Guia de preparação

Edição 202004

Conteúdo

1. Visão geral

EXIN Privacy & Data Protection Foundation (PDPF.PR)

Escopo

EXIN Privacy & Data Protection Foundation (PDPF) é uma certificação que valida o conhecimento e compreensão de um profissional sobre a proteção de dados pessoais, as regras e regulamentos da União Europeia (UE) em matéria de proteção de dados.

Resumo

Onde quer que os dados pessoais sejam coletados, armazenados, usados e, finalmente, excluídos ou destruídos, surgem preocupações sobre privacidade. Com o Regulamento Geral de Proteção de Dados (GDPR) da UE, o Conselho da União Europeia tem por objetivo reforçar e unificar a proteção de dados para todos os indivíduos da União Europeia (UE). Este regulamento afeta todas as organizações que processam os dados pessoais de titulares dados localizados em território da EU e tem efeitos além de suas fronteiras. A certificação EXIN Privacy & Data Protection Foundation abrange os principais assuntos relacionados ao GDPR.

A nova norma na série ISO/IEC 27000: ISO/IEC 27701:2019 Técnicas de Segurança – Extensão da ISO/IEC 27001 e da ISO/IEC 27002 para Gestão de Informações de Privacidade – Requisitos e Diretrizes, é útil para organizações que desejam demonstrar a conformidade com o GDPR. O conteúdo da nova norma ISO ajuda no cumprimento das obrigações do GDPR pelas organizações em relação ao processamento de dados pessoais.

Nem o GDPR nem a norma ISO fazem parte da literatura do exame. Contudo, a matriz de literatura no capítulo 4 é projetada para mostrar a ligação entre os requisitos do exame, a literatura, o GDPR e a norma ISO/IEC 27701:2019 de modo a fornecer um contexto mais amplo à certificação.

Contexto

A certificação EXIN Privacy & Data Protection Foundation faz parte do programa de qualificação EXIN Privacy & Data Protection.

Público-alvo

Todos os colaboradores precisam ter uma compreensão da proteção de dados e dos requisitos legais europeus, conforme definido no GDPR. Essa certificação é destinada a:

- Data Protection Officers (DPO),
- Compliance Officers,
- Security Officesr,
- Funcionários de RH,
- Gerentes de Processos e de Projetos.

Requisitos para a certificação

- Conclusão bem sucedida do exame EXIN Privacy & Data Protection Foundation.

Detalhes do exame

Tipo do exame:	Questões de múltipla escolha
Número de questões:	40
Mínimo para aprovação:	65% (26/40 questões)
Com consulta/anotações:	Não
Equipamentos eletrônicos permitidos:	Não
Tempo designado para o exame:	60 minutos

As Regras e Regulamentos dos exames EXIN aplicam-se a este exame.

Nível Bloom

A certificação EXIN Privacy & Data Protection Foundation testa os candidatos nos Níveis Bloom 1 e 2 de acordo com a Taxonomia Revisada de Bloom:

- Nível Bloom 1: Lembrança – depende da recuperação de informações. Os candidatos precisarão absorver, lembrar, reconhecer e recordar.
- Nível Bloom 2: Compreensão – um passo além da lembrança. O entendimento mostra que os candidatos compreendem o que é apresentado e podem avaliar como o material de aprendizagem pode ser aplicado em seu próprio ambiente. Este tipo de pergunta pretende demonstrar que o candidato é capaz de organizar, comparar, interpretar e escolher a descrição correta de fatos e ideias.

Treinamento

Horas de contato

A carga horária recomendada para este treinamento é de 14 horas. Isto inclui trabalhos em grupo, preparação para o exame e pausas curtas. Esta carga horária não inclui pausas para almoço, trabalhos extra aula e o exame.

Indicação de tempo de estudo

60 horas, dependendo do conhecimento pré-existente.

Provedor de treinamento

Você encontrará uma lista de nossos provedores de treinamento credenciados em www.exin.com.

2. Requisitos do exame

Os requisitos do exame são definidos nas especificações do exame. A tabela a seguir lista os tópicos (requisitos do exame) e subtópicos (especificações do exame) do módulo.

Requisitos do exame	Especificações do exame	Peso
1. Fundamentos e regulamentação de privacidade e proteção de dados		**47,5%**
	1.1 Definições	7,5%
	1.2 Dados pessoais	17,5%
	1.3 Fundamentos legítimos e limitação de finalidade	5%
	1.4 Requisitos adicionais para processamento legítimo de dados pessoais	5%
	1.5 Direitos dos titulares dos dados	2,5%
	1.6 Violação de dados pessoais e procedimentos relacionados	10%
2. Organizando a proteção de dados		**35%**
	2.1 Importância da proteção de dados para a organização	12,5%
	2.2 Autoridade supervisora[1]	7,5%
	2.3 Transferência de dados pessoais para países terceiros	7,5%
	2.4 Regras corporativas vinculantes (BCR) e proteção de dados em contratos	7,5%
3. Práticas de proteção de dados		**17,5%**
	3.1 Proteção de dados desde a concepção (by design) e por padrão (by default)	5%
	3.2 Avaliação de Impacto sobre a Proteção de Dados (DPIA)	5%
	3.3 Dados pessoais em uso	7,5%
	Total	**100%**

[1] Antes da introdução do GDPR, a *autoridade de proteção de dados* era chamada de autoridade nacional, sendo esta a responsável pela aplicação do regulamento sobre proteção de dados. Após a entrada em vigor do GPDR, ela agora é chamada de *autoridade supervisora*.

Especificações do exame

1 Fundamentos e regulamentação de privacidade e proteção de dados

1.1 Definições

O candidato é capaz de …

1.1.1 definir privacidade.

1.1.2 relacionar privacidade a dados pessoais e proteção dos dados.

1.1.3 descrever o contexto da legislação da União e do Estado-Membro.

1.2 Dados pessoais

O candidato é capaz de …

1.2.1 definir dados pessoais de acordo com o GDPR.

1.2.2 distinguir dados pessoais e categorias especiais de dados, como dados pessoais sensíveis.

1.2.3 descrever os direitos do titular dos dados com relação aos dados pessoais.

1.2.4 definir processamento de dados pessoais que se enquadre no escopo do GDPR.

1.2.5 listar os papéis, responsabilidades e partes interessadas conforme o GDPR.

1.3 Fundamentos legítimos e limitação de finalidade

O candidato é capaz de …

1.3.1 listar os seis fundamentos legítimos para processamento.

1.3.2 descrever o conceito e a limitação de finalidade.

1.3.3 descrever proporcionalidade e subsidiariedade.

1.4 Requisitos adicionais para processamento legítimo de dados pessoais

O candidato é capaz de …

1.4.1 descrever os requisitos para processamento legítimo de dados.

1.4.2 descrever a finalidade do processamento de dados.

1.4.3 explicar os princípios relacionados ao processamento de dados pessoais.

1.5 Direitos dos titulares dos dados

O candidato é capaz de…

1.5.1 descrever os direitos relacionados à portabilidade de dados e direito de inspeção.

1.5.2 descrever o direito ao esquecimento.

1.6 Violação de dados pessoais e procedimentos relacionados

O candidato é capaz de …

1.6.1 descrever o conceito de violação de dados pessoais.

1.6.2 explicar os procedimentos sobre como agir quando ocorre uma violação de dados pessoais.

1.6.3 dar exemplos de categorias de violação de dados pessoais.

1.6.4 descrever a diferença entre uma violação de segurança (incidente) e violação de dados pessoais.

1.6.5 listar as partes interessadas relevantes que devem ser informadas no caso de uma violação de dados pessoais.

2 Organizando a proteção de dados

2.1 Importância da proteção de dados para a organização

O candidato é capaz de …

2.1.1 listar os diferentes tipos de administração (artigos 28 e 30 do GDPR).

2.1.2 indicar quais atividades são necessárias para estar em conformidade com o GDPR.

2.1.3 definir a proteção de dados desde a concepção (by design) e por padrão (by default).

2.1.4 dar exemplos de violação de dados pessoais.

2.1.5 descrever a obrigação de notificação de violação de dados pessoais conforme estabelecido no GDPR.

2.1.6 descrever a execução das regras mediante a emissão de sanções, incluindo multas administrativas.

2.2 Autoridade supervisora

O candidato é capaz de …

2.2.1 descrever as responsabilidades gerais de uma autoridade supervisora.

2.2.2 descrever o papel e as responsabilidades de uma autoridade supervisora em relação a violações de dados pessoais.

2.2.3 descrever como uma autoridade supervisora contribui para a aplicação do GDPR.

2.3 Transferência de dados pessoais para países terceiros

O candidato é capaz de …

2.3.1 descrever a regulamentação que é aplicada na transferência de dados dentro da Área Econômica Europeia (AEE).

2.3.2 descrever a regulamentação que é aplicada na transferência de dados fora da AEE.

2.3.3 descrever a regulamentação que é aplicada na transferência de dados entre a AEE e os Estados Unidos da América (EUA).

2.4 Regras corporativas vinculantes (BCR) e proteção de dados em contratos

O candidato é capaz de …

2.4.1 descrever o conceito de BCR.

2.4.2 descrever como a proteção de dados é formalizada em contratos entre o controlador e o processador.

2.4.3 descrever as cláusulas desse tipo de contrato.

3 Práticas de proteção de dados

3.1 Proteção de dados desde a concepção (by design) e por padrão (by default)

O candidato é capaz de …

3.1.1 descrever os benefícios da proteção de dados desde a concepção e por padrão.

3.1.2 descrever os sete princípios da proteção de dados desde a concepção.

3.2 Avaliação de Impacto sobre a Proteção de Dados (DPIA)

O candidato é capaz de …

3.2.1 descrever o que um DPIA aborda e quando um DPIA deve ser realizado.

3.2.2 mencionar os oito objetivos de um DPIA.

3.2.3 listar os tópicos de um relatório de DPIA.

3.3 Dados pessoais em uso

O candidato é capaz de …

3.3.1 descrever os objetivos da Gestão do Ciclo de Vida do Dado (GCVD).

3.3.2 explicar a retenção e minimização de dados.

3.3.3 descrever o que é um cookie e qual a sua finalidade.

3.3.4 descrever o direito de oposição ao processamento de dados pessoais com finalidade de marketing direto, inclusive definição de perfis.

3. Lista de conceitos básicos

Este capítulo contém os termos e abreviaturas com que os candidatos devem se familiarizar.

Por favor, note que o conhecimento destes termos de maneira independente não é suficiente para o exame; O candidato deve compreender os conceitos e estar apto a fornecer exemplos.

Inglês	Português
adequate	adequado
appropriate technical and organizational measures	medidas técnicas e organizacionais apropriadas
authenticity	autenticidade
availability	disponibilidade
awareness	conscientização
benchmark	benchmark (referência comparativa)
binding corporate rules (BCR)	regras corporativas vinculantes (BCR)
certification / certification bodies	certificação / organismos de certificação
codes of conduct	códigos de conduta
collecting personal data	coletar dados pessoais
commission reports	relatórios de comissão
complaint	reclamação
compliance	conformidade
consent • child's consent • conditions for consent • explicit consent	consentimento • consentimento da criança / do menor de idade • condições para o consentimento • consentimento explícito
consistency / consistency mechanism	consistência / mecanismo de consistência
constitution	constituição
controller	controlador
cross-border processing	processamento transfronteiriço
data accuracy	exatidão de dados
data breach	violação de dados
data classification system	sistema de classificação de dados
data concerning health	dados relativos à saúde
data lifecycle management (DLM)	Gestão do Ciclo de Vida do Dado (GCVD / DLM)
data mapping	mapeamento dos dados
data privacy breach response plan	plano de resposta à violação de dados
data protection	proteção de dados
data protection authority (DPA)	Autoridade de Proteção de Dados (DPA)
data protection by default / privacy by default	proteção de dados por padrão (by default) / privacidade por padrão (by default)
data protection by design / privacy by design	proteção de dados desde a concepção (by design) / privacidade desde a concepção (by design)

data protection impact assessment (DPIA)	Avaliação de Impacto sobre a Proteção de Dados (DPIA)
data protection officer (DPO) • designation • position • tasks	Data Protection Officer (DPO) • designação • posição • tarefas / responsabilidades
data subject	titular dos dados
data subject access (facilities)	acesso do titular dos dados (instalações)
data transfer	transferência de dados
declaration of consent	declaração de consentimento
delegated acts and implementing acts • committee procedure	atos delegados e atos de implementação • procedimento de comitê
derogation	exceção
documentation obligation	obrigação de documentar
enforcement • administrative fines • administrative penalties • criminal penalties • dissuasive penalties • effective penalties • proportionate penalties	execução / fiscalização • multas administrativas • sanções administrativas • sanções criminais • sanções dissuasivas • sanções efetivas • sanções proporcionais
enterprise	empresa
EU types of legal act • decision • directive • opinion • recommendation • regulation	tipos de atos legais da União Europeia (UE) • decisão • diretiva • opinião • recomendação • regulamento
European Data Protection Board • chair • confidentiality • independence • procedure • reports • secretariat • tasks	Comitê Europeu para Proteção de Dados • presidência • confidencialidade • independência • procedimento • relatórios • secretariado • tarefas / responsabilidades
European Data Protection Supervisor (EDPS)	Autoridade Europeia para a Proteção de Dados (EDPS)
European Economic Area (EEA)	Área Econômica Europeia (AEE)
European Union legal acts on data protection	Atos jurídicos da União Europeia sobre proteção de dados
exchange of information	troca de informações
exemption	isenção
filing system	sistema de arquivos
General Data Protection Regulation (GDPR)	Regulamento Geral de Proteção de Dados (GDPR)
governing body	órgão do governo
group of undertakings	grupo empresarial
information society service	serviço da sociedade da informação
international organization	organização internacional

joint controllers	co-controladores
judicial remedy	medida judicial
lawfulness of processing	legalidade do processamento
legal basis	base legal
legitimate basis (GDPR recital 40)	fundamento legítimo (item 40 do preâmbulo do GDPR)
legitimate ground (GDPR Article 17(1c), Article 18(1d), Article 21(1))	base legítima (artigo 17(1c), artigo 18(1d), artigo 21(1) do GDPR)
legitimate interest	interesse legítimo
liability	responsabilidade
main establishment	sede da empresa
material scope	escopo de aplicação material
non-repudiation	não repúdio
notification obligation	obrigação de notificar
opinion of the board	parecer do Comitê
personal data	dados pessoais
personal data breach	violação de dados pessoais
personal data relating to criminal convictions and offences	dados pessoais relativos a condenações e infrações criminais
principles relating to processing of personal data (GDPR, Article 5) • accountability • accuracy • confidentiality • data minimization • fairness • integrity • lawfulness • purpose limitation • storage limitation • transparency	princípios relacionados ao processamento de dados pessoais (artigo 5 do GDPR) • responsabilidade • exatidão • confidencialidade • minimização de dados • equidade • integridade • legalidade • limitação de finalidade • limitação de armazenamento • transparência
prior consultation	consulta prévia
privacy	privacidade
privacy analysis	análise de privacidade
privacy officer/chief privacy officer	Privacy Officer/Chief Privacy Officer
processing (of personal data)	processamento (de dados pessoais)
processing situations • data protection rules of churches and religious associations • employment • for archiving purposes in the public interest • for scientific or historical research purposes • for statistical purposes • freedom of expression and information • National Identification Number • obligations of secrecy • public access to official documents	situações de processamento • regras de proteção de dados de igrejas e associações religiosas • emprego • para fins de arquivamento por interesse público • para fins de pesquisa histórica ou científica • para fins estatísticos • liberdade de expressão e informação • Número de Identificação Nacional • obrigações de sigilo • acesso público a documentos oficiais

