# EDPBの「AIモデルにおける個人データ処理に関する意見書」について

2025年 2月 6日

（株）国際社会経済研究所　小泉 雄介

## ○目次

- 「AIモデルにおける個人データ処理に関する意見書」の概要
- アイルランドのデータ保護監督機関（DPC）からの質問事項
- （1）AIモデルを「匿名」と見なすことができるのはどのような場合か
- （3）AIモデルの開発時に個人データが違法に処理された場合、その後のAIモデルの処理や運用にどのような影響が及ぶか

## ○付録

- 付録１：EDPBの「ChatGPTタスクフォースによる業務報告書」について
- 付録２：EDPBの「GDPR第6条(1)(f)（正当な利益）に基づく個人データ処理に関するガイドラインver1.0」について

# 「AIモデルにおける個人データ処理に関する意見書」の概要（1/2）

IISE

- EUのデータ保護諮問機関である欧州データ保護会議（EDPB）は2024年12月17日、「AIモデルの文脈における個人データ処理に関連したデータ保護の側面に関する意見書」を採択。
  - 「Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models」
  - https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf
- 同意見書は、大きくは以下の3点について検討。
  - (1) どのような場合、AIモデルが「匿名」であると見なすことができるか
  - (2) どのような場合、AIモデルの開発や利用時の適法性の根拠として「正当な利益」を使用できるか
  - (3) 適法性の根拠のない「違法に処理された個人データ」を用いてAIモデルが開発された場合、当該AIモデルを引き続き利用することができるか
- 同意見書は、欧州全体の規制の整合を求める観点から、アイルランドのデータ保護監督機関（DPC、Data Protection Commission）からの要請によるもの。また、EDPBは欧州委員会AIオフィスとも意見交換を実施。
  - アイルランドのDPCは2024年2月以来、GDPR適用に関してOpenAI社の主たる監督機関となっている。
- 上記(2) については、EDPBが2024年10月8日に採択した「GDPR第6条(1)(f)（正当な利益）に基づく個人データ処理に関するガイドラインver1.0」（後述）が参照されている。
- さらにEDPB は、AIモデル学習時のWeb スクレイピングなどのより具体的な質問をカバーするガイドラインを策定中。これは、2024年5月23日に公表されたEDPB「ChatGPTタスクフォースによる業務報告書」（後述）に続くもの。

# 「AIモデルにおける個人データ処理に関する意見書」の概要（2/2）

IISE

- (1) の「匿名性」に関しては、AIモデルが匿名であるかどうかは、各データ保護監督機関によってケースバイケースで評価されるべき。AIモデルが匿名であるためには、「AIモデルの作成に使用されたデータの個人を直接的または間接的に識別することが非常に困難なこと」および「クエリを通じてAIモデルからそのような個人データを抽出することが非常に困難なこと」が必要。同意見書では、匿名性の実証方法を例示したリストも提供。
- (2) の「正当な利益」に関しては、正当な利益がAIモデルの開発および導入（ディプロイメント）のための個人データ処理の適切な適法性の根拠であるかどうかを監督機関が評価する際に考慮すべき事項を提示。管理者はバランシングテストを含む3段階のテストで、正当な利益の使用できるか評価すべき。
- EDPB は、ユーザーを支援する会話エージェントや、サイバーセキュリティを向上させるためのAI使用を正当な利益の適用事例として挙げる。これらのサービスは個人にとって有益であり、適法性の根拠として正当な利益に依拠可能だが、当該処理が厳密に必要であることが示され、個人と管理者の権利のバランスが尊重される場合に限られる。
- 同意見書では、データ処理に対するデータ主体の合理的な期待を評価するための基準（個人データが公開されていたか、個人と管理者の関係、自分のデータがオンラインにあることを個人が実際に認識していたか等）も提示。バランシングテストにおいて個人への悪影響のために当該処理を行うべきではないと評価した場合であっても、軽減措置によりこの悪影響を制限可能である。
- (3) の「違法に処理された個人データ」を使用してAIモデルが開発された場合には、AIモデルが適切に匿名化されていない限り、当該モデル導入時の適法性に影響を及ぼす可能性がある。

# アイルランドのデータ保護監督機関（DPC）からの質問事項

IISE

- アイルランドのDPCは、GDPR第64条2項に基づき、EDPBにGDPR適用に関する意見を出すよう要請。この要請は、AIモデルの開発・導入フェーズにおける個人データ処理に関するもので、以下の4つの質問から成る。
  - （1）AIモデルを「匿名」と見なすことができるのはどのような場合か。
  - （2）管理者は開発フェーズにおいて、正当な利益が法的根拠として適切であることをどのように実証できるか。
  - （2）’管理者は導入フェーズにおいて、正当な利益が法的根拠として適切であることをどのように実証できるか。
  - （3）AIモデルの開発フェーズで個人データが違法に処理された場合、その後のAIモデルの処理や運用にどのような影響が及ぶか。

※EDPB意見書では実際には上記(2)’は(3)、(3)は(4)と記載されているが、本資料では便宜的に上記の番号で記載する。

- ※これらの質問は、「（2）（OpenAI社のChatGPTにおける）Webスクレイピングで収集した個人データの学習データとしての利用、およびプロンプトでのユーザーからの個人データ収集に、正当な利益を使うことが適切なのか」→「（3）学習時に正当な利益を使うことが不適切等の理由でGDPR違反があった場合、そのAIモデルをその後（OpenAI社もしくは第三者）が利用することは違法ではないのか」→「（1）この違法可能性を除去するために、AIモデルを匿名化するには、どうしたらよいのか」という形で一連のものと考えられる。

