
# Guia de preparação

Edição 201812

# Conteúdo

# 1. Visão geral

EXIN Privacy & Data Protection Practitioner (PDPP.PR)

### Escopo

EXIN Privacy & Data Protection Practitioner é uma certificação que valida o conhecimento e a compreensão de um(a) profissional sobre a legislação de privacidade europeia (proteção de dados) e sua relevância internacional, assim como sua capacidade de aplicar este conhecimento e compreensão na prática profissional.

### Resumo

Com a explosão cada vez maior de informações que inundam a internet, todas as empresas devem planejar como gerenciar e proteger a privacidade das pessoas e seus dados. Não é à toa que muitas novas leis - na UE, assim como nos EUA e em muitas outras regiões - estão sendo formuladas para a sua regulação.
Recentemente, a Comissão Europeia publicou o General Data Protection Regulation (GDPR) na UE, o que significa que todas as organizações envolvidas devem cumprir regras específicas. Esta certificação de nível Practitioner é baseada nos temas abordados pelo exame Foundation, enfocando o desenvolvimento e a implementação de políticas e procedimentos para o cumprimento da legislação nova e da já existente, aplicação de diretrizes e melhores práticas para privacidade e proteção de dados e estabelecimento de um Sistema de Gestão de Proteção de Dados e Privacidade.

### Contexto

O certificado EXIN Privacy & Data Protection Practitioner (PDPP) faz parte do programa de qualificação em EXIN Privacy & Data Protection.

## Público alvo

Esta certificação em nível Practitioner será particularmente útil para Data Protection Officers (DPOs) ou “Encarregados pelo Tratamento de Dados Pessoais” em uma organização / Privacy Officers, Legal/Compliance Officers, Security Officers, Gerentes de Continuidade de Negócios, Controladores dos Dados, Auditores de Proteção de Dados (internos e externos), Analistas de Privacidade e gerentes de RH.
Uma vez que esta é uma certificação de nível avançado, a aprovação prévia no EXIN Data & Protection Foundation é altamente recomendada.

## Requisitos para a certificação

- Treinamento credenciado para Privacy & Data Protection Practitioner, incluindo a conclusão bem-sucedida das Atividades Práticas;
- Aprovação no exame EXIN Privacy & Data Protection Practitioner.

## Detalhes do exame

| | |
|---|---|
| Tipo de exame: | Perguntas de múltipla escolha |
| Número de questões: | 40 |
| Mínimo para aprovação: | 65% |
| Com consulta/observações: | Não, com exceção da literatura C, que pode ser consultada durante todo o exame. Ela é fornecida como um apêndice no exame digital. Traga sua cópia se o exame for realizado em papel. |
| Equipamentos eletrônicos permitidos: | Não |
| Tempo designado para o exame: | 120 minutos |

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

## Taxonomia de Bloom

A certificação EXIN Privacy & Data Protection Practitioner testa candidatos nos Níveis Bloom 2, 3 e 4 de acordo com a Taxonomia Bloom Revisada:

- 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.
- Nível Bloom 3: Aplicação – mostra que os candidatos têm a capacidade de utilizar as informações em um contexto diferente daquele em que elas foram aprendidas.
  Este tipo de pergunta pretende demonstrar que o candidato é capaz de resolver problemas em novas situações, aplicando o conhecimento adquirido, fatos, técnicas e regras de um modo novo ou diferente. A pergunta geralmente contém um breve cenário
- Nível Bloom 4: Análise – mostra que os candidatos têm a capacidade de decompor as informações aprendidas em suas partes, para compreendê-las. Este nível Bloom é testado principalmente nas Atividades Práticas. As Atividades Práticas têm o objetivo de demonstrar que o candidato é capaz de examinar e decompor a informação em partes, identificando motivos ou causas, fazer inferências e encontrar evidências para respaldo de generalizações.

# Treinamento

## Horas de contato

O número recomendado de horas presenciais para esse treinamento é de 21 horas. Isso inclui atividades em grupo, preparação para o exame e intervalos curtos (breaks). Este número de horas não inclui tarefas para casa, a logística (preparação) relacionada à realização do exame, a efetiva realização do exame e intervalos de almoço. O número recomendado de horas para as Atividades Práticas corresponde a no máximo 8 horas. As Atividades Práticas podem ser realizadas fora do treinamento. Elas também podem ser incluídas no treinamento, se a duração do treinamento for prolongada.
Se o provedor de treinamento quiser dedicar algum tempo para a legislação nacional de privacidade e proteção de dados, isto exigirá horas de treinamento adicionais além das 21 horas de treinamento recomendadas.

## Carga de estudos indicada

120 horas, dependendo do conhecimento existente. A matriz da literatura no Capítulo *4*. *Literatura* neste Guia de Preparação refere-se ao corpo de conhecimento que é testado no exame.

## 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. Políticas de proteção de dados** | | **10%** |
| | 1.1 O candidato compreende o objetivo das políticas de proteção de dados/privacidade em uma organização. | 5% |
| | 1.2 O candidato compreende os conceitos de proteção de dados desde a concepção (by design) e por padrão (by default). | 5% |
| **2. Gerenciando e organizando a proteção de dados** | | **35%** |
| | 2.1 O candidato é capaz de aplicar as fases do Sistema de Gestão de Proteção de Dados (DPMS). | 35% |
| | 2.2 O candidato é capaz de aplicar a teoria de um plano de ação para conscientização sobre a proteção de dados.[1] | 0% |
| **3. Papéis do Controlador, Processador e Data Protection Officer (DPO)** | | **15%** |
| | 3.1 O candidato é capaz de implementar os papéis do controlador e processador de dados. | 7.5% |
| | 3.2 O candidato é capaz de estabelecer o papel e as responsabilidades de um DPO. | 7.5% |
| **4. Avaliação de Impacto sobre a Proteção de Dados (AIPD)** | | **30%** |
| | 4.1 O candidato é capaz de aplicar os critérios para uma AIPD. | 15% |
| | 4.2 O candidato é capaz de aplicar as etapas de uma AIPD. | 15% |
| **5. Violação de dados, notificação e resposta a incidentes** | | **10%** |
| | 5.1 O candidato é capaz de aplicar os requisitos do GDPR em relação a violações de dados pessoais. | 5% |
| | 5.2 O candidato é capaz de aplicar os requisitos para notificação. | 5% |
| | Total | 100% |

[1] A especificação de exame 2.2 não está incluída no exame, uma vez que ainda não existe um material de referência adequado. As perguntas do exame sobre esta especificação serão acrescentadas em uma versão posterior.

## Especificações do exame

**1 Políticas de proteção de dados**

1.1 O objetivo das políticas de proteção de dados/privacidade em uma organização

O candidato é capaz de ...

1.1.1 explicar as políticas e os procedimentos necessários em uma organização para cumprir a legislação de proteção de dados.

1.1.2 explicar o teor das políticas.

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

O candidato é capaz de ...

1.2.1 explicar o conceito de proteção de dados desde a concepção (by design) e por padrão (by default).

1.2.2 descrever os sete princípios da proteção de dados desde a concepção (by design) e por padrão (by default).

1.2.3 ilustrar de que modo os princípios de privacidade desde a concepção (by design) e por padrão (by default) podem ser implementados.

**2 Gerenciando e organizando a proteção de dados**

2.1 Fases do Sistema de Gestão de Proteção de Dados (DPMS).

O candidato é capaz de ...

2.1.1 ilustrar como aplicar a fase 1 do DPMS: Proteção de Dados e Privacidade: Preparação

2.1.2 ilustrar como aplicar a fase 2 do DPMS: Proteção de Dados e Privacidade: Organização

2.1.3 ilustrar como aplicar a fase 3 do DPMS: Proteção de Dados e Privacidade: Desenvolvimento e implementação

2.1.4 ilustrar como aplicar a fase 4 do DPMS: Proteção de Dados e Privacidade: Governança

2.1.5 ilustrar como aplicar a fase 5 do DPMS: Proteção de Dados e Privacidade: Avaliação e melhoria

2.2 Um plano de ação para conscientização sobre a proteção de dados[2]

O candidato é capaz de ...

2.2.1 preparar um plano de ação para conscientização sobre proteção de dados em uma situação específica.

**3 Papéis do Controlador, Processador e Data Protection Officer (DPO)**

3.1 Os papéis do controlador e processador de dados

O candidato é capaz de ...

3.1.1 estabelecer as responsabilidades do controlador.

3.1.2 estabelecer as responsabilidades do processador.

3.1.3 explicar a relação entre o controlador e o processador em uma situação específica.

[2] A especificação de exame 2.2 não está incluída no exame, uma vez que ainda não existe um material de referência adequado. As perguntas do exame sobre esta especificação serão acrescentadas em uma versão posterior.

3.2 O papel e as responsabilidades de um DPO

O candidato é capaz de ...

3.2.1 explicar quando um DPO é obrigatório de acordo com o GDPR.

3.2.2 estabelecer o papel do DPO.

3.2.3 explicar a posição do DPO em relação à autoridade supervisora.

**4 Avaliação de Impacto sobre a Proteção de Dados (AIPD)**

4.1 Os critérios para uma AIPD

O candidato é capaz de ...

4.1.1 aplicar os critérios para a condução de uma AIPD.

4.1.2 descrever os objetivos e os resultados de uma AIPD.

4.2 As etapas de uma AIPD

O candidato é capaz de ...

4.2.1 descrever as etapas de uma AIPD.

4.2.2 realizar uma AIPD em uma situação específica.

**5 Violação de dados, notificação e resposta a incidentes**

5.1 Do GDPR em relação a violações de dados pessoais

O candidato é capaz de ...

5.1.1 determinar se houve uma violação de dados nos termos do GDPR.

5.2 Os requisitos para notificação

O candidato é capaz de ...

5.2.1 notificar a autoridade supervisora sobre uma violação de dados pessoais.

5.2.2 notificar o titular dos dados sobre a violação de dados pessoais.

5.2.3 descrever os elementos da obrigação de documentação do GDPR.

# 3. Lista de conceitos básicos

Este capítulo contém os termos com os quais 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.

| English | Portuguese |
|---|---|
| adequate | adequado |
| appropriate technical and organizational measures | medidas técnicas e organizacionais apropriadas |
| audit<br>• initial data (protection) audit<br>• internal and external data (protection) audit | auditoria<br>• auditoria inicial de (proteção de) dados<br>• auditoria interna e externa de (proteção de) dados |
| authenticity | autenticidade |
| availability | disponibilidade |
| awareness | conscientização (sensibilização/capacitação) |
| benchmark | benchmark (referência comparativa) |
| binding | compulsório / vinculante |
| binding corporate rules | regras corporativas compulsórias (BCR) / vinculantes |
| biometric data | dados biométricos |
| Bring Your Own Device (BYOD) | Bring Your Own Device (BYOD) |
| certification | certificação |
| certification bodies | organismos de certificação |
| child's consent | consentimento da criança / do menor de idade |
| cloud computing | computação em nuvem (cloud computing) |
| 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 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 controller | controlador dos dados |
| data lifecycle management (DLM) | Gestão do Ciclo de Vida do Dado (GCVD / DLM) |
| data mapping | mapeamento dos dados |

| | |
|---|---|
| data portability | portabilidade de dados |
| data protection | proteção de dados |
| (data privacy) breach response plan / data privacy incident response plan | plano de resposta a violações (dos dados) / plano de resposta a incidentes de privacidade |
| data protection authority (DPA) | Autoridade de Proteção de Dados (DPA)[3] |
| data protection by default / privacy by default | proteção de dados por padrão |
| data protection by design / privacy by design | proteção de dados desde a concepção (by design) |
| data protection impact assessment (DPIA) / privacy impact assessment (PIA) | Avaliação de Impacto sobre a Proteção de Dados (AIPD) |
| Data Protection Management System (DPMS) / Data Protection and Privacy Management System (DPMS) | Sistema de Gestão de Proteção de Dados (SGPD) / Sistema de Gestão de Privacidade e Proteção de Dados (SGPPD) |
| data protection officer (DPO)<br>• designation<br>• position<br>• tasks | data protection officer (DPO)<br>• designação<br>• posição<br>• tarefas |
| data protection policy | política de proteção de dados |
| data protection program | programa de proteção de dados |
| data protection provisions | disposições em matéria de proteção de dados |
| 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<br>• committee procedure | atos delegados e atos de implementação<br>• procedimento de comitê |
| derogation | derrogação / exceção |
| 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 |
| documentation obligation | obrigação de documentar |
| enterprise | empresa |
| European Economic Area (EEA) | Área Econômica Europeia (AEE) |
| 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 / regulamento |

