



Guía de preparación

Edición 201805

Copyright © EXIN Holding B.V. 2018. 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.



Índice

1. Visión general	4
2. Requisitos del examen	6
3. Lista de conceptos básicos	10
4. Bibliografía	14

1. Visión general

EXIN Privacy & Data Protection Foundation (PDPF.SP)

Alcance

EXIN Privacy & Data Protection Foundation (PDPF) es una certificación que valida el conocimiento de un profesional sobre la organización de la protección de los datos personales, las normas de la Unión Europea y los reglamentos referentes a la protección de datos.

Resumen

Allá donde se recopilen, almacenen, utilicen y, por último, se eliminen o destruyan datos personales, surgen las preocupaciones sobre privacidad. Con el Reglamento General de Protección de Datos de la UE (RGPD) el Consejo de la Unión Europea procura fortalecer y unificar la protección de datos para todos los individuos dentro de la Unión Europea (UE).

Este reglamento afecta a todas las organizaciones que hagan un tratamiento de datos personales dentro de la UE. PDPF cubre los principales temas relacionados con el RGPD.

Contexto

La certificación de EXIN Privacy & Data Protection Foundation (PDPF) forma parte del programa de cualificación de EXIN Privacy & Data Protection.



Grupo objetivo

Todos los empleados que necesiten tener una comprensión de la protección de datos y los requerimientos legales europeos tal como se definen en el RGPD. Más concretamente, podría ser interesante para los siguientes roles: Delegado de Protección de Datos, Responsable de Privacidad, Responsable Legal/Responsable de Conformidad, Responsable de Seguridad, Gestor de la Continuidad del Negocio.

Requisitos para la certificación

- Realización satisfactoria del examen EXIN Privacy & Data Protection Foundation.

Detalles del examen

Tipo de examen:	Preguntas de opción múltiple
Número de preguntas:	40
Calificación mínima para el aprobado:	65%
Consulta de libro o apuntes:	No
Equipos electrónicos permitidos:	No
Duración del examen:	60 minutos

Las normas y reglamentos de exámenes EXIN se aplican a este examen.

Taxonomía de Bloom

La certificación de EXIN Privacy & Data Protection Foundation pone a prueba a los candidatos a los niveles 1 y 2 de la Taxonomía de Bloom revisada:

- Bloom nivel 1: Recordar - se refiere a la capacidad de recordar información. Los candidatos necesitarán asimilar, recordar, reconocer y evocar. Este es el bloque de aprendizaje que los candidatos deberán superar antes de poder pasar a los niveles superiores.
- Bloom 2: Comprender – un paso más allá de recordar. La comprensión demuestra que los candidatos comprenden lo que se les presenta y son capaces de determinar cómo aplicar el material formativo en su propio entorno.

Formación

Horas de contacto

El número recomendado de horas de contacto para este curso de formación es de 15. Estas horas de contacto incluyen las prácticas de grupos, la preparación de exámenes y pausas breves. El número de horas no incluye el tiempo dedicado a los deberes, la logística relacionada con la preparación del examen o las pausas para almorzar.

Indicación de la carga de estudio

60 horas, en función de los conocimientos previos.

Proveedor de la formación

Puede consultar una lista de nuestros proveedores de formación acreditados en www.exin.com.

2. Requisitos del examen

Los requisitos del examen están detallados en las especificaciones del examen. La siguiente tabla presenta un listado de los distintos temas de cada módulo (requisitos de examen) con sus correspondientes subtemas (especificaciones del examen).

Requisito del examen	Especificación del examen	Peso
1. Fundamentos y regulación de la privacidad y la protección de datos		44.5%
	1.1 Definiciones	7.5%
	1.2 Datos personales	12%
	1.3 Motivos legítimos y limitación de la finalidad	5%
	1.4 Requisitos adicionales para el tratamiento legítimo de los datos personales	5%
	1.5 Derechos de los interesados	5%
	1.6 Violación de la seguridad de los datos y procedimientos relacionados	10%
2. Organizar la protección de datos		35.5%
	2.1 La importancia de la protección de datos para la organización	13%
	2.2 Autoridad Europea de Supervisión ¹	7.5%
	2.3 Transferencia de datos personales a terceros países	7.5%
	2.4 Normas Corporativas vinculantes y Privacidad en los contratos	7.5%
3. Práctica de la protección de datos		20%
	3.1 Protección de los datos desde el diseño y por defecto en relación a la seguridad de la información	5%
	3.2 Evaluación de impacto relativa a la protección de datos (EIPD)	5%
	3.3 Aplicaciones relacionadas con la práctica del uso de datos, marketing y redes sociales	10%
	Total	100%

¹ Antes de la introducción del RGPD la *autoridad de protección de datos* era la autoridad nacional encargada con la aplicación de la normativa sobre protección de datos. En el RGPD esta autoridad se llama ahora la *autoridad de control*.

Especificaciones del examen

1 Fundamentos y regulación de la privacidad y la protección de datos

1.1 Definiciones

El candidato es capaz de ...

1.1.1 dar definiciones validas del concepto privacidad.

1.1.2 relacionar la privacidad, en particular datos personales, con el concepto de protección de datos.

1.1.3 describir el contexto de la legislación de la Unión y de los Estados miembros.

1.2 Datos Personales

El candidato es capaz de ...

1.2.1 dar una definición de datos personales de acuerdo al Reglamento General de Protección de Datos (RGPD).

1.2.2 hacer una distinción entre datos personales y categorías especiales como datos personales sensibles.

1.2.3 describir los derechos de los interesados en relación a los datos personales.

1.2.4 describir el tratamiento de los datos personales.

1.2.5 hacer un listado de los roles, responsabilidades y de las partes interesadas.

1.3 Motivos legítimos y limitación de la finalidad

El candidato es capaz de ...

1.3.1 enumerar los seis motivos legítimos de tratamiento.

1.3.2 describir el concepto del propósito de la limitación.

1.3.3 describir los principios de proporcionalidad y la subsidiariedad.

1.4 Requisitos adicionales para el tratamiento legítimo de los datos personales

El candidato es capaz de ...

1.4.1 describir los requisitos para el tratamiento de datos.

1.4.2 describir el propósito del tratamiento de datos personales.

1.4.3 explicar los principios relacionados con el tratamiento de datos personales.

1.5 Derechos de los interesados

El candidato es capaz de ...

1.5.1 puede describir los derechos en relación a la portabilidad de los datos y el derecho de inspección.

1.5.2 es consciente del derecho al olvido.

1.6 Violación de la seguridad de los datos y procedimientos relacionados

El candidato es capaz de ...

1.6.1 describir el concepto de violación de la seguridad de los datos.

1.6.2 explicar los procedimientos sobre cómo actuar cuando se produce una violación de la seguridad de los datos.

1.6.3 proporcionar ejemplos de categorías de violación de la seguridad de los datos.

1.6.4 describir la diferencia entre incidentes de seguridad y una violación de la seguridad de los datos.

1.6.5 mencionar las partes interesadas que deberían ser informadas.

2 Organizar la protección de datos

- 2.1 La importancia de la protección de datos para la organización
El candidato es capaz de ...
 - 2.1.1 hacer una lista de los diferentes tipos de administración (RGPD art 28 & 30).
 - 2.1.2 indicar cuáles son las acciones requeridas para cumplir con el RGPD.
 - 2.1.3 dar una definición sobre la protección de datos desde el diseño y por defecto.
 - 2.1.4 dar ejemplos de violaciones de la seguridad de los datos.
 - 2.1.5 describir la obligación de notificación de la violación de la seguridad de los datos establecida en el RGPD.
 - 2.1.6 describir la aplicación de las normas mediante la emisión de sanciones incluyendo multas administrativas.
- 2.2 Autoridad Europea de Supervisión
El candidato es capaz de ...
 - 2.2.1 describir las responsabilidades generales de una autoridad europea de supervisión.
 - 2.2.2 describir el rol y la responsabilidad de una Autoridad europea de supervisión en relación con las violaciones de la seguridad de los datos.
 - 2.2.3 describir cómo una autoridad europea de supervisión contribuye a la aplicación del RGPD.
- 2.3 Transferencia de datos personales a terceros países
El candidato es capaz de ...
 - 2.3.1 de describir la normativa aplicable a la Transferencia de Información dentro del Espacio Económico Europeo (EEE).
 - 2.3.2 de describir la normativa aplicable a la Transferencia de Información fuera del EEE.
 - 2.3.3 de describir la normativa aplicable a la Transferencia de Información entre el EEE y USA.
- 2.4 Normas Corporativas vinculantes y Privacidad en los contratos
El candidato es capaz de ...
 - 2.4.1 describir el concepto de normas corporativas vinculantes (NCV).
 - 2.4.2 describir cómo se formaliza la protección de datos en los contratos escritos entre el Responsable y el encargado del tratamiento.
 - 2.4.3 describir las cláusulas de dicho contrato escrito.

