# EXIN Privacy & Data Protection

FOUNDATION


## Guia de preparação

Edição 201809

# 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 de um profissional sobre a organização da proteção de dados pessoais, as regras e regulamentos da UE (União Europeia) em matéria de proteção de dados.

### Resumo

Onde quer que os dados pessoais sejam coletados, armazenados, usados e, finalmente, excluídos ou destruídos, surgem preocupações de privacidade. Com o Regulamento Geral de Proteção de Dados da UE (GDPR), o Conselho da União Europeia tenta 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 cidadãos da EU e tem efeitos além destas fronteiras. O PDPF abrange os principais assuntos relacionados ao GDPR e tem sido usado como um guia para diversos países fora da UE em fase de elaboração das suas próprias leis..

### Contexto

O certificado EXIN Privacy & Data Protection Foundation (PDPF) faz parte do programa de qualificação EXIN Privacy & Data Protection.

### Grupo alvo

Todos os colaboradores precisam ter uma compreensão da proteção de dados e dos requisitos legais, conforme definido no GDPR. As seguintes funções mais específicas podem se interessar: DPO (Diretor de Proteção de Dados), Privacy Officer (Diretor de Privacidade), Legal Officer / Compliance Officer (Diretor Jurídico / Diretor de Conformidade), Security Officer (Diretor de Segurança), Business Continuity Manager (Gerente de Continuidade de Negócios).

### Requisitos para a certificação

- Conclusão do exame EXIN Privacy & Data Protection Foundation com sucesso.

### Detalhes do exame

| | |
|---|---|
| Tipo de exame: | Pergunta de múltipla escolha |
| Número de questões: | 40 |
| Mínimo para aprovação: | 65% |
| Com consulta/observações: | Não |
| Equipamentos eletrônicos permitidos: | Não |
| Tempo designado para o exame: | 60 minutos |

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

### Taxonomia de Bloom

A certificação EXIN Privacy & Data Protection Foundation testa candidatos no Bloom Nível 1 e Nível 2 de acordo com a Taxonomia Bloom Revisada:

- Bloom Level 1: Remembering (Lembrança) - depende da recuperação de informações. Os candidatos precisarão absorver, lembrar, reconhecer e recordar. Este é o elemento fundamental da aprendizagem antes que os candidatos possam avançar para níveis mais elevados.
- Bloom Level 2: Understanding (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.

## Treinamento

### Horas de contato

O número recomendado de horas presenciais para esse treinamento é de 15 horas. Isso inclui atribuições em grupo, preparação para o exame e paradas curtas (breaks). Este número de horas não inclui tarefas para casa, a logística (preparação) relacionada à sessão do exame, a sessão do exame e intervalos de almoço.

### Carga de estudos indicada

60 horas, dependendo do conhecimento existente.

### Provedores de Treinamentos

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 do módulo (requisitos do exame) e subtópicos (especificações do exame).

| Requisito do exame | Especificação do exame | Peso |
|---|---|---|
| **1. Fundamentos e regulamentação de privacidade e proteção de dados** | | **44.5%** |
| | 1.1 Definições | 7.5% |
| | 1.2 Dados pessoais | 12% |
| | 1.3 Fundamentos legítimos e limitação de propósito | 5% |
| | 1.4 Requisitos adicionais para processamento legítimo de dados pessoais | 5% |
| | 1.5 Direitos do titular dos dados | 5% |
| | 1.6 Violação de dados e procedimentos relacionados | 10% |
| **2. Organizando a proteção de dados** | | **35.5%** |
| | 2.1 Importância da proteção de dados para a organização | 13% |
| | 2.2 Autoridade Fiscalizadora[1] | 7.5% |
| | 2.3 Transferência de dados pessoais para outros países | 7.5% |
| | 2.4 Normas Corporativas Globais e proteção de dados em contratos | 7.5% |
| **3. Práticas de proteção de dados** | | **20%** |
| | 3.1 Proteção de dados *by design* e por padrão | 5% |
| | 3.2 Avaliação de Impacto sobre a Proteção de Dados (DPIA) | 5% |
| | 3.3 Aplicações práticas relacionadas ao uso de dados, marketing e mídias sociais | 10% |
| | Total | 100% |

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

## Especificações do exame

**1 Fundamentos e regulamentação de Privacidade e Proteção de Dados**

1.1 Definições

O candidato é capaz de …

1.1.1 dar definições válidas de privacidade.

1.1.2 relacionar a privacidade, em dados pessoais específicos, ao conceito de proteção de 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 dar uma definição de dados pessoais de acordo à GDPR.

1.2.2 fazer a distinção entre dados pessoais e categorias especiais como dados pessoais sensíveis.