[3] Antes da introdução do GDPR, a Autoridade de Proteção de Dados (DPA) era a autoridade nacional em países da UE encarregada da execução da legislação sobre a proteção de dados. No GDPR, ela é chamada atualmente de autoridade supervisora.

| | |
|---|---|
| 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 |
| filing system | sistema de arquivos |
| General Data Protection Regulation (GDPR) | General Data Protection Regulation (GDPR) |
| genetic data | dados genéticos |
| governing body | órgão administrativo |
| group of undertakings | grupo empresarial |
| incident response | resposta a incidente |
| 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 Security Management System (ISMS) | Sistema de Gestão de Segurança da Informação (ISMS) |
| information society service | serviço da sociedade da informação |
| international organization | organização internacional |
| Internet of Things (IOT) | Internet das Coisas (IoT) |
| joint controllers | joint controllers (responsáveis conjuntos) |
| judicial remedy | medida judicial |
| lawfulness of processing | legalidade do tratamento / processamento |
| legal basis | base legal |
| legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) and legitimate basis (GDPR article 40) | interesse legítimo (GDPR artigo 17/1c, artigo 18/1d, artigo 21/1) e base legítima (GDPR artigo 40) |
| legitimate interest | interesse legítimo |
| liability | responsabilidade |
| main establishment | sede da empresa |
| material scope | escopo de aplicação material |
| measures based on DPIA results | medidas baseadas nos resultados da AIPD |
| National Identification Number | Número de Identificação Nacional |
| 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<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 tratamento 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 |
| policy | política |
| policy rule(s) | regra(s) da política |
| prior consultation | consulta prévia |
| privacy | privacidade |
| privacy analysis | análise de privacidade |
| privacy officer/chief privacy officer | privacy officer/chief privacy officer |
| processing | processamento |
| processing (of personal data) | processamento (de dados pessoais) |
| processing agreement | acordo de 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 |
| proportionality, the principle of | proporcionalidade, princípio da |
| pseudonymization | pseudonimização |
| quality cycle | ciclo de qualidade |
| recipient | destinatário |
| relevant and reasoned objection | objeção relevante e fundamentada |
| repealed | revogado / anulado |
| representative | representante |
| restriction of processing | limitação de processamento |
| retention period | período de retenção / armazenamento |
| 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 |
| risk management | gerenciamento de risco |
| 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 |
| service provider | provedor de serviços |
| seven principles for privacy by design (Lit. A Chapter 5, paragraph Privacy by design and by default) | sete princípios da privacidade desde a concepção e por padrão (by design / by default) |
| Social, Mobile, Analytics, Cloud, Things (SMACT) | Social, Móvel, Analytics, Nuvem, Coisas (SMANC) |
| 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 |
| 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<br>• adequacy decision<br>• appropriate safeguards<br>• binding corporate rules<br>• derogations<br>• disclosures<br>• international protection of personal data | transferência de dados pessoais para países terceiros e para organizações internacionais<br>• decisão de adequação<br>• salvaguardas apropriadas<br>• regras vinculantes aplicáveis à empresas<br>• derrogações<br>• divulgações<br>• proteção internacional de dados pessoais |
| unified communications and collaboration (UCC) | Comunicações e Colaborações Unificadas (CCU) |
| vulnerability | vulnerabilidade |

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 | 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 do exame

## Literatura do exame

O conhecimento necessário para o exame EXIN Privacy and Data Protection Practitioner é coberto pela seguinte literatura.

**A.** IT Governance Privacy Team
**EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide**
IT Governance Publishing, Cambridgeshire (2016)
ISBN 978-1-84928-8354 (versão impressa)
ISBN 978-1-84928-8378 (e-book)

**B.** Kyriazoglou, J.
**Data Protection and Privacy Management System. Data Protection and Privacy Guide - Vol. 1**
bookboon.com primeira edição (2016)
ISBN 978-87-403-1540-0

**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, available at 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

**D.** Article 29 Data Protection Working Party
**Guidelines on Data Protection Officers ('DPOs'), wp 243rev.01**, 5 April 2017 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

**E.** Article 29 Data Protection Working Party
**Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248**, 4 April 2017 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

### Comentário

Os requisitos do exame são baseados na literatura do exame. A literatura C não representa uma literatura de exame essencial porque outras literaturas de exame proporcionam um conteúdo suficiente sobre o GDPR. Os candidatos devem estar familiarizados com a literatura C em relação às referências presentes em outras literaturas. A literatura C pode ser consultada durante todo o exame. Ela é fornecida como um apêndice no exame digital. Traga sua cópia se o exame for realizado em papel.

## Literatura adicional

**F.** Example of Privacy by Design Framework
https://www.privacycompany.eu/files/DPbD_Framework.pdf

### Comentário

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

## Visão geral da literatura

| Requisito do exame | Especificação do exame | Literatura |
|---|---|---|
| **1. Políticas de proteção de dados** | | |
| | 1.1 O candidato compreende o objetivo das políticas de proteção de dados/privacidade em uma organização. | A: Capítulo 16 parágrafo Using policies to demonstrate compliance |
| | 1.2 O candidato compreende os conceitos de proteção de dados desde a concepção (by design) e por padrão (by default). | A: Capítulo 5 parágrafo Privacy by design and by default |
| **2. Gerenciando e organizando a proteção de dados** | | |
| | 2.1 O candidato é capaz de aplicar as fases do Sistema de Gestão de Proteção de Dados (DPMS). | A: Capítulo 12 parágrafo Records of processing<br>A: Capítulo 14 introdução + parágrafo Notification<br>B: Capítulo 2, parágrafo 2 DP&P System Phases |
| | 2.2 O candidato é capaz de aplicar a teoria de um plano de ação para conscientização sobre a proteção de dados. | *Sem literatura ainda* |
| **3. Papéis do Controlador, Processador e Data Protection Officer (DPO)** | | |
| | 3.1 O candidato é capaz de implementar os papéis do controlador e processador de dados. | A: Capítulo 12 |
| | 3.2 O candidato é capaz de estabelecer o papel e as responsabilidades de um DPO. | A: Capítulo 2<br>B: Capítulo 2 parágrafo 2 Phase 4<br>D: Capítulo 2 parágrafo 1 Mandatory designation<br>D: Capítulo 4 Tasks of the DPO<br>D: Capítulo 5 parágrafo 1 Which organizations must appoint a DPO? |
| **4. Avaliação de Impacto sobre a Proteção de Dados (AIPD)** | | |
| | 4.1 O candidato é capaz de aplicar os critérios para uma AIPD. | A: Capítulo 5 introdução, parágrafo Privacy Impact Assessments e parágrafo When to conduct a DPIA<br>A: Capítulo 6 parágrafo DPIA's as part of risk management<br>A: Capítulo 8 parágrafo Objectives and outcomes<br>E: Capítulo 3 DPIA: the Regulation explained |

| | | |
|---|---|---|
| | 4.2 O candidato é capaz de aplicar as etapas de uma AIPD. | A: Capítulo 5 parágrafo Privacy Impact Assessments<br>A: Capítulo 7<br>A: Capítulo 8 parágrafo Five key stages in a DPIA and parágrafo Consultation<br>E: Capítulo 3 DPIA: the Regulation explained |
| **5. Violação de dados, notificação e resposta a incidentes** | | |
| | 5.1 O candidato é capaz de aplicar os requisitos do GDPR em relação a violações de dados pessoais. | E: Capítulo 3 parágrafo Personal data breaches, Anatomy of a data breach, Sites of attack<br>E: Capítulo 14 parágrafo Notification, parágrafo Events vs incidents, parágrafo Types of incidents |
| | 5.2 O candidato é capaz de aplicar os requisitos para notificação. | E: Capítulo 14 parágrafo Notification, parágrafo Key roles in incident management, parágrafo Respond e parágrafo Follow up |
| | | |

### Comentário

A literatura C (o GPDR) não conta com referências detalhadas.

# Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER