Guide de préparation

Édition 201805

Table de matières

1. Résumé

EXIN Privacy & Data Protection Foundation (PDPF.FR)

Portée

La certification EXIN Privacy & Data Protection Foundation (PDPF) valide des connaissances professionnelles relatives à l'organisation de la protection des données personnelles, à la règlementation et législation de l'Union Européenne en matière de protection des données.

Sommaire

La protection des renseignements personnels se trouve au centre de l'attention, chaque fois que des données personnelles sont collectées, enregistrées, utilisées puis finalement effacées ou détruites. Avec le Règlement Général de Protection des Données (RGPD), le Conseil de l'Union Européenne vise le renforcement et l'harmonisation en matière de protection des données de tous les individus au sein de l'Union Européenne (UE). Cette réglementation affecte toutes les organisations qui traitent les données personnelles au sein de l'UE. EXIN Privacy & Data Protection Foundation couvre les principaux thèmes du RGPD.

Contexte

La certification EXIN Privacy and Data Protection Foundation (PDPF) fait partie du programme de qualification de la Privacy and Data Protection.

Groupe cible

Tous les employés devant comprendre le concept de protection des données et les exigences légales européennes telles que définies dans le RGPD. Les fonctions suivantes seront plus particulièrement intéressées : Délégué à la protection des données, Responsable de la protection des renseignements personnels, Juriste / Responsable de la conformité, Responsable de la sécurité, Gestionnaire de la continuité du business.

Exigences de la certification

- Réussite à l'examen d'EXIN Privacy & Data Protection Foundation.

Précisions sur l'examen

Type d'examen :	Questions à choix multiples
Nombre de questions :	40
Note minimale pour réussir :	65%
Accès aux notes / au manuel :	Non
Matériel / supports électroniques autorisés :	Non
Durée de l'examen :	60 minutes

Les règles et règlements de l'EXIN en matière d'examens s'appliquent à cet examen.

Niveau Bloom

La certification d'EXIN Privacy & Data Protection Foundation teste les candidats au niveau 1 de la taxonomie révisée de Bloom :

- Niveau 1 : Connaissance - s'appuie sur le rappel de l'information. Les candidats doivent absorber des informations, se souvenir, reconnaître et se rappeler. Il s'agit du bloc de base de l'apprentissage, avant que les candidats puissent passer aux niveaux supérieurs.
- Niveau 2 : Compréhension – va une étape plus loin que la connaissance. À cette étape, le candidat montre qu'il comprend ce qui est présenté et qu'il peut identifier dans son propre environnement des applications de ce qu'il a appris.

Formation

Heures de contact

Le nombre d'heures de contact recommandé pour cette formation est de 15. Cela comprend les exercices de groupe, la préparation aux examens et de brèves pauses. Ce nombre d'heures n'inclut pas les devoirs, la logistique liée à la session de l'examen ni les pauses déjeuner.

Charge de travail estimée

60 heures, en fonction de connaissances existantes

Formateur

Une liste de centres de formation accrédités est disponible sur notre site : www.exin.com.

2. Conditions de l’examen

Les conditions de l’examen sont détaillées dans les spécifications de l’examen. Le tableau suivant énumère les sujets du module (conditions de l’examen) et les sous-rubriques (spécifications de l'examen).

Condition de l’examen	Spécification de l’examen	Pondération
1. Principes fondamentaux de protection des renseignements personnels et des données		**44.5%**
	1.1 Définitions	7.5%
	1.2 Donnée personnelle	12%
	1.3 Motifs légitimes et limitation de la finalité	5%
	1.4 Autres exigences pour le traitement légitime des données personnelles	5%
	1.5 Droit des personnes concernées	5%
	1.6 Violation de données et procédures associées	10%
2. Organisation de la protection des données		**35.5%**
	2.1 Importance de la protection des données pour l'organisation	13%
	2.2 Autorité de contrôle[1]	7.5%
	2.3 Transfert de données personnelles vers des pays tiers	7.5%
	2.4 Les règles d'entreprise contraignantes et la protection des données dans les contrats	7.5%
3. Pratique de la protection des données		**20%**
	3.1 Protection des données dès la conception et protection des données par défaut	5%
	3.2 Analyse d'impact relative à la protection des données (DPIA)	5%
	3.3 Pratique des applications liées à l'utilisation des données, du marketing et des médias sociaux	10%
	Total	100%

[1] Avant l'introduction du RGPD, l'autorité de protection des données était l'autorité nationale chargée de l'application de la réglementation sur la protection des données. Dans le RGPD, elle est désormais appelée autorité de contrôle.

Spécifications de l'examen

1 Principes fondamentaux de protection des renseignements personnels et des données

1.1 Définitions

Le candidat est capable de …

1.1.1 donner des définitions correctes de la protection des renseignements personnels.

1.1.2 faire le lien entre protection des renseignements personnels, sous la forme de données personnelles spécifiques, jusqu'au concept de protection des données.

1.1.3 décrire le contexte de loi de l'Union et de loi d'un état membre.

1.2 Donnée personnelle

Le candidat est capable de …

1.2.1 donner une définition des données personnelles selon le RGPD.

1.2.2 faire une distinction entre les données personnelles et les catégories spéciales telles que les données personnelles sensibles.

1.2.3 décrire les droits de la personne concernée en matière de données personnelles.

1.2.4 décrire le traitement des données personnelles.

1.2.5 lister les rôles, les responsabilités et les parties prenantes.

1.3 Motifs légitimes et limitation de la finalité

Le candidat est capable de …

1.3.1 énumérer les six motifs légitimes de traitement.

1.3.2 décrire le concept de limitation de la finalité.

1.3.3 décrire la proportionnalité et la subsidiarité.

1.4 Autres exigences pour le traitement légitime des données personnelles

Le candidat est capable de …

1.4.1 décrire les exigences pour le traitement des données.

1.4.2 décrire la finalité du traitement des données personnelles.

1.4.3 expliquer les principes relatifs au traitement des données personnelles.

1.5 Droit des personnes concernées

Le candidat est capable de …

1.5.1 peut décrire les droits concernant la portabilité des données et le droit d'inspection.

1.5.2 connaît le droit à l'oubli.

1.6 Violation de données et procédures associées

Le candidat est capable de …

1.6.1 décrire le concept de violation de données.

1.6.2 expliquer les procédures à déclencher en cas de violation de données.

1.6.3 donner des exemples de catégories de violations de données.

1.6.4 décrire la différence entre une violation de sécurité (incident) et une violation de données.

1.6.5 mentionner les parties prenantes pertinentes qui devraient être informées.

2 Organisation de la protection des données

2.1 Importance de la protection des données pour l'organisation

Le candidat est capable de …

2.1.1 énumérer les différents types d'activités administratives (RGPD art 28 & 30).

2.1.2 indiquez quelles activités sont requises pour se conformer au RGPD.

2.1.3 donner une définition de la protection des données dès la conception et par défaut.

2.1.4 donner des exemples de violations de données.

2.1.5 décrire l'obligation de notification de violation de données telle que définie dans le RGPD.

2.1.6 décrire l'application des règles en imposant des pénalités, y compris des amendes administratives.

2.2 Autorité de contrôle

Le candidat est capable de …

2.2.1 décrire les responsabilités générales d'une autorité de contrôle.

2.2.2 décrire le rôle et la responsabilité d'une autorité de contrôle en matière de violation de données.

2.2.3 décrire comment une autorité de contrôle contribue à l'application du RGPD.

2.3 Transfert de données personnelles vers des pays tiers

Le candidat est capable de …

2.3.1 décrire les règlements qui s'appliquent à transfert de données à l'intérieur de l'EEE.

2.3.2 décrire les règlements qui s'appliquent à transfert de données à l'extérieur de l'EEE.

2.3.3 décrire les règlements qui s'appliquent à transfert de données entre l'EEE et les États-Unis.

2.4 Les règles d'entreprise contraignantes et la protection des données dans les contrats

Le candidat est capable de …

2.4.1 décrire le concept de règles d'entreprise contraignantes.

2.4.2 décrire comment la protection des données est formalisée dans les contrats formels entre le responsable du traitement et le sous-traitant.

2.4.3 décrire les clauses d'un tel contrat formel.

3 Pratique de la protection des données

3.1 Protection des données dès la conception et protection des données par défaut

Le candidat est capable de …

3.1.1 décrire les avantages de l'application des principes de la protection des données dès la conception et par défaut.

3.1.2 décrire les sept principes de la protection des données dès la conception.

3.2 Analyse d'impact relative à la protection des données (DPIA)

Le candidat est capable de …

3.2.1 décrire ce que comprend un DPIA et quand réaliser un DPIA.

3.2.2 mentionner les huit objectifs d'un DPIA.

3.2.3 énumérer les chapitres d'un rapport de DPIA.

3.3 Pratique des applications liées à l'utilisation des données, du marketing et des médias sociaux

Le candidat est capable de …

3.3.1 décrire l'objectif de la gestion du cycle de vie des données (DLC).

3.3.2 expliquer la rétention et la minimisation des données.

3.3.3 décrire ce qu'est un cookie et quel est son but.

3.3.4 décrire, du point de vue de la protection des données, comment l'utilisation répandue de l'internet a affecté le domaine du marketing.

3.3.5 donner des exemples d'utilisation des informations sur les médias sociaux pour des activités de marketing.

3. Liste des concepts de base

Ce chapitre dresse une liste des termes et abréviations que les candidats sont censés maîtriser.

Veuillez noter que la connaissance de ces termes seule ne suffit pas pour l'examen ; le candidat doit comprendre le concept et être en mesure de fournir des exemples.

Anglais	Français
adequate	adéquat
appropriate technical and organizational measures	mesures techniques et organisationnelles appropriées
authenticity	authenticité
availability	disponibilité
binding	contraignant
binding corporate rules	règles d'entreprise contraignantes
biometric data	données biométriques
certification	certification
certification bodies	organismes de certification
child's consent	consentement des enfants
codes of conduct	code de conduite
collection of personal data (verb.)	collecte des données personnelles
commission reports	rapports de la commission
complaint	réclamation
compliance	conformité
conditions for consent	conditions du consentement
Consent	consentement
consistency	cohérence
consistency mechanism	mécanisme de cohérence
constitution	constitution
contract	contrat
controller	responsable du traitement
cross-border processing	traitement trans-frontalier
data breach	violation de données
data concerning health	données relatives à la santé
data controller	responsable du traitement des données
data protection	protection des données
data protection authority (DPA)	autorité de protection des données / Autorité de Contrôle (DPA)
data protection by default	protection des données par défaut
data protection by design	protection des données dès la conception
data protection impact assessment (DPIA)	analyse d'impact relative à la protection des données (DPIA)

data protection officer (DPO) • designation • position • tasks	délégué à la protection des données (DPO) • Nomination • Poste • Tâches
data subject	personne concernée par les données
data transfer	transfert de données
delegated acts and implementing acts • committee procedure	actes délégués et actes d'exécution • procédure du comité
derogation	dérogation
enforcement • administrative fines • administrative penalties • criminal penalties • dissuasive penalties • effective penalties • proportionate penalties	obligation • Amendes administratives • Pénalités administratives • Pénalités criminelles • Pénalités dissuasives • Pénalités efficaces • Pénalités proportionnées
enterprise	entreprise
European Economic Area (EEA)	Zone Économique Européenne
EU types of legal act • decision • directive • opinion • recommendation • regulation	types de textes Européens • décision • directive • avis • recommandation • réglementation
European Data Protection Board (EDPB) • chair • confidentiality • independence • procedure • reports • secretariat • tasks	Comité européen de la protection des données (EDPB) • présidence • confidentialité • indépendance • procédure • rapports • secrétariat • tâches
European Data Protection Supervisor (EDPS)	Contrôleur Européen pour la Protection des Données (EDPS)
European Union legal acts on data protection	textes légaux de l'Union Européenne sur la protection des données
exchange of information	échanges d'information
exemption	exemption / Exclusion
explicit consent	consentement explicite
genetic data	données génétiques
filing system	système de stockage
General Data Protection Regulation (GDPR)	Réglement Général de Protection des Données (RGPD)
governing body	organe de gouvernance
group of undertakings	motif des entreprises
independent supervisory authorities • activity reports • competence • establishment • powers • tasks	autorités de surveillance indépendantes • rapports d'activité • compétence • établissement • pouvoirs • tâches

information society service	service de la société de l'information
international organization	organisation internationale
joint controllers	responsables conjoints du traitement
judicial remedy	recours judiciaire
lawfulness of processing	légalité du traitement
legal basis	base légale
legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) and legitimate basis (GDPR article 40)	fondement légitime (RGPD article 17/1c, article 18/1d, article 21/1) et base légitime (RGPD article 40)
legitimate interest	intérêt légitime
Liability	responsabilité (légale)
main establishment	établissement principal
material scope	portée matérielle
National Identification Number	Numéro d'Identification National
non-repudiation	non répudiation
opinion of the board	Avis du Comité
personal data	donnée personnelle
personal data breach	violation de données personnelles
personal data relating to criminal convictions and offences	données personnelles relatives à des condamnations pénales et des infractions
principles relating to processing of personal data • accountability • accuracy • confidentiality • data minimization • fairness • integrity • lawfulness • purpose limitation • storage limitation • transparency	principes relatifs au traitement des données personnelles • responsabilité • justesse • confidentialité • limitation des données • equité • intégrité • légalité • limitation de finalité • limitation de stockage • transparence
prior consultation	consultation préalable
privacy	protection des renseignements personnels
processing	traitement
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	situations de traitement • règles de protection des données des églises et des associations religieuses • emploi • à des fins d'archivage dans l'intérêt public • à des fins de recherche scientifique ou historique • à des fins statistiques • liberté d'expression et d'information • numéro d'identification national • obligations de secret • l'accès du public aux documents officiels
processing which does not require identification	traitement ne nécessitant pas d'identification

processor	sous-traitant
profiling	profilage
pseudonymization	pseudonymisation
recipient	receveur / destinataire
relevant and reasoned objection	objection pertinente et raisonnée
representative	représentant
restriction of processing	restriction de traitement
retention period	période de rétention
right to compensation	droit à compensation
rights of the data subject • 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	droits de la personne concernée • prise de décision individuelle automatisée • portabilité des données • information et accès • modalités • obligation de notification • rectification et effacement • restriction de traitement • restrictions • droit à l'oubli • droit de contestation • transparence
rules of procedure	règles de procédure
security breach (security incident)	violation de sécurité (incident de sécurité)
security of personal data	sécurité des données personnelles
security of processing	sécurité du traitement
sensitive data	données sensibles
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 • trade union membership	catégories spéciales de données personnelles • données biométriques • données relatives à la santé / données médicales • données génétiques • opinions politiques • origine raciale ou etnique • croyances religieuses ou philosophiques • vie sexuelles ou orientation sexuelle • appartenance à un syndicat
supervisory authority	autorité de contrôle
supervisory authority concerned	autorité de contrôle concernée
suspension of proceedings	suspension des traitements
territorial scope	périmètre territorial
third party	tiers
transfer of personal data to third countries and to international organizations • adequacy decision • appropriate safeguards • binding corporate rules • derogations • disclosures • international protection of personal data	transfert de données personnelles vers des pays étrangers et vers des organisations internationales • décision d'adéquation • garde-fous appropriés • règles d'entreprise contraignantes • dérogations • communications • protection internationale des données personnelles

4. Bibliographie

Bibliographie

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

B. L. Besemer
White Paper – EXIN Privacy and Data Protection Foundation
Téléchargement gratuit sur www.exin.com

C. European Commission
General Data Protection Regulation (GDPR) Regulation (EU) 2016/679) Regulation of the European Parliament and the Council of the European Union. Bruxelles, le 6 avril 3016, disponible sur:
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

Commentaires

Les conditions de l'examen sont basées sur la bibliographie. Les ouvrages C ne font pas partie des ouvrages principaux pour l'examen car les autres ouvrages fournissent un contenu suffisant sur le RGPD. Les candidats doivent se familiariser avec les ouvrages C dans la mesure où il y est fait référence dans les autres ouvrages.

Matrice de littérature

Condition de l'examen	Spécification de l'examen	Littérature	Référence RGPD
1. Principes fondamentaux de protection des renseignements personnels et des données			
	1.1 Définitions	A: Ch. 1, Ch. 3 B: §1.1.1	rec. 1, 2 & art 96-99
	1.2 Donnée personnelle	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 Motifs légitimes et limitation de la finalité	B: §3.1, §3.2, §3.3	art 6.1, art 24
	1.4 Autres exigences pour le traitement légitime des données personnelles	B: §2.1, §6.1	art 25, art 27-32, art 5
	1.5 Droit des personnes concernées	B: §4.3, §4.4.2	pas de référence
	1.6 Violation de données et procédures associées	B: §5.1-5.3	art 4(12), art 33, art 34
2. Organisation de la protection des données			
	2.1 Importance de la protection des données pour l'organisation	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 Autorité de contrôle	A: Ch. 3 B: §7.1, §7.3	art 36, art 33, art 34
	2.3 Transfert de données personnelles vers des pays tiers	B : §7.4	art 29, art 30, art 45
	2.4 Les règles d'entreprise contraignantes et la protection des données dans les contrats	A: Ch. 3 B: §7.4.3.3, §8.2	art 47, art 24, art 28
3. Pratique de la protection des données			
	3.1 Protection des données dès la conception et protection des données par défaut	B: §5.2, §8.1.1	pas de référence
	3.2 Analyse d'impact relative à la protection des données (DPIA)	§6.1.3, §8.3, §8.5	pas de référence
	3.3 Pratique des applications liées à l'utilisation des données, du marketing et des médias sociaux	§8.4, §8.6	pas de référence

Contacter EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER