Exame simulado

Edição 202601

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 esse exame.

Esse exame contém 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 nesse exame é 40. Cada resposta correta vale 1 ponto. Você precisa de 26 pontos ou mais para passar no exame.

O tempo permitido para esse exame é de 60 minutos.

Boa Sorte!

Exame simulado

1 / 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.

2 / 40
No sistema jurídico da União Europeia (UE), diferentes ferramentas são utilizadas para atingir vários objetivos. Algumas dessas ferramentas são vinculativas, enquanto outras permitem que os Estados-Membros da UE decidam como utilizá-las, oferecendo-lhes flexibilidade.

O GDPR permite essa flexibilidade?

A) Sim, porque se trata de uma diretiva que estabelece objetivos para os Estados-Membros da UE e define medidas nacionais.
B) Sim, porque é uma recomendação que dá conselhos sem outras obrigações jurídicas específicas.
C) Não, porque é uma decisão vinculativa apenas para partes específicas e não para todos os Estados-Membros da UE.
D) Não, porque é um regulamento que se aplica a todos os Estados-Membros da UE e é diretamente aplicável.

3 / 40
Como o GDPR define dados pessoais?

A) Qualquer informação relacionada a um residente do Espaço Econômico Europeu (EEE)
B) Qualquer informação relativa a uma pessoa física identificada ou identificável
C) Dados diretamente relacionados a uma pessoa física identificada ou identificável
D) Dados que revelem as origens raciais ou étnicas de uma pessoa, suas crenças religiosas, condições de saúde, vida sexual ou orientação sexual

4 / 40
De acordo com o GDPR, qual é a definição de tratamento de dados pessoais?

A) Qualquer operação que possa ser realizada com dados pessoais
B) Qualquer operação que possa ser realizada com dados pessoais, exceto exclusão e destruição
C) Apenas operações nas quais os dados pessoais sejam compartilhados ou transferidos de qualquer modo
D) Apenas operações nas quais os dados pessoais sejam usados para as finalidades para as quais foram coletados

5 / 40
O GDPR define alguns dados pessoais como dados de categoria especial, por vezes denominados ”dados sensíveis”.

Qual é um exemplo desse tipo de dado?

A) Uma coleta de endereços de e-mail profissionais de funcionários
B) Um registro genealógico dos ancestrais de uma pessoa
C) Uma lista de pagamentos efetuados com um cartão de crédito
D) Uma lista de endereços dos membros de um partido político

6 / 40
Uma das funções descritas no GDPR é definida como:

Uma pessoa física ou jurídica, autoridade pública, agência ou outro órgão que, isoladamente ou em conjunto com outras partes, determina as finalidades e os meios de tratamento de dados pessoais.

Qual função é definida aqui?

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

7 / 40
O tratamento de dados pessoais deve ser legal. Uma empresa coleta dados pessoais de seus clientes.

O que é **sempre** necessário para um tratamento legal ao se coletar dados pessoais?

A) Pedir permissão à autoridade supervisora para o tratamento
B) Documentar uma base legal para o tratamento dos dados pessoais
C) Implementar um código de conduta descrevendo a natureza do tratamento

8 / 40
De acordo com o GDPR, o controlador deve manter um registro de todas as atividades de tratamento.

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

A) Um registro de todas as medidas técnicas e organizacionais implementadas de todos os operadores
B) Um registro de todo o tratamento pretendido, juntamente com as finalidades do tratamento e as justificativas legais
C) Um registro de violações de dados com todas as características relevantes, incluindo notificações

9 / 40
Um dos sete princípios da proteção de dados desde a concepção (by design) é a *funcionalidade total – soma positiva, não soma igual a zero*.

Qual é a essência desse princípio?

A) A proteção de dados coexiste com a segurança para criar uma situação vantajosa para todos, que acomoda legítimos interesses juntamente com a privacidade.
B) A proteção de dados inclui informar os titulares dos dados sobre as formas como seus dados são tratados, o que ajuda os titulares dos dados a manter o controle.
C) A proteção de dados está incorporada na arquitetura e no design dos sistemas, o que a torna uma funcionalidade essencial.

10 / 40
Qual é uma descrição de proteção de dados desde a concepção (by design) e por padrão (by default)?

A) Uma abordagem que implementa a proteção de dados desde o desenvolvimento
B) Uma indicação de prazos caso o tratamento esteja relacionado a apagamento
C) Os dados só podem ser coletados para finalidades explícitas e legítimas
D) Não manter mais dados do que o estritamente necessário para o tratamento

11 / 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. Pela comparação dos horários de entrada e saída das placas, é calculado o número de carros presentes a cada momento de cada dia.

Foi obtida uma permissão para coletar dados sobre o número de carros presentes no centro da cidade. 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 tratamento e o fato de que os números das placas serão armazenados em segurança por até dois anos, porque as medições serão repetidas no ano seguinte.

Qual princípio básico do tratamento legal de dados pessoais é **violado** nesse cenário?

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

12 / 40
Após o cumprimento do objetivo original, o tratamento 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 tratamento 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

13 / 40
Uma organização fornece sua declaração de privacidade em vários idiomas e formatos, incluindo online, impresso e em áudio, para garantir que todos os titulares dos dados possam acessá-la e compreendê-la.

Qual direito do GDPR essa prática apoia **mais** diretamente?

A) O direito ao apagamento, porque os titulares dos dados são auxiliados a compreender que têm o direito de excluir seus dados a qualquer momento.
B) O direito à oposição, pois os titulares dos dados podem se opor ao tratamento de forma melhor quando compreendem totalmente a declaração de privacidade.
C) O direito à restrição, pois os titulares dos dados são informados sobre os objetivos da empresa e as bases legais para o tratamento.
D) O direito à transparência das informações, comunicações e modalidades, porque os titulares dos dados são auxiliados a compreender o aviso de privacidade.

14 / 40
Qual 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.

15 / 40
Um indivíduo compra um terno e fornece à loja o consentimento para utilizar seu endereço de e-mail para publicidade. Quando chega em casa, ele pede que a loja apague todos os seus dados pessoais e pare de lhe enviar e-mails.

De acordo com o GDPR, o que a loja deve fazer?

A) A loja não deve excluir nenhum dado pessoal desse indivíduo, pois as informações sobre as vendas devem ser retidas.
B) A loja deve excluir todos os dados pessoais desse indivíduo para os quais a base legal é o consentimento.
C) A loja deve excluir os outros dados pessoais desse indivíduo, mas pode continuar a enviar e-mails.

16 / 40
Um indivíduo recebe regularmente ofertas de uma loja onde ele fez compras cinco anos atrás. Ele quer que a empresa pare de enviar ofertas e exclua seus dados pessoais.

Qual direito do titular dos dados esse indivíduo está exercendo?

A) O direito ao acesso
B) O direito à objeção
C) O direito à retificação
D) O direito à restrição do tratamento

17 / 40
Uma empresa utiliza inteligência artificial (IA) para analisar cartas de candidatura a empregos e decidir automaticamente se irá convidar os candidatos para uma entrevista.

Qual direito do GDPR é **mais** relevante para esse cenário?

A) O direito de não estar sujeito a uma decisão baseada exclusivamente em tratamento automatizado
B) O direito de apresentar uma reclamação a uma autoridade supervisora
C) O direito à restrição do tratamento
D) O direito à transparência das informações, comunicações e modalidades

18 / 40
Dados pessoais devem ser coletados para finalidades especificadas, explícitas e legais e não devem ser tratados adicionalmente de um modo incompatível com essas finalidades.

Qual princípio do tratamento de dados é descrito aqui?

A) Exatidão
B) Minimização de dados
C) Legalidade, lealdade e transparência
D) Limitação de finalidade

19 / 40
O GDPR descreve o princípio de minimização de dados.

Como as organizações podem estar em conformidade com esse princípio?

A) Aplicando o conceito de privilégio mínimo aos dados pessoais coletados, armazenados ou de outro modo tratados
B) Limitando os direitos de acesso aos funcionários que precisarem dos dados pessoais para as operações de tratamento pretendidas
C) Limitando os tamanhos dos arquivos, salvando todos os dados pessoais tratados no menor formato possível
D) Limitando os dados pessoais àquilo que for adequado, relevante e necessário para as finalidades do tratamento

20 / 40
O GDPR faz referência aos princípios de proporcionalidade e subsidiariedade.

O que **subsidiariedade** significa?

A) Os dados pessoais devem ser coletados para finalidades específicas, explícitas e legítimas e não devem ser tratados adicionalmente.
B) Os dados pessoais devem ser mantidos de modo que permita a identificação dos titulares dos dados por um período não maior do que o necessário.
C) Ao tratar dados pessoais, o controlador só recolherá os dados necessários para a finalidade.
D) Ao tratar dados pessoais, os meios utilizados devem infringir a privacidade o mínimo possível.

21 / 40
Qual é a finalidade da Gestão do Ciclo de Vida dos Dados (GCVD)?

A) Avaliar se os dados devem ser tratados como dados pessoais ou dados normais
B) Assegurar que os dados pessoais sejam excluídos assim que não houver mais base legal para retê-los
C) Gerenciar o fluxo de dados em uma empresa em conformidade com o GDPR

22 / 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 de computador para descobrir senhas
D) Salvar as páginas que um usuário marcar como favoritas no histórico de navegação do usuário

23 / 40
Uma instituição de caridade de resgate de gatos possui muitos doadores. Eles processam os dados pessoais desses doadores, a fim de manter registros tanto para fins fiscais quanto para doadores recorrentes. Todos os doadores deram o consentimento para esse tratamento.

A instituição de resgate de gatos deseja utilizar um sistema de inteligência artificial (IA) para agradecer automaticamente aos doadores recorrentes, enviando-lhes vídeos de seus gatos favoritos. O sistema de IA também enviará um e-mail aos doadores não recorrentes, informando que mais gatos precisam de ajuda e sugerindo doações mensais.

Qual princípio do GDPR é **especialmente** importante para esse sistema de IA?

A) Exatidão, porque a organização de resgate de gatos deve garantir que o sistema de IA associe adequadamente os vídeos de gatos aos doadores para obter os melhores resultados e aumentar as doações a longo prazo.
B) Anonimização, porque a organização de resgate de gatos deve garantir que o sistema de IA não tenha acesso a dados pessoais em um formato que torne os doadores reconhecíveis.
C) Legalidade, porque a organização de resgate de gatos não é um negócio, o que torna mais difícil encontrar um legítimo interesse para que o tratamento seja necessário e legal.
D) Transparência, porque a organização de resgate de gatos deve informar claramente os doadores sobre como seus dados são usados e dar a eles a chance de se oporem caso a finalidade original seja alterada.

24 / 40
Uma empresa utiliza inteligência artificial (IA) para otimizar seu processo de aprovação de empréstimos. Os requerentes de empréstimo preenchem um formulário online. O sistema de IA analisa essas informações e decide automaticamente se uma pessoa se qualifica para um empréstimo e quanto ela pode pegar emprestado. Esse processo é mais rápido e eficiente do que os métodos tradicionais, permitindo que a empresa processe um número maior de solicitações rapidamente, sem a necessidade de intervenção humana.

De acordo com o GDPR, o que essa empresa deve fazer?

A) Anonimizar os dados pessoais que a IA utiliza para garantir que os requerentes de empréstimo não possam ser identificados
B) Informar os requerentes de empréstimo sobre as decisões automatizadas e oferecer-lhes uma maneira fácil de solicitar uma revisão humana
C) Declarar claramente que os requerentes de empréstimo devem concordar com a IA tomando decisões automatizadas sem intervenção humana
D) Deixar de utilizar decisões automatizadas e voltar a utilizar decisões humanas para garantir os direitos dos requerentes de empréstimo

25 / 40
De acordo com o GDPR, quando contratos adicionais **não** são necessários para a transferência de dados pessoais?

A) Quando tanto o remetente quanto o destinatário se encontram no Espaço Econômico Europeu (EEE)
B) Quando o remetente criptografa os dados antes de enviá-los para outra empresa
C) Quando os dados não são considerados dados pessoais de categoria especial
D) Quando os dados são transferidos para fins jornalísticos ou artísticos

26 / 40
Uma empresa dentro do Espaço Econômico Europeu (EEE) deve elaborar regras corporativas vinculantes (BCR).

De acordo com o GDPR, qual é uma descrição de BCR?

A) Uma decisão sobre a segurança da transferência de dados pessoais para um país fora da EEE
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 EEE
D) Um conjunto de regras aprovadas sobre a proteção de dados pessoais usadas por um grupo de empresas

27 / 40
Um controlador deseja terceirizar o tratamento de dados pessoais para um operador.

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

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

28 / 40
Uma empresa multinacional está planejando transferir dados pessoais entre suas filiais localizadas em diferentes países, incluindo aqueles fora do Espaço Econômico Europeu (EEE). A empresa decide implementar regras corporativas vinculantes (BCR) para facilitar essas transferências.

Qual é um componente necessário dessas BCR?

A) As BCR devem garantir uma compensação financeira aos titulares dos dados em caso de violação de dados pessoais e especificar o montante.
B) As BCR devem incluir um mecanismo para garantir a conformidade com as regras por parte de todos os funcionários envolvidos no tratamento de dados.
C) As BCR devem descrever as medidas organizacionais e técnicas específicas utilizadas para proteger os dados pessoais durante as transferências.
D) As BCR devem especificar que todos os titulares dos dados devem ser notificados sobre cada transferência de dados pessoais de forma acessível.

29 / 40
Uma empresa pretende transferir dados pessoais para fora do Espaço Econômico Europeu (EEE).

De acordo com o GDPR, quais transferências para **fora** do EEE são sempre legais?

A) Transferências baseadas nas leis do país não pertencente ao EEE 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

30 / 40
Uma empresa na França possui regras corporativas vinculantes (BCR) para suas operações em todo o mundo. A empresa deseja transferir dados de clientes para um provedor terceirizado localizado nos Estados Unidos (EUA), com o qual não mantém uma operação conjunta. O provedor dos EUA não é certificado pelo Data Privacy Framework UE-EUA (DPF), mas assinou cláusulas contratuais padrão (SCCs) aprovadas pela Comissão Europeia (CE). Essas SCCs fazem parte de um contrato assinado com a empresa francesa.

Nos termos do GDPR, essa transferência de dados pessoais para o provedor dos EUA é legal?

A) Sim, porque o DPF foi declarado inválido.
B) Sim, porque o provedor dos EUA assinou as SCCs.
C) Não, porque transferências de dados para os EUA são proibidas.
D) Não, porque o provedor dos EUA deve assinar as BCR.

31 / 40
Uma cafeteria quer usar inteligência artificial (IA) e vigilância por vídeo para monitorar quantas xícaras de café os funcionários servem. O objetivo é entender quais são os horários mais movimentados da semana, monitorando a produtividade.

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

A) Sim, porque é provável que o tratamento resulte em um risco elevado aos direitos dos titulares dos dados.
B) Sim, porque o projeto inclui tecnologias de IA ou processos que utilizam dados pessoais.
C) Não, porque dados pessoais de categoria especial não são coletados durante o monitoramento.
D) Não, porque o objetivo não é avaliar diretamente a produtividade dos funcionários.

32 / 40
Durante a Avaliação de Impacto sobre a Proteção de Dados (DPIA), uma equipe que trabalha em uma plataforma online para crianças explora se o uso de avatares em vez de nomes reais atende às necessidades de funcionalidade.

Qual objetivo da DPIA é **mais** apoiado por essa ação?

A) Avaliar a necessidade e a proporcionalidade
B) Descrever o tratamento
C) Envolver as partes interessadas relevantes
D) Identificar e avaliar os riscos para os titulares dos dados

33 / 40
O GDPR estabelece os atributos mínimos de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA).

Qual é um desses atributos mínimos?