3 Práctica de la protección de datos

- 3.1 Protección de los datos desde el diseño y por defecto en relación a la seguridad de la información
El candidato es capaz de ...
 - 3.1.1 describir los beneficios de la aplicación de los principios de la protección de datos desde el diseño y por defecto.
 - 3.1.2 describir los siete principios de la protección de datos desde el diseño.
- 3.2 Evaluación de impacto relativa a la protección de datos (EIPD)
El candidato es capaz de ...
 - 3.2.1 esbozar qué comprende una EIPD y cuándo aplicarlo.
 - 3.2.2 mencionar los ocho objetivos de una EIPD.
 - 3.2.3 hacer un listado de los aspectos de una informe de un EIPD.

3.3 Aplicaciones relacionadas con la práctica del uso de datos, marketing y redes sociales

El candidato es capaz de ...

- 3.3.1 describir el propósito de la gestión del Ciclo de Vida de los Datos.
- 3.3.2 explicar la retención y minimización de datos.
- 3.3.3 describir qué es una cookie y cuál es su propósito.
- 3.3.4 describir, desde una perspectiva de protección de datos, cómo el uso generalizado de Internet ha afectado al campo del marketing.
- 3.3.5 proporcionar ejemplos de cómo la información de las redes sociales se emplea en las actividades de Marketing.

3. Lista de conceptos básicos

Este capítulo contiene los términos y abreviaturas con los que los candidatos deben estar familiarizados.

Tenga en cuenta que el conocimiento de estos términos por sí solo no es suficiente para el examen, el candidato debe entender los conceptos y ser capaz de dar ejemplos.

English	Español
adequate	adecuado
appropriate technical and organizational measures	medidas técnicas y organizativas apropiadas
authenticity	autenticidad
availability	disponibilidad
binding	vinculante
binding corporate rules	normas corporativas vinculantes
biometric data	datos biométricos
certification	certificación
certification bodies	organismos de certificación
child's consent	consentimiento del niño
codes of conduct	códigos de conducta
collection of personal data (verb.)	obtener datos personales
commission reports	informes de la comisión
complaint	reclamaciones
compliance	conformidad / cumplimiento
conditions for consent	condiciones para el consentimiento
consent	consentimiento (del interesado)
consistency	coherencia
consistency mechanism	mecanismos de coherencia
constitution	constitución
contract	contrato
controller	responsable (del tratamiento)
cross-border processing	tratamiento transfronterizo
data breach	violación de la seguridad de los datos (personales)
data concerning health	datos relativos a la salud
data controller	responsable (del tratamiento)
data protection	protección de datos
• privacy	• privacidad
data protection by default	protección de datos por defecto
• privacy by default	• privacidad por defecto
data protection by design	protección de datos desde el diseño
• privacy by design	• privacidad desde el diseño
data protection impact assessment (DPIA)	evaluación de impacto relativa a la protección de datos (EIPD)

data protection officer	delegado de protección de datos
<ul style="list-style-type: none"> • designation • position • takss 	<ul style="list-style-type: none"> • designación • posición / cargo • funciones
data subject	el interesado
data transfer	transferencia de datos
delegated acts and implementing acts	actos delegados y actos de ejecución
<ul style="list-style-type: none"> • committee procedure 	<ul style="list-style-type: none"> • procedimiento de comité
derogation	excepciones
enforcement	ejecución / aplicación
<ul style="list-style-type: none"> • administrative fines • administrative penalties • criminal penalties • dissuasive penalties • effective penalties • proportionate penalties 	<ul style="list-style-type: none"> • multas administrativas • sanciones administrativas • sanciones penales • sanciones disuasorias • sanciones efectivas • sanciones proporcionadas
enterprise	empresa
European Economic Area (EEA)	Espacio Económico Europeo (EEE)
EU types of legal act	tipos de actos jurídicos europeos
<ul style="list-style-type: none"> • decision • directive • opinion • recommendation • regulation 	<ul style="list-style-type: none"> • decisión • directiva • opinión / dictamen • recomendación • reglamento / regulación
European Data Protection Board	Consejo Europeo de Protección de Datos
<ul style="list-style-type: none"> • chair • confidentiality • independence • procedure • reports • secretariat • tasks 	<ul style="list-style-type: none"> • presidente • confidencialidad • independencia • procedimiento • informes • secretaría • funciones
European Data Protection Supervisor (EDPS)	Supervisor Europeo de Protección de Datos (SEPD)
European Union legal acts on data protection	actos jurídicos de la Unión Europea en materia de protección de datos
exchange of information	intercambio de información
exemption	exención
explicit consent	consentimiento explícito
genetic data	datos genéticos
filing system	fichero
General Data Protection Regulation (GDPR)	Reglamento General de Protección de Datos (RGPD)
governing body	órgano de gobierno
group of undertakings	grupo empresarial
independent supervisory authorities	autoridades de control independientes
<ul style="list-style-type: none"> • activity reports • competence • establishment • powers • tasks 	<ul style="list-style-type: none"> • informes de actividad • competencia • establecimiento • poderes • funciones
information society service	servicio de la sociedad de la información

international organization	organización internacional
joint controllers	corresponsables (del tratamiento)
judicial remedy	tutela judicial
lawfulness of processing	licitud del tratamiento
legal basis	base jurídica
legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) and legitimate basis (GDPR article 40)	motivos legítimos (RGPD artículo 17/1c, artículo 18/1d, artículo 21/1) y base legítima (RGPD artículo 40)
legitimate interest	interés legítimo
liability	responsabilidad
main establishment	establecimiento principal
material scope	ámbito de aplicación material
National Identification Number	número nacional de identificación
non-repudiation	no repudio
opinion of the board	dictamen del Comité
personal data	datos personales
personal data breach	violación de la seguridad de los datos personales
personal data relating to criminal convictions and offences	datos personales relativos a condenas e infracciones penales
principles relating to processing of personal data	principios relativos al tratamiento (de los datos personales)
<ul style="list-style-type: none"> • accountability • accuracy • confidentiality • data minimization • fairness • integrity • lawfulness • purpose limitation • storage limitation • transparency • prior consultation 	<ul style="list-style-type: none"> • responsabilidad proactiva • exactitud • confidencialidad • minimización de datos • justicia / lealtad (fairness) • integridad • licitud • limitación de la finalidad • limitación del plazo de conservación • transparencia • consulta previa
processing	tratamiento
processing situations	situaciones de tratamiento
<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 	<ul style="list-style-type: none"> • normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas • empleo • con fines de archivo en interés público • con fines de investigación científica o histórica • con fines estadísticos • libertad de expresión y de información • número nacional de identificación • obligaciones de secreto • acceso del público a documentos oficiales
processing which does not require identification	tratamiento que no requiere identificación
processor	encargado (del tratamiento)
profiling	elaboración de perfiles
pseudonymization	seudonimización

recipient	destinatario
relevant and reasoned objection	objección pertinente y motivada
representative	representante
restriction of processing	limitación del tratamiento
retention period	periodo de retención
right to compensation	derecho a indemnización
rights of the data subject	derechos del interesado
<ul style="list-style-type: none"> • automated individual decision-making • data portability • information and access • modalities • notification obligation • rectification and erasure • restriction of processing • restrictions • 'right to be forgotten' • right to objection • transparency 	<ul style="list-style-type: none"> • decisiones individuales automatizadas • portabilidad de los datos • información y acceso • modalidades • obligación de notificación • rectificación y supresión • limitación del tratamiento • limitaciones • "derecho al olvido" • derecho de objeción • transparencia
rules of procedure	reglamento interno
security breach (security incident)	violación de la seguridad (incidente de seguridad)
security of personal data	seguridad de los datos personales
security of processing	seguridad del tratamiento
sensitive data	datos sensibles
special categories of personal data	categorías especiales de datos personales
<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 	<ul style="list-style-type: none"> • datos biométricos • datos concernientes a la salud • datos genéticos • opiniones políticas • origen racial o étnico • convicciones religiosas o filosóficas • vida sexual u orientación sexual • afiliación sindical
Supervisory Authority	autoridad de control
Supervisory Authority concerned	autoridad de control interesada
suspension of proceedings	suspensión de los procedimientos
territorial scope	ámbito territorial
third party	terceros
transfer of personal data to third countries and to international organizations	transferencias de datos personales a terceros países u organizaciones internacionales
<ul style="list-style-type: none"> • adequacy decision • appropriate safeguards • binding corporate rules • derogations • disclosures • international protection of personal data 	<ul style="list-style-type: none"> • decisión de adecuación • garantías adecuadas • normas corporativas vinculantes • excepciones • comunicaciones • protección internacional de datos personales

4. Bibliografía

- A. A. Calder
**Reglamento General de Protección de Datos (RGPD) de la UE:
Una guía de bolsillo**
IT Governance Publishing
ISBN13: 9781849288835
(e-libro ISBN13: 9781849288842)
- B. L. Besemer
White Paper – EXIN Privacy and Data Protection Foundation
Descarga gratuita en www.exin.com
- C. Comisión Europea
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) Regulation of the European Parliament and the Council of the European Union. Brussels, Abril 6 2016, disponible en:
<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>

Nota

Las especificaciones de este examen están basadas en la literatura. Literatura C no es literatura primaria, porque la otra literatura proporciona suficiente contenido sobre el RGPD. Los candidatos deben familiarizarse con la literatura C en la medida de las referencias hechas en la otra literatura.

Referencia bibliográfica²

Requisito del examen	Especificación del examen	Literatura	RGPD (GDPR) referencia
1. Fundamentos y regulación de la privacidad y la protección de datos			
	1.1 Definiciones	A: Ch. 1, Ch. 3 B: §1.1.1	rec. 1, 2 & art 96-99
	1.2 Datos personales	A: Ch. 2, Ch. 3 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 Motivos legítimos y limitación de la finalidad	B: §3.1, §3.2, §3.3	art 6.1, art 24
	1.4 Requisitos adicionales para el tratamiento legítimo de los datos personales	B: §2.1, §6.1	art 25, art 27-32, art 5
	1.5 Derechos de los interesados	B: §4.3, §4.4.2	no hay ref.
	1.6 Violación de la seguridad de los datos y procedimientos relacionados	B: §5.1-5.3	art 4(12), art 33, art 34
2. Organizar la protección de datos			
	2.1 La importancia de la protección de datos para la organización	A: Ch. 3, Ch. 4 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 Autoridad Europea de Supervisión	A: Ch. 3 B: §7.1, §7.3	art 36, art 33, art 34
	2.3 Transferencia de datos personales a terceros países	B: §7.4	art 29, art 30, art 45
	2.4 Normas Corporativas vinculantes y Privacidad en los contratos	A: Ch. 3 B: §7.4.3.3, §8.2	art 47, art 24, art 28
3. Práctica de la protección de datos			
	3.1 Protección de los datos desde el diseño y por defecto en relación a la seguridad de la información	B: §5.2, §8.1.1	no hay ref.
	3.2 Evaluación de impacto relativa a la protección de datos (EIPD)	§6.1.3, §8.3, §8.5	no hay ref.
	3.3 Aplicaciones relacionadas con la práctica del uso de datos, marketing y redes sociales	§8.4, §8.6	no hay ref.

² Las referencias están hechas a la literatura A, original en inglés. Por eso los números de página de la versión en castellano pueden ser diferentes. A. Calder EU GDPR, A pocket guide IT Governance Publishing, ISBN 978-1-84928-855-2, (o el e-libro con ISBN 978-1-84928-857-6)

Contacto EXIN

www.exin.com

