堀部政男情報法研究会　第9回 シンポジウム

OECDプライバシーガイドライン改正について

JIPDEC（一般財団法人日本情報経済社会推進協会）
電子情報利活用研究部
野村　至

2013-12-22

※ 本報告にあたり、堀部先生、新保先生に多大なご支援いただきました。感謝の意を申し上げます。

本日の報告内容

① ガイドライン改正の背景
- 個人データの利用状況の変化
- プライバシー保護に対する新たなアプローチの出現

② ガイドライン改正の経緯
- 進化するプライバシーその背景：OECDプライバシーガイドライン制定から30年
- プライバシーを保護する法の執行における越境協力に関する理事会勧告

③ ガイドライン改正の内容
- プライバシー執行機関
- プライバシーマネジメントプログラム
- データセキュリティ侵害の通知
- 個人データの国際流通
- 国内実施
- 国際協力と相互運用性

1980年 OECDプライバシーガイドライン採択の背景

1980年9月23日 採択

プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data

【状況】

（1960年代後半から）第一世代のメインフレーム･コンピュータが導入 技術革新

→　脱工業化情報革命（postindustrial information revolution）

→　コンピュータによるデータ処理の効率化による利益

【OECDプライバシーガイドライン採択の背景】

① コンピュータ処理の進展による個人データの利用の拡大による個人のプライバシーへの懸念

② 各国のプライバシー保護に関する国内法が、自由な情報流通の障壁となり、経済成長を阻害するのではないかという懸念

OECDプライバシーガイドライン ８原則

① **収集制限の原則**
- 適法かつ公正な手段によって本人への通知又は同意に基づく収集を行うこと

② **データ内容の原則**
- データ内容の正確性、完全性、最新性を確保すること

③ **目的明確化の原則**
- 利用目的を明確にすること

④ **利用制限の原則**
- 利用目的以外の目的での利用は行わないこと

⑤ **安全保護の原則**
- 個人データの安全管理を行うこと

⑥ **公開の原則**
- 個人データの収集事実、所在、利用目的や管理者等に関する情報を公開すること

⑦ **個人参加の原則**
- 本人が関与できる機会を提供すること

⑧ **責任の原則**
- これら原則を遵守する責任があること

オーストラリア、カナダ、アイスランド、アイルランド、トルコ、イギリスは棄権

- 「勧告」は法的には拘束力はないが、政治的・道義的には大きな影響力を持っている。
- 棄権の理由の一つに国内法の整備ができていないことがある。

国内法の整備ができていない日本がなぜ棄権しなかったのか？

OECDプライバシーガイドラインの見直しの背景

1980年 OECDプライバシーガイドライン採択（世界初の国際的合意）

- 1980年9月17日に欧州評議会で「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」 が採択されたが、批准は1981年1月28日であり、それまで公開されなかった。
- OECDはガイドライン作成作業を通じて、欧州評議会と緊密な接触を保っており、テキスト間の不必要な相違を避けるためあらゆる努力がなされた。そのため、保護についての一連の基本原則は、多くの点において類似している。

30年を経て

個人データの利用状況の変化

- 個人データの爆発的な量の増加
- 個人データのグローバルな接続性、インターネットの発達
- 個人データの分析（機器、技術）

これらリスク増加の対策をする必要があるのではないか？

プライバシー保護に対する新たなアプローチの出現

- EU：*拘束的企業準則*
- APEC：越境プライバシールール
- OECD：プライバシーを保護する法の執行における越境協力に関する理事会勧告

これら有効なアプローチの導入や調和を検討した方が良いのではないか？

OECDプライバシーガイドラインの見直しの経緯

検討の端緒	
2008	**インターネット経済の未来のための2008年宣言** （Declaration for the Future of the Internet Economy） • 1980年のプライバシーガイドラインも含め、特定のOECD文書を再評価することとした。
予備調査（再評価）作業	
2010	**進化するプライバシーの背景：OECDプライバシーガイドラインの30年** （Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines）
	プライバシーを保護する法の執行における越境協力に関する理事会勧告の実施報告（Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy）
改正検討作業	
2011	**情報セキュリティ・プライバシー作業部会（Working Party on Information Security and Privacy：WPISP）にて改正の検討を始める。** • 専門家グループ（Expert Group）の結成し、WPISPの検討を補助。 • 政府、プライバシー執行機関、学界、企業、市民団体、インターネット技術コミュニティ、欧州連合及び欧州評議会の代表、APECの専門家も参加したマルチステークホルダー・グループ。
採択	
2013	**改正の採択**

30年での変化

30年の変化	概要
技術の変化 • ネットワーク • センシング技術	• 携帯機器、カメラ機能や位置情報を利用可能とした • 医療や防災、交通システム、地図ナビゲーションなど • 個人、産業界、政府も利便性やコスト削減の恩恵を受ける • **個人の行動や居場所は他者に知られるリスクが増加**
• 個人データの大量保有 • 長期間保有 • 処理能力の向上	• 大量のデータ保存、長期間の保存が安価にできるようになった • コストの観点から不必要な情報を削除する必要がなくなった • **長期間の追跡が可能性が増大** • **データ処理能力の向上により、検索、リンク、追跡が容易になった（文字だけでなく、顔の認識も可能に）**
• 生体情報の利用	• 生体認証による入退管理、ログイン。遺伝子研究による病気解明と治療法の開発 • **個人のプライバシーと尊厳の問題** • **遺伝子については、個人だけでなく、その家族、民族や社会のメンバーと共有するという点で「集団のプライバシー」の問題**
組織活動の変化	• コストの大幅な削減に向けて、クラウドへの転換が図られ、業務の改善、拡大の方法が模索されている。 • データ管理者、下請業者、複数関係者がデータに関与することになった • 公共部門が市民への情報提供や意見聴取のために、ソーシャルメディアを活用するようにもなった • **データ管理の責任や管轄権の問題**
個人活動の変化	• SNS等で自分の情報を創造し、発信し、共有するようになった • 個人はデータの提供について、利用される目的や方法、データの種類、共有範囲、第三者提供など、理解せずに利用している場合がある • 家族や友人など他者の情報についても発信している場合もある • **ガイドラインの前提にある「データ管理者」といった概念への疑問**

変化に伴うプライバシー・リスク

リスク	概要
セキュリティ	• 個人データの量、流通の規模が大きくなることによって、たった一度の侵害から多くのデータが漏えいしてしまうといったリスクが高まった • 漏えいは内部から起こることも多く、例えば、個人データを保管したUSBの記録媒体を紛失することが起きており、**内部関係者の教育や訓練の重要視することが必要**になった。 • 外的要因から漏えいも増えている。国内外も含めて、フィッシング詐欺、不正アクセス、悪意あるソフトウェア（マルウェア）が増加。 • セキュリティ強化だけでなく、**プライバシー執行機関、民間組織間の協力が必要** • 直接的に犯罪を防止することを目的とはしていない**OECDプライバシーガイドラインの在り方への疑問**。
意図しない利用	• SNSで、個人の行動や、プロフィール、興味などについて、データマイニングを含めて分析するということが利用目的に入っていたとしても、個人は自分の情報がどのような範囲で、どのように使われるのか、理解していない場合がある。意図しない利用がなされている。 • 組織も個人データが収集された際は意図していなかった個人データに関する価値のある利用を見つける場合もある。 • **個人の理解と同意、組織のデータ利用について衝突が生まれている。**
監視	• 2001年以来、世界的に安全性への意識が高まり、監視カメラの設置や、自動車のナンバープレート自動認識システムなどの導入が進んでいる。政府によるウェブサイトの閲覧履歴の監視もある。 • 企業が職員に対して監視を行うこともある。社内の行動やブログの監視まで様々な形をとる。 • 監視は、安全や機密保持には貢献することがあるが、**個人のプライバシー空間の縮小、不当な差別を招く懸念**がある。

既存のプライバシー保護における課題

課題	概要
プライバシー保護の範囲	• 「個人データ」であるものとそうでないものとの区別は、難しくなってきている。 • ウェブの分析により、ほんのわずかの情報でも、ある一人の個人と紐づけることが可能。 • 「個人データ」が増え、このようなデータに対して、様々な**プライバシー管理体制の範囲内に持ち込む必要性があるのかという課題**がある。 • 同時に、**識別不能性、仮名の使用、匿名化の概念の明確さが求められている**。 • 「データ管理者」という概念についても、検討が必要。 • 個人は、SNS等、他者のデータに対してデータ管理者としても作用しうる。 • 多くの国のプライバシー法は、個人に対する行動は適用範囲外なので、**個人は自身の行動に対して責任を負わないまま**となっている。
透明性の確保、利用目的、同意の役割	• 利用規約は、長文で、明確に書かれておらず、データの使用条件が複雑。 • サービス利用開始時点に、プライバシーポリシーや同意に関する集中度合いが強く、個人が耐えられない。 • 個人は提示された文書をほとんど読まないか**理解しないまま同意する**。 • 基本的に「同意するか否か」ということが求められる。 • サービスに直接は関係しない利用目的があったとしても、組織が提示する目的すべてに関して同意しなければならない。 • 個人が**情報にアクセスすることが難しい**場合がある。例えば、個人がネットサーフィンをしている際に、特定の広告がなぜ掲示されているのか知りたいとき、どのようにしてその方法を見つけ、どの組織に聞けば良いのか、アクセスすれば良いのかわからない場合。 • データの拡散、インデックスやタグ付、キャッシングやミラーリングも、**個人データを修正（あるいは削除）**しようとする個人に課題を提起している。 • OECDプライバシーガイドラインは、**保存や廃棄に直接関連した原則**が含まれていない。

プライバシー保護のための新たな取組

取組み	概要
データセキュリティのための規制	• OECDプライバシーガイドラインをもとに新たな規定を設けるようになった。 • プライバシー侵害発生時に、**個人又は関係当局に通知することを求める**など。 • 関連する新たな法律を定めるようになってきた。スパムメールを規制する法律を定めるなど。
情報マネジメント / プライバシー・バイ・デザイン	• 欧州をはじめとして、プライバシーを保護する取組みとして、情報マネジメントや**プライバシー・バイ・デザイン**の導入が盛んになっている。 • **プライバシー影響評価**（Privacy impact assessment：PIAs）も重要視されるようになってきた。 • **プライバシー強化技術**（Privacy Enhancing Technologies：PETs）の活用は、有用な手法であると認識されている。
責任の役割	• 責任（accountability）は、OECDガイドラインに含まれている原則だが、加盟国の多くの法律にも含まれている。 • 責任を含んだ文書としてEUの**データ保護指令**がある。欧州連合では、欧州委員会によってデータの十分（adequate）な法的保護が存在するか、その他の手段で十分性が確保されていると判断されない限り、個人データをEUの管轄区域外に持ち出すことができないようにしている。 • APECの「**APEC越境プライバシー規則**」（APEC Cross-Border Privacy Rules：CBPRs）において、責任は鍵となる要素であり、アカウンタビリティ・エージェント（認証機関）の役割、トラストマークなどの手段が採られている。
越境執行協力	• OECDの**プライバシーを保護する法の執行における越境協力に関する理事会勧告** • APECの「**越境プライバシー執行に関する協力協定**」 • **国際プライバシー執行ネットワーク（GPEN）**の立ち上げ。

プライバシーを保護する法の執行における越境協力に関する理事会勧告（2007）

2007年6月12日 採択

プライバシーを保護する法の執行における越境協力に関する理事会勧告

Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy

【目的と範囲】

- 情報又は個人の所在に関わらず、個人データの保護に関する問題を解決するため、**プライバシー執行機関間で国際協力を促進させることを目的**としている。
- 対象は**民間部門の個人データ処理の侵害に関する執行協力を主**としているが、**公共部門での個人データの処理を含んだ事案における協力**も含まれている。
- 執行協力は侵害の中でも、侵害の性質、損害またはリスクの大きさ、影響を受ける人数などを鑑み、**深刻な事案を主な対象**としている。
- プライバシー執行機関間の執行協力の促進に焦点を当てているが、刑事法執行機関、公共及び民間組織のプライバシーオフィサー、民間の監督機関といった、**他の組織との協力も奨励**している。

【内容】

① 国内措置

- 加盟国の方針
- プライバシー執行機関の権限および能力拡大

② 国際協力

- プライバシー執行機関間の相互支援
- 相互支援の補助
- ステークホルダーとの協力

執行協力勧告（国内措置）

加盟国の方針
加盟国は、外国及び国内の他の**プライバシー執行機関**と有効に協力できるように、**効果的な国内措置の設置及び維持**に動くこと。
加盟国は、執行における越境協力が有効に機能しているか、必要に応じて見直すこと。
加盟国は、被害を受けた個人が、**個人の所在に関わらず、救済措置を採れるように検討**すること。
加盟国は、入手した**証拠が他国と相互に利用できるように検討**すること。

プライバシー執行機関の権限および能力拡大
加盟国は、プライバシー執行機関に、**侵害の阻止及び制裁の権限を与える**こと。
加盟国は、プライバシー執行機関に、**侵害の調査許可の権限を与える**こと。
加盟国は、プライバシー執行機関に、侵害に携わったデータ管理者に対する**是正措置の許可の権限を与える**こと。
加盟国は、自国のプライバシー執行機関が、侵害の発生に関連した外国の機関と**適切に情報を共有するメカニズムを提供**すること。

執行協力勧告（国際協力）

プライバシー執行機関間の相互支援

加盟国及びプライバシー執行機関は、本勧告と国内法の調和を図り、**加盟国同士及びプライバシー執行機関同士、互いに協力**すること。

プライバシー執行機関が他の国のプライバシー執行機関に支援を要請する場合は、要請される他の国のプライバシー執行機関が行動するのに**十分な情報を与え**、情報を要求する際には**目的を特定し**、支援の要請が**過度な負担にならないこと調査**すること。

支援を要請されたプライバシー執行機関は、**支援を拒否、限定、条件の設定**をしてもよく、支援の拒否または制限をする場合には、**理由を述べる**こと。

支援を受けるプライバシー執行機関は、調査の進行を手助けするため、**互いに連絡を取り合う**こと。

相互支援の補助

加盟国は、執行協力勧告にもとづく協力及び相互支援に関する**国内のコンタクト・ポイントを指定**し、OECD事務局にその情報を提供し、**プライバシーを保護する法の更新**も、OECD事務局に提供すること。

プライバシー執行機関は、**プライバシー法執行の処理状況や執行結果の情報を共有**すること。

加盟国は、**プライバシー執行機関及び適切な他のステークホルダーとの非公式なネットワークの設立**を促進すること。

ステークホルダーとの協力

加盟国は、プライバシー執行機関に対し、刑事法執行機関、公共及び民間組織のプライバシーオフィサー、民間の監督機関といった、**他の組織との情報交換を奨励**すること。

2013年 OECDプライバシーガイドライン

2013年7月11日 採択

プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data

主な改正内容

① プライバシー執行機関

② プライバシーマネジメントプログラム

③ データセキュリティ侵害の通知

④ 個人データの国際流通

⑤ 国内実施

⑥ 国際協力と相互運用性

仮日本語訳を公開しました
http://www.jipdec.or.jp/publications/oecd/index.html

プライバシー執行機関

19. ガイドラインを履行するにあたり、加盟国は以下の事項を実施すべきである。
c) **プライバシー執行機関を設立して維持し**、当該機関の権限を効果的に行使し、客観的かつ公正で一貫した基準に基づく決定を行うために必要な管理組織、リソース、技術的専門知識を備え、

- 1980年のガイドラインと2007年の執行協力勧告は、どちらもプライバシー執行機関の設置を明示的には要求していない。
- 2007年の執行協力勧告は、プライバシー執行機関の存在を想定し、関連する権限を付与するように提言している。
- 2013年のガイドライン改正では、**プライバシー執行機関の設置と維持の必要性を明確にしている。**

1. c) **「プライバシーを保護する法」**とは、国内の法律または規則を意味し、当該法令の施行により、本ガイドラインと一貫性を有する個人データ保護の効果を有する。

- **柔軟な定義とした**
  - 包括的プライバシー法
  - 分野別のプライバシー法
    （信用報告法、電気通信法）
  - 個人データを保護するその他法令を含む
    （消費者保護法）

1. d) **「プライバシー執行機関」**とは、プライバシーを保護する法の執行に係る責任を有し、調査の実施又は執行手続きを遂行する権限を有する各加盟国が設置する公的機関を意味する。

- **柔軟な定義とした**
  - 単一の組織であることは求めない。

なぜ独立や単一をという言葉を定義を含めなかったのか？

プライバシーマネジメントプログラム

15. データ管理者は以下のことに責任を有する。

a) **以下のプライバシーマネジメントプログラムを構築すること。**
   i. **管理下にあるすべての個人データに対するガイドラインを実施し、**
   ii. **取扱いの体制、規模、量、センシティビティに応じて、**
   iii. **プライバシー・リスク評価に基づく適切な保護措置を実施し、**
   iv. **ガバナンス体制への組み入れと内部監査メカニズムを確立し、**
   v. **問合せ及びインシデントへの対応計画を含め、**
   vi. **継続的なモニタリングと定期的評価を考慮した見直しを実施すること。**

b) **当該プライバシーマネジメントプログラムが適切に実施されていることを証明する準備を行い、特に、権限を有するプライバシー執行機関又は行動規範若しくは本ガイドラインに拘束力を与えるのと同等の取り決めの遵守を促進させる上で責任を有するその他の組織からの求めに応じて対応すること。**

近時、責任の原則が重要視されており、その原則を促進させる手段として**プライバシーマネジメントプログラムの概念を導入した。**

OECDプライバシーガイドラインを指すが、実際には国内法、国際的義務、自主規制、契約条項を反映する必要がある。

柔軟な対応が必要。大量の個人データを保有する大規模な管理者は小規模な管理者より包括的な管理が必要。逆に小規模でもセンシティブな情報を扱うときはより慎重な管理体制が必要となる。適したプログラムを採用すべき。

プライバシー・リスク評価、プライバシー・バイ・デザインの必要性について何度も繰り返し議論された。

プログラムの実行性と有効性の証明を確立することで、セキュリティ侵害や法令違反の申立てがない場合でも責任が強化される。同等な取決めにはシールプログラムや認証制度を含めることができる。

データセキュリティ侵害の通知

15. データ管理者は以下のことに責任を有する。
c) 個人データに影響を及ぼす重大なセキュリティ侵害があった場合、必要に応じてプライバシー執行機関又は他の関連機関に通知すること。当該セキュリティ侵害がデータ主体に不利益を及ぼすと思料される場合は、データ管理者は不利益を被るデータ主体に通知しなければならない。

- **データセキュリティ侵害の通知を導入した**
- 偶発的な紛失であれ、意図的な盗難であれ、個人データの悪用で個人が重大な被害を被るおそれがある。社会的評価に対する影響も甚大である。
- セキュリティ侵害が発生したときに、個人及び/又は関係機関に通知することをデータ管理者に求める法律は、多くの国で成立している。このような法律が制定される理由は、侵害があった場合にデータ管理者が自らの信用が失墜することを恐れて積極的に侵害事実を公開しようとしないことによる。
- 通知を義務づけることによって、被害に対して**個人が自らを守るための措置を講じることが可能**となる。通知が義務づけられる事項は、プライバシー執行機関やその他の機関にとっても、**事故調査の実施又はその他の措置を決定する際の有益な情報**となる。侵害通知義務を定める法律が、データ管理者が自ら保持する個人データの適切な安全保護措置を講じるインセンティブにもなることが望ましい。
- すべてのデータ・セキュリティ侵害について、いかに軽微な侵害であっても通知を要求することは、**データ管理者及び執行機関に過度な負担を強いる可能性**があるため、あまりメリットはない。さらに、データ主体に対する過剰な通知は、**通知の軽視を引き起こす可能性がある**。ガイドラインには、**リスクベースの通知方法**を反映している。

個人データの国際流通

16. データ管理者は、管理下にある個人データに対して、**当該データの所在に関係なく責任を有し続ける。**
17. 加盟国は、自国と他の国との間における個人データの国際流通について、ガイドラインに一致する継続的な保護のレベルを保つために、(a) **他の国がガイドラインを実質的に遵守している場合**、又は(b) **効果的な執行メカニズム及びデータ管理者により導入される適切な措置**を含め、**十分な保護措置がある場合、この流通を制限することを控えるべき**である。

- **OECDの個人データの国際流通のアプローチを明確化し、統合することを目指している。**
- 1980年ガイドラインは、データ流通を原則として認めることを前提としているが、特定の状況においては制限できることを認めている。
  - 今まで個人の保護のために様々なアプローチがあった。
    国別の措置：EUの十分性モデル、**データ管理者の措置**：BCR、標準契約。
- 1980年ガイドライン起草時：企業又は政府間での特定二者間でのデータ流通が主流
  今日：世界中のあらゆる場所に保管されたデータにアクセスすることが可能
- 2013年の改正では、 **当該データの所在に関係なく責任を有し続ける**ことを明言した。
- 国レベルだけではなく、データ管理者単位でも、**十分な保護措置がある場合、この流通を制限することを控えるべき**であるとした。
- 十分な保護措置には、技術的及び組織的セキュリティ保護措置、契約、苦情処理プロセス、監査等により、データ管理者が持続的に保護レベルを維持するための措置を含める。
- こうした措置が有効でないことが明らかになった場合には、執行等によって必要な措置を補完することが求められる。
- 第17項(b)は、データ管理者が実施する措置をサポートするために、執行のために有効な仕組みを利用できるか否かについて検討を行うことについても定めている。

国内措置

19. ガイドラインを履行するにあたり、加盟国は以下の事項を実施すべきである。
a) **政府機関全体で調整を行った提案を反映した国内のプライバシー保護方針を発展**させ、
……
g) **教育及び普及啓発、能力開発**並びに**プライバシー保護に資する技術的措置**の向上を含め、**補完となる基準**の採択を検討し、
h) **データ管理者以外の者が果たすべき役割を、各個人の役割に応じて検討**し、
……

政府機関全体で調整した提案を反映した国内プライバシー方針を発展させることを加盟国に奨励している。政府内でプライバシー保護の重要性を最高レベルに高めることは、プライバシー保護の有効性の向上にも資する。

子供は特に被害を受けやすいデータ主体にあたるため、オンラインにおける子どもの安全を維持し、自身のためにインターネットを使用するのに必要な知識とスキルを身に付けることの必要性

プライバシーの専門家は、プライバシーマネジメントプログラムの実施と管理に重要。データ保護及びプライバシーに係る資格を認定するプログラムは、専門的な教育や専門家を養成するサービスの支援

プライバシーを尊重し強化する技術（PETs）の開発と展開を促進する措置

認定プログラム及びシール・プログラムは、プライバシー保護に有用な技術の採用を更に促進させることができる

データ管理者の定義には含まれないその他の関係者であっても、個人データの保護レベルを決定するにあたって重要な役割を果たす。例えば、SNSでの、個人による友人、親類及びその他の人々に関する個人データの作成、投稿、共有。
個人が他人のプライバシーに係る権利利益 を侵害したときは、不法行為法又は民法によって救済することが可能であり、その他の措置も同様に検討される必要がある。

国際協力と相互運用性

20. 加盟国は、**プライバシー法の国境を越えた執行協力を容易にするために**、特に、プライバシー執行機関の間で情報共有を強化することにより、適切な措置を講ずるべきである。

21. 加盟国は、本ガイドラインに実質的に影響を及ぼす**プライバシーフレームワーク間の相互運用性を促進させる国際協定醸成を推進し、支援**すべきである。

- プライバシー執行機関相互の協力を強化するために、2007年の執行協力勧告の実施を再確認している。
- 特に加盟国は、プライバシー執行機関間の情報共有に向けて、協調的で効果的な執行を容易にするために、法的又は実務的に障害を克服することが求められている。
- 情報共有に対する障壁を低くすることが、この問題において特に重要な課題となっている。

- ガイドラインに実質的に効果を与える国際的な取り決めを通じて、プライバシー・フレームワークの国際相互運用性を改善するための加盟国の一般的な目標を表現している。
- プライバシー・フレームワーク間の相互運用性については多様なアプローチが存在する。
  - 米国とEU間のセーフハーバーの枠組みがある。
  - EUの拘束的企業準則（BCR）
  - APECの越境プライバシー・ルール制度
  - 欧州評議会の「個人データの自動処理に関する条約第108号」
- グローバルなプライバシー・ガバナンスの一層の均一化を図るために、政策レベルにおいて更なる支援や検討が必要。