

第45回世界プライバシー会議クローズドセッション
2023年10月

データ保護に係るグローバル基準の達成に向けて：
世界規模で高水準のデータ保護・プライバシーを確保するための諸原則（仮訳）

この決議は以下の機関によって提出された。

スポンサー：

- ・ 情報コミッショナーオフィス、英国

共同スポンサー：

- ・ 透明性、情報アクセス及び個人データ保護に関する国家機関（メキシコ（世界プライバシー会議（GPA）議長））
- ・ データ保護コミッショナー（欧州評議会）
- ・ 欧州データ保護監察機関（欧州連合）
- ・ 情報処理と自由に関する国家委員会（CNIL、フランス）
- ・ 連邦データ保護・情報自由監察官（BfDI、ドイツ）
- ・ データ保護機関（ガーンジー管轄区）
- ・ データ保護機関（イタリア）
- ・ 連邦データ保護情報コミッショナー（FDPIIC、スイス）
- ・ 個人データ規制管理ユニット（ウルグアイ）

2023年の第45回世界プライバシー会議は、

データ保護・プライバシーを基本的権利として支持すること並びに個人データの適切な処理を通じた個人の権利及び利益を保護することの両方において高い基準であることの重要性を強調し、

高い基準を維持し、明確な規制環境を促進するには、管轄区域間で一貫した解釈が重要であることを認識する。その結果、人々の個人データが保護されるとともに、人々の権利が守られ、組織は人々の信頼を獲得するとともに、デジタル経済のための革新的な製品・サービスを開発することが確保される。

個人データの処理に関して、プライバシーの効果的な保護を保証する一連の原則及び権利を明記した、2009年に採択されたマドリッド決議¹を想起し、また、その貢献と世界的な影響力を認識し、

世界の各管轄区域が、自らの文化や社会の価値観、優先順位及びニーズを反映した、自らのデータ保護法・制度を策定していることを認識し、また、各国の法・制度の間における将来の相互運用性を促進するため、共通性、補完性及び収れんの要素に基づいて構築することを継続するための国際的な取組の必要性をさらに認識し、

技術、イノベーション及びデジタル化の発展に伴い、新しく徐々に複雑化する方法による大量の個人データの処理にますます依存する新しい活動やビジネスモデルが誕生するため、データ保護・プライバシーの原則及び法律が適用されなければならない状況は変化し、進化し続けていることを強調し、また、法律、原則及びそれらの実施方法が引き続き高水準の保護を提供し続けなければならないことを認識し、

このような動向は、一般的なサービスのデジタル化から、人工知能の広範な開発と導入、自動化された意思決定の利用、生体認証技術を利用したイノベーションまで、多岐にわたっていることに留意し、

このような動向は、データ最小化、セキュリティ、透明性及び正確性に関連するリスクをもたらし、個人にとって不公平、差別的及び偏りのある結果などの重大な悪影響を引き起こし、又はデータ保護やプライバシー権を行使する能力に影響を与える可能性があるため、データ保護及びプライバシー法の実施と執行に新たな課題をもたらす可能性があることを懸念し、

¹ 「個人データ・プライバシー保護に関する国際基準—マドリッド決議」

<https://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf> (原文・英語)

この広範な文脈には、特に子供や社会的に弱い立場の人々など、権利が保持され、行使できるようにする必要性が特に深刻な又は重要な場合、より侵入的な要配慮個人データを含む個人データの処理が含まれることが、避けられないことを懸念し、

このような懸念によって、様々な管轄区域におけるGPAメンバーが、罰金の賦課、不必要なデータやアルゴリズムの削除の要求、処理停止命令の発出などの執行措置を講ずるに至っていることに留意する。GPAメンバーはまた、透明性、公平性、バイアス及び差別に関して懸念を示してきている。

先端及び未来の技術によるデータ保護・プライバシーへの影響を特定するための、様々な管轄区域におけるGPAメンバーの取組を歓迎し、

先端技術に対する人間中心で倫理的なアプローチをとることの重要性に留意し、また、デジタル環境における個人の権利及び利益の認識を保護するためには、データ保護・プライバシーがデータ・ガバナンスの促進のための基礎であることを強調し、

急速に発展している世界のデジタル経済の状況は、人々のデータ保護・プライバシーの権利を保護する方法で国境を越えてデータを送受信する必要性も強調し、

越境データ流通を可能にするためには、グローバル化された社会で必要とされる個人データの国際的な流通を促進しつつ、個人の権利の一貫した保護を確保する、同等の高い基準を備えた枠組み及びメカニズムが必要であることをさらに強調し、

高水準のデータ保護・プライバシーを達成し、将来の相互運用性を促進し、そして、信頼性のある自由なデータ流通を促進するために、法的枠組みと手段における保護の間の収れんを特定し、それに向けて取り組むための協力の重要性を強調し、

GPAメンバーが信頼性のある専門アドバイザーとして行動する能力とともに、今日の世界的なデジタル経済の文脈において、政策立案者、当局その他の関係者が、個人データを保護して人々の権利を保持するために協働することの重要性を確認し、

GPAは、データ保護・プライバシーに係るグローバル基準の価値を認めており、そのため、今日の世界的なデジタル経済の文脈において、個人データ保護・プライバシーに係る高い基準を達成するためには、次に掲げる高水準の原則、権利その他の要素が重要であると認識し、推進する。

1. 適法性と公平性

個人データの処理は、適用される国内法及び国際協定に従って、適法に行われなければならない。我々は、また、公平性の原則を強調しつつ、個人データが欺瞞的又

は不正な手段によって取得されてはならないことを強調する。これらにより、データ主体の利益の保護とプライバシーの合理的な期待を優先するとともに、処理が不公平な、差別的な又はバイアスのある結果をもたらさないことを確保する。

2. 目的の明確化

個人データの処理は、特定の、明示的で、正当な目的の達成に限定されるべきであり、それらの目的と矛盾する方法によりさらに処理されるべきではない。

3. 必要性和比例性

我々は、個人データは、処理の目的に関連して、適切であり、関連性があり、そして過剰ではないものに限定されるべきであるというのが、データ最小化の原則であることを再確認する。我々は、また、人々の情報の権利に関連して、処理の全体的な目的に関連した全体的な比例性と必要性を重視する。これにより、要配慮の若しくは特別なカテゴリーのデータ又は生体認証データを処理するような、新しいタイプの処理や技術の利用について適切な決定が可能となる。

4. データ内容

処理される個人データが正確であり、目的を達成するために必要に応じて最新の状態に保たれるよう、全ての合理的な措置を講ずるべきである。これは、不正確な情報に基づいて個人に対して行われる重大な決定が行われるリスクが、自動化された意思決定、アルゴリズム及びAIの利用によって悪化する場合には、特に重要である。その結果、金融、研究、犯罪等に関する決定に重大な影響を与える可能性がある。自動化された決定は、正確な情報に基づくべきであるとともに、正確で、バイアスのない情報によって学習されたシステムに基づかなければならない。

5. 保持・保管の制限

個人データは、処理目的を達成するために必要な場合に限り保持されるべきであり、当該目的で不要になった場合には、削除又は匿名化されるべきである。

6. 透明性

我々は、人々が自分の個人データがどのように処理されるかについて、適切に情報を受け取り、権利を行使できるように、明確さ、アクセスしやすさ及び理解しやすさを重視する。人々は処理がなされることを確実に認識できるように、情報は積極的に提供されるべきであるが、状況に応じて異なるメカニズムが必要となる場合がある。

7. 説明責任

我々は、実務的な要素に従って、高水準の原則を遵守していることを証明することを重視するとともに、必ずしもこれに限定されるわけではないが、後述する積極的な措置など、説明責任の原則を具体化する。

8. セキュリティ

管理者及び処理者は、個人データの機密性、完全性及び可用性を確保するために適切な措置を講じなければならない。セキュリティは、技術の進歩、デジタル環境への参加の増加及びグローバルなデジタル経済で処理される個人データの量の増加に伴い、セキュリティのリスクが高まる可能性があるため、ますます重要な要件となっている。

特に、これはサイバーセキュリティのリスクの増加につながる可能性がある。サイバーセキュリティが規制上の領域を交差することに留意し、我々は、グローバルなセキュリティ・リスクに効果的に対処するためには、明確で一貫した法律と規制アプローチとともに、規制当局、サイバーセキュリティ団体その他の関連する関係者間の協力を重視する。

9. 個人データの処理の正当性と根拠

我々は、処理の目的や状況に応じて、契約、公共の利益、法的義務、正当な利益、同意等、個人データの処理に関して、様々な種類の適切で、比例的な法的根拠を提供することを重視する。同意が根拠として利用可能な場合には、我々は、同意が、意味のある有効なものであり、実際の選択とコントロールを提供し、そして言葉や明確な積極的行動により示された合意によって、データ主体により自由に与えられた、具体的で、曖昧さのない、十分な情報に基づいた意思であるべきであるという要件を我々は重視する。

10. 要配慮データ

人種や民族の出身、政治的意見、宗教的又は哲学的信念、労働組合のメンバーシップ、健康及び性生活、犯罪に関連するデータ等、特定の側面や特性に関連する個人データに対しては、特別な保護を導入すべきである。また、我々は、個人データの識別を可能にし、その要配慮の性質（例えば、生体認証又は遺伝情報及びニューロテクノロジーに関連するデータ）に関するリスクを引き起こす可能性のある技術開発に対応するために、このカテゴリーに含まれる個人データの種類を見直す必要性を強調する。さらに、我々は、それ自体では要配慮ではないデータが、他のデータと関連付けられた場合に要配慮データとなる可能性があることに留意する。これには、特定の状況において、個人の民族性、信念、政治的見解、健康状態又は性的指向を推測するために、例えば、閲覧や視聴の習慣に関する記録が利用される可能性がある場合には、推測されたデータが含まれ得る。

11. 子供と社会的弱者の保護

子供や社会的弱者は、自分の個人データの処理に伴うリスクをあまり認識していない可能性があり、そのためデータ保護・プライバシーの権利を行使することが難しくなる可能性があるため、我々は、彼らの保護のための具体的な規定を設けることを重視する。我々は、行動規範やガイダンスで法的要件を補完するためのGPAメンバーその他の当局の取組を歓迎する。

12. 管理者と処理者

管理者及び管理者の代理として、又は管理者の指示に従って行動する処理者やサービス提供者の間において、それぞれの義務と責任、処理に関する具体的な詳細及び契約に定められた指示について、明確な取決めが定められていることが重要である。

13. 個人データの国際的な移転

我々は、保護がデータとともに移動することを確保するため、充分性、モデル条項、認証、管理取決めなど、様々な移転メカニズムにより国境を越えて個人データを保護することを重視する。我々は、安全で信頼性のある越境データ流通を可能にする既存の規制アプローチとメカニズムの間における将来の相互運用性を促進するために、共通性、補完性及び取れんの要素に基づいて構築することの利点に留意する。我々は、信頼性のある自由なデータ流通の開発と具体化に関するG7メンバーとそのデータ保護・プライバシー機関ラウンドテーブルの取組を歓迎するとともに、世界的なデジタル経済によりデータの流れが増大する中、このトピックに取り組む重要性を認識する。

我々は、「データへのガバメント・アクセス、プライバシー及び法の支配：国家安全保障と公共の安全を目的として民間部門が保有する個人データへのガバメント・アクセスの原則」に関するGPA決議を再確認するとともに、経済協力開発機構(OECD)の「民間部門が保有する個人データへのガバメント・アクセスに関する宣言」を歓迎する。

14. 情報を知る権利

我々は、どのような個人データが、どのように、誰によって、どのような目的で処理されているか、そしてその処理に関して人々がどのような権利を持っているかについて、人々が知る権利を重視する。我々は、透明性の原則との関連に留意し、自動化された処理操作はますます複雑で、不透明になる可能性があるため、個人が適切な情報を得ることをますます重視する。

15. アクセス、訂正、削除及び異議申立ての権利

我々は、データ主体のアクセス、訂正、削除及び異議申立ての権利を重視するとともに、人々のその他のデータ保護の権利を実現する重要な要素として、特にアクセス権を重視する。

16. 制限

我々は、また、個人データの処理を制限する権利を重視しており、この権利は、個人データの利用を制限するとともに、データが不正確であったり、違法に処理されたり、異議が唱えられたり、争われたりしている場合において行われる、不正確で、差別的で、不公平な決定に係るリスクから人々を保護する。

17. データ・ポータビリティ

我々は、データ主体が様々なサービス間でデータを再利用したり、必要に応じて別の管理者に転送したりできるようにするため、データ主体が管理者から構造化された一般的に利用されている電子フォーマットで自分の個人データのコピーを取得できることの重要性に留意する。

18. プロファイリング及び自動決定に関する権利

我々は、人的介入なしに自動化された手段に基づいて、プロファイリングが実行されたり、重大な決定が行われたりする場合には、人々に権利が確実に提供されることを重視する。これらの権利には、例えば、処理に関連するロジックに関する情報を取得する権利、人的介入を受ける権利又は決定に異議を唱える権利が含まれる場合がある。

19. 権利を行使する能力

我々は、また、人々が権利を行使するための簡素で、効率的な方法を提供することを重視する。これは、個人データの種類が進化し、処理の操作がより複雑になるにつれて、特に重要である。権利に対するいかなる制限も、法律で規定されるべきであり、公共の利益の目的や他人の権利及び自由を保護するために必要で、適切な範囲で適用されなければならない。

20. 積極的な措置

我々は、実務的な段階において、データ保護・プライバシーを実施するための積極的な措置を講ずる必要性を強調する。説明責任の原則と密接に関連しており、我々は、データ保護・プライバシーの要件の実務的な実施とコンプライアンスとともに、規制当局と自分のデータが処理される人々の両方に対するコンプライアンスを証明することを重視する。

特に、我々は、次のことを重視する。

- プライバシー・個人データ保護・バイ・デザイン**：新しくイノベーティブな商品・技術・個人データの処理方法が発展するにつれて、危害を特定、防止及び軽減するために当該プロジェクトの開始からデータ保護・プライバシーを構築するとともに、権利が保持されて行使されることを確保することが重要である。これには、プライバシー強化技術や規制サンドボックスの利用などの勝訴が含まれ得る。
- プライバシー・個人データ保護・バイ・デフォルト**：これは、プログラム、サービス、コンピューティング・システム又はプラットフォーム、電子アプリケーション、個人データを処理するその他の全ての技術に適用されるべきである。
- 積極的なコンプライアンス措置**には、次のことが含まれる。
 - ・データ保護・プライバシーのリスクを特定して軽減するための**プライバシー・データ保護影響評価**
 - ・人々のデータ保護の権利を保護するために必要に応じて、不遵守を特定し、適切な措置を講ずる**独立した監査**
 - ・スタッフが遵守しなければならない**内部データ保護ポリシーの採用と実施**
 - ・必要に応じて、個人データを処理するスタッフに対して行う**研修、教育及び啓発活動**及びコンプライアンスを監督するデータ保護責任者又は同等の責任あるスタッフの存在
 - ・規制当局及び必要に応じて、影響を受ける人々に対する**通知**を含む漏えいの**予防、検出及び対応措置**
 - ・効果的な保護措置とデータ保護・プライバシー要件へのコンプライアンスを提供し、証明する**プライバシー管理プログラム**その他の同様のアプローチ
 - ・各セクター内の主要なデータ保護・プライバシーの課題に効果的に対処する、セクターごとの特定のガイドラインを作成するための**実践又は行動規範**
 - ・承認されたスキームを通じて、組織が、データ保護・プライバシー要件のコンプライアンスを証明する**認証**
 - ・データ主体が、個人データの処理に関する質問や苦情を提出することを支援する**メカニズム**

21. 監督機関

我々は、独立した監督機関の存在を重視する。各監督機関は独立し、調査して行動を起こすための十分な権限を与えられ、その職務を効果的に遂行できる十分なリソースを備えている必要があり、そのリーダーとスタッフは適切な水準の専門知識と技術的能力を備えているべきである。我々は、データ保護・プライバシー法の適用の一貫性を確保するために、監督機関が公的部門と民間部門を監督する十分な権限を有することを重視する。我々は、独立したデータ保護・プライバシー当局の主要

な機能に関するGPAグローバル枠組み及び基準作業部会の分析と報告²を再確認する。

我々は、また、コンプライアンスの監視と執行に加えて、監督機関の重要性として、啓発活動を行うこと、可能であり、適切な場合には、例えば、ガイダンスの作成、関係者との協議、規制のサンドボックス等のコンプライアンス推進プロジェクトを強調する。

22. 協力

我々は、監督機関による、他のデータ保護・プライバシー機関との協力及び競争、消費者、金融、サイバーセキュリティ等の他の分野の規制当局との協力の双方を重視する。我々は、データ保護・プライバシー機関が他の管轄の機関と必要な情報を共有して、当局間の協力を強化する権限を与える規定を重視する。我々は、能力構築、知識の共有、効率性、作業の重複の防止及びより適切で一貫性のある規制上の決定に関する協力、特に世界の異なる管轄区域における同じ企業や同じ課題の調査に関する協力及びグローバルなデジタル経済における組織の活動の様々な規制上の側面に関連する協力には、メリットがあることを強調する。

我々は、規制当局が共通のアプローチをとることにより、より強力なメッセージを組織に伝えたとともに、規制上のより良い結果と世界市民にとってより良い成果を得ることが可能になることを強調したい。

23. 法的責任と賠償

我々は、また、適切な法的責任の枠組みを整備すること及びデータ主体が裁判所を通じて直接権利を行使できることを重視する。

以上を踏まえ、第45回世界プライバシー会議は、次のことを決議する。

- ・ この決議に記載した原則、権利その他の要素が、新しい先端技術やイノベーションによるデータの処理では、全ての状況において効果的に実施され、適用されることができるとを確保するため、これらの原則、権利その他の要素を提唱し、普及し、そして促進すること。
- ・ 立法者及び政策立案者に対し、データ保護・プライバシー法及びその関連法を実施し、改正する際には、信頼性のある専門アドバイザーとしてのデータ保護・プライバシー機関に意見照会するよう、要請すること。

² 「ポリシー戦略ワーキンググループ1：グローバルな枠組みと基準 2021年報告書」（付属書B・8ページ参照）
<https://globalprivacyassembly.org/wp-content/uploads/2021/10/1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf>（原文・英語）

解説：

現在のGPAメンバーは、2009年のGPAで採択され、データ保護・プライバシーの一連の原則及び権利を明記した「マドリッド決議」の貢献と世界的な影響力を認めており、その多くは今日でもよく知られている。しかし、デジタル化、イノベーション及び技術開発が進む中、国境を越えてより多くのデータが処理されるグローバルなデジタル経済の今日の状況において、この決議は、現在の高水準の期待がある原則、権利その他の重要な要素を規定しており、それらは、2023年にデータ保護・プライバシーに係る高い基準を確保するのに重要であるとともに、各管轄区域内の法律の導入及び改正が行われる際などにおいて、政策決定者に検討するよう我々が提唱するものである。

GPAメンバー当局は、世界の各管轄区域が新しいプライバシー・データ保護法の制定や古い法律の見直しを進めており、多くの場合、同様の要素に基づいていることを認識しており、喜ばしく考えている。これには、特定の国際的な移転制度の開発の強化が含まれる。我々は、欧州評議会の108号+条約、プライバシーの保護及び個人データの越境流通に関するOECDガイドライン、民間部門が保有する個人データへのガバメント・アクセスに関するOECD宣言、プライバシー保護法の施行における国境を越えた協力に関するOECD勧告、コンピュータ化された人事データファイルの規制に関する国連ガイドライン及びイベロアメリカン諸国の個人データ保護基準など、既存のグローバルな枠組み及び基準を歓迎するとともに、世界規模でデータ保護・プライバシーの高い基準を実施するためにこれらに基づいて構築する取り組みを歓迎する。

現在の「戦略計画2021～23」³の下におけるGPAの取組を通じ、世界的に高水準のデータを確保するために、各地域の監督機関間の協力が促進された。近年の我々の作業を通じ、グローバル枠組み及び基準作業部会による10のグローバル枠組みの2020年分析⁴、移転メカニズムの2021年分析⁵等、核となる原則、権利その他の要素に関するグローバル枠組みの広範な共通点に注目し、強調しようと努めてきた。

管轄区域が異なれば法制度も異なるため、プライバシー・データ保護法のアプローチと詳細は異なるが、特に核となる原則と権利には共通性と収束が見られる。この

³ 「会議体の戦略的指令に関する決議」（2021年10月第43回世界プライバシー会議クローズドセッション採択）
<https://globalprivacyassembly.org/wp-content/uploads/2021/10/2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf>（原文・英語）

⁴ 「ポリシー戦略ワーキンググループ1：グローバルな枠組と基準 2022年報告書」
https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf（原文・英語）

⁵ 「ポリシー戦略ワーキンググループ1：グローバルな枠組と基準 2021年報告書」（原文リンクは脚注1と同一）

決議の中で、GPAは、包括的な原則と基準と、それらが収れんと相互運用性の促進にもたらす利点、ひいては世界中の人々の個人データを保護するための国際協力への支援を重視することを目指している。我々はまた、OECDや欧州評議会、G7やG20などの国際機関や多国間機関のほか、データ保護機関やネットワーク（イberoアメリカン・データ保護ネットワーク（RIPD）、東南アジア諸国連合（ASEAN）、アジア太平洋経済協力（APEC）、欧州データ保護会議（EDPB）、アフリカ・データ保護当局ネットワーク（NADPA/RAPDP）、フランス国家保護協会担当者（AFAPDPを含む）及び国際標準化機構（ISO）などの標準化団体が、この目的のために積極的に貢献できることにも焦点を当てたい。