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

1.2.4 descrever o processamento/tratamento dos dados pessoais.

1.2.5 listar os papéis, responsabilidade e stakeholders.

1.3 Fundamentos legítimos e limitação de propósito

O candidato é capaz de …

1.3.1 listar os seis fundamentos legítimos para processamento/ tratamento.

1.3.2 descrever o conceito e a limitação de propósito.

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 requerimentos para processamento/ tratamento dos dados.

1.4.2 descrever o propósito do processamento/ tratamento dos dados.

1.4.3 explicar os princípios relacionados ao processamento/ tratamento de dados pessoais.

1.5 Direitos do titular dos dados

O candidato …

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

1.5.2 está ciente do “direito ao esquecimento”.

1.6 Violação de dados e procedimentos relacionados

O candidato é capaz de …

1.6.1 descrever o conceito de violação de dados.

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

1.6.3 dar exemplos de categorias de violação de dados.

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

1.6.5 mencionar os *stakeholders* importantes que deveriam ser informados.

## 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 (GDPR art 28 & 30).

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

2.1.3 dar uma definição de proteção de dados *by design* e por padrão.

2.1.4 dar exemplos de violação de dados.

2.1.5 descrever a obrigação de notificação de violação de dados conforme estabelecido na GDPR.

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

2.2 Autoridade Fiscalizadora

O candidato é capaz de …

2.2.1 descrever as responsabilidades de uma autoridade fiscalizadora.

2.2.2 descrever o papel de uma autoridade fiscalizadora com relação às violações de dados.

2.2.3 descrever como uma autoridade fiscalizadora contribui para a aplicação da GDPR.

2.3 Transferência de dados pessoais para outros países

O candidato é capaz de …

2.3.1 descrever a regulamentação que é aplicada na transferência de Dados dentro da EEA (Economic European Area).

2.3.2 descrever a regulamentação que é aplicada na transferência de Dados fora da EEA.

2.3.3 descrever a regulamentação que é aplicada na transferência de Dados entre a EEA e USA.

2.4 Regras Corporativas compulsórias e proteção de dados em contratos

O candidato é capaz de …

2.4.1 descrever o conceito de regras corporativas compulsórias (BCR).

2.4.2 descrever como a proteção de dados é formalizada em contratos escritos entre o *controller* e o *processor* (operador).

2.4.3 descrever as cláusulas deste contrato escrito.

## 3 Práticas de Proteção de Dados

3.1 Proteção de Dados *by design* e por padrão

O candidato é capaz de …

3.1.1 descrever os benefícios da aplicação dos princípios de Proteção de Dados *by design* e por padrão.

3.1.2 descrever os sete princípios da proteção de dados *by design*.

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

O candidato é capaz de …

3.2.1 descrever o que é um DPIA e quando aplicar um DPIA.

3.2.2 mencionar os oito objetivos de um DPIA.

3.2.3 listar os tópicos de um relatório DPIA.

3.3 Aplicações práticas relacionadas ao uso de dados, marketing e mídias sociais

O candidato é capaz de …

3.3.1 descrever os objetivos do Gerenciamento do Ciclo de Vida do Dado ( Data Life Cycle - DLC).

3.3.2 explicar a retenção e minimização de dados.

3.3.3 descrever o que é um cookie e qual o seu objetivo.

3.3.4 descrever, do ponto de vista da proteção de dados, como o uso generalizado da internet afetou a área de marketing.

3.3.5 dar exemplos sobre como as informações de midia social são usadas para atividades de Marketing.

# 3. Lista de conceitos básicos

Este capítulo contém os termos 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 |
| binding | compulsório |
| binding corporate rules (BCR) | Regras Corporativas Compulsórias |
| biometric data | dados biométricos |
| certification | certificação |
| certification bodies | organismos de certificação |
| child's consent | consentimento da criança / do menor de idade |
| codes of conduct | códigos de conduta |
| collection of personal data (verb.) | coletar dados pessoais |
| commission reports | relatórios de comissão |
| complaint | reclamação |
| compliance | conformidade |
| conditions for consent | condições para consentimento |
| consent | consentimento |
| consistency | consistência |
| consistency mechanism | mecanismo consistente |
| constitution | constituição |
| contract | contrato |
| controller | controlador |
| cross-border processing | processamento transfronteiriço |
| data breach | violação de dados |
| data concerning health | dados relativos à saúde |
| data controller | responsável pelo tratamento dos dados |
| data protection | proteção de dados |
| data protection authority | Autoridade de Proteção de Dados (DPA) |
| data protection by default | proteção de dados por padrão |
| data protection by design | proteção de dados desde a concepção (by design) |
| Data Protection Impact Assessment (DPIA) | Avaliação de Impacto sobre a Proteção de Dados (AIPD) |

| | |
|---|---|
| data protection officer (DPO)<br>• designation<br>• position<br>• tasks | Data Protection Officer (DPO)<br>• designação<br>• posição<br>• tarefas |
| data subject | titular dos dados |
| data transfer | transferência de dados |
| delegated acts and implementing acts<br>• committee procedure | atos delegados e atos de implementação<br>• procedimento de comitê |
| derogation | derrogação |
| enforcement<br>• administrative fines<br>• administrative penalties<br>• criminal penalties<br>• dissuasive penalties<br>• effective penalties<br>• proportionate penalties | Execução<br>• multas administrativas<br>• sanções administrativas<br>• sanções criminais<br>• sanções dissuasivas<br>• sanções efetivas<br>• sanções proporcionais |
| enterprise | empresa |
| European Economic Area (EEA) | Área Econômica Europeia |
| EU types of legal act<br>• decision<br>• directive<br>• opinion<br>• recommendation<br>• regulation | Tipos de atos legais da União Europeia (UE)<br>• decisão<br>• diretiva<br>• opinião<br>• recomendação<br>• regulamentação |
| European Data Protection Board<br>• chair<br>• confidentiality<br>• independence<br>• procedure<br>• reports<br>• secretariat<br>• tasks | Comitê Europeu para Proteção de Dados<br>• presidência<br>• confidencialidade<br>• independência<br>• procedimento<br>• relatórios<br>• secretariado<br>• tarefas |
| European Data Protection Supervisor (EDPS) | Autoridade Europeia para a Proteção de Dados (AEPD / EDPS) |
| European Union legal acts on data protection | Atos jurídicos da União Europeia sobre proteção de dados |
| exchange of information | troca de informações |
| exemption | isenção |
| explicit consent | consentimento explícito |
| genetic data | dados genéticos |
| filing system | sistema de arquivos |
| General Data Protection Regulation (GDPR) | General Data Protection Regulation (GDPR) |
| governing body | órgão administrativo |
| group of undertakings | grupo empresarial |
| independent supervisory authorities<br>• activity reports<br>• competence<br>• establishment<br>• powers<br>• tasks | autoridades supervisoras independentes<br>• relatórios de atividades<br>• competência<br>• estabelecimento<br>• atribuições, poderes<br>• tarefas |
| information society service | serviço da sociedade da informação |

| | |
|---|---|
| international organization | organização internacional |
| joint controllers | joint controllers (responsáveis conjuntos) |
| judicial remedy | medida judicial |
| lawfulness of processing | legalidade do processamento |
| legal basis | base legal |
| legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) | interesse legítimo (RGPD artigo 17/1c, artigo 18/1d, artigo 21/1) |
| legitimate basis (GDPR article 40) | base legítima (RGPD artigo 40) |
| legitimate interest | interesse legítimo |
| liability | responsabilidade |
| main establishment | sede da empresa |
| material scope | escopo de aplicação material |
| National Identification Number | Número de Identificação Nacional |
| non-repudiation | não repúdio |
| 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<br>• accountability<br>• accuracy<br>• confidentiality<br>• data minimization<br>• fairness<br>• integrity<br>• lawfulness<br>• purpose limitation<br>• storage limitation<br>• transparency | princípios relacionados ao processamento de dados pessoais<br>• responsabilidade<br>• precisão<br>• confidencialidade<br>• tratamento mínimo dos dados<br>• equidade<br>• integridade<br>• legalidade<br>• limitação de propósito<br>• limitação de armazenamento<br>• transparência |
| prior consultation | consulta prévia |
| privacy | privacidade |
| processing | processamento |
| processing situations<br>• data protection rules of churches and religious associations<br>• employment<br>• for archiving purposes in the public interest<br>• for scientific or historical research purposes<br>• for statistical purposes<br>• freedom of expression and information<br>• National Identification Number<br>• obligations of secrecy<br>• public access to official documents | situações de processamento<br>• regras de proteção de dados de igrejas e associações religiosas<br>• emprego<br>• para fins de arquivamento por interesse público<br>• para fins de pesquisa histórica ou científica<br>• para fins estatísticos<br>• liberdade de expressão e informação<br>• Número de Identificação Nacional<br>• obrigações de sigilo<br>• acesso públco a documentos oficiais |

| | |
|---|---|
| processing which does not require identification | processamento que não requer identificação |
| processor | processador |
| profiling | definição de perfis |
| 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 |
| right to compensation | direito a compensação |
| rights of the data subject<br>• automated individual decision-making<br>• data portability<br>• information and access<br>• modalities<br>• notification obligation<br>• rectification and erasure<br>• restriction of processing<br>• restrictions<br>• 'right to be forgotten'<br>• right to objection<br>• transparency | direitos do titular do dado:<br>• tomada de decisão individual automatizada<br>• portabilidade de dados<br>• Informação e acesso<br>• modalidades<br>• obrigação de notificação<br>• retificação e apagamento<br>• restrição de processamento<br>• restrições<br>• "direito ao esquecimento"<br>• direito à objeção, oposição ou questionamento<br>• transparência |
| rules of procedure | regras de procedimento |
| security breach (security incident) | violação de segurança (incidente de segurança) |
| security of personal data | segurança de dados pessoais |
| security of processing | segurança de processamento |
| sensitive data | dados sensíveis |
| special categories of personal data<br>• biometric data<br>• data concerning health<br>• genetic data<br>• political opinions<br>• racial or ethnic origin<br>• religious or philosophical beliefs<br>• sex life or sexual orientation<br>• trade union membership | categorias especiais de dados pessoais<br>• dados biométricos<br>• dados sobre saúde<br>• dados genéticos<br>• opiniões políticas<br>• origem étnica ou racial<br>• crenças religiosas ou filosóficas<br>• vida sexual ou orientação sexual<br>• associação sindical |
| 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 |

transfer of personal data to third countries and to international organizations
- adequacy decision
- appropriate safeguards
- binding corporate rules
- derogations
- disclosures
- international protection of personal data

transferência de dados pessoais para países terceiros e para organizações internacionais
- decisão de adequação
- salvaguardas apropriadas
- regras vinculantes aplicáveis à empresas
- derrogações
- divulgações
- proteção internacional de dados pessoais

# 4. Literatura do exame

## Literatura do exame

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

**B.** L. Besemer
**White Paper – Privacidade, Dados Pessoais e GDPR**
Faça o download gratuito em www.exin.com

**C.** European Commission
**General Data Protection Regulation (GDPR)** Regulation (EU) 2016/679) Regulation of the European Parliament and the Council of the European Union. Brussels, 6 April 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

### Comentário

Os requisitos do exame são baseados na literatura do exame. Literatura C não é uma literatura de exame primário porque a literatura de outros exames fornece conteúdo suficiente sobre o GDPR. Os candidatos devem estar familiarizados com a literatura C na extensão das referências feitas nas outras literaturas.

## Referência de literatura

| Requisito do exame | Especificação do exame | Literatura | GDPR referência |
|---|---|---|---|
| **1. Fundamentos e regulamentação de privacidade e proteção de dados** | | | |
| | 1.1 Definições | A: Cap. 1, Cap. 3<br>B: §1.1.1 | rec. 1, 2 & art 96-99 |
| | 1.2 Dados pessoais | A: Cap. 2, Cap. 3<br>B: §1.1.3, §1.3.6, §1.3.7, §4 | art. 4.1 (a), art 9.1, art 17, art 4.10 |
| | 1.3 Fundamentos legítimos e limitação de propósito | B: §3.1, §3.2, §3.3 | art 6.1, art 24 |
| | 1.4 Requisitos adicionais para processamento legítimo de dados pessoais | B: §2.1, §6.1 | art 25, art 27-32, art 5 |
| | 1.5 Direitos do titular dos dados | B: §4.3, §4.4.2 | sem ref. |
| | 1.6 Violação de dados e procedimentos relacionados | B: §5.1-5.3 | art 4(12), art 33, art 34 |
| **2. Organizando a proteção de dados** | | | |
| | 2.1 Importância da proteção de dados para a organização | A: Cap. 3, Cap. 4<br>B: §5.2, §5.3, §6.1, §6.3, §8.1 | art 7, art 8, art 13, art 30, art 25(1), art 83 |
| | 2.2 Autoridade Fiscalizadora | A: Cap. 3<br>B: §7.1, §7.3 | art 36, art 33, art 34 |
| | 2.3 Transferência de dados pessoais para outros países | B: §7.4 | art 29, art 30, art 45 |
| | 2.4 Normas Corporativas Globais e proteção de dados em contratos | A: Cap. 3<br>B: §7.4.3.3, §8.2 | art 47, art 24, art 28 |
| **3. Práticas de proteção de dados** | | | |
| | 3.1 Proteção de dados by design e por padrão | B: §5.2, §8.1.1 | sem ref. |
| | 3.2 Avaliação de Impacto sobre a Proteção de Dados (DPIA) | B: §6.1.3, §8.3, §8.5 | sem ref. |
| | 3.3 Aplicações práticas relacionadas ao uso de dados, marketing e mídias sociais | B: §8.4, §8.6 | sem ref. |
| | | | |

# Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER