

Guia de preparação

Edição 202509

Copyright © EXIN Holding B.V. 2025. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Conteúdo

1. Visão geral 4
2. Requisitos do exame 8
3. Lista de conceitos básicos 11
4. Literatura 16
5. Career Path 19

1. Visão geral

EXIN Privacy & Data Protection Professional (PDPP.PR)

Escopo

A certificação EXIN Privacy & Data Protection Professional valida o conhecimento do candidato sobre:

- políticas de proteção de dados
- Sistema de Gestão de Informações de Privacidade (PIMS)
- papéis do controlador, processador e Data Protection Officer (DPO)
- Avaliação de Impacto sobre a Proteção de Dados (DPIA)
- violação de dados, notificação e resposta a incidentes

Resumo

A certificação EXIN Privacy & Data Protection Professional abrange a legislação europeia sobre privacidade e proteção de dados e sua relevância internacional, assim como a capacidade do profissional de aplicar esse conhecimento e compreensão à prática profissional diária.

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 de seus dados. Portanto, muitas novas leis na UE, assim como nos EUA e em muitas outras regiões, estão sendo formuladas para regulamentar a privacidade e a proteção de dados.

A Comissão Europeia publicou o Regulamento Geral de Proteção de Dados (GDPR) na UE, o que significa que, a partir de 25 de maio de 2018, todas as organizações envolvidas devem cumprir regras específicas. Essa certificação de nível avançado é baseada nos temas abordados pelo exame EXIN Privacy & Data Protection 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 (SGPD).

A 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 dessa 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 do exame, o GDPR e a norma ISO/IEC 27701:2019 para fornecer um contexto mais amplo à certificação.

Contexto

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



Público-alvo

Esta certificação em nível avançado será particularmente útil para:

- Data Protection Officers (DPOs) / privacy officers
- legal/compliance officers
- security officers
- gerentes de continuidade de negócios
- controladores de dados
- auditores de proteção de dados (internos e externos)
- analistas de privacidade
- gerentes de RH

Requisitos para a certificação

- Conclusão bem-sucedida do exame EXIN Privacy & Data Protection Professional.
- Treinamento credenciado de EXIN Privacy & Data Protection Professional, incluindo exercícios práticos.

Detalhes do exame

Tipo do exame:	Questões de múltipla escolha
Número de questões:	40
Mínimo para aprovação:	65% (26/40 questões)
Com consulta:	O texto do GDPR pode ser consultado durante todo o exame. Ele é fornecido como um apêndice no exame digital. Os candidatos devem trazer suas próprias cópias para exames em papel.
Anotações:	Não
Equipamentos eletrônicos permitidos:	Não
Tempo designado para o exame:	120 minutos

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

Nível Bloom

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

- 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. Esse 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. Esse 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. Esse nível Bloom é testado principalmente nos exercícios práticos. Os exercícios práticos 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

A carga horária recomendada para este treinamento é de 21 horas. Isso inclui exercícios práticos, preparação para o exame e pausas curtas. Essa carga horária não inclui pausas para almoço, trabalhos extra-aula e o exame.

Indicação de tempo de estudo

112 horas (4 ECTS), 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. Políticas de proteção de dados		**10%**
	1.1 O objetivo das políticas de proteção de dados e privacidade em uma organização	5%
	1.2 A proteção de dados desde a concepção (by design) e por padrão (by default)	5%
2. Sistema de Gestão de Informações de Privacidade (PIMS)		**32,5%**
	2.1 Os fundamentos do Sistema de Gestão de Informações de Privacidade (PIMS)	12,5%
	2.2 Os benefícios de um Sistema de Gestão de Informações de Privacidade (PIMS)	10%
	2.3 As relações do Sistema de Gestão de Informações de Privacidade (PIMS)	10%
3. Papéis do controlador, processador e Data Protection Officer (DPO)		**17,5%**
	3.1 Os papéis do controlador e processador	10%
	3.2 O papel e as responsabilidades de um Data Protection Officer (DPO)	7,5%
4. Avaliação de Impacto sobre a Proteção de Dados (DPIA)		**27,5%**
	4.1 Os critérios para uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)	15%
	4.2 As etapas de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)	12,5%
5. Violação de dados, notificação e resposta a incidentes		**12,5%**
	5.1 Os requisitos do GDPR em relação a violações de dados pessoais	2,5%
	5.2 Os requisitos para notificação	10%
	Total	**100%**

Especificações do exame

1 Políticas de proteção de dados

1.1 O objetivo das políticas de proteção de dados e 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 A 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 Sistema de Gestão de Informações de Privacidade (PIMS)

2.1 Os fundamentos do Sistema de Gestão de Informações de Privacidade (PIMS)

O candidato é capaz de...

2.1.1 explicar os diferentes termos usados na norma ISO/IEC 27701 (questões internas e externas, partes interessadas).

2.1.2 listar que meios devem ser considerados ao implementar um PIMS.

2.1.3 definir o que é uma Declaração de Aplicabilidade (SoA).

2.1.4 explicar a finalidade da documentação em um PIMS.

2.1.5 explicar a finalidade das avaliações feitas pela alta liderança em um PIMS.

2.2 Os benefícios de um Sistema de Gestão de Informações de Privacidade (PIMS)

O candidato é capaz de...

2.2.1 explicar a objetivo das auditorias em um PIMS.

2.2.2 explicar como determinar os requisitos específicos de um PIMS à luz das regras locais pertinentes e dos requisitos contratuais.

2.2.3 explicar como um PIMS e as auditorias ajudam a demonstrar conformidade com normas e regulamentações.

2.2.4 explicar como um PIMS pode ajudar na seleção de fornecedores.

2.3 As relações do Sistema de Gestão de Informações de Privacidade (PIMS)

O candidato é capaz de...

2.3.1 explicar a diferença entre um Sistema de Gestão de Informações de Privacidade (PIMS) e um Sistema de Gestão de Segurança da Informação (ISMS).

2.3.2 explicar a relação entre o princípio que determina a proteção de dados por meio de medidas apropriadas de segurança da informação e a norma ISO/IEC 27701.

2.3.3 explicar a utilidade da norma ISO/IEC 27002 para a implementação de um PIMS.

2.3.4 explicar como aplicar controles do PIMS.

3 Papéis do controlador, processador e Data Protection Officer (DPO)

3.1 Os papéis do controlador e processador

O candidato é capaz de...

3.1.1 desempenhar as responsabilidades do controlador.

3.1.2 desempenhar as responsabilidades do processador.

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

3.2 O papel e as responsabilidades de um Data Protection Officer (DPO)
O candidato é capaz de...
3.2.1 explicar quando a indicação de um DPO é obrigatória de acordo com o GDPR.
3.2.2 desempenhar 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 (DPIA)

4.1 Os critérios para uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)
O candidato é capaz de...
4.1.1 aplicar os critérios para a condução de uma DPIA.
4.1.2 descrever os objetivos e os resultados de uma DPIA.

4.2 As etapas de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)
O candidato é capaz de...
4.2.1 descrever as etapas de uma DPIA.
4.2.2 realizar uma DPIA em uma situação específica.

5 Violação de dados, notificação e resposta a incidentes

5.1 Os requisitos 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 e abreviaturas com que os candidatos devem se familiarizar.

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

Inglês	**Português**
appropriate technical and organizational measures	medidas técnicas e organizacionais apropriadas
audit	auditoria
authenticity	autenticidade
availability	disponibilidade
awareness	conscientização
bring your own device (BYOD)	bring your own device (BYOD)
certification (bodies)	certificação (organismos)
cloud computing	computação em nuvem (cloud computing)
code of conduct	código 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 consentimento • consentimento explícito
consistency mechanism	mecanismo de consistência
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 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 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)	Data Protection Officer (DPO)
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 • committee procedure	atos delegados e atos de implementação • procedimento de comitê
documentation obligation	obrigação de documentar
enforcement	execução/cumprimento
EU types of legal act	tipos de atos legais da União Europeia (UE)
European Data Protection Board	Comitê Europeu para Proteção de Dados
European Data Protection Supervisor (EDPS)	Autoridade Europeia para a Proteção de Dados (AEPD/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
General Data Protection Regulation (GDPR)	Regulamento Geral de Proteção de Dados (GDPR)
governing body	órgão administrativo / órgão do governo
group of undertakings	grupo empresarial
incident response	resposta a incidentes
independent supervisory authorities • activity reports • competence • establishment • powers • tasks	autoridades supervisoras independentes • relatórios de atividade • competência • estabelecimento • poderes • tarefas/responsabilidades
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	co-controladores
judicial remedy	medida judicial
lawfulness of processing	legalidade do processamento
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
policy (rules)	política (regras)

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 • lealdade • integridade • licitude • limitação de finalidade • limitação de armazenamento • transparência
prior consultation	consulta prévia
privacy	privacidade
privacy analysis	análise de privacidade
privacy information management system (PIMS)	Sistema de Gestão de Informações de Privacidade (PIMS)
privacy officer	Privacy Officer
processing (of personal data)	processamento (de dados pessoais)
processing agreement	acordo de processamento
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
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

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 • 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 • direto à compensação • direito à oposição • transparência
risk management	gerenciamento de risco
rules of procedure	regras de procedimento
security breach	violação de segurança
security incident	incidente de segurança
service provider	provedor de serviços
seven principles for privacy by design	sete princípios da privacidade desde a concepção (by design) e por padrão (by default)
Social [media], Mobile [technology], [advanced] Analytics, Cloud and [internet of] Things (SMACT)	[mídias] Sociais, [tecnologia] Mobile, Analytics [avançado], Nuvem e [internet das] Coisas (no inglês, SMACT)
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	categorias especiais de dados pessoais • dados biométricos • dados sobre saúde • dados genéticos • opiniões políticas • origem étnica ou racial • crenças religiosas ou convicções filosóficas • vida sexual ou orientação sexual
trade union membership	filiação a sindicato
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
unified communications and collaboration (UCC)	Comunicações e Colaborações Unificadas (CCU)
vulnerability	vulnerabilidade

Comentário

A tabela abaixo apresenta a tradução dos termos utilizados no GDPR, que se encontra 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
coima	multa
tratamento	processamento
derrogação	exceção
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. IT Governance Privacy Team
EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide
IT Governance Publishing (quarta edição, 2020)
ISBN 9781787782495 (pdf)
ISBN 9781787782501 (e-book)
ISBN 9781787782518 (Kindle)
ISBN 9781787782488 (versão impressa)
ISBN 9781787782495 (audiobook)

B. Alan Shipman & Steve Watkins
ISO/IEC 27701:2019: An introduction to privacy information management
IT Governance Publishing (2020)
ISBN 9781787781993 (versão impressa)
ISBN 9781787782013 (e-book)

Literatura adicional

C. Comissão Europeia
Regulamento Geral de Proteção de Dados (GDPR) (Regulamento (UE) 2016/679)
Regulamento do Parlamento Europeu e do Conselho da União Europeia. Bruxelas, 27 de abril de 2016

D. Grupo de Trabalho do Artigo 29º Para a Proteção de Dados
Orientações sobre os encarregados da proteção de dados (EPD), wp 243rev.01, 5 de abril de 2017

E. Grupo de Trabalho do Artigo 29º Para a Proteção de Dados
Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679, wp248, 4 de abril de 2017

F. A. Cavoukian
Privacy by Design - The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

G. ISO/IEC 27701:2019 (EN)
Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines
Suíça, ISO/IEC (2019)
https://www.iso.org/home.html

Comentário

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

O texto do GDPR (fonte C) não representa uma literatura de exame primária porque outras literaturas do exame proporcionam um conteúdo suficiente sobre o GDPR. Os candidatos devem estar familiarizados com as referências ao GDPR presentes nas outras literaturas.

Matriz da literatura

Requisitos do exame	Especificações do exame	Referência na literatura	Referência no GDPR	Referência na ISO/IEC 27701
1. Políticas de proteção de dados				
	1.1 O objetivo das políticas de proteção de dados e privacidade em uma organização	A, Capítulo 1, Capítulo 16	*sem referência*	*sem referência*
	1.2 A proteção de dados desde a concepção (by design) e por padrão (by default)	A, Capítulo 5	Artigo 25	Sessão B.8.4, Subcláusula 6.11.2.1, Subcláusula 6.11.2.5, Subcláusula 7.4.2
2. Sistema de Gestão de Informações de Privacidade (PIMS)				
	2.1 Os fundamentos do Sistema de Gestão de Informações de Privacidade (PIMS)	B, Capítulo 1, Capítulo 2, Capítulo 3, Capítulo 4	*sem referência*	*Documento completo*
	2.2 Os benefícios de um Sistema de Gestão de Informações de Privacidade (PIMS)	B, Capítulo 2, Capítulo 3, Capítulo 4, Capítulo 5	*sem referência*	*Documento completo*
	2.3 As relações do Sistema de Gestão de Informações de Privacidade (PIMS)	B, Capítulo 3, Capítulo 4, Capítulo 5, Capítulo 6	*sem referência*	*Documento completo*
3. Papéis do controlador, processador e Data Protection Officer (DPO)				
	3.1 Os papéis do controlador e processador	A, Capítulo 12	Artigo 24, Artigo 26, Artigo 27, Artigo 28, Artigo 29	Subcláusula 5.2.1, Subcláusula 6.3.1.1, Subcláusula 6.12.1.2, Subcláusula 6.15.1.1, Subcláusula 7.2.6, Subcláusula 7.2.7, Subcláusula 8.2.1, Subcláusula 8.2.4, Subcláusula 8.2.5, Subcláusula 8.5.4, Subcláusula 8.5.6, Subcláusula 8.5.7, Subcláusula 8.5.8
	3.2 O papel e as responsabilidades de um DPO	A, Capítulo 2	Artigo 37, Artigo 38, Artigo 39	Subcláusula 6.3.1.1, Subcláusula 6.4.2.2, Subcláusula 6.10.2.4

4. Avaliação de Impacto sobre a Proteção de Dados (DPIA)				
	4.1 Os critérios para uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)	A, Capítulo 5, Capítulo 6, Capítulo 7, Capítulo 8	Artigo 35	Subcláusula 5.2.2, Subcláusula 7.2.5, Subcláusula 8.2.1
	4.2 As etapas de uma Avaliação de Impacto sobre a Proteção de Dados (DPIA)	A, Capítulo 5, Capítulo 7, Capítulo 8	*sem referência*	Subcláusula 5.2.2, Subcláusula 7.2.5, Subcláusula 8.2.1
5. Violação de dados, notificação e resposta a incidentes				
	5.1 Os requisitos do GDPR em relação a violações de dados pessoais	A, Capítulo 3, Capítulo 14	Artigo 4(12), Artigo 33, Artigo 34	Subcláusula 6.13.1.1, Subcláusula 6.13.1.5
	5.2 Os requisitos para notificação	A, Capítulo 14	Artigo 33, Artigo 34	Subcláusula 6.13.1.1, Subcláusula 6.13.1.5

5. Career Path

O EXIN acredita no valor do aprendizado contínuo e na importância de combinar diversas habilidades para prosperar no atual mundo dinâmico e em evolução. Com os EXIN Career Paths, os candidatos podem se preparar para funções específicas e continuar crescendo e avançando em sua jornada profissional. Para obter mais informações sobre os EXIN Career Paths, consulte https://www.exin.com/career-paths/.

A certificação EXIN Privacy & Data Protection Professional faz parte do seguinte EXIN Career Path.

EXIN Data Protection Officer

EXIN Data Protection Officer capacita os profissionais a implementar medidas para o gerenciamento da segurança da informação que visam à conformidade com as regulamentações de proteção de dados.





Contato EXIN

www.exin.com