Europrivacy™® Academy
GDPR Audit and Certification Courses

ユーロプライバシー アカデミー

ユーロプライバシー実装コース

www.academy.europrivacy.com

ユーロプライバシーアカデミー

ユーロプライバシー
実装コース

v.3（2024 年）

ユーロプライバシーについて

ユーロプライバシーは、データ取扱いの欧州一般データ保護規則（GDPR）及び補完的各国規制の遵守状況を評価及び認証するために開発された認証制度です。欧州データ保護会議（EDPB）から、EU全管轄で適用可能な欧州データ保護シールとして承認を受けています。

ユーロプライバシーは、ISO 原則に準拠した信頼性が高く体系的な遵守状況評価を可能にします。補完的規制及び先端技術への拡張が容易です。内部監査の実施、残存する不遵守の特定、及び、認証のためのデータ取扱いの準備を行うための効率的な手法を提供します。データ保護オフィサー（DPO）、内部監査人、コンサルタント及び認証機関が利用できます。

ユーロプライバシーは、データ保護分野におけるユーロプライバシー国際専門家委員会によって管理及び監督され、EDPB の公表物を含む個人データ保護に関する法学の進化に応じて更新されています。ユーロプライバシーは、ルクセンブルクにある欧州認証・プライバシーセンター（ECCP）によって管理運営され、認定認証機関、法律事務所及びコンサルティング会社によって、その顧客のデータ保護規制遵守支援のために適用されます。

ユーロプライバシーアカデミーについて

ユーロプライバシーアカデミーは、ユーロプライバシーの専門家としての公式資格取得に関心のある方々向けにトレーニングコースを提供しています。ユーロプライバシーアカデミーは、ユーロプライバシー認証制度の手法及び規則に焦点を当てています。受講生は、既にデータ保護規制に精通していることが前提です。ユーロプライバシーアカデミーのコースは、多様な関心を持つ専門家向けにカスタマイズされた学習体験を提供します。

本ハンドブックについて

ユーロプライバシーアカデミー – ユーロプライバシー実装コースハンドブックは、ユーロプライバシーアカデミーにおけるユーロプライバシー実装コースの受講生向けに提供される補足文書です。本ハンドブックは、認証手続、実装者の役割及びユーロプライバシー基準の補足的な支援及び要約を提供することを目的としています。専門知識の証明書を取得するには試験に合格する必要があるため、ハンドブックには模擬試験が用意されており、受講生は準備しなければならない最終試験の形式及び問題に慣れることができます。

序文

ユーロプライバシー認証制度は、データ取扱活動が一般データ保護規則（GDPR）その他の補完的な国家固有若しくは分野固有、又は、その両方の義務を遵守しているか否かを評価し、正式に認証するための明確かつ効率的な手法を規定しています。これは、プロセス及びサービスからデータ保護マネジメントシステムに至るまで、幅広いデータ取扱活動に適用されます。

入門コース修了後、あなたは既に GDPR 認証及びユーロプライバシー認証制度の一般的枠組みに精通しています。実装コース及び本ハンドブックでは、実装者の役割を含む、認証手続の仕組みについての理解をさらに深めます。

第 1 章では、ユーロプライバシー認証手続における実装者の役割を説明し、認証の維持及び更新の手続について詳述します。また、異議申立て及び苦情手続についても詳述します。**第 2 章**では、認証書及び遵守マークの使用を含む情報管理に関連する規則に焦点を当てます。**第 3 章**では、評価対象の適用及び特定を含む、ユーロプライバシー基準、確認項目及び管理項目一覧について詳述します。本ハンドブックは、25 問の模擬試験を通じて最終試験に向けた候補者が準備をするためのセクションで締めくくられます。

いかなる文書への言及も、その最新版への参照と理解されます。最新版の文書が公開された場合、当該文書は、その公開日又は移行期間の終了時において、同一文書の全ての旧バージョンに取って代わります。認証及び監査手続では、当該手続開始時点において利用可能な最新版のユーロプライバシー認証制度及び関連文書を使用しなければなりません。認証及び監査手続中に文書の新バージョンが公開された場合、当該認証手順はこれを考慮に入れ、可能な限り新バージョンを遵守するのが望ましいです。ただし、進行中の手続は、開始時点の公式バージョンに基づき完了させることが可能です。

本認証制度の要件の適用若しくは解釈、又は、その両方に関する疑義が生じた場合、参照すべき文書は本認証制度の最新版です。

本認証制度固有の規範文書及び情報提供文書は、国際専門家委員会による支援の下、本制度オーナーの管理下に置かれます。

ユーロプライバシーの専門家は、ユーロプライバシー・コミュニティウェブサイトを通じ、利用文書の最新版を入手する責任を負います。ユーロプライバシーアカデミー経由で提供される文書は、厳に教育・訓練をその目的とし、認証活動実施のための公式資料を構成しません。

目次

ユーロプライバシー認証手続

実装者の役割

ユーロプライバシーのエコシステムにおいて、認定実装者は、コンサルティング会社及び支援組織に所属し、適用可能なデータ保護規制の継続的遵守を確保します。コンサルティング会社は、申請者がそのデータ取扱活動の認証を準備するにとどまらず、認証手続及び維持段階を通じて継続的に支援を行います。

コンサルティング会社の主な目的は、申請者の法的・財務的リスクを低減することです。実装者は、申請者が対処しなければならない潜在的なギャップ及び残存する不遵守を特定するため、ユーロプライバシー基準を用います。

実装者は、データ取扱いの遵守状況を確認し、場合によっては認証に関心を有するデータ保護オフィサー（DPO）が兼ねることも可能です。

先ほど解説したとおり、実装者の役割は、以下の二面性を持ちます。

- 一方で、体系的な遵守状況評価を適用することで、法的・財務的リスクを低減すること
- 他方で、認証対象となるデータ取扱いの準備及び文書化を支援すること

コンサルティング会社は、ユーロプライバシー・ウェルカムパックを活用し、申請者に対して包括的な支援を提供できます。

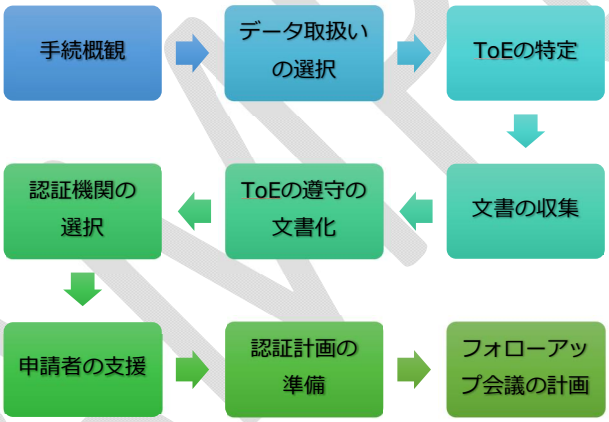

図 1 実装者の歩み

ユーロプライバシー準備手続

	段階	主任	目的	リソース
1	初回見積提案	パートナー	申請者のためのユーロプライバシー初回見積提案の準備	ユーロプライバシー・ウェルカムパックのプレゼンテーション
2	見積提案書への署名	申請者	見積提案書の確認及び署名	NA
3	ウェルカムパックの有効化	パートナー	申請者の DPO のためのウェルカムパックの有効化	ECCP の支援によるウェルカムパックの有効化
4	データ取扱いの選択	パートナー	申請者とともに実施する準備対象となる優先度の高いデータ取扱いの選択	NA
5	評価対象の特定	パートナー	評価対象の特定	A – 申請&ToE チェックリスト
6	文書の用意	パートナー	インベントリ及び NOCAR を含む、必要書類の準備	申請者向けガイドライン D – 文書チェックリスト テンプレート
7	遵守状況の確認	パートナー	評価対象のユーロプライバシー基準、確認項目及び管理項目への遵守状況の評価	G, C, T 基準、確認項目及び管理項目 基準使用に関するガイドライン

8	ギャップの報告	パートナー	特定された不遵守の一覧化及び申請者への共有	不遵守一覧 ユーロプライバシー評価報告書テンプレート
9	不遵守の是正	申請者	特定された不遵守の対処及び解決	不遵守一覧
10	遵守状況の確認	パートナー	不遵守が十分に対処されたことの確認及び検証	G、C、T 基準、確認項目及び管理項目
11	申請の準備	パートナー	申請書の作成及び認証機関への提出	ユーロプライバシー申請書テンプレート A – 申請&ToE チェックリスト
12	認証の申請	申請者	選択された 2 件のデータ取扱いの認証のための認証機関の選択及び申請	ユーロプライバシーオンライン申請フォーム
13	認証の支援	パートナー	認証手続中の申請者の支援	NA
14	認証計画	パートナー	申請者の残りのデータ取扱活動に対する認証計画の策定	認証計画テンプレート
15	補足見積提案	パートナー	残りのデータ取扱いのための補足見積提案の作成	NA
16	最終会議&次の段階	パートナー	結果の提示、フィードバックの収集及び補足見積提案の提示	NA
17	新たな見積提案書への署名	申請者	新たな見積提案書の確認及び署名	NA

維持、更新及び異議申立て

認証の維持

GDPR の第 42 条及び第 43 条に基づき、監視期間中の認証維持のため、定期的な監視措置が義務付けられています。各認証の監視期間は文書化されなければなりません。原則として、ユーロプライバシー認証は、最新の認証日から始まり、認証の有効期限日で終了する **3 年間の更新可能な期間**で付与されるのが望ましいです。

この期間中、申請者は、評価対象が本認証制度の要件及び基準を遵守していることを確保し、認証機関に対し、遵守に関する変更及び懸念を通知しなければなりません。認証機関は、申請者が本認証制度の要件を継続的に遵守しているという証明に基づき、認証を維持します。監視及びサーベイランス活動は、申請者により全面的に支援されなければなりません。

初回認証の周期は、認証決定日に開始し、認証の有効期限日に終了します。認証及び再認証に成功した場合、以下の監査が実施されなければなりません。

- 認証日から 12 か月以内の初回のサーベイランス監査
- 認証日から 24 か月以内の 2 回目のサーベイランス監査
- 該当する場合、認証日から 36 か月以内の再認証監査

認証期間の満了前に再認証が完了した場合、36 か月の認証周期が新たに開始されます。再認証の決定が、前回の認証書の有効期限日前の 3 か月間に採択された場合、新しい認証書の開始日は、前回の認証書の有効期限の翌日に設定することができる。

監視活動は、申請者の評価対象が本認証制度の要件を継続的に遵守しているか否かを判断するために実施されます。監査の頻度は、認証を受けた申請者の要件遵守能力に応じて増える場合があります。

法改正、各国若しくは国際的な裁判所の決定、EDPB の決定、又は、欧州委員会の決定といった適用可能なデータ保護規制の変更は、認証機関によって監視及び対応されます。かかる変更が付与された認証に影響を及ぼす場合、認証機関は、以下の事項を行います。

- 認証の有効性への影響度の評価
- 行動計画の策定
- 関連するデータ保護機関に連絡し、提案された行動計画の確認を要請すること

- データ保護機関の同意を得た後、行動計画の実施

再認証

ユーロプライバシー認証書の有効期間は 3 年間であり、更新には再認証評価が必要です。認証機関は、再認証監査の結果、認証期間中のシステムレビューの結果、認証の利用者から受領した苦情を踏まえ、認証更新の可否を決定します。再認証監査の目的は、評価対象がユーロプライバシー要件の遵守を継続していることを確認することです。

異議申立て及び苦情

決定に対する異議申立ては、申請者から認証機関に対し、又は、認証機関から本制度オーナーに対し、行うことができます。

第三者が、認証を受けたデータ取扱いが本認証制度又は適用可能なデータ保護規制を遵守していないと考える場合、認証を受けた申請者、認証機関又は所管官庁に苦情を申し立てることができます。

提出された証拠に基づき、受領者は、認証機関若しくはデータ保護機関、又は、その両方に通知しなければなりません。苦情によって明らかになった情報が、本認証制度の社会的信頼性及び評判に影響を及ぼすおそれがある場合、遅滞なく本制度オーナーに通知されます。

苦情が認証機関によって適切に取り扱われなかった場合、当該苦情申立者は、その問題を本制度オーナーに通知するよう求められます。

認証機関及びその従業者は、受領した全ての苦情、異議申立て及びその後の措置を記録する責任を負います。認証活動に関連する苦情又は異議申立てを受領した場合、認証機関は以下の事項を行わなければなりません。

- 正式な苦情又は異議申立て受領の確認
- 全ての関連情報の収集及び検証
- 苦情申立者又は異議申立者に対する手続の結果の正式な通知
- 苦情又は異議申立てを解決するために必要なその後の措置を講じること
- 本制度オーナーに対する本認証制度又はその評判にとってリスクとなるおそれのある重大な問題の通知

苦情が正当であると認められた場合、認証機関はそれに適切に対処しなければならず、また、それを解決するために合理的な努力を行わなければなりません。申請者及び認証機関は、当該苦情の取扱い及び解決のため、当該苦情を調査し、明確化を提供するために全面的な支援を行わなければなりません。根拠のある苦情は、認証書の一時停止又は取消しに繋がる可能性があります。

偏りのない手続を確保するために、苦情又は異議申立てに関連する決定は、以下の条件を満たす個人によって採択されます。

- 関連する認証手続に直接関与していない者
- 異議申立者又は認証を受けた申請者にサービスを提供していない者

情報管理及び機密保持

情報管理及び機密保持

認証機関は、標準化された文書化手法を確立するのが望ましいです。評価中に作成される文書は、以下の 3 つの主な点に焦点を当てるのが望ましいです。

- 実施された評価手法の一貫性及び整合性
- 評価対象が認証基準、ひいてはデータ保護規制を遵守していることを証明するための手法の十分性

- 意思決定手続の公平性

認証機関は、認証手続が詳細に規定され、信頼性が認められ、そして、明確かつ利用者に分かりやすいことを確保するため、文書を分類及び識別するための明確かつ一貫性のある手法及び手続を用いなければなりません。本認証制度の公式文書の分類及び識別は、*ユーロプライバシー文書の管理及び分類*に定める運用指針に従います。改訂された文書は、繰り上げられたバージョン番号とともに公開されます。

本制度オーナーによって提供される文書に関し、認証及び監査手続では、手続の開始時点で入手可能な本認証制度及び関連文書が使用されます。認証及び監査手続中に文書の最新版が公開された場合、当該最新版を考慮し、可能な限り当該最新版を遵守するのが望ましいです。

認証機関は、認証手続中に収集又は作成された情報を適切に管理及び保護する責任を負います。

認証活動に関与し、又は、内部情報にアクセスする全ての要員は、認証に関連する全ての機密情報の機密性を保持し、保護しなければなりません。原則として、申請者によって提供された情報又は申請者及びその認証に関連する情報は、情報が以下の条件に該当しない限り、機密情報として扱われます。

- 公開情報
- 申請者によって非機密情報として分類された情報
- 申請者の同意を得て開示された情報
- 法律上又は契約上の理由により開示しなければならない情報

機密保持義務は、認証レジストリに公表されなければならない情報には適用されず、データ保護機関等の権限を有する者による正当な情報へのアクセスを妨げるものではありません。認証機関は、法律により機密情報の開示を求められた場合、そのような要請に従わなければなりません。各国データ保護機関及び本制度オーナーは、認証のサーベイランス及び苦情取扱いなどの責務を果たすため、機密情報へのアクセスを要請することがあります。情報の機密性を保持する公式な契約上の義務を負う権限ある者のみが、保管されているデータ及びファイルにアクセスできるべきです。

認証機関は、その情報発信プラットフォームにおける公開情報の開示に関する明確な規定を持たなければなりません。

認証機関は、原則として、以下の事項に関する**一般的な情報を公開**しなければなりません。

- 認証評価手続
- 認証及びその範囲に関する決定手続
- 認証機関が運営するマネジメントシステム及び認証制度の種類
- 認証機関の名称、ロゴ及び遵守マークの使用
- 情報の要請、苦情及び不服申立てを取り扱うための手続
- 公平性方針及び公平性メカニズム
- 郵便所在地など、認証機関の連絡先の詳細
- 認証機関の個人情報保護ポリシー及びデータ保護オフィサー（DPO）への連絡方法

要請に基づき、認証機関は、以下の事項に関する補足情報を提供しなければなりません。

- 認証機関が業務を遂行する地理的領域
- 特定の認証のステータス
- 認証を受けた申請者の名称、関連する規範文書、適用範囲及び地理的場所
- 本認証制度に関する情報
- 認証機関が財務的支援を受ける手段の記述、及び、申請者に課される料金に関する一般的情報
- 申請者の権利及び義務の記述
- 苦情及び異議申立ての取扱手順に関する情報

本制度オーナーは、公式引用文書のリポジトリ、及び、発行済みのユーロプライバシー認証書の公式オンラインレジストリを備えたユーロプライバシー公式ウェブサイトの管理及び監視を担当します。認証機関は、本制度オーナーが提供する情報と一致する限り、自機関のウェブサイトに公開情報を複製することができます。認証機関は、公式ユーロプライバシー認証レジストリで公開される情報を更新し、情報更新の遅延を避けなければなりません。ライセンスを取得した認証機関は、そのウェブサイトからユーロプライバシー認証レジストリ及び公開情報ウェブサイトへのリンクを提供しなければなりません。

遵守マーク、ライセンス及び認証書の使用

認証手続が完了し、付与された認証がユーロプライバシー認証レジストリで公開されると、認証を受けた申請者は、ユーロプライバシーロゴ及び遵守マークの使用を開始できます。**ユーロプライバシーロゴ及び遵守マークは、本制度オーナーの財産です。**申請者は、認証機関による承認後、認証機関の監督の下で、ユーロプライバシーロゴ及び遵守マークを使用することができます。認証機関及び申請者は、認証書及び遵守マークの使用に関する本認証制度の規則、並びに、ユーロプライバシーの情報発信に関する規定及びガイドラインを遵守しなければなりません。

遵守マークは、以下の事項を行います。

- 本認証制度及びその適用範囲に関する明確な情報を提供すること
- 認証の適用範囲に関する誤解を招くような発信を防止すること
- 認証機関及びそのレジストリへのトレーサビリティを可能にすること

マーク又は付随するテキストにおいて、認証を付与した認証機関又は認証範囲に関して、一切の曖昧さも存在してはなりません。

認証機関及び本制度オーナーは、ライセンス、認証書、遵守マーク、並びに、データ取扱いが認証機関によって認証されていることを示すその他の仕組みの保有、使用及び表示について管理権を有します。認証機関及び本制度オーナーは、本認証制度への不正確な参照、又は、ライセンス、認証書、マーク若しくはその他の仕組みの誤解を招く使用が、資料又はその他の広報文書に存在するかを確認します。

ECCP は、ユーロプライバシーパートナー又は外部機関が制作した全ての出版物、販促品及び機器において、ユーロプライバシー商標、ロゴ、シール及びセカンダリーロゴの正しい使用及び完全性を確保する責任を負います。

基本原則

ユーロプライバシーは、商標の使用に関し、以下の基本原則を定めています。

- ユーロプライバシー若しくは ECCP の商標、又は、その両方の使用には、ECCP からの事前の書面による明示的な許可又はライセンスが必要である。
- ユーロプライバシーの用語若しくはユーロプライバシーロゴ、又は、その両方の使用は、常に特定のガイドラインを遵守しなければならない。
- ECCP は、以下のいずれかの可能性のある発表、広告、出版物又は報告書において、ユーロプライバシーの名称又はグラフィックの使用を許可しない。
    - ユーロプライバシーと関連しない製品又はサービスの推奨を暗示する可能性がある場合
    - 付与された認証に関して第三者を誤解させる可能性がある場合
- ECCP が提供するユーロプライバシーの文書及び情報発信資料は著作権で保護され、ECCP の書面による明示的な許諾なく、複製、複写、配布、改変又は販売することはできない。
- ユーロプライバシー商標を使用する第三者は、ECCP から受けた指示に従わなければならない。

ユーロプライバシーマーク及びロゴ

図 1 ユーロプライバシーマーク及びロゴ

ユーロプライバシーという用語及びユーロプライバシーロゴは、ECCP によって管理される国際商標です。テキスト及びビジュアル商標は、米国を含むいくつかの法域に登録されています。

ユーロプライバシーの文字商標は「ユーロプライバシー」です。

ユーロプライバシーのロゴは、図に示すとおり、青色で「E」及び「P」の文字、並びに、6 つの黄色の星で構成されています。このレターマークは、通常、商標記号及び登録商標記号、並びに、補足テキストと、しばしば関連付けられます。

ユーロプライバシーの**レターマーク**及びシグネット（シンボルマーク）は、改変、変形、分割、又は、新規若しくは異なるブランドと認識される可能性のある方法で使用してはなりません。 **ワードマーク**及びレターマークは、周囲の余白領域に明確に表示され、視認できなければなりません。

認証書

認証を受けたデータ取扱いは、認証機関の管理及び承認の下で、ユーロプライバシー認証書を取得することができます。認証書には、以下の事項が含まれなければなりません。

- 認証機関及びユーロプライバシーロゴ
- 認証を受けた申請者の名称
- 申請者がデータ管理者、データ処理者又は共同データ管理者のいずれか
- 該当する場合、共同管理者の名称
- 評価対象及びその地理的適用範囲の明確な記述
- 該当する場合、認証に適用された拡張
- 認証書の発行日及び有効期限
- 発行された認証書の固有識別子
- 「詳細はこちら」という記載に続き、本認証制度のウェブサイト及びオンライン認証レジストリのドメイン名
- 認証書を発行した認証機関の名称及び所在地

認証書は明確で、データ主体が容易に理解できるものでなければなりません。1 ページを超えないのが望ましいです。

遵守マーク

認証されたデータ取扱い活動は、認証機関の管理及び承認の下で、ユーロプライバシー遵守マークを付与することができます。遵守マークには以下が含まれます。

- ユーロプライバシーロゴ
- 固有認証識別子
- 本認証制度ウェブサイトのドメイン名

さらに、遵守マークには、例に示すように、認証範囲の拡張が含まれる場合があります。

図 3 ユーロプライバシー遵守マーク

遵守表明

Statement of Conformity
with the GDPR and Europrivacy

Applicant
COMPANYNAME.SA
123 Address street
1111 City, Country
declares under its sole responsibility that the following data processing is in conformity with the following requirements:

Certification

Target of Evaluation:	Personal data processing by the smart parking solution deployed on the municipal territory of the city ABC.
Normative Scope:	Europrivacy criteria, v. 05.03.2019
Certified on and until:	April 27 2019 – April 26 2022
Certificate ID:	83F4:A014
Detailed information at:	www.europrivacy.com
Certification Body:	CERTIFICATION.SA 567 Address street 2222 City, Country

Signature

Authorized representative:	Mr ABC
Date:	May 3 2019
Signature:	XXXXXX

図 2 ユーロプライバシー認証表明

申請者は、認証機関の事前の書面による承認を条件として、ウェブサイト又はその他の関連情報及び文書に認証表明を含めることができます。

本声明には、以下の事項が含まれます。

- ユーロプライバシーへの参照、許可されている場合はユーロプライバシーロゴ
- 認証を受けた申請者の名称
- 該当する場合、共同管理者の名称
- 評価対象及びその地理的適用範囲の明確な表示
- 該当する場合、追加された補完的規範又は補完的要件の明確な表示
- 認証書の発行日及び有効期間
- 発行された認証書の固有識別子
- 「詳細はこちら」という記載に続き、本認証制度のウェブサイト及びオンライン認証レジストリのドメイン名
- 認証書を発行した認証機関の名称及び所在地

GDPR 第 42 条及び第 43 条に基づく有効性を申請者が求めることなく、自発的に認証が付与される場合、遵守表明にはその旨が明記されなければなりません。

その他の考慮事項

ユーロプライバシー認証に関連する認証書、遵守表明又は遵守マークをウェブページ又は PDF 文書等の電子媒体に表示する場合、本認証制度のメインホームページ、オンラインレジストリ内の認証を受けた評価対象のページへの直接のハイパーリンクを含めるのが望ましいです。
遵守マーク、認証書及び認証表明は、その認証を受けた評価対象について混乱又は誤解を招くおそれのある方法で使用してはいけません。

認証機関は、発行した認証書の使用及び参照について、権利の適切な管理を行わなければならず、認証状態への不適切な参照、認証文書、マーク又は監査報告書の誤解を招く使用に対処するための措置を講じなければなりません。当該措置には、修正及び是正措置の要請、認証の一時停止、取消し、違反の公表、並びに、必要な場合は法的措置が含まれます。

基準、確認項目及び管理項目の明細一覧

ユーロプライバシー基準、確認項目及び管理項目

評価基準

評価基準は、ユーロプライバシー認証制度の最新版の要件を遵守して適用されます。認証機関は、以下のとおり評価基準を適用します。

- データ主体の権利及び個人データに対する潜在的リスクに留意すること
- 一貫性のある均質的方法で行われること
- 検証可能かつ監査可能な方法で行われること
- 組織の規模、データ取扱いの性質、並びに、データ及びデータ主体に対する特定されたリスクを考慮すること

詳細なユーロプライバシー評価基準、確認項目及び管理項目は、以下の側面を評価することを目的としています。

- 取り扱われる個人データの特定
- データ主体に提供されるデータ取扱いに関する情報の要件遵守
- 取扱いの適法性、及び、「事前のインフォームドコンセント」要件の遵守
- 未成年者に関する要件の遵守
- デザイン及びデフォルトによるデータ最小化の原則の遵守
- GDPR が定める透明性の原則の遵守
- データ処理者及び越境データ移転の問題を含む個人データの流通分析
- 個人データのライフサイクル及び個人データの保持期間の最小化
- データ主体の権利の効果的な実施
- 間接的に収集したデータの存在及び遵守
- 自動的な個人の決定において、データ主体の権利、自由及び正当な利益の安全性を確保するための適切な措置の実施
- 収集したデータの安全性、並びに、効果的な保護及び完全性
- 管理者によるデータ保護のための適切な技術的・組織的措置の実施
- データ処理者が用いられる場合、管理者が処理者による適切な技術的・組織的措置を実施するための十分な保証を提供することを確保するための手順・契約
- 認証範囲に含まれる場合、補完的国家固有若しくは分野固有、又は、その両方の規範的要件及び基準

評価基準は、本制度オーナーが維持する基準、確認項目及び管理項目の明細一覧に変換され、データ保護機関及びライセンスを受けた第三者は使用可能になります。認証機関は、評価対象におけるデータ取扱いの遵守状況を体系的に評価するため、基準、確認項目及び管理項目の一覧を使用します。

ユーロプライバシー基準、確認項目及び管理項目は、ウェルカムパック及びユーロプライバシー・コミュニティウェブサイトを通じて様々な形式で提供されます。ユーロプライバシー基準は、認定パートナーの遵守状況評価ソフトウェア及びソリューションを通じても利用できます。

コア基準

コアとなる GDPR の義務に加え、評価対象は、補完的各国固有規制又は分野固有規制の対象となる場合があります。

最も重要な基準一覧は、以下のとおりです。

1. ユーロプライバシー**GDPR コア基準**

全てのデータ取扱いに適用可能な GDPR の要件を網羅したもの

以下の 3 つの補完的要件によって補完されます。

2. **補完的文脈的確認項目及び管理項目**
   分野・技術固有の要件の遵守状況を評価するためのもの
3. **技術的措置及び組織的措置の確認項目及び管理項目**
   取り扱われるデータを保護するために設定した安全性対策の評価のためのもの
4. 補完的データ保護を伴う**国家固有データ保護義務**

補完的国家固有要件及び規範的要件

第 43 条に基づく GDPR 認証では、認証対象のデータ取扱いが、データ管理者又は処理者の本社が所在する EU 加盟国の国内義務を遵守することが求められます。これらの義務には、評価対象に適用可能な個人データ保護に関連する全ての分野固有の各国規制も含まれます。各国には、データ保護の要件に影響を与え、拡張する固有の各国法規制が存在します。申請者は、評価対象が適用可能な各国規制を遵守していることを確保するとともに、それらの改正をモニタリングしなければなりません。
欧州経済領域（EEA）からの申請者は、申請国において GDPR の義務を超える補完的国家固有義務への評価対象の遵守状況を評価するため、十分な法的専門知識を有する専門家に依頼しなければなりません。その評価結果は、*国家固有義務遵守状況評価報告書*（NOCAR）として提出されます。NOCAR が存在しない場合、認証機関は、申請国における適用可能な国家固有義務への評価対象の遵守状況の評価を代替的に実施可能であり、その要件水準は NOCAR と同等です。

補完的技術的措置及び組織的措置の要件

ユーロプライバシー認証では、取り扱われ、及び、記録保存されるデータを保護するための十分な技術的・組織的措置が講じられていることが求められます。

補完的技術的・組織的措置の確認項目及び管理項目は、データ取扱いの安全性の十分性を評価するために規定されています。当該確認項目及び管理項目は、コア基準を補完し、以下の両方の条件を充足しない限り、全ての評価対象で必須です。

- 有効な ISO/IEC 27001 認証の対象であること
- 高いリスクのデータ取扱いを一切実施しないこと

補完的文脈的及び分野固有要件

補完的文脈的確認項目及び管理項目には、特定の技術又は適用分野に対応する様々な確認項目及び管理項目の小分類が含まれます。認証機関は、評価対象に含まれるデータ取扱活動に適用可能な全ての確認項目及び管理項目の小分類を適用及び評価します。

認証手続

ユーロプライバシー遵守状況評価は、基準、確認項目及び管理項目の体系的な順序で構成されています。

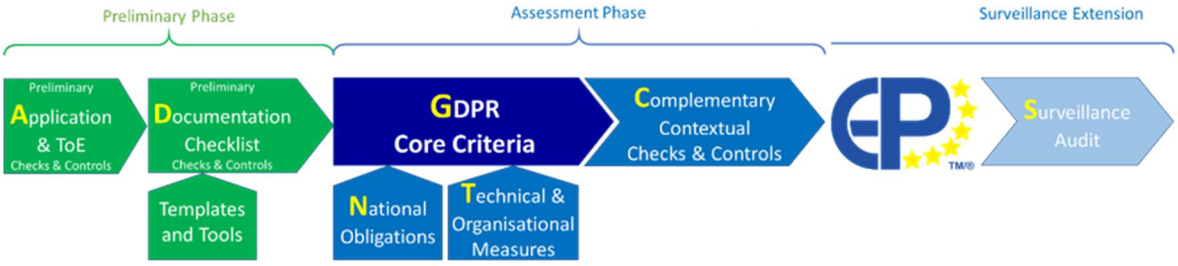

図 5 ユーロプライバシー認証手続、並びに、適用可能な確認項目及び管理項目

事前段階では、評価対象の評価準備が整っていることを確保します。

申請及び評価対象の確認項目及び管理項目は、評価対象の特定が EDPB によって定められたガイドラインを遵守しているか否かを評価するため、認証機関によって使用されます。これらの確認項目及び管理項目は、申請者が準備できますが、評価手続開始前に認証機関によって確認されなければなりません。

文書チェックリストは、文書の収集を容易にするとともに、監査チームが必要な文書にアクセスできることを確保することを目的としています。申請者が記入し、評価開始前に主任監査人による確認を受けるのが望ましいです。

評価対象及び利用可能な文書の十分性は、評価手続開始前に、主任監査人によって確認されるのが望ましいです。

以下の確認項目及び管理項目は、評価対象がユーロプライバシーを遵守しているか否かを評価するために用いられます。申請者は様々な基準を充足する証拠を準備できますが、正式な確認は認証機関の排他的な責任となります。

GDPR コア基準は、全てのユーロプライバシー認証手続の基盤を成し、適用分野及び場所に関わらず、認証機関の監査人によって、あらゆる評価対象に適用されます。GDPR コア基準は、GDPR が定める義務の遵守状況を体系的に評価することを可能にします。これにより、全てのユーロプライバシー認証が、GDPR のハイレベルの遵守を確保します。この一覧は、全ての認証において必須です。

補完的文脈確認項目及び管理項目は、分野及び技術固有のデータ保護要件を評価するために規定されます。これらは、EDPB 及び各国データ保護機関の公表物及びガイドライン、並びに、研究コミュニティからの専門知識を考慮しています。本一覧は、各認証において必須です。補完的文脈確認項目及び管理項目は、特定技術及び分野に適用可能な様々な確認項目及び管理項目の小分類に分類されます。認証機関は、本一覧を精査し、評価対象に適用される全ての小分類を評価及び検証しなければなりません。

ユーロプライバシー認証では、取り扱われたデータを保護するために十分な技術的・組織的措置が講じられていることが求められます。**技術的・組織的措置の確認項目及び管理項目**は、申請者によって取り扱われるデータの安全性確保及び保護のために講じられた措置の遵守状況を評価することを目的としています。

ユーロプライバシーは、加盟国の言語で認証を受けたデータ取扱いに関する情報を提供する義務など、既に認証を受けたデータ取扱いに固有の義務を評価するため、**サーベイランス又は再認証**を実施する際に適用されるいくつかの補完的確認項目及び管理項目を規定しています。

不遵守一覧のテンプレートは、申請者が認証を受けるために是正しなければならない特定された不遵守を報告及び一覧化するため、認証機関によって使用されるものです。代替案として、認証機関は、不遵守を報告するため、独自のテンプレートを用いることもできます。

認証書公表のための**参考チェックリスト**は、ユーロプライバシー認証書交付前に全ての管理要件を充足していることを確保するため、認証機関に提供されます。

ID	確認項目及び管理項目の一覧	ステータス	主任	代替案	CF	CB
A	**申請及び評価対象**	**必須**	**認証機関**	**無し**	**X**	**X**
I	申請者によって完成又は提供されるインベントリー	情報提供	申請者	データ取扱いレジストリ	X	X
D	**文書の確認項目**	**情報提供**	**申請者＆認証機関**	**無し**	**X**	**X**
E	データセットの評価	情報提供	申請者＆認証機関	認証機関マネジメントシステム	X	X
G	**GDPRコア基準**	**必須**	**認証機関**	**無し**	X	X
C	**補完的文脈的確認項目及び管理項目**	**必須**	**認証機関**	**無し**	**X**	**X**
T	**技術的措置及び組織的措置（TOM）**	**必須**	**認証機関**	**ISO 27001/27701**	**X**	**X**
N	国別要件	情報提供	認証機関	法的評価	X	X
S	**サーベイランス監査**	**必須**	**認証機関**	**No**	**X**	**X**
NC	**不遵守一覧**	**必須**	**認証機関のみ**	**認証機関マネジメントシステム**		**X**
Z	認証公表チェックリスト	情報提供	認証機関のみ	認証機関マネジメントシステム		X

図 6 確認項目及び管理項目の適用範囲

特定の適用範囲

ユーロプライバシー基準、確認項目及び管理項目は、その適用範囲を決定し、簡素化するため、個々に区別され、明確なカテゴリーにリンクされています。

各列は、本基準、確認項目及び管理項目措置が、以下のいずれに適用されるかを示しています。

- データ管理者（**C**）
- データ処理者（**P**）
- データ管理者（**C**）及び処理者（**P**）の両方

比例原則に対応し、単純なデータ取扱いとより大規模で機微性が高いデータ取扱いを区別するため、別の列では、本基準、確認項目及び管理項目を以下のカテゴリーに区別しています。

- 原則として、全ての認証手続で必須
- 単純なデータ取扱いの認証には求められていないが、以下のような高いリスクのデータ取扱いの認証には必須である。
    - 特別な種類の個人データ又は有罪判決に関するデータを取り扱う場合
    - 特に未成年者の個人データを対象とする場合
    - 自然人の権利及び自由にとって高いリスクをもたらす可能性が高い場合
- 適用除外（**E**）のカテゴリーは、基準要件に対する適用除外が正当化できるか否かを判断するためのものである。

もう 1 つの列は、本基準、確認項目及び管理項目が以下に該当するかを定めています。

- データ取扱いごとに固有のもの（**S**）
- 複数のデータ取扱いに共通する一般的なもの（**G**）

別の列には、以下のとおり、欧州経済領域（EEA）外に所在し、GDPR の直接の対象ではないデータ輸入者に対して本基準が適用可能かを定めています。

- **R** は、EEA 外に所在するデータ輸入者に本基準が必要となることを示しています。
- **NR** は、EEA 外に所在するデータ輸入者には本基準が必要とならないことを示しています。

基準の形式

基準は、「～しなければならない」、「～されなければならない」、「～してはならない」といった shall 条項として定式化され、「AND」、「OR」、「IF…THEN」を用いて明確な論理関係で表現されます。

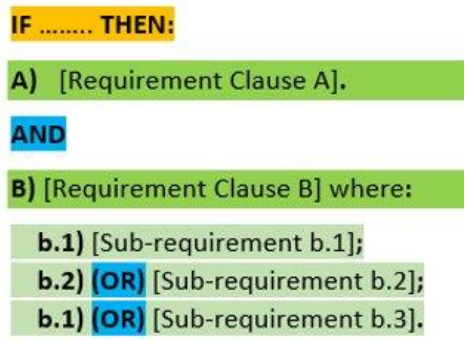

図 3 基準の形式

条件条項は、基準の適用範囲を特定の条件に制限します。文頭は「IF」、そして、文末は「THEN」です。条件がデータ取扱いに適用可能な場合、関連する後続の基準を評価しなければなりません。条件が適用されない場合、関連する後続の基準はスキップできます。

基準は、**要件条項**と呼ばれる形式要件を規定する 1 つ又は複数の条項で構成されます。1 つの基準には、複数の要件条項が含まれる場合があります。主要な要件条項は、大文字のアルファベット及び括弧で始まります。

基準が複数の条項を含む場合、各要件条項の間に**ブール関係**項が規定されます。

各主要条項は、任意で一連の**サブ要件**を含むことができます。サブ要件の一覧はコロン（:）で始まります。各サブ要件は、以下のとおりです。

- 対応する主要な要件条項の文字で始まり、ドット及び数字が続く。
- 一覧の最初のサブ要件を除き、括弧内にブール関係項を含む。
- 後続に別のサブ要件が続く場合はセミコロンで終了し、一覧で最後のサブ要件の場合はドットで終了する。

評価対象の特定

評価対象は、認証を受ける個人データ取扱活動の適用範囲を特定及び限定します。データ主体を含む第三者が明確に理解できる形で規定されなければなりません。GDPR 認証は、企業単位、又は、そのマネジメントシステム単位に対して発行することはできません。範囲が広すぎて特定性が不足し、効果的かつ信頼性のある認証とはみなされないためです。代わりに、顧客データベース、カスタマーサポートサービス、給与・会計サービス、企業ウェブサイト又はスマートフォンアプリケーションなどのデータ取扱活動が考慮されるのが望ましいです。

評価対象の特定には、一定の柔軟性及び自由度があります。異なる目的の 1 つ又は複数の取扱業務を含めることが可能です。ただし、評価対象は、取り扱われるデータの出所、認証を受ける取扱活動の一般的な目的に関して、一定水準の均質性を持たなければなりません。評価対象が複数の管轄若しくは法人、又は、その両方を跨ぐ場合、その特定は、認証を受けるデータ取扱活動に対する効果的な管理及び責任と整合していなければなりません。これは、複数のセグメントで認証を実施及び付与することを意味し得るところです。

認証機関は、評価対象に含まれる各データ取扱活動を評価しなければなりません。認証文書は、完全に透明かつ明確である必要があります。

評価対象は、認証を受ける個人データの取扱活動を明確に記述し、正式に特定されなければなりません。その特定には、データの出所、個人データのカテゴリー、データ主体のカテゴリー、データ取扱いの目的、取扱いが行われる国、データ処理者の利用、取扱いの記述的説明など、詳細な情報を含めなければなりません。

評価対象を特定する手続は、主に 6 つの段階で構成されます。

1. **データ取扱活動の選択**
   申請者にとってのリスクの観点から、優先度の高いデータ取扱い活動から始めます。
2. **評価対象の特定及びマッピング**

ユーロプライバシー認証申請書を用いて、評価対象における個人データの流通の特定及びマッピングを行います。

3. **評価対象の十分性の確認**
   評価対象の特定内容の完全性及び十分性を確認するため、申請及び評価対象－事前確認項目及び管理項目を適用することによって、確認します。
4. **評価対象の遵守の文書化**
   評価対象におけるデータ取扱活動がどのように適用可能なユーロプライバシー基準を遵守しているかを確認及び文書化します。この段階で、既にリスクは大幅に低減されます。
5. **評価対象の認証**
   遵守認証書により、申請者は自らの遵守を証明、価値化及び発信することが可能となります。
6. **コンプライアンスの維持及び享受**
   認証取得後、規制変更の通知機能などを含むオンラインリソースを活用し、データ取扱活動のコンプライアンスを維持します。その後のサーベイランス監査により、申請者が継続的にコンプライアンスを維持しているかが証明されます。

表の構造及びその記入方法

水平（横）方向の表構造

一覧は複数のタブで構成されています。「コア基準」タブには、全ての監査で対象となるコア基準、確認項目及び管理項目が集約されています。

Ref ID	Target	Specific/	Level	TITLE	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	Suggested Means of Verification (for the Auditor)	GDPR Art.	Evidences & Reference Documents (or Justification if Not Applicable)	Recommendations / Comments (if applicable)	Status Appraisa l	NC #
G.1				Lawfulness of Data Processing Objective: To ensure that the data processing in the Target of Evaluation is lawful and proportionate. Condition: IF the Applicant is the Data Controller of the personal data processed in the Target of Evaluation, THEN:							
G.1.1				Lawfulness of processing				L			
G.1.1.1	C	S	A	Lawfulness assessment of the processing	A) There shall be a written report or document demonstrating that the data processing in the Target of Evaluation has been assessed as lawful by the Applicant's DPO or by a legal expert with adequate expertise. AND B) Where the lawfulness is conditional to corrective actions, the Applicant shall have implemented them. AND C) The assessment (or reassessment) report of lawfulness shall: c.1) cover all personal data processing specified in the Target of Evaluation; c.2) (AND) indicate the lawfulness basis of the data processing; c.3) (AND) where applicable, include the justifications documents or references; c.4) (AND) have been performed within the last 12 months before the initial assessment.	Record and documentation of the lawfulness assessment and validation. DPO interview. DPO or law firm written statement.	6.1				
G.1.1.2	C	S	A	Lawfulness justification	The data processing shall comply with at least one of the following justifications:		6.1				

図 8 表の水平構造

Excel 表は以下の列で構成されています。

1. **参照 ID** の列は、各確認項目及び管理項目に固有の識別子を付与しています。
2. **対象**の列は、確認項目及び管理項目の適用対象を以下のとおり定義しています。
   - 管理者（**C**）のみ
   - 処理者（**P**）のみ
   - 管理者（**C**）及び処理者（**P**）両方
3. **固有／一般**の列は、確認項目及び管理項目が、固有のものか一般的なものかを明確化しています。
4. **レベル**の列は、確認項目及び管理項目のレベルを特定しています。
5. **タイトル**の列は、確認項目及び管理項目のタイトルを示します。
6. **基準**の列は、申請者が実施し、監査人が評価すべき正式な要件を記述しています。基準は、申請者が遵守すべき規定条項です。
7. **推奨される検証手段**の列は、情報が所在する通常の情報源について監査人に指針を提供します。これは参考情報であり、監査人は他の関連情報源を選択できます。
8. **GDPR 条項**の列は、確認項目及び管理項目に関連する主な GDPR 条項を示しています。

9. **証拠及び参照文書**の列は、監査人が遵守又は不遵守の決定に考慮された証拠を明確に示し、監査人によって記入される必要があります。認証に適用されないと判断された確認項目及び管理項目を除き、この欄は必須です。
10. （該当する場合、）**推奨／コメント**の列は、監査チームが申請者によって対処されるべき問題及び要素を特定できるようにします。
11. **ステータス**の列は、監査人が確認項目及び管理項目における所見の状況を判定するために使用します。
12. **NC #** の列は、特定された不遵守の識別番号を示すために用いられます。

確認項目及び管理項目は、GDPR の構造に沿って異なる基準ごとにグループ化されています。

垂直（縦）方向の表構造

1. **ヘッダー**には、各列のタイトル及び機能が記載されています。
2. **上部セクション**は、主要セクションの開始を示しています。
3. **サブセクション**は、主要セクション内のサブセクションの開始を示しています。
4. **確認項目及び管理項目**は、必須要件の列において、セルの白色背景で特定されます。
5. **事前確認項目**は、必須要件の列において、セルの薄緑色背景で特定されます。

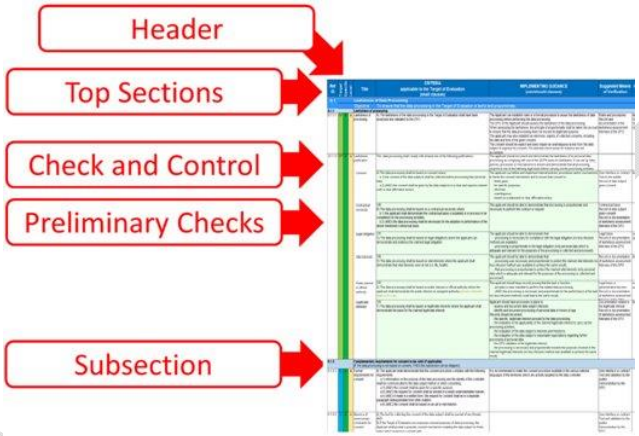

図 9 表の垂直構造

手続概観

セクションの確認項目及び管理項目を評価する際の手続は、以下のとおりです。

1. 上位カテゴリーにおいて要求される確認項目及び管理項目の実施
2. 確認項目及び管理項目の体系的検討
3. 事前確認項目の完成

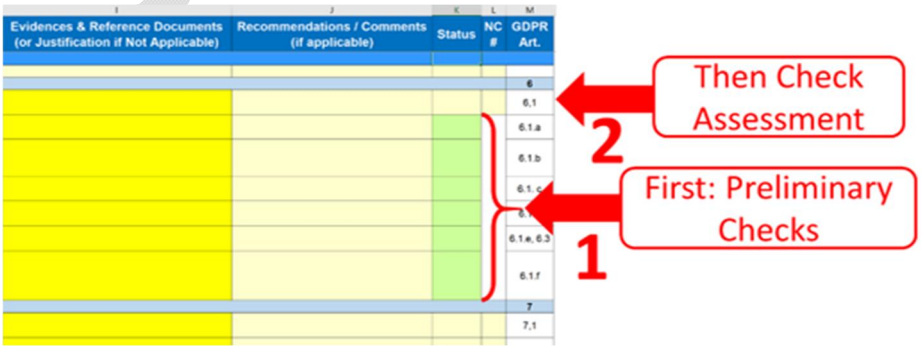

図 10 手続概観

各確認項目及び管理項目

4. 対応するセルにおける明確な証拠の提示
5. コメント及び推奨による補完（「推奨／コメント」）
6. 確認項目及び管理項目のステータスの決定
7. 不遵守が特定された場合、対応する列（「NC#」）に、明確な識別子（数字又はアルファベット）を付して記載すること
8. ダッシュボードは表の下部に用意され、確認項目及び管理項目の結果、並びに、ステータスの要約を提供

Status Code		Meaning / Explanation	Tot	%
OK		Conformity: Requirement has been controlled and appears to be respected and no non-conformities have been identified.	2	22%
OK+		Good practice moving beyond simple conformity	2	22%
Obs		Observation	1	11%
			5	56%
Min NC		A Minor Non-Conformity (non-critical) has been identified.	1	11%
Maj NC		A Major Non-Conformity (critical) has been identified.	1	11%
?		Missing Information / Don't know	0	0%
NA		Control is Not Applicable for the targeted certification	2	22%
			9	

図 11 指標ダッシュボード

ステータスの選択肢

黄色セルのステータス欄には、異なるステータスに対応する複数の選択肢一覧が表示されます。

図 12 通常のステータスセル

ステータスコード	意味／説明
?	情報不足／不明
OK	遵守：要件は管理され、遵守されているようであり、また、不遵守は特定されなかった
OK+	単なる遵守を超えた優良実務（プラクティス）
Obs	観察
Min NC	軽微な（重大でない）不遵守が特定された
Maj NC	重大な不遵守が特定された
NA	対象となる認証には管理項目は**適用されない**

図 12 ステータスの選択肢

一部のセルは、確認項目及び管理項目のステータスの評価に使用される補足質問に対応しています。そのステータスのための該当セルの背景色は、黄色ではなく緑色です。緑色セルのステータス欄には、異なるステータスに対応する簡略化されたオプションの一覧が表示されます。

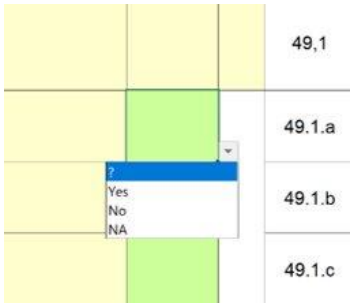

図 13 サブ質問ステータスセル

ステータスコード	意味／説明
?	情報不足／不明
YES	はい
NO	いいえ
NA	対象となる認証には管理項目は適用されない

図 13 サブ質問のステータスの選択肢

試験準備

公式な証明書を取得し、ユーロプライバシー実装者になるためには、参加者は最終試験に合格する必要があります。本ハンドブックの本セクションは、試験の種類に慣れ親しむための準備を目的としています。

試験は多肢選択式問題（実装コースは 50 問）で構成され、制限時間（1 時間 15 分）内に終了する必要があります。各問題には 4 つの選択肢があります。正解が 1 つだけの問題もあれば、複数の正解がある問題もあります。試験中、単一解答か複数解答かを集中して判断する必要があるか、ヒントが表示されます。詳細は、コースページの最終試験に関する免責事項 をご参照ください。

本ハンドブックの模擬試験は 25 問で構成され、45 分以内に解答することを推奨します。本番の試験と同様に、各問題には 4 つの選択肢があります。問題に正解すると 1 点が加算されます。複数の正解がある問題もあり、採点基準は以下のとおりです。

- 問題に正解した場合：1 点
- 複数の正解がある問題で正解を 1 つでも逃した場合：0 点
- （正解を選択したか否かに関わらず、）不正解の場合： 0 点

模擬試験に合格するためには、25 点中 19 点以上の獲得が必要です。解答シートはセクション終了時に利用可能です。

例

	QUESTION	A	B	C	D
15	Which of the following is NOT a key principle of Europrivacy certifications?	Independence	Fair presentation	Favouritism	Confidentiality
16	Which of the following are considered a Europrivacy Complementary Normative Documents?	Europrivacy Guidelines for NOCAR completion	Europrivacy Communication and Marketing Rules	Guidelines on Accountability and Openness	Europrivacy Guidelines on the Use Criteria, Checks and Controls
17	Which of the following provides definitions for the Europrivacy Certification Scheme?	GDPR and EDPB Guidelines	Oxford Dictionary	Other relevant normative sources, such as ISO	Wikipedia

このシナリオでは、受講生は以下の回答（オレンジ色で表示）を選択しました。

- 問題 15：C
- 問題 16：D
- 問題 17：A、B、C

解答シートには以下の正解が示されています。

問題番号	正解
15	C
16	B D
17	A C

これは、以下を意味します。

- 問題 15 の解答は正解であり、受講生は 1 点を獲得します。
- 問題 16 の解答は部分的に正解（B が欠落）です。受講生は点数を獲得しません。
- 問題 17 では、A 及び C が正解です。しかし、受講生は不正解の B も選択したため、問題全体で点数を獲得しません。

説明

正解には、問題がどのモジュールに関連しているかが示されています。不明な点がある場合は、これらのポイントを注意深く学習してください。

模擬試験

	問題	A	B	C	D
1	実装者に該当する記述は？	データ保護コンプライアンスの認証のため認証機関に所属する	本制度オーナーの法的・財務的リスクを低減させるため、コンサルティング会社に所属する	潜在的ギャップ及び残存する不遵守特定のため認証機関に所属する	認証手続前後を通じて申請者を支援するためコンサルティング会社に所属する
2	管理項目及び管理項目に適用されるカテゴリーは？	E 適用除外	S 固有	O 目的	NC 不遵守
3	次の記述のうち、正しいものはどれか？	ユーロプライバシー若しくは ECCP の商標、又は、その両方の使用には、データ保護機関からの事前の書面による明示的な許可又はライセンスが必要である	遵守マーク、認証書及び認証表明は、その認証を受けた評価対象について混乱又は誤解を招くおそれのある方法で使用してはいけない	認証機関は、発行した認証書の使用及び参照について、権利の適切な管理を行わなければならない	認証を受けたデータ取扱いは、認証機関の管理及び承認の下で、ユーロプライバシー認証書を取得することができる
4	コンサルティング会社及び申請者との間で、最終会議中に起こることは？	コンサルティング会社が補足見積提案を提示する	コンサルティング会社が本制度オーナーに提出する申請書に記入する	コンサルティング会社が結果の提示及びフィードバックの収集を行う	コンサルティング会社が認証機関の監査人を申請者に紹介する
5	ユーロプライバシー GDPR コア基準とは何か？	GDPR に含まれる主要な義務の遵守状況を体系的に評価することを可能にする	認証機関が全てのデータ取扱いに対して適用すべき必須のチェックリストである	コンサルティング会社からの要請があった場合に各国データ保護機関によって適用される補完的チェックリストである	これにより、分野及び技術固有のデータ保護要件を評価することが可能となる
6	次の記述のうち、正しいものはどれか？	認証機関は、自らのウェブサイトに公開情報を複製できない	原則として、認証機関は認証評価手続に関する一般的な情報を公開しなければならない	原則として、申請者から提供された情報、又は、申請者とその認証に関連する全ての情報は公開情報である	コンサルティング会社は、ユーロプライバシー公式ウェブサイトの管理及び監督に責任を負う
7	ユーロプライバシー基準はどの形式で利用可能か？	パワーポイントプレゼンテーション	スウェイページ	エクセルシート	本制度オーナーは本基準を誰にも公開しない
8	次の記述のうち、正しいものはどれか？	データ保護機関は、再認証監査の結果に基づき、認証の更新に関する決定を行う	認証取得後 3 年間、申請者は、本認証制度の要件を遵守し、その遵守に関する変更又は懸念を認証機関に通知しなければならない	軽微な不遵守が特定された場合、認証は自動的に一時停止され、場合によっては取り消される	認証は、現地監査に基づくものであり、その後 5 年ごとにサーベイランス監査が行われる
9	次の記述のうち、ユーロプライバシー基準の表構造における「基準列」に当てはまるものはどれか？	各確認項目及び管理項目に固有の識別子を付与する	監査チームが、申請者によって対処されるべき問題又は要素を特定できるようにする	情報が通常どこにあるかについて、監査人に指針を示す	申請者が実施し、監査人が評価すべき正式な要件を記述する

10	認証機関は、苦情や異議申立てを受領した際、どのように対応するのが望ましいか？	申請者に対し、本認証制度又はその評判に対するリスクとなり得る重大な問題を通知する	データ保護機関に対し、苦情又は異議申立てを解決するために必要な措置を講じるよう要請する	関連する一切の情報を収集及び検証する	苦情申立人又は異議申立人に対し、正式に手続の結果を通知する
11	ユーロプライバシー準備段階において、実装者は特定されたギャップに関する報告後、どのような対応をとるのが望ましいか？	特定されたギャップの是正について顧客に助言する	報告書を本制度オーナーに転送する	データ保護機関に当該ギャップに関するセカンドオピニオンを求める	いずれの回答も正しくない
12	次の記述のうち、事前段階で用いられるチェックリストはどれか？	GDPR コア基準	申請及び評価基準	国家固有データ保護義務	文書チェックリスト
13	認証に関する情報の機密保持義務を負うのは誰か？	一般公衆	本制度オーナー	認証機関	義務ではなく推奨
14	次の記述のうち、正しいものはどれか？	セクションの確認項目及び管理措置を評価する際、データ主体は要求された確認項目及び管理項目を実施する	技術的・組織的措置チェックリストには、全てのデータ取扱いに適用される GDPR の要件がまとめられている	分野及び技術固有のデータ保護要件を評価するため、補完的文脈的確認項目及び管理項目が規定されている	不遵守一覧のテンプレートは、データ保護機関が特定された不遵守を報告及び一覧化するために使用するものである
15	ウェルカムパックの主な対象は誰か？	データ主体	データ保護機関	認証機関	申請者
16	維持期間中に適用可能なデータ保護規制が変更された場合、どうなるか？	法改正は、既に付与された認証には影響しない	認証機関は行動計画を策定し、データ保護機関の確認を受けなければならない	本制度オーナーは、既に付与された全ての認証を一時停止し、無効にしなければならない	申請者は、認証の有効性に対する影響の程度を評価しなければならない
17	以下の記述のうち、遵守マークに該当するものはどれか？	認証機関の管理及び承認の下にある	トレーサビリティを妨げる	申請者の財産である	欧州議会の決定に対する企業の同意を示す
18	苦情及び異議申立ての仕組みには何が定められているか？	EDPB を代表して本手続を担当するのは誰か	誰が苦情又は異議申立てを行うことができるか	データ保護機関が適切な是正措置を講じることを確保するための手続	本制度オーナーが認証機関に支払わなければならない追加料金
19	以下の記述のうち、正しいものはどれか？	データ主体は、認証活動に関する職務及び責任に関する文書を保持する	申請者は、認証を受けたコンサルティング会社から情報を提供されるよう、十分な契約上の取決めを確立する	原則として、付与された認証に関する記録は、関連する認証周期に 20 年を加えた期間保存される	各国データ保護機関及び本制度オーナーは、機密情報へのアクセスを要求することができる
20	以下の要素のうち、認証機関が確保しなければならないものはどれか？	文書又はその他の広報文書において、遵守マークに関する不正確な参照が見られないこと	申請者が遵守マークの使用に関するガイドラインを公表すること	データ保護機関が遵守マークの権利を行使すること	遵守マークが、評価対象の手続に関するデータ主体の見解を表していること
21	以下の記述のうち、正しいものはどれか？	ユーロプライバシー基準、並びに、補完的確認項目及び管理項目は、全ての認証手続に適用され、必須である	NOCAR は、評価対象による申請者の居住国の規制への遵守状況を評価することが求められる	本基準、確認項目及び管理項目の一覧は、ユーロプライバシーのライセンスを取得したコンサルティング会社によって管理されている	不遵守一覧チェックリストは、申請によって策定された方針及び手順が、ユーロプライバシーの要件に対応するために十分に包括的であるか否かを事前に確認することを可能にする

22	以下の記述のうち、遵守表明に含まれる要素はどれか？	全ての認証を受けた者の名称及び連絡先	認証書の更新条件	認定監査人の氏名	いずれの回答も正しくない
23	以下の記述のうち、ユーロプライバシーのウェブサイトで公開されている情報はどれか？	ユーロプライバシーオンライン認証レジストリ	認証機関及び申請者間の契約書の写し	認証に失敗した事例のオンラインライブラリ	認証を受けた申請者の連絡先
24	以下の記述のうち、サーベイランス活動に該当し**ない**ものはどれか？	サーベイランス活動は、データ主体によって全面的に支援されなければならない	原則として、2ヶ月ごとのサーベイランス活動が標準であるのが望ましい	認証機関は、申請者が本認証制度の要件を継続的に遵守しているという証明に基づき、認証を維持しなければならない	認証機関は、サーベイランス監査で検証する確認項目及び管理項目一式を選択する
25	以下の記述のうち、正しいものはどれか？	認証手続において、コンサルティング会社は、申請者が潜在的不遵守に対処及び解決するのを支援することができる	ライセンスを取得するため、コンサルティング会社は、ユーロプライバシー関連のサービスを提供する前に、関連するデータ保護機関と合意書を締結しなければならない	コンサルティング会社は、認証を受けたデータ取扱いに対する継続的支援を提供し、認証対象となり得る残りのデータ取扱いの準備支援を目的とした補足見積提案を作成する	ECCP は、申請者が最初に認証を受けるべき 2 件のデータ取扱活動を特定し、その後、評価対象を正式に特定するのを支援する

正解

問題番号	正解	説明
1	D	**モジュール 1 – 実装者の役割（スライド 3）** 認定実装者はコンサルティング会社に所属し、組織が適用可能なデータ保護規制を継続的に遵守できるよう支援する。コンサルティング会社は、申請者がデータ取扱活動について認証を取得できるよう準備を支援するだけでなく、認証手続及び維持段階においても継続的支援を行う。
2	A B	**モジュール 3 – 基準、確認項目及び管理項目の適用範囲（スライド 9）** 基準、確認項目及び管理項目は、必須、適用除外及び固有など、いくつかのカテゴリーに分類される。
3	B C	**モジュール 5 – 遵守マーク、ライセンス、認証書の使用** 本問題は、モジュール 5 のいくつかの点を問題としています。ユーロプライバシー商標の使用に関し、事前の同意を行うのは、データ保護機関ではなく、ECCP であるため、*解答 A* は誤りです。認証書は申請者ではなく、認証機関の管理及び承認の下にあるため、*解答 D* は誤りです。
4	A C	**モジュール 1 – 認証後のサービス（スライド 7）** 最終会議において、コンサルティング会社は、準備手続の結果の提示、申請者からのフィードバックの収集、及び、必要に応じて補足見積提案の提示を行います。申請書は本制度オーナーではなく、認証機関に提出されるため、*回答 B* は誤りです。監査人の紹介は最終会議の一部ではないため、*回答 D* は誤りです。
5	A B	**モジュール 4 – 評価段階（スライド 5）** GDPR コア基準は、全てのユーロプライバシー認証手続の基盤を成し、適用分野及び場所に関わらず、認証機関の監査人によって、あらゆる評価対象に適用されなければなりません。GDPR コア基準は、GDPR に含まれる主要な義務の遵守状況の体系的評価を可能にします。
6	C	**モジュール 2 – 情報管理及び機密保持** 本問題は、本モジュールの情報を要約したものです。*回答 A* について、認証機関は ECCP の承認を得ている限り、公開情報を自らのウェブサイトに複製することができます。*回答 C* について、原則として、申請者に関する一切の情報は機密情報として取り扱われなければなりません。*回答 D* について、ユーロプライバシーウェブサイトの管理は、コンサルティング会社ではなく、ECCP の責任です。
7	C	**モジュール 3 – 評価基準（スライド 3）** ユーロプライバシー基準、確認項目及び管理項目は、遵守状況の評価を容易にするため、ウェルカムパック及びユーロプライバシー・コミュニティウェブサイトを通じて、Excel ファイル、PDF ファイル及び Word テンプレートなど、様々な形式で提供されています。
8	B	**モジュール 5 – 維持、更新及び異議申立て** 本問題は、モジュールの内容を要約したものです。*回答 A* について、更新の決定を行うのは、データ保護機関ではなく、認証機関です。*回答 C* について、不遵守が特定されたとしても、自動的に認証の一時停止又は取消しに繋がるわけではありません。*回答 D* について、サーベイランス監査の頻度は年 1 回と定められており、現地及び遠隔の両方で行われます。
9	D	**モジュール 3 – 表の構造（スライド 12）** 誤った回答：*回答 A* は Ref ID の列を指し、*回答 B* は推奨の列を指し、*回答 C* は実装ガイダンスの列を指します。
10	C D	**モジュール 6 – 異議申立て及び苦情取扱い方針（スライド 8-11）** 誤った回答：

		回答 A　通知を受けるべきなのは本制度オーナーです。 *回答 B*　データ保護機関は、苦情又は不服申立ての解決の責任を負いません。
11	**A**	**モジュール 1 – ユーロプライバシー準備手続（スライド 5）** 実装者は、申請者が特定されたギャップの是正を支援することができます。実装者は、これを本制度オーナーに転送したり、セカンドオピニオンを求めたりする必要はありません。
12	**B D**	**モジュール 4 – 事前段階（スライド 4）** GDPR のコア基準（*回答 A*）及び国家固有データ保護義務（*回答 C*）は、評価段階の一環として用いられます。
13	**B C**	**モジュール 2 – 情報管理及び機密保持** 一般公衆は認証手続に関する機密保持義務の対象となる利害関係者ではないため、*解答 A* は誤りです。同様に、機密保持義務は推奨ではなく、義務であるため、*解答 D* も誤りです。
14	**C**	**モジュール 3 & モジュール 4** 本問題は、基準に関する 2 つのモジュールの情報をまとめたものです。確認項目及び管理項目を実施するのは、データ主体ではなく、監査人（及び実装者）であるため、*解答 A* は誤りです。GDPR の要件をまとめたのは、TOM チェックリストではなく、GDPR コア基準であるため、*解答 B* は誤りです。不遵守を報告するために不遵守一覧を使用できるのは、監査人（及び実装者）であるため、*解答 D* は誤りです
15	**D**	**モジュール 1 – 実装者の役割（スライド 3）** コンサルティング会社は、ユーロプライバシー・ウェルカムパックを活用し、申請者に対して包括的な支援を提供することができます。
16	**D**	**モジュール 6 – 認証に変更を及ぼす認証（スライド 6）** 法改正、各国若しくは国際的な裁判所の決定、EDPB の決定、又は、欧州委員会の決定といった適用可能なデータ保護規制の変更は、認証機関によって監視及び対応されます。これらの変更が付与された認証に影響を及ぼす場合、認証機関は、（1）認証の有効性への影響度の評価、（2）行動計画の策定、（3）関連するデータ保護機関に連絡し、提案された行動計画の確認の要請、並びに、（4）データ保護機関の同意を得た後、行動計画の実施を行います。
17	**A**	**モジュール 5 – 遵守マーク（スライド 9）** 認証を受けたデータ取扱活動には、認証機関の管理及び承認の下で、ユーロプライバシー遵守マークをラベル付けすることができます。
18	**B**	**モジュール 6 – 異議申立て及び苦情取扱い方針（スライド 9）** EDPB ではなく、認証機関に代わって行われるものであるため、*解答 A* は誤りです。データ保護機関ではなく、認証機関又は本制度オーナーによるものであるため、*解答 C* は誤りです。本制度オーナーに支払う追加料金はないため、*解答 D* は誤りです。
19	**D**	**モジュール 2 – 情報管理及び機密保持** 本問題は、本モジュールの情報を要約したものです。認証活動に関する記録の保持は、データ主体の義務ではなく、認証機関の義務であるため、*解答 A* は誤りです。認証を受けた申請者との契約上の取決めを確立するのは、認証機関であるため、*解答 B* は誤りです。記録は 10 年間保存されるため、*解答 C* は誤りです。
20	**A**	**モジュール 5 – 認証機関の管理（スライド 13）** 遵守マークの使用に関するガイドラインを公表しているのは本制度オーナーであるため、*解答 B* は誤りです。同様に、遵守マークの管理権を行使するのは認証機関であるため、*解答 C* も誤りです。遵守マークとは、

		認証手順が完了したことを示すために使用できるシール又はマークであるため、*解答 D* は誤りです。
21	**A B**	**モジュール 3 & モジュール 4** 本問題は、本基準に関する 2 つのモジュールの情報を要約したものです。一覧を管理するのは、コンサルティング会社ではなく、本制度オーナーであるため、*解答 C* は誤りです。不遵守一覧チェックリストは、申請者が認証を受けるために是正しなければならない、特定された不遵守を報告及び一覧化するためのものであるため、*解答 D* は誤りです。
22	**D**	**モジュール 5 – 遵守表明（スライド 10）** 遵守表明には以下が含まれるため、いずれの回答も正しくありません。 ・ユーロプライバシーへの参照 ・許可されている場合はユーロプライバシーロゴ ・認証を受けた申請者の名称 ・該当する場合、共同管理者の名称、 ・評価対象及びその地理的適用範囲の明確な表示 ・該当する場合、追加された補完的規範又は補完的要件の明確な表示 ・認証書の発行日及び有効期間 ・発行された認証書の固有識別子 ・「詳しくはこちら」という記載に続き、本認証制度のウェブサイト及びオンライン認証レジストリのドメイン名 ・認証書を発行する認証機関の名称及び所在地
23	**A**	**モジュール 2 – 情報管理及び機密保持** ユーロプライバシーオンライン認証レジストリは、ユーロプライバシーのウェブサイトから利用可能です。
24	**A B**	**モジュール 6 – 監視及びサーベイランス監査（スライド 5）** *解答 A* は、データ主体がサーベイランス監査のような活動を支援する必要がないため、サーベイランス監査には当てはまりません。*回答 B* は、サーベイランス監査のような活動が隔月ではなく年 1 回行われるため、サーベイランス監査には当てはまりません。
25	**A C**	**モジュール 1 – 実装者の役割** 本問題は、本モジュールの情報を要約したものです。コンサルティング会社は、ユーロプライバシー関連のサービスを提供するため、データ保護当局ではなく、ECCP と契約を締結しなければならないことから、*解答 B* は誤りです。最初の 2 件のデータ取扱活動の選択において申請者を支援するのは、ECCP ではなく、コンサルティング会社であるため、*解答 D* は誤りです。