Europrivacy.com
Privacy Audit and Certification

# ユーロプライバシー™/®
# 認証制度
# 一般仕様及び要件

| | |
|---|---|
| 識別子 | EP-CS.1 |
| バージョン | 77 更新 |
| 日付 | 2024 年 1 月 24 日／2023 年 8 月 15 日 |
| 公開状況 | 公開（ただし、知的財産権の対象。） |
| ウェブサイト | http://www.europrivacy.com |
| | www.eccpcenter.com |
| 連絡先 | contact@europrivacy.com |

 

# 目次



  

  

  

  

  

  

  

本日本語訳は、英語が母国語ではない人々がユーロプライバシー認証制度を利用しやすくするため、最善の努力を尽くして提供されたものであるが、翻訳版（日本語版）とオリジナル版（英語版）との間に乖離がある場合は、オリジナル版（英語版）が優先する。

# 1. 序文及び謝辞

情報通信技術（ICT）の進化に伴い、データ保護は個人及び社会にとって高まる懸念となっている。欧州連合（EU）及び各国は、自然人の基本権及び自由、並びに、特に個人データ保護の権利を保護するため、正式な法律及び規制を採択している。

ユーロプライバシー認証制度は、データ管理者及び処理者による個人データ取扱業務が欧州一般データ保護規則（GDPR）の義務を遵守しているか否かを評価するため、また、各国規制若しくは分野固有義務、又は、その両方などの補完的データ保護義務にも容易に拡張可能なように開発された。

ユーロプライバシー基準は、欧州データ保護会議（EDPB）によって承認され、データ管理者又は処理者が実施するデータ取扱活動に適用可能な公式の欧州データ保護シールとして機能する。

認証制度の手法及び基準を用いることにより、全ての当事者のリスクを軽減することができる。個人データの取扱いが明確な要件に基づいて厳重に監視される場合、データ主体、データ管理者及びデータ処理者のリスクは軽減される。

認証制度及びその基準は、次のとおり使用されることを前提に設計されている。

a) GDPR 第 42 条に基づく公式の欧州データ保護シールとして
b) データ輸入者による国際的なデータ移転の仕組みとして[1]
c) GDPR を遵守し、他の管轄で認められる認証方法として[2]
d) GDPR に基づく通常の認証と混同されるリスクがないことを条件に、公式の GDPR に基づく認証のメリット及び強みが認められない内部監査及び任意の認証のため
e) 必ずしも公式の認証取得を目指さなくとも、遵守状況を文書化し、コンプライアンス違反のリスクを低減するため

ユーロプライバシー認証制度は、欧州委員会及びスイス研究・教育庁が共同出資した欧州研究プロジェクトの支援を受けて開発された。最初の認証制度は Archimede Solutions SARL によって開発された。本制度オーナーの役割及び機能は、ルクセンブルクの欧州認証・プライバシーセンター（ECCP）に委任された。ECCP は、データ保護、ICT セキュリティ及び認証の国際専門家委員会（以下「ユーロプライバシー国際専門家委員会」という。）の支援を受けて、認証制度の概観、改善及び更新を担当している。

本認証制度は、主に ISO/IEC 17065 に基づく個人データ取扱いの遵守を認証することを意図している。ISO/IEC 17065 が、ISO/IEC 17021-1 のような補完的な認証の要求事項に向けて拡張可能であることを最大限に活用するように最適化されている。該当する場合、ユーロプライバシーは、適用可能な規制及び補完的要件を遵守すれば、異なる認証範囲にも適用することができる。

[1] GDPR 第 46 条に基づく国際的なデータ移転の仕組みとしてのユーロプライバシーの利用は、EDPB の承認待ちである。GDPR の適用を受けないデータ輸入者は、契約上拘束力のある十分な文書を採用しなければならない。
[2] 他の管轄における正式な承認には、補完的な要件が課される場合がある。

  

# 2. 認証制度の適用範囲及び目的

## 2.1. 本文書の適用範囲

本文書は、認証機関（以下「認証機関」という。）が適用及び尊重すべき方針、手続及び手順を含む、ユーロプライバシー認証制度（以下「本認証制度」という。）の一般仕様及び要件を提示する。本基本文書は、より詳細な情報を提供する補完的文書一式によって完成し、これらもまた本認証制度の一部である。

第 2 節から第 5 節は、定義及び参照を含む、ユーロプライバシーの一般的な概要に焦点を当てている。

第 6 節から第 11 節は、本基準を含む、認証活動に焦点を当てている。

第 12 節から第 17 節は、認証機関の組織的要件に焦点を当てている。

第 18 節及び第 19 節は、認定及びライセンスを含む、本認証制度の管理に焦点を当てている。

## 2.2. ユーロプライバシー認証の目的及び適用範囲

ユーロプライバシーは、GDPR を中心とする個人データ保護規制へのデータ取扱いの遵守に関する明確かつ包括的な認証制度を提供するために設計された。本認証制度は、データ取扱いが GDPR 及び対応するデータ主体の基本権を遵守していること、並びに、該当する場合、各国規制及び分野固有要件などの補完的要件を遵守していることについて、独立、公平かつ合理的な保障レベルを提供することを意図している。

国際法、ISO の原則及び世界貿易機関（WTO）の要件を尊重するよう設計されている。

本認証制度は、データ管理者若しくはデータ処理者、又は、その両方（以下「申請者」という。）が実施する多様なデータ取扱活動に適用できるように研究及び構成されている。本認証制度は、モノのインターネット（IoT）及び人工知能（AI）のような革新的技術の使用から生じるリスクに特別な注意を払って開発された。この構造（アーキテクチャ）は、そのコア基準を、補完的な国家固有要件及び分野固有要件で拡張することを可能にしている。

ユーロプライバシーは、中小企業にとって信頼性が高く、費用効率も高く構成されている。該当する場合、認証の負担及び費用の重複を避けるため、ISO/IEC27001 及び 27701 などの他の認証を補完及び活用する。

ユーロプライバシー認証の適用範囲には、次のいくつかの制限がある。

- 申請者は、認証されるデータ取扱活動の遵守状況を監視する担当者として、データ保護オフィサー（又は外部に委託可能な同等機能）を指名しなければならない。
- 申請者は、個人データ取扱活動の記録を保持しなければならない。
- ECCP は、通常のユーロプライバシー認証の適用範囲から除外される申請分野の一覧を保持する。特定分野に対する認証の適用性に疑義が存する場合、申請者又は認証機関は、ECCP に連絡しなければならない。

**ユーロプライバシー認証は、認証拡張（第 11.1 節参照）を活用することにより、欧州一般データ保護規則、及び、該当する場合、各国規制又は分野固有要件などのデータ保護に関する補完的要件を遵守したデータ取扱いについて、独立した公平かつ合理的な保証レベルを提供することを意図している。**

  

### 2.2.1. 認証の規範的適用範囲

ユーロプライバシー認証制度は、GDPR（具体的には次のとおり）の要件に対応するように設計されている。

- 個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、欧州議会及び理事会の規則（EU）2016/679

本認証制度は、データ主体の権利及び自由、その個人データ又は申請者を不遵守によってリスクにさらす可能性のある GDPR の義務に焦点を当てている。

GDPR 第 42 条及び第 43 条を遵守する GDPR 認証の付与には、次の遵守が必要である。

- 次を含む、適用可能な欧州データ保護会議のガイドライン
  - 一般データ保護規則（2016/679）第 43 条に基づく認証機関の認定に関するガイドライン 4/2018
  - 規則 2016/679 第 42 条及び第 43 条に基づく認証及び認証基準の特定に関するガイドライン 1/2018
  - 移転ツールとしての認証に関するガイドライン 7/2022
- EU 加盟国のデータ保護法が定める適用義務

本認証制度が GDPR の遵守に焦点を当てる一方で、申請者及び認証機関は、次のような補完的要件を追加することにより、認証の規範的適用範囲の拡張を合意できる。

- e プライバシー指令及び NIS 指令などの欧州指令並びに規則[3]
- 各国データ保護規制
- 分野固有要件又は ISO/IEC の要求事項

規範的適用範囲の拡張にかかわらず、認証は、常に通常の GDPR 要件を遵守していることも証明されなければならない。規範的適用範囲の拡張は、第 11.1 節のとおり、認証書に明記されなければならない。

本認証制度は、適用可能な場合には法学及び技術的環境の進化を含む、上記の規則のその後の進化及び更新に適応することを意図している。

### 2.2.2. 認証の実体的適用範囲

本認証制度は、データ保護コンプライアンスに関する包括的、均質的及び体系的評価を提供するために研究、開発され、具体化されている。本認証制度は、**個人データの取扱業務遂行を認証することに主たる焦点を当てている**が、データ保護に焦点を当て、製品、プロセス及びサービスを評価するために適用可能な ISO の要求事項（ISO/IEC 17065）、並びに、ISO/IEC 17021-1 と整合させることにより、可能な限り包括的になるよう設計されている。

評価対象に応じ、本制度オーナーが定める特定かつ補完的な確認項目及び管理項目は監査人によって適用されなければならない。この仕組みは、分野及び技術固有要件に対応することにより、本認証制度を多様なデータ取扱活動に適用することが可能となる。

### 2.2.3. 認証の地理的適用範囲

本認証制度の地理的適用範囲は、正式には限定されておらず、申請者が利用することができるが、次のとおりである。

a. GDPR に基づき EEA 域外に居住する申請者に付与される欧州データ保護シールは、補完的要件の対象となる[4]。
b. 法的環境が個人データ及びデータ主体の権利に十分な保護を与えていない国では、認証基準を充足することは困難であり、不可能な場合もある。

### 2.2.4. 認証範囲及び評価対象の明確化

認証の規範的適用範囲及び発行された各認証書の評価対象は、明確に定められなければならない。発行された認証書はユーロプライバシー認証レジストリ（以下「レジストリ」という。）で

[3] 欧州議会及び理事会の指令（EU）2002/58/EC 及び 2016/1148/EC
[4] 非 EEA の申請者へのユーロプライバシーの適用については、EDPB が検討中であり、決定待ちである。

  

公表され、各遵守マークに付された認証書の識別子及びウェブサイトアドレスにより、容易にアクセスし、検証できる。

## 2.3. 欧州データ保護規則との整合性

### 2.3.1. データ保護規制の進化への適応

データ保護規制の進化により、本認証制度は、データ保護関連の法的環境及び法学の進化を考慮に入れた定期的更新が期待される。また、継続的な改善手続を可能にすることも意図されている。

本制度オーナーは、国際専門家委員会の支援を受け、本認証制度の見直し及び更新を担当する。

### 2.3.2. 認証制度の要件

認証制度は、次の要素を考慮して設計されている。

a) 本認証制度は、零細企業及び中小企業が利用しやすいものでなければならない。
b) 本認証制度は、透明性のある手続で利用できる。
c) 本認証制度は、データ保護規制の義務を遵守する申請者の責任を軽減するものではないことを明確にする。
d) 本認証制度は、欧州データ保護会議若しくは所轄データ保護機関、又は、その両方によって承認された本基準を遵守する。
e) 適用可能な ISO/IEC 規格の関連要求事項に準拠している。
f) 申請者は、認証手順を実施するために必要な全ての情報及びその取扱活動へのアクセスを認証機関に提供することが期待される。
g) 認証の有効期間は最長 3 年間である。
h) 認証の更新は、申請者が当該更新のために定める条件及び要件を充足することを条件として認められる。

### 2.3.3. 認証機関の要件

認証機関は、適用可能な認定要件及び規制を遵守しなければならない。

GDPR によれば、認証機関は具体的に次のことを行うことが望ましい。

a) **データ保護に関する適切なレベルの専門知識を証明すること**
b) **独立性及び公平性を証明すること**
c) 適切な手順及び組織を含む、認証を発行するための **ISO/IEC 17065[5]の要求事項に準拠すること**
   - 認証、シール及びマークの発行、並びに、定期的レビュー及び撤回を行うこと
   - 認証を受けた組織のデータ主体及び公衆に対する透明性を管理すること
   - 認証の侵害に関する苦情、又は、認証が実施され、若しくは、現在実施されている方法に関する苦情、あるいは、その両方を取り扱うこと
d) 次のような、**所轄データ保護機関が定める適用可能な認定要件を遵守すること**
   - 個人データの取扱時、データ保護のための十分な手続を証明すること
   - 所轄データ保護機関又は認定機関により認定されていること

認証機関に代わって認証活動の一部を実施する試験所及び監査人などの外部機関は、データ保護に関する十分な専門知識、及び、その作業に関連する本認証制度に関する適切な知識を証明しなければならない。

各国データ保護機関及び欧州データ保護機関は、適用可能な規制、本認証制度要件を遵守し、かつ、本制度オーナーの同意を得て本認証制度を利用する場合、公式のライセンスを必要としない。

[5] ISO/IEC 17065/2012 又はそれ以降（最新版が入手可能）。

  

## 2.4. 継続的改善手続

実効的なデータ保護を確保するためには、規範（法学、EDPB の出版物など）、技術環境（例えば、データの非匿名化リスクに影響する可能性があるもの）の進展、及び、プラクティスを通じて得られた教訓を考慮する必要がある。

本認証制度、並びに、本基準、確認項目及び管理項目を含む関連リソースは、これらの変更に対応し、本認証制度要件及び法的要件との間の隔たりの発生を回避するための継続的改善手続を通じて、必要に応じて見直し及び更新を行うことができる。

また、本制度オーナーに改善提案を提出するよう招へいされた監査人及び技術専門家の経験も活用される。提出された改善提案は、本制度オーナーの国際専門家委員会によって審査され、承認された改善案は更新版として公開される。いかなる適応も、認証手続の適用性及び信頼性の向上に寄与するものでなければならず、認証手続を弱めるものであってはならない。

次の図面は、当該手続を要約したものである。

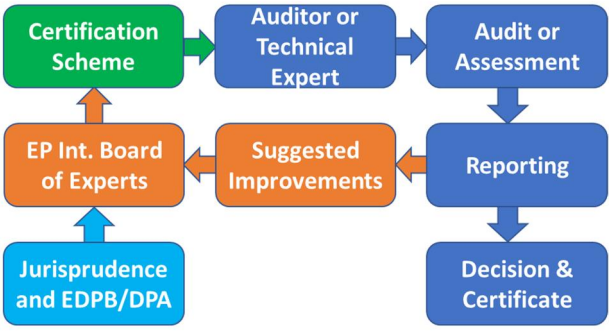


*図 1 ユーロプライバシー認証制度の継続的改善手続*

  

## 2.5. 認証の内在的制約

### 2.5.1. 一般的制約

ユーロプライバシー認証書は認証手続の最終的な成果物であり、参照された本認証制度の要件及び手順に従って認証が実施されたこと、認証を受けた評価対象が、評価若しくは監査手続、又は、その両方において、当該評価対象のための本認証制度の特定の要件を適切に充足すること、並びに、申請者が、認証書の有効期間、これらを遵守することを約したことを示す。

認証手続は、明確に定められた体系的手法に従った後、監査人が特定した所見に基づくものである。認証手続は、分析されたサンプル若しくは一定期間に実施された対象監査、又は、その両方に依拠する。認証書は、独立した第三者によって検証された専門的かつ公平な遵守状況の表示であるが、認証を受けた評価対象に不遵守がないこと、及び、将来もないことを保証するものではない。法的遵守は、認証を受けた評価対象が本認証制度の要件及び適用可能なデータ保護規制を完全に遵守していることを継続的に確保しなければならない申請者の単独の責任である。

認証は、製品、プロセス、サービス及びマネジメントシステムの使用を推奨するものでも、悪用可能な脆弱性が全くないことを保証するものでもない。

念のため、次の事項について付言する。

1) 本制度オーナーの基本的な役割は、本認証制度を維持及び更新することである。
2) 認証機関は、評価された評価対象が本認証制度の要件を遵守していることを評価、監査し、認証する決定を行う責任を負う。
3) 申請者は、その個人データ取扱いのデータ保護規制への遵守について単独で責任を負う。

認証機関及び本制度オーナーは、認証を受けた製品、プロセス、サービス又は認証の対象となるその他の要素を使用した結果生じる、いかなる種類の損失又は損害に対しても責任を負わない。

ユーロプライバシー認証書は、適用可能なデータ保護規制の不遵守を含む、当該認証書保有者の法的責任を免除するものではない。

本認証制度の利用は、ユーロプライバシーのウェブサイト（https://europrivacy.com）でオンライン公開されているユーロプライバシーの一般利用規約に同意することを条件とする。

### 2.5.2. GDPR 固有の制約

GDPR 第 42 条及び第 43 条に基づき付与される認証は、欧州データ保護会議の方針、運用指針、及び、次のような要件を遵守しなければならない。

- 認証範囲を個人データ取扱いに焦点を合わせることを義務付ける。

### 2.5.3. 認証制度及び基準の無秩序な利用に対する制限

**ユーロプライバシーは、GDPR の要件及び適用可能な各国データ保護規制を遵守しているという認証を付与することを目的としている。本基準は、GDPR 認証との混同のリスクを防止することを条件に、GDPR の適用範囲外の認証を付与するための基準として利用することができる。例えば、発行される認証書は、異なる名称及び遵守マークを使用しなければならない。このような認証は、本制度オーナーが別の文書で定める補完的規則を遵守しなければならない。また、適用法及び知的財産権を遵守しなければならない。GDPR 外で付与された認証は、GDPR 認証として認められない。**

  

# 3. 引用文書

## 3.1. 引用規範及び引用規格

本認証制度は、ISO 規格及びデータ保護規制などの外部引用文書、並びに、本認証制度を補完及び詳述する内部引用文書を含む、複数の文書を参照している。

### 3.1.1. ユーロプライバシー補完的規範文書

本認証制度は、ECCP 及びその国際専門家委員会が管理する、次を含む複数の文書によって補完されている。

a) ユーロプライバシー一般利用規約
b) ユーロプライバシー認証の適用範囲制約
c) 本基準、確認項目及び管理項目の使用に関するユーロプライバシーガイドライン
d) ユーロプライバシー認証のために監査人が使用する本基準、確認項目及び管理項目の一覧
e) ユーロプライバシー認証制度の拡張及び適応（任意）
f) ユーロプライバシー認証に関与する要員の力量管理
g) 認証書、ロゴ及び遵守マークの使用に関するユーロプライバシー規則及びガイドライン
h) ユーロプライバシー情報発信及びマーケティングに関する規則

規範文書は、運用指針及びテンプレートを含む、多くの情報提供文書によって補完される。ユーロプライバシーの正式かつ公式の資料は全て最新の状態に維持され、ユーロプライバシー・コミュニティ＆リソースのウェブサイトで利用できる。

### 3.1.2. 主な外部引用規範

該当する場合、認証機関は、本認証制度及び認証手続を適用する際、次の引用規範を利用しなければならない。

- 欧州一般データ保護規則（GDPR）としても知られる欧州議会及び理事会の規則（EU）2016/679
- 一般データ保護規則（2016/679）第 43 条に基づく認証機関の認定に関するガイドライン 4/2018
- 規則（2016/679）第 42 条及び第 43 条に基づく認証及び認証基準の特定に関するガイドライン 1/2018
- 移転ツールとしての認証に関するガイドライン 7/2022
- ISO/IEC 17065「適合性評価－製品、プロセス及びサービスの認証を行う機関に対する要求事項」（、並びに、該当する場合、その各国追補版）
- ISO/IEC 17021-1「適合性評価－マネジメントシステムの審査及び認証を行う機関に対する要求事項」
- ISO/IEC 17030「適合性評価－第三者適合マークに対する一般要求事項」
- 評価対象に適用可能なデータ保護に関する補完的各国法
- 各国の認定手順で要求される場合、製品のマーケティングと関連する認定及び市場調査の要件を定めた欧州議会及び理事会の欧州規則（EC）765/2008

認証範囲に含まれる場合、次のような補完的規範を参照することができる。

- 各国規制
- 欧州指令及び規則
- ISO/IEC 27001 又は 27701 などの ISO 規格
- 分野固有の規範、規格及び要件

認証機関は、評価手続において、常にこれらの規範の最新版を考慮しなければならない。

  

## 3.2. 引用文書に関する規則及び原則

### 3.2.1. 適用バージョン

別段の定めがない限り、文書への全ての引用は、その最新版を暗黙的に指すものと解釈されなければならない。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が特定されている場合には、当該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代わるとみなされるのが望ましい。

認証及び監査手続では、評価手続開始時点で入手可能な最新版の本認証制度及び関連文書を利用しなければならない。評価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、可能な限りこれを遵守するのが望ましいが、進行中の評価手続を開始した時点の公式版に基づき完了させることは許容される。

### 3.2.2. 拡散及びコントロール

本認証制度固有の規範文書及び情報提供文書は、国際専門家委員会の支援を受けた本制度オーナーの管理下に置かれる。本制度オーナーは、許可された認証機関及び第三者が関連文書を電子形式で利用可能な状態にする。

外部引用文書は独立して管理されており、対応する外部ソースウェブサイトからアクセスされるのが望ましい。

認証機関及びその監査人は、適切なバージョンの文書を使用していることを確認及び確保する責任を負う。

### 3.2.3. 参照言語

本認証制度は、データ保護分野の国際的専門家によって開発され、見直されている。その参照言語は英語である。全ての制度文書は、他の言語に翻訳されることがある。本制度オーナーによって承認された翻訳文書は、公式版として利用してもよい。ただし、解釈の齟齬が生じた場合、英語版を正文とする。

  

# 4. 用語及び定義

本認証制度制及び本認証制度に関連する全ての文書では、次の表現を用いる。

「～しなければならない」、「～されなければならない」及び「～してはならない」（"shall" 及び"must"）は、要件（要求事項）を示す。

「～が望ましい」（"should"）は、推奨事項を示す。

「～してもよい」（"may"）は、許可を示す。

「～できる」及び「～してもよい」（"**can**"及び"**could**"）は、可能性又は能力を示す。

（ISO/IEC 17065:2012 より引用）。

## 4.1. 特定の用語の定義及び文脈上の使用

本認証制度において、本書における特定の用語は、次の定義に従って解釈されなければならない。

「**適応**」とは、特定の評価対象に対応するために、個別文書に定められた本認証制度の補完的規則及び手順をいう。

「**申請者**」とは、認証を申請し又は認証手続に参加する認証機関の顧客をいう。申請者は、ISO 規格における「顧客」の概念を包含すると解釈することができる。申請者は、評価対象のデータ管理者又はデータ処理者でなければならない。

「**被監査対象**」とは、監査チームを受け入れる申請者の組織の部門をいう。

「**データ保護マネジメントシステム（DPMS）**」とは、ビジネスリスクアプローチに基づき、適用可能なデータ保護規制を遵守するデータ保護の確立、実装、運用、監視、レビュー、維持及び改善のために使用される全体的マネジメントシステムの一部をいう。これは、*「組織の構造、方針、計画作成活動、責任、実践、手順、手続及び経営資源」*（出典：ISO/IEC 27000）を含む、申請者が取り扱う個人データを保護するために設定した資源の枠組みを包含する。

「**データ保護規制**」とは、欧州規制及び補完的に適用可能な各国規制の両方をいう。

「**調査**」とは、本基準で定められた要件の充足性の検証及び判断のため、データ取扱いが実施又は管理される施設を訪問若しくは遠隔評価すること、又は、対象物若しくはシステムを直接的に観察することをいう。これには、目視による観察及びデータ取扱いに関与する利害関係者への質問も含まれ得る。

「**拡張**」とは、他の各国データ保護規制、又は、他の欧州規則若しくは指令など、補完的規制の遵守状況を評価するために定められた一切の補完的基準をいう。

「**検査**」とは、現在の本認証制度で用いられる場合には、上記に定義される「調査」をいう。

「**規範的適用範囲**」とは、評価及び認証実施の対象となる法的及び規範的義務をいう。

「**評価対象**」とは、認証手続において評価され、認証を受けるデータ取扱いをいう。評価対象は明確に特定され、最終的な認証はデータ主体に明確に通知され、かつ、容易に理解可能なものでなければならない。

「**試験**」とは、基準に定める要件を有効に充足しているかの検証及び判断のためのデータ取扱い又は手順の実施をいう。原則として、試験は現地で実施されるが、該当する場合、遠隔地又は試験所での実施が可能である。

  

## 4.2. 一般的定義

別段の定めがない限り、本認証制度で使用される用語は、GDPR、欧州データ保護会議（EDPB）のガイドライン及び ISO などのその他の関連規範リソースが定める適用可能な定義に従い解釈されなければならない。解釈に矛盾が生じた場合は、EDPB の定義が他の定義に優先するものとする。

次の一覧において、本文書に関連する最も重要な用語及び定義を示す。

**認定：** *「遵守状況評価機関が、特定の遵守状況評価活動を実施するため、調和された規格で定める要求事項、及び、該当する場合、関連する分野別制度が定める要件を含む追加の要件を充足していることの国家認定機関による証明」*（出典：EDPB ガイドライン 4/2018）

**匿名情報：** *「識別された自然人若しくは識別可能な自然人に関する情報、又は、データ主体を識別できないように匿名化された個人データ」*（出典：GDPR 前文第 26 項）。

**認証書：** *「法令遵守の表明」*（出典：EDPB ガイドライン 1/2018）。

**認証：** *「認証基準の充足を証する評価及び公平な第三者機関の証明」*（出典：EDPB ガイドライン 4/2018）。

**認証機関：** *「認証方法を運営する第三者遵守状況評価機関」*（出典：EDPB ガイドライン 4/2018）。

**認証制度：** *「特定の製品、プロセス及びサービスに関連する認証制度であって、同一の特定の要件、規則及び手順が適用されるもの」*（出典：EDPB ガイドライン 4/2018）。

**確認項目及び管理項目：**評価対象が評価されるための具体的な要件

**同意：** *「自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するもの」*を意味する（出典：GDPR 第 4 条）。同意は「*データ主体が、自己のデータが使用される方法について十分かつ明確に説明を受けた上で、データ取扱いに自由に同意している*」ことを要求する（出典：GDPR 第 13 条及び第 14 条）。

**基準又は認証基準：** *「認証（遵守状況評価）が実施される基準」*（出典：EDPB ガイドライン 4/2018）。ユーロプライバシーは、補完的確認項目及び管理項目により、正式なコア基準を補完している。

**越境取扱い：次のいずれかをいう。**

A) 管理者又は取扱者が複数の国に拠点がある場合、管理者又は処理者の複数の国の拠点の活動の過程における個人データの取扱い。

B) EU 域内の管理者又は取扱者の単一の拠点の活動の過程における個人データの取扱いであって、複数の加盟国のデータ主体に実質的に影響を及ぼすか、又は、及ぼすおそれのあるもの（出典：GDPR 第 4 条）。

**データ侵害：** *「偶発的又は違法な、破壊、喪失、改変、無権限の開示又は無権限のアクセスを導くような、送信され、記録保存され、又は、その他の取扱いが行われる個人データの安全性に対する侵害」*（出典：GDPR 第 34 条）。

**データ管理者：** *「自然人又は法人、公的機関、部局若しくはその他の組織であって、単独で又は他の者と共同で、個人データの取扱いの目的及び方法を決定する者」*（出典：GDPR 第 4 条）。

**データ輸出者**：データ管理者又は処理者が、同じデータ保護規制の適用を受けない他国に所在する別のデータ管理者又は処理者にデータを移転することをいう。

**データ輸入者：**データ管理者又は処理者が、同じデータ保護規制の適用を受けない他国に所在する別のデータ管理者又は処理者からデータを取得することをいう。

**データ最小化：** *「データ主体が要求した機能を実行するために厳密に必要なデータのみを収集するデータ管理者の義務。換言すれば、収集されるデータは、不必要かつ潜在的に違法なデータ取扱いを防止するため、当該個人データが取扱われる目的との関係において、十分かつ関連性があり、過剰であってはならない」*（出典：GDPR 第 5 条 1 項（c））。

  

**データポータビリティ**：データ主体が、他の使用又は他のサービスプロバイダーに対し、自身の個人データを取得及び移転する権利。GDPR では*「データ主体が、管理者に対して提供した自己に関係する個人データを、構造化され、一般的に利用され機械可読性のある形式で受け取る権利、及び、技術的に可能な場合、その個人データの提供を受けた管理者から妨げられることなく、別の管理者に対し、それらのデータを移行する権利」*と定義されている。*ポータビリティの権利は、取扱いが自動化された手段によって行われる場合で、かつ、a)データ主体の同意に基づく場合、b)データ主体が当事者である契約に基づく場合、又は、c)契約締結前にデータ主体の要求に応じて措置を講じる必要がある場合にのみ適用される」*（出典：GDPR 第 20 条）。

**データ処理者：規則（EU）**45/2001 の第 2 条（e）によれば、データ処理者とは、*「管理者の代わりに個人データを取扱う自然人若しくは法人、公的機関、部局又はその他の組織」*をいう。したがって、重要な要素は、取扱者が「*管理者の代わりに*」及び管理者の指示の下でのみ行動することである。GDPR 第 28 条によれば、「処理者は、管理者から事前に個別的又は一般的な書面による承認を得ないで、別の処理者を業務に従事させてはならない。一般的な書面による承認の場合、処理者は、管理者に対し、別の処理者の追加又は交代に関する変更の予定を通知し、それによって、管理者に、そのような変更に対して異議を述べる機会を与えなければならない。」としていることに留意が必要である。

**データ取扱い：***「自動的な手段によるか否かを問わず、収集、記録、編集、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとすること、整列若しくは結合、遮断、消去若しくは破壊のような、個人データに実施される業務遂行又は一群の業務遂行」*（出典：GDPR 第 4 条 2 項）。

**データ保護機関（DPA）**：データ保護規制の適用及びデータ主体の権利保護の監視を担当する独立した公的機関。EEA では、データ保護機関は「監督機関」と呼ばれる。

**データ保護オフィサー（DPO）**：データ保護に関する専門家であり、組織が GDPR に定められている方針及び手順を遵守していることを確保するために独立して作業する者（出典：EDPS 用語集）。データ保護オフィサーは、データ保護の問題に関する管理者（又は処理者）への通知及び助言、GDPR の遵守状況の監視、データ取扱業務に関与する職員の意識向上及び教育・訓練、データ保護機関との協力などの責任がある人物である（出典：GDPR 第 39 条）。

**データ保持：**データ保持とは、管理者又は処理者が特定の目的のために個人データを保持することをいう。

**データ主体：***「当該データに関する識別された自然人又は又は識別可能な自然人」*（出典：GDPR 第 4 条 1 項）。

**データ移転：**データ移転とは、あらゆる手段による取得者へのデータの送信又は通信を意味する。

**高いリスクのデータ取扱い：**特別な種類の個人データもしくは有罪判決に関するデータの取扱い、又は、特に未成年者の個人データを対象とすることにより、自然人の権利及び自由にとってより高いリスクとなり、又は、自然人の権利及び自由にとって高いリスクとなる可能性が高い性質を有するデータ取扱活動。

**遵守マーク（又は遵守シール）：***「シール又はマークは、認証手順が完了したことを示すために使用できる。シール又はマークは、一般に、（認証書に加え、）認証の評価対象が認証手順において独立に評価され、規則、規格又は技術仕様書などの規範文書に定められている特定の要件を遵守していることを示すロゴ又は記号を示す」*（出典：EDPB ガイドライン 1/2018)。

**仕組み：***「制御及び管理タスクを実行するソフトウェア要素」*（出典：ISO/IEC 12087-1）。

**個人データ：***「識別された自然人又は識別可能な自然人（「データ主体」）に関する情報を意味する。識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、*

  

*文化的又は社会的な同一性を示す一つ又は複数の要素を参照することによって、直接的又は間接的に、識別されうる者。」*（出典：GDPR 第 4 条）。

**個人データの漏えい：***「偶発的又は違法な、破壊、喪失、改変、無権限の開示又は無権限のアクセスを導くような、送信され、記録保存され、又は、その他の取扱いが行われる個人データの安全性に対する侵害。」*（出典：GDPR 第 4 条）。

**プライバシー：**プライバシーとは、個人が公の視線から離れ、自身に関する情報を管理できる、個人の能力のことである。プライバシーの権利は、世界人権宣言（第 12 条）、欧州基本権憲章（第 7 条）及び欧州人権条約（第 8 条）に明記されている(出典：EDPS 用語集）。プライバシーの概念は、個人データ保護の概念と共通する部分はあるが一致はしない。データ保護の概念は、公開されている個人データを含む全ての個人データを意味するため、適用範囲が異なる。また、個人データ保護はデータ主体の一連の権利を意味する。

**プライバシーリスク**：プライバシーに対する不確実性の影響。GDPR の文脈では、プライバシーリスクは、主に個人データの保護、並びに、データ主体の権利及び自由への潜在的影響に関連する。

**手順：***「活動又は手続を実施するための特定の方法」*（出典：ISO 30000）。

**仮名化**：*「分離して保管されており、かつ、その個人データが識別された自然人又は識別可能な自然人に属することを示さないことを確保するための技術上及び組織上の措置の下にある追加的な情報の利用なしには、その個人データが特定のデータ主体に属することを示すことができないようにする態様で行われる個人データの取扱い」*（出典：GDPR 第 4 条）。仮名化は、データ最小化において、例えば、個人データを取り扱う際、データ主体の識別を制限し、正当な必要性のある者のみがアクセスできるようにするために役立つ。

**目的：**個人データを取り扱う目的をいう。

**取得者***「第三者であるか否かを問わず、個人データの開示を受ける自然人若しくは法人、公的機関、部局又はその他の組織をいう。ただし、EU 法又は加盟国の国内法に従って特別の調査の枠組み内で個人データを取得できる公的機関は、取得者とはみなされてはならない。公的機関によるそのデータの取扱いは、その取扱いの目的に従い、適用可能なデータ保護規則を遵守しなければならない。」*（出典：GDPR 第 4 条）。

**保持期間：***「管理者又は処理者によって個人データが記録保存される期間。「記録保存の制限」の原則に従い、個人データは、当該個人データが取扱われる目的のために必要な期間だけ、データ主体の識別を許容する方式が維持され得る。データ主体の権利及び自由の安全性を確保するために本規則によって求められる適切な技術上及び組織上の措置の実装の下で、第 89 条第 1 項に従い、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のみのために取扱われる個人データである限り、その個人データをより長い期間記録保存できる」*(出典：GDPR 第 5 条）。

**制度オーナー**：*「遵守状況評価の基準となる認証基準及び要件を設定した特定可能な組織」*（（出典：EDPB ガイドライン 4/2018）。

**特別な種類のデータ***「特別な種類のデータとは、特に機微性が高く、より高い水準の保護を必要とする個人データである。これには、人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータが含まれる」*（出典：GDPR 第 9 条）。

  

# 5. 認証の一般原則及びガイドライン

## 5.1. 認証の目的

本認証制度は、認証を受けた評価対象が本認証制度の要件、並びに、より一般的には GDPR 及び適用可能な補完的各国データ保護規制を遵守しているという**信頼を全ての関係者に提供することを目的とする**。その結果、認証機関は、公平性、力量（データ保護の専門性を含む）、責任、透明性、守秘義務、苦情及び異議申立てへの対応、並びに、リスクベースアプローチという強固な原則を通じて、その手続に対する信頼を維持することを目指さなければならない。

## 5.2. 基本理念及び基本原則

### 5.2.1. 信頼性及び信用の構築

監査人は、ユーロプライバシーが、評価対象が適用可能な要件を遵守しているという信頼性及び信用を構築するために設計されていることを常に念頭に置かなければならない。

### 5.2.2. 誠実性

認証手続に関与する認証機関の監査人及び要員は、誠実性、勤勉性及び責任をもって業務を遂行するのが望ましい。当該監査人らは、専門性及び公平性をもって本認証制度の要件を適用するのが望ましい。

### 5.2.3. 独立性

監査人は、可能な限り監査対象の活動から独立しているのが望ましく、いかなる場合も偏見及び利益相反のないよう行動するのが望ましい。

### 5.2.4. 公平性

認証機関は、その認証手続において公平性を確保し、全ての活動において公正かつ偏りのない立場を保持しなければならない。認証機関の決定は、遵守（又は不遵守）の客観的証拠に基づいて行われ、その決定が他の利益又は第三者の影響を受けないことを確保しなければならない（詳細は第 13 節参照）。

### 5.2.5. 証拠に基づくアプローチ

監査の所見及び結論は、監査基準に関連する証拠に基づくのが望ましい。証拠は記録され、検証可能であるのが望ましい。

### 5.2.6. 公正提示

監査の所見、結論及び報告書は、監査活動を事実に基づき正確に反映するのが望ましい。これらの伝達は、事実性、正確性、客観性、適時性、明確性及び完全性を備えるのが望ましい。

### 5.2.7. 機密保持

認証機関及び本制度オーナーは、認証手続に関連して取得した情報の機密性を保護するための手順を採用し、効果的な方針を実施しなければならない。監査人及び認証機関の全職員は、収集した情報の機密性を保護しなければならない。

認証機関若しくは本制度オーナー、又は、その両方が、申請者と共有する文書又は情報は、かかる文書又は情報の公開が明示的に意図されている場合を除き、申請者の機密情報として保護され、取り扱われなければならない（詳細は第 15 節参照）。

### 5.2.8. 透明性

認証機関は、その認証手続及び手順に関する明確な情報を十分に一般公開することにより、ISO の原則である透明性を遵守しなければならない。

ただし、認証機関は、申請者関連情報及び機密情報として共有される文書などの機密情報の保持及び保護に常に努めなければならない。

  

### 5.2.9. 非差別条件

認証機関の方針及び手順は、非差別的でなければならない。認証機関は、その業務遂行の範囲内の活動に従事し、必要かつ十分な資源を有する全ての申請者に対し、そのサービスを提供しなければならない。

申請者の受入れ又は拒否の判断は、本認証制度の定めに基づくものでなければならない。認証機関は、客観的かつ比例的な理由が存する場合、申請者からの認証のための申請の受入れ又は契約の維持を拒否することができる。認証機関がかかる決定に考慮できる合理的理由の例には、次が含まれる。

- 申請者が違法行為に従事している場合
- 申請者が、本認証制度又はデータ保護規制、又は、その両方の反復する不遵守歴を有する場合
- 申請者が、制御不能なデータ処理者、若しくは、個人データ保護規制及び政策が不十分な国に所在するデータ処理者、又は、その両方に過度に依存している場合
- 申請者がデータ保護に関する法的訴訟に従事している場合
- 申請者に本認証制度の評判を傷付けるおそれを構成する場合
- 申請者の遵守状況の評価及び認証が過度に複雑又は困難である場合
- 認証機関が評価対象の信頼性ある評価を提供するために必要な資源又は可用性が、不足又は欠如している場合

### 5.2.10. 先端技術への対応

ユーロプライバシーは、先端技術に関連するリスクを包含するよう、また、認証手続を支援するために最先端の技術を活用するように設計されている。

### 5.2.11. 継続的改善

ユーロプライバシー認証制度は、継続的改善手法を適用し、その恩恵を受けるように設計されている。

### 5.2.12. 基本理念及び基本原則の保護

上記各原則の維持を危うくし得る不当な影響の合理的疑いが存する場合、認証機関の執行委員会に通知されるのが望ましい。認証機関により問題が解決されない場合、不当な影響の関連証拠とともに、本制度オーナーに通知されるのが望ましい。

  

# 6. 評価基準

評価基準は、ユーロプライバシー認証制度要件の最新版を遵守して適用されなければならない。評価基準は、次のとおり、認証機関によって適用されなければならない。

**a) 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**
**b) 一貫性のある均質的方法で行われること**
**c) 検証可能かつ監査可能な方法で行われること**
**d) 次の事項を考慮すること**
- 組織の規模
- データ取扱活動の性質
- データ及びデータ主体に対する特定されたリスク

## 6.1. 主要な評価基準の概要

**認証機関は、GDPR の第 42 条及び第 43 条が定める適用可能な基準を遵守し、適用しなければならない。**

ユーロプライバシーの詳細な評価基準、確認項目及び管理項目は、評価対象の次の側面を評価することを目的としている。

a) 該当する場合、特別な種類のデータの識別を含む、**取扱われる個人データの識別**
b) 次を含む、**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
- アクセスしやすく、理解しやすいこと
- 個人データ収集の明確な目的
- データ管理者のプライバシーポリシー
- 個人データへのアクセス、訂正又は消去を要求する権利、データ取扱に対して異議を述べる権利、データ取扱いの制限を要求する権利、同意を撤回する権利、及び、データポータビリティの権利を含む、データ主体の権利
- データ管理者に関する情報、及び、該当する場合、データ処理者に関する情報

c) **取扱いの適法性**、及び、該当する場合、データ収集目的の明確な表示、又は、個人データ取扱いに関する他の法的根拠（公的機関に与えられた法的権限など）の存在を含む「事前に説明を受けた上での同意」（事前のインフォームドコンセント）要件の遵守
d) **未成年者に関する要件**の遵守
e) **デザイン及びデフォルトによる個人データ最小化の原則**の遵守
f) GDPR が定める**透明性の原則**の遵守。GDPR は、個人データの取扱いに関連するあらゆる情報及び連絡に容易にアクセスでき、理解しやすく、明確かつ平易な文言を用いることを要求している。
g) 次の点を確保した、**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**
- （十分性認定、適切な保護措置などに基づき、）個人データが第三国に移転される際、十分に保護されること
- EU 域内に拠点のない管理者又は処理者が、EU に拠点のある組織から個人データを受領する場合、適切な保護措置が講じられていること

h) **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**
i) 次を含む**データ主体の権利の効果的な実施**
- 個人データへのアクセスの権利、個人データの訂正又は消去の権利
- データ取扱いに対して異議を述べる権利、又は、データ取扱いの制限を要求する権利
- 利用者の同意を撤回する権利
- データポータビリティの権利

j) クッキー若しくは自動的なプロファイリング、又は、その両方などの**間接的なデータ収集**の存在及び**法令遵守**
k) **自動的な個人の決定**において、データ主体の権利及び自由並びに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

  

l) 次のような**収集したデータの安全性、効果的な保護及び完全性**
- バックアップソリューションの使用
- ファイアウォール及びアンチウイルスソリューションの使用
- 役割及び責任を中心に定義された（物理的又はリモートアクセスによる）データへの信頼性のあるアクセス制御の仕組みの使用
- 信頼性のある暗号化プロトコルの使用
- 信頼性のある認証（authentication）メカニズムの使用
- データ保護バイデザインアプローチの使用

m) 次を含む**データ保護のため**管理者が**適切な技術的措置及び組織的措置を**実施すること
- 明確な役割及び責任
- 次を備えた**データ保護オフィサー**（DPO）の指定
    - 十分な資格
    - 求められる行動の自律性及び方針へのアクセス
    - 行為の有効性（活動及び行動の証明）
    - 個人情報の保護に関する全ての問題への関与
- 管理者の指示がない限り、その権限下で行動する自然人がデータを取り扱わないこと
- 個人データ侵害に気づいてから不当な遅滞なく又は 72 時間以内に、（データ主体に対するリスクを発生させるおそれがない場合を除き、）**全てのデータ侵害を内部レジストリに記録し、監督機関に対し通知する手順**
- 個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合、データ主体に対し、不当な遅延なく、当該個人データ侵害を連絡する手順
- 潜在的にリスクのあるデータ取扱いなど、該当する場合、DPO とともに実施される**データ保護影響評価（DPIA）**、及び、DPIA で高いリスクが指摘された場合、データ取扱前の監督機関との協議
- 管理者（及び、該当する場合、その代理人）は、**取扱活動に関する書面による記録**を保管すること
- EU 域内に拠点のない管理者については、EU 加盟国のいずれかに拠点のある代理人を書面で指定する義務

n) **データ処理者**が用いられている場合、管理者が**データ**処理者による適切な技術的措置及び組織的措置を実施するための十分な保証の提供を確保するための次を含む手順及び契約
- データ取扱者の義務を含む全ての取扱者との書面による契約及び契約上の義務の存在
- 処理者は、取扱いの適切な安全性を確保するため、適切な技術的措置及び組織的措置を実施しなければならないこと
- 処理者は、管理者の書面による事前の許可なく、他の処理者と関与してはならないこと
- 処理者は、管理者からの指示に基づく場合を除き、個人データを取扱ってはならないこと
- 処理者（及びその代理人）は監督機関に協力しなければならないこと
- 処理者は、自己の権限の下で行動する自然人が管理者の指示に基づく場合を除きデータを取り扱わないことを確保しなければならないこと
- 取扱者は、個人データ侵害に気付いた後、不当な遅滞なく、管理者に対して通知しなければならないこと
- 処理者は、個人データが第三国に移転される際に十分に保護されるよう、GDPR 第 5 章に定める条件を遵守しなければならないこと
- 処理者は、処理者に対して特に課された GDPR の義務（上記参照）を遵守していない場合、又は、管理者の適法な指示の範囲外若しくはそれに反して行動した場合、当該不遵守の取扱いによって生じた損害について責任を負わなければならないこと

o) **合意された規範的適用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**

  

## 6.2. ユーロプライバシー基準、確認項目及び管理項目の明細一覧

上記の基準は、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、監督機関及び認可を受けた第三者は使用可能になる。

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なければならない。

**適用可能な各基準、確認項目及び管理項目は、要件遵守を評価するための十分な証拠とともに、十分に記入され、文書化されなければならない。**

### *基準、確認項目及び管理項目の適用範囲*

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る。

「申請者」の列は、基準、確認項目及び管理項目が次に適用可能かを示す。

**C** データ管理者

**P** データ処理者

**CP** データ管理者及び処理者の両方

比例原則に対応し、高いリスクのデータ取扱いと通常のデータ取扱いを区別するため、「レベル」の列では、本基準、確認項目及び管理項目を次のカテゴリーに区別している。

**A** **原則として、全ての認証手続で必須。**

**B** 単純なデータ取扱いの認証には求められていない**が、次のいずれかの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[6]

**E** **適用除外**：基準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。

もう1つの「固有／一般」の列は、本基準、確認項目及び管理項目が次に該当するかを定める。

**S** データ取扱いごとに**固有のもの**（すなわち、データ取扱いの適法性）。

**G** 複数のデータ取扱いに共通する**一般的なもの**（すなわち、DPOの十分な資格）。

さらに、コア基準の別の列には、次のとおり、GDPRの直接の対象ではないものの、国際的なデータ移転の仕組みとして認証を利用する意思のある、欧州経済領域（EEA）外に所在するデータ輸入者を認証するために必要となるコア基準の要否を定める[7]。

**R** EEA域外に所在するデータ輸入者にコア基準が**必要となることを**示す。

**NR** EEA域外に所在するデータ輸入者にはコア基準が**必要とならないこと**を示す。

本基準、確認項目及び管理項目は、「**IF**」で始まり「**THEN**」で終わる**条件条項**の対象となる場合がある。条件を充足しない場合、関連要件は適用されず、省略することができる。

各確認項目及び管理項目は、複数の条件を包含し、組み合わせてもよい。これらの要件は、その関係性の明確化のため、「AND」及び「OR」という用語で相互に関連付けられている。2つ以上の条件間で「AND」を使用する場合は、全条件を充足することを要求し、「OR」を使用する場合は、少なくとも1つの条件を充足することを要求する。

[6] 認証機関は、当該事項に関するEDPBの関連ガイドラインを考慮しなければならない。
[7] EEA域外の申請者は、EEA域内で個人データを直接収集する場合、GDPRの対象となる（GDPR第3条）。

  

### 6.2.1. コア基準、並びに、補完的確認項目及び管理項目

ユーロプライバシーは、多様なデータ取扱活動に適用可能な均質的で一貫性のある認証手続を提供できるように設計されている。コアとなる GDPR の義務以外にも、評価対象は、補完的な各国又は分野固有の規制の対象となる場合がある。その結果、ユーロプライバシーのコア基準は、申請者に適用可能な各国規制及びデータ取扱いの特殊性を考慮するため、文脈的要件によって補完される。

#### *ユーロプライバシーコア基準*

ユーロプライバシーコア基準の一覧は、全ての認証手続の基盤を成し、認証機関の監査人によって、一つひとつの評価対象に適用されなければならない。

#### *補完的要件*

ユーロプライバシーは、次の 3 つの補完的要件を考慮している。

- **各国規制**：国家固有義務遵守状況評価報告書（NOCAR）若しくは補完的国家固有基準、又は、その両方を通じて評価される。
- **安全性要件**：技術的措置及び組織的措置の確認項目及び管理項目（TOM）又は ISO/IEC27001 を通じて評価される。
- **技術及び分野固有要件**：補完的文脈的確認項目及び管理項目を通じて評価される。

これらの補完的要件の適用範囲は、国家固有要件にとっての申請者の場所、並びに、技術的要件及び分野固有の要件にとっての評価対象におけるデータ取扱いの性質といった客観的要因によって決定される。

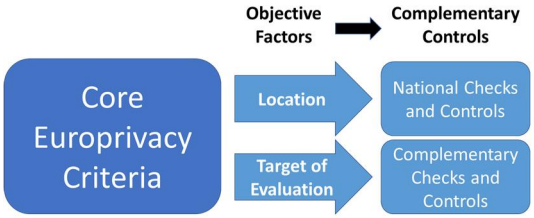


*図 2 客観的要因によって決定される補完的確認項目及び管理項目*

#### *コア要件と補完的要件の関係*

ユーロプライバシーのコア基準は、評価対象が適用可能な補完的要件の遵守状況の評価を要求している。

次の図は、本認証制度の規範的根拠及びユーロプライバシーのコア基準及び補完的要件との間の補完性を示している。

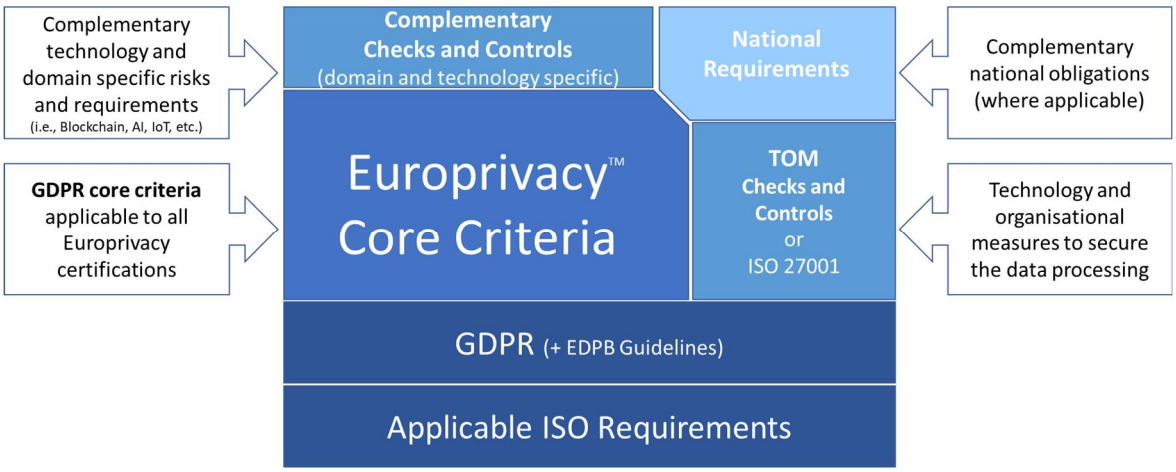


*図 3 ユーロプライバシーコア基準、並びに、補完的確認項目及び管理項目*

  

### 6.2.2. 補完的国家固有要件及び規範的要件

欧州経済地域（EEA）から申請する申請者は、適切な法的専門知識を有する専門家に、GDPR に基づく通常の義務を超える**申請国の補完的国家固有義務への評価対象の遵守状況の評価**を要請しなければならない。評価結果は、書面による報告書（***国家固有義務遵守状況評価報告書***（**NOCAR**））で報告されるのが望ましい。NOCAR が提出されない場合、認証機関は、NOCAR と同水準の要件に従い、評価対象の申請国の適用可能な国家固有義務の遵守状況の代替評価を実施できる。本制度オーナーは、特定された補完的国家固有要件の一覧を含むオンラインリソースを提供する。これらの国家固有要件の一覧は、専門家が評価を実施する際に考慮しなければならない。

ユーロプライバシー認証は、補完的 EU 規制だけでなく、補完的な EU 域外のデータ保護規制にも対応するように拡張することができる。その場合、補完的要件及び基準は、専用のユーロプライバシー認証制度「拡張」（第 11.1 節参照）を通じて定められ、提供することができる。

### 6.2.3. 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は、取り扱われ、記録保存されたデータを保護するために十分な技術的措置及び組織的措置（TOM）が実施されていることを要求する。

補完的技術的措置及び組織的措置、並びに、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定められている。これらの確認項目及び管理項目はコア基準を補完し、次の要件をいずれも充足する評価対象の場合を除いて必須である。

a) 有効な ISO/IEC 27001 認証の対象であること
b) 高いリスクのデータ取扱いを一切行わないこと

### 6.2.4. 補完的文脈的要件及び分野固有の要件

補完的文脈的確認項目及び管理項目には、特定の技術又は申請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る。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し、評価しなければならない。

### 6.2.5. 補完的確認項目及び管理項目の開発

本制度オーナーは、確認項目及び管理項目の補完的一覧、並びに、補完的一覧によって定義済みの確認項目及び管理項目を補完する仕組みを提供する。

各確認項目及び管理項目は、次のとおりでなければならない。

- 対応する法的要件の遵守状況を評価するのに**十分であること**
- 要件が効果的に評価及び証明されることを確保することにより、**監査可能であること**
- 評価の主観性を最小化するため、検証可能な事実及び証拠に焦点を当てることにより、**客観的かつ事実に基づいていること**
- 曖昧さ又は解釈の余地が生じないようにするため、**明確な表現であること**
- 多様なデータ取扱活動及びデータ管理者に同一の関連性をもって適用されるよう努めることにより、**均質的に適用可能であること**
- 不必要な作業負荷をかけることなく、信頼性の高い遵守状況の評価を提供できるよう**効率的であること**
- 申請者自身、認証機関及び第二者又は第三者が利用できるようにすることにより、（ISO が定義する）**当事者中立性を確保すること**

### *新しい確認項目及び管理項目を定めるための手続及び要件*

補完的確認項目及び管理項目を作成するために、認証機関は、次の事項を行わなければならない。

1. これらの要件を評価するために、確認項目及び管理項目の十分な補完的一覧が使用可能か否かを、まず本制度オーナーの文書リポジトリで確認する。
2. これらの補完的規範的要件が既存の確認項目及び管理項目で十分にその対象とならない場合、認証機関は、（A）補完的要件を規範的適用範囲から除外するか、又は（B）補完的要件を特定及び抽出するために、かかる追加的規範を分析可能である。
3. B の場合、本制度オーナーが提供するテンプレートに、関連する要件を一覧化し、対応する確認項目及び管理項目を定めなければならない。
4. 補完的確認項目及び管理項目の新しい一覧を本制度オーナーに送付しなければならない。
5. 評価の実施に際しては、確認項目及び管理項目の一覧を評価対象に適用しなければならない。
6. 補完的評価の結果は、最終的な遵守状況評価の該当項目で報告しなければならない。

当該テンプレートは、欧州又は各国データ保護機関が、補完的要件並びに確認項目及び管理項目を本制度オーナーに連絡する際にも使用できる。

本制度オーナーは、一貫性を確保するため、これらの追加的確認項目及び管理項目を収集、レビュー、及び、他の認証機関との共有を担当する。

## 6.2.6. 基準、確認項目及び管理項目の一覧

必要的基準、確認項目及び管理項目は、次のとおりである。

- *「A - 申請及び評価対象－事前確認項目及び管理項目」*申請及び評価対象の十分性を確認するためのもの。
- *「G - GDPR コア基準」*コアとなるデータ保護要件の遵守状況を評価するためのもの。
- *「C - 補完的文脈的確認項目及び管理項目」*分野固有及び技術固有の補完的要件の遵守状況を評価するためのもの。
- *「T - 技術的措置及び組織的措置の確認項目及び管理事項」*取扱われたデータを保護するための措置を評価するためのもの（評価対象に高いリスクのデータ取扱いが含まれない場合は、ISO/IEC 27001 認証で代用可能）。
- *「S-補完的サーベイランス確認項目及び管理項目」*サーベイランス監査及び再認証で使用するためのもの。

確認項目及び管理項目が評価対象に関連し、かつ、適用可能である場合、当該確認項目及び管理項目を適用しなければならない。確認項目及び管理項目の除外は、正当な理由が示されなければならない。

**附属書 1 は、GDPR 第 42 条及び第 43 条に基づく認証を付与するため、申請者の場所及び活動に応じて適用可能な基準を総合的に示している。GDPR 第 42 条及び第 43 条に基づく認証を付与するための申請者の所在地及び活動に応じて、適用可能な基準の総合的視点を提供する。**

該当する場合、認証機関は、評価対象の適用可能なデータ保護規制の遵守状況をより適切に評価できる限り、補完的確認項目及び管理項目を考慮することができる。

ユーロプライバシーは、認証手続を容易にし、改善するため、次のような補完的情報提供文書及びチェックリストによって支援されている。

- *「D - ユーロプライバシー認証のための文書チェックリスト」*文書の準備及びレビューを容易にするためのもの。
- *「N - 国家固有データ保護義務」*国家固有データ保護義務遵守状況評価報告書（NOCAR）の作成を支援するため、国家ごとに主要な補完的データ保護要件を列挙したプロファイル。
- *「P-方針チェックリスト」*補完的チェックリストで、実施されている方針及び手順が完全か否かを確認するためのもの。

  

- テンプレート（DPO 声明書、NOCAR、取扱われるデータ目録、データ処理者、データ保管場所など）。

  

# 7. データ取扱認証の標準手続

ユーロプライバシー認証は任意であり、認証機関の役割は、認証手続を通じて、認証対象のデータ取扱いが認証要件を充足しているか否かを確認することである。

認証を申請する前に、申請者は、適用可能なデータ保護規制を遵守したデータ取扱活動を行うのが望ましい。申請者は、手続前に、データ保護規制、ユーロプライバシー基準及び要件へのデータ取扱いの遵守を文書化することが推奨される。自己評価ツール及び認定コンサルティング会社の利用は、認証手続の迅速化に貢献する。ECCP は、申請者、法律事務所及びコンサルティング会社に対し、ユーロプライバシー認証の準備のための多くのリソースを提供している。

データ取扱いの認証のための標準手続は、ISO/IEC 17065 のモデル及び要求事項に基づいている。評価手続は評価対象に焦点を当てている。

認証は最長 3 年間付与される。再認証は、監視活動の結果に応じて付与される場合がある。

データ取扱いの認証のための標準手続には、次の段階が含まれる。


*図 4 標準認証手続*

  

## 7.1. 適応可能な手続モデル

### 7.1.1. 適応可能な手続モデルの概要

ユーロプライバシー認証制度の主たる焦点は個人データ取扱いの評価にある一方で、可能な限り包括的に設計されている。本制度は、データ保護マネジメントシステムなど、専用の適応（第11節参照）が規定する追加要件及び認定手順の対象となる様々な範囲に適応可能である。

**本認証制度は多種多様なデータ取扱活動に適用可能であるが、GDPR 第 42 条及び第 43 条に基づく認証への適用は、欧州データ保護委員会が定める関連する方針、指示及び制限を厳格に遵守しなければならない。**

### 7.1.2. 複合申請

ユーロプライバシー認証制度は、拡張（第 11 節参照）に定められているデータ保護における補完的義務を包含するよう拡張することができる。このような場合、認証手続は、二重認証又は複合認証ではなく、単一の認証手続としてみなされるのが望ましい。

### 7.1.3. 申請者及び適用範囲

認証手続は、データ管理者又はデータ処理者として行動する公的組織及び私的組織に公開されてる。GDPR 第 42 条及び第 43 条に基づき、本認証は、データ管理者及びデータ処理者による個人データの取扱業務にのみ適用され、欧州データ保護会議の定める制限を受ける場合がある。

## 7.2. 事前認証活動

### 7.2.1. 申請手続

申請手続は、認証の評価対象を決定するために必要となる情報を収集し、適切に文書化されなければならない。

申請者は、認証の評価対象となるデータ取扱いのデータ管理者又はデータ処理者でなければならない。

原則として、申請者は、その権限を有する代表者が署名した申請書に記入し、提出するのが望ましい。あるいは、申請者は、その権限を有する代表者と認証機関との対面での会議による申請も可能である。

申請手続では、次の情報を収集及び文書化しなければならない。

a) 申請者に関する情報（法的名称、所在地、ウェブサイト及び活動分野を含む）
b) データ取扱活動の記述
c) 希望する認証の規範的適用範囲及び評価対象
d) 該当する場合、データ保護に関して評価対象に適用可能な国家固有又は分野固有の補完的規制に関する情報
e) 権限を有する連絡担当者
f) 評価対象に対してコンサルティングが提供されたか否か、及び、提供された場合はその提供者

**加えて、EDPB の運用指針の要請に従い、評価対象は、申請段階において、次の内容を含め、詳述しなければならない。**

- **他のシステム及び組織とのインターフェイス及び移転**
- **使用されるプロトコル及びその他の関連する保証**
- **関与するデータ処理者の職務及び責任の特定**

**認証機関及び申請者が適切な機密保持契約条項の対象となっている場合、その申請は、自身及びそのデータ処理者との間の関連契約条項の写しを添付して完了されなければならない。**

申請者から提供された情報に加え、認証機関は、出典を文書に明記して、申請に追加する補足情報を収集してもよい。

  

### 7.2.2. 申請者の暫定的コミットメント

申請書に署名することにより、申請者は、本認証制度に添付されたユーロプライバシー一般利用規約を遵守することに同意しなければならない。また、監査人に対し、必要な情報、支援及び必要となるアクセスを提供することにより、認証手続を尊重し、容易にすることを誓約しなければならない。

### 7.2.3. 評価対象の明確化及び特定

評価対象は、慎重に特定され、確認されなければならない。申請者及び認証機関は、次の事項を行わなければならない。

a) 次の事項によって**評価対象を特定**すること
   a. **明確な表題（タイトル）を付けること**
   b. **データ取扱いを記述する**こと
   c. 外部データ取扱いとの個人データの流れ（データフロー）の特定を含む、**個人データの流れ（データフロー）を図又は図面で可視化すること**
   d. 評価対象内で取扱われる**データのカテゴリーを特定すること**
   e. 評価対象に関連する**全てのデータ取扱業務及びシステムを特定及び記述すること**
   f. **データ取扱いの開始点及び終了点を示すこと**
   g. **該当する場合、評価対象のデータ取扱いのインターフェイスと独立した取扱業務を特定し、記述すること**
   h. **使用されるプロトコル**及びその他の関連する保証を**特定すること**
b) 評価対象からの**相互依存するデータ取扱いの除外を正当化すること**
c) 評価対象に関与する**全てのデータ処理者を一覧化**し、その業務、責任及び関連する契約条項を記述**すること**
d) **該当する場合、次の事項を特定すること**
   a. **共同管理者**
   b. データ**受領者**又は受領者のカテゴリー
   c. 第三国又は国際機関への**データ移転**
e) **国家固有及び分野固有の規範など、補完的要件が認証の対象となるのか否かを決定すること**

**評価対象のデータ管理者又はデータ処理者としての申請者の役割は明確化されなければならない**。申請者が共同管理者として行動する場合、評価対象及び認証への影響を慎重に分析しなければならない。

**評価対象及び規範的適用範囲の最終的な仕様は、認証機関の管理下に留まり、認証機関が**その適用範囲に含まれる要素の**遵守状況を効果的に評価する能力と整合しなければならない**。認証機関は、認証手続の過程において、評価対象及び規範的適用範囲の適応を決定してもよい。

**認証機関は、評価対象を十分に評価できることを確保しなければならない。**

**認証機関は、データ主体に明確な情報を通知するために、評価対象が十分に特定されていることを確保しなければならない。認証機関は、誤解を招く認証又は評価対象の過度な広範さを防止しなければならない。認証機関は、曖昧で、誤解を招く、又は、データ主体若しくはその他の第三者によって誤解釈されるするリスクのある評価対象を拒否しなければならない。**

### 7.2.4. 規範的適用範囲の明確化

**評価対象を規定する際、申請者及び認証機関は、意図する認証の規範的適用範囲に、各国又は分野固有の補完的データ保護規制が含めなければならないか否かを評価及び決定しなければならない。**

これは、データ主体による誤解釈の潜在的リスク、並びに、データ保護に関する業界及び申請分野固有の期待などの文脈を考慮しなければならない。

**認証の規範的適用範囲は明確に特定されるのが望ましい。**

  

  

### 7.2.5. 申請のレビュー及び妥当性確認

認証機関は、次の事項を確保するため、申請手続を通じて受領した情報をレビューしなければならない。

a) 申請書が全て記入されていること
b) 申請者及び評価対象に関する情報が、決定及び認証手続に必要となる負担の評価に十分であること
c) 評価対象が明確に定義されており、認証活動に影響を及ぼすその他の点（監査完了に必要となる時間、言語、安全性条件、公平性への脅威など）が考慮されていること
d) 認証機関と申請組織との間に、評価対象に関する相互理解及び合意があること
e) 利用される規範的適用範囲は、誤解を招く認証を回避するために十分であること
f) 全ての評価及び監査活動を実施するための手段が利用可能であり、特に、**認証機関が要請を受けた認証のための十分な技術的専門知識及び法的専門知識を利用できること**
g) **ユーロプライバシー確認項目及び管理項目は、評価対象を評価するために十分であること**

GDPR 第 43 条に基づく認証は、申請及び評価対象の仕様が特定の要件を遵守していることを要求する。これらの要件の遵守状況を確認するため、**認証機関は、ユーロプライバシー確認項目及び管理項目専用の一覧を適用して、申請及び評価対象[8]を確認しなければならない。**

### 7.2.6. 申請者への簡易確認及び明確化

適切な場合、認証機関は、意図される評価対象を明確化するため、会議又はテレカンファレンス（遠隔会議・電話会議）を提案するのが望ましい。当該会議は、関連するデータ取扱いの文脈及び特殊性のより良い理解、認証の実現可能性の判断、認証の負担のより良い評価、並びに、意図する認証手続に関する議論及び合意に役立つ。

### 7.2.7. 評価基準及び評価方法の決定

**EDPB の要請に従い、認証機関は、**評価対象を評価するための**評価方法を特定**し、申請者との認証契約に明記しなければならない。

**認証機関は、比較可能な評価対象のため、**次のような**一貫性のある評価方法を持たなければならない。**

- 目的及びデータ主体の同意に関し、データ取扱いの必要性及び比例性を評価する方法
- データ管理者及びそのデータ処理者によるリスクアセスメントの包括性を評価する方法
- 評価対象における個人データ取扱いの保護を確保するための救済措置、保護措置及び手順を評価するための方法

**認証機関は、その手法及び所見について、適切かつ利用可能な資料が存在することを確保しなければならない。**

**認証機関は、評価対象に適用可能なユーロプライバシー基準及び評価方法を決定しなければならない。**

**認証契約書は、ユーロプライバシー認証基準を参照しなければならない。**評価対象の遵守状況を評価するため、各国及び分野固有の規制など、追加の規範的要件が利用される場合は、これを明確化しなければならない。

### 7.2.8. リスク及び要員要件の評価

規範的適用範囲が明確化された後、認証機関は、データ保護に関する主なリスク、並びに、評価対象の評価、監査及び認証に必要となる作業負担を特定しなければならない。認証機関は、認証手続を実施するために必要となる要員及び資源の有無を評価するのが望ましい。

### 7.2.9. 申請決定

認証機関は、申請をレビューした後、受入れ又は拒否の決定を行わなければならない。認証機関は、評価対象について信頼性のある認証を付与できるか否かを評価しなければならない。

[8]「A - 申請及び評価対象 - 事前確認項目及び管理項目」

  

受入れの決定である場合、申請者に対し、当該決定に関する説明を通知しなければならず、他の認定認証機関を推薦してもよい。

拒否の決定である場合、当該レビューに基づき認証手続を実施するために必要となる力量を決定し、見積提案を作成しなければならない。

## 7.3. 見積提案

### 7.3.1. 評価に必要となる工数の見積り

認証機関は、データ取扱活動の全対象領域が必要な強度で十分に評価されることを確保するために必要となる予想監査時間を見積もらなければならない。その際、次の要素を考慮しなければならない。

a) 評価対象に適用される基準数
b) 補完的規範及び規制への遵守状況を評価するための補完的拡張基準を含める可能性
c) 評価対象の地理的適用範囲及び検査対象となる拠点数

本制度オーナーは、必要となる負担及び時間の見積りに役立つリソース及びツールを提供する。

### 7.3.2. 見積提案の作成

申請の受入れが決定された場合、認証機関は、少なくとも次の内容を含む見積提案を作成しなければならない。

a) 提案された認証の規範的適用範囲、目的及び基準
b) 次を含む認証手続全体に関する情報
    - 認証及び認証維持に使用される手法
    - 本認証制度の公式ウェブサイトへのリンク
c) 次を含む契約条件
    - 本認証制度に記載されている申請者の義務
    - 様々な関係者の役割及び責任の明確化
d) サービスの費用見積もり（又は、少なくとも、費用モデル及び 1 時間あたりの費用の表示）
e) 見積提案自体を含む、申請者との間で取り交わされる全ての文書に原則として適用可能な機密保持義務条項
f) 管理手続簡素化のため、認証機関は、申請者への見積提案の一部として、最初の認証プログラム案を提出することを決定することもできる。

### 7.3.3. 見積提案の提出

提出される見積提案は、明確な期限付きでなければならない。

申請者が条件に同意した場合、申請者は見積提案若しくは関連する認証契約書、又は、その両方に署名し、定められた期間内に支払を進めなければならない。

申請者が契約書に署名しない場合、又は、期限内に初回請求書を支払わない場合、当該申請は拒否されたものとみなすことができる。認証機関は、法律で求められる場合を除き、他のコミットメントを引き受ける自由があり、提出された見積提案に対して、それ以上の義務を負わないものとする。また、新たな申請を受け入れる義務もないものとする。

### 7.3.4. 見積提案の承諾

申請者による正式な見積提案の承諾は、申請者の権限を有する署名者による正式な署名及び提案された契約条件の正式な承諾によって正式に行われなければならない。

見積提案が認証手続開始前に初回の支払を要求する場合、申請者が必要な支払を行った後にのみ、当該契約は完了したものとみなされなければならない。

  

### 7.3.5. 請求書及び支払

監査の初見は、認証手続、必要となる作業時間数及び認証の最終費用に影響を与える可能性がある。認証機関は、申請者に対し、当初の見積提案から予想される変更について通知するのが望ましい。

申請者は、認証手続に関して認証機関から発行される全ての請求書を期限までに支払うことを誓約しなければならない。認証機関は、申請者による未払い又は著しい支払の遅延があった場合、認証手続を一時停止又は取り消すことができる。

## 7.4. 監査チームの構成及び関連機能

認証機関は、見積提案の提出と並行して、又は、遅くとも申請者が見積提案を承諾した時点で、評価手続に必要な手配を行わなければならない。認証機関は、少なくとも主任監査人及びプロジェクトマネジャー（主任監査人と同一人物でも可）を任命し、必要に応じて補充監査人及び技術専門家を含む監査チームの補充メンバーを特定するのが望ましい。

レビュアーは監査チームの一員ではなく、後の段階で特定することができる。

**EDPB の認証に関するガイドラインが定めるとおり、評価は *「認証機関が認めた外部専門家によって実施する」*ことができる。**

### 7.4.1. 必要となる資格

監査チームは、監査を実施し、選択された評価対象に対して本認証制度を適用するために必要となる専門知識及び技能を収集しなければならない。各チームは、より具体的には次を含むのが望ましい。

- データ保護規制の専門知識
- ユーロプライバシー認証制度の要件に関する十分な専門知識及び理解
- 取扱われるデータを保護するための技術的措置及び組織的措置の十分性を分析するための十分な技術的専門知識

監査人は、ユーロプライバシー・オンラインアカデミーのウェブサイト（https://academy.europrivacy.com）において、ユーロプライバシー評価コースを修了し、対応する試験に合格しなければならない。

監査チームの選択は、要員及び資源の管理に関する節（第 14 節参照）及び文書「ユーロプライバシー認証手続に関与する要員の力量のマネジメント」に定められている資格に関する特定の要件を尊重しなければならない。

### 7.4.2. 認証チーム全体の構成

認証チームは、次を含む、複数の役割及び機能で構成される場合がある。

*正式な監査チームの一員として…*

- 主任監査人
- 追加の監査人（任意）
- 技術専門家若しくは法律専門家、又は、その両方（監査人が評価対象の評価に十分な専門知識を有する場合は任意）

*監査チームを補完する追加機能*

- プロジェクトマネージャー
- レビュアー

プロジェクトマネジャー及び主任監査人の機能は、一人で兼任して遂行することも、二人の別個の者に割り当てることもできる。

共同監査人の配置は任意である。

申請者が提供する案内役及びオブザーバなどの追加機能が含まれる場合がある。

  

認証機関は、主任監査人及びレビュアーが、認証手続の結論の評価及び確認のため、データ保護に関する十分なレベルの専門知識を有することを確保しなければならない。

次の図は、監査手続における認証機関における主要な機能を要約したものである。

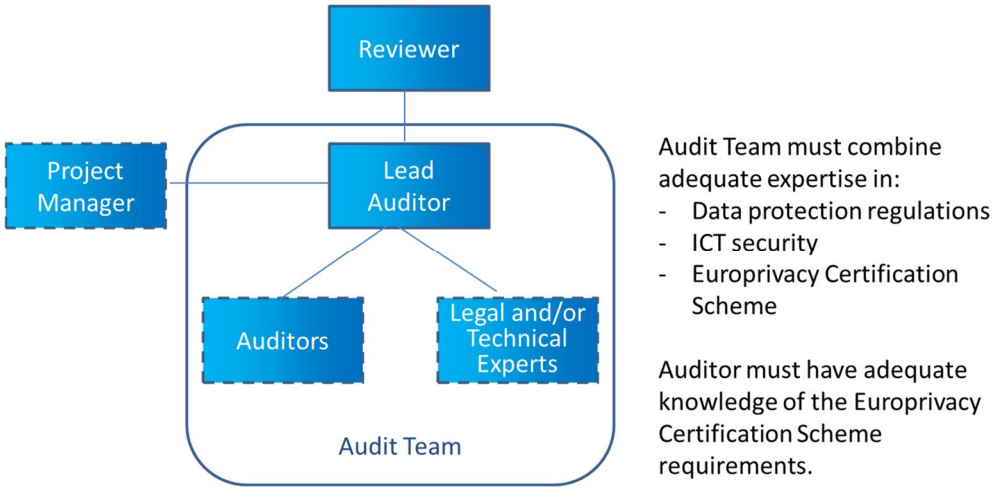


*図 5 通常の監査チームの体制*

### 7.4.3. プロジェクトマネージャー

プロジェクトマネージャーは、申請者の主な連絡窓口として機能し、申請者の認証手続に関連する活動を監視する責任を負わなければならない。プロジェクトマネージャーは、次の事項を確保しなければならない。

- 全ての必要となる契約書類に署名し、回収すること
- 認証手続に必要となる全ての情報を申請者から収集すること
- 監査計画及び関連する会議が適切に開催されること
- 監査報告書が完成し、レビューされ、申請者と共有されること
- 全ての関連情報、資料及び報告書が、認証機関のデータ保護マネジメントシステムに保存されること
- 全ての請求書及び支払は適切に処理されること
- 適切な場合、認証書が発行され、オンラインレジストリで公開されること

認証機関は、これらの職務の全部又は一部を主任監査人に委譲することを決定してもよい。

### 7.4.4. 主任監査人

提案の承諾後、認証機関は、監査の調整及び実施、並びに、レビュアーに提出する監査報告書の作成を主な責任を負う主任監査人を指名しなければならない。

主任監査人は、ユーロプライバシー・オンラインアカデミー（https://academy.europrivacy.com）において監査人としての資格を取得することにより、本認証制度の仕様及び要件に関する包括的な知識を有さなければならない。

### 7.4.5. 監査人

追加監査人は、主任監査人の権限の下、監査チームに加入してもよい。追加監査人は、本認証制度に関する適切な知識を有し、ユーロプライバシー・オンラインアカデミー（https://academy.europrivacy.com）で監査人としての資格を取得することにより、本認証制度で定める仕様及び要件を遵守しなければならない。

### 7.4.6. 技術専門家及び法律専門家

技術専門家及び法律専門家は、追加の専門知識を提供することにより、監査チームを補完してもよい。監査実施時、当該専門家は、主任監査人の権限の下で行動し、特定の任務に焦点を当てなければならない。

  

認証機関は、認証活動への技術専門家の関与について、事前に申請者に通知しなければならない。

  

### 7.4.7. 評価者

監査チームのメンバーは、主任監査人若しくは監査チームメンバー、又は、その両方を指導及び評価する評価者を務めることができる。評価者は、本制度オーナー、認証機関若しくは所轄国家機関、又は、その両方によって指名される。評価者は、申請者の認証手続において、通常の監査人又は技術専門家として作業し、行動しなければならない。評価員は、監査チームに対し、及び、該当する場合、認証機関若しくは本制度オーナー、又は、その両方に対し、観察、明確化及び改善の推奨を報告する。

### 7.4.8. オブザーバ

オブザーバを監査チームに招待してもよい。オブザーバには、申請者の組織のメンバー、コンサルタント、認定機関の要員、データ保護機関の要員、本制度オーナーの代表者、規制当局、その他の参加が正当化される者が含まれる場合がある。

**オブザーバは、監査への参加する前に機密保持義務を負わなければならない。**

認証機関がオブザーバを監査に招待することを計画する場合、オブザーバの出席に異議を唱える機会を与えるため、事前に申請者に通知しなければならない。

オブザーバは、監査及び認証手続に直接関与してはならない。オブザーバは、監査チームによる本認証制度の不遵守を特定した場合、厳密に二者間報告会の文脈において、主任監査人又は監査チームに対し、その観察を連絡しなければならない。

### 7.4.9. 案内役

現地監査を実施する場合、主任監査人及び被監査対象の間で別段の合意がない限り、案内役が監査人に同行しなければならない。

案内役の責務は、監査人が認証手続に関連すると判断した施設、従業者、文書、情報、その他の資源へのアクセスを容易にすることにより、監査人の作業を促進することである。案内役は次の項目を担当してもよい。

a) 訪問及び面談の開催及び計画
b) 監査チームのメンバーの安全及びセキュリティの確保
c) 申請者に代わって監査に立ち会うこと
d) 監査人から求められた説明及び情報の提供

被監査対象は、案内役がその責務を果たすための十分な権限及び力量を有していることを確保しなければならない。

監査チームは、案内役が監査手続及び監査結果に影響を及ぼさず、又は、妨害とならないことを確保しなければならない。

### 7.4.10. 翻訳者及び通訳者

翻訳者及び通訳者が必要となる場合があり、監査期間に影響を及ぼす可能性がある。認証機関は、公平で監査に不当な影響を及ぼす立場にない翻訳者及び通訳者を選択しなければならない。

### 7.4.11. レビュアー

レビュアーの主な機能は、監査人の報告書及び所見をレビューし、認証に関する決定を行うことである。レビュアーの機能は、評価の手続に関与していない個人又はグループ（委員会など）によって行わなければならない。レビュアーは、他の認証手続において主任監査人又は監査人を務めることができるが、レビューの対象となる認証手続では務めることができない。

レビュアーは、認証機関若しくは認証機関の組織統制の元にある団体に雇用されるか、又はその契約を締結していなければならない。認証機関に直接雇用されていないレビュアーは、認証機関の従業者に課される適格性要件と同一の適格性要件を充足しなければならない。

  

## 7.5. 評価対象の一部に関する事前認証の利用

**EDPB によれば、評価対象の一部に関する事前認証は、認証手続において考慮される可能性があるが、その評価は、少なくとも次のいずれかの要件を充足しなければならない。**
- **完全な認証報告書の入手可能性**
- **前回の認証活動及びその結果を評価するための十分な情報**

ISO/IEC 17065 は、認証機関は*「認証の申請に先立って行われた認証に関連する評価結果」*のみを使用することを要求している[9]。**文書化された証拠の再利用は認められている。**

## 7.6. 評価計画

認証機関は、評価対象の特殊性に対応するのに十分な評価計画を定めなければならない。評価計画は、要請された認証の規範的適用範囲に含まれる分野固有義務若しくは国家固有義務、又は、その両方など、潜在的な追加要件を考慮しなければならない。

評価計画には、次の事項を規定しなければならない。

a) 評価対象
b) 認証チームの構成及び役割
c) 評価活動の暫定的な全体計画

## 7.7. データ保護機関への通知義務

**欧州経済地域の他の加盟国で運営される認証機関は、認証手続を開始する前に、所轄データ保護機関に通知しなければならない。**

[9] 7.4.5 ISO/IEC 17065 を参照。

  

# 8. 遵守状況評価及び報告

## 8.1. 評価活動

評価対象は、合意された評価対象及び規範適用範囲の制約内で、本認証制度が定める要件及び基準に基づき評価されなければならない。評価対象に適用可能な各基準が評価されなければならない。

遵守状況評価には、適宜、文書及びファイルのレビュー、サンプリング、試験、調査、面談、並びに、監査などの活動を含めることができる。基準評価は「基準、確認項目及び管理項目の使用に関するユーロプライバシー・ガイドライン」に従って実施されなければならない。

認証機関は、内部資源を用いて評価活動を実施し、評価計画に従って外部資源を管理しなければならない。評価は、十分な法的専門知識及び技術的専門知識を有する監査チームによって実施されなければならない。

## 8.2. 文書レビュー

### 8.2.1. 文書へのアクセス

認証機関は、評価対象の遵守状況を評価するために必要となる文書、ファイル及び記録へのアクセスを受けなければならない。該当する場合、文書及び証拠は電子的手段で収集され、セキュアなオンラインリポジトリで利用されるようにすることができる。

セキュリティ上の理由（ファイアウォールの設定など）から、申請者のみが現地で利用できる文書があってもよい。ただし、**文書及び証拠は、認証機関が必要に応じて保管及び保存することができる。**

ECCP は、認証機関が認証手続のためにアクセスすべき文書の参照一覧を提供する。ECCP は、申請者が必要となる文書を収集し、アクセスを容易にするために使用することができる。

### 8.2.2. 事前文書レビュー

正式な評価を開始する前に、プロジェクトマネージャー又は主任監査人は、**全ての必要となる文書が存在し、監査チームが利用できる**ことを確保しなければならない。必要となる文書の参照一覧は、本制度オーナーによって提供され、認証機関によって適応可能である。

初回の資料レビューは、評価対象の遵守状況を評価することを目的としたものではなく、次の事項を検証するものであるのが望ましい。

- **DPO が十分な専門知識を有していること**（DPO によって提供される文書が確認される前に、確認されなければならない）
- **文書は、**日付若しくはバージョン番号、又は、その両方で**明確に識別可能であること**
- **文書が評価手続に完全かつ十分なものであること**

文書が不十分と認められる場合、申請者に通知されなければならず、また、評価手続の計画については、認証機関及び申請者で協議及び再確認されるのが望ましい。

## 8.3. 試験手順

認証機関は、取扱いが本認証制度要件の遵守状況を評価するため、試験を実施することができる。提案された検証手段における試験又は試験実施への参照は、試験所の利用を意味するものではなく、また、その利用を要求するものでもない。

ISO/IEC 17025 への適合性を証明することは認証機関によって求められないが、外部試験所に試験を委託する場合、外部試験所は ISO/IEC 17025 の要求事項を尊重しなければならない。

  

### 8.3.1. サンプルの使用

認証機関は、要件の遵守状況を評価するため、代表サンプルを使用することができる。

認証手続においてサンプリングアプローチが有意義で信頼できるものであることを確保するため、監査人は、次の事項を実施するのが望ましい。

a) サンプリング計画の目的の確立
b) サンプリング対象の母集団の規模及び構成の選択
c) サンプリング方法の選択
d) サンプルサイズの決定
e) サンプリング活動の実施
f) 結果のまとめ、評価、報告及び文書化

監査人は、判断に基づくサンプリング及び統計的サンプリングの両方を使用できる。

判断に基づくサンプリングアプローチを適用する場合、サンプルサイズは、最小3件とし、検討対象となる項目の総数の各桁に少なくとも1件を含めなければならない。

統計的サンプリングアプローチを適用する場合、監査人は、不遵守の場合の関連するリスクレベル及び影響に応じて、許容できる信頼水準のパーセンテージを調整することができる。原則として、監査人は、少なくとも95%の信頼水準を使用し、誤差の最大許容範囲は5%とするのが望ましい[10]。

### 8.3.2. 技術的試験

適切な場合、データ保護に関連する脆弱性を特定するため、若しくは、本認証制度によって求められる確認項目及び管理項目（脆弱性評価、ペネトレーションテストなど）を実施するため、又は、その両方のため、一連の技術的試験を実施しなければならない。この手続は、必要となる専門知識を有する技術専門家又は試験所によって取り扱われなければならない。技術専門家及び試験所は、特定の試験及び所見を要求することが可能な主任監査人の監督下で行動しなければならない。

## 8.4. 調査及び現地評価

### 8.4.1. 調査の原則

調査とは、基準で定める要件充足性の検証及び判断するために、データ取扱いが実施又は管理されている施設を訪問若しくは遠隔評価すること、又は、対象物を直接観察することをいう。これには、目視による観察、実証の要請、データ取扱いに関与する利害関係者への質問などが含まれる場合があるが、これらに限定されない。

### 8.4.2. 現場評価及び現地監査－一般原則

評価対象によっては、現地評価（「監査」ともいう。）が必要となる場合がある。現地評価では、遠隔調査のための技術を活用することができる。

認証機関は、現地評価の明確な必要性が生じた場合、又は、主任監査人が評価対象の遵守状況について信頼できる意見を表明するために現地評価が必要であると認める場合、いつでも現地評価を実施しなければならない。

現地評価実施の決定は、原則として、申請が処理され、全ての必要文書が修正された後、評価計画とともに、手続の早い段階で申請者に通知されるのが望ましい。しかし、現地評価の決定は、例えば、初回の試験及び評価結果が主任監査人に提出された後など、後の段階で行われてもよい。

監査基準は、遵守状況を判断するための確認項目及び管理項目の明細一覧を含む、本認証制度に定められている。

[10] オンライン計算機を使用することもできる（例：サンプルサイズ計算機 - Qualtrics）。

  

### 8.4.3. 監査の証拠は、本基準に関連する記録、事実の表明及びその他の情報で構成され、検証可能でなければならない。現地評価の準備

プロジェクトマネージャーは、現地評価又は監査を実施するため、認定主任監査人又は監査チームを任命しなければならない。認証機関は、監査チームの資格が、申請者が実施する活動の種類に十分であることを確認しなければならない。

主任監査人は、確認及び承認のため、評価又は監査の少なくとも 2 週間前に、申請者の代表者に監査計画を送付しなければならない。当該監査計画には、現地監査のために申請者が準備する要件、資源及び文書の暫定的な一覧を記載しなければならない。

### 8.4.4. 現地評価の手続

現地評価又は監査の段階には、次の事項を含めるのが望ましい。

a) 主任監査人が次の事項を提示する初回会議
   - 評価及び監査計画（目的、適用範囲及び主な確認項目を含む）
   - 前段階から得られた証拠及び所見の要約
b) 文書の分析及び評価
c) 関連する情報源の特定
d) 適切なサンプリング、試験、調査及び検証による情報収集（必要に応じて、現地訪問及び従業者との面談を含む）
e) 前段階から得た評価又は監査の証拠の確立
f) 収集した情報及び証拠の本認証制度の要件に対する評価
g) 評価又は監査所見の策定
h) 評価又は監果所見の策定のため、評価又は監査の所見、並びに、証拠をレビューすること
i) 主任監査人が評価又は監査の結論を提示する最終会議

### 8.4.5. 現地評価の概要報告書

認証機関は、評価又は監査の初見及び結論、並びに、特定された不遵守に関する情報を提供するため、正式な評価又は監査の概要報告書を作成しなければならない。

### 8.4.6. 複数拠点評価

評価対象は、申請者の効果的な管理の下にある複数の拠点に分散した個人データ取扱いを含むことができる。認証機関は、本基準への遵守を証明するために複数拠点評価の必要性を判断しなければならない。

複数拠点評価が必要となる場合、認証機関は、類似のデータ取扱活動を実施する拠点間で拠点サンプリングを適用することができる。拠点サンプリングは、申請者が関連拠点で効果的な管理及び監視を行っている場合にのみ適用可能である。

拠点は、次の事項を考慮して選択されなければならない。

a) 取扱われたデータのリスクレベル
b) 拠点の多様性

また、該当する場合、次の事項を考慮して選択されなければならない。

c) 前回の監査結果
d) 報告された苦情

さらに、該当する場合、少なくとも 25%の拠点が無作為に選択されなければならない。

評価対象となる拠点の最小数は、拠点数の平方根に比例させ、次の比率としなければならない。

- 初回監査：単純平方根を直下の整数に切り上げる。
- サーベイランス監査：平方根の結果の 60%を直下の整数に切り上げる。
- 再認証：平方根の結果の 80%を直下の整数に切り上げる。

複数拠点評価を実施する場合、サンプリングされた各拠点における現地監査の時間は、通常の監査時間の 50%に短縮することができる。

  

## 8.5. 他の認証機関による監査結果の利用

認証機関が、他の認証機関から申請者に既に付与された認証を考慮する場合、認証機関は、不遵守に関する是正措置の報告書及び文書などの十分な証拠を取得及び保持しなければならない。認証機関は、既存の監査プログラムへの調整を正当化及び記録し、前回の不遵守に関する是正措置の実施状況をフォローアップしなければならない。

## 8.6. 遵守状況の評価

### 8.6.1. 推奨される評価手段

本基準には、推奨される評価手段が記載されている。**評価対象によっては、異なる評価手段が適用可能な場合があり、また、複数の評価手段が必要となる場合がある。**例えば、個人データへのアクセスを要求するデータ主体の権利のための手順の評価は、かかる要求が申請者によってどのように取り扱われたかを確認することによって実施可能である。しかし、申請者がまだ要求を受けていない場合、申請者の規則、方針若しくは手順の文書レビュー、又は、手順の有効性を試験すること、あるいは、その両方は、妥当な代替手段になり得る。

**監査人は、最も効率的な評価手段を用い、適用可能な各基準の遵守又は不遵守を高い信頼性をもって判断するために十分な証拠を収集しなければならない。**

ISO/IEC 17007 に従い、*「（もしあれば）どのような遵守状況評価活動を利用するか、誰がどのような条件で遵守状況評価を実施するかは、規範文書の利用者に委ねられるのが望ましい。***各基準について、監査人は、要件の充足性を判断するために十分な証拠が収集されるまで、一つ以上の評価方法を用いなければならない。**

**原則として、次の優先順位が推奨される。**

a. ファイル及び記録のレビューを含む文書レビュー
b. 面談
c. 調査
d. 試験
e. その他の効率的かつ信頼できる検証手段

優先順位は、ある評価手段が適用できない場合、又は、異なる順序によって評価の効率性及び信頼性を高めることができる場合、適応することができる。他の検証手段の使用は、記録及び正当化されなければならない。

面談は、評価対象の評価の一環として実施されなければならない。

基準評価に関する詳細は、基準、確認項目及び管理項目の使用に関するユーロプライバシー・ガイドライン、並びにユーロプライバシー・リソース＆コミュニティウェブサイト（https://community.europrivacy.com）の FAQ セクションに記載されている。

### 8.6.2. 証拠の記録

基準、確認項目及び管理項目のステータスを評価するため、監査人は、要件の遵守又は不遵守を証明する明確な証拠を収集及び記録しなければならない。

認証機関は、その所見が明確な証拠に基づいていることを証明できなければならない。

  

### 8.6.3. 基準、確認項目及び管理項目の所見、並びに、ステータス

ほとんどの確認項目及び管理項目は、次の状態カテゴリーのいずれかに従って評価及び決定される。

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

*図 6 初見のステータスカテゴリー*

管理項目が適用されないと判定された場合、その理由は正当化及び文書化されるのが望ましい。

### 8.6.4. 不遵守の判定

基準（又は確認項目及び管理項目）の評価の結果が「要件不充足」を特定した場合、それは不遵守を構成する。

全ての不遵守は、明確な識別番号を付して一覧化され、尊重されていない特定の規範及び要件を参照して明記されなければならない。各不遵守は、「軽微な」又は「重大な」不遵守のいずれかに判定されなければならない。[11]

*「重大な」不遵守*

**重大な不遵守とは、評価対象のデータ取扱活動が、本文書が定める基本的なデータ保護要件、データ主体の権利、又は、ユーロプライバシー認証制度の要件を遵守しない不遵守をいう。**

**申請者が GDPR の定める法的義務に違反する不遵守は、すべて重大な不遵守を構成する。**

*「軽微な」不遵守*

**軽微な不遵守とは、重大な不遵守に該当しない不遵守である。**

*観察*

評価手続の結果、評価対象の要件に対する正式な不遵守を構成しないものの、ボーダーライン又は最適でないとみなされる場合がある。かかる場合、評価者はそのステータスを「観察」と判定し、所見及び懸念を記録しなければならない。

### 8.6.5. 不遵守の影響

**次のいずれかに該当する場合、認証を付与してはならない。**

- **未解決の重大な不遵守がある場合**
- **検証待ちの軽微な不遵守が 5 件以上ある場合**
- **認証が第三者及びデータ主体の誤解を招くおそれがある場合**

**軽微な不遵守が残存する場合、申請者は、是正計画を提示し、次回のサーベイランス監査までに、特定された軽微な不遵守に対処することを誓約しなければならない。**

**軽微な不遵守が特定され、是正措置計画が認証機関によって容認された場合、認証機関は、最大 5 件の軽微な不遵守について、次回サーベイランス監査までに遵守に関する証拠を提出するためにのみ、再評価を延期する権限を有する。**

[11] この区別は ISO/IEC 17021-1 に準拠するために必要となる。

  

重大な不遵守については、認証機関は、当該不遵守が解決済みかつ終了したとみなすため、その修正及び是正措置をレビュー、容認及び検証しなければならない。

軽微な不遵守については、認証機関は、当該不遵守が解決済みかつ終了したとみなすため、その是正をレビュー、容認及び検証し、又は、次回の監査において、評価及び確認される申請者の是正措置計画を容認しなければならない。

前回の評価で特定された軽微な不遵守で、申請者が対処していないものは、認証機関により「重大な不遵守」として再判定される可能性がある。

**評価手続中に認証の妨げとなる不遵守が発生**し、申請者が認証手続の継続を希望した場合、認証機関は次の事項を行わなければならない。

a) 是正が必要な不遵守が是正されたことを検証するために必要な追加評価業務に関する情報を提供すること
b) 特定された不遵守を是正するために必要となる遅延（6 か月を超えないのが望ましい）について、申請者と合意すること

申請者が追加評価業務の完了に同意し、かつ、**適切な場合、遵守状況評価の信頼性を確保するため、**ISO/IEC 17065 の要求事項に準拠して**追加評価業務を完了するために評価手続を繰り返さなければならない。**文書化された証拠は再利用することができる。

### 8.6.6. 是正措置計画

申請者が認証手続の継続を希望する場合、是正措置計画が次のとおり策定されなければならない。

認証機関は、申請者に対し、特定された不遵守の一覧及びそれらが認証要件とどのように関連するかを連絡しなければならない。

申請者は、特定された不遵守ごとの是正措置及びその根拠を含む是正措置計画を作成及び提案しなければならない。是正措置計画は、潜在的な不遵守を列挙し、その重大性（「重大な」不遵守又は「軽微な」不遵守）に従って分類しなければならない。講じるべき適切な措置及びその適用方法が詳述されなければならない。申請者が提案する是正措置は、認証手続を継続するために適切かつ包括的でなければならず、仮に適切かつ包括的でない場合、認証機関は、申請者に対し、新たな是正措置を提案するよう求めなければならない。

是正措置計画は、申請者が合意した期間内（6 か月を超えないのが望ましい）に完了されなければならない。

### 8.6.7. 継続的な不遵守の影響

不遵守が継続した場合の認証への影響は、不遵守の性質、重大性、発生及び不正行為のリスクに応じて定義される。

是正計画に関する適切な措置は、次の措置があり得る。

a) 条件付きでの認証の継続
b) 認証範囲の縮小
c) 認証の一次停止又は取消し

  

## 8.7. 評価報告書

評価活動の終了後、主任監査人は、申請者のために評価報告書を作成する責任を負う。

評価報告書は、**改善領域を特定してもよいが、**コンサルティングの提供を避けるため、**具体的な解決策を提言してはならない。**

***評価報告書は、「要件がどのように充足しているかを記述し、当初充足していない場合は、修正及び是正措置並びにその適切性を記述し、その結果、認証を付与及び維持する理由を提供す」るのが望ましい。****これには、認証書の発行、更新又は取消しに関する個々の決定の概要も含まれる。それには、****基準の適用による理由、主張及び証拠****、並びに、認証過程で収集された事実又は前提に基づく結論、判断又は推論****を提示****するのが望ましい（EDPB）。*

評価報告書には、申請者に情報を提供し、情報に基づく認証の決定を可能にするため、正確、簡潔及びかつ明確な評価の記録が含まれなければならない。本報告書には、次の内容を含まなければならない。

a) 次の事項を含む識別情報
   - 認証機関の名称
   - 申請者の名称
   - 申請者の所在地
   - 申請者の代表者の氏名
b) 監査は入手可能な情報のサンプリングに基づくことを示す免責事項
c) 該当する場合、次の監査計画に関する情報
   - 監査の種類（初回／サーベイランス／再認証／特別監査）
   - 監査基準
   - 監査の目的
   - 評価対象、特に監査対象の組織単位若しくは機能単位又は取扱い、及び、監査時期の特定
   - 該当する場合、結合監査、共同監査又は統合監査の表示
d) 潜在的逸脱に関する情報
   - 監査計画からの逸脱とその理由
   - 監査プログラムに影響を及ぼす重大な問題
e) 監査チームの構成に関する情報
f) 該当する場合、監査活動の日付及び場所
g) 次の評価及び監査の初見
   - 要件がどのように充足するかを説明する関連する証拠を参照した初見
   - **要件が当初充足しなかった場合、修正及び是正措置並びにその適切性の説明[12]**
   - 監査の種類に応じた要件と整合する結論
   - 該当する場合、申請者のマネジメントシステムに影響を与える重要な変更
   - 特定された場合、未解決の問題
h) 該当する場合、監査チームによる観察及び推奨
i) 該当する場合、申請者が認証及び遵守マークを管理している方法の評価
j) 該当する場合、以前に特定された不遵守に対処するために申請者が講じた是正措置に関する報告書
k) データ保護の遵守状況及び有効性に関する表明、並びに、次の事項に関連する証拠の要約
   - 個人データを効果的に保護するマネジメントシステムの能力
   - 内部監査、並びに、実施されている技術的措置及び組織的措置のレビュー
l) 評価対象の適切性に関する結論
m) 監査目的が達成されたことの確認

評価報告書は、正式に次の事項を確認しなければならない。

[12] 特定された不遵守の根本原因に関する情報の収集を強く推奨する。

  

a) 規範的適用範囲及び評価対象は、認証の誤解を招くリスクを回避するために十分に明確であること
b) 申請者及びその代表者は、認証手続において透明性があり、協力的であったこと
c) 評価対象の個人データ次のとおりであること
   - データ主体との関係において、適法であり、公正であり、かつ、透明性のある態様で取扱われること
   - 特定され、明確であり、かつ、正当な目的のために収集されること
   - 当該目的に適合しない態様で追加的取扱いをしないこと
   - その個人データが取り扱われる目的との関係において、十分であり、関連性があり、かつ、必要のあるものに限定されること
   - 正確であり、かつ、それが必要な場合、最新の状態に維持されること
   - 当該個人データが取り扱われる目的のために必要な期間だけ、データ主体の識別を許容する方式が維持されること
   - 無権限による取扱い若しくは違法な取扱いに対して、並びに、偶発的な喪失、破壊又は損壊に対して、適切な技術上又は組織上の措置を用いて行われる保護を含む、個人データの適切な安全性を確保する態様により、取扱われること

評価報告書の所有権及び著作権は、認証機関によって保有されなければならない。

### 8.7.1. 初回認証付与のための情報

評価手続の終了時、主任監査人は、次の情報を準備するとともに、初見をレビューし、決定を準備するレビュアーに提供しなければならない。

*a)* 評価報告書
*b)* *不遵守に関するコメント、並びに、該当する場合、申請者によって講じられた修正及び是正措置*
*c)* *申請のレビューに使用され、認証機関に提供された情報の確認*
*d)* *監査目的が達成されたことの確認*
*e)* *認証を与えるか否かの推奨を条件又は観察を付して行うこと*[13]

### 8.7.2. 結論の等級付け

各監査において、主任監査人は、次の等級付けを用いて結論を要約するのが望ましい。

A. **本認証制度の遵守**
通常、申請者は正式なユーロプライバシー認証及びラベル付けの恩恵を受けることが許可される。

B. **改善事項を伴う本認証制度の遵守**
通常、申請者は、特定された懸念事項に対処及び改善することのコミットメントにより、正式なユーロプライバシー認証及びラベル付けの恩恵を受けることが許可される。改善事項への対処を怠ると、次回のサーベイランス監査（定期監査）において認証の維持が認められない場合がある。

C. **認証前に是正が必要な不遵守**
認証が付与される前に、申請者が不遵守に対処し、信頼性のある是正計画を提供することを要求するものである。

D. **不遵守の過多**
通常、正式な認証の拒否及び認証手続の終了に繋がる。どのような場合でも、必要となる不遵守の是正を行わない限り、認証は同意されない。

[13] ISO/IEC 17021:2015 の第 9.5.3.1 節を参照。

  

# 9. レビュー手続、決定及び公表

## 9.1. レビュー手続

### 9.1.1. レビュー前の監査初見の文書化義務

主査監査人は、レビューのための報告書を提出する前に、評価活動、証拠及び初見を文書化しなければならない。

### 9.1.2. レビュー手続

認証機関は、認証の付与、認証範囲の拡大若しくは縮小、更新、一時停止若しくは復帰、又は、認証の取消しを決定する前に、効果的なレビューを実施する手続を持たなければならない。認証機関は、次の事項を確認しなければならない。

a) 監査チームから提供された情報が、要件を充足し、認証の規範的適用範囲を対象とするのに十分であること
b) 重大な不遵守について、是正措置をレビューし、同意したこと
c) 残存する軽微な不遵守について、申請者の是正措置計画をレビューし、承認したこと

レビュー及び認証決定が別個の者によって完了される場合、認証決定のための推奨事項は文書化されなければならない。

## 9.2. 認証決定

### 9.2.1. 認証決定の主要な要件及び手続

レビュー手続が完了した後、認証機関は認証に関する正式な決定を行わなければならない。**ISOの要求に従い、*「認証機関は、認証に関連する決定について責任を負い、その権限を保持しなければならない*[14]*」*** *「評価、そのレビュー及びその他の全ての関連情報に基づいて認証決定を行うため、少なくとも1名の者を任命しなければならない」*[15]。認証機関は、この権限をレビュアーに委任してもよい。

認証機関は、次の事項を確保しなければならない。

a) **認証に関する正式な決定**[16]**を行う者又は委員会は、監査を実施した者とは異なること**
b) 認証決定を実施するために任命された個人が、**本認証制度の要件について適切な力量及び理解を有していること**
c) 認証決定を実施するために任命された**個人は*「認証機関*[17]*に雇用されているか、又は、認証機関と契約下にある者であること*[18]*」***

### 9.2.2. 決定

決定は認証機関によって行われ、次の結果につながることがある。

a) 認証の付与又は拒否
b) 認証範囲の拡大又は縮小
c) 認証の一時停止又は復帰
d) 認証の取消し又は更新

**認証書の有効期間は3年を超えてはならず、再認証により更新可能である。**

**認証機関は、補足情報の要請を含む、認証決定を記録及び文書化しなければならない。**

[14] ISO/IEC 17065:2012 の第 7.6.1 節
[15] ISO/IEC 17065:2012 の第 7.6.2 節
[16] 例えば、認定の付与、拒否、適用範囲の拡大若しくは縮小、一時停止若しくは復帰、認証の取消し、又は認証の更新などである。
[17] 又は、同等の要件を充足する認証機関の組織統制下にある組織。

  

## 9.3. 認定なき又は認定前の認証付与

正式な GDPR 認証には、GDPR 第 43 条に基づき、EDPB のガイドラインを遵守して、認証機関が正式な認定又はデータ保護機関の同意を受けることが必要である。

法律で禁止されている場合を除き、認証機関は、正式な認定又は同意を受ける前に評価を開始及び実施することができる。ただし、GDPR 第 43 条に基づく正式な認証書の発行には、所轄国家機関による同意又は認定が必要である。

**GDPR 第 43 条の適用範囲外で付与される任意の認証は、明確に区別され、正式な GDPR 認証と混同されるリスクは防止されなければならない。**

## 9.4. 認証書の移転

有効な認証書は、その有効期間中に、次の手順に従って、他の認証機関に移転させることができる。

a) 申請者は、新しい認証機関の申請書に必要事項を記入しなければならない。
b) 申請者は、新しい認証機関に対し、現在の認証周期の全ての関連文書へのアクセスを提供しなければならない。
c) 新しい認証機関は、当該提供された文書をレビューし、認証に関する決定を下すため、サーベイランス監査又は再認証監査を実施しなければならない。

移転は、移転元の認証書のサーベイランス監査の期間及び頻度を尊重しなければならない。

## 9.5. 認証の一時停止、撤回又は適用範囲の縮小

### 9.5.1. 当局の決定への遵守義務

**GDPR 第 58 条の定めるとおり、*「認証機関は、認証の要件を充足せず、又は、充足しなくなった場合、所轄データ保護機関からの申請者への認証を取り消す、又は、発行しない決定及び命令を受け入れなければならない」*。**

### 9.5.2. 一時停止、取消し及び適用範囲適応の手順

認証機関は、認証書の一時停止若しくは取消し、又は、規範的適用範囲若しくは評価対象の潜在的な適応、あるいは、規範的適用範囲及び評価対象の潜在的な適応の両方について、透明性のある手順を持たなければならない。これは、申請者が本認証制度の要件遵守を常態的かつ深刻に維持できない場合、又は、契約違反若しくは第三者の誤解を招くおそれのある活動を行う場合など、その他の行動を行う場合に適用される。認証証明の一時停止、取消し又は適用範囲の変更を行う妥当な理由の例には、次のものが含まれるが、これらに限定されない。

a) 申請者の認証を受けたデータ取扱いが、次のような認証要件を常態的に又は深刻に充足しない場合
   - 特定された不遵守に対する十分な対処を行わないこと
   - 個人データ保護のための技術的措置及び組織的措置が不十分であること
b) 申請者の不合理な行為又は不作為により、サーベイランス監査又は再認証監査が、必要となる頻度又は計画どおりに実施されない場合
c) 次のような、署名された認証契約の条項に違反する場合
   - 料金又は請求書の未払
   - 不適切な認証マークの使用若しくは認証への参照、又は、その両方
d) 申請者が自発的に一時停止を要請した場合
e) 認証書のステータスに影響を及ぼし得る次の証拠を入手した場合
   - 認証を受けたデータ取扱いの不遵守の証拠
   - 重大なインシデント又は事故が発生した場合に、効果的でない技術的措置及び組織的措置の証拠

  

### 9.5.3. 認証の一時停止の管理

認証の一時停止の場合、認証機関は、一時停止を終了させ、本認証制度を遵守して認証を復帰させるために必要な措置を策定し、申請者に通知するため、1 名以上の者を任命しなければならない。

当該被任命者は、必要な措置が講じられた場合、手続を取り扱い、一時停止を解決するため、問題となっている本認証制度の要件及び問題について十分な知識及び理解を有さなければならない。

一時停止中、申請者のデータ取扱いの認証は一時的に無効となる。

認証機関は、申請者が一時停止の原因となった問題に対処及び解決する期限を規定しなければならない。ほとんどの場合、一時停止は 6 か月を超えることはなく、適応可能である。

一時停止の原因となった問題が申請者によって解決された場合、認証は復帰されるものとする。ただし、認証機関によって定められた期間内に問題が申請者によって解決されない場合、認証機関は認証の適用範囲の縮小又は認証の取消しを行わなければならない。

### 9.5.4. 適応及び認証の適用範囲の縮小

認証を受けた申請者が、評価対象又は規範的適用範囲の特定の部分の認証要件を常態的又は深刻に充足しない場合、次の条件を満たす場合に限り、認証機関は、当該要件を充足しない部分を除外するため、評価対象又は規範的適用範囲の修正及び縮小を検討してもよい。

a) かかる縮小は、ユーロプライバシーの要件を遵守しなければならない。
b) 修正された評価対象及び規範的適用範囲は、誤解を招くものではなく、十分に一貫性があり、第三者及び公衆に理解可能なものでなければならない。

### 9.5.5. 認証文書及び情報の更新義務

認証が終了、一時停止若しくは撤回、復帰又は範囲縮小された場合、認証機関は次の事項を行わなければならない。

a) 本認証制度が規定する措置を講じること
b) **必要な場合、所轄データ保護機関若しくは各国認定機関、又は、その両方に通知すること**[19]
c) 決定が申請者に明確に通知されることを確保すること
d) 申請者に対し、決定を遵守し、それに応じて情報発信を適応するよう要請すること
e) 正式な認証文書、公開情報、マークの使用許可などに必要な全ての変更及び更新を行うこと
f) ユーロプライバシー認証レジストリを更新すること

本認証制度を遵守するために認証機関によって実施された作業の料金は、申請者に課されなければならない。

### 9.5.6. 終了

認証機関は、次のような場合、認証手続の終了を決定してもよい。

a) 信頼性のある認証手続を実施するための条件を充足していない場合
b) 申請者が誤解を招く情報を提供した場合、又は、協力しなかった場合
c) 申請者及び認証機関が認証手続の終了を共同で決定した場合

早期終了を含む終了の場合、認証機関は決定に関連する作業（決定の報告、記録及び文書化、オンラインレジストリの更新など）を完了させなければならず、申請者は関連する正当な理由のある費用を負担しなければならない。

[19] 取消し又は一時停止の場合、認証機関は、その決定の理由も提示しなければならない。

  

## 9.6. 認証の通知及び文書化

### 9.6.1. 第 43 条に基づくデータ保護機関への通知義務

*「第 43 条第 1 項は、所轄監督機関が第 58 条第 2 項(h)項に基づく是正権限を行使できるよう、認証機関に対し、認証を発行又は更新する前に監督機関に通知することを義務付けている。さらに、第 43 条第 5 項は、認証機関に対し、要請された認証の付与又は取消しの理由を所轄監督機関に提供することも義務付けている。より一般的には、GDPR 第 42 条及び第 43 条に基づき、「認証機関は、認証方法の適用を監視するために必要となる情報（...）を監督機関に提供しなければならない」（EDPB ガイドライン 1/2018）。*

### 9.6.2. 認証決定通知

認証機関は、認証を付与するか否かの決定を申請者に通知しなければならない。認証が付与されない場合、認証機関は、決定の理由を特定し、申請者に通知しなければならない。

### 9.6.3. 認証文書発行前の事前要件

認証機関は、認証文書を発行する前に、次の事項を確保しなければならない。

a) 認証手続が認証機関によって文書化及び記録されていること
b) 認証範囲の付与又は拡大の決定がなされたこと
c) 認証料の本制度オーナーへの支払を含む、認証要件を充足していること
d) 認証契約書が申請者によって完成及び署名されていること

**認証付与の前に、申請者は、本認証制度要件及びユーロプライバシー一般利用規約を遵守することを明示的に同意しなければならない。**

上記の条件を充足する場合、認証機関は次の事項を行わなければならない。

a) ユーロプライバシー認証レジストリへの認証の記録
b) 申請者への認証文書の送付

### 9.6.4. 認証文書の内容

認証文書には、次の事項を明記しなければならない。

a) **認証を受けた申請者の名称及び所在地**
b) **認証を受けた評価対象の名称及び識別情報**（該当する場合、バージョン若しくはモデル、又は、その両方を含む。）
c) 次の項目を含む、**評価対象についての簡単な仕様**
   - データ取扱活動の種類
   - 該当する場合、認証の地理的適用範囲
d) 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**として行動しているか否か
e) 該当する場合、**共同管理者**の名称
f) 該当する場合、認証に適用可能な拡張又は適応
g) **発行日及び有効期限日**（該当する場合、認証の適用範囲の拡大若しくは縮小の日付、又は認証の更新日を含む。）
h) **有効期限日**
i) 認証書の**固有識別コード**
j) **ユーロプライバシーのロゴ又は遵守マーク**（その使用が誤解を招くものでもなく、曖昧でない場合に限る。）
k) 認証に利用される**本認証制度のバージョン**（改訂の日付又はバージョン番号）の引用
l) **認証機関の名称及び所在地**
m) **認証決定を行った者**又は当該決定を行った機関の議長を務める者**の氏名、役職及び署名**
n) 該当する場合、改訂された文書と以前に廃止された文書を区別する手段

認証文書は、上記の内容を含むことを条件に、第 15.6.4 節に定めるとおり認証書の形式をとることができる。

本制度オーナーは、発行及び署名された認証文書の電子コピーを要請することができる。

  

## 9.7. ユーロプライバシー認証レジストリ

*「認定認証機関は、どの認証がどのような根拠（又は認証方法若しくは制度）に基づいて実施されたか、どの枠組み及び条件の下でどれだけの期間有効であるかを恒常的かつ継続的に公開しなければならない。（EDPB）」*

ユーロプライバシー認証書が有効であるためには、本制度オーナーが管理するユーロプライバシー認証公式オンラインレジストリに登録及び公開されなければならない。認証機関は、当該公式レジストリの情報を登録及び更新しなければならない。

### 9.7.1. ユーロプライバシー認証レジストリに含まれる公開情報

発行されたユーロプライバシー認証レジストリには、少なくとも、次の当該認証に関する情報が含まれなければならない。

a) 申請者の名称
b) 評価対象の名称、及び、該当する場合、そのモデル若しくはバージョン、又は、その両方
c) 評価対象及び潜在的な適用範囲の除外に関する記述
d) 法令遵守の認証を受けた本認証制度及び本基準（バージョンを含む）の引用
e) 基準を評価するために実施された評価方法及び試験（現地評価、文書レビュー、技術的試験など）
f) 評価結果の要約
g) 認証機関の識別
h) 認証書の発行日、更新日、失効日
i) 認証書の有効期限

データ保護機関による妥当性の確認手続の支援、及び、本認証制度改善の目的で、追加情報を本レジストリに保存することができる。

### 9.7.2. 本制度オーナーに提供される非公開情報

認証機関は、要請があれば、本制度オーナーに対し、次の情報を提供しなければならない。

a) PDF 形式の認証報告書のコピー
b) 権限を有する者の署名ある認証文書の PDF ファイル
c) 評価のために申請者に請求された作業時間数
d) 評価対象の規模及び複雑性を考慮した場合、算出された監査時間が完全に信頼できる評価を完了するために十分かつ適切であったか否か
e) 本認証制度若しくは確認項目及び管理項目の一覧、又は、その両方の改善のための提案

### 9.7.3. 認証機関が保管する追加情報

**認証機関は、実施された認証に関する全ての文書を**、次の事項を含む、***「完全、包括的、最新かつ監査に適した」*状態に維持しなければならない。**

a) 申請及び情報
b) 認証に関する契約書
c) 該当する場合、監査プログラム
d) 監査時間決定の正当性
e) 修正及び是正活動の検証
f) 認証決定文書
g) 監査人及び技術専門家の力量に関する証拠を含む、認証の信頼性を証明するための関連記録
h) 該当する場合、次の事項
   - 初回サーベイランス監査報告書及び（再）認証監査報告書
   - 拠点のサンプリングに使用された手法の正当性
   - 苦情及び異議申立ての記録、並びに、その後の是正又は是正活動
   - 評価対象を含む前回の認証文書
   - 委員会の審議及び決定

  

### 9.7.4. データ保護機関によるレジストリへのアクセス

GDPR 第 43 条に基づき、所轄データ保護機関は、本制度オーナーに送信された個人情報若しくはレジストリに保存された個人情報、又は、その両方にアクセスできるものとする。

  

# 10. 認証の維持及び更新

**認証を維持するためには、定期的な監視措置が義務付けられている。各認証の監視期間は文書化されなければならない。**

## 10.1. 認証の維持 – -一般原則

原則として、ユーロプライバシー認証は3年間の更新可能な有効期間が付与される。当該期間、**申請者は次の事項をいずれも遵守しなければならない。**

- **認証を受けた評価対象が、適用可能な本認証制度の要件及び基準を遵守していることの確保**
- **認証機関に対する当該遵守状況に関する変更又は懸念の通知**

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ことを示す証拠に基づき、認証を維持しなければならない。**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らない。**

**重大な不遵守が特定された場合、認証の一時停止及び取消しに繋がらなければならない。**申請者が本認証制度の要件（サーベイランス活動、料金の支払など）を遵守しない場合、認証機関は、認証書を一時停止又は取り消さなければならない。該当する場合、かかる決定は本制度オーナー若しくは所轄国家機関、又は、その両方によっても実行される場合がある。

### 10.1.1. 認証手続の周期

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する。認証及び再認証に成功した場合、次の監査が実施されなければならない。

a) 認証日から12か月以内の初回のサーベイランス監査
b) 認証日から24か月以内の2回目のサーベイランス監査
c) 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 か月の認証サイクルが新たに開始される。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。

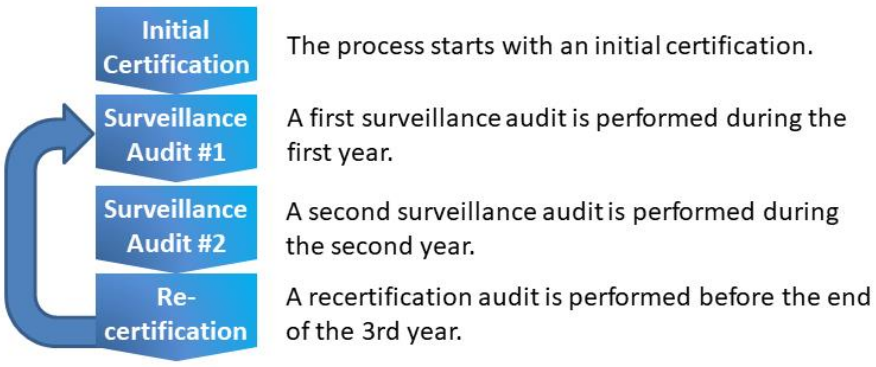


*図 7 認証周期*

### 10.1.2. 監視及びサーベイランス

監視活動は、再認証監査の間隔において、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る。

認証機関は、評価対象に適用可能な主要なデータ保護要件が定期的に監視されるよう、監視及びサーベイランス活動の年次で計画し、策定しなければならない。

サーベイランス監査は、適切なツール及び手法に基づく現地監査若しくは遠隔監査、又は、その両方となる。

  

### 10.1.3. サーベイランス活動の優先分野

サーベイランス活動は、全ての基準を再評価することを要求しないが、特に、次の事項に焦点を置かなければならない。

a) 申請者によって前回の評価以降に実施された**内部監査レビュー、評価報告書**（リスクアセスメント、データ保護影響評価など）、及び、トップマネジメントレビューの**見直し**
b) **申請者による次の事項に関する作業の進捗状況及び講じられた措置のレビュー**
   - 前回の監査で特定された不遵守
   - 前回の評価以降の規制要件及び規範的要件の変更
   - 苦情取扱い
   - 能力構築及び継続的改善のために計画された活動
c) 次の事項の**評価**
   - データ取扱いの適法性の継続性
   - データ主体の権利を尊重するための措置の有効性
   - 技術的措置及び組織的措置の有効性
   - 記録及び登録の効果的利用
   - 運営管理の継続性
   - 認証マークその他認証への参照の適切な使用及び連絡
d) **評価対象に含まれるデータ取扱いの変更のレビュー**

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しなければならない。さらに、サーベイランス監査のための補完的確認項目及び管理項目の特定の一覧（*「S-補完的サーベイランス確認項目及び管理項目」*）を適用しなければならない。

### 10.1.4. 認証に影響を与える変更

適用可能なデータ保護規制の変更（法改正、各国又は国際的な裁判所の決定、EDPB の決定、又は、欧州委員会の決定など）は、認証機関によって監視され、対応されなければならない。かかる変更が付与された認証に影響を及ぼす場合、認証機関は次の事項を行わなければならない。

1. 認証の有効性への影響度の評価
2. 次の事項を規定した行動計画の策定
   - 特定された規範的変更
   - 特定された認証書
   - 提案された適応手段（対象となる再評価、移行期間、一時停止、取消しなど）
3. 該当する場合、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妥当性の検証を要請すること
4. データ保護機関の同意を得た後、行動計画の実施

## 10.2. 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ある。

### 10.2.1. 再認証付与のための情報

認証更新の決定は、評価対象の遵守状況維持のために申請者が講じた措置、及び、該当する場合、当該遵守状況について受領した苦情を含む、再認証評価の結果に基づかなければならない。

### 10.2.2. 再認証活動（認証の更新）

再認証の目的は、評価対象のユーロプライバシー認証要件への継続的遵守状況を確認することである。**再認証は、**直近の認証周期における**直近の監査報告書の結論をレビューし、考慮しなければならない。**

  

# 11. 認証範囲の拡大

本認証制度は、2 つの方法で補完的適用範囲に対応するように拡大することができる。

a) 認証拡張基準
b) ユーロプライバシー認証制度及び適用範囲の適応

## 11.1. ユーロプライバシー認証拡張基準

申請者は、補完的な EU 域外の各国データ保護規制又は他の欧州規制への遵守状況を評価するため、認証の当初の GDPR 規範的適用範囲の拡張を要請することができる。本制度オーナーは、認証機関によって評価される対応する補完的基準とともに、別の文書で各拡張を特定及び規定する。全ての拡張基準は、ユーロプライバシー・リソース＆コミュニティのウェブサイト（https://community.europrivacy.com）で利用できる。

### 11.1.1. 監査時間及び労力の適応

評価時間及び労力は、拡張なく通常の基準数と比較して、拡張によって必要となる追加の基準数に比例して、適宜適応されなければならない。例えば、評価される通常のユーロプライバシー認証が 50 の基準の評価を要求し、申請者が、評価手続に 5 の基準の追加が必要となる各国規制への認証の拡張を希望する場合、認証の費用は 10%増加されるのが望ましい。

### 11.1.2. 遵守マークへの影響

拡張基準は、次の二重認証を付与することができる。

a) 通常基準への遵守状況認証
b) 追加基準に基づく第二の遵守状況認証

各認証は、本制度オーナーが指定する異なる遵守マークで表示される。

## 11.2. ユーロプライバシー制度の適応

非 EU 管轄では、データ保護認証は、個人データ保護マネジメントシステムなど、異なる活動に適応可能である。ユーロプライバシーは、認証機関によって適用されなければならない補完的規則及び要件を規定する認証制度適応手段によって、当該適応の場合に対処することを認めている。認証制度適応は、文書「ユーロプライバシー認証制度適応一覧」に列挙されており、ユーロプライバシー・コミュニティウェブサイト（https://community.europrivacy.com）で利用できる。

認定の観点からは、認証制度適応は別個の認証制度とみなされ、本制度オーナーが規定する異なる遵守マークで表示される。

  

# 12. 構造的要件及び組織的要件

## 12.1. 組織上の構造及びトップマネジメント

ISO/IEC17065 の規則及び原則に従って、認証機関は、次の内容を含むその組織上の構造を文書化しなければならない。

a) 認証活動に関与する要員の役割及び責任
b) 次の事項を担当するトップマネジメントの権限の特定
- 次の事項の開発及び監督
    - 認証機関のマネジメントシステム
    - 認証要件
- 認証関連の方針、手続及び手順
- 認証活動
- 次の事項の十分な評価、監視及び確保
    - 要員の力量要件
    - 苦情及び異議申立てへのパフォーマンス及び対応
    - 認証活動のための資源配分
- 次の事項の決定
    - 認証の評価及びレビュー
    - 認証に関する正式な決定
- 委員会又は個人への権限の委譲
    - 契約上の取決め

### 12.1.1. データ保護オフィサー（DPO）の機能

認証機関は、データ保護オフィサーの機能に関連する義務を含む、データ保護規制の社内遵守を確保する担当者又は事務所を指定しなければならない。

### 12.1.2. 運営管理

ISO の要求事項に従い、支社若しくは第三者、又は、その両方と協働する認証機関は、自らに代わって行われる認証活動を監視し、管理する適切な手続を確立しなければならない。

## 12.2. 主要な役割及び責任

### 12.2.1. 申請者の専属的責任

認証要件の充足及び遵守の責任を有するのは、認証申請者（認証機関ではない）である。申請者は、認証を受けた評価対象が本認証制度の要件、及び、より一般的に適用可能なデータ保護規制を完全に遵守していることを確保しなければならない。

### 12.2.2. 認証機関の役割及び責任

認証機関は、本認証制度を遵守した認証決定の根拠となる十分な監査証拠を収集し、評価する責任を有する。監査結果に基づき、認証機関は、遵守状況の十分な証拠がある場合は認証を付与する決定を行い、遵守状況の十分な証拠がない場合は認証を付与しない決定を行わなければならない。

法律の範囲内において、認証機関は、認証を受けた製品、プロセス、サービス又はマネジメントシステムの使用に起因するいかなる損失又は損害に対しても、その原因の如何に関わらず、一切の責任を負わないものとする。

### 12.2.3. 本制度オーナーの役割

本制度オーナーは、本認証制度の維持及び更新、並びに、認証機関へのユーロプライバシーライセンスの付与、一時停止及び取消しを担当する。本制度オーナーは、ユーロプライバシー認証レジストリの維持、及び、本認証制度に関する公開情報にも責任を負う。認証決定（これは関連

  

する認証機関の責任である）、及び、評価対象がデータ保護規制を継続的に遵守すること（これは申請者の単独の責任である）については責任を負わない。

本制度オーナーの権利及び能力は、認証機関及びその申請者を拘束する契約上の義務において認められ、確保されなければならない。

### 12.2.4. データ保護機関の役割

GDPR 第 43 条に基づき、各国データ保護機関は、認証手続の GDPR への遵守を監視及び管理を担当する。

## 12.3. 法的事項及び契約上の事項

ISO/IEC17065 で求められるように、認証機関は、その認証活動に法的責任を負う法的組織でなければならない。

### 12.3.1. 申請者との認証契約

認証機関は、本認証制度の関連要件に基づき認証活動を提供するために、各申請者との間で法的強制力のある契約（又は一連の契約）を締結しなければならない。認証契約は、認証機関及び申請者の責任を明確にし、認証範囲に関連する申請者の全ての拠点に適用されなければならない。

### 12.3.2. 認証契約の主要な要件

ISO の要求事項に準拠し、認証契約には、少なくとも申請者に対する次の義務が含まなければならない。

a) 申請者は、**本認証制度の要件及び関連する諸条件を遵守することを誓約しなければならない。申請者は、認証を受けた評価対象が、適用可能な基準及びデータ保護規制を遵守していることを確保しなければならない**。申請者は、次の事項を行わなければならない。
   - （認証決定の如何にかかわらず、）サーベイランス監査、並びに、監査及び認証の請求書の支払を含む、**適用可能な期限及び手順を遵守することを誓約すること**
   - 本認証制度の要件及び適用可能なデータ保護規制を遵守するための**完全かつ排他的な責任を認めること**
   - **認証は、**適用可能なデータ保護規制に関する**責任を軽減するものではないことを認めること**

b) 申請者は、次の措置を含む、**認証機関の作業を支援するために必要となるあらゆる手配を講じ**なければならない。
   - 意図された認証を実施するために必要な全ての関連する取扱活動、拠点、施設、手続、手順、情報、データ及び要員に対する完全な透明性及びアクセスを許可すること
   - 関連する文書、記録、設備、場所、区域、要員及びデータ処理者などの申請者の下請業者へのアクセス、並びに、調査のためのガイドを提供し、規定を採用することを含む、評価及び監視活動の実施を支援すること
   - 認証に関するあらゆる苦情を記録し、調査すること
   - 該当する場合、オブザーバの参加を支援すること

c) 申請者は、認証機関（及び求められた場合は所轄データ保護機関）に対し、認証手続に関する関連情報を一切秘匿することなく、**明確、完全かつ透明性のある情報を提供しなければならない**。

d) 申請者は、認証を受けた評価対象の本認証制度及び本基準への**遵守を維持するため、**次の措置を含む、**必要となるあらゆる手配を講じ**なければならない。
   - 認証機関から連絡された適切な変更を実施すること
   - 継続中の認証を受けた生産、サービス提供若しくは活動、又は、その両方が、関連製品及び本認証制度の要件を継続的に充足することを確保すること。

e) 申請者は、**誤解を招くような情報発信**及び遵守マークの使用**を避けなければならない**。具体的には、申請者は、次の措置を講じなければならない。
   - 次の事項と一貫性のある認証に関する主張のみを行わなければならない。
     - 取得した有効な認証範囲

  

    - 認証機関の書面による指示及び運用指針
  - 次のおそれのある一切の態様において、認証を利用又は発信してはならない。
    - 第三者が誤解を招くおそれがある場合
    - 認証機関又は本認証制度に損害を与え、又は、評判を傷付けるおそれがある場合
  - 評価対象[20]に関連する情報を含む、認証の発信のための認証機関及び本認証制度の要件を遵守しなければならない。
  - ロゴ、認証書、遵守マークの使用のため、本制度オーナーが定める規則を遵守しなければならない。

f) 申請者は、データ侵害などのインシデントが発生した場合を含む、「***本認証制度の遵守に影響を及ぼすおそれのある変更について、遅滞なく認証機関に通知しなければならない***」[21]。

g) ***認証の一時停止、取消し又は終了の場合、申請者は、次の事項を行わなければならない。***
  - **関連する認証の利用及び発信を中止すること**
  - 本認証制度が定める**対応する義務**及び認証機関から受けた指示**を、過度な遅滞なく遵守すること**

h) 申請者は、受領した**全ての苦情を記録**し、**これに対するフォローアップ措置を文書化**しなければならない**。**

i) 申請者は、認証機関が認証手続又は認証の継続的維持に必要と認める**補完的又は追加的な監査、サンプリング、若しくは、その他の調査に同意しなければならない。**

j) 申請者は**、所見が、認証手続に対し、次を含む影響を与える可能性があることを認め、受け入れなければならない。**
  - 認証手続の延期又は取消し
  - 重大な不遵守又は評価対象の取扱いに影響を及ぼす変更があった場合、認証機関は認証手続の全部又は一部を再実施しなければならない場合があり得る。
  - 認証機関も、手配及び費用見積もりを修正する必要がある場合があり得る。

k) 申請者は**、ユーロプライバシー認証書を受領した後**、かつ、本制度オーナーが規定する使用規則を遵守している場合にのみ**、ユーロプライバシー認証書を参照し、ユーロプライバシー遵守マーク及びラベル付けを使用しなければならない。**

l) 申請者が第三者に認証文書の写しを提供する場合、当該文書は全文又は本認証制度で規定するとおりに複製されなければならない。

m) 申請者は、認証手続の管理、レビュー又は更新を目的として、機密保持の下、本制度オーナーが認証手続のために提供された情報にアクセスできることに同意しなければならず、同様の権利が認証機関の認定機関にも適用されなければならない。

n) **本契約は次の事項を明確にしなければならない。**
  - **認証の有効性、更新及び取消しに関する規則**
  - **苦情及び異議申立てのための構造及び手順**
  - **認証機関の認定が一時停止又は取り消された場合、消費者のニーズに対応するために講じる措置**

### 12.3.3. 認証決定の責任

ISO の原則に従って、**認証機関は、**認証の付与、拒否、維持、認証範囲の拡大若しくは縮小、認証の更新、一時停止若しくは一時停止後の復帰、又は、認証の取消しなど、**認証に関する決定の責任を負い、その権限を保持する。**

本制度オーナーには、個々の認証若しくは認証を受けた評価対象の不遵守、又は、その両方を積極的に監視する義務はない。ただし、認証を受けた評価対象に重大な不遵守が認められること

[20] ISO/IEC 17030、ISO/IEC Guide 23 及び ISO Guide 27 も参照。

[21] ISO/IEC 17065:2012 の第 4.1.2.2 項 k 注記を参照。かかる変更例には、生産又はマネジメントシステムに対する変更、*「法律上、商業上、組織上の地位又は所有権の変更、組織及び経営層（例えば、主要な管理層、意思決定又は専門業務に携わる要員）の変更、製品又は生産方法に対する変更、連絡先及び生産拠点に対する変更、品質マネジメントシステムの重大な変更」*が含まれる。

  

を示す証拠が本制度オーナーに提供され、かつ、認証機関が迅速にレビュー及び措置を行わなかった場合、本制度オーナーは調査を実施し、発行された認証書を一方的に一時停止若しくは取り消す権利、又は、その両方の権利を留保する。

  

# 13. 公平性及びリスクの管理

## 13.1. 公平性の義務

**認証機関は、その独立性を証明し、付与される認証との利益相反を防止するための手順を持つことを証明しなければならない。**

認証活動は、公平に実施されるものとする。**認証機関は、その公平性を損なうおそれのある申請者との過去又は現在のいかなる関係も有してはならない。**

認証機関及びそのトップマネジメントは、*「認証活動の公平性に責任を負い、公平性を損なう商業的、財務的又はその他の圧力を容認してはならない*[22]」。

**認証機関は、所轄データ保護機関に対し、その独立性を示す証拠の提出を求められる場合がある。**

## 13.2. 公平性を確保する仕組み

### 13.2.1. 公平性を確保する本仕組みの役割及び機能

*ISO の要請に基づき、「認証機関は、****その公平性を確保するための仕組みを有さなければならない****[23]」*。本仕組みの目的は、次の措置により、認証機関の公平性を改善することである。

a) 認証機関の公平性方針のレビュー及び改善
b) 認証の公平性に影響を及ぼすおそれのある潜在的又は特定された利益相反の対処及び運用指針の提供

本仕組みには、公平性を確保する機能と整合する限り、追加の業務及び責務が割り当てられてもよい。

### 13.2.2. 公平性を確保するための仕組みの形態

本仕組みは、次の要件を充足しなければならない。

a) 正式に文書化されていること
b) 構成員の多様性及び均衡を確保すること
c) 全ての機能を果たすために必要な全ての情報にアクセスできること

### 13.2.3. 本仕組みの構成

認証機関は、重要な利害関係者を特定し、招へいしなければならない。かかる利害関係者には、次の者が含まれ得る。

- 個人データ保護の専門家
- データ保護の研究者
- 認証機関の申請者
- データ保護機関などの政府規制機関の代表者
- 申請者又は認証を受けた評価対象の消費者若しくはエンドユーザー、又は、その両方
- 遵守状況評価の専門家
- 消費者団体などの非政府組織の代表者
- 監査人
- 技術専門家

本仕組みには、いずれか一つの利害関係者だけが支配的にならないように、多様な利害関係者を代表する多様な代表者を持つことが推奨される。認証機関の内部要員又は外部の要員は、単一の利害関係者とみなされる。

[22]ISO/IEC 17065:2012 の第 4.2.2 節項
[23]ISO/IEC 17065:2012 の第 5.2.1 節項

  

  

### 13.2.4. 認証機関の決定に対する本仕組みのインプットの影響

原則として、認証機関は、本仕組みが提供するインプット及び手引きを考慮し、これに従わなければならない。

ただし、認証機関の運営手順又はその他の必須要件に抵触するインプットは従ってはならない。同様に、悪影響を低減させるため、認証手続の効率性又は有効性に過大な影響を及ぼすインプットには従ってはならず、又は、適応してはならない。経営陣は、提供されたインプットに従わない決定の理由を文書化し、本制度オーナー若しくは所轄データ保護機関、又は、その両方によるレビューのために当該文書を保持しなければならない。

## 13.3. 利益相反の特定及び対処手続

認証機関は、その関係又はその要員の関係から生じる利益相反を含む、認証活動から生じる利益相反に関連するリスクを特定、分析、評価、対応、監視及び文書化する手続を持たなければならない。

### 13.3.1. 公平性への脅威の例

公平性への脅威は、次のような形態をとる場合がある。

- 自己の利害関係（認証結果に関連する経済的利益又は現物的利益を含む）
- 自己レビュー（例えば、認証機関又は監査チームのメンバーが被監査対象のためのコンサルティングに関与していた場合）
- 評価の信頼性に影響を与えるおそれのある慣れ及び慢心
- 脅威及び威圧
- 取引関係、所有関係、委託関係などの関係

### 13.3.2. 特定の制限

認証機関及び監査人は、その公平性を保持するため、次の事項を行ってはならない。

- 認証申請者に対するコンサルティング又は内部監査サービスを提供すること[24]
- 直近 24 か月以内にコンサルティングを提供した申請者の認証
- 直近 24 か月以内に内部監査を実施した申請者の認証
- 認証対象のデータ取扱いの開発、設計、製造、流通、据付け、実施、運用又は利用に関与していること
- 他の認証機関の認証

上記の制限は、認証機関による次の事項を妨げるものではない。

- 申請者と情報を共有し、初見及び期待される要件を明確化すること（要件を充足するために必要な事項を一般的な用語で説明することはできるが、特定された不遵守を解決する方法を説明することはできない）
- 評価目的の認証対象の製品の利用、据付け若しくは保守、又は、その複数

### 13.3.3. 内部監査に関する特定のリスク

認証機関が認証を付与した申請者に対して内部監査を実施することは、公平性に対する脅威を構成する。したがって、**認証機関は、認定を付与した申請者に内部監査の提案又は提供を行ってはならない**。これは、同一法人内のいかなる部分にも、認証機関の組織統制下にあるあらゆる組織にも適用される。

[24] ISO/CEI 17065:2012 の第 3.2 項及び ISO/IEC 17021:2011 の定義 3.3 参照。

  

### 13.3.4. コンサルティングに関連する特定のリスク

*「認証機関及び同一法人の一部並びに認証機関の組織統制下にある組織は、認証範囲に関連するマネジメントシステムコンサルティング又は類似のコンサルティングサービスを提案又は提供してはならない」*[25]。

同様に、認証機関は、認証機関の公平性に対する容認できない脅威を引き起こすため、**認証範囲に関連するコンサルタント業務を提供する組織に監査を委託してはならない。**これは、監査人として契約した個人には適用されない。

申請者に対してコンサルティングを提供した要員、又は、申請者の管理職を務めた要員は、コンサルティング終了後、最低2年間、当該申請者の認証活動に参加するために認証機関によって利用されてはならない。

### 13.3.5. 連結法人に関連するリスク

認証機関は、その連結法人によって認証の公平性が損なわれないよう確保しなければならない。認証機関の連結法人がコンサルティングを提供する場合[26]、又は、認証を受ける製品若しくはサービスを開発する場合、認証評価及び決定手続に直接関与する要員は、他の組織の活動に関与してはならず、また、相互に関与してはならない。

### 13.3.6. コンサルティング会社からの独立性

認証機関は、コンサルティングを提供する組織と共同マーケティングを展開し又は当該組織と関連しているように見せてはならない。認証機関は、認証機関を利用した場合に認証がより簡単、容易、迅速又は安価になることを明示又は暗示するコンサルティング組織による不適切な関連付け又は表明について、是正措置を講じなければならない。

本条項は、ユーロプライバシー関連サービス及びユーロプライバシーパートナーのエコシステム（そのサービスへのアクセスを含む）の共同プロモーションのため、ECCP が主催する共同による情報発信及びマーケティング活動への認証機関の参加を妨げるものではない。また、ECCP は、ユーロプライバシー認証制度及び認定サービスプロバイダーのエコシステムを協力、支援及び促進するため、ライセンスを取得した認証機関及びコンサルティング会社を招へいしてもよい。

## 13.4. 公平性に関連する特定の義務

### 13.4.1. 正式な公平性方針の採用義務

認証機関は、次の要素を含む書面による正式な公平性方針を採用しなければならない。

- 認証活動の実施における公平性の重要性を強調するトップマネジメントの明確なコミットメント及び表明
- 認証活動における利益相反の管理方法及び客観性の確保方法に関する明確な運用指針
- 認証機関の関係又はその要員の関係から生じる利益相反も含む、認証活動から生じる利益相反に関連するリスクを特定、分析、評価、対応、監視及び文書化する手続

認定を受けた認証機関の公平性方針は、本制度オーナーが利用できなければならない。

### 13.4.2. 公平性に関する要員の義務

認証活動に関与する認証機関の要員は、認証活動の公平性を維持及び保護しなければならない。当該要員は、認証の公平性に影響を及ぼすおそれのあるリスク又は圧力を特定した場合、認証機関に通知しなければならない。

*「認証機関は、内部及び外部の要員に対し、自身又は認証機関に利益相反を生じさせるおそれのある一切の知り得る状況を明らかにするよう要求しなければならない。認証機関は、当該要員の活動又は当該要員を雇用する組織によって生じる公平性への脅威を特定するためのインプットと*

[25] ISO/IEC 17021-1:2015 の第 5.2.5 項
[26] ISO/IEC 17065:2012 の第 3.2 項参照

  

*して、当該情報を記録及び利用し、利益相反のないことを証明できない限り、当該内部又は外部の要員を利用しないものとする"*[27]。

### 13.4.3. 公平性管理の文書化義務

認証機関が公平性への脅威を特定した場合、かかる脅威をどのように排除又は最小化する方法を文書化及び証明し、残存するリスクを文書化しなければならない。認証機関は、公平性への内外の脅威を評価し、対処しなければならない。

公平性監視報告書は、本制度オーナーがアクセスできなければならない。

### 13.4.4. 公平性問題への対応義務

認証機関は、その公平性へのリスクに対処するための措置を講じなければならない。認証機関は、その公平性に対するリスクが特定された場合、当該リスクを排除し、又は、少なくとも限定的かつ容認可能な水準まで最小化するための措置を講じなければならない。

認証機関は、他の個人、機関又は組織の行為から生じる公平性への脅威に対応するため、是正措置及び必要となる場合は法的措置を講じなければならない。

関係が公平性に容認できない脅威を引き起こす場合（認証機関の完全子会社がその親会社から認証を要請される場合など）、認証は提供されてはならない。

## 13.5. リスクマネジメント

### 13.5.1. 認証機関によるリスク分析

認証手続の公平性又は信頼性に悪影響を及ぼし得るリスクが特定された場合、必ずトップマネジメントに通知され、リスクアセスメントを実施しなければならない。リスクアセスメント手続では、公開性及び社会的認知を含む公平性に影響を与える問題について助言する適切な利害関係者への諮問を利用することができる。かかる適切な利害関係者との諮問は、特定の利益が優越することのないよう、均衡が保たなければならない[28]。

トップマネジメントは、残留リスクが許容可能なリスク水準にあるか否かを判断するため、あらゆる残留リスクをレビューしなければならない。

### 13.5.2. 申請者に関するリスクベースアプローチ

認証機関は、適切で一貫性のある公平な認証の提供に伴うリスクを考慮しなければならない。**資源及び時間の配分には、特定されたリスクを考慮するのが望ましい。**

認証手続を実行する際、データ主体にとってより重要性が高く、より重要なリスクを構成する監査事項を優先するのが望ましい。

### 13.5.3. リスクの特定、責任及び財務

認証機関は、該当する評価機関又はデータ保護機関に対し、次の事項を証明しなければならない。

- 認証手続に関連するリスクを特定、分析及び評価したこと
- 業務を遂行する地域における認証活動に関連する責任をカバーするための適切な措置を採用していること
- 財源が経済的圧力にさらされていないこと

### 13.5.4. 適用範囲の制限

認証機関は、各認証範囲を明確に規定しなければならない。

認証手順及び活動は、合意された認証範囲に焦点を当て、当該範囲を超えてはならない。

[27] ISO/IEC 17021-1:2015 の第 5.2.13 項
[28] 該当する場合、リスク分析は公平性メカニズムに委任することができる。

  

# 14. 要員及び資源の管理

## 14.1. 要員の力量

**EDPB の要請に応じて、認証機関は、次を含むデータ保護規制に関する適切かつ継続的な専門知識を有していることを証明しなければならない。**
- **GDPR の要件**
- **データ保護法の適用**
- **関連する技術的データ保護措置及び組織的データ保護措置**

### 14.1.1. 要員の定義

「認証機関の要員」とは、認証機関の権限の下で勤務する者又は契約に基づき勤務する者の一切を意味する[29]。

### 14.1.2. 要員管理手続の保持義務

認証機関は、認証手続に関与する要員が適切な知識及び技能を有することを確保するための手続を持たなければならない。認証機関は、監査人及び監査チームリーダーが一般的な監査技能及び知識、並びに、特定の技術分野の監査のために適切な技能及び知識を有することを証明できなければならない。

認証機関は、各関係者に対し、その義務、責任及び権限を明確に示さなければならない。

### 14.1.3. 力量基準

**GDPR 第 42 条に基づく認証を行う要員の能力基準は、次の要件を遵守しなければならない。**
- **EDPB の認証に関するガイドラインの一般的要件**
- **認証機関に適用可能な補完的国家固有要件**

認証機関は、認証活動に関与する要員の力量基準を確立し、評価する手続を持たなければならない。監査チームを設置する場合、力量基準は、評価対象の特定の要件を考慮しなければならない。

大企業、複数国に展開する企業、又は、特別な種類のデータを取り扱う会社の認証を担当する主任監査人には、より高度の専門知識が必要とされなければならない。

最低限の力量基準は「ユーロプライバシー認証手続に関与する要員の力量のマネジメント」と題する文書に詳細に規定されており、これは拘束力のある文書であり、認証機関はこれを尊重しなければならない。当該文書は、ユーロプライバシーの認証業務に必要となる知識及び技能の基準を文書化したものである。

### 14.1.4. 要員能力要件及び補完的な専門知識

認証機関は、本認証制度を適用し、GDPR 及びその他の補完的に適用可能なデータ保護規制の遵守状況について信頼性のある評価を提供できる認定監査人及び専門家にアクセスできなければならない。認証機関は、認証機関が業務を遂行する全ての適用分野及び地理的領域における認証活動に直接関連する事項についての助言を得るため、必要な専門知識にアクセスできなければならない。かかる専門知識は、外部から提供してもよい。

### 14.1.5. 意思決定者の能力

認証手続における意思決定に関与する者は、次の事項を証明しなければならない。
- 本認証制度を理解していること
- 監査手続の結果を評価できること

認証における意思決定の概念は、包括的なものとして理解されなければならず、認証の付与、拒否、維持、更新、一時停止及び復帰の決定、並びに、認証範囲の変更の決定も含まれる。

[29] ISO/IEC 17065:2012 の第 6.1.3 項を参照。

  

### 14.1.6. 監査人及び専門家に提供される情報及び文書

*「認証機関は、監査人（、及び、必要とされる場合、技術専門家）が監査手続、認証要件及びその他の関連要件について十分な知識をもつことを確保しなければならない。認証機関は、監査人及び技術専門家に対し、監査指示及び認証活動に関する全ての関連情報を文書化された最新の手順へのアクセスを与えなければならない"*[30]。

## 14.2. 要員の契約上の義務

### 14.2.1. 要員との契約

認証機関は、認証手続に関与する要員に対し、次の事項を誓約する契約書に署名するよう要求しなければならない。

a) 本認証制度に定める規則を尊重すること
b) アクセスした情報の機密性を保持すること
c) 利益相反を防止し、かかる相反を引き起こすおそれのある状況又は関係を表明すること

### 14.2.2. 要員の機密保持義務

認証機関を代表して行動する全ての要員は、法律又は本認証制度の規定によって求められる場合を除き、認証手続中に入手又は作成された**全ての情報の機密を保持しなければならない**。

## 14.3. 力量のマネジメント

### 14.3.1. 力量のマネジメントの手順

**認証機関は、**監査及びその他の認証活動の管理及び実施に関与する**要員の力量をマネジメントするための手順及び手続を確立し、実施及び維持しなければならない**[31]。

**認証機関は、本認証制度が定める要員の力量基準及び所轄データ保護機関が求める要件を遵守しなければならない。**認証機関は、認証手続における各機能について、本認証制度の要件に関する要員の追加の力量基準を採用してもよい。適切な場合、特定の技術分野の専門知識に関連する特定の要件を利用するのが望ましい。認証機関は、データ保護に関する必要となる専門性を確保しなければならない。

力量のマネジメントの一環として、認証機関は次の事項を行わなければならない。

a) 認証活動に関与する要員の業務遂行能力を確保するための**教育・訓練の必要性の特定及び対応**
b) 要員が責務及び責任を果たすために必要な力量を有していることの文書化及び証明
c) 要員のメンバーに対する認証関連機能を果たす正式な許可
d) 要員のパフォーマンスの監視及び評価

### 14.3.2. 選択手続

認証機関は、認証に利用する監査人及び技術専門家の選択、教育・訓練及び正式な許可のための手続を持たなければならない。監査人の初期力量評価には、監査人による監査実施の観察を含む、監査中に必要となる知識及び技能を適用する能力が含まれる。

監査人の個人的な行動は、特定の機能を果たす能力に影響を及ぼすおそれがある。認証機関は、選択及び教育・訓練手続において、個人的な行動を考慮しなければならない。認証機関は、個人的な行動の強みを活かし、弱みの影響を最小化しなければならない。

現地監査については、ISO/IEC 17021-1:2015 の附属書 D に、認証活動に関与する要員の望ましい個人的な行動に関する記述がある。

[30] ISO/IEC17021-1:2015 の第 7.2.6 項
[31] ISO/IEC 17065:2012 の第 7 節及び ISO/IEC 17021-1:2015 の第 9 項参照。

  

### 14.3.3. 評価手続

認証機関は、認証活動に関与する全ての要員の初期力量評価、並びに、力量及びパフォーマンスの継続的監視のための文書化された手続及び力量基準を持たなければならない。認証機関は、ユーロプライバシー認証のための活動のパフォーマンスに責任を負う前に、その評価方法が、要員の力量を評価及び監視し、並びに、十分な水準の力量を有する要員を選択していることを確保するために効果的であることを証明しなければならない。

### 14.3.4. 要員記録

認証機関は、監査人、専門家及び管理要員を含む、ユーロプライバシー認証に関与する全ての要員の最新の記録を保持しなければならない。

ISO/IEC の要求事項に従って、要員記録には、次の情報を含めるのが望ましい[32]。

a) 個人情報（氏名、住所など）
b) 職歴（雇用主、役職など）
c) 教育及び資格
d) 経験及び補完的な教育・訓練
e) 力量の評価
f) パフォーマンスの監視
g) 認証機関が保有する機能及び権限
h) 各記録の最終更新日

### 14.3.5. 要員の全体的なパフォーマンス

認証機関は、要員の力量及びパフォーマンスを監視及び文書化しなければならない。また、定期的に力量をレビューし、教育・訓練の必要性を特定しなければならない。

認証機関は、監査人の力量を監視する際、次の事項を行わなければならない。

- 定期的に各監査人の現地でのパフォーマンスを評価すること
- 現地評価、監査報告書のレビュー及び申請者（又は関連する利害関係者）からのフィードバックを組み合わせること
- 認証手続及び申請者への影響又は障害を最小化すること

## 14.4. 評価のための外部資源の活用

### 14.4.1. 一般的義務

認証機関が外部資源を活用して評価活動を実施する際、当該外部資源は、公平性の要件を含む本認証制度の要件を遵守しなければならない。

### 14.4.2. 個別の外部監査役及び外部技術専門家の活用

認証機関は、全ての外部監査人及び外部技術専門家に対し、次の事項を誓約する同意書に署名することを要求しなければならない。

a) 認証機関の規則、手続及び手順を遵守すること
b) 機密性及び公平性を保持すること
c) 認証機関に対し、監査対象となり得る組織との既存又は過去の関係を通知すること

### 14.4.3. 外部委託の概念の明確化

ISO9001:2008 の第 4.1 項は、外部委託手続を*「組織がその品質マネジメントシステムのために必要で、かつ、組織が外部者に実施させることを選択した手続」*と定義している。「外部委託」と「下請」という用語は、しばしば同義語とみなされる。ただし、「外部委託」は、第三者から認証機関に請求される場合であっても、認証機関の直接の権限の下で作業を行うために個別に契約された外部要員の活用を意味するものではない。

[32] ISO/IEC17065:2012 の第 6 節参照。

  

### 14.4.4. 外部委託の活用

認証機関は、次の要件を含む本認証制度の適用可能な要件を充足する機関に対してのみ、評価活動を委託してもよい。

- **データ保護に関する適切な水準の専門知識**
- 公平性及び機密保持の要件
- 製品、プロセス及びサービスに関連するデータ取扱いを認証する際に適用可能な ISO/IEC 17065 の要求事項

これには、他の認証機関へのアウトソーシングも含まれる。

### 14.4.5. 意思決定の外部委託の禁止

認証に関する全ての決定（第 6.3 節を参照）は、認証機関の直接かつ効果的な管理下になければならず、外部に委託することはできない。

### 14.4.6. 外部委託に必要となる手続及び契約

認証機関は認証活動に利用する外部委託業務の提供者の承認及び監視のための手続を持たなければならない。また、認証機関は次の事項を行わなければならない。

- 十分な専門知識を有することの確保
- 認証活動に関与する全ての要員の力量の記録保持の確保
- 確認されたサービス提供者の文書化された記録を保持すること[33]
- 認証を受ける申請者との関係及び公平性の問題を表明する義務を含む、機密保持及び利益相反に関する適切な定めを設けた法的強制力のある契約を締結すること

認証機関は、政府機関、認定機関又は同等性評価機関など、第三者の監視及び評価に依拠することができる。

### 14.4.7. 外部委託における認証機関の責任

**認証機関は、外部委託した活動に対する責任を保持する。認証機関は、外部委託した業務を担当する機関が、力量、公平性及び機密保持の観点を含め、本認証制度を遵守し、適用可能な ISO 要求事項に適合していることを確保しなければならない。**

[33] また、ISO/IEC 17065:2012 の第 6.2.2.4 項は、*「契約又はその他の要求事項の違反を認識した場合、是正措置を実施すること」*、及び、*「申請者に異議を唱える機会を提供するため、外部委託活動前に申請者に通知すること」*を要求している。

  

# 15. 情報管理及び機密保持

本節は、認証機関に適用される。

## 15.1. 文書の管理及び分類

*「**認証方法は、標準化された文書化手法を提供するのが望ましい。**その後、評価によって、認証文書及び現地の実際のステータス、並びに、認証基準との比較が可能になる。…したがって、評価中に作成される文書は、次の 3 つの主な点に焦点を当てるのが望ましい。*
***-実施された評価方法の一貫性及び整合性***
***-認証対象が**認証基準、ひいては本規則を**遵守していることを証明するための**評価方法*
*-評価結果が**独立かつ公平な認証機関によって承認された**こと（EDPB ガイドライン 1/2018）*

### 15.1.1. 文書分類の目的

認証機関は、文書ごとの明確かつ一貫性のある分類及び識別を使用しなければならない。ユーロプライバシー関連文書の識別及び分類は、次の点を確保にするために構成されなければならない。

- 詳細に規定された信頼性のある認証手続
- 更新された情報及び文書への明確かつ利用者に分かりやすいアクセス

## 15.2. 情報の機密保持及びデータ保護

### 15.2.1. 機密保持義務及びデータ保護

認証機関は、認証手続中に収集若しくは作成された情報、又は、その両方を適切に管理し、保護する責任を負う。

認証機関及び認証手続に関与する全ての関係者は、個人データを保護し、GDPR 及びその他の適用可能なデータ保護規制の規定を完全に遵守しなければならない。

認証機関は、当該機関及び代理人が上記の義務を遵守することを確保するため、十分な契約上の措置を講じなければならない。

### 15.2.2. 機密保持のための要員の義務

認証活動に関与し、又は、内部情報を利用できる全ての要員は、認証に関連する全ての機密情報の機密性を保持し、保護しなければならない。

### 15.2.3. 機密保持の適用範囲

**原則として、申請者から提供され、又は、申請者及びその認証に関連する全ての**情報は、次のいずれかの情報を除き、**機密情報として取り扱われなければならない。**

- 公開されている情報
- 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、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、データ保護機関などの権限を有する者による情報への正当なアクセスを妨げるものではない。

### 15.2.4. 機密情報への正当な第三者によるアクセス

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、かかる要請に従わなければならない。

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してもよい。正当な理由がある場合、認証機関は、アクセスする当事者が機密保持義務を負うことを条件として、要請された情報への十分かつ比例的なアクセスを提供しなければならない。

  

認証手続の通常のサーベイランス及び監視の一部である情報へのアクセスは、申請者への特別な通知を要求しない。その他の場合は、法律で禁止されていない限り、申請者に通知されるのが望ましい。

### 15.2.5. 機密保持及びプライバシーを遵守するインフラストラクチャ

**認証機関は、申請者の情報の安全かつ機密保持された取扱いを確保しなければならない。認証機関は、次を持たなければならない。**

**a)** 申請者の**機密情報**及び記録を、**安全に記録保存、取扱い及び送信するための十分なインフラストラクチャ**
**b) データ保持及び個人データ最小化に関する文書化された方針及び手順**
**c) ウェブサイトで利用できるプライバシー及びデータ保護ポリシー**

情報の機密性を保持する契約上又は法律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なければならない。

認証機関は、そのオンラインツール及びウェブサイトが GDPR を遵守していることを確保しなければならない。

## 15.3. 認証機関及び申請者間の情報交換

### 15.3.1. 申請者に提供される初期情報

認証機関は、次の内容を含む明確な情報を申請者に提供しなければならない。

a) 次のいずれかの内容を含む**認証手続の記述**
  - 申請
  - 監査及び評価（該当する場合、サーベイランス監査を含む）
  - 認証書の発行、拒否、維持、更新、一時停止、取消し及び復帰の決定手続
  - 認証範囲の拡大又は縮小の手続
b) 認証の**引用規範**及び規範的要件
c) **申請者の費用及び料金**に関する情報（認証の維持及び再認証を含む）
d) 次を含む**申請者の義務**
  - **本認証制度の規則及び要件を遵守すること**
  - **認証機関の作業を容易に**し、手続の全段階において、全ての関連分野、文書、ファイル及び要員への十分なアクセスを提供**するために必要となるあらゆる手配を行うこと**
  - 監査人の作業を評価するためのオブザーバの参加を許可すること
e) 認証の連絡時を含む、**認証を受けた申請者の権利及び義務**に関する情報
f) **苦情及び異議申立て**に関する情報及び連絡先

### 15.3.2. 業務及び責任に関する文書及び情報

**認証機関は、次の目的のため、申請手続を含む、認証活動に関する業務及び責任の文書を保管しなければならない。**
- 申請ステータスに関する情報
- 所轄データ保護機関による評価

### 15.3.3. 認証機関による変更の通知

本認証制度は、法学の進展を含む変更の可能性がある欧州データ保護規制に対応するために開発された。技術的進化も、本認証制度によって必要となる技術要件及び評価基準に影響を与える場合がある。同様に、本認証制度の要件も時間とともに進化することが予想される。

本制度オーナーは、国際専門家委員会の支援を受けて、本認証制度の必要な適応を決定するものとする。

本認証制度の変更が本制度オーナーにより採択された場合、認証機関は、申請者の認証を受けた評価対象が新しい要件を遵守していることを検証しなければならない。

  

認証機関は、認証を受けた申請者に対し、当該認証に影響を及ぼすおそれのある認証要件の変更について適切に通知し、新たな要件に関する情報を提供しなければならない。

### 15.3.4. 認定を受けた申請者による変更の通知

認証機関は、認証を受けた評価対象が本認証制度の要件の遵守を継続する能力に影響を及ぼすおそれのある変更について、認証を受けた申請者から遅滞なく通知を受けるための十分な契約上の取決めを確立しなければならない。これには、次の事項に関連する変更が含まれる。

a) データ取扱いの目的及び適用範囲の拡大
b) 評価対象において取り扱われる個人データの種類の拡大
c) 評価対象に関与する新たなデータ処理者
d) 新しい拠点の場所（個人データを取り扱い又は記録保存するサーバーインフラストラクチャの地理的場所を含む）
e) 個人データの新たな越境移転
f) 重要な法的、商業的、組織的変更（申請者若しくは認証を受けた評価対象、又は、その両方の効果的な管理若しくは保有権、又は、その両方の変更を含む）
g) 認証を受けた評価対象に影響を及ぼすおそれのある重要な組織的決定及び管理上の決定（データ保護オフィサーの変更など）
h) 該当する場合、認証を受けた評価対象における業務の適用範囲
i) 認証を受けた評価対象に対する重大な変更（新たなバージョンの公開など）
j) 連絡先

かかる変更が生じた場合、認証機関は、次の措置を含み得る適切な措置を講じなければならない。

a) 評価
b) レビュー
c) 認証決定
d) 認証範囲を拡大又は縮小するために改訂された正式な認証文書（監視又はサーベイランス活動を含む）の発行

記録には、上記の活動のいずれかを除外した場合のフォローアップ措置及び根拠を含めなければならない。

## 15.4. 公開情報

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則を持たなければならない。

### 15.4.1. 要請なく利用可能な公開情報

認証機関は、その業務を遂行する全ての地域的領域において、**要請なく**、次の事項に関する一般的な情報を保管し、（出版物、電子媒体又はその他の手段を通じて）公開しなければならない。

a) 認証評価手続
b) 認証及び認証範囲に関する決定手続[34]
c) 認証を受けるデータ取扱活動の種類
d) 付与された認証に付された名称、ロゴ及び遵守マークの使用
e) 情報の要請、苦情、不服申立てを取り扱うための手続
f) 公平性方針及び公平性メカニズム
g) 認証機関の連絡先の詳細（郵便住所など）
h) 認証機関の個人データ保護ポリシー及び個人データ保護オフィサーへの連絡方法

[34] 例えば、認証の付与、拒否、維持、更新、一時停止、復帰、取消し、又は、認証範囲の拡大若しくは縮小の決定など。

  

### 15.4.2. 要請に応じて利用可能な情報

ISO の要求事項に従い、認証機関は**要請に応じて**次の項目に関する補足情報を提供しなければならない。

*a) 認証機関が業務を遂行する地理的領域*
*b) 特定の認証のステータス*
*c) 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（都市及び国）*[35]
*d) 評価手順、規則、認証の付与、維持、適用範囲の拡大若しくは縮小、一時停止、取消し又は拒否の手順を含む本認証制度に関する情報（又は本認証制度への参照）*
*e) 認証機関が財務的支援を受ける手段の記述、並びに、申請及び申請者に課される料金に関する一般的情報*
*f) 認証機関の名称及び認証マークの使用に関する要件、制約又は制限、並びに、付与された認証の言及方法に関する要件、制約又は制限を含む、申請者、並びに、申請者の権利及び義務の記述*
*g) 苦情及び異議申立ての取扱手順に関する情報"*[36]

認証機関は、利害関係者に対し、当該情報を書面にて郵便で要請し、返信に使用できる電子メールアドレスを記載することを要求してもよい。

特定の情報へのアクセスは、申請者の要請（セキュリティの理由など）又は機密保持若しくはデータ保護の理由により、正当な利益によって制限されることがある。

また、認証機関は、そのインターネットウェブサイトで、要請なく当該情報を公開することができる。

### 15.4.3. 共通レジストリ及び公開情報ウェブサイト

本制度オーナーは、公式引用文書を含むユーロプライバシー公式ウェブサイト、並びに、ユーロプライバシー認証レジストリの管理及び監視を担当する。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る。

認証機関は、その申請者及び認証手続の情報を中央レジストリに更新し、情報更新の遅延を避けなければならない。

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らない。

### 15.4.4. 情報の信頼性

広告を含む認証機関が申請者又は市場に提供する情報は、正確かつ誤解を招かないものでなければならない。商標及びロゴを含むユーロプライバシー関連の標章の使用は、マーケティング及び情報発信に関するユーロプライバシー規則及びガイドラインを尊重しなければならない。

## 15.5. 認証手続の記録保存義務

### 15.5.1. 記録保管義務

認証機関は、全ての認証手続の要件を有効に充足していることを証明するための記録を保管しなければならない。認証機関は、当該記録が、機密保持が確保された方法で移送、伝送及び記録保存されることを確保しなければならない。

### 15.5.2. アクセスの権利

本制度オーナー、及び、該当する場合、データ保護機関若しくはライセンス取得機関、又は、その両方は、サーベイランス及び苦情管理などの責務を果たすため、機密情報及び記録へのアク

[35] ISO/IEC 17021-1:2015 の 第 8.1.2 項 a～c 参照
[36] ISO/IEC 17065:2012 の第 4.6 項 a ～ d

  

セスを要請することがある。認証機関は協力し、求められた情報へのアクセスを提供しなければならない。

### 15.5.3. 保持期間

**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 10 年間加えた期間保持されなければならない**。保存期間は、法令で求められる場合、又は、法的リスクの軽減若しくは想定される再認証の文脈において過去のデータにアクセスする必要性がある場合など、認証機関の正当な利益に対応するため、延長されることがある。保持期間を延長する場合、その根拠は認証機関によって記録されなければならない。保持期間の終了時、記録は消去されなければならない。

## 15.6. 認証及び遵守マーク、ライセンス、認証書の使用への参照

### 15.6.1. 認証書、ラベル、遵守マークの使用

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あり、引き続き本制度オーナーの財産であり続けなければならない。申請者は、認証機関による承認後、認証機関の監督の下でのみ、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る。

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らない。**主な規則は本制度オーナーによって規定され、認証機関によって規定される追加規則で補完することができる。

遵守認証書は、次の事項を遵守しなければならない。

- 本認証制度及び評価対象に関する**明確な情報を提供する**こと
- 認証範囲に関する**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**

**認証範囲については、一切の曖昧さも存在してはならない。例えば、認証を受けたデータ取扱いを用いて会社全体が認証されていると主張することは禁止されており、認証書の一時停止又は取消しにつながる場合がある。**

ユーロプライバシー認証書及び遵守マークの使用に関する詳細な規則及び仕様は、全当事者が尊重しなければならない拘束力ある文書「ユーロプライバシーロゴ、認証書及び遵守マークの使用に関する規則」に定められている。

### 15.6.2. 適正使用の管理権

認証機関及び本制度オーナーは、ライセンス、認証書、遵守マーク及び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する。

認証機関は、「*認証制度への不適切な参照、ライセンス、認証書、マーク、又は、製品、プロセス若しくはサービスが認証されていることを示す可能性のある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*」[37]を確認しなければならない。かかる事態が生じた場合、認証機関による適切な処理により対処されるのが望ましい。

### 15.6.3. 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ロゴは、次の例のように、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る。

[37] ISO/IEC 17065:2012 の第 4.1.3.2 項

  


*図 8 ユーロプライバシーロゴ及び遵守マーク*

ユーロプライバシーという用語及びロゴは、本制度オーナーの商標である。その使用には、書面による許可及び厳格な規則が適用される。

### 15.6.4. 認証書

***「GDPR に基づく認証書、シール又はマークは、認定認証機関又は所轄監督機関による、認証基準を充足することを示す証拠の独立した評価後にのみ発行することができる。」***（出典：EDPB ガイドライン 1/2018）

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。認証書には、少なくとも次の事項が含まれなければならない。

a) **認証機関のロゴ及びユーロプライバシーロゴ**
b) **申請者の名称**
c) 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**のいずれの立場で行動しているか
d) 該当する場合、**共同管理者の名称**
e) **評価対象**及びその**地理的範囲の**明確な**記述**
f) 該当する場合、認証に適用された**拡張**
g) **認証書の発行日及び有効期限**
h) 発行された認証書の**固有識別子**
i) 「*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ユーロプライバシー認証オンラインレジストリのドメイン名（http://www.europrivacy.com）
j) 認証書を発行する**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らない。1 ページを超えないのが望ましい。

### 15.6.5. 遵守マーク

該当する場合、認証を受けたデータ取扱いには、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る。

遵守マークは常に次の事項を含まなければならない。

a) ユーロプライバシーロゴ
b) 固有認証識別子
c) 固有識別子により、発行された認証書の詳細な情報を含む**オンラインユーロプライバシー認証レジストリにアクセス**できる本認証制度ウェブサイトのドメイン名（http://www.europrivacy.com）

拡張基準の遵守マークは、本制度オーナーによって規定され、関連する規範拡張を明示する。

次に遵守マークの例を示す。


*図 9 遵守マークの例*

  

### 15.6.6. 遵守表明

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る。

本表明には、常に次の事項を含めなければならない。

a) ユーロプライバシーへの参照、及び、許可されている場合はユーロプライバシーロゴ
b) 認定を受けた申請者の名称
c) 該当する場合、共同管理者の名称
d) 評価対象及びその地理的適用範囲の明確な表示
e) 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
f) 認証書の発行日及び有効期限
g) 発行された認証書の固有識別子
h) 「*詳細はこちら（Detailed information at）*」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ユーロプライバシー認証レジストリのドメイン名（http://www.europrivacy.com）
i) 認証書を発行する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、任意に付与される場合、遵守表明にはその旨が明記されなければならない。**

次は認証表明の例である。

**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<br>567 Address street<br>2222 City, Country |

**Signature**

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

*図 10 認証表明*

### 15.6.7. 電子媒体に表示される遵守表明及び遵守マーク

ユーロプライバシー認証に関連する認証書、表明又は遵守マークが、ウェブページ又は PDF 文書などの電子媒体上に表示される場合、本認証制度のメインホームページ（http://www.europrivacy.com）、又は、オンラインレジストリ内の認証を受けた評価対象の特定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。

  

### 15.6.8. 認証書及び遵守マークの使用制限

**遵守マーク、認証書及び認証表明は、言及される認証の評価対象について混乱又は誤解を招く発信方法で使用してはならない。**

### 15.6.9. 申請者の契約上の義務

認証機関は、法的強制力のある合意により、認証を受けた申請者に対し、次の措置を講じることを要求しなければならない。

a) 認証に関する発信を行う際、本認証制度の要件及び認証機関の指示を遵守すること
b) 認証の有効な適用範囲及び実際のステータスを含む、認証に関する誤解を招く情報発信を防止し、排除すること[38]
c) 付与された認証に関連して遵守マークを使用する前に、認証機関の承認を受けること
d) 認証の適用範囲の縮小、一時停止又は取消しなど認証の変更が発生した場合、当該認証を参照する情報発信資料の使用を修正又は中止することにより、遅滞なく情報発信内容を適応させること
e) 認証機関及び本認証制度の評判及び信頼性を損なうおそれのある方法で認証を利用しないこと

### 15.6.10. データ輸入者として行動する申請者のための追加表明

**十分性認定を受けていない第三国に所在する申請者がデータ輸入者として行動する場合、認証機関及び申請者は、評価対象に適用可能な法令及び実務が、申請者による認証に基づく義務の履行を妨げる可能性があると信じる理由がないことを書面により表明しなければならない。**

### 15.6.11. 認証機関の管理

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、*「認証ステータスへの不適切な参照、又は、認証文書、マーク若しく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」なければならない。かかる措置には、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、及び、必要な場合は法的措置が含まれ得る*[39]。

本制度オーナーは、認証機関に対し、誤用又は潜在的な不遵守のケースを調査するよう要請することができる。認証機関は、その後、不当な遅延なく対応しなければならない。

認証を受けた評価対象に重大な不遵守が認められ、又は、本認証制度の評判及び信頼性に悪影響を与えるおそれがあるという事実に関する証拠がある場合、本制度オーナーは、認証機関の同意なく、認証の一時停止若しくは取消し、又は、その両方を行う暫定的又は例外的措置を講じることができる。

[38] さらに、ISO は、製品及びプロセス認証、並びに、マネジメントシステム認証の間の曖昧さを避ける認証に関する情報発信を明示的に要求する。
[39] ISO/IEC 17021-1:2015 の第 8.3.5 項

  

# 16. 認証機関の品質マネジメント

ISO/IEC 17065 又は 17021-1 に基づく有効かつ継続中の国家認定を受けている認証機関は、本節の要件を遵守しているとみなされる。

## 16.1. 認証機関のマネジメントシステム要件

認証機関は、ISO/IEC 17065 で提案されている次の 2 つの選択肢のいずれかに従い、本認証制度の要件を遵守する十分なマネジメントシステムを確立及び維持しなければならない。

a) オプション A：認証機関は、次を含むマネジメントシステムを確立しなければならない。
   - マネジメントシステムの明確な文書
   - 文書及び記録の効果的な管理
   - 年次内部監査
   - 年次マネジメントレビュー
   - 是正措置及び予防措置

b) オプション B：認証機関は、ISO9001 の要求事項に準拠したマネジメントシステムを確立しなければならない。認証機関は、当該要求事項の一貫した準拠を証明することができなければならない。

*「認証機関の認定が一時停止又は取り消された場合の手順は、消費者への通知を含め、認証機関のマネジメントシステムに組み込まれなければならない。(EDPS)」*

## 16.2. オプション A の具体的要件

### 16.2.1. マネジメントシステム文書

マネジメントシステム文書は、本認証制度の要件を遵守するため、全ての関連文書（手続及び記録を含む）を参照しなければならない。

認証機関のトップマネジメントは、次の事項を行わなければならない。

a) 本認証制度の要件を遵守するための一連の**方針及び目標**を採用し、維持すること
b) 当該方針及び目標が、**認証活動に関与する全ての人々による認知**、組織全体における**効果的な実施**を確保すること[40]
c) マネジメントシステムの改善及び遵守への**コミットメントを示す証拠を提供すること**
d) 次の目的のため、**責任者を任命すること**
   - *「マネジメントシステムに必要な手続及び手順の確立、実装及び維持を確保すること*
   - *マネジメントシステムのパフォーマンス及び改善の必要性について、トップマネジメントに報告すること」*[41]

### 16.2.2. 文書管理

認証機関は、認証活動に関連する文書を管理し、本認証制度を遵守するための手順を持たなければならない。これは、形式及び媒体を問わず、全ての関連文書が含まなければならない。

当該手順は、次の措置のために必要となる管理を決定し、規定しなければならない。

a) 文書の正式な承認（発行前若しくは効力発生前、又は、その両方）
b) 次を含む文書の改訂、更新及び再承認
   - 文書の改訂及び現在の改訂状況を示すこと
   - 適用可能な文書の全ての関連するバージョンを利用可能にすること
   - 廃止文書が誤って使用されないようにするとともに、適切な識別を適用すること
c) 次の事項を確保すること
   - 文書は読みやすく、容易に識別可能であること

[40] ISO/IEC 17065 によれば、認証活動に関与する全ての要員は、マネジメントシステム文書及び関連情報の自身の責任に該当する部分にアクセスできなければならない。
[41] ISO/IEC 17065:2012 の第 8.2.3 節

  

- 外部文書は識別され、その配布が管理されていること

### 16.2.3. 記録の管理

認証機関は、監査記録の識別、保管、保護、検索、保持期間及び廃棄を含む、監査記録の管理及び統制方法について規定した手順を整備しなければならない。

### 16.2.4. マネジメントレビュー

認証機関のトップマネジメントは、マネジメントシステムの十分性及び有効性を少なくとも年 1 回レビューするための手順を持たなければならない。

#### インプットのレビュー

マネジメントレビューへのインプットには、次に関連する情報が含まれなければならない。

a) 内部監査及び外部監査の結果
b) 認証活動の利用者からの関連する異議申立て及び苦情に関する情報
c) 次から受け取ったフィードバック
   - 申請者
   - 本制度オーナー若しくはその他の適格な当局、又は、その両方を含む関係利害関係者
   - 公平性確保の仕組み
d) 次の事項のレビュー
   - 公平性
   - 異議申立て及び苦情
   - 要員の資格及び教育・訓練の必要性
   - 予防措置及び是正措置
   - 前回のマネジメントレビューからのフォローアップ
   - 目標の達成状況
   - マネジメントシステムに影響を及ぼし得る変更

#### アウトプットのレビュー

マネジメントレビューには、次の措置のための決定及び措置が含まれなければならない。

a) マネジメントシステム及びその手続の有効性の改善
b) 本認証制度の遵守及び実装の改善
c) 資源の必要性の評価

### 16.2.5. 内部監査

認証機関は、確認及び改善を目的として、年次内部監査[42]の手順を確立し、実施しなければならない。

a) 本認証制度の要件遵守
b) マネジメントシステム

認証機関は、前回の監査結果を考慮した監査プログラムを計画しなければならない。認証機関は、次の事項を確保しなければならない。

a) 内部監査人は認証、監査及び本認証制度の要件の十分な知識を持つこと
b) 内部監査人は自身の業務を監査しないこと
c) 監査領域の責任者は、監査結果を通知されること
d) 監査の結果として適切な措置が適時適切に実施されること
e) 改善のための適切な機会を特定すること

監査人は、全般的な評価及び特定された相違点を含む総合監査報告書を作成しなければならない。特定された相違点は、改善のための書式に記載されなければならない。

### 16.2.6. 是正措置及び予防措置

認証機関は、**不遵守を管理**し、有効又は潜在的な不遵守の原因を排除するために適切な措置を講じるための**手順を持たなければならない**。

[42] ISO 19011 は、内部監査を実施するための運用指針を提供している。

  

ISO/IEC 17021-1 の要求事項に基づき、次の手続を持たなければならない。

*a) （苦情及び内部監査などからの）不遵守の特定*
*a) その原因の決定*
*b) 特定された不遵守の是正*
*c) 不遵守の再発防止を確実にするための措置の必要性の評価*
*d) 必要な措置の決定及び適時の実施*
*e) 講じられた措置の結果の記録*
f) *是正措置の有効性のレビュー*[43]

### 16.2.7. 方針レビュー会議

年に一度、認証手続に関与する全従業者は、本認証制度の実装状況及び品質マネジメントをレビューするための会議を開催しなければならない。役員は、方針レビュー会議への出席を招へいされなければならない。

方針レビュー会議は、その議題において、次の事項を審議しなければならない。

a) 前回の方針レビュー会議の行動項目のフォローアップ
b) 苦情、不服申立て、不遵守及び例外
c) 品質マネジメントシステム
d) 要員の監視及び能力構築
e) ICT インフラストラクチャ及びセキュリティ
f) 外部情報及び情報発信

方針レビューは、適切な場合には次の項目を含む、総合報告書を作成しなければならない。

a) 予防措置及び改善措置を含む行動計画
b) 品質マネジメント計画
c) 要員の必要性の評価（採用及び教育・訓練など）
d) ICT インフラストラクチャセキュリティ強化のための推奨

[43] ISO/IEC 17065:2012 の第 8.7.4 節

  

# 17. 異議申立て及び苦情

ISO/IEC 17065 又は 17021-1 に基づく有効かつ継続中の国家認定を受けている認証機関は、本節の要件を充足しているものとみなされる。

## 17.1. 一般原則

決定に対する異議申立ては、申請者から当該決定を行った認証機関に対し、又は、認証機関から当該決定を行った本制度オーナーに対し行うことができる。

第三者が、認証を受けた評価対象が本認証制度又は認証認証書の対象である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る。苦情は、事実認定及び証拠に基づかなければならない。

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らない。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なければならない。

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、当該問題を本制度オーナーに通知するよう求められる。

## 17.2. 異議申立て及び苦情取扱方針

認証機関は、苦情又は不服申立てを収集、文書化及び対処するための明確な仕組みを持たなければならない。

苦情又は異議申立て、調査及び決定は、認証機関が苦情又は異議申立者に対し差別的措置を講じる結果となってはならない。

苦情及び異議申立ての仕組みは、次の事項を規定しなければならない。

a) **苦情又は異議申立者**（少なくとも、公的機関及び認証を受けた評価対象によって個人データが取り扱われるデータ主体を含む）
b) 次を含む、**異議申立て及び苦情の受領、妥当性の確認、調査及び取扱手続**
   - 苦情又は異議申立てが認証機関によって付与された認証に関連しているか否かを確認するための手順及び期限
   - **利害関係者の諮問の可能性**
   - **該当する場合、期限**
c) 認証機関を代表して手続を担当する者
d) **異議申立て及び苦情**、並びに、それらを解決するために講じられた措置**を体系的に記録、文書化及び監視する手続**
e) **適切な是正措置が講じられることを確保する手続**

本制度オーナーは、苦情及び異議申立てを取り扱うための補完的手続及び仕組みを確立することができ、当該手続及び仕組みは認証機関及び申請者によって支援され、尊重されなければならない。

### 17.2.1. 苦情及び異議申立ての収集及び文書化義務

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う。

認証活動に関連する苦情又は提訴を受領した場合、認証機関は次の事項を行わなければならない。

a) 正式な苦情又は異議申立て受領の確認
b) 全ての関連情報の収集及び検証
c) 苦情申立人又は異議申立人に対する手続の結果の正式な通知
d) 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の実施

  

e) 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

### 17.2.2. 取扱義務及び善管注意義務

苦情が妥当であると認められる場合、認証機関は当該苦情に適切に対処し、その解決に合理的な努力を行わなければならない。

申請者及び認証機関は、苦情を取り扱い、解決するため、調査及び説明を行うための全面的な支援を提供しなければならない。根拠のある苦情は、認証書の一時停止又は取消しにつながり得る。

### 17.2.3. 中立的な人物を起用する義務

公平な手続を確保するため、苦情又は異議申立てに関する決定は、次の個人によって採択されなければならない。

- 関連する認証手続には直接関与していない者[44]
- 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

[44] ISO/IEC 17065:2012 の第 7.13.5 節を参照

  

# 18. 制度オーナー

## 18.1. 本制度オーナーの役割

本制度オーナーは、次の事項を担当する。

a) 本認証制度、確認項目及び管理項目、並びに、規約その他の関連文書を維持、更新及び改善すること
b) 本認証制度に関する情報の公開を維持すること
c) 認証機関によって提供される、公式ユーロプライバシー認証オンラインレジストリを維持し、利用可能にすること
d) 関連料金を含む、本認証制度のライセンス及び利用に関する利用条件を定めること
e) 本認証制度及び関連する知的財産権（ブランド及び遵守マークなど）の使用に関するライセンスを付与し、該当する場合、かかる権利の停止又は取消しを行うこと
f) 本認証制度を適用する専門家を教育・訓練し、認定を付与すること

法律によって次の権限の一部又は全部が官庁に留保されている場合を除き、本制度オーナーは、次の措置によっても介入することができる。

g) ユーロプライバシー認証に関する苦情の対処及び調査
h) 認証機関の本認証制度への遵守状況の監視
i) ライセンスを取得した認証機関間の協力、並びに、経験及び情報交換の促進
j) 次のいずれかの認証の一時停止若しくは取消し、又は、その両方
   - 本認証制度に遵守していない認証機関から付与された認証
   - 受益者によって欺瞞的に入手又は利用された認証
   - 本認証制度の評判を傷付ける可能性のある方法で利用されている認証
k) その他、本認証制度が必要若しくは有用、又は、その両方とみなす関連する措置

本制度オーナーは、認証の一時停止、取消し又は無効化のために事後的に介入することができるが、認証の手続及び決定については一切責任を負わず、これらの責任は認証機関のみが負う。本制度オーナーは、認証手続における不履行若しくは誤り（これは認証機関の責任である）、又は申請者の不遵守について責任を負わない。データ保護規制及び本認証制度の遵守は、認証を受けた申請者のみが責任を負う。全てのユーロプライバシー認証制度の利用者は、本制度オーナーがライセンスを取得した認証機関の不履行又は認証を受けた申請者の不遵守について責任を負わないことを承諾しなければならない。

本制度オーナーは、認証機関に対し、提供したサービスの料金を請求してもよい。

## 18.2. 国際専門家委員会

本制度オーナーは、データ保護、サイバーセキュリティ及び認証の専門家を集めた国際専門家委員会を設置しなければならない。国際専門家委員会は、次の事項において、本制度オーナーを支援しなければならない。

a) ユーロプライバシー認証制度の見直し、維持及び更新
b) 本制度オーナーから本委員会に送信した質問への対応
c) 本制度オーナーから求められた場合、公平性メカニズムとしての役割を果たすこと

## 18.3. 認証のための GDPR の特定要件の遵守

本認証制度は、GDPR 第 42 条及び第 43 条の認証に関する具体的な条項を含む、GDPR の要件を遵守しなければならない。

### 18.3.1. データ保護機関との協力

本制度オーナーは、関連するデータ保護機関に通知し、緊密な協力関係を維持するのが望ましい。

  

### 18.3.2. 欧州データ保護会議

本制度オーナーは、欧州データ保護会議の決定及びガイダンスを参照し、これらに従わなければならない。

### 18.3.3. 欧州委員会の規則

欧州委員会は、認証方法、データ保護シール及びデータ保護マークのための技術基準、並びに、認証方法、データ保護シール及びデータ保護マークを推奨し、周知するための仕組みを定める規則を採択してもよい。

### 18.3.4. 責任

認証は、適用可能なデータ保護規制の遵守に関するデータ管理者又はデータ処理者の責任を軽減するものではなく、所轄データ保護機関の職務及び権限を妨げることなく提供される。

## 18.4. 認証制度文書の改善

### 18.4.1. 認証制度の改善

本制度オーナーは、国際専門家委員会の支援を受けて、本認証制度の定期的な変更及び改善を主導しなければならない。

***認証機関は、「法的枠組みの変更、関連するリスク、最新技術、並びに、技術的措置及び組織的措置の実施費用に伴い」、評価方法の変更及び更新の手順を確立しなければならない（EDPB）。***

### 18.4.2. 改善提案

認証機関及びその監査チームは、適切な改善提案を収集し、本制度オーナーに連絡しなければならない。当該提案は、本制度自体、若しくは、詳細な確認項目及び管理項目、又は、その両方に関するものである場合がある。本制度オーナーは、受領した提案を収集及び整理し、ユーロプライバシー国際専門家委員会で議論するために最も適切なものを選択し、本認証制度の変更で考慮するのが望ましい。

### 18.4.3. 文書の改訂又は追加

必要に応じ、本制度オーナーは、国際専門家委員会の支援を受けて、本認証制度関連文書を改訂、適応、若しくは、新たな文書の作成、又は、その両方が可能である。

**本制度オーナーは、所轄データ保護機関に対し、認証基準の更新を連絡し、当該更新が認証基準に重大な変更を及ぼすのか否かを示す。**

ユーロプライバシー認証制度の変更は、次のとおりである。

a) ユーロプライバシー・オンラインコミュニティ＆リソースのウェブサイトに組み込まれる。
b) ライセンスを取得し、許可された関係する利害関係者が利用できる。

本認証制度の要件が変更され、認証を受けた申請者に影響を及ぼし得る場合、認証機関は、申請者に対し、当該変更を連絡し、次回のサーベイランス監査において、認証を受けたデータ取扱活動が当該変更を遵守していることを確認しなければならない。

### 18.4.4. バージョン管理

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るのが望ましい。

### 18.4.5. 履歴及び変更履歴バージョン

旧バージョンからの変更履歴付きの文書のバージョンは、編集者が保管し、利用可能にするのが望ましい。旧バージョンからの主な変更点の要約は、文書の冒頭部分又は別の文書に含めることができる。

### 18.4.6. 参照分類

本認証制度の公式資料の分類及び識別は「*ユーロプライバシー文書の管理及び分類*」と題する文書に定める運用指針に従う。

  

## 18.5. 公式文書の公開

### 18.5.1. 内部ピアレビュー

規範文書、情報提供文書及び報告書は、正式に承認及び公開される前に、正式な内部ピアレビュー及び確認を受けるのが望ましい。

### 18.5.2. 公式ユーロプライバシー文書リポジトリ

本認証制度の適用に必要な全ての文書（既存の文書の新しい公式版を含む）は、ユーロプライバシーコミュニティ＆リソースのウェブサイト（http://community.europrivacy.com）で利用できる。

### 18.5.3. 公開の効果

文書が更新され、ユーロプライバシー・コミュニティ＆リソースのウェブサイトで及び公開された時点で、当該文書は使用されるべき参照文書とみなされなければならず、旧バージョンは置き換えられる。

認証及び監査手続では、当該手続開始時点で入手可能な最新バージョンの本認証制度及び関連文書を利用しなければならない。認証及び監査手続中に新しいバージョンの文書が公開された場合、当該新しいバージョンの文書を考慮し、可能な限りこれを遵守するのが望ましいが、監査手続開始時の公式版に従って進行中の手続を完了することは許容される。

  

# 19. 認証機関のライセンス及び認定

## 19.1. 一般原則

ユーロプライバシー認証を付与することができるのは、次の要件を遵守する認証機関に限られる。

a) **認証機関は、**ユーロプライバシーを利用する際の認証機関の義務を明確化したライセンス契約を通じて、ユーロプライバシー認証制度及び関連リソースの利用について、**本制度オーナーから許可を受けなければならない**。許可された認証機関の一覧は、ユーロプライバシーの公開ウェブサイトで維持される。

b) **認証機関は**、適用可能な各国規制を遵守した**正式かつ十分な認定又は同意を要請し、これを取得しなければならない**。

c) **認証機関は、本認証制度の仕様及び適用可能な各国規制を遵守しなければならず**、GDPR 第 43 条に基づく認証を付与する場合、関連する EDPB の運用指針を遵守しなければならない。

認証機関は、本認証制度によって明示的に予期され、かつ、許可されていない、いかなる適応、制限又は拡張なく、提供されたとおりに本認証制度を適用しなければならない。

データ保護認証を付与する認証機関の認定は、原則として、各国データ保護機関又は認定機関の権限の下にある。本制度オーナーは、ユーロプライバシーのライセンスを監視、確認及び管理する権利を有する。

該当する場合、各国の規制及び仕組みは、本節で述べる規定を補完、訂正、又は、置き換えることができる。

### 19.1.1. 認定機関及びデータ保護機関との関係

GDPR 第 43 条に基づき、欧州連合の認定認証機関は、各国データ保護機関若しくは認定機関、又は、その両方の管理下にある。当該機関が認証機関の作業の監視及び管理を担当する場合、本制度オーナーは、当該機関を尊重及び支援し、これに協力する。

## 19.2. ライセンス手順

ライセンス手順は、認定を受け、かつ、信頼性の認められるサービス提供者のみに、他社にサービスを提供するためにユーロプライバシーを利用することを許可されるのを確保することにより、ユーロプライバシー認証に対する信頼性を構築することを意図している。ライセンス手続は、ユーロプライバシーの不適切な利用若しくは信頼できない認証付与、又は、その両方のリスクを低減する。

本制度オーナーは、ユーロプライバシー認証の実施及び付与のライセンス取得を希望する会社のため、手順、方針及び一連の要件を定義、維持及び更新するものとする。

関心を有する会社は、認証手続及び個人データ規制の経験を示す詳細なプレゼンテーションファイルを添付した申請書を提出することにより、ユーロプライバシーライセンスを申請できる。初回申請に必要な要件の一覧は、要請に応じて、本制度オーナーによって提供される。申請会社は、手順を遵守し、ライセンス関連の費用及び料金を負担することを誓約しなければならない。

原則として、申請手順は 2 段階の手続に従わなければならない。ただし、本認証制度を利用して認証を付与することを希望する欧州各国機関は、簡略化された手順により、本制度オーナーに無償ライセンスを要請することができる。

### 19.2.1. 第一段階の手続－適格性評価及びライセンス

第一段階として、本制度オーナーは、本制度オーナーによって採用された手順及び要件に従い、受け入れた申請の初期評価を実施しなければならない。当該評価では、意図されている認証活動の評判、発展、公平性、品質及び信頼性に影響を及ぼし得る次の要素を評価しなければならない。

a) 多数の申請者に高品質のサービスを提供する能力

  

b) 申請会社の認証における実績及び経験
c) データ保護法、サイバーセキュリティ及び認証に関する専門知識を含む、申請会社の要員の資格
d) 認証手続の公平性、独立性及び信頼性に影響を及ぼし得る場所、規制環境、並びに、ビジネス慣行
e) ユーロプライバシー関連サービスを提供するための戦略の質及び意欲

認証手続の公平性、独立性及び信頼性に関するリスクを評価するため、本制度オーナーは、申請会社の本社が所在する国の法の支配の尊重、汚職の程度、並びに、報道及び情報の自由に関する指標を使用してもよい。GDPR 第 5 章に基づく十分性認定が考慮される。

本制度オーナーは、評判及び信頼性、本認証制度の長期的な持続可能性、市場構造並びに需要など、その他の項目を考慮してもよい。

申請会社が本基準を充足すると認められる場合、本制度オーナーは次の事項を行う。
a) 申請会社との会議の開催
b) 申請会社が公式パートナーになる適格性を有するか否かの判断
c) 本基準の充足を認める決定である場合、申請会社に対し、署名するための正式なライセンス契約書の提供

### 19.2.2. 第二段階－準備状況及び認定

ライセンス手順の第二段階では、認証機関が次の措置を行うことを要求する。
a) ライセンス契約書への署名
b) 準備手続（専門家の教育・訓練、ウェブページの作成など）の完了
c) 官庁に対する正式な認定又は同意の要請

### 19.2.3. ライセンス取得認証機関の義務

ライセンス取得認証機関は、次の事項を行わなければならない。
a) 本認証制度の規則及び要件を遵守し、認証を受けた評価対象に適用可能なユーロプライバシー基準への遵守を確保すること
b) 本制度オーナーと緊密に協力し、該当する場合、各国データ保護機関若しくは認定機関、又は、その両方と緊密に協力すること
c) 認証活動に関する透明性のある情報を報告し、提供すること
d) 継続中の認証が本認証制度の要件を継続的に遵守していることを毎年監視すること
e) 本認証制度を促進し、その良好な評判に貢献すること
f) 本制度オーナーに対し、本基準、確認項目及び管理項目を含む本認証制度の改善案を提出すること

### 19.2.4. ライセンス取得認証機関の監視

ライセンス取得認証機関の監視には、次のようないくつかの形態がある。
a) 認証文書（記録及び所見を含む）をレビューすること
b) 認証機関が実施する監査にオブザーバ又は専任監査人を提供すること
c) 監査人に資格を要求すること
d) 本制度オーナーが必要と判断したその他の措置又は手続

認証機関は、適用可能な各国データ保護機関、認定機関又は本制度オーナーに求められた情報及び文書について、全面的に協力し、不当な遅延なく提供しなければならない。

### 19.2.5. ライセンス期間

本制度オーナーは、ライセンス契約を毎年監視し、レビューすることが推奨され、パートナー又は認証機関がその要件を充足しない場合、ライセンス契約の一時停止又は終了を決定できる。

### 19.2.6. ライセンス有効期限

認証機関に付与されたライセンスが満了又は終了した場合、データ保護機関又は本制度オーナーが当該認証は信頼できないとみなす理由がある場合を除き、当該認証機関が既に付与した認証には遡及効果がない。かかる場合、認証書は、他のライセンス取得認証機関によってレビュー及

  

び確認されるまで一時停止されてもよい。データ保護機関、認定機関若しくは本制度オーナー、又は、その複数は、申請者に代替認証機関を提案してもよい。

## 19.3. 認定又は合意手順

**GDPR 又はその他の各国データ保護規制の下で認証が有効であるためには、認証機関は、所轄国家機関から正式な認定又は同意を受けなければならない。**

**GDPR 第 43 条に基づき付与される認定は、ISO/IEC 17065 に基づかなければならない。**

### 19.3.1. 認定要件

認定は、認証機関が本認証制度を遵守及び適用する能力を正式に評価することを要求する。特に、次のような評価を要求する。

a) 申請する認証機関に必要となる次の専門知識及び経験
   - ISO 関連の専門知識及び経験
   - データ保護に関する専門知識及び経験

b) 次の要件を含む、インフラストラクチャ及び手順の要件を遵守していること
   - 適用可能な ISO 及びユーロプライバシー関連の要件
   - データ保護関連の要件

c) 次の事項に関する十分な知識及び専門知識を有する認定監査人の活用可能性を含む、人的資源の能力、技能及び資格
   - ISO 認証手続
   - GDPR 及び適用可能なデータ保護規制
   - サイバーセキュリティ
   - ユーロプライバシー認証制度の基準、規則及び手順

本認証制度の規則及び手順は、認証機関が ISO/IEC 17020 及び 17025 への準拠を証明する必要がないよう、十分に詳細かつ包括的であるとみなされる。

本認証の規則及び手順は均質的であり、産業分野及びデータ取扱いの複雑さに関係なく同じである。そのため、認定の付与に、特定の業界に限定される必要はない。

**認定は、補完的国家固有要件の対象となる場合がある。**

**本制度オーナーは、認定手順に関する補完的運用指針を規定することができる。**

## 19.4. 一時停止及び取消しの手続

認証の第一の目的は、認証を受けた評価対象に対する公衆の信頼性を確保することである。当該信頼性を危険にさらした場合、ライセンス及び認証書は一時停止又は取り消される。

### 19.4.1. 認定及びライセンスの一時停止及び取消し

各国データ保護機関若しくは認定機関、又は、その両方は、認証機関の認定を一時停止し、又は、取り消す権限を有する。同様に、本認証制度の重大な不遵守又は軽微な不遵守が反復される場合、本制度オーナーは、認証機関に付与されたライセンスを一時停止し、又は、取り消してもよい。

### 19.4.2. 付与された認証の一時停止及び取消し

上記の機関は、認証の評判を傷付け、又は、公衆の誤解を招くおそれがある場合、認証機関によって付与された認証を一時停止し、又は、取り消すこともできる。認証書の一時停止又は取消しにつながり得る状況の例には、次の例が含まれる。

a) 認証機関が、本認証制度に規定された義務及び要件を軽視又は無視していると認められる場合
b) 認証の受益者が本認証制度を遵守していないと認められる場合
c) 認証の受益者が、そのデータ保護ポリシー及びプラクティスに関連する情報を秘匿していると認められる場合

  

d) 認証を受けたデータ取扱いがデータ保護規制を遵守していることについて公衆の誤解を招くおそれのある認証書の存在又は使用

### 19.4.3. 一時停止及び取消しの決定手続

公衆若しくは本認証制度の評判、又は、その両方を保護するために正当な理由がある場合、ライセンス又は発行された認証書の一時停止が直ちに実施されることがある。決定機関は、受益者に対し、迅速に一時停止の理由を通知し、受益者が説明を提供し、若しくは、一連の是正措置を提案するため、又は、その両方のため、合理的な措置を講じなければならない。

原則として、ライセンス又は発行された認証書の取消しは、受益者が説明を行い、若しくは、一連の是正措置を提案し、又は、その両方を行うための合理的期間後にのみ実施されなければならない。取下げの対象となる可能性のある受益者は、適格機関が認証取下げの要否を決定する前に、少なくとも 30 日の明確化又は是正措置を提示するため、少なくとも 30 日の期間が与えられる。当該 30 日の期間は、決定機関が、対象となる受益者に取消手続の開始を通知した時点から起算される。

認証の一時停止又は取消しを決定する場合、当該決定機関は、本認証制度の信頼性及び信用性に対する公衆の信用を維持することの重要性とともに、比例原則を考慮しなければならない。

全ての認証機関及び申請者は、データ保護機関、認定機関若しくは本制度オーナー、又は、その複数の決定を遵守し、これを受諾することに同意しなければならず、法令で認められる範囲において、認証若しくはライセンス、一時停止又は取消しに関する決定に関連する補償の権利を、放棄することに同意しなければならない。

  

# 附属書 1-適用基準の概要表

次の表は、申請者の場所及び活動に応じて、ユーロプライバシー基準の適用範囲を要約したものである。

| | Applicant in the EEA | | Applicant outside the EEA | | | |
|---|---|---|---|---|---|---|
| | Subject to GDPR under Art. 3 GDPR | | | | NOT subject to GDPR under Art. 3 GDPR | |
| | **No transfer to third countries** | **Transfers to third countries** | **No transfer to third countries** | **Transfers to third countries** | **Data Importer only** (no onward transfers) | **Data Importer with onward transfers** |
| **CRITERIA** | Art. 42 and 3(1) GDPR | | Art. 42 and 3(2) GDPR | | Art. 46 and 42 GDPR | |
| **G.1** | YES | YES | YES | YES | YES | YES |
| **G.2** | YES | YES | YES | YES | YES | YES |
| **G.3** | YES | YES | YES | YES | YES | YES |
| **G.4** | YES | YES | YES | YES | YES, except G.4.1.4 | YES, except G.4.1.4 |
| **G.5** | YES | YES | YES | YES | YES | YES |
| **G.6** | YES | YES | YES | YES | YES | YES |
| **G.7** | YES | YES | YES | YES | YES | YES |
| **G.8** | YES | YES | YES | YES | YES | YES |
| **G.9** | YES | YES | YES | YES | YES, except G.9.1.3 | YES, except G.9.1.3 |
| **G.10.1** | NO | YES | NO | YES | NO | YES |
| **G.10.2** | NO | NO | NO | NO | YES | YES |
| **C Criteria** | YES | YES | YES | YES | YES | YES |
| **T Criteria** | YES | YES | YES | YES | YES | YES |
| **S Criteria** | YES | YES | YES | YES | YES | YES |

  