processing which does not require identification	processamento que não requer identificação
processor	processador
profiling	definição de perfis
proportionality, the principle of	proporcionalidade, princípio da
pseudonymization	pseudonimização
recipient	destinatário
relevant and reasoned objection	objeção relevante e fundamentada
representative	representante
restriction of processing	limitação de processamento
retention period	período de retenção
rights of the data subject • 'right to be forgotten' • automated individual decision-making • data portability • information and access • modalities • notification obligation • rectification and erasure • restriction of processing • restrictions • right to compensation • right to objection • transparency	direitos do titular dos dados: • 'direito ao esquecimento' • tomada de decisão individual automatizada • portabilidade de dados • informação e acesso • modalidades • obrigação de notificação • retificação e apagamento • limitação do processamento • restrições • direito à compensação • direito à oposição • transparência
rules of procedure	regras de procedimento
security breach	violação de segurança
security incident	incidente de segurança
security of personal data	segurança de dados pessoais
security of processing	segurança de processamento
sensitive data	dados sensíveis
seven principles for privacy by design	sete princípios da privacidade desde a concepção (by design) e por padrão (by default)
special categories of personal data • biometric data • data concerning health • genetic data • political opinions • racial or ethnic origin • religious or philosophical beliefs • sex life or sexual orientation • trade union membership	categorias especiais de dados pessoais • dados biométricos • dados relativos à saúde • dados genéticos • opiniões políticas • origem racial ou étnica • crenças religiosas ou convicções filosóficas • vida sexual ou orientação sexual • associação sindical
subsidiarity, the principle of	subsidiariedade, princípio da
supervisory authority	autoridade supervisora
supervisory authority concerned	autoridade supervisora competente
suspension of proceedings	suspensão do processo
territorial scope	escopo de aplicação territorial
third party	terceiro

threat	ameaça
transfer of personal data to third countries and to international organizations • adequacy decision • appropriate safeguards • binding corporate rules (BCR) • derogations • disclosures • international protection of personal data	transferência de dados pessoais para países terceiros e para organizações internacionais • decisão de adequação • salvaguardas apropriadas • regras corporativas vinculantes (BCR) • exceções • divulgações • proteção internacional de dados pessoais
vulnerability	vulnerabilidade

Comentário

A tabela abaixo apresenta a tradução dos termos utilizados no GDPR, que encontra-se escrito em Português de Portugal, para Português do Brasil. (Por favor note que os materiais de exame do EXIN estão todos escritos em Português do Brasil).

Portugal	**Brasil**
responsável pelo tratamento	controlador
subcontratante	processador
encarregado da proteção de dados	Data Protection Officer (DPO)
autoridade de controlo	autoridade supervisora
coimas	multa
tratamento	processamento
derrogação	exeção
ficheiro	arquivo
por defeito	por padrão *(by default)*
pessoa singular	pessoa física
pessoa coletiva	pessoa jurídica
cláusulas-tipo	cláusulas padrão
vinculativo	vinculante

4. Literatura

Literatura do exame

O conhecimento necessário para o exame é coberto na seguinte literatura:

A. L. Besemer
White Paper – Privacidade, Dados Pessoais e GDPR
Faça o download gratuito em http://bit.ly/PDPF_PR_literature

Literatura adicional

B. European Commission
General Data Protection Regulation (GDPR) Regulation (EU) 2016/679) Regulation of the European Parliament and the Council of the European Union. Bruxelas, 6 de abril de 2016, disponível em:
http://eur-lex.europa.eu
PDF:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
HTML:
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=EN

C. A. Cavoukian
Privacy by Design – The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

D. A. Calder
EU GDPR, A pocket guide
IT Governance Publishing
ISBN 978-1-84928-855-2
(ou ISBN 978-1-84928-857-6 parar e-book)

Comentário

A literatura adicional destina-se exclusivamente à referência e aprofundamento do conhecimento.

O GDPR (literatura B) não é uma literatura primária de exame porque a literatura do exame fornece conteúdo suficiente sobre o GDPR. Os candidatos devem estar familiarizados com o GDPR na extensão das referências feitas na literatura do exame.

