Exame simulado

Edição 201805

Conteúdo

Introdução

Este é o modelo de exame de 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 somente uma resposta é a correta.

O número máximo de pontos que pode ser obtido neste exame é 40. Cada resposta correta vale um ponto. Para ser aprovado você deve obter 26 pontos ou mais.

O tempo permitido para este exame simulado é de 60 minutos.

Boa Sorte!

Exame simulado

1 / 40
A coleta, armazenamento, modificação, divulgação ou disseminação ilegal de dados pessoais constitui uma ofensa de acordo com a lei europeia.

Que tipo de ofensa é essa?

A) Uma ofensa relacionada ao conteúdo
B) Uma ofensa econômica
C) Uma ofensa à propriedade intelectual
D) Uma ofensa à privacidade

2 / 40
Como a privacidade e a proteção de dados estão relacionadas entre si?

A) A proteção de dados decorre da privacidade.
B) A privacidade decorre da proteção de dados.
C) São a mesma coisa.
D) Você não pode ter privacidade sem proteção de dados.

3 / 40
Qual é o **principal** objetivo do General Data Protection Regulation (GDPR)?

A) Ser uma base comum sobre a qual os estados membros possam criar suas próprias leis
B) Fazer com que países fora da UE respeitem o direito à privacidade dos indivíduos na UE
C) Garantir a privacidade como um direito humano fundamental para todos
D) Fortalecer e unificar a proteção de dados para indivíduos na UE

4 / 40
O General Data Protection Regulation (GDPR) está relacionado à proteção de dados pessoais.

Qual é a definição de dados pessoais?

A) Qualquer informação relativa a uma pessoa física identificada ou identificável
B) Qualquer informação que os cidadãos europeus queiram proteger
C) Dados que diretamente ou indiretamente revelam origens raciais ou étnicas, visões religiosas de alguém, e seus dados relacionados a saúde e hábitos sexuais
D) Preservação da confidencialidade, integridade e disponibilidade de informações

5 / 40
De acordo com o General Data Protection Regulation (GDPR), que categoria de dados pessoais é considerada como dados sensíveis?

A) Detalhes do cartão de crédito
B) Associação sindical
C) Número do passaporte
D) Número do CPF

6 / 40
De acordo com o General Data Protection Regulation (GDPR), qual é a definição de " processamento" 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 sejam compartilhados em mídias sociais ou transferidos por e-mail ou de outro modo pela internet
D) Apenas operações nas quais os dados pessoais sejam usados para as finalidades para as quais foram coletados

7 / 40
"*Uma autoridade pública independente que seja estabelecida por um Estado Membro conforme o Artigo 51.*"

Que papel na proteção de dados é definido aqui?

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

8 / 40
O "consentimento livre e informado" é uma base legal para o processamento de dados pessoais de acordo com o General Data Protection Regulation (GDPR). Deve-se documentar a finalidade do processamento para a qual o consentimento é fornecido.

Em que momento do processo deve ser obtido o consentimento do titular dos dados?

A) Após a apresentação da especificação da finalidade e antes da coleta dos dados pessoais
B) Antes que a especificação do propósito seja concebida e apresentada
C) Antes do processamento dos dados pessoais
D) Antes da publicação ou disseminação dos dados pessoais

9 / 40
O General Data Protection Regulation (GDPR) é baseado nos princípios de proporcionalidade e subsidiariedade.

Qual é o significado de “proporcionalidade” 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 se não houver outros meios para atingir a finalidade.
D) Os dados pessoais devem ser adequados, relevantes e não excessivos em relação às finalidades.

10 / 40
O processamento de dados pessoais deve satisfazer alguns requisitos de qualidade.

Qual seria um destes requisitos de qualidade definidos pelo General Data Protection Regulation (GDPR)?

A) Os dados processados devem ser arquivados.
B) Os dados processados devem ser criptografados.
C) Os dados processados devem ser indexados.
D) Os dados processados devem ser relevantes.

11 / 40
Todas as vezes que dados pessoais forem processados, a proporcionalidade e a subsidiariedade devem ser verificadas.

Qual é o requisito para os dados pessoais que estão sendo processados?

A) Eles devem ser sempre limitados ao que for necessário para atingir os objetivos definidos e devem ser limitados aos dados menos “invasivos”.
B) Eles devem ser manipulados pelo menor número de funcionários possível, e estes devem trabalhar para o controlador ou uma afiliada.
C) Eles devem ser limitados a um tamanho de armazenamento predefinido e o sistema usado deve ser financiado pelo controlador.
D) Eles devem ser usados para o menor número de finalidades possível e isto não pode ser realizado fora das premissas do processador.

12 / 40
“O controlador deve implementar medidas técnicas e organizacionais apropriadas para garantir que (...) sejam processados apenas dados pessoais que sejam necessários para cada finalidade específica do processamento."

Qual termo do General Data Protection Regulation (GDPR) está sendo definido?

A) Conformidade
B) Proteção de dados como padrão
C) Privacidade desde a concepção (by design)
D) Proteção incorporada

13 / 40
Qual é o termo usado no General Data Protection Regulation (GDPR) para a divulgação de, ou acesso não autorizados a dados pessoais?

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

14 / 40
Foi verificada a ocorrência de uma violação de dados pessoais sensíveis.

A quem isto deve ser relatado em última análise, de acordo com o General Data Protection Regulation (GDPR)?

A) À Autoridade Supervisora
B) Ao Data Protection Officer (DPO)
C) Ao gerente do departamento
D) À polícia

15 / 40
Durante a realização de um backup, ocorre 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 sensível.

Qual tipo de incidente é esse?

A) Violação de dados
B) Violação de segurança
C) Incidente de segurança

16 / 40
Uma pessoa que trabalha para um sindicato levou para casa a minuta de um informativo para finalizá-la. O pen drive contendo a minuta e a lista de contatos foi perdido.

A quem, entre outros, deve ser relatada esta violação de dados?

A) A todos os membros da lista de contatos
B) Ao staff do sindicato
C) À polícia

17 / 40
Uma organização de assistência social pretende projetar uma nova base de dados para administrar seus clientes e os cuidados de que necessitam.

Para solicitar a permissão junto à autoridade supervisora, qual seria uma das primeiras medidas importantes a serem tomadas?

A) Coletar dados sobre os clientes e a quantidade e tipo de cuidados necessários e fornecidos.
B) Conduzir uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) para determinar os riscos do processamento pretendido.
C) Obter o consentimento dos clientes para o processamento pretendido de seus dados pessoais.

18 / 40
Em que caso os titulares dos dados devem ser sempre notificados de uma violação de dados?

A) Os dados pessoais foram processados em uma instalação do processador que não está localizada dentro das fronteiras da UE.
B) Os dados pessoais foram processados por uma parte que concordou com a minuta de um contrato de processamento enviada pelo controlador, mas ainda não o assinou.
C) Os dados pessoais foram processados por uma parte que ainda não tinha assinado um contrato compulsório com o controlador.
D) Existe uma probabilidade significativa de que a violação conduza a consequências prejudiciais para a privacidade dos titulares dos dados.