A) Um relatório detalhado sobre as responsabilidades e deveres do Data Protection Officer (DPO)
B) Uma revisão dos acordos de compartilhamento de dados da organização com terceiros
C) Uma avaliação das medidas de segurança tomadas para proteger as transferências de dados
D) Medidas para lidar com os riscos identificados aos direitos e liberdades dos titulares dos dados

34 / 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 de clientes e outros dados sensíveis da empresa.

O operador afirma que isso constitui uma violação de dados pessoais, de acordo com o GDPR.

A afirmação do operador é verdadeira?

A) Sim, porque os dados pessoais no disco do servidor foram tratados de modo ilegal.
B) Sim, porque os dados sensíveis da empresa também estavam no mesmo disco do servidor.
C) Não, porque os dados pessoais no disco não foram tratados, apenas destruídos.
D) Não, porque isso se trata apenas de uma violação de dados comum e não de uma violação de dados pessoais.

35 / 40
Uma empresa tem planos para tratar dados pessoais. O Data Protection Officer (DPO) recentemente indicado executa uma Avaliação de Impacto sobre a Proteção de Dados (DPIA). O DPO descobre 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 suas mesas, eles 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

36 / 40
Um arquiteto está saindo de uma construção. Ele coloca seu notebook no chão para atender o telefone. Um caminhão passa por cima do notebook. Todos os arquivos sobre o projeto da construção e os cálculos em que ele estava trabalhando são perdidos. Uma cópia de segurança de uma versão anterior dos arquivos está disponível na nuvem.

De acordo com o GDPR, isso constitui uma violação de dados pessoais?

A) Sim, porque a destruição da última cópia de um arquivo faz com que os dados não estejam disponíveis.
B) Sim, porque os arquivos destruídos eram arquivos pessoais do arquiteto.
C) Não, porque arquivos do projeto e cálculos não são dados pessoais.
D) Não, porque os arquivos ainda estão disponíveis na forma de uma cópia de segurança.

37 / 40
Após uma violação de dados pessoais, um controlador no Espaço Econômico Europeu (EEE) deve determinar quem deve ser informado:

- Ninguém
- Apenas a autoridade supervisora
- A autoridade supervisora e todos os titulares dos dados afetados

De acordo com o GDPR, em qual situação os **titulares dos dados** devem ser notificados de uma violação de dados pessoais?

A) Quando os dados pessoais forem tratados em uma unidade do operador que não esteja localizada dentro das fronteiras do EEE
B) Quando os dados pessoais forem tratados por uma parte que concordou com o contrato de tratamento, mas ainda não o assinou
C) Quando o sistema no qual os dados pessoais são tratados for atacado, causando uma avaria em seus dispositivos de armazenamento
D) Quando houver uma probabilidade considerável de que a violação provoque um risco elevado à privacidade dos titulares dos dados

38 / 40
Um sistema contendo dados pessoais foi invadido e foi constatado que pessoas não autorizadas tiveram acesso aos dados pessoais.

De acordo com o GDPR, o que o controlador deve fazer **antes** de notificar a autoridade supervisora?

A) Avaliar se dados pessoais de caráter sensível foram ou possam ter sido acessados
B) Conduzir uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) para determinar os riscos às pessoas físicas
C) Notificar os titulares dos dados envolvidos sobre a violação de dados pessoais e suas possíveis consequências
D) Notificar a polícia e relatar o acesso não autorizado ao(s) sistema(s)

39 / 40
As autoridades supervisoras têm determinadas tarefas que visam garantir o cumprimento do GDPR.

Qual é uma dessas tarefas?

A) Avaliar códigos de conduta para setores específicos em relação ao tratamento de dados pessoais
B) Definir um conjunto mínimo de medidas que devem ser adotadas para a proteção de dados pessoais e a privacidade
C) Redigir cláusulas contratuais padrão (SCCs) e regras corporativas vinculantes (BCR)
D) Investigar todas as violações de dados que tenham sido notificadas à autoridade supervisora

40 / 40
Um controlador tem sua sede no Espaço Econômico Europeu (EEE). Ele terceirizou o tratamento de dados pessoais sensíveis para um operador situado fora do EEE, sem consultar a autoridade supervisora antes. Essa transgressão foi descoberta e a empresa foi multada pela autoridade supervisora. Seis meses depois, a autoridade supervisora descobre que o controlador é culpado da mesma transgressão, mas para uma operação de tratamento diferente e com outro operador.

Qual é a multa **máxima** que a autoridade supervisora pode impor nesse caso?

A) Nada, porque a empresa já foi multada por essa transgressão
B) Nada, mas poderá ser emitida uma advertência formal sem penalidades financeiras.
C) Uma multa de até € 10 milhões ou 2% do faturamento da empresa, o que for maior
D) Uma multa de até € 20 milhões ou 4% do faturamento da empresa, o que for maior

Gabarito de respostas

1 / 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)

2 / 40
No sistema jurídico da União Europeia (UE), diferentes ferramentas são utilizadas para atingir vários objetivos. Algumas dessas ferramentas são vinculativas, enquanto outras permitem que os Estados-Membros da UE decidam como utilizá-las, oferecendo-lhes flexibilidade.

O GDPR permite essa flexibilidade?

A) Sim, porque se trata de uma diretiva que estabelece objetivos para os Estados-Membros da UE e define medidas nacionais.
B) Sim, porque é uma recomendação que dá conselhos sem outras obrigações jurídicas específicas.
C) Não, porque é uma decisão vinculativa apenas para partes específicas e não para todos os Estados-Membros da UE.
D) Não, porque é um regulamento que se aplica a todos os Estados-Membros da UE e é diretamente aplicável.

A) Incorreto. Uma diretiva estabelece objetivos para os Estados-Membros da UE, que depois decidem como incluí-los em sua legislação nacional. No entanto, o GDPR é um regulamento.
B) Incorreto. Uma recomendação não é vinculativa e não exige quaisquer medidas jurídicas por parte dos Estados-Membros da UE. No entanto, o GDPR é um regulamento.
C) Incorreto. Uma decisão é vinculativa apenas para as partes específicas a que se refere, não para todos os Estados-Membros da UE, e não se aplica a todos. No entanto, o GDPR é um regulamento.
D) Correto. O GDPR é um regulamento totalmente vinculativo e diretamente aplicável em toda a UE, sem necessidade de medidas nacionais. (Literatura: A, Capítulo 1)

3 / 40
Como o GDPR define dados pessoais?

A) Qualquer informação relacionada a um residente do Espaço Econômico Europeu (EEE)
B) Qualquer informação relativa a uma pessoa física identificada ou identificável
C) Dados diretamente relacionados a uma pessoa física identificada ou identificável
D) Dados que revelem as origens raciais ou étnicas de uma pessoa, suas crenças religiosas, condições de saúde, vida sexual ou orientação sexual

A) Incorreto. Informações só são consideradas dados pessoais se estiverem relacionadas a uma pessoa física identificada ou identificável. O local de residência não é relevante para determinar se os dados são dados pessoais.
B) Correto. Essa é a definição oficial do GDPR. (Literatura: A, Capítulo 1; Artigo 4(1) do GDPR)
C) Incorreto. Dados também são dados pessoais se estiverem indiretamente relacionados a uma pessoa física identificada ou identificável.
D) Incorreto. Essa é a definição de dados pessoais especiais, não de dados pessoais.

4 / 40
De acordo com o GDPR, qual é a definição de tratamento de dados pessoais?

A) Qualquer operação que possa ser realizada com dados pessoais
B) Qualquer operação que possa ser realizada com dados pessoais, exceto exclusão e destruição
C) Apenas operações nas quais os dados pessoais sejam compartilhados ou transferidos de qualquer modo
D) Apenas operações nas quais os dados pessoais sejam usados para as finalidades para as quais foram coletados

A) Correto. Tratamento significa qualquer operação realizada com dados pessoais. (Literatura: A, Capítulo 1; Artigo 4(2) do GDPR)
B) Incorreto. Exclusão e destruição também são formas de tratamento de dados.
C) Incorreto. Qualquer operação, incluindo a distribuição, se enquadra no tratamento de dados.
D) Incorreto. Qualquer operação realizada com dados pessoais é considerada tratamento.

5 / 40
O GDPR define alguns dados pessoais como dados de categoria especial, por vezes denominados ”dados sensíveis”.

Qual é um exemplo desse tipo de dado?

A) Uma coleta de endereços de e-mail profissionais de funcionários
B) Um registro genealógico dos ancestrais de uma pessoa
C) Uma lista de pagamentos efetuados com um cartão de crédito
D) Uma lista de endereços dos membros de um partido político

A) Incorreto. Endereços de e-mail profissionais são considerados dados pessoais, mas não se enquadram na categoria especial de dados pessoais.
B) Incorreto. Informações genealógicas de pessoas vivas constituem dados pessoais, mas não dados pessoais de categoria especial. O GDPR não é aplicável aos dados de pessoas falecidas.
C) Incorreto. Dados de cartão de crédito são dados pessoais, mas não dados pessoais de categoria especial.
D) Correto. Dados pessoais que revelem opiniões políticas constituem dados pessoais de categoria especial. (Literatura: A, Capítulo 4; Artigo 9(1) do GDPR)

6 / 40
Uma das funções descritas no GDPR é definida como:

Uma pessoa física ou jurídica, autoridade pública, agência ou outro órgão que, isoladamente ou em conjunto com outras partes, determina as finalidades e os meios de tratamento de dados pessoais.

Qual função é definida aqui?

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

A) Correto. O controlador determina a finalidade e os meios de tratamento. (Literatura: A, Capítulo 2; Artigo 4(7) do GDPR)
B) Incorreto. O controlador determina a finalidade do tratamento, enquanto o operador trabalha de acordo com as instruções do controlador.
C) Incorreto. A autoridade supervisora monitora e garante a conformidade com os requisitos do GDPR.
D) Incorreto. Um terceiro não tem qualquer participação na determinação da finalidade do tratamento. Qualquer parte que determine a finalidade se tornaria um novo controlador.

7 / 40
O tratamento de dados pessoais deve ser legal. Uma empresa coleta dados pessoais de seus clientes.

O que é **sempre** necessário para um tratamento legal ao se coletar dados pessoais?

A) Pedir permissão à autoridade supervisora para o tratamento
B) Documentar uma base legal para o tratamento dos dados pessoais
C) Implementar um código de conduta descrevendo a natureza do tratamento

A) 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)
B) Correto. O tratamento só é legal quando existir uma finalidade legítima. (Literatura: A, Capítulo 4; Artigo 6 do GDPR)
C) Incorreto. Códigos de conduta podem ser um modo de harmonizar contratos entre o controlador e o operador.

8 / 40
De acordo com o GDPR, o controlador deve manter um registro de todas as atividades de tratamento.

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

A) Um registro de todas as medidas técnicas e organizacionais implementadas de todos os operadores
B) Um registro de todo o tratamento pretendido, juntamente com as finalidades do tratamento e as justificativas legais
C) Um registro de violações de dados com todas as características relevantes, incluindo notificações

A) Correto. Embora o controlador deva verificar se os operadores utilizam medidas técnicas e organizacionais adequadas, essas medidas não precisam ser registradas. (Literatura: A, Capítulo 2; Artigo 28(1) do GDPR)
B) Incorreto. Deve ser mantido um registro de todo o tratamento pretendido, com a(s) finalidade(s) e justificativas legais.
C) Incorreto. Deve ser mantido um registro de violações de dados.

9 / 40
Um dos sete princípios da proteção de dados desde a concepção (by design) é a *funcionalidade total – soma positiva, não soma igual a zero*.

Qual é a essência desse princípio?

A) A proteção de dados coexiste com a segurança para criar uma situação vantajosa para todos, que acomoda legítimos interesses juntamente com a privacidade.
B) A proteção de dados inclui informar os titulares dos dados sobre as formas como seus dados são tratados, o que ajuda os titulares dos dados a manter o controle.
C) A proteção de dados está incorporada na arquitetura e no design dos sistemas, o que a torna uma funcionalidade essencial.

A) Correto. Essa é a essência da *funcionalidade total – soma positiva, não soma igual a zero*. (Literatura: A, Capítulo 2)
B) Incorreto. Essa é a essência da *visibilidade e transparência – manter tudo aberto*.
C) Incorreto. Essa é a essência da *privacidade incorporada ao design*.

10 / 40
Qual é uma descrição de proteção de dados desde a concepção (by design) e por padrão (by default)?

A) Uma abordagem que implementa a proteção de dados desde o desenvolvimento
B) Uma indicação de prazos caso o tratamento esteja relacionado a apagamento
C) Os dados só podem ser coletados para finalidades explícitas e legítimas
D) Não manter mais dados do que o estritamente necessário para o tratamento

A) Correto. Essa é uma descrição correta. (Literatura: A, Capítulo 2; Artigo 25 do GDPR)
B) Incorreto. Essa é a descrição de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA).
C) Incorreto. Essa é uma descrição de medidas adotadas para conformidade com o princípio de limitação de finalidade.
D) Incorreto. Essa é uma descrição dos procedimentos usados para conformidade com o princípio de minimização de dados.

11 / 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. Pela comparação dos horários de entrada e saída das placas, é calculado o número de carros presentes a cada momento de cada dia.

Foi obtida uma permissão para coletar dados sobre o número de carros presentes no centro da cidade. 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 tratamento e o fato de que os números das placas serão armazenados em segurança por até dois anos, porque as medições serão repetidas no ano seguinte.

Qual princípio básico do tratamento legal de dados pessoais é **violado** nesse cenário?

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

A) Incorreto. O governo local especificou sua finalidade legal de coletar dados sobre o número de carros presentes.
B) Correto. Nesse cenário, não há necessidade de reter os dados de um carro específico, identificando o proprietário, após ele ter deixado a área. (Literatura: A, Capítulo 3; Artigo 5 do GDPR)
C) Incorreto. O cenário não sugere uma segurança inadequada.
D) Incorreto. O tratamento está ocorrendo de um modo transparente, pois é comunicado adequadamente aos titulares dos dados.

12 / 40
Após o cumprimento do objetivo original, o tratamento 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 tratamento 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 tratamento adicional para fins de arquivamento por interesse público é permitido.
B) Correto. Essa não é uma finalidade permitida, se não constituir a finalidade legal original do tratamento. (Literatura: A, Capítulo 3)
C) Incorreto. Com salvaguardas estabelecidas, o tratamento adicional para fins estatísticos em geral é permitido.
D) Incorreto. Com salvaguardas estabelecidas, o tratamento adicional para fins de pesquisa é permitido.

13 / 40
Uma organização fornece sua declaração de privacidade em vários idiomas e formatos, incluindo online, impresso e em áudio, para garantir que todos os titulares dos dados possam acessá-la e compreendê-la.

Qual direito do GDPR essa prática apoia **mais** diretamente?

A) O direito ao apagamento, porque os titulares dos dados são auxiliados a compreender que têm o direito de excluir seus dados a qualquer momento.
B) O direito à oposição, pois os titulares dos dados podem se opor ao tratamento de forma melhor quando compreendem totalmente a declaração de privacidade.
C) O direito à restrição, pois os titulares dos dados são informados sobre os objetivos da empresa e as bases legais para o tratamento.
D) O direito à transparência das informações, comunicações e modalidades, porque os titulares dos dados são auxiliados a compreender o aviso de privacidade.

A) Incorreto. Embora seja importante compreender seus direitos, a prática de fornecer avisos de privacidade em vários formatos apoia principalmente a transparência, em vez de facilitar diretamente o direito ao apagamento.
B) Incorreto. Compreender as declarações de privacidade pode ajudar os titulares dos dados a exercer seus direitos, mas o foco principal dessa prática é aumentar a transparência, em vez de apoiar diretamente o direito à oposição.
C) Incorreto. Embora seja necessário informar os titulares dos dados sobre o tratamento, o principal objetivo de fornecer avisos de privacidade acessíveis é garantir a transparência, e não especificamente apoiar o direito à restrição.
D) Correto. Fornecer avisos de privacidade em vários idiomas e formatos garante que todos os titulares dos dados recebam informações claras e acessíveis, apoiando seu direito à transparência. (Literatura: A, Capítulo 5)

14 / 40
Qual 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, comumente 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 5)
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 defesa de reivindicações legais.

15 / 40
Um indivíduo compra um terno e fornece à loja o consentimento para utilizar seu endereço de e-mail para publicidade. Quando chega em casa, ele pede que a loja apague todos os seus dados pessoais e pare de lhe enviar e-mails.

De acordo com o GDPR, o que a loja deve fazer?

A) A loja não deve excluir nenhum dado pessoal desse indivíduo, pois as informações sobre as vendas devem ser retidas.
B) A loja deve excluir todos os dados pessoais desse indivíduo para os quais a base legal é o consentimento.
C) A loja deve excluir os outros dados pessoais desse indivíduo, mas pode continuar a enviar e-mails.

A) Incorreto. A loja tem a obrigação legal de reter os dados relativos à compra. O titular dos dados retirou o consentimento, de modo que apenas o tratamento baseado numa base legal que não seja o consentimento pode continuar, e a loja deve parar de enviar e-mails para fins publicitários.
B) Correto. A loja tem a obrigação legal de reter os dados relativos à compra (que também são dados pessoais), mas os outros dados devem ser apagados. O titular dos dados retirou o consentimento, de modo que a loja deve parar de enviar e-mails para fins publicitários. (Literatura: A, Capítulo 5; Artigo 17 do GDPR)
C) Incorreto. O titular dos dados retirou o consentimento, portanto a loja deve parar de enviar e-mails.

16 / 40
Um indivíduo recebe regularmente ofertas de uma loja onde ele fez compras cinco anos atrás. Ele quer que a empresa pare de enviar ofertas e exclua seus dados pessoais.

Qual direito do titular dos dados esse indivíduo está exercendo?

A) O direito ao acesso
B) O direito à objeção
C) O direito à retificação
D) O direito à restrição do tratamento

A) Incorreto. O direito ao acesso envolve a obtenção de informações sobre os dados pessoais de alguém e como eles são tratados, não parar comunicações ou solicitar a exclusão.
B) Correto. O direito à objeção permite que o indivíduo solicite que a empresa pare de tratar seus dados para fins de marketing, o que inclui parar as ofertas. (Literatura: A, Capítulo 5; Artigo 21 do GDPR)
C) Incorreto. O direito à retificação refere-se à correção de dados imprecisos ou incompletos, não parar comunicações ou apagar os dados.
D) Incorreto. A restrição consiste em bloquear dados incorretos ou tratados em contradição com as regulamentações legais.

17 / 40
Uma empresa utiliza inteligência artificial (IA) para analisar cartas de candidatura a empregos e decidir automaticamente se irá convidar os candidatos para uma entrevista.

Qual direito do GDPR é **mais** relevante para esse cenário?

A) O direito de não estar sujeito a uma decisão baseada exclusivamente em tratamento automatizado
B) O direito de apresentar uma reclamação a uma autoridade supervisora
C) O direito à restrição do tratamento
D) O direito à transparência das informações, comunicações e modalidades

A) Correto. Esse direito é o mais relevante, pois aborda especificamente as preocupações sobre decisões tomadas sem intervenção humana, como as tomadas pela IA nesse cenário. (Literatura: A, Capítulo 5; Artigo 22 do GDPR)
B) Incorreto. Apresentar uma reclamação é um direito geral para qualquer violação do GDPR, mas não se refere especificamente à tomada de decisões automatizadas.
C) Incorreto. A restrição do tratamento envolve limitar o uso de dados pessoais, não abordar decisões tomadas pela IA.
D) Incorreto. Embora a transparência seja importante, ela não aborda diretamente a questão da tomada de decisão automatizada nesse cenário.

18 / 40
Dados pessoais devem ser coletados para finalidades especificadas, explícitas e legais e não devem ser tratados adicionalmente de um modo incompatível com essas finalidades.

Qual princípio do tratamento de dados é descrito aqui?

A) Exatidão
B) Minimização de dados
C) Legalidade, lealdade e transparência
D) Limitação de finalidade

A) Incorreto. A exatidão diz respeito a garantir que os dados estejam corretos e atualizados, não a especificar as finalidades da coleta de dados.
B) Incorreto. A minimização de dados diz respeito à coleta apenas dos dados necessários para uma finalidade específica, não à especificação das finalidades em si.
C) Incorreto. A legalidade, lealdade e transparência envolvem ter uma base legal e ser claro sobre o tratamento, mas não abordam especificamente a especificação da finalidade.
D) Correto. A limitação de finalidade exige que os dados pessoais sejam coletados para finalidades específicas, explícitas e legais. (Literatura: A, Capítulo 3; Artigo 5 do GDPR)

19 / 40
O GDPR descreve o princípio de minimização de dados.

Como as organizações podem estar em conformidade com esse princípio?

A) Aplicando o conceito de privilégio mínimo aos dados pessoais coletados, armazenados ou de outro modo tratados
B) Limitando os direitos de acesso aos funcionários que precisarem dos dados pessoais para as operações de tratamento pretendidas
C) Limitando os tamanhos dos arquivos, salvando todos os dados pessoais tratados no menor formato possível
D) Limitando os dados pessoais àquilo que for adequado, relevante e necessário para as finalidades do tratamento

A) Incorreto. A minimização de dados não aborda o privilégio mínimo, em que os usuários recebem o mínimo possível de direitos de acesso.
B) Incorreto. Isso descreve o conceito de limitação de autorização, por exemplo, para estar em conformidade com o princípio de integridade e confidencialidade.
C) Incorreto. A minimização de dados não envolve o tamanho do armazenamento, e sim a redução do uso de dados pessoais ao que é absolutamente necessário.
D) Correto. Essa é a essência da descrição do princípio de minimização de dados de acordo com o GDPR. (Literatura: A, Capítulo 3; Artigo 5(1)(c) do GDPR)

20 / 40
O GDPR faz referência aos princípios de proporcionalidade e subsidiariedade.

O que **subsidiariedade** significa?

A) Os dados pessoais devem ser coletados para finalidades específicas, explícitas e legítimas e não devem ser tratados adicionalmente.
B) Os dados pessoais devem ser mantidos de modo que permita a identificação dos titulares dos dados por um período não maior do que o necessário.
C) Ao tratar dados pessoais, o controlador só recolherá os dados necessários para a finalidade.
D) Ao tratar dados pessoais, os meios utilizados devem infringir a privacidade o mínimo possível.

A) Incorreto. Essa é uma definição de limitação de finalidade.
B) Incorreto. Essa é uma definição de limitação de armazenamento.
C) Incorreto. Essa é uma definição de minimização de dados.
D) Correto. Se a subsidiariedade for aplicada à proteção de dados, isso significa utilizar os meios menos intrusivos para tratar os dados, minimizando o impacto sobre a privacidade. (Literatura: A, Capítulo 3; Considerando 170 do GDPR)

21 / 40
Qual é a finalidade da Gestão do Ciclo de Vida dos Dados (GCVD)?

A) Avaliar se os dados devem ser tratados como dados pessoais ou dados normais
B) Assegurar que os dados pessoais sejam excluídos assim que não houver mais base legal para retê-los
C) Gerenciar o fluxo de dados em uma empresa em conformidade com o GDPR

A) Incorreto. A finalidade da GCVD é gerenciar o fluxo de todos os dados em uma empresa e garantir que os dados sejam tratados com segurança e em conformidade com o GDPR. Ela não diz respeito apenas aos dados pessoais, mas a todos os dados.
B) Incorreto. Essa não é a finalidade da GCVD. No entanto, a GCVD ajuda a rastrear dados que devem ser excluídos se não houver base legal para mantê-los.
C) Correto. A GCVD é uma abordagem estruturada para gerenciar o fluxo de dados, determinar os controles de segurança necessários e garantir a conformidade com o GDPR. (Literatura: A, Capítulo 6; Artigo 5 do GDPR)

22 / 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 de computador para descobrir senhas
D) Salvar as páginas que um usuário marcar como favoritas no histórico de navegação do usuário

A) Incorreto. Os cookies não são usados para armazenar dados no servidor.
B) Correto. Essa é a principal finalidade de um cookie persistente. (Literatura: A, Capítulo 7)
C) Incorreto. Os cookies não são maliciosos por natureza, mas o mecanismo pode ser explorado de forma maliciosa.
D) Incorreto. Os favoritos e o histórico de navegação são salvos, mas não em um cookie.

23 / 40
Uma instituição de caridade de resgate de gatos possui muitos doadores. Eles processam os dados pessoais desses doadores, a fim de manter registros tanto para fins fiscais quanto para doadores recorrentes. Todos os doadores deram o consentimento para esse tratamento.

A instituição de resgate de gatos deseja utilizar um sistema de inteligência artificial (IA) para agradecer automaticamente aos doadores recorrentes, enviando-lhes vídeos de seus gatos favoritos. O sistema de IA também enviará um e-mail aos doadores não recorrentes, informando que mais gatos precisam de ajuda e sugerindo doações mensais.

Qual princípio do GDPR é **especialmente** importante para esse sistema de IA?

A) Exatidão, porque a organização de resgate de gatos deve garantir que o sistema de IA associe adequadamente os vídeos de gatos aos doadores para obter os melhores resultados e aumentar as doações a longo prazo.
B) Anonimização, porque a organização de resgate de gatos deve garantir que o sistema de IA não tenha acesso a dados pessoais em um formato que torne os doadores reconhecíveis.
C) Legalidade, porque a organização de resgate de gatos não é um negócio, o que torna mais difícil encontrar um legítimo interesse para que o tratamento seja necessário e legal.
D) Transparência, porque a organização de resgate de gatos deve informar claramente os doadores sobre como seus dados são usados e dar a eles a chance de se oporem caso a finalidade original seja alterada.

A) Incorreto. No contexto do GDPR, a exatidão refere-se ao caráter correto dos dados em si, não do algoritmo. Exatidão, lealdade e imparcialidade são requisitos obrigatórios na Lei de IA.
B) Incorreto. A organização deve usar dados identificáveis para enviar mensagens personalizadas, de modo que a anonimização não seria relevante.
C) Incorreto. A organização de resgate de gatos deve ter uma base legal ou um legítimo interesse. No entanto, encontrar um não é mais difícil por se tratar de uma instituição de caridade. Os doadores já deram o consentimento ao tratamento (de dados pessoais). A única coisa que falta é informar os doadores e permitir que eles se oponham ao tratamento adicional.
D) Correto. A transparência é muito importante para esse sistema de IA, porque o uso de um sistema de IA é uma nova atividade de tratamento. É essencial informar os doadores caso a finalidade do tratamento de dados mude. (Literatura: A, Capítulo 3 e 7.2)

24 / 40
Uma empresa utiliza inteligência artificial (IA) para otimizar seu processo de aprovação de empréstimos. Os requerentes de empréstimo preenchem um formulário online. O sistema de IA analisa essas informações e decide automaticamente se uma pessoa se qualifica para um empréstimo e quanto ela pode pegar emprestado. Esse processo é mais rápido e eficiente do que os métodos tradicionais, permitindo que a empresa processe um número maior de solicitações rapidamente, sem a necessidade de intervenção humana.

De acordo com o GDPR, o que essa empresa deve fazer?

A) Anonimizar os dados pessoais que a IA utiliza para garantir que os requerentes de empréstimo não possam ser identificados
B) Informar os requerentes de empréstimo sobre as decisões automatizadas e oferecer-lhes uma maneira fácil de solicitar uma revisão humana
C) Declarar claramente que os requerentes de empréstimo devem concordar com a IA tomando decisões automatizadas sem intervenção humana
D) Deixar de utilizar decisões automatizadas e voltar a utilizar decisões humanas para garantir os direitos dos requerentes de empréstimo

A) Incorreto. A anonimização dos dados não permitirá que a IA faça seu trabalho adequadamente. O GDPR não exige a anonimização, mas exige a oportunidade de uma revisão humana.
B) Correto. Essa opção está em conformidade com o GDPR, garantindo que os requerentes sejam informados sobre as decisões da IA e possam solicitar uma revisão humana se discordarem de uma decisão. (Literatura: A, Capítulo 7.2)
C) Incorreto. Declarar que os requerentes devem concordar com as decisões automatizadas não cumpre os requisitos do GDPR. A empresa também deve oferecer opções para revisão humana.
D) Incorreto. O GDPR não exige que as empresas parem de usar IA para tomar decisões. Em vez disso, o GDPR enfatiza a transparência e a possibilidade de solicitar uma intervenção humana.

25 / 40
De acordo com o GDPR, quando contratos adicionais **não** são necessários para a transferência de dados pessoais?

A) Quando tanto o remetente quanto o destinatário se encontram no Espaço Econômico Europeu (EEE)
B) Quando o remetente criptografa os dados antes de enviá-los para outra empresa
C) Quando os dados não são considerados dados pessoais de categoria especial
D) Quando os dados são transferidos para fins jornalísticos ou artísticos

A) Correto. Contratos adicionais não são necessários para transferências de dados dentro do EEE, uma vez que todos os Estados-Membros devem aderir às normas de proteção de dados do GDPR. (Literatura: A, Capítulo 8; Artigo 44 do GDPR)
B) Incorreto. Embora a criptografia seja uma boa prática de segurança, medidas adicionais ainda podem ser necessárias se os dados forem transferidos para fora do EEE, dependendo das leis de proteção de dados do país de destino.
C) Incorreto. A necessidade de medidas adicionais não depende apenas do fato de os dados serem de categoria especial, mas também do destino da transferência de dados.
D) Incorreto. Mesmo para fins jornalísticos ou artísticos, as transferências de dados pessoais para fora do EEE exigem medidas adicionais para garantir a conformidade com o GDPR.

26 / 40
Uma empresa dentro do Espaço Econômico Europeu (EEE) deve elaborar regras corporativas vinculantes (BCR).

De acordo com o GDPR, qual é uma descrição de BCR?

A) Uma decisão sobre a segurança da transferência de dados pessoais para um país fora da EEE
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 EEE
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 EEE.
D) Correto. BCR constituem um conjunto de regras aprovadas pelas autoridades supervisoras. (Literatura: A, Capítulo 9; Artigo 47 do GDPR)

27 / 40
Um controlador deseja terceirizar o tratamento de dados pessoais para um operador.

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

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

A) Correto. Deve existir um contrato por escrito que garanta a confidencialidade dos dados, listando as finalidades e os meios de tratamento definidos pelo controlador e especificando que o operador apenas tratará os dados sob instruções do controlador. Ambas as partes devem assinar esse contrato. (Literatura: A, Capítulo 2; Artigo 28(3) do GDPR)
B) Incorreto. O controlador não precisa solicitar autorização à autoridade supervisora para cada terceirização. O operador nunca precisa solicitar autorização.
C) Incorreto. A autoridade supervisora não é um conselho jurídico e não verifica a conformidade de contratos.
D) Incorreto. Um ANS não é suficiente porque ele focará as operações, não necessariamente as finalidades.

28 / 40
Uma empresa multinacional está planejando transferir dados pessoais entre suas filiais localizadas em diferentes países, incluindo aqueles fora do Espaço Econômico Europeu (EEE). A empresa decide implementar regras corporativas vinculantes (BCR) para facilitar essas transferências.

Qual é um componente necessário dessas BCR?

A) As BCR devem garantir uma compensação financeira aos titulares dos dados em caso de violação de dados pessoais e especificar o montante.
B) As BCR devem incluir um mecanismo para garantir a conformidade com as regras por parte de todos os funcionários envolvidos no tratamento de dados.
C) As BCR devem descrever as medidas organizacionais e técnicas específicas utilizadas para proteger os dados pessoais durante as transferências.
D) As BCR devem especificar que todos os titulares dos dados devem ser notificados sobre cada transferência de dados pessoais de forma acessível.

A) Incorreto. As BCR não garantem compensação financeira em caso de violação de dados pessoais. Elas focam a conformidade com as normas de proteção de dados.
B) Correto. As BCR devem incluir mecanismos para garantir a conformidade por parte de todos os funcionários, pois as BCR devem ser vinculativas e sujeitas à aplicação dentro do grupo corporativo. (Literatura: A, Capítulo 9)
C) Incorreto. Embora as BCR devam garantir a proteção de dados, elas não precisam especificar as tecnologias utilizadas. As BCR focam a conformidade e a aplicabilidade.
D) Incorreto. As BCR são regras internas para a transferência de dados dentro de um grupo corporativo. Os titulares dos dados devem saber como seus dados pessoais são tratados, mas não é necessário notificá-los sobre cada transferência.

29 / 40
Uma empresa pretende transferir dados pessoais para fora do Espaço Econômico Europeu (EEE).

De acordo com o GDPR, quais transferências para **fora** do EEE são sempre legais?

A) Transferências baseadas nas leis do país não pertencente ao EEE 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. Isso também exigiria um parecer de adequação confirmando 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 9; Artigo 47 do GDPR)
D) Incorreto. Isso também exigiria a adoção de BCR oficiais.

30 / 40
Uma empresa na França possui regras corporativas vinculantes (BCR) para suas operações em todo o mundo. A empresa deseja transferir dados de clientes para um provedor terceirizado localizado nos Estados Unidos (EUA), com o qual não mantém uma operação conjunta. O provedor dos EUA não é certificado pelo Data Privacy Framework UE-EUA (DPF), mas assinou cláusulas contratuais padrão (SCCs) aprovadas pela Comissão Europeia (CE). Essas SCCs fazem parte de um contrato assinado com a empresa francesa.

Nos termos do GDPR, essa transferência de dados pessoais para o provedor dos EUA é legal?

A) Sim, porque o DPF foi declarado inválido.
B) Sim, porque o provedor dos EUA assinou as SCCs.
C) Não, porque transferências de dados para os EUA são proibidas.
D) Não, porque o provedor dos EUA deve assinar as BCR.

A) Incorreto. O DPF é considerado adequado. No entanto, a validade do DPF não é relevante nesse caso, uma vez que as SCCs já fornecem uma base jurídica independente para a transferência de dados.
B) Correto. O uso de SCCs aprovadas pela CE é um mecanismo jurídico válido para transferências internacionais de dados nos termos do GDPR, tornando a transferência legal. (Literatura: A, Capítulo 9; Artigo 46(2)(c) do GDPR)
C) Incorreto. As transferências de dados para os EUA não são categoricamente proibidas. Elas podem ser legais se salvaguardas apropriadas, como SCCs ou o DPF, estiverem em vigor.
D) Incorreto. As BCR destinam-se a transferências de dados dentro de um grupo e não se aplicam a provedores terceirizados, como o provedor de nuvem dos EUA. As SCC servem como mecanismo adequado para essa transferência.

31 / 40
Uma cafeteria quer usar inteligência artificial (IA) e vigilância por vídeo para monitorar quantas xícaras de café os funcionários servem. O objetivo é entender quais são os horários mais movimentados da semana, monitorando a produtividade.

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

A) Sim, porque é provável que o tratamento resulte em um risco elevado aos direitos dos titulares dos dados.
B) Sim, porque o projeto inclui tecnologias de IA ou processos que utilizam dados pessoais.
C) Não, porque dados pessoais de categoria especial não são coletados durante o monitoramento.
D) Não, porque o objetivo não é avaliar diretamente a produtividade dos funcionários.

A) Correto. A vigilância por vídeo pode afetar significativamente a privacidade e os direitos dos funcionários, exigindo, portanto, uma DPIA para avaliar e mitigar potenciais riscos elevados aos seus direitos e liberdades. (Literatura: A, Capítulo 10; Artigo 35 do GDPR)
B) Incorreto. Embora seja necessária uma DPIA, isso não se deve ao uso de dados pessoais ou à utilização de IA. O que torna a DPIA obrigatória é o risco elevado que o monitoramento do desempenho representa para a privacidade e os direitos dos funcionários.
C) Incorreto. Mesmo que não sejam coletados dados pessoais de categoria especial, uma DPIA ainda é necessária se houver um risco elevado para os direitos dos indivíduos, como no caso da vigilância por vídeo.
D) Incorreto. O motivo da coleta de dados não altera a necessidade de uma DPIA se houver um risco elevado para os direitos dos indivíduos.

32 / 40
Durante a Avaliação de Impacto sobre a Proteção de Dados (DPIA), uma equipe que trabalha em uma plataforma online para crianças explora se o uso de avatares em vez de nomes reais atende às necessidades de funcionalidade.

Qual objetivo da DPIA é **mais** apoiado por essa ação?

A) Avaliar a necessidade e a proporcionalidade
B) Descrever o tratamento
C) Envolver as partes interessadas relevantes
D) Identificar e avaliar os riscos para os titulares dos dados

A) Correto. Ao explorar se o uso de avatares em vez de nomes reais atende às necessidades de funcionalidade, a equipe está avaliando se o tratamento de dados é necessário e proporcional para atingir os objetivos da plataforma. (Literatura: A, Capítulo 10)
B) Incorreto. A avaliação do avatar não descreve as atividades de tratamento, mas avalia alternativas para atender às necessidades de funcionalidade.
C) Incorreto. A avaliação do avatar não envolve o envolvimento das partes interessadas, mas avalia se menos dados pessoais podem ser usados para atender às necessidades de funcionalidade.
D) Incorreto. A avaliação do avatar não identifica ou avalia diretamente os riscos. Seu objetivo é avaliar a necessidade e a proporcionalidade do uso de dados pessoais (nomes reais) em comparação com a não necessidade deles (avatares).

33 / 40
O GDPR estabelece os atributos mínimos de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA).

Qual é um desses atributos mínimos?

A) Um relatório detalhado sobre as responsabilidades e deveres do Data Protection Officer (DPO)
B) Uma revisão dos acordos de compartilhamento de dados da organização com terceiros
C) Uma avaliação das medidas de segurança tomadas para proteger as transferências de dados
D) Medidas para lidar com os riscos identificados aos direitos e liberdades dos titulares dos dados

A) Incorreto. Embora a função do DPO seja importante nos termos do GDPR, a DPIA não exige especificamente um relatório sobre suas responsabilidades e deveres como um de seus atributos mínimos.
B) Incorreto. Embora a revisão dos acordos de compartilhamento de dados seja importante para a conformidade geral com a proteção de dados, ela não está especificamente listada como um atributo mínimo de uma DPIA nos termos do GDPR.
C) Incorreto. Embora a avaliação das medidas de segurança faça parte da garantia da proteção de dados, uma DPIA foca especificamente a avaliação dos riscos aos direitos e liberdades dos titulares dos dados e as medidas para mitigar esses riscos, em vez de apenas avaliar as medidas de segurança para transferências de dados.
D) Correto. O GDPR estabelece os atributos mínimos de uma DPIA: uma descrição das operações de tratamento previstas e das finalidades do tratamento; uma avaliação da necessidade e proporcionalidade do tratamento; uma avaliação dos riscos aos direitos e liberdades dos titulares dos dados; as medidas previstas para abordar os riscos e demonstrar conformidade com o GDPR. (Literatura: A, Capítulo 10; Artigo 35(7), Considerando 84 e Considerando 90 do GDPR)

34 / 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 de clientes e outros dados sensíveis da empresa.

O operador afirma que isso constitui uma violação de dados pessoais, de acordo com o GDPR.

A afirmação do operador é verdadeira?

A) Sim, porque os dados pessoais no disco do servidor foram tratados de modo ilegal.
B) Sim, porque os dados sensíveis da empresa também estavam no mesmo disco do servidor.
C) Não, porque os dados pessoais no disco não foram tratados, apenas destruídos.
D) Não, porque isso se trata apenas de uma violação de dados comum e não de uma violação de dados pessoais.

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 11; Artigo 4(12) do GDPR)
B) Incorreto. Os dados sensíveis da empresa não são importantes para determinar se houve uma violação de dados pessoais.
C) Incorreto. O GDPR considera a perda acidental de dados pessoais como tratamento ilegal, porque não é por instrução do controlador ou operador. Isso a torna uma violação de dados pessoais.
D) Incorreto. Perder dados da empresa seria uma perda de dados, não uma violação de dados. Perder dados pessoais é remover o acesso aos dados pessoais, o que é considerado uma violação de dados pessoais (violação de disponibilidade) nos termos do GDPR.

35 / 40
Uma empresa tem planos para tratar dados pessoais. O Data Protection Officer (DPO) recentemente indicado executa uma Avaliação de Impacto sobre a Proteção de Dados (DPIA). O DPO descobre 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 suas mesas, eles 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. Sendo assim, isso não é uma violação.
C) Incorreto. O tratamento 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 11; Artigo 5(1)(f) do GDPR)

36 / 40
Um arquiteto está saindo de uma construção. Ele coloca seu notebook no chão para atender o telefone. Um caminhão passa por cima do notebook. Todos os arquivos sobre o projeto da construção e os cálculos em que ele estava trabalhando são perdidos. Uma cópia de segurança de uma versão anterior dos arquivos está disponível na nuvem.

De acordo com o GDPR, isso constitui uma violação de dados pessoais?

A) Sim, porque a destruição da última cópia de um arquivo faz com que os dados não estejam disponíveis.
B) Sim, porque os arquivos destruídos eram arquivos pessoais do arquiteto.
C) Não, porque arquivos do projeto e cálculos não são dados pessoais.
D) Não, porque os arquivos ainda estão disponíveis na forma de uma cópia de segurança.

A) Incorreto. Nenhum dado pessoal foi destruído.
B) Incorreto. Um arquivo pessoal não é sinônimo de dados pessoais.
C) Correto. Nenhum dado pessoal foi destruído, portanto, isso não se trata de uma violação de dados pessoais. (Literatura: A, Capítulo 11; Artigo 4(12) do GDPR)
D) Incorreto. Não houve violação de dados pessoais, mas não por esse motivo. Nenhum dado pessoal foi destruído.

37 / 40
Após uma violação de dados pessoais, um controlador no Espaço Econômico Europeu (EEE) deve determinar quem deve ser informado:

- Ninguém
- Apenas a autoridade supervisora
- A autoridade supervisora e todos os titulares dos dados afetados

De acordo com o GDPR, em qual situação os **titulares dos dados** devem ser notificados de uma violação de dados pessoais?

A) Quando os dados pessoais forem tratados em uma unidade do operador que não esteja localizada dentro das fronteiras do EEE
B) Quando os dados pessoais forem tratados por uma parte que concordou com o contrato de tratamento, mas ainda não o assinou
C) Quando o sistema no qual os dados pessoais são tratados for atacado, causando uma avaria em seus dispositivos de armazenamento
D) Quando houver uma probabilidade considerável de que a violação provoque um risco elevado à privacidade dos titulares dos dados

A) Incorreto. O local onde os dados são tratados não tem importância para a obrigação de notificar os titulares dos dados sobre violações de dados pessoais.
B) Incorreto. O tratamento de dados pessoais por outra parte diferente do controlador sem um contrato por escrito válido é considerado como uma violação de dados. Nessa situação, porém, consequências negativas para os titulares dos dados são improváveis. A notificação dos titulares dos dados não é obrigatória nesse caso.
C) Incorreto. Uma avaria de dispositivos de armazenamento dificulta ou até mesmo impossibilita o acesso aos dados, mas não implica um tratamento 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 11)

38 / 40
Um sistema contendo dados pessoais foi invadido e foi constatado que pessoas não autorizadas tiveram acesso aos dados pessoais.

De acordo com o GDPR, o que o controlador deve fazer **antes** de notificar a autoridade supervisora?

A) Avaliar se dados pessoais de caráter sensível foram ou possam ter sido acessados
B) Conduzir uma Avaliação de Impacto sobre a Proteção de Dados (DPIA) para determinar os riscos às pessoas físicas
C) Notificar os titulares dos dados envolvidos sobre a violação de dados pessoais e suas possíveis consequências
D) Notificar a polícia e relatar o acesso não autorizado ao(s) sistema(s)

A) Correto. De acordo com o artigo 33(1) do GDPR, não é necessária qualquer notificação se "a violação de dados pessoais não for suscetível de resultar em um risco para os direitos e liberdades de pessoas naturais". O controlador deve verificar esse fato antes de proceder à notificação. (Literatura: A, Capítulo 11; Artigo 33(1) do GDPR)
B) Incorreto. Uma DPIA é realizada antes do tratamento propriamente dito para determinar como o tratamento será organizado e quais riscos precisam ser mitigados.
C) Incorreto. A notificação do titular dos dados só é necessária se a violação de dados pessoais puder resultar em um risco elevado para os direitos e liberdades dos titulares dos dados.
D) Incorreto. De acordo com o GDPR, informar a polícia não é obrigatório, apesar de ser sensato.

39 / 40
As autoridades supervisoras têm determinadas tarefas que visam garantir o cumprimento do GDPR.

Qual é uma dessas tarefas?

A) Avaliar códigos de conduta para setores específicos em relação ao tratamento de dados pessoais
B) Definir um conjunto mínimo de medidas que devem ser adotadas para a proteção de dados pessoais e a privacidade
C) Redigir cláusulas contratuais padrão (SCCs) e regras corporativas vinculantes (BCR)
D) Investigar todas as violações de dados que tenham sido notificadas à autoridade supervisora

A) Correto. Uma das responsabilidades das autoridades supervisoras é fornecer orientações gerais sobre como estar em conformidade com os regulamentos. (Literatura: A, Capítulo 12)
B) Incorreto. Uma autoridade supervisora dará orientações gerais sobre o que é um nível adequado de segurança. Ela não prescreve medidas específicas.
C) Incorreto. As SCCs são criadas pela Comissão Europeia (CE). As autoridades supervisoras podem aprovar as BCR para transferências de dados, mas são as empresas que as redigem.
D) Incorreto. Uma autoridade supervisora não tem a obrigação nem a capacidade de investigar todas as violações de dados pessoais que lhe tenham sido notificadas.

40 / 40
Um controlador tem sua sede no Espaço Econômico Europeu (EEE). Ele terceirizou o tratamento de dados pessoais sensíveis para um operador situado fora do EEE, sem consultar a autoridade supervisora antes. Essa transgressão foi descoberta e a empresa foi multada pela autoridade supervisora. Seis meses depois, a autoridade supervisora descobre que o controlador é culpado da mesma transgressão, mas para uma operação de tratamento diferente e com outro operador.

Qual é a multa **máxima** que a autoridade supervisora pode impor nesse caso?

A) Nada, porque a empresa já foi multada por essa transgressão
B) Nada, mas poderá ser emitida uma advertência formal sem penalidades financeiras.
C) Uma multa de até € 10 milhões ou 2% do faturamento da empresa, o que for maior
D) Uma multa de até € 20 milhões ou 4% do faturamento da empresa, o que for maior

A) Incorreto. Cada violação do GDPR pode ser multada separadamente, especialmente se envolver diferentes operações de tratamento ou operadores. Portanto, multas anteriores não isentam a empresa de novas penalidades.
B) Incorreto. Dado que se trata de uma violação repetida das regras do GDPR, é improvável que apenas seja emitida uma advertência, uma vez que normalmente são aplicadas multas por descumprimento continuado.
C) Incorreto. A terceirização do tratamento de dados sensíveis sem a devida consulta é uma violação grave, e infrações repetidas podem resultar em multas mais elevadas nos termos do GDPR.
D) Correto. Essa é a multa máxima para uma violação repetida dessa natureza. As transferências de dados pessoais para um destinatário num país terceiro ou para uma organização internacional são puníveis com a multa mais elevada. (Literatura: A, Capítulo 12; Artigo 33 do GDPR)

Avaliação

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

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

Contato EXIN

www.exin.com