Matriz da literatura

Requisitos do exame	Especificações do exame	Referência na literatura	Referência no GDPR	Referência na ISO/IEC 27701
1. Fundamentos e regulamentação de privacidade e proteção de dados				
	1.1 Definições	A, Capítulo 1	Preâmbulo 1, 2 & Artigo 96-99	*sem referência*
	1.2 Dados pessoais	A, Capítulo 1, Capítulo 2	Artigo 4.1(a), Artigo 9.1, Artigo 17, Artigo 4.10	Sub-cláusula 7.2.2, Sub-cláusula 7.3.6
	1.3 Fundamentos legítimos e limitação de propósito	A, Capítulo 3	Artigo 6.1, Artigo 24	Sub-cláusula 7.2.2
	1.4 Requisitos adicionais para processamento legítimo de dados pessoais	A, Capítulo 3	Artigo 25, Artigo 27-32, Artigo 5	Sub-cláusula 5.2.1. *Artigo 5 é citada ao longo da norma.*
	1.5 Direitos dos titulares dos dados	A, Capítulo 4	Artigo 15, Artigo 16, Artigo 17, Artigo 18, Artigo 20, Artigo 21, Artigo 22	Sub-cláusula 7.2.2, Sub-cláusula 7.3.2, Sub-cláusula 7.3.6, Sub-cláusula 7.3.9, Sub-cláusula 7.3.10, Sub-cláusula 7.5.1
	1.6 Violação de dados pessoais e procedimentos relacionados	A, Capítulo 5	Artigo 4(12), Artigo 33, Artigo 34	Sub-cláusula 6.13.1.5
2. Organizando a proteção de dados				
	2.1 Importância da proteção de dados para a organização	A, Capítulo 2, Capítulo 3, Capítulo 5, Capítulo 6, Capítulo 7	Artigo 7, Artigo 8, Artigo 13, Artigo 25(1), Artigo 30, Artigo 83	Sub-cláusula 6.11.2.1, Sub-cláusula 6.11.2.5, Sub-cláusula 7.2.3, Sub-cláusula 7.2.4, Sub-cláusula 7.2.5, Sub-cláusula 7.2.8, Sub-cláusula 7.3.2, Sub-cláusula 7.3.6, Sub-cláusula 7.3.10, Sub-cláusula 7.5, Sub-cláusula 8.2.6, Sub-cláusula 8.5.2, Sub-cláusula 8.5.3
	2.2 Autoridade supervisora	A, Capítulo 7	Artigo 33, Artigo 34, Artigo 36	Sub-cláusula 5.2.2, Sub-cláusula 6.13.1.1, Sub-cláusula 6.13.1.5, Sub-cláusula 7.2.5
	2.3 Transferência de dados pessoais para países terceiros	A, Capítulo 7	Artigo 29, Artigo 30, Artigo 45	Sub-cláusula 7.2.8, Sub-cláusula 7.5, Sub-cláusula 8.2.2, Sub-cláusula 8.2.6

	2.4 Regras corporativas vinculantes (BCR) e proteção de dados em contratos	A, Capítulo 7	Artigo 24, Artigo 28, Artigo 47	Sub-cláusula 5.2.1, Sub-cláusula 6.12.1.2, Sub-cláusula 7.2.6, Sub-cláusula 7.2.8, Sub-cláusula 7.5.1, Sub-cláusula 8.5
3. Práticas de proteção de dados				
	3.1 Proteção de dados desde a concepção (by design) e por padrão (by default)	A, Capítulo 7, Capítulo 8	Artigo 25	Seção B.8.4, Sub-cláusula 6.11.2.1, Sub-cláusula 6.11.2.5, Sub-cláusula 7.4.2
	3.2 Avaliação de Impacto sobre a Proteção de Dados (DPIA)	A, Capítulo 8	Artigo 35	Sub-cláusula 5.2.2, Sub-cláusula 7.2.5, Sub-cláusula 8.2.1
	3.3 Dados pessoais em uso	A, Capítulo 4, Capítulo 8	*sem referência*	Seção B.8.2.3

Contato EXIN

www.exin.com