準備ガイド

2018 年 5 月版

目次

1. 概要

EXIN Privacy & Data Protection Foundation (PDPF.JP)

要約

EXIN Privacy & Data Protection Foundation (PDPF) は、個人データの保護、EU の規則及び、データ保護に関する規則の整理に関する専門家の知識を認証する資格です。

サマリ

個人情報が収集、保存、使用され、最終的に削除または破棄される場合は、プライバシーに関する懸念が生じます。欧州連合理事会は、EU の一般データ保護規制 (GDPR) によって、欧州連合 (EU) 内のすべての個人に対するデータ保護を強化し統一しようとしています。この規則は EU の個人データを取扱うすべての組織に影響します。EXIN Privacy & Data Protection Foundation (PDPF)は、GDPR に関連する主要な項目を網羅します。

背景

EXIN Privacy & Data Protection Foundation (PDPF)資格は、プライバシー及びデータ保護に関する、EXIN の資格プログラムの一部です。

対象グループ

GDPR に定義されているデータ保護と欧州の法的要件を理解する必要があるすべての従業員、具体的には、データ保護責任者、プライバシー責任者、法務責任者／コンプライアンス責任者、セキュリティ責任者、ビジネス継続マネージャの役割を担う方にとって関心のあるものであると考えます。

認定のための要件

- EXIN Privacy & Data Protection Foundation-試験の合格。

試験の詳細内容

試験の形式:	多肢選択形式
問題数:	40
合格点:	65%
参考書やノートの持ち込み:	不可
電子機器の持ち込み:	不可
試験時間:	60 分

EXIN の試験規則はこの試験に適用されます。

ブルーム分類法（Bloom’s Taxonomy）によるレベル

EXIN Privacy & Data Protection Foundation ファンデーション資格では、改訂版ブルームの分類法に基づき、ブルームレベル１およびレベル２の受験者をテストします。

- ブルームレベル１：「記憶」　情報を思い出すことに依存します。受験者は、吸収し、記憶し、認識して思い出すことを必要とします。これは、受験者がより高いレベルに進む前の学習の土台となります。
- ブルームレベル２：「理解」　「記憶」よりも上のステップです。「理解」することにより、受験者は提示された内容を理解していることを示し、学習教材が受験者の環境でどのように適応できるかを評価することができます。

教育・訓練

授業時間

最小限の教育・訓練コースの最小受講時間は、15 時間です。グループ課題、試験準備や休憩時間が含まれます。宿題、試験準備、昼休みはこの時間に含まれません。

学習時間の目安

60 時間、個人が習得している知識によります。

認定教育機関

認定教育事業者のリストを www.exin.com で参照できます。

2. 試験要件と試験仕様

試験要件は、試験仕様に明記されています。以下の表にモジュールトピック（試験要件）とサブトピック（試験仕様）の一覧を示します。

試験要件	試験仕様	配分
1. プライバシー及びデータ保護の基本と規則		**44.5%**
	1.1 定義	7.5%
	1.2 個人データ	12%
	1.3 正当な事由と目的の制限	5%
	1.4 個人データの処理についての追加の要求事項	5%
	1.5 データ主体の権利	5%
	1.6 データ侵害及び関連する手続き	10%
2. データ保護の構成		**35.5%**
	2.1 組織におけるデータ保護の重要性	13%
	2.2 監督機関[1]	7.5%
	2.3 第三国への個人データの移転	7.5%
	2.4 拘束的企業準則(BCR)及び契約におけるデータ保護	7.5%
3. データ保護の実践		**20%**
	3.1 データ保護バイ・デザイン及びデータ保護バイ・デフォルト	5%
	3.2 データ保護影響評価（DPIA）	5%
	3.3 データ、マーケティング及びソーシャルメディアの利用に関連するアプリケーションの実践	10%
	合計	100%

[1] GDPR が導入される前は、「*データ保護機関*」がデータ保護に関する規制の施行を担う国家機関でした。GDPR では、現在「*監督機関*」と呼びます。

試験仕様

1 プライバシー及びデータ保護の基本と規則

1.1 定義

受験者に要求される能力

1.1.1 有効なプライバシーに関する定義の説明ができる

1.1.2 特定個人データのプライバシーとデータ保護の概念との関連付けができる

1.1.3 EU 連合及び加盟国の法律の背景について記述ができる

1.2 個人データ

受験者に要求される能力

1.2.1 GDPR の対象となる個人データの定義の説明ができる

1.2.2 個人データと機微な個人データ（センシティブデータ）などの「特別な種類の個人データ」との区別ができる

1.2.3 個人データにおけるデータ主体の権利について記述ができる

1.2.4 個人データの取扱いについて記述ができる

1.2.5 役割、責任、ステークホルダーについて列挙できる

1.3 正当な事由と目的の制限

受験者に要求される能力

1.3.1 ６種類の処理の正当な事由について列挙できる

1.3.2 目的の制限についての概要について記述ができる

1.3.3 比例原則と補完性の原理について記述ができる

1.4 個人データの処理についての追加の要求事項

受験者に要求される能力

1.4.1 データの処理についての要求事項について記述ができる

1.4.2 個人データの処理の目的について記述ができる

1.4.3 個人データの処理に関する原理について説明ができる

1.5 データ主体の権利

受験者に要求される能力

1.5.1 データポータビリティ（データの携行）の権利及びアクセス権（検査できる権利）について記述ができる

1.5.2 削除権（忘れられる権利）について認識している

1.6 データ侵害及び関連する手続き

受験者に要求される能力

1.6.1 データ侵害の概念について記述ができる

1.6.2 データ侵害が発生した場合の対応方法についての手順が説明できる

1.6.3 データ侵害の事例について説明ができる

1.6.4 セキュリティ侵害（インシデント）とデータ侵害の違いについて記述ができる

1.6.5 通知すべく関連するステークホルダーについて言及できる

2 データ保護の構成

2.1 組織におけるデータ保護の重要性

受験者に要求される能力

2.1.1 各種管理について列挙できる（GDPR 第 28 条及び第 30 条）

2.1.2 GDPR を順守するために必要な活動を示すことができる

2.1.3 データ保護バイ・デザイン及びデータ保護バイ・デフォルトの定義の説明ができる

2.1.4 データ侵害の事例について説明ができる

2.1.5 GDPR に規定されたデータ侵害通知義務について記述ができる

2.1.6 過料（制裁金）などの罰の発行による規則の執行について記述ができる

2.2 監督機関

受験者に要求される能力

2.2.1 監督機関の一般的な責任について記述ができる

2.2.2 データ侵害に関する監督機関の役割と責任について記述ができる

2.2.3 監督機関が GDPR の適用にどのように貢献しているかを記述できる

2.3 第三国への個人データの移転

受験者は次の場合に適用される規則について記述ができる

2.3.1 欧州経済領域（EEA）内への個人データの移転

2.3.2 欧州経済領域（EEA）外への個人データの移転

2.3.3 欧州経済領域（EEA）と米国間の個人データの移転

2.4 拘束的企業準則(BCR)及び契約におけるデータ保護

受験者に要求される能力

2.4.1 拘束的企業準則(BCR)の概念について記述ができる

2.4.2 管理者（コントローラ）と取扱者間の書面による契約書でどのようにデータ保護が形式化されるかについて記述ができる

2.4.3 データ保護を形式化する書面による契約の条項について記述ができる

3 データ保護の実践

3.1 データ保護バイ・デザイン及びデータ保護バイ・デフォルト

受験者に要求される能力

3.1.1 データ保護バイ・デザイン及びデータ保護バイ・デフォルトの原則を適用する利点について記述ができる

3.1.2 データ保護バイ・デザインの 7 つの原則について記述ができる

3.2 データ保護影響評価（DPIA）

受験者に要求される能力

3.2.1 DPIA の構成と適用時期についての概要が説明できる

3.2.2 DPIA の 8 つの目的について言及できる

3.2.3 DPIA 報告書（データ保護影響評価報告書）の項目について列挙できる

3.3 データ、マーケティング及びソーシャルメディアの利用に関連するアプリケーションの実践

受験者に要求される能力

3.3.1 データライフサイクル(DLC)管理の目的について記述ができる

3.3.2 データの保存及び最小化について説明ができる

3.3.3 クッキーの内容とその目的について記述ができる

3.3.4 データ保護の観点から、インターネットの普及がマーケティングの分野にどのように影響しているかを記述ができる

3.3.5 マーケティング活動において、ソーシャルメディア情報を利用する事例について説明ができる

3. 基本概念の一覧

受験者が知っておくべき用語を記載します。各用語の概念を理解しておいてください。

これらの用語の知識だけでは試験に十分ではないことに注意してください。受験者は、その概念を理解し、例を提示できる必要があります。

English	Japanese
Adequate	十分な
appropriate technical and organizational measures	適切な技術及び組織的な対策
Authenticity	真正性
Availability	可用性
Binding	拘束
binding corporate rules	拘束的企業準則(BCR)
biometric data	生体認証データ
certification	認証
certification bodies	審査機関
child's consent	子供の同意
codes of conduct	行動規範
collection of personal data (verb.)	個人データを収集する（動詞）
commission reports	欧州委員会報告書
complaint	苦情
compliance	コンプライアンス
conditions for consent	同意の条件
consent	同意
consistency	一貫性
consistency mechanism	統一する仕組み（一貫性メカニズム）
constitution	憲法
contract	契約
controller	管理者（コントローラ）
cross-border processing	国境を越えた取扱い（越境的取扱い）
data breach	データの侵害
data concerning health	健康に関するデータ
data controller	データ管理者（コントローラ）
data protection	データ保護
data protection authority	データ保護機関(DPA)
data protection by default	データ保護バイデフォルト
data protection by design	データ保護バイデザイン
data protection impact assessment	データ保護影響評価(DPIA)
data protection officer (DPO) • designation • position • tasks	*データ保護*責任者(DPO) • 指名 • 地位 • 役割
data subject	データ主体

data transfer
delegated acts and implementing acts
- committee procedure

derogation
enforcement
- administrative fines
- administrative penalties
- criminal penalties
- dissuasive penalties
- effective penalties
- proportionate penalties

enterprise

European Economic Area (EEA)
EU types of legal act
- decision
- directive
- opinion
- recommendation
- regulation

European Data Protection Board
- chair
- confidentiality
- independence
- procedure
- reports
- secretariat
- tasks

European Data Protection Supervisor (EDPS)
European Union legal acts on data protection
exchange of information
exemption
explicit consent
genetic data
filing system
General Data Protection Regulation (GDPR)
governing body
group of undertakings
independent supervisory authorities
- activity reports
- competence
- establishment
- powers
- tasks

information society service
international organization
joint controllers

データ移転
委任法及び施行法
- 委員会手続

免除（除外）
執行
- 過料（制裁金）
- 行政罰
- 刑事罰
- 抑止的な罰
- 効果的な罰
- 均衡がとれた罰

事業者または企業
欧州経済領域 (European Economic Area (EEA))
EU の法令（法律・規制類）の体系
- 決定
- 指令
- 意見
- 勧告
- 規則

欧州データ保護評議会
- 議長
- 機密性
- 独立性
- 手続き
- 報告書
- 事務局
- 役割

欧州データ保護監督官 (EDPS：European Data Protection Supervisor)
データ保護に関する EU 法令

情報交換
除外（免除）
明確な同意
遺伝子データ
ファイリングシステム
一般データ保護規則（GDPR）
運営組織
事業体グループ
独立監督機関
- 活動報告書
- 管轄
- 創設・設置
- 権限
- 役割

情報社会サービス
国際組織
共同管理者

judicial remedy	司法的救済
lawfulness of processing	適法な取扱い
legal basis	法的根拠
legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) and legitimate basis (GDPR article 40)	正当な事由（GDPR 17条 1c、 18条 1d、21条1）及び法的根拠（GDPR 40条）
legitimate interest	正当な利益
liability	法的責任
main establishment	主たる事業所
material scope	実体的範囲
National Identification Number	国民識別番号
non-repudiation	否認防止
opinion of the board	欧州データ保護会議の意見
personal data	個人データ
personal data breach	個人データ侵害
personal data relating to criminal convictions and offences	有罪判決及び犯罪に関する個人データ
principles relating to processing of personal data • accountability • accuracy • confidentiality • data minimization • fairness • integrity • lawfulness • purpose limitation • storage limitation • transparency	個人データの取扱いに関する原則 • 説明責任（アカウンタビリティ） • 正確性 • 機密性 • データの最小化 • 公正性 • 完全性 • 適法性 • 目的の制限 • 保存の制限 • 透明性
prior consultation	事前協議
privacy	プライバシー
processing	取扱（処理）
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	取扱い状況 • 教会及び宗教組織のデータ保護規則 • 雇用 • 公共の利益における保管目的 • 科学的若しくは歴史的研究の目的 • 統計目的 • 表現及び情報の自由 • 国民識別番号 • 守秘義務 • 公式文書へのパブリック・アクセス
processing which does not require identification	識別を要求しない取扱い

processor
profiling
pseudonymization
recipient
relevant and reasoned objection
representative
restriction of processing
retention period
right to 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

rules of procedure

security breach (security incident)
security of personal data
security of processing
sensitive data
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

supervisory authority
supervisory authority concerned
suspension of proceedings
territorial scope
third party

取扱者
プロファイリング
仮名化
取得者
適切及び合理的な不服
代表者
取扱いの制限
保存期間
賠償請求権
データ主体の権利
- 自動化された個人意思決定
- データ・ポータビリティ
- 情報及びアクセス（情報及び認証手続）
- 手続
- 通知義務
- 訂正若しくは消去
- 取扱いの制限
- 制限
- ‘忘れられる権利’
- 不服申立ての権利
- 透明性

手続規定
セキュリティ侵害（セキュリティ　インシデント）
個人データの保護
取扱いの保護
機微データ
特別な種類の個人データ
- 生体データ
- 健康に関するデータ
- 遺伝データ
- 政治的思想
- 人種的または民族的素性
- 政治的または宗教的信条
- 性生活または性的指向
- 労働組合員資格

監督機関
関係監督機関
訴訟の一時停止
地理的範囲
第三者

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

第三国または国際機関への個人データの移転

- 十分性の決定（十分性認定）
- 十分な保護措置
- 拘束的企業準則
- 逸脱
- 開示
- 国際的な個人データ保護

4. 試験の参考文献

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

B. L. Besemer
White Paper – EXIN Privacy and Data Protection Foundation
Free download on 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. Brussels, 6 April 2016, available at:
http://eur-lex.europa.eu
PDF:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
HTML:
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=EN

コメント

試験要件は試験の参考文献に基づきます。GDPRに関する十分な内容が他の文献に含まれているため、文献Cは主要参考文献ではありません。受験者は、他の文献でなされた参考文献の範囲内で文献Cについて精通しておく必要があります。

参考文献と試験仕様

試験要件	試験仕様	参考文献	GDPR 参照箇所
1. プライバシー及びデータ保護の基本と規則			
	1.1 定義	A: Ch. 1, Ch. 3 B: §1.1.1	rec. 1, 2 & art 96-99
	1.2 個人データ	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 正当な事由と目的の制限	B: §3.1, §3.2, §3.3	art 6.1, art 24
	1.4 個人データの処理についての追加の要求事項	B: §2.1, §6.1	art 25, art 27-32, art 5
	1.5 データ主体の権利	B: §4.3, §4.4.2	no ref.
	1.6 データ侵害及び関連する手続き	B: §5.1-5.3	art 4(12), art 33, art 34
2. データ保護の構成			
	2.1 組織におけるデータ保護の重要性	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 監督機関	A: Ch. 3 B: §7.1, §7.3	art 36, art 33, art 34
	2.3 第三国への個人データの移転	B: §7.4	art 29, art 30, art 45
	2.4 拘束的企業準則(BCR)及び契約におけるデータ保護	A: Ch. 3 B: §7.4.3.3, §8.2	art 47, art 24, art 28
3. データ保護の実践			
	3.1 データ保護バイ・デザイン及びデータ保護バイ・デフォルト	B: §5.2, §8.1.1	no ref.
	3.2 データ保護影響評価 (DPIA)	§6.1.3, §8.3, §8.5	no ref.
	3.3 データ、マーケティング及びソーシャルメディアの利用に関連するアプリケーションの実践	§8.4, §8.6	no ref.

EXIN の連絡先

www.exin.com

YOUR ICT COMPETENCE PARTNER