19 / 40
Um controlador holandês contratou um processador em um país da África Setentrional para processar dados pessoais sensíveis, sem consultar a autoridade supervisora. Isso foi descoberto e ele foi penalizado pela autoridade supervisora. Seis meses depois, a autoridade descobre que o controlador é novamente culpado da mesma transgressão em outra operação de processamento.

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

A) € 750.000
B) € 1.230.000
C) € 10.000.000 ou 2% do volume global de negócios da empresa, o que for maior
D) € 20.000.000 ou 4% do volume global de negócios da empresa, com um mínimo de € 20.000.000, o que for maior

20 / 40
As Autoridades Supervisoras assumem várias responsabilidades destinadas a garantir que os regulamentos para proteção de dados sejam cumpridos.

Qual é uma dessas responsabilidades?

A) Avaliar códigos de conduta para setores específicos em relação ao processamento de dados pessoais
B) Definir um conjunto mínimo de medidas que devem ser adotadas para a proteção de dados pessoais
C) Investigar todas as violações que forem notificadas à eles
D) Examinar contratos e Regras Corporativas Compulsórias em relação à conformidade com os regulamentos

21 / 40
Uma associação religiosa deseja compartilhar dados pessoais com sua autoridade religiosa, em um país não europeu, para cumprir uma solicitação legal do governo envolvido.

Qual regulamento do General Data Protection Regulation (GDPR) é aplicável nesse caso?

A) Como exceção, o processamento de dados sensíveis que revelem as crenças religiosas é permitido para uma associação religiosa.
B) Não é permitido transferir dados pessoais para fora da Área Econômica Europeia em resposta a uma exigência de um terceiro país.
C) O processamento é legal, desde que seja adquirido o consentimento específico e inequívoco do titular de dados.
D) O processamento de dados pessoais fora da Área Econômica Europeia é permitido usando as cláusulas do modelo de contrato projetado pela Comissão da UE.

22 / 40
Em 12 de julho de 2016 a Comissão Europeia implementou uma disposição regulamentar relativa à transferência de dados pessoais com os EUA (EU-US Privacy Shield).

Em termos do General Data Protection Regulation (GDPR), que tipo de disposição é essa?

A) Uma decisão de adequação
B) Um decreto de exceção
C) Um contrato compulsório padrão
D) Um tratado que substitui o GDPR

23 / 40
Regras Corporativas Compulsórias constituem um meio para facilitar a carga administrativa das organizações no cumprimento do GDPR.

Como estas regras podem ajudar?

A) Elas permitem que as organizações tenham contratos de apoio com todas as partes envolvidas no exterior.
B) Elas permitem que as organizações deixem terceiros fora da Área Econômica Europeia processarem os dados pessoais.
C) Elas evitam a necessidade de abordar separadamente cada autoridade supervisora na UE.
D) Elas previnem que as organizações precisem pedir permissão a uma autoridade supervisora para o processamento dos dados após suas Regras Corporativas Compulsórias serem aceitas.

24 / 40
Caso uma contratada contrate um processamento externo de dados pessoais, esta deverá assinar um contrato com a outra parte. Este contrato define o assunto e a duração do processamento, a natureza e a finalidade do processamento e o tipo de dados pessoais e categorias de titulares dos dados.

Que outro aspecto deve ser governado por este contrato?

A) A responsabilidade do processador
B) A obrigação de notificação de violações de dados
C) A obrigação por parte dos processadores de cooperação com a autoridade supervisora
D) As obrigações e os direitos do controlador

25 / 40
O que deve ser feito para que um controlador possa terceirizar o processamento de dados pessoais para um processador?

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 firmado está em conformidade com seus 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 combinadas no Acordo de Nível de Serviço (ANS) são cumpridas.

26 / 40
A proteção de dados desde a concepção (by design), conforme a descrição no artigo 25 do General Data Protection Regulation (GDPR), é baseada em sete princípios básicos. Um desses geralmente é chamado de *"Funcionalidade – Soma Positiva, Soma Diferente de Zero"*.

Qual é a essência desse 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 riscos e impacto na privacidade e devem ser realizadas e publicadas, documentando com clareza os riscos para a privacidade.

27 / 40
Muitas vezes, os funcionários que trabalham com dados pessoais consideram privacidade e segurança da informação como questões separadas.

Por que isso está errado?

A) A privacidade não pode ser garantida sem a identificação, implementação e monitoramento de medidas de segurança da informação adequadas.
B) A autoridade supervisora espera que os papéis do Data Protection Officer (DPO) e security officer sejam integrados.
C) Os regulamentos identificam medidas de segurança da informação específicas que devem ser adotadas antes que a manipulação de dados pessoais seja permitida.

28 / 40
Um dos objetivos de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) é "fortalecer a confiança dos clientes ou cidadãos no modo como os dados pessoais são processados e a privacidade é respeitada".

Como uma AIPD 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 General Data Protection Regulation (GDPR) e minimiza o risco de multas.
C) A organização prova que considera a privacidade com seriedade e visa à conformidade com o GDPR.

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

A) Atender a obrigação do General Data Protection Regulation (GDPR) de implementar medidas técnicas e organizacionais apropriadas para proteção de dados
B) Monitorar e impor a aplicação do GDPR, determinando se o processamento está sendo realizado em conformidade com o GDPR
C) Aconselhar o controlador sobre a mitigação de riscos à privacidade para proteger o controlador de pedidos de indenização de responsabilidade civil por descumprimento do GDPR

30 / 40
O que **melhor** descreve o princípio de minimização de dados?

A) Deve-se ter o cuidado de coletar o mínimo de dados possível para proteger a privacidade e os interesses dos titulares dos dados.
B) Os dados devem ser adequados, relevantes e limitados ao que for necessário em relação às finalidades para as quais são processados.
C) Para que os dados permaneçam gerenciáveis, eles devem ser armazenados de uma maneira que exija um espaço mínimo de armazenamento.
D) O número de itens coletados por titular dos dados não pode exceder o limite superior declarado pela autoridade supervisora.

31 / 40
Cookies de sessão constituem um dos tipos de cookies mais comuns.

Qual é a **melhor** descrição de um cookie de sessão?

A) Ele contém informações sobre o que você está fazendo, por exemplo, os produtos que você seleciona em um comércio eletrônico antes de efetivar o pedido.
B) Ele revela o histórico do seu navegador para que outros sites possam descobrir que sites você visitou antes de chegar ali.
C) Ele armazena o histórico do seu navegador para que você possa rastrear onde esteve na internet e revisitar o(s) site(s), se quiser.
D) Ele coleta seus dados pessoais para que o site possa dirigir-se a você pelo nome e reutilizar suas configurações quando você retornar.

32 / 40
Às vezes os sites rastreiam os visitantes e armazenam suas informações para fins de marketing.

O site é obrigado a informar o visitante que suas informações estão sendo usadas para fins de marketing?

A) Sim
B) Não

33 / 40
Uma empresa pode se apresentar como especialista em uma área de competência específica fazendo uso da mídia social.

Qual é o **melhor** modo de demonstrar competência em um setor específico?

A) Publicando informações sobre a empresa nas mídias sociais
B) Respondendo ativamente as perguntas sobre seus produtos nas mídias sociais
C) Publicando posts sobre como o produto do concorrente é inferior ao da empresa
D) Publicando posts sobre novos produtos que a empresa esteja desenvolvendo

34 / 40
Ocorreu uma violação de segurança em um sistema de informação que também contém dados pessoais.

Qual é a **primeira** coisa que o controlador deve fazer?

A) Verificar se a violação pode ter provocado a perda ou o processamento ilícito 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 (AIPD)
C) Determinar se dados pessoais de caráter sensível foram ou possam ter sido processados ilegalmente
D) Relatar a violação imediatamente à autoridade supervisora relevante

35 / 40
A palavra “privacidade” não é mencionada no GDPR.

Como a “privacidade” está relacionada à “proteção de dados”?

A) Proteção de dados é um conjunto de regras e regulamentos sobre o processamento de dados pessoais. A privacidade é o resultado da proteção de dados.
B) Privacidade é o direito a ser protegido de uma interferência em assuntos pessoais. A proteção de dados representa o modo para implementar essa proteção.
C) Privacidade é o direito de manter assuntos pessoais em segredo. Proteção de dados é o direito de manter os dados pessoais em segredo.
D) Os termos “privacidade” e “proteção de dados” são intercambiáveis. Não há uma diferença real no significado.

36 / 40
O Regulamento (EU) 2016/679, conhecido como General Data Protection Regulation (GDPR), anula uma Diretiva anterior da UE.

Que diretiva está sendo anulada (substituída)?

A) Diretiva 2002/58/EC de 12 de julho de 2002
B) Diretiva 2006/24/EC de 15 de março de 2006
C) Diretiva 95/46/EC de 24 de outubro de 1995
D) Diretiva 97/66/EC de 15 de dezembro de 1997

37 / 40
Que direito dos titulares de dados é definido explicitamente pelo General Data Protection Regulation (GDPR)?

A) Uma cópia dos dados pessoais deve ser fornecida no formato solicitado pelo titular dos dados.
B) Acesso aos dados pessoais sem qualquer 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 isto for solicitado pelo titular dos dados.

38 / 40
O General Data Protection Regulation (GDPR) distingue “dados pessoais sensíveis” como uma categoria especial de dados pessoais.

Qual seria um exemplo desse tipo de dados?

A) Uma consulta com especialista médico no hospital
B) Um Número de Conta Bancária Internacional (IBAN)
C) Assinatura de uma revista científica sobre política
D) Afiliação a uma associação de classe

39 / 40
Qual função na proteção de dados determina as finalidades e os meios de processamento de dados pessoais?

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

40 / 40
Que informações são consideradas como dados pessoais, de acordo com o General Data Protection Regulation (GDPR)?

A) Informações sobre uma pessoa que possam comprometer a privacidade daquela pessoa, mesmo que sejam falsas.
B) Qualquer informação relativa a uma pessoa física identificável.
C) Informações relativas a uma pessoa física identificável que tenham sido digitalizadas.

Gabarito de respostas

1 / 40
A coleta, armazenamento, modificação, divulgação ou disseminação ilegal de dados pessoais constitui uma ofensa de acordo com a lei europeia.

Que tipo de ofensa é essa?

A) Uma ofensa relacionada ao conteúdo
B) Uma ofensa econômica
C) Uma ofensa à propriedade intelectual
D) Uma ofensa à privacidade

A) Incorreto. Uma ofensa relacionada ao conteúdo envolve a disseminação de declarações racistas, pornografia (infantil) ou informações que incitem a violência.
B) Incorreto. Ofensas econômicas estão relacionadas ao acesso não autorizado a sistemas (invasão, disseminação de vírus, etc.) espionagem cibernética, falsificação e fraude.
C) Incorreto. Ofensas à propriedade intelectual são referentes a violações dos direitos autorais e outros relacionados.
D) Correto. Qualquer processamento ilegal de dados pessoais constitui uma ofensa. Nenhuma fonte: conhecimento básico.

2 / 40
Como a privacidade e a proteção de dados estão relacionadas entre si?

A) A proteção de dados decorre da privacidade.
B) A privacidade decorre da proteção de dados.
C) São a mesma coisa.
D) Você não pode ter privacidade sem proteção de dados.

A) Incorreto. A privacidade abrange vários conceitos, como privacidade de localização, relacional, corporal e de informações. A proteção de dados não tem nenhuma relação com eles.
B) Incorreto. A privacidade abrange vários conceitos, como privacidade de localização, relacional, corporal e de informações. A proteção de dados ajuda a garantir alguns deles.
C) Incorreto. A proteção de dados, por exemplo, não tem nada a ver com privacidade de localização.
D) Correto. A proteção de dados é uma medida necessária para proteger o direito à privacidade. Fonte: White Paper – Privacy, Personal Data and the GDPR - §1.3 Definitions

3 / 40
Qual é o **principal** objetivo do General Data Protection Regulation (GDPR)?

A) Ser uma base comum sobre a qual os estados membros possam criar suas próprias leis
B) Fazer com que países fora da UE respeitem o direito à privacidade dos indivíduos na UE
C) Garantir a privacidade como um direito humano fundamental para todos
D) Fortalecer e unificar a proteção de dados para indivíduos na UE

A) Incorreto. O GDPR é um regulamento, o que significa que ele revoga as leis para proteção de dados nos estados membros.
B) Incorreto. Seu principal objetivo consiste em definir os direitos à proteção de dados de indivíduos na UE.
C) Incorreto. O GDPR declara explicitamente que a proteção de dados é um direito fundamental, mas sua abrangência está limitada aos indivíduos na UE.
D) Correto. A abrangência do GDPR é limitada à proteção de dados como um direito dos indivíduos na UE e tem como objetivo harmonizar as regras para tanto, dentro da UE. Fonte: EU GDPR, Um guia de bolso – Introdução.

4 / 40
O General Data Protection Regulation (GDPR) está relacionado à proteção de dados pessoais.

Qual é a definição de dados pessoais?

A) Qualquer informação relativa a uma pessoa física identificada ou identificável
B) Qualquer informação que os cidadãos europeus queiram proteger
C) Dados que diretamente ou indiretamente revelam origens raciais ou étnicas, visões religiosas de alguém, e seus dados relacionados a saúde e hábitos sexuais
D) Preservação da confidencialidade, integridade e disponibilidade de informações

A) Correto. Esta é a definição oficial da proteção de dados. Fonte: EU GDPR, Um guia de bolso - Capítulo 2 Termos e definições GDPR 2016/679 Artigo 4: definição
B) Incorreto. Esta definição é muito genérica.
C) Incorreto. Esta é a definição de dados sensíveis, não de dados pessoais em geral.
D) Incorreto. Esta é a definição de segurança da informação da ISO/IEC 27000:2014.

5 / 40
De acordo com o General Data Protection Regulation (GDPR), que categoria de dados pessoais é considerada como dados sensíveis?

A) Detalhes do cartão de crédito
B) Associação sindical
C) Número do passaporte
D) Número do CPF

A) Incorreto. Os detalhes do cartão de crédito não são dados sensíveis de acordo com o GDPR.
B) Correto. A associação sindical é um dado sensível. Fonte: GDPR art. 9, §10 - Categorias especiais de dados pessoais.
C) Incorreto. Os detalhes do passaporte não são dados sensíveis de acordo com o GDPR.
D) Incorreto. O número do CPF não é um dado sensível de acordo com o GDPR.

6 / 40
De acordo com o General Data Protection Regulation (GDPR), qual é a definição de "processamento" 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 sejam compartilhados em mídias sociais ou transferidos por e-mail ou de outro modo pela internet
D) Apenas operações nas quais os dados pessoais sejam usados para as finalidades para as quais foram coletados

A) Correto. Fonte: GDPR art.4 (2)
B) Incorreto. "Processamento" significa qualquer operação que seja realizada com dados pessoais.
C) Incorreto. "Processamento" significa qualquer operação que seja realizada com dados pessoais.
D) Incorreto. "Processamento" significa qualquer operação que seja realizada com dados pessoais.

7 / 40
"Uma autoridade pública independente que seja estabelecida por um Estado Membro conforme o Artigo 51."

Que papel na proteção de dados é definido aqui?

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

A) Incorreto. Ver Regulamento 2016/679, Artigo 4.
B) Incorreto. Ver Regulamento 2016/679, Artigo 4.
C) Correto. Fonte: GDPR 2016/679, Artigo 4 e Artigo 51.
D) Incorreto. Ver Regulamento 2016/679, Artigo 4.

8 / 40
O “consentimento livre e informado” é uma base legal para o processamento de dados pessoais de acordo com o General Data Protection Regulation (GDPR). Deve-se documentar a finalidade do processamento para a qual o consentimento é fornecido.

Em que momento do processo deve ser obtido o consentimento do titular dos dados?

A) Após a apresentação da especificação da finalidade e antes da coleta dos dados pessoais
B) Antes que a especificação do propósito seja concebida e apresentada
C) Antes do processamento dos dados pessoais
D) Antes da publicação ou disseminação dos dados pessoais

A) Correto. O consentimento só pode ser informado depois que a especificação da finalidade for apresentada ao titular dos dados.
B) Incorreto. O consentimento só pode ser informado depois que a especificação da finalidade for apresentada ao titular dos dados.
C) Incorreto. A coleta de dados pessoais constitui um “processamento” e, como tal, requer o consentimento livre e informado do titular dos dados.
D) Incorreto. A publicação e a disseminação de dados pessoais constituem um “processamento” e, como tal, requerem o consentimento livre e informado do titular dos dados.

9 / 40
O General Data Protection Regulation (GDPR) é baseado nos princípios de proporcionalidade e subsidiariedade.

Qual é o significado de “proporcionalidade” 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 se não houver outros meios para atingir a finalidade.
D) Os dados pessoais devem ser adequados, relevantes e não excessivos em relação às finalidades.

A) Incorreto. Esta é uma das limitações legais.
B) Incorreto. Esta é uma das limitações legais.
C) Incorreto. Esta é a definição de subsidiariedade.
D) Correto. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 3.1.2 Proporcionalidade e subsidiariedade & GDPR art. 35 (7)

10 / 40
O processamento de dados pessoais deve satisfazer alguns requisitos de qualidade.

Qual seria um destes requisitos de qualidade definidos pelo General Data Protection Regulation (GDPR)?

A) Os dados processados devem ser arquivados.
B) Os dados processados devem ser criptografados.
C) Os dados processados devem ser indexados.
D) Os dados processados devem ser relevantes.

A) Incorreto. Nenhum requisito deste tipo é definido pelo GDPR.
B) Incorreto. Nenhum requisito deste tipo é definido pelo GDPR.
C) Incorreto. Nenhum requisito deste tipo é definido pelo GDPR.
D) Correto. Este requisito é definido pelo GDPR. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 3.1.2 Proporcionalidade e subsidiariedade

11 / 40
Todas as vezes que dados pessoais forem processados, a proporcionalidade e a subsidiariedade devem ser verificadas.

Qual é o requisito para os dados pessoais que estão sendo processados?

A) Eles devem ser sempre limitados ao que for necessário para atingir os objetivos definidos e devem ser limitados aos dados menos “invasivos”.
B) Eles devem ser manipulados pelo menor número de funcionários possível, e estes devem trabalhar para o controlador ou uma afiliada.
C) Eles devem ser limitados a um tamanho de armazenamento predefinido e o sistema usado deve ser financiado pelo controlador.
D) Eles devem ser usados para o menor número de finalidades possível e isto não pode ser realizado fora das premissas do Processador.

A) Correto. Estes termos significam que você não deve coletar mais dados do que o necessário para atingir o(s) objetivo(s) predefinido(s) e você sempre deve tentar usar os dados que tenham o menor impacto sobre a privacidade do titular dos dados. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Processamento legal
B) Incorreto. O número de funcionários ou sua afiliação a alguma subsidiária não têm nenhuma relação com estes termos.
C) Incorreto. O tamanho do armazenamento e quem financia os sistemas usados não têm nenhuma relação com estes termos.
D) Incorreto. Desde que o titular dos dados forneça seu consentimento, o número de objetivos não é explicitamente restrito, nem o local.

12 / 40
"O controlador deve implementar medidas técnicas e organizacionais apropriadas para garantir que (...) sejam processados apenas dados pessoais que sejam necessários para cada finalidade específica do processamento."

Qual termo do General Data Protection Regulation (GDPR) está sendo definido?

A) Conformidade
B) Proteção de dados como padrão
C) Privacidade desde a concepção (by design)
D) Proteção incorporada

A) Incorreto. Conformidade é o estado ou fato que esteja de acordo com ou satisfaça regras e 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. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Proteção de dados desde a concepção (by design) e como padrão & GDPR art. 20 (2).
C) Incorreto. A proteção de dados desde a concepção (by design) refere-se a um projeto que inclua medidas apropriadas para implementar os princípios de proteção de dados.
D) Incorreto. Proteção de dados incorporada é o resultado da proteção de dados desde a concepção (by design).

13 / 40
Qual é o termo usado no General Data Protection Regulation (GDPR) para a divulgação de, ou acesso não autorizados a dados pessoais?

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

A) Incorreto. O GDPR utiliza o termo violação de dados. Nem toda violação de dados constitui uma violação de confidencialidade.
B) Correto. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Violações de dados & GDPR artigo 4 (12)
C) Incorreto. O GDPR utiliza o termo violação de dados. Nem todo incidente constitui uma violação de dados.
D) Incorreto. O GDPR utiliza o termo violação de dados. Nem todo incidente de segurança constitui uma violação de dados.

14 / 40
Foi verificada a ocorrência de uma violação de dados pessoais sensíveis.

A quem isto deve ser relatado em última análise, de acordo com o General Data Protection Regulation (GDPR)?

A) À Autoridade Supervisora
B) Ao Data Protection Officer (DPO)
C) Ao gerente do departamento
D) À polícia

A) Correto. Violações de dados devem ser relatadas à Autoridade de Proteção de Dados (DPA) se puderem ter um impacto significante sobre a segurança do titular dos dados ou de seus dados pessoais. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Violações de dados GDPR artigo 4 (12)
B) Embora isto possa ser relatado a um DPO interno, no final, deverá ser relatado à Autoridade de Proteção de Dados (DPA).
C) Incorreto. Embora isto possa ser relatado ao gerente, deverá também ser relatado à Autoridade de Proteção de Dados (DPA).
D) Incorreto. Violações de dados não precisam necessariamente ser relatadas à polícia, mas devem sempre ser relatadas à Autoridade de Proteção de Dados (DPA).

15 / 40
Durante a realização de um backup, ocorre 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 sensível.

Qual tipo de incidente é esse?

A) Violação de dados
B) Violação de segurança
C) Incidente de segurança

A) Correto. Dados pessoais perdidos de modo irrecuperável são considerados como um processamento não autorizado, o que configura uma violação de dados. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Violações de dados GDPR Capítulo I, Artigo 4, Definições
B) Incorreto. Dados pessoais perdidos de modo irrecuperável são considerados como um processamento não autorizado, o que configura violação de dados.
C) Incorreto. Dados pessoais perdidos de modo irrecuperável são considerados como um processamento não autorizado, o que configura violação de dados.

16 / 40
Uma pessoa que trabalha para um sindicato levou para casa a minuta de um informativo para finalizá-la. O pen drive contendo a minuta e a lista de contatos foi perdido.

A quem, entre outros, deve ser relatada esta violação de dados?

A) A todos os membros da lista de contatos
B) Ao staff do sindicato
C) À polícia

A) Correto. Este é um dado sensível, portanto a perda deve ser reportada tanto à autoridade responsável quanto aos titulares dos dados. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Violações de dados
B) Incorreto. Estes são dados sensíveis, portanto sua perda deve ser relatada tanto à autoridade responsável pela privacidade quanto aos titulares dos dados.
C) Incorreto. Estes são dados sensíveis, portanto sua perda deve ser relatada tanto à autoridade responsável pela privacidade quanto aos titulares dos dados.

17 / 40
Uma organização de assistência social pretende projetar uma nova base de dados para administrar seus clientes e os cuidados de que necessitam.

Para solicitar a permissão junto à autoridade supervisora, qual seria uma das primeiras medidas importantes a serem tomadas?

A) Coletar dados sobre os clientes e a quantidade e tipo de cuidados necessários e fornecidos.
B) Conduzir uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) para determinar os riscos do processamento pretendido.
C) Obter o consentimento dos clientes para o processamento pretendido de seus dados pessoais.

A) Incorreto. A coleta de dados pessoais médicos, por definição, constitui um “processamento de dados sensíveis”. É necessária a permissão prévia da Autoridade de Proteção de Dados (DPA) e dos titulares dos dados.
B) Correto. Ao solicitar o consentimento para o processamento dos dados, os titulares dos dados “devem ser informados dos riscos, regras, salvaguardas e direitos...” Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Consentimento & Exposição do GDPR (39)
C) Incorreto. Ao solicitar o consentimento para o processamento dos dados, os titulares dos dados “devem ser informados dos riscos, regras, salvaguardas e direitos...” Antes, é necessária uma AIPD para determinar estes riscos e salvaguardas.

18 / 40
Em que caso os titulares dos dados devem ser sempre notificados de uma violação de dados?

A) Os dados pessoais foram processados em uma instalação do processador que não está localizada dentro das fronteiras da UE.
B) Os dados pessoais foram processados por uma parte que concordou com a minuta de um contrato de processamento enviada pelo controlador, mas ainda não o assinou.
C) Os dados pessoais foram processados por uma parte que ainda não tinha assinado um contrato compulsório com o controlador.
D) Existe uma probabilidade significativa de que a violação conduza a consequências prejudiciais para a 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 a violação dos mesmos.
B) Incorreto. Os dados pessoais processados por outra parte, contratada pelo controlador, sem um contrato escrito válido é considerado como violação de dados. No entanto, na situação dada, as conseqüências negativas para os titulares dos dados em questão são improváveis. Notificar os titulares dos dados não é obrigatório nesse caso.
C) Incorreto. O dano aos dispositivos de armazenamento tornará o acesso aos dados difícil ou mesmo impossível, mas não implica em processamento ilegal.
D) Correto. Se houver uma probabilidade significativa de impacto negativo aos titulares dos dados, o controlador é obrigado a notificá-los da violação. Fonte: Livro Branco - Privacidade, Dados Pessoais e o GDPR - § 5.2 Procedimentos sobre como agir quando ocorre uma violação de dados.

19 / 40
Um controlador holandês contratou um processador em um país da África Setentrional para processar dados pessoais sensíveis, sem consultar a autoridade supervisora. Isso foi descoberto e ele foi penalizado pela autoridade supervisora. Seis meses depois, a autoridade descobre que o controlador é novamente culpado da mesma transgressão em outra operação de processamento.

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

A) € 750.000
B) € 1.230.000
C) € 10.000.000 ou 2% do volume global de negócios da empresa, o que for maior
D) € 20.000.000 ou 4% do volume global de negócios da empresa, com um mínimo de € 20.000.000, o que for maior

A) Incorreto. De acordo com o art. 83.3 do GDPR, a multa máxima corresponde a 4% do volume global de negócios da empresa, com um mínimo de € 20.000.000.
B) Incorreto. De acordo com o art. 83.3 do GDPR, a multa máxima corresponde a 4% do volume global de negócios da empresa, com um mínimo de € 20.000.000.
C) Incorreto. De acordo com o art. 83.3 do GDPR, a multa máxima corresponde a 4% do volume global de negócios da empresa, com um mínimo de € 20.000.000.
D) Correto. Este é o valor máximo para uma violação. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 7.3.3 Condições gerais para a imposição de multas administrativas.

20 / 40
As Autoridades Supervisoras assumem várias responsabilidades destinadas a garantir que os regulamentos para proteção de dados sejam cumpridos.

Qual é uma dessas responsabilidades?

A) Avaliar códigos de conduta para setores específicos em relação ao processamento de dados pessoais
B) Definir um conjunto mínimo de medidas que devem ser adotadas para a proteção de dados pessoais
C) Investigar todas as violações que forem notificadas à eles
D) Examinar contratos e Regras Corporativas Compulsórias em relação à conformidade com os regulamentos

A) Correto. Uma das responsabilidades das autoridades de proteção de dados (DPA) é fornecer uma orientação geral sobre como cumprir com os regulamentos. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 7.1.4 Definição de normas.
B) Incorreto. Uma Autoridade de Proteção de Dados (DPA) fornecerá uma orientação geral sobre o que é considerado um nível de segurança apropriado. Contudo, ela não vão dizer quais medidas específicas devem ser adotadas para chegar a esse nível. Mesmo que quisesse, ela não poderia porque não existe uma solução única que funcione para todos.
C) Incorreto. Autoridades de proteção de dados (DPA) não têm a obrigação, nem a capacidade, de investigar todas as violações de que tenham conhecimento. Mas investigarão aquelas que julgarem significativas ou dignas de atenção.
D) Incorreto. Uma Autoridade de Proteção de Dados (DPA) não é um conselho legal. Ela não examinará contratos ou Regras Corporativas Compulsórias. Contudo, no decorrer de uma investigação, eles podem analisar um contrato específico ou um conjunto de Regras Corporativas Compulsórias.

21 / 40
Uma associação religiosa deseja compartilhar dados pessoais com sua autoridade religiosa, em um país não europeu, para cumprir uma solicitação legal do governo envolvido.

Qual regulamento do General Data Protection Regulation (GDPR) é aplicável nesse caso?

A) Como exceção, o processamento de dados sensíveis que revelem as crenças religiosas é permitido para uma associação religiosa.
B) Não é permitido transferir dados pessoais para fora da Área Econômica Europeia em resposta a uma exigência de um terceiro país.
C) O processamento é legal, desde que seja adquirido o consentimento específico e inequívoco do titular de dados.
D) O processamento de dados pessoais fora da Área Econômica Europeia é permitido usando as cláusulas do modelo de contrato projetado pela Comissão da UE.

A) Incorreto. Associações religiosas têm permissão para processar dados relativos a seus membros anteriores e atuais, mas não tem permissão para transferir dados pessoais para fora da Área Econômica Europeia em resposta a uma exigência legal de um terceiro país.
B) Correto. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 7.5.2 Regulamentos aplicáveis à transferência de dados para fora da Área Econômica Europeia EU GDPR, Um guia de bolso - Capítulo 3: O regulamento – Transferências internacionais GDPR art. 48.
C) Incorreto. Não é permitido transferir dados pessoais para fora da Área Econômica Europeia em resposta a uma exigência legal de um terceiro país, nem mesmo com o consentimento do titular dos dados.
D) Incorreto. O processamento de dados sensíveis fora da Área Econômica Europeia pode ser permitido, mas não em resposta à solicitação do governo de um terceiro país.

22 / 40
Em 12 de julho de 2016 a Comissão Europeia implementou uma disposição regulamentar relativa à transferência de dados pessoais com os EUA (EU-US Privacy Shield).

Em termos do General Data Protection Regulation (GDPR), que tipo de disposição é essa?

A) Uma decisão de adequação
B) Um decreto de exceção
C) Um contrato compulsório padrão
D) Um tratado que substitui o GDPR

A) Correto. A disposição regulamentar constitui uma decisão de adequação de acordo com o GDPR, em relaçãno que diz respeito ao processamento em terceiros países. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 7.5.4 Regulamentos aplicáveis à transferência de dados entre a Área Econômica Europeia e os EUA EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento - Transferências internacionais Exposições do GDPR 104 e 106.
B) Incorreto. Uma exceção refere-se a transferências essenciais para responder a ataques terroristas ou crimes graves (art. 11)
C) Incorreto. A disposição regulamentar constitui uma decisão de adequação ao GDPR, no que diz respeito ao processamento em terceiros países.
D) Incorreto. A disposição regulamentar constitui uma decisão de adequação de acordo com o GDPR, no que diz respeito ao processamento em terceiros países.

23 / 40
Regras Corporativas Compulsórias constituem um meio para facilitar a carga administrativa das organizações no cumprimento do GDPR.

Como estas regras podem ajudar?

A) Elas permitem que as organizações tenham contratos de apoio com todas as partes envolvidas no exterior.
B) Elas permitem que as organizações deixem terceiros fora da Área Econômica Europeia processarem os dados pessoais.
C) Elas evitam a necessidade de abordar separadamente cada autoridade supervisora na UE.
D) Elas previnem que as organizações precisem pedir permissão a uma autoridade supervisora para o processamento dos dados após suas Regras Corporativas Compulsórias serem aceitas.

A) Incorreto. Regras Corporativas Compulsórias são preparadas para que as organizações não precisem usar contratos de apoio separados para cada afiliada.
B) Incorreto. Regras Corporativas Compulsórias são válidas apenas dentro de uma organização e em todas as suas afiliadas. Não são aplicadas a nenhuma outra parte.
C) Correto. Quando as Regras Corporativas Compulsórias são aprovadas por uma autoridade de proteção de dados (DPA dentro da UE, não é necessário pedir a aprovação de outras autoridades dentro da UE. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Regras corporativas vinculativas
D) Incorreto. Um conjunto de regras compulsórias deve ser autorizado por uma Autoridade de Proteção de Dados (DPA).

24 / 40
Caso uma contratada contrate um processamento externo de dados pessoais, esta deverá assinar um contrato com a outra parte. Este contrato define o assunto e a duração do processamento, a natureza e a finalidade do processamento e o tipo de dados pessoais e categorias de titulares dos dados.

Que outro aspecto deve ser governado por este contrato?

A) A responsabilidade do processador
B) A obrigação de notificação de violações de dados
C) A obrigação por parte dos processadores de cooperação com a autoridade supervisora
D) As obrigações e os direitos do controlador

A) Incorreto. Esta é uma obrigação direta do General Data Protection Regulation (GDPR) para os processadores.
B) Incorreto. Esta é uma obrigação direta do GDPR para os processadores.
C) Incorreto. Esta é uma obrigação direta do GDPR para os processadores.
D) Correto. Esta é uma obrigação direta do GDPR para os processadores. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Contratos de controladores/processadores & GDPR art. 28 (3).

25 / 40
O que deve ser feito para que um controlador possa terceirizar o processamento de dados pessoais para um processador?

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 firmado está em conformidade com seus 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 combinadas no Acordo de Nível de Serviço (ANS) são cumpridas.

A) Incorreto. Não é necessário pedir a permissão da Autoridade de Proteção de Dados (DPA) para cada caso de terceirização.
B) Incorreto. A Autoridade de Proteção de Dados (DPA) não é um conselho legal e não verifica a conformidade de contratos.
C) Correto. Deve haver um contrato por escrito garantindo a confidencialidade dos dados, no qual o controlador define os objetivos e os métodos de processamento. As duas partes devem assinar esse contrato. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Contratos de controladores/processadores GDPR art. 28 (3).
D) Incorreto. Um ANS não é suficiente porque ele enfocará as operações, não definindo necessariamente os objetivos.

26 / 40
A proteção de dados desde a concepção (by design), conforme a descrição no artigo 25 do General Data Protection Regulation (GDPR), é baseada em sete princípios básicos. Um desses geralmente é chamado de *"Funcionalidade – Soma Positiva, Soma Diferente de Zero"*.

Qual é a essência desse 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 riscos e impacto na privacidade e devem ser realizadas e publicadas, documentando com clareza os riscos para a privacidade.

A) Incorreto. Este é um aspecto da Segurança End-to-End – Proteção do Ciclo de Vida, um dos outros seis princípios básicos.
B) Incorreto. A privacidade desde a concepção (by design) rejeita a abordagem de que a Privacidade deve competir com outros interesses legítimos, objetivos do projeto e capacidades técnicas. Todos os objetos devem ser acomodados em uma soma positiva, de um modo "ganha-ganha".
C) Correto, esta é a essência. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 8.1.1 Os sete princípios da proteção de dados desde a concepção (by design) GDPR art. 25.
D) Incorreto. Este é um aspecto da "privacidade *incorporada* ao projeto", um dos outros seis princípios básicos.

27 / 40
Muitas vezes, os funcionários que trabalham com dados pessoais consideram privacidade e segurança da informação como questões separadas.

Por que isso está errado?

A) A privacidade não pode ser garantida sem a identificação, implementação e monitoramento de medidas de segurança da informação adequadas.
B) A autoridade supervisora espera que os papéis do Data Protection Officer (DPO) e security officer sejam integrados.
C) Os regulamentos identificam medidas de segurança da informação específicas que devem ser adotadas antes que a manipulação de dados pessoais seja permitida.

A) Correto. Privacidade e proteção de dados referem-se à garantia de confidencialidade de dados pessoais, entre outros. Isto requer a implementação de medidas de segurança. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 2.1.6 Integridade e confidencialidade.
B) Incorreto. A Autoridade de Proteção de Dados (DPA) não espera que estes papéis sejam integrados.
C) Incorreto. Os regulamentos especificam os objetivos que devem ser atingidos, mas nenhuma medida específica que deva ser adotada.

28 / 40
Um dos objetivos de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) é “fortalecer a confiança dos clientes ou cidadãos no modo como os dados pessoais são processados e a privacidade é respeitada”.

Como uma AIPD 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 General Data Protection Regulation (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. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Avaliações de Impacto sobre a Proteção de Dados

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

A) Atender a obrigação do General Data Protection Regulation (GDPR) de implementar medidas técnicas e organizacionais apropriadas para proteção de dados
B) Monitorar e impor a aplicação do GDPR, determinando se o processamento está sendo realizado em conformidade com o GDPR
C) Aconselhar o controlador sobre a mitigação de riscos à privacidade para proteger o controlador de pedidos de indenização de responsabilidade civil por descumprimento do GDPR

A) Incorreto. A auditoria não constitui a implementação das medidas, e sim uma avaliação de sua eficácia.
B) Correto. De acordo com o GDPR, esta é uma tarefa importante, própria da Autoridade de Proteção de Dados (DPA).
C) Incorreto. A Autoridade de Proteção de Dados (DPA) tem a tarefa de monitorar a conformidade e aconselhar sobre aprimoramentos, mas seu objetivo não é proteger o controlador.

30 / 40
O que **melhor** descreve o princípio de minimização de dados?

A) Deve-se ter o cuidado de coletar o mínimo de dados possível para proteger a privacidade e os interesses dos titulares dos dados.
B) Os dados devem ser adequados, relevantes e limitados ao que for necessário em relação às finalidades para as quais são processados.
C) Para que os dados permaneçam gerenciáveis, eles devem ser armazenados de uma maneira que exija um espaço mínimo de armazenamento.
D) O número de itens coletados por titular dos dados não pode exceder o limite superior declarado pela autoridade supervisora.

A) Incorreto. Na verdade, o General Data Protection Regulation (GDPR) declara que os dados coletados devem ser adequados, implicando que não precisam ser o mínimo absoluto.
B) Correto. Esta é a definição exata de minimização de dados. Isto tem o objetivo de garantir que apenas os dados necessários para atingir os objetivos definidos sejam coletados. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - §2.1 Princípios do processamento de dados GDPR artigo 5.1.c.
C) Incorreto. O tamanho do armazenamento não tem nenhuma relação com este princípio.
D) Incorreto. As autoridades supervisoras não estabelecem um limite superior para o número de itens coletados, desde que sejam limitados ao necessário para atingir os objetivos definidos.

31 / 40
Cookies de sessão constituem um dos tipos de cookies mais comuns.

Qual é a **melhor** descrição de um cookie de sessão?

A) Ele contém informações sobre o que você está fazendo, por exemplo, os produtos que você seleciona em um comércio eletrônico antes de efetivar o pedido.
B) Ele revela o histórico do seu navegador para que outros sites possam descobrir que sites você visitou antes de chegar ali.
C) Ele armazena o histórico do seu navegador para que você possa rastrear onde esteve na internet e revisitar o(s) site(s), se quiser.
D) Ele coleta seus dados pessoais para que o site possa dirigir-se a você pelo nome e reutilizar suas configurações quando você retornar.

A) Correto. Um cookie de sessão é mantido na memória para salvar informações sobre a sessão. Ele é apagado quando você encerra a sessão. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 8.6.3 Cookies
B) Incorreto. Um cookie de sessão é apagado quando a sessão é encerrada; portanto, não pode ser usado em uma sessão futura.
C) Incorreto. Um cookie de sessão é apagado quando a sessão é encerrada; portanto, não pode ser usado em uma sessão futura.
D) Incorreto. Um cookie de sessão é apagado quando a sessão é encerrada; portanto, não pode ser usado em uma sessão futura.

32 / 40
Às vezes os sites rastreiam os visitantes e armazenam suas informações para fins de marketing.

O site é obrigado a informar o visitante que suas informações estão sendo usadas para fins de marketing?

A) Sim
B) Não

A) Correto. O site tem a obrigação de informar ao visitante que suas informações estão sendo usadas para fins de marketing. Os visitantes têm o direito de recusar o processamento de dados pessoais referentes a eles para fins de marketing. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 8.6.3 Cookies
B) Incorreto. O site tem a obrigação de informar ao visitante que suas informações estão sendo usadas para fins de marketing. Os visitantes têm o direito de recusar o processamento de dados pessoais referentes a eles para fins de marketing.

33 / 40
Uma empresa pode se apresentar como especialista em uma área de competência específica fazendo uso da mídia social.

Qual é o **melhor** modo de demonstrar competência em um setor específico?

A) Publicando informações sobre a empresa nas mídias sociais
B) Respondendo ativamente as perguntas sobre seus produtos nas mídias sociais
C) Publicando posts sobre como o produto do concorrente é inferior ao da empresa
D) Publicando posts sobre novos produtos que a empresa esteja desenvolvendo

A) Incorreto. Simplesmente publicar informações sobre a empresa não faz de você um especialista no setor.
B) Correto. Responder (e responder ativamente) a perguntas sobre um produto específico nas mídias sociais pode transformar sua empresa em uma especialista. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 8.6 Aplicações relativas à prática do uso de dados, marketing e mídia social.
C) Incorreto. Isto simplesmente é alardear o quanto seu produto é bom (e talvez nem seja).
D) Incorreto. Isso simplesmente mostra que a empresa está desenvolvendo novos produtos e, sim, isso pode ajudar a melhorar as vendas, mas não faz da empresa uma especialista.

34 / 40
Ocorreu uma violação de segurança em um sistema de informação que também contém dados pessoais.

Qual é a **primeira** coisa que o controlador deve fazer?

A) Verificar se a violação pode ter provocado a perda ou o processamento ilícito 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 (AIPD)
C) Determinar se dados pessoais de caráter sensível foram ou possam ter sido processados ilegalmente
D) Relatar a violação imediatamente à autoridade supervisora relevante

A) Correto. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 5.2 Procedimentos sobre como agir quando houver uma violação de dados.
B) Incorreto. Uma AIPD é conduzida durante o projeto das operações de processamento de dados pessoais.
C) Incorreto. O controlador deve primeiro verificar se o incidente constitui uma violação de dados que precise ser relatada.
D) Incorreto. O controlador deve primeiro verificar se o incidente constitui uma violação de dados que precise ser relatada.

35 / 40
A palavra “privacidade” não é mencionada no GDPR.

Como a “privacidade” está relacionada à “proteção de dados”?

A) Proteção de dados é um conjunto de regras e regulamentos sobre o processamento de dados pessoais. A privacidade é o resultado da proteção de dados.
B) Privacidade é o direito a ser protegido de uma interferência em assuntos pessoais. A proteção de dados representa o modo para implementar essa proteção.
C) Privacidade é o direito de manter assuntos pessoais em segredo. Proteção de dados é o direito de manter os dados pessoais em segredo.
D) Os termos “privacidade” e “proteção de dados” são intercambiáveis. Não há uma diferença real no significado.

A) Incorreto. A privacidade é um direito, a proteção de dados é um meio para garanti-la.
B) Correto. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 1.3 Definições
C) Incorreto. A privacidade é um direito, a proteção de dados é um meio para garanti-la.
D) Incorreto. A privacidade é um direito, a proteção de dados é um meio para garanti-la.

36 / 40
O Regulamento (EU) 2016/679, conhecido como General Data Protection Regulation (GDPR), anula uma Diretiva anterior da UE.

Que diretiva está sendo anulada (substituída)?

A) Diretiva 2002/58/EC de 12 de julho de 2002
B) Diretiva 2006/24/EC de 15 de março de 2006
C) Diretiva 95/46/EC de 24 de outubro de 1995
D) Diretiva 97/66/EC de 15 de dezembro de 1997

A) Incorreto. A diretiva 2002/58/EC retifica algumas partes da diretiva 97/66/EC.
B) Incorreto. Esta diretiva refere-se à retenção de dados coletados, por exemplo, por provedores de internet.
C) Correto. Esta substituição é mencionada no (sub)título do regulamento. Fonte: GDPR.
D) Incorreto. Esta diretiva complementa a diretiva 95/46/EC para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais nos estados membros.

37 / 40
Que direito dos titulares de dados é definido explicitamente pelo General Data Protection Regulation (GDPR)?

A) Uma cópia dos dados pessoais deve ser fornecida no formato solicitado pelo titular dos dados.
B) Acesso aos dados pessoais sem qualquer 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 isto for solicitado pelo titular dos dados.

A) Incorreto. Isso deve ser fornecido 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. Contudo, apenas a primeira cópia precisa ser fornecida sem custos. Fonte: EU GDPR, Um guia de bolso - Capítulo 3 O Regulamento – Direitos dos titulares dos dados
C) Incorreto. Apenas dados errôneos precisam ser retificados.
D) Incorreto. O artigo 17 apresenta algumas exceções a estes casos, por exemplo, quando os dados são necessários para o estabelecimento, exercício ou defensa de reclamações legais.

38 / 40
O General Data Protection Regulation (GDPR) distingue “dados pessoais sensíveis” como uma categoria especial de dados pessoais.

Qual seria um exemplo desse tipo de dados?

A) Uma consulta com especialista médico no hospital
B) Um Número de Conta Bancária Internacional (IBAN)
C) Assinatura de uma revista científica sobre política
D) Afiliação a uma associação de classe

A) Correto. Uma consulta com um especialista médico constitui um “dado pessoal relativo à saúde”. Fonte: GDPR art. 9.1.
B) Incorreto. Um IBAN constitui um dado especificamente relacionado a uma pessoa, ou seja, um dado pessoal. Mas não constitui um dado pessoal sensível de acordo com GDPR art. 9.
C) Incorreto. Uma revista científica sobre política não constitui “dados pessoais que revelem opiniões políticas, crenças religiosas ou filosóficas” e, portanto, não constitui um dado pessoal sensível de acordo com GDPR art. 9.
D) Incorreto. Apenas a associação a sindicatos e outros dados pessoais” que revelem (...) opiniões políticas, crenças religiosas ou filosóficas” constituem dados pessoais sensíveis de acordo com GDPR art. 9.

39 / 40
Qual função na proteção de dados determina as finalidades e os meios de processamento de dados pessoais?

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

A) Correto. Controlador: a 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. Fonte: White Paper – Privacidade, Dados Pessoais e o GDPR - § 1.4 Funções, responsabilidades, partes interessadas.
B) Incorreto.
C) Incorreto.

40 / 40
Que informações são consideradas como dados pessoais, de acordo com o General Data Protection Regulation (GDPR)?

A) Informações sobre uma pessoa que possam comprometer a privacidade daquela pessoa, mesmo que sejam falsas.
B) Qualquer informação relativa a uma pessoa física identificável.
C) Informações relativas a uma pessoa física identificável que tenham sido digitalizadas.

A) Incorreto. Qualquer afirmação sobre uma pessoa física identificável constitui um dado pessoal de acordo com o GDPR.
B) Correto. Fonte: EU GDPR, Um guia de bolso - Capítulo 2 Termos e definições – Dados pessoais & GDPR art. 4 (1).
C) Incorreto. Qualquer afirmação sobre uma pessoa física identificável constitui um dado pessoal de acordo com o GDPR.

Avaliação

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

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

Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER