



Guia de preparação

Edição 202001

Copyright © EXIN Holding B.V. 2020. 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	7
3. Lista de conceitos básicos	10
4. Literatura	16

1. Visão geral

EXIN Privacy & Data Protection Practitioner (PDPP.PR)

Escopo

EXIN Privacy and Data Protection Practitioner é uma certificação que valida o conhecimento e a compreensão de um profissional em relação à legislação de privacidade e proteção de dados europeia e sua relevância internacional, assim como sua capacidade de aplicar esse conhecimento e compreensão a sua prática profissional diária.

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. 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. 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 (SGPD).

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 para fornecer um contexto mais amplo à certificação.

Contexto

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



Público-alvo

Esta certificação em nível Practitioner 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 e Gerentes de RH.

Requisitos para a certificação

- Conclusão bem sucedida do exame EXIN Privacy & Data Protection Practitioner.
- Treinamento credenciado de EXIN Privacy & Data Protection Practitioner, 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/anotações:	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.
Equipamentos eletrônicos permitidos:	Não
Tempo designado para o exame:	120 minutos

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

Nível Bloom

A certificação EXIN Privacy & Data Protection Practitioner 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. 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 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 mínima recomendada para este treinamento é de 21 horas. Isto inclui exercícios práticos, preparação para o exame e pausas curtas. Esta carga horária não inclui pausas para almoço, trabalhos extra aula e o exame.

Se o provedor de treinamento desejar dedicar algum tempo para a legislação nacional de privacidade e proteção dos dados, isto irá requerer tempo adicional de treinamento em relação às 21 horas recomendadas de treinamento.

Indicação de tempo de estudo

120 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.

Requisito do exame	Especificação 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 Proteção de dados desde a concepção (by design) e por padrão (by default)	5%
2. Gerenciando e organizando a proteção de dados		32,5%
	2.1 Fases do Sistema de Gestão de Proteção de Dados (SGPD).	32,5%
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 DPO	7,5%
4. Avaliação de Impacto sobre a Proteção de Dados (DPIA)		27,5%
	4.1 Os critérios para uma DPIA	15%
	4.2 As etapas de uma 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 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 (SGPD)
O candidato é capaz de ...
 - 2.1.1 ilustrar como aplicar a fase 1 do SGPD: Proteção de Dados e Privacidade: Preparação.
 - 2.1.2 ilustrar como aplicar a fase 2 do SGPD: Proteção de Dados e Privacidade: Organização.
 - 2.1.3 ilustrar como aplicar a fase 3 do SGPD: Proteção de Dados e Privacidade: Desenvolvimento e implementação.
 - 2.1.4 ilustrar como aplicar a fase 4 do SGPD: Proteção de Dados e Privacidade: Governança.
 - 2.1.5 ilustrar como aplicar a fase 5 do SGPD: Proteção de Dados e Privacidade: Avaliação e melhoria.

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 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.
- 3.2 O papel e as responsabilidades de um 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 estabelecer o papel do DPO.
 - 3.2.3 explicar a posição do DPO em relação à autoridade supervisora.¹

¹Antes da introdução do GDPR, a Autoridade de Proteção de Dados (DPA) era a autoridade nacional encarregada pela fiscalização da aplicação prática da regulamentação em proteção de dados nos países da UE. Com o GDPR, a Autoridade de Proteção de Dados atualmente é chamada de autoridade supervisora.

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

4.1 Os critérios para uma 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 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 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
audit <ul style="list-style-type: none"> initial data (protection) audit internal and external data (protection) audit 	auditoria <ul style="list-style-type: none"> auditoria inicial de (proteção de) dados auditoria interna e externa de (proteção de) dados
authenticity	autenticidade
availability	disponibilidade
awareness	conscientização
benchmark	benchmark (referência comparativa)
binding corporate rules	regras corporativas vinculantes (BCR)
Bring Your Own Device (BYOD)	Bring Your Own Device (BYOD)
certification / certification bodies	certificação / organismos de certificação
cloud computing	computação em nuvem (cloud computing)
codes of conduct	códigos de conduta
collecting personal data	coletar dados pessoais
commission reports	relatórios de comissão
complaint	reclamação
compliance	conformidade
consent <ul style="list-style-type: none"> child's consent conditions for consent explicit consent 	consentimento <ul style="list-style-type: none"> consentimento da criança / do menor de idade condições para consentimento consentimento explícito
consistency mechanism	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 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 management system (DPMS)	Sistema de Gestão de Proteção de Dados (SGPD)
data protection officer (DPO) <ul style="list-style-type: none"> • designation • position • tasks 	Data Protection Officer (DPO) <ul style="list-style-type: none"> • designação • posição • tarefas / responsabilidades
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 <ul style="list-style-type: none"> • committee procedure 	atos delegados e atos de implementação <ul style="list-style-type: none"> • procedimento de comitê
derogation	exceção
documentation obligation	obrigação de documentar
enforcement <ul style="list-style-type: none"> • administrative fines • administrative penalties • criminal penalties • dissuasive penalties • effective penalties • proportionate penalties 	execução / cumprimento <ul style="list-style-type: none"> • multas administrativas • sanções administrativas • sanções criminais • sanções dissuasivas • sanções efetivas • sanções proporcionais
enterprise	empresa
EU types of legal act <ul style="list-style-type: none"> • decision • directive • opinion • recommendation • regulation 	tipos de atos legais da União Europeia (UE) <ul style="list-style-type: none"> • decisão • diretiva • opinião • recomendação • regulamento
European Data Protection Board <ul style="list-style-type: none"> • chair • confidentiality • independence • procedure • reports • secretariat • tasks 	Comitê Europeu para Proteção de Dados <ul style="list-style-type: none"> • presidência • confidencialidade • independência • procedimento • relatórios • secretariado • tarefas / responsabilidades
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

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 administrativo / órgão do governo
group of undertakings	grupo empresarial
incident response <ul style="list-style-type: none"> • activity reports • competence • establishment • independent supervisory authorities • powers • tasks 	resposta a incidentes <ul style="list-style-type: none"> • relatórios de atividade • competência • estabelecimento • autoridades supervisoras independentes • 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
legal basis	base legal
legitimate basis (GDPR recital 40)	fundamento legítimo (item 40 do Preâmbulo do GDPR)
legitimate ground	base legítima
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 do DPIA
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 / policy rules	política / regras da política

principles relating to processing of personal data (GDPR, Article 5) <ul style="list-style-type: none"> • accountability • accuracy • confidentiality • data minimization • fairness • integrity • lawfulness • purpose limitation • storage limitation • transparency 	princípios relacionados ao processamento de dados pessoais (artigo 5 do GDPR) <ul style="list-style-type: none"> • 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 officer/chief privacy officer	Privacy Officer/Chief Privacy Officer
processing (of personal data)	processamento (de dados pessoais)
processing agreement	acordo de processamento
processing situations <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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
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

<p>rights of the data subject</p> <ul style="list-style-type: none"> • '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 objection • transparency 	<p>direitos do titular dos dados:</p> <ul style="list-style-type: none"> • 'direito ao esquecimento' • tomada de decisão individual automatizada • portabilidade de dados • informação e acesso • modalidades • obrigação de notificação • retificação e apagamento • limitação o processamento • restrições • 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
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	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)
<p>special categories of personal data</p> <ul style="list-style-type: none"> • 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 	<p>categorias especiais de dados pessoais</p> <ul style="list-style-type: none"> • dados biométricos • dados sobre saúde • dados genéticos • opiniões políticas • origem étnica ou racial • 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
<p>transfer of personal data to third countries and to international organizations</p> <ul style="list-style-type: none"> • adequacy decision • appropriate safeguards • binding corporate rules (BCR) • derogations • disclosures • international protection of personal data 	<p>transferência de dados pessoais para países terceiros e para organizações internacionais</p> <ul style="list-style-type: none"> • 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

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, Cambridgeshire (segunda edição, 2017)
ISBN 978-1-84928-9450 (versão impressa)
ISBN 978-1-84928-9474 (e-book)
- B. Kyriazoglou, J.
Data Protection and Privacy Management System. Data Protection and Privacy Guide - Vol. I
bookboon.com (primeira edição, 2016)
ISBN 978-87-403-1540-0

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, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>
- D. Grupo de Trabalho do Artigo 29.º Para a Proteção de Dados
Orientações sobre os encarregados da proteção de dados (EPD), wp 243rev.01, 5 de abril de 2017, disponível em http://ec.europa.eu/newsroom/Artigo29/item-detail.cfm?item_id=612048
- E. Grupo de Trabalho do Artigo 29.º Para a Proteção de Dados
Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «susceptível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, wp248rev.01, 4 de abril de 2017, disponível em http://ec.europa.eu/newsroom/Artigo29/item-detail.cfm?item_id=611236
- 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. **Example of Privacy by Design Framework**
https://www.privacycompany.eu/files/DPbD_Framework.pdf
- H. 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 a referência e 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 em outras literaturas.

Matriz da literatura

Requisito do exame	Especificação 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	<i>sem referência</i>	<i>sem referência</i>
	1.2 Proteção de dados desde a concepção (by design) e por padrão (by default)	A, Capítulo 5	Artigo 25	Sessão B.8.4, Sub-cláusula 6.11.2.1, Sub-cláusula 6.11.2.5, Sub-cláusula 7.4.2
2. Gerenciando e organizando a proteção de dados				
	2.1 Fases do Sistema de Gestão de Proteção de Dados (SGPD)	A, Capítulo 12 Capítulo 14 B, Capítulo 2	<i>sem referência</i>	<i>sem referência</i>
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	Sub-cláusula 5.2.1, Sub-cláusula 6.3.1.1, Sub-cláusula 6.12.1.2, Sub-cláusula 6.15.1.1, Sub-cláusula 7.2.6, Sub-cláusula 7.2.7, Sub-cláusula 8.2.1, Sub-cláusula 8.2.4, Sub-cláusula 8.2.5, Sub-cláusula 8.5.4, Sub-cláusula 8.5.6, Sub-cláusula 8.5.7, Sub-cláusula 8.5.8
	3.2 O papel e as responsabilidades de um DPO	A, Capítulo 2	Artigo 37, Artigo 38, Artigo 39	Sub-cláusula 6.3.1.1, Sub-cláusula 6.4.2.2, Sub-cláusula 6.10.2.4

4. Avaliação de Impacto sobre a Proteção de Dados (DPIA)			
4.1 Os critérios para uma DPIA	A, Capítulo 5, Capítulo 6, Capítulo 7, Capítulo 8	Artigo 35	Sub-cláusula 5.2.2, Sub-cláusula 7.2.5, Sub-cláusula 8.2.1
4.2 As etapas de uma DPIA	A, Capítulo 5, Capítulo 7, Capítulo 8	<i>sem referência</i>	Sub-cláusula 5.2.2, Sub-cláusula 7.2.5, Sub-cláusula 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	Sub-cláusula 6.13.1.1, Sub-cláusula 6.13.1.5
5.2 Os requisitos para notificação	A, Capítulo 14	Artigo 33, Artigo 34	Sub-cláusula 6.13.1.1, Sub-cláusula 6.13.1.5

Contato EXIN

www.exin.com

