicita que o hospital A encaminhe seu prontuário médico diretamente ao hospital B.

De acordo com o GDPR, o que é permitido?

A) O hospital em A pode enviar os dados diretamente ao hospital B, como solicitado pelo paciente.
B) O hospital em A pode enviar o prontuário ao hospital B, antes que seja solicitado pelo paciente.
C) O hospital em A pode enviar o prontuário médico ao titular dos dados, mas não a outro hospital.
D) O hospital em A não pode enviar o prontuário porque não há uma base legítima para o processamento.

18 / 40
Uma empresa tem planos para processar dados pessoais. O Data Protection Officer (DPO) recentemente indicado executa uma Avaliação de Impacto sobre a Proteção de Dados (DPIA). O DPIA constata que todos os computadores têm uma configuração que faz os monitores exibirem um protetor de tela após cinco segundos de inatividade. Contudo, os computadores não são bloqueados automaticamente. Quando os funcionários deixam sua mesa, geralmente também não bloqueiam seus computadores.

Isso é um exemplo de quê?

A) Acesso a dados
B) Violação de dados pessoais
C) Incidente de segurança
D) Vulnerabilidade da segurança

19 / 40
O GDPR refere-se aos princípios de proporcionalidade e subsidiariedade.

Qual é o significado de subsidiariedade neste contexto?

A) Dados pessoais só podem ser processados de acordo com a especificação da finalidade.
B) Dados pessoais não podem ser reutilizados sem um consentimento explícito e informado.
C) Dados pessoais só podem ser processados quando não houver outros meios para obter a finalidade.
D) Dados pessoais devem ser adequados, relevantes e não excessivos em relação às finalidades.

20 / 40
"O controlador deve implementar medidas técnicas e organizacionais apropriadas para garantir que (...) sejam processados somente os dados pessoais que sejam necessários para cada finalidade específica do processamento."

Que termo do GDPR é definido aqui?

A) Conformidade
B) Proteção de dados desde a concepção (by design) e por padrão (by default)
C) Proteção de dados incorporada

21 / 40
Durante a realização de um backup, ocorreu uma falha no disco rígido do servidor de dados. Tanto os dados quanto o backup são perdidos. O disco continha dados pessoais, mas nenhum dado pessoal de categoria especial.

O processador afirma que isto constitui uma violação de dados pessoais.

A afirmação do processador é verdadeira?

A) Sim, porque os dados pessoais no disco foram processados de modo ilegal.
B) Sim, porque não havia dados pessoais de categoria especial armazenados no disco.
C) Não, porque nenhum dado pessoal no disco foi processado, apenas destruído.
D) Não, porque isto é apenas um incidente de segurança, e não uma violação de dados.

22 / 40
As organizações têm a obrigação de manter diversos registros para demonstrar conformidade com o GDPR.

Qual registro **não** é obrigatório de acordo com o GDPR?

A) Um registro de todo o processamento pretendido, juntamente com a(s) finalidade(s) do processamento e as justificativas legais
B) Um registro de violações de dados com todas as características relevantes, incluindo notificações
C) Um registro das notificações enviadas à autoridade supervisora, relativas ao processamento de dados pessoais
D) Um registro de processadores, incluindo os dados pessoais fornecidos e o período pelo qual estes dados podem ser retidos

23 / 40
Houve uma violação de dados pessoais e o controlador está redigindo uma notificação à autoridade supervisora. As seguintes informações já constam da notificação:

- A natureza da violação de dados pessoais e suas possíveis consequências.
- Informações sobre as partes que podem fornecer mais informações sobre a violação dos dados.

Que outras informações o controlador deve fornecer?

A) A informação de que as autoridades locais e nacionais foram notificadas da violação dos dados
B) O nome e os detalhes de contato dos titulares dos dados que possam ter tido seus dados violados
C) As medidas sugeridas para mitigar as consequências adversas da violação de dados
D) As informações necessárias para acessar os dados pessoais que foram violados

24 / 40
De acordo com o Artigo 33 do GDPR, o controlador deve notificar uma violação de dados pessoais à autoridade supervisora sem demora injustificada e, quando possível, no máximo 72 horas após tomar ciência do fato.

Qual é a sanção máxima para o descumprimento desta obrigação de notificar?

A) € 10.000.000 ou 2% do volume global anual de negócios, o que for maior
B) € 20.000.000 ou 4% do volume global anual de negócios, o que for maior
C) Até € 500.000 com um mínimo de € 120.000
D) Até € 820.000 com um mínimo de € 350.000

25 / 40
De acordo com o GDPR, qual é uma tarefa da autoridade supervisora?

A) Implementar medidas técnicas e organizacionais para garantir a conformidade
B) Investigar violações de segurança de informações corporativas
C) Monitorar e impor a aplicação do GDPR

26 / 40
Uma empresa belga tem sua sede na França por motivos fiscais. Ela firma um contrato juridicamente vinculante com um processador nos Países Baixos para o processamento de dados pessoais de titulares dos dados de várias nacionalidades.

Ocorre uma violação de dados pessoais. A autoridade supervisora inicia uma investigação.

Por que a autoridade supervisora francesa é considerada como a autoridade supervisora principal?

A) Porque a França está localizada no meio da Europa
B) Porque a França é o maior dos três países da Área Econômica Europeia (AEE)
C) Porque a sede da empresa está na França

27 / 40
Em 10 de julho de 2023 a Comissão Europeia implementou uma disposição regulamentar relativa à transferência de dados pessoais entre a Área Econômica Europeia (AEE) e os Estados Unidos da América (EUA). A disposição regulamentar é baseada nas medidas para proteção de dados descritas no Framework de Privacidade de Dados UE-EUA.

Que tipo de disposição é essa?

A) Decisão de adequação
B) Exceção
C) Contrato juridicamente vinculante
D) Tratado que substitui o GDPR

28 / 40
Um controlador deseja terceirizar o processamento de dados pessoais para um processador.

O que deve ser realizado **antes** da terceirização?

A) O controlador deve pedir permissão à autoridade supervisora para terceirizar o processamento dos dados.
B) O controlador deve perguntar à autoridade supervisora se o contrato por escrito combinado está em conformidade com os regulamentos.
C) O controlador e o processador devem preparar uma minuta e assinar um contrato por escrito garantindo a confidencialidade dos dados.
D) O processador deve demonstrar ao controlador que todas as demandas acordadas no acordo de nível de serviço (ANS) são cumpridas.

29 / 40
Qual é o objetivo de uma auditoria de proteção de dados pela autoridade supervisora?

A) Aconselhar o controlador sobre a mitigação de riscos à privacidade para proteger o controlador de pedidos de indenização de responsabilidade civil por não conformidade
B) Atender a obrigação no GDPR de implementar medidas técnicas e organizacionais apropriadas para proteção de dados
C) Monitorar e impor a aplicação do GDPR, determinando se o processamento está sendo realizado em conformidade com o GDPR

30 / 40
Para que um processamento de dados pessoais seja legal, o que **sempre** será exigido?

A) Um código de conduta deve ser estabelecido, descrevendo exatamente o que o processamento envolve.
B) O processamento deve relatado e autorizado pela autoridade supervisora.
C) Deve haver uma base legítima para o processamento de dados pessoais.

31 / 40
Dados pessoais podem ser transferidos para fora da Área Econômica Europeia (AEE).

De acordo com o GDPR, que transferências para fora da AEE são sempre legais?

A) Transferências baseadas nas leis do país não pertencente à AEE envolvido
B) Transferências sujeitas às regras da Organização Mundial do Comércio (OMC)
C) Transferências governadas por regras corporativas vinculantes (BCR) aprovadas
D) Transferências dentro de uma corporação ou organização global

32 / 40
De acordo com o GDPR, qual seria uma descrição de regras corporativas vinculantes (BCR)?

A) Uma decisão sobre a segurança da transferência de dados pessoais para um país fora da Área Econômica Europeia (AEE)
B) Uma medida para compensar a ausência de proteção de dados em um país terceiro
C) Um conjunto de acordos abordando transferências de dados pessoais entre países situados fora da AEE
D) Um conjunto de regras aprovadas sobre a proteção de dados pessoais, usadas por um grupo de empresas

33 / 40
Um contrato por escrito entre um controlador e um processador é chamado de acordo de processamento.

De acordo com o GDPR, o que **não** precisa ser abordado no contrato por escrito?

A) O código de ética comercial e conduta da contratada que será utilizado
B) Os procedimentos para violações de segurança das informações e de dados pessoais
C) As medidas técnicas e organizacionais implementadas
D) Quais dados são cobertos pelo acordo de processamento de dados

34 / 40
Um dos objetivos de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) é fortalecer a confiança dos clientes ou cidadãos no modo como os dados pessoais são processados e a privacidade é respeitada.

Como um DPIA pode fortalecer a confiança?

A) A organização minimiza o risco de ajustes dispendiosos dos processos ou remodelamento dos sistemas em um estágio mais tardio.
B) A organização previne a não conformidade com o GDPR e minimiza o risco de multas.
C) A organização prova que considera a privacidade com seriedade e visa à conformidade com o GDPR.

35 / 40
Um dos sete princípios da proteção de dados desde a concepção (by design) é a *Funcionalidade – Soma Positiva, Diferente de Zero*.

Qual é a essência deste princípio?

A) As normas de segurança aplicadas devem garantir a confidencialidade, a integridade e a disponibilidade dos dados pessoais durante todo o seu ciclo de vida.
B) Se diferentes tipos de objetivos legítimos forem contraditórios, os objetivos de privacidade devem ter prioridade em relação a outros objetivos de segurança.
C) Ao incorporar a privacidade em uma determinada tecnologia, processo ou sistema, isto deve ser realizado de tal modo que a funcionalidade completa não seja prejudicada.
D) Sempre que possível, avaliações detalhadas de impacto na privacidade e riscos devem ser realizadas e publicadas, documentando com clareza os riscos para a privacidade.

36 / 40
Uma empresa deseja utilizar os dados pessoais de seus clientes. Ela pretende começar a enviar um informativo personalizado a todas as clientes do sexo feminino.

Que direito todos os titulares dos dados terão nesta situação?

A) O direito à compensação
B) O direito de se opor à definição de perfis
C) O direito à retificação

37 / 40
Qual seria uma descrição de proteção de dados desde a concepção (by design) e como padrão (by default)?

A) Uma abordagem que implementa a proteção dos dados desde o início.
B) Uma indicação de prazos se o processamento estiver relacionado ao apagamentos.
C) Os dados só podem ser coletados para finalidades explícitas e legítimas.
D) Não manter mais dados que o estritamente necessário para o processamento.

38 / 40
De acordo com o GDPR, quando uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) é obrigatória?

A) Quando um projeto incluir tecnologias ou processos que utilizem dados pessoais
B) Quando for provável que o processamento cause um alto risco para os direitos dos titulares dos dados
C) Quando operações de processamento semelhantes com riscos comparáveis forem repetidas

39 / 40
O GDPR descreve o princípio de minimização de dados.

Como as organizações podem obedecer a esse princípio?

A) Aplicando o conceito de privilégio mínimo aos dados pessoais coletados, armazenados ou de outro modo processados.
B) Limitando o direito de acesso às pessoas que precisarem dos dados pessoais para as operações de processamento pretendidas.
C) Limitando os tamanhos dos arquivos, salvando todos os dados pessoais processados no menor formato possível.
D) Limitando os dados pessoais àquilo que for adequado, relevante e necessário para os objetivos do processamento.

40 / 40
Qual é a **principal** utilização de um cookie persistente?

A) Garantir que os dados pessoais do usuário sejam armazenados com segurança no servidor
B) Personalizar a experiência do usuário do site durante uma próxima visita
C) Registrar cada tecla pressionada por um usuário computador para descobrir senhas
D) Salvar as páginas que um usuário marcar como favoritas no histórico do navegador do usuário

Gabarito de respostas

1 / 40
Um lojista deseja registrar quantos visitantes entram em sua loja todos os dias. Um sistema detecta o endereço MAC do smartphone de cada visitante. É impossível o lojista identificar o proprietário do telefone a partir deste sinal, mas os provedores de serviços de telefonia podem relacionar o endereço MAC ao proprietário do telefone.

De acordo com o GDPR, é permitido que o lojista utilize este método?

A) Sim, porque o lojista não pode identificar o proprietário do telefone.
B) Sim, porque o visitante consentiu automaticamente quando se conectou ao Wi-Fi.
C) Não, porque o endereço MAC do telefone deve ser considerado como um dado pessoal.
D) Não, porque os provedores de serviços de telefonia são os proprietários dos endereços MAC.

A) Incorreto. O problema não é o lojista conseguir identificar o visitante, mas o fato de que isto seria tecnicamente possível.
B) Incorreto. O consentimento deve consistir em um ato ativo, informado e voluntário de anuência ao processamento. Para ver um endereço MAC, o visitante não precisa estar conectado ao Wi-Fi.
C) Correto. O sinal do telefone é um código específico que pode ser relacionado a seu proprietário. Os dados devem ser considerados como dados pessoais, porque tecnicamente é possível identificar o visitante. (Literatura: A, Capítulo 3; Artigos 26 e 30 do GDPR)
D) Incorreto. O lojista não pode manter nem processar os dados porque eles devem ser considerados como dados pessoais. O provedor de serviços de telefonia não é o proprietário do endereço MAC e não é protegido pelo GDPR.

2 / 40
Os dados pessoais, de acordo com a definição no GDPR, podem ser divididos em vários tipos. Um desses tipos é descrito do seguinte modo:

Dados que revelem direta ou indiretamente as origens raciais ou étnicas de uma pessoa, suas visões políticas, filosóficas ou religiosas, afiliação sindical e dados relacionados à saúde, vida sexual ou orientação sexual.

Que categoria de dados pessoais é esta?

A) Dados pessoais diretos
B) Dados pessoais indiretos
C) Dados pseudonimizados
D) Dados pessoais de categoria especial

A) Incorreto. Tanto dados diretos quanto indiretos são descritos.
B) Incorreto. Tanto dados diretos quanto indiretos são descritos.
C) Incorreto. Dados pseudonimizados não são capazes de revelar informações diretamente.
D) Correto. Esta é a definição de dados pessoais de categoria especial. (Literatura: A, Capítulo 1; Artigo 4 do GDPR)

3 / 40
Uma pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, isoladamente ou em conjunto com outras partes, determina os objetivos e os meios de processamento de dados pessoais.

Que papel na proteção de dados é definido aqui?

A) Controlador
B) Processador
C) Autoridade supervisora
D) Terceiro

A) Correto. O controlador determina o objetivo e os meios de processamento. (Literatura: A, Capítulo 1; Artigo 4(7) do GDPR)
B) Incorreto. O controlador determina os objetivos do processamento, o processador trabalha de acordo com as instruções do controlador.
C) Incorreto. A autoridade supervisora monitora e exige o cumprimento dos requisitos do GDPR.
D) Incorreto. Um terceiro não atua para determinar o objetivo do processamento. Qualquer parte que determine o objetivo se tornaria um novo controlador.

4 / 40
Ocorreu uma violação de segurança em um sistema de informação que também contém dados pessoais.

De acordo com o GDPR, qual é a **primeira** coisa que o controlador deve fazer?

A) Verificar se a violação pode ter provocado a perda ou o processamento ilegal de dados pessoais
B) Avaliar o risco de efeitos adversos para os titulares dos dados usando uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)
C) Determinar se dados pessoais de caráter sensível foram ou possam ter sido processados ilegalmente
D) Relatar a violação imediatamente a todos os titulares dos dados e à autoridade supervisora relevante

A) Correto. A primeira coisa que deve ser feita é verificar se o incidente de segurança realmente constitui uma violação de dados pessoais. (Literatura: A, Capítulo 5)
B) Incorreto. Um DPIA é conduzido durante o delineamento de operações de processamento de dados pessoais. Isso não faz parte do procedimento para uma violação de dados.
C) Incorreto. Esta é a etapa seguinte, se for comprovado que o incidente constitui uma violação de dados pessoais – verificar o tipo de violação de dados.
D) Incorreto. A necessidade de relatar uma violação de dados, e a quem ela deve ser relatada, depende de ter havido ou não uma violação de dados e, se for o caso, do tipo de violação de dados.

5 / 40
Uma violação da segurança que provoque a destruição, perda, alteração, divulgação não autorizada ou acesso acidental ou ilegal de dados pessoais transmitidos, armazenados ou processados de outro modo.

Qual é o termo **exato** associado a esta definição no GDPR?

A) Violação da confidencialidade
B) Violação de dados pessoais
C) Violação de segurança
D) Incidente de segurança

A) Incorreto. O GDPR utiliza o termo violação de dados pessoais. Nem toda violação de dados constitui uma violação de confidencialidade.
B) Correto. Esta é a definição de uma violação de dados pessoais. (Literatura: A, Capítulo 5; Artigo 4(12) do GDPR)
C) Incorreto. O GDPR utiliza o termo violação de dados pessoais. Nem toda violação de segurança constitui uma violação de dados. Nem toda violação de dados constitui uma violação de dados pessoais.
D) Incorreto. O GDPR utiliza o termo violação de dados pessoais. Nem todo incidente de segurança constitui uma violação de dados.

6 / 40
Que direito do titular dos dados é definido explicitamente pelo GDPR?

A) Uma cópia dos dados pessoais deve ser fornecida no formato solicitado pelo titular dos dados.
B) O acesso aos dados pessoais deve ser fornecido sem custo para o titular dos dados.
C) Os dados pessoais sempre devem ser alterados mediante solicitação do titular dos dados.
D) Os dados pessoais devem ser apagados sempre que isso for solicitado pelo titular dos dados.

A) Incorreto. Os dados devem ser fornecidos em um formato estruturado, rotineiramente usado e que permita a leitura em um computador, mas não necessariamente em qualquer formato especificado pelo titular dos dados.
B) Correto. Os titulares dos dados têm direito a uma cópia de seus dados, sem custos. Contudo, apenas a primeira cópia precisa ser gratuita. (Literatura: A, Capítulo 4)
C) Incorreto. Apenas os dados incorretos precisam ser retificados.
D) Incorreto. O direito ao apagamento apresenta várias exceções, por exemplo, quando os dados forem necessários para o estabelecimento, exercício ou defensa de reclamações legais.

7 / 40
Quando dados pessoais são processados, quem é o responsável final por demonstrar conformidade com o GDPR?

A) O controlador
B) O Data Protection Officer (DPO)
C) O processador
D) A autoridade supervisora

A) Correto. O controlador é responsável por medidas de segurança dos dados adequadas e deve ser capaz de demonstrar a conformidade com o GDPR. (Literatura: A, Capítulo 2)
B) Incorreto. O DPO tem um conhecimento especializado e ajuda o controlador ou o processador a monitorar a conformidade interna.
C) Incorreto. O processador é aquele que processa os dados pessoais de acordo com as instruções do controlador. Mesmo assim, o controlador ainda é o responsável final.
D) Incorreto. O controlador deve demonstrar a conformidade com o GDPR, se solicitado pela autoridade supervisora.

8 / 40
De acordo com o princípio de limitação de finalidade, os dados não devem ser processados além do objetivo legítimo definido. Contudo, o processamento adicional é permitido em alguns casos específicos, desde que sejam adotadas salvaguardas apropriadas aos direitos e liberdades dos titulares dos dados.

Para qual finalidade o processamento adicional **não** é permitido?

A) Para fins de arquivamento por interesse público
B) Para fins comerciais e de marketing direto
C) Para fins estatísticos em geral
D) Para fins de pesquisa histórica ou científica

A) Incorreto. Com salvaguardas estabelecidas, o processamento adicional para fins de arquivamento por interesse público é permitido.
B) Correto. Esta não é uma finalidade permitida, se não constituir a finalidade legítima original do processamento. (Literatura: A, Capítulo 2)
C) Incorreto. Com salvaguardas estabelecidas, o processamento adicional para fins estatísticos em geral é permitido.
D) Incorreto. Com salvaguardas estabelecidas, o processamento adicional para fins de pesquisa é permitido.

9 / 40
De acordo com o GDPR, em que situação os titulares dos dados devem ser **sempre** notificados de uma violação de dados pessoais?

A) Quando os dados pessoais forem processados em uma unidade do processador que não esteja localizada dentro das fronteiras da Área Econômica Euopeia (AEE)
B) Quando os dados pessoais forem processados por uma parte que concordou com o contrato de processamento, mas ainda não o assinou
C) Quando o sistema no qual os dados pessoais são processados for atacado, causando uma avaria em seus dispositivos de armazenamento
D) Quando houver uma probabilidade considerável de que a violação provoque um alto risco à privacidade dos titulares dos dados

A) Incorreto. O local onde os dados são processados não tem importância para a obrigação de notificar os titulares dos dados sobre violações de dados pessoais.
B) Incorreto. O processamento de dados pessoais por outra parte diferente do controlador sem um contrato por escrito válido é considerado como uma violação de dados. Nesta situação, porém, consequências negativas para os titulares dos dados são improváveis. A notificação dos titulares dos dados não é obrigatória neste caso.
C) Incorreto. Uma avaria de dispositivos de armazenamento dificulta ou até mesmo impossibilita o acesso aos dados, mas não implica um processamento ilegal.
D) Correto. Se houver uma probabilidade significativa de impacto negativo para os titulares dos dados, o controlador é obrigado a notificá-los sobre a violação. (Literatura: A, Capítulo 5)

10 / 40
Alguns processamentos de dados estão fora do escopo material do GDPR.

Que tipo de processamento **não** está sujeito ao GDPR?

A) Coleta de informações de nome e endereço para um clube de ginástica
B) Criação de um backup de dados biométricos para fins de segurança dos dados
C) Edição de fotografias pessoais antes de imprimi-las em casa

A) Incorreto. A coleta também é considerada como um processamento de dados.
B) Incorreto. O armazenamento também é considerado como um processamento de dados.
C) Correto. O GDPR não é aplicável ao uso domiciliar de suas próprias fotografias. (Literatura: A, Capítulo 1; Artigo 4 do GDPR)

11 / 40
O GDPR não define privacidade como um termo, mas emprega o conceito de modo implícito em todo o seu texto.

Qual seria uma definição correta de privacidade, conforme implicitamente utilizado por todo o GDPR?

A) O direito fundamental à proteção de dados pessoais, independentemente do modo como foram obtidos
B) O direito de não ser incomodado por pessoas não convidadas, não ser seguido, vigiado ou monitorado
C) O direito ao respeito pela vida privada e familiar de uma pessoa, seu lar e sua correspondência pessoal
D) O direito à liberdade de opinião e expressão e o direito a buscar, receber e divulgar informações

A) Incorreto. Esta é uma definição de proteção dos dados.
B) Incorreto. Esta é uma definição de privacidade física. Contudo, o GDPR não diz respeito à privacidade física.
C) Correto. Esta é a definição empregada de modo implícito ao longo do GDPR. (Literatura: A, Capítulo 1)
D) Incorreto. Esta é uma versão resumida do Artigo 19 da Declaração Universal de Direitos Humanos: liberdade de opinião e expressão.

12 / 40
Qual é a relação entre privacidade e proteção de dados?

A) Proteção de dados e privacidade são sinônimos e têm o mesmo significado.
B) Proteção de dados é a parte da privacidade que protege a integridade física de um indivíduo.
C) Proteção de dados refere-se às medidas necessárias para proteger a privacidade de um indivíduo.

A) Incorreto. A proteção dos dados ajuda a proteger a privacidade de um indivíduo, mas os termos não são sinônimos.
B) Incorreto. A proteção de dados não está relacionada à integridade física ou à privacidade física.
C) Correto. A proteção de dados consiste em algumas medidas necessárias para proteger a privacidade de um indivíduo. (Literatura: A, Capítulo 1)

13 / 40
Qual é a situação jurídica do GDPR?

A) O GDPR é uma lei funcional em todos os estados membros da Área Econômica Europeia (AEE). Alguns artigos permitem que a legislação dos estados membros forneça regras mais específicas.
B) O GDPR é uma recomendação da Comissão Europeia para que as autoridades legais dos países da AEE melhorem suas leis sobre proteção de dados pessoais.
C) O GDPR estabelece condições e requisitos mínimos. Os estados membros devem aprovar leis nacionais que atendam a estes requisitos mínimos.

A) Correto. O GDPR é uma lei europeia, mas o Regulamento não exclui uma legislação dos estados membros que estabeleça as circunstâncias para situações de processamento específicas. (Literatura: A, Capítulo 1; Item 10 do Preâmbulo do GDPR)
B) Incorreto. Uma recomendação da UE não é obrigatória. O GDPR é uma lei europeia funcional em todos os estados membros.
C) Incorreto. Esta é a descrição de uma Diretiva da UE.

14 / 40
No GDPR, alguns tipos de dados pessoais são considerados como dados pessoais de categoria especial.

Quais dados pessoais são considerados como dados pessoais de categoria especial?

A) Uma lista de pagamentos efetuados usando um cartão de crédito
B) Uma lista de endereços dos membros de um partido político
C) Um registro genealógico dos ancestrais de uma pessoa

A) Incorreto. Dados de cartão de crédito são dados pessoais, mas não dados de categoria especial.
B) Correto. Dados pessoais que revelem opiniões políticas constituem dados pessoais especiais. (Literatura: A, Capítulo 1; Artigo 9(1) do GDPR)
C) Incorreto. Informações genealógicas de pessoas vivas constituem dados pessoais, mas não de categoria especial. O GDPR não é aplicável aos dados de pessoas falecidas.

15 / 40
Para planejar o tamanho da área de estacionamento necessária, um governo local monitora e salva o número da placa de cada carro que entra e sai do centro da cidade. Foi obtida uma permissão para coletar dados sobre o número de carros presentes no centro da cidade.

Pela comparação dos horários de entrada e saída para as placas, é calculado o número de carros presentes a cada momento de cada dia. A cada mês é gerado um relatório detalhando o número médio de carros presentes no centro da cidade em momentos específicos para cada dia da semana. Em todas as entradas no centro da cidade, um cartaz explica com clareza quais dados são coletados por quem, a finalidade do processamento e o fato de que os números das placas serão armazenados em segurança por até dois anos, porque as medidas serão repetidas no ano seguinte.

Que princípio básico do processamento legítimo de dados pessoais está sendo **violado** neste caso?

A) Os dados pessoais devem ser coletados para finalidades especificadas, explícitas e legítimas e não devem ser processados adicionalmente.
B) Os dados pessoais devem ser mantidos de modo que permita a identificação dos titulares dos dados por um período não maior que o necessário.
C) Os dados pessoais devem ser processados de modo que garanta a segurança apropriada dos dados pessoais.
D) Os dados pessoais devem ser processados de modo transparente em relação ao titular dos dados.

A) Incorreto. O governo local está autorizado a coletar dados sobre o número de carros presentes.
B) Correto. Nessa situação, não há necessidade de reter os dados de um carro específico, identificando o proprietário, após ele ter deixado a área. (Literatura: A, Capítulo 2; Artigo 5 do GDPR)
C) Incorreto. Essa situação não sugere uma segurança inadequada.
D) Incorreto. O processamento está ocorrendo de um modo transparente, pois é comunicado adequadamente aos titulares dos dados.

16 / 40
Os dados pessoais devem ser adequados, relevantes e limitados ao que for necessário em relação às finalidades para as quais são processados.

Que princípio do processamento de dados é descrito aqui?

A) Exatidão
B) Minimização de dados
C) Equidade e transparência
D) Limitação de finalidade

A) Incorreto. Exatidão é o princípio pelo qual os dados pessoais devem ser exatos e atualizados.
B) Correto. Minimização de dados significa que os dados pessoais devem ser adequados, relevantes e limitados ao que for necessário. (Literatura: A, Capítulo 2; Artigo 5(1) do GDPR)
C) Incorreto. Equidade e transparência significam que os dados pessoais devem ser processados de um modo legal, imparcial e transparente em relação ao titular dos dados.
D) Incorreto. Limitação das finalidades significa que os dados pessoais devem ser coletados para finalidades especificadas, explícitas e legítimas e não devem ser processados adicionalmente de um modo incompatível com essas finalidades; o processamento adicional para fins de arquivamento por interesse público, fins de pesquisa científica ou histórica ou fins estatísticos, de acordo com o Artigo 89(1) do GDPR, não deve ser considerado incompatível com as finalidades iniciais.

17 / 40
Um indivíduo está se mudando da cidade A para a cidade B, em um estado membro da Área Econômica Europeia (AEE). Na cidade A, ele era um paciente do hospital local A. Na cidade B, passa a ser um paciente do hospital B. O paciente optou pela não inclusão no sistema nacional de prontuários eletrônicos de pacientes.

O paciente solicita que o hospital A encaminhe seu prontuário médico diretamente ao hospital B.

De acordo com o GDPR, o que é permitido?

A) O hospital em A pode enviar os dados diretamente ao hospital B, como solicitado pelo paciente.
B) O hospital em A pode enviar o prontuário ao hospital B, antes que seja solicitado pelo paciente.
C) O hospital em A pode enviar o prontuário médico ao titular dos dados, mas não a outro hospital.
D) O hospital em A não pode enviar o prontuário porque não há uma base legítima para o processamento.

A) Correto. O direito à portabilidade permite isso. (Literatura: A, Capítulo 3)
B) Incorreto. O hospital em B só pode adquirir o prontuário de A com o consentimento ou se for de interesse vital para o titular dos dados e o consentimento não puder ser obtido.
C) Incorreto. O titular dos dados pode pedir que os dados sejam enviados diretamente.
D) Incorreto. Uma solicitação do titular dos dados, que implica consentimento, constitui uma base legítima suficiente.

18 / 40
Uma empresa tem planos para processar dados pessoais. O Data Protection Officer (DPO) recentemente indicado executa uma Avaliação de Impacto sobre a Proteção de Dados (DPIA). O DPIA constata que todos os computadores têm uma configuração que faz os monitores exibirem um protetor de tela após cinco segundos de inatividade. Contudo, os computadores não são bloqueados automaticamente. Quando os funcionários deixam sua mesa, geralmente também não bloqueiam seus computadores.

Isso é um exemplo de quê?

A) Acesso a dados
B) Violação de dados pessoais
C) Incidente de segurança
D) Vulnerabilidade da segurança

A) Incorreto. Os dados não foram acessados.
B) Incorreto. Nenhum dado pessoal foi processado sem autorização até o momento; portanto, isto não é uma violação.
C) Incorreto. O processamento ainda vai ser iniciado; não há motivos para supor que um incidente tenha ocorrido.
D) Correto. A confidencialidade dos dados não pode ser garantida se os funcionários deixarem suas estações de trabalho sem bloquear o computador. (Literatura: A, Capítulo 2; Artigo 5(1)(f) do GDPR)

19 / 40
O GDPR refere-se aos princípios de proporcionalidade e subsidiariedade.

Qual é o significado de subsidiariedade neste contexto?

A) Dados pessoais só podem ser processados de acordo com a especificação da finalidade.
B) Dados pessoais não podem ser reutilizados sem um consentimento explícito e informado.
C) Dados pessoais só podem ser processados quando não houver outros meios para obter a finalidade.
D) Dados pessoais devem ser adequados, relevantes e não excessivos em relação às finalidades.

A) Incorreto. Essa é uma das limitações legais.
B) Incorreto. Essa é uma das limitações legais.
C) Correto. Essa é a definição de subsidiariedade. (Literatura: A, Capítulo 3; Artigo 35(7) do GDPR)
D) Incorreto. Essa é a definição de proporcionalidade.

20 / 40
"O controlador deve implementar medidas técnicas e organizacionais apropriadas para garantir que (...) sejam processados somente os dados pessoais que sejam necessários para cada finalidade específica do processamento."

Que termo do GDPR é definido aqui?

A) Conformidade
B) Proteção de dados desde a concepção (by design) e por padrão (by default)
C) Proteção de dados incorporada

A) Incorreto. Conformidade significa cumprir regras ou normas.
B) Correto. Como padrão, o mínimo de dados pessoais deve ser processado durante o período mais curto possível, usando as melhores medidas de segurança possíveis para prevenir um acesso não autorizado. A proteção de dados desde a concepção refere-se a um processamento que inclua medidas apropriadas para implementar os princípios de proteção de dados. (Literatura: A, Capítulo 8; Artigo 25 do GDPR)
C) Incorreto. Proteção de dados incorporada é o resultado da proteção desde a concepção.

21 / 40
Durante a realização de um backup, ocorreu uma falha no disco rígido do servidor de dados. Tanto os dados quanto o backup são perdidos. O disco continha dados pessoais, mas nenhum dado pessoal de categoria especial.

O processador afirma que isto constitui uma violação de dados pessoais.

A afirmação do processador é verdadeira?

A) Sim, porque os dados pessoais no disco foram processados de modo ilegal.
B) Sim, porque não havia dados pessoais de categoria especial armazenados no disco.
C) Não, porque nenhum dado pessoal no disco foi processado, apenas destruído.
D) Não, porque isto é apenas um incidente de segurança, e não uma violação de dados.

A) Correto. A perda irrecuperável de dados pessoais é considerada como uma violação de segurança que provoca a destruição ilegal de dados pessoais, o que também faz com que represente uma violação de dados pessoais. (Literatura: A, Capítulo 5; Artigo 4(12) do GDPR)
B) Incorreto. A perda acidental de dados constitui um incidente de segurança (os dados já não estão disponíveis). De acordo com o GDPR, isto também representa um processamento ilegal de dados pessoais e, portanto, uma violação de dados pessoais. Os dados não precisam pertencer à categoria de dados pessoais especiais para que sejam enquadrados na categoria de violação de dados pessoais.
C) Incorreto. Uma falha técnica que faça com que os dados deixem de estar disponíveis constitui um incidente de segurança. O GDPR considera uma perda acidental de dados pessoais como um processamento ilegal (não por instrução do controlador ou do processador) e, portanto, como uma violação de dados pessoais.
D) Incorreto. Dados pessoais perdidos de modo irrecuperável são considerados pelo GDPR como um processamento não autorizado, portanto, uma violação de dados pessoais. O fato de que os dados foram destruídos acidentalmente também faz com que este evento seja um incidente de segurança.

22 / 40
As organizações têm a obrigação de manter diversos registros para demonstrar conformidade com o GDPR.

Qual registro **não** é obrigatório de acordo com o GDPR?

A) Um registro de todo o processamento pretendido, juntamente com a(s) finalidade(s) do processamento e as justificativas legais
B) Um registro de violações de dados com todas as características relevantes, incluindo notificações
C) Um registro das notificações enviadas à autoridade supervisora, relativas ao processamento de dados pessoais
D) Um registro de processadores, incluindo os dados pessoais fornecidos e o período pelo qual estes dados podem ser retidos

A) Incorreto. Deve ser mantido um registro de todo o processamento pretendido, com a(s) finalidade(s) e justificativas legais.
B) Incorreto. Deve ser mantido um registro de violações de dados.
C) Correto. Uma consulta prévia sobre um processamento de alto risco é obrigatória, mas não há necessidade de um registro separado das notificações enviadas. (Literatura: A, Capítulo 6; Artigo 36(1) do GDPR)
D) Incorreto. Deve ser mantido um registro de processadores e dados fornecidos.

23 / 40
Houve uma violação de dados pessoais e o controlador está redigindo uma notificação à autoridade supervisora. As seguintes informações já constam da notificação:

- A natureza da violação de dados pessoais e suas possíveis consequências.
- Informações sobre as partes que podem fornecer mais informações sobre a violação dos dados.

Que outras informações o controlador deve fornecer?

A) A informação de que as autoridades locais e nacionais foram notificadas da violação dos dados
B) O nome e os detalhes de contato dos titulares dos dados que possam ter tido seus dados violados
C) As medidas sugeridas para mitigar as consequências adversas da violação de dados
D) As informações necessárias para acessar os dados pessoais que foram violados

A) Incorreto. A autoridade supervisora deve ser informada de relatos a autoridades supervisoras de outros países da Área Econômica Europeia (AEE). Relatos a autoridades locais, por exemplo, a polícia, não precisam ser notificados.
B) Incorreto. A autoridade supervisora requer uma estimativa do número de titulares de dados envolvidos, não seus dados pessoais.
C) Correto. O controlador deve acrescentar as medidas sugeridas para mitigar as consequências adversas da violação dos dados. (Literatura: A, Capítulo 7; Artigo 33(d) do GDPR)
D) Incorreto. A autoridade supervisora precisa conhecer o tipo de dados pessoais envolvido, mas não precisa ter acesso aos dados em si.

24 / 40
De acordo com o Artigo 33 do GDPR, o controlador deve notificar uma violação de dados pessoais à autoridade supervisora sem demora injustificada e, quando possível, no máximo 72 horas após tomar ciência do fato.

Qual é a sanção máxima para o descumprimento desta obrigação de notificar?

A) € 10.000.000 ou 2% do volume global anual de negócios, o que for maior
B) € 20.000.000 ou 4% do volume global anual de negócios, o que for maior
C) Até € 500.000 com um mínimo de € 120.000
D) Até € 820.000 com um mínimo de € 350.000

A) Correto. Este é o valor máximo, de acordo com o GDPR, para uma infração da obrigação de notificar de violação de dados pessoais. (Literatura: A, Capítulo 7; Artigo 33 do GDPR)
B) Incorreto. Esta é a multa aplicada para descumprimento ou não conformidade com os princípios básicos de processamento, incluindo as condições para o consentimento.
C) Incorreto. Este é um valor desatualizado, baseado no Código penal Holandês. As regras do GDPR especificam multas mais altas.
D) Incorreto. Este é um valor desatualizado, baseado no Código penal Holandês. As regras do GDPR especificam multas mais altas.

25 / 40
De acordo com o GDPR, qual é uma tarefa da autoridade supervisora?

A) Implementar medidas técnicas e organizacionais para garantir a conformidade
B) Investigar violações de segurança de informações corporativas
C) Monitorar e impor a aplicação do GDPR

A) Incorreto. Esta é a tarefa do controlador.
B) Incorreto. Apenas violações de dados pessoais interessam à autoridade supervisora.
C) Correto. Esta é a principal tarefa da autoridade supervisora. (Literatura: A, Capítulo 7)

26 / 40
Uma empresa belga tem sua sede na França por motivos fiscais. Ela firma um contrato juridicamente vinculante com um processador nos Países Baixos para o processamento de dados pessoais de titulares dos dados de várias nacionalidades.

Ocorre uma violação de dados pessoais. A autoridade supervisora inicia uma investigação.

Por que a autoridade supervisora francesa é considerada como a autoridade supervisora principal?

A) Porque a França está localizada no meio da Europa
B) Porque a França é o maior dos três países da Área Econômica Europeia (AEE)
C) Porque a sede da empresa está na França

A) Incorreto. A posição geográfica dos países é irrelevante.
B) Incorreto. O tamanho dos países é irrelevante.
C) Correto. O país do estabelecimento principal determina a autoridade supervisora principal. O estabelecimento principal é o local da administração central da organização ou, em outras palavras, sua sede. (Literatura: A, Capítulo 7)

27 / 40
Em 10 de julho de 2023 a Comissão Europeia implementou uma disposição regulamentar relativa à transferência de dados pessoais entre a Área Econômica Europeia (AEE) e os Estados Unidos da América (EUA). A disposição regulamentar é baseada nas medidas para proteção de dados descritas no Framework de Privacidade de Dados UE-EUA.

Que tipo de disposição é essa?

A) Decisão de adequação
B) Exceção
C) Contrato juridicamente vinculante
D) Tratado que substitui o GDPR

A) Correto. A disposição regulamentar constitui uma decisão de adequação relativa ao processamento em terceiros países. (Literatura: A, Capítulo 7; Artigo 45 e Itens (104) e (106) do preâmbulo do GDPR)
B) Incorreto. Uma exceção é usada para situações específicas nas quais uma transferência seja necessária, mas não exista uma disposição que permita isso. (Literatura: Artigo 49(1)(d) do GDPR)
C) Incorreto. A disposição regulamentar constitui uma decisão de adequação. Um contrato juridicamente vinculante é estabelecido entre um processador e um controlador.
D) Incorreto. A disposição regulamentar constitui uma decisão de adequação. Ela não substitui o GDPR.

28 / 40
Um controlador deseja terceirizar o processamento de dados pessoais para um processador.

O que deve ser realizado **antes** da terceirização?

A) O controlador deve pedir permissão à autoridade supervisora para terceirizar o processamento dos dados.
B) O controlador deve perguntar à autoridade supervisora se o contrato por escrito combinado está em conformidade com os regulamentos.
C) O controlador e o processador devem preparar uma minuta e assinar um contrato por escrito garantindo a confidencialidade dos dados.
D) O processador deve demonstrar ao controlador que todas as demandas acordadas no acordo de nível de serviço (ANS) são cumpridas.

A) Incorreto. O controlador não precisa pedir a permissão da autoridade supervisora para cada caso de terceirização.
B) Incorreto. A autoridade supervisora não é um advogado ou departamento jurídico e não verifica a conformidade de contratos.
C) Correto. Deve haver um contrato por escrito garantindo a confidencialidade dos dados, listando os objetivos e os métodos de processamento do modo definido pelo controlador e especificando que o processador conduzirá o processamento unicamente conforme as instruções do controlador. As duas partes devem assinar este contrato. (Literatura: A, Capítulo 8; Artigo 28(3) do GDPR)
D) Incorreto. Um ANS não é suficiente porque ele focará nas operações, não necessariamente nos objetivos.

29 / 40
Qual é o objetivo de uma auditoria de proteção de dados pela autoridade supervisora?

A) Aconselhar o controlador sobre a mitigação de riscos à privacidade para proteger o controlador de pedidos de indenização de responsabilidade civil por não conformidade
B) Atender a obrigação no GDPR de implementar medidas técnicas e organizacionais apropriadas para proteção de dados
C) Monitorar e impor a aplicação do GDPR, determinando se o processamento está sendo realizado em conformidade com o GDPR

A) Incorreto. A autoridade supervisora tem a tarefa de monitorar a conformidade e aconselhar sobre aprimoramentos, mas seu objetivo não é proteger o controlador.
B) Incorreto. A auditoria não constitui a implementação das medidas, e sim uma avaliação de sua eficácia.
C) Correto. De acordo com o GDPR, esta é uma tarefa importante da autoridade supervisora. (Literatura: A, Capítulo 7; Artigo 57(1)(a) do GDPR)

30 / 40
Para que um processamento de dados pessoais seja legal, o que **sempre** será exigido?

A) Um código de conduta deve ser estabelecido, descrevendo exatamente o que o processamento envolve.
B) O processamento deve relatado e autorizado pela autoridade supervisora.
C) Deve haver uma base legítima para o processamento de dados pessoais.

A) Incorreto. Códigos de conduta podem representar um modo de harmonizar contratos entre o controlador e o processador.
B) Incorreto. Uma consulta prévia é obrigatória somente quando uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) indicar um alto risco. (Artigo 36 do GDPR)
C) Correto. O processamento só é legal quando existir uma finalidade legítima. (Literatura: A, Capítulo 3; Artigo 6 do GDPR)

31 / 40
Dados pessoais podem ser transferidos para fora da Área Econômica Europeia (AEE).

De acordo com o GDPR, que transferências para fora da AEE são sempre legais?

A) Transferências baseadas nas leis do país não pertencente à AEE envolvido
B) Transferências sujeitas às regras da Organização Mundial do Comércio (OMC)
C) Transferências governadas por regras corporativas vinculantes (BCR) aprovadas
D) Transferências dentro de uma corporação ou organização global

A) Incorreto. Isto também exigiria um parecer de adequação, confiando que essas leis são suficientes.
B) Incorreto. A OMC abrange apenas o livre comércio de bens e serviços.
C) Correto. BCR aprovadas pela autoridade supervisora envolvida tornam a transferência legal. (Literatura: A, Capítulo 7; Artigo 47 do GDPR)
D) Incorreto. Isso também exigiria a adoção de BCR oficiais.

32 / 40
De acordo com o GDPR, qual seria uma descrição de regras corporativas vinculantes (BCR)?

A) Uma decisão sobre a segurança da transferência de dados pessoais para um país fora da Área Econômica Europeia (AEE)
B) Uma medida para compensar a ausência de proteção de dados em um país terceiro
C) Um conjunto de acordos abordando transferências de dados pessoais entre países situados fora da AEE
D) Um conjunto de regras aprovadas sobre a proteção de dados pessoais, usadas por um grupo de empresas

A) Incorreto. Isso se refere às decisões de adequação.
B) Incorreto. Isso se refere às salvaguardas apropriadas.
C) Incorreto. O GDPR não abrange acordos entre países não pertencentes à AEE.
D) Correto. BCR constituem um conjunto de regras aprovadas pelas autoridades supervisoras. (Literatura: A, Capítulo 3; Artigo 47 do GDPR)

33 / 40
Um contrato por escrito entre um controlador e um processador é chamado de acordo de processamento.

De acordo com o GDPR, o que **não** precisa ser abordado no contrato por escrito?

A) O código de ética comercial e conduta da contratada que será utilizado
B) Os procedimentos para violações de segurança das informações e de dados pessoais
C) As medidas técnicas e organizacionais implementadas
D) Quais dados são cobertos pelo acordo de processamento de dados

A) Correto. Embora o GDPR endosse o uso de códigos de conduta e certificação, não é obrigatório incluir esta cláusula para demonstrar a conformidade com o GDPR. (Literatura: A, Capítulo 8; Artigo 28(3) do GDPR)
B) Incorreto. Isso é obrigatório porque descreve as obrigações do processador em relação à notificação de uma violação de dados pessoais (pelo controlador) à autoridade supervisora.
C) Incorreto. Isso é obrigatório porque descreve as medidas técnicas e organizacionais que devem ser adotadas pelo processador.
D) Incorreto. Isso é obrigatório porque descreve os dados pessoais, incluindo dados pessoais de categoria especial, cobertos pelo contrato.

34 / 40
Um dos objetivos de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) é fortalecer a confiança dos clientes ou cidadãos no modo como os dados pessoais são processados e a privacidade é respeitada.

Como um DPIA pode fortalecer a confiança?

A) A organização minimiza o risco de ajustes dispendiosos dos processos ou remodelamento dos sistemas em um estágio mais tardio.
B) A organização previne a não conformidade com o GDPR e minimiza o risco de multas.
C) A organização prova que considera a privacidade com seriedade e visa à conformidade com o GDPR.

A) Incorreto. Este aspecto pode fortalecer a confiança da gerência, mas não de clientes ou cidadãos.
B) Incorreto. A prevenção de multas pode fortalecer a confiança da gerência, mas não de clientes ou cidadãos.
C) Correto. A realização de um DPIA mostra aos clientes ou cidadãos que a empresa leva a proteção de dados a sério. (Literatura: A, Capítulo 8)

35 / 40
Um dos sete princípios da proteção de dados desde a concepção (by design) é a *Funcionalidade – Soma Positiva, Diferente de Zero*.

Qual é a essência deste princípio?

A) As normas de segurança aplicadas devem garantir a confidencialidade, a integridade e a disponibilidade dos dados pessoais durante todo o seu ciclo de vida.
B) Se diferentes tipos de objetivos legítimos forem contraditórios, os objetivos de privacidade devem ter prioridade em relação a outros objetivos de segurança.
C) Ao incorporar a privacidade em uma determinada tecnologia, processo ou sistema, isto deve ser realizado de tal modo que a funcionalidade completa não seja prejudicada.
D) Sempre que possível, avaliações detalhadas de impacto na privacidade e riscos devem ser realizadas e publicadas, documentando com clareza os riscos para a privacidade.

A) Incorreto. Este é um aspecto da Segurança de Ponta-a-Ponta – Proteção do Ciclo de Vida, um dos outros seis princípios básicos.
B) Incorreto. A proteção de dados desde a concepção rejeita a ideia de que a privacidade compete com outros interesses, objetivos do projeto e capacidades técnicas.
C) Correto. Esta é a essência. (Literatura: A, Capítulo 8; Artigo 25 do GDPR)
D) Incorreto. Este é um aspecto da Privacidade Incorporada ao Design, um dos outros seis princípios básicos.

36 / 40
Uma empresa deseja utilizar os dados pessoais de seus clientes. Ela pretende começar a enviar um informativo personalizado a todas as clientes do sexo feminino.

Que direito todos os titulares dos dados terão nesta situação?

A) O direito à compensação
B) O direito de se opor à definição de perfis
C) O direito à retificação

A) Incorreto. É improvável que todos os titulares dos dados sofram um prejuízo que deva ser compensado nessa situação.
B) Correto. Todos os titulares dos dados têm direito de se opor ao processamento de dados pessoais para marketing direto, incluindo a definição de perfis. Isto claramente constitui uma definição de perfis. (Literatura: A, Capítulo 4)
C) Incorreto. É improvável que a empresa tenha dados incorretos sobre todos os titulares de dados. Portanto, o direito à retificação não é aplicável.

37 / 40
Qual seria uma descrição de proteção de dados desde a concepção (by design) e como padrão (by default)?

A) Uma abordagem que implementa a proteção dos dados desde o início.
B) Uma indicação de prazos se o processamento estiver relacionado ao apagamentos.
C) Os dados só podem ser coletados para finalidades explícitas e legítimas.
D) Não manter mais dados que o estritamente necessário para o processamento.

A) Correto. Esta é a descrição correta. (Literatura: A, Capítulo 8; Artigo 25(1) do GDPR)
B) Incorreto. Esta é a descrição de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA).
C) Incorreto. Esta é uma descrição de medidas adotadas para conformidade com o princípio de limitação de finalidade.
D) Incorreto. Esta é uma descrição dos procedimentos usados para conformidade com o princípio de minimização de dados.

38 / 40
De acordo com o GDPR, quando uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) é obrigatória?

A) Quando um projeto incluir tecnologias ou processos que utilizem dados pessoais
B) Quando for provável que o processamento cause um alto risco para os direitos dos titulares dos dados
C) Quando operações de processamento semelhantes com riscos comparáveis forem repetidas

A) Incorreto. O DPIA é obrigatório apenas para tecnologias e processos que tenham a probabilidade de gerar um alto risco para os direitos dos titulares dos dados.
B) Correto. Para operações de processamento que tenham a probabilidade de gerar um alto risco, um DPIA é obrigatório para avaliar esses riscos e projetar medidas de mitigação. (Literatura: A, Capítulo 6; Artigo 35 do GDPR)
C) Incorreto. Esse é um caso em que o DPIA não precisa ser repetido.

39 / 40
O GDPR descreve o princípio de minimização de dados.

Como as organizações podem obedecer a esse princípio?

A) Aplicando o conceito de privilégio mínimo aos dados pessoais coletados, armazenados ou de outro modo processados.
B) Limitando o direito de acesso às pessoas que precisarem dos dados pessoais para as operações de processamento pretendidas.
C) Limitando os tamanhos dos arquivos, salvando todos os dados pessoais processados no menor formato possível.
D) Limitando os dados pessoais àquilo que for adequado, relevante e necessário para os objetivos do processamento.

A) Incorreto. A minimização dos dados não aborda o privilégio mínimo.
B) Incorreto. Isso descreve o conceito de limite de autorização, por exemplo, para obedecer ao princípio de integridade e confidencialidade.
C) Incorreto. De acordo com o GDPR, a minimização dos dados não envolve o tamanho do armazenamento, e sim a redução do uso de dados pessoais a um mínimo.
D) Correto. Essa é a essência da descrição no GDPR. (Literatura: A, Capítulo 2; Artigo 5(1)(c) do GDPR)

40 / 40
Qual é a **principal** utilização de um cookie persistente?

A) Garantir que os dados pessoais do usuário sejam armazenados com segurança no servidor
B) Personalizar a experiência do usuário do site durante uma próxima visita
C) Registrar cada tecla pressionada por um usuário computador para descobrir senhas
D) Salvar as páginas que um usuário marcar como favoritas no histórico do navegador do usuário

A) Incorreto. Cookies não são usados para armazenar dados no servidor.
B) Correto. Essa é a principal finalidade de um cookie persistente. (Literatura: A, Capítulo 8)
C) Incorreto. Os cookies não são maliciosos por natureza, porém o mecanismo pode ser explorado de um modo malicioso.
D) Incorreto. Os favoritos e o histórico do navegador são salvos, mas não em um cookie.

Avaliação

A tabela a seguir mostra as respostas corretas às questões apresentadas neste exame simulado.

Questão	Resposta	Questão	Resposta
1	C	**21**	A
2	D	**22**	C
3	A	**23**	C
4	A	**24**	A
5	B	**25**	C
6	B	**26**	C
7	A	**27**	A
8	B	**28**	C
9	D	**29**	C
10	C	**30**	C
11	C	**31**	C
12	C	**32**	D
13	A	**33**	A
14	B	**34**	C
15	B	**35**	C
16	B	**36**	B
17	A	**37**	A
18	D	**38**	B
19	C	**39**	D
20	B	**40**	B

Contato EXIN

www.exin.com