# （1）AIモデルを「匿名」と見なすことができるのはどのような場合か（1/4）

- ※これまで日本やEUにおいては、学習データに個人情報が含まれていても、通常、作成されたAIモデルは個人情報に該当しないとされてきた。
  - 「複数人の個人情報を機械学習の学習用データセットとして用いて生成した学習済みパラメータ（重み係数）であっても、当該パラメータと特定の個人との対応関係が排斥されている限りにおいては個人情報に該当しないと考えられます。」（「個人情報保護法ガイドラインＱ＆Ａ」Q&A1-8、https://www.ppc.go.jp/personalinfo/faq/APPI_QA/）
  - 「個人データを学習データとして作成されたAIモデルは、基本的には、それ自体を個人データとみなすことはできない。・・・ただしAIモデルが プライバシー攻撃（メンバーシップ推論、モデル回避、モデル反転など）を受け、それが成功した場合、 これは個人データ侵害（漏洩等）とみなされる可能性がある。その場合、当該モデルを速やかに撤去し、個人データ侵害をデータ保護監督機関に報告しなければならない。」（フランスのデータ保護監督機関CNIL、2022年9月、https://www.cnil.fr/en/ai-ensuring-gdpr-compliance）

- ※EDPBの本意見書では、学習データに個人データが含まれている場合、AIモデルが一概に「匿名」であるとは言えず、匿名であること（個人データに該当しないこと）を実証するためにはかなりの労力が必要となることが主張されている。

# （1）AIモデルを「匿名」と見なすことができるのはどのような場合か（2/4）

- 一部のAIモデルは、モデルの学習にデータが用いられた個人に関する個人データを提供するように、又は何らかの方法でそのようなデータを利用できるように特別に設計されている。このような場合、そのようなAIモデルには、識別された又は識別可能な自然人に関する情報が本質的に（通常は必然的に）含まれ、したがって個人データの処理を伴う。したがって、これらのタイプのAIモデルは匿名であるとは見なされない。これは例えば、以下の場合に当てはまる。（29項）
  - （i）個人の音声録音に基づいて微調整され、その個人の声を模倣する生成モデルの場合。
  - （ii）特定の人物に関する情報を求められたときに学習により個人データで応答するように設計されたモデルの場合。
- その他の場合でも、個人データを含む学習データセットの情報が、AIモデルのパラメータに「吸収」されたままの可能性、すなわち数学的オブジェクトを通じて表現されている可能性がある。元の学習データポイントとは異なる可能性はあるが、それらのデータの元の情報は保持されている可能性があり、最終的にはモデルから直接的または間接的に抽出または取得される可能性がある。モデルの学習にデータが用いられた、識別された又は識別可能な個人に関する情報が、合理的に使用される可能性のある手段でAIモデルから取得される場合はいつでも、そのようなモデルは匿名ではない。（31項）

# （1）AIモデルを「匿名」と見なすことができるのはどのような場合か（3/4）

- 例えば、既存の研究発表ではAIモデルに存在しうる幾つかの潜在的な脆弱性が強調されており、その結果、個人データが処理されてしまう可能性がある（メンバーシップ推論攻撃やモデル反転攻撃など）。また、AIモデルがAPIや「プロンプト」インターフェースを通じて他のデータと共に使用されるようにディプロイされるときに、個人データの処理が行われる可能性がある。（32項）
- 上記の考察に基づき、EDPB は、個人データで学習したAIモデルは、すべてのケースで必ずしも匿名であるとは見なせないと考える。その代わりに、AIモデルが匿名であるかどうかの判断は、監督機関によってケースバイケースで評価されるべきである。（34項）
- 情報は、技術的に構造化またはエンコードされている場合でも、その自然人との関係がすぐには明らかにならない方法で自然人に関連している可能性がある。このような場合、ソフトウェアアプリケーションを使用して、特定のデータを簡単に識別、認識、抽出できるかもしれない。これは、パラメータが学習データ間の統計的関係を表し、AIモデルに含まれるデータ間の関係から直接、またはそのAIモデルをクエリすることによって、正確な、又は（統計的に推論されるため）不正確な個人データを抽出できる可能性があるAIモデルに特に当てはまる。（37項）

# （1）AIモデルを「匿名」と見なすことができるのはどのような場合か（4/4） IISE

- AIモデルには通常、直接分離またはリンクされる可能性のあるレコードは含まれず、むしろAIモデルの学習データ間の確率的関係を表すパラメータが含まれるため、現実的なシナリオでは、メンバーシップ推論など、情報をAIモデルから推論できる可能性がある。したがって、監督機関が特定のAIモデルを匿名と見なすことに管理者と合意するには、少なくとも以下に関する十分な証拠を受領するべきである。（38項）
  - (i) 学習データに関連する個人データがAIモデルから抽出できない。（抽出には、クエリインターフェイスをほとんど又は全く使用せずに、AIモデル自体から個人データが導き出される場合が特に含まれる。）
  - (ii) AIモデルをクエリしたときに生成される出力が、モデルの学習にデータが用いられた個人に関連しない。
- 上記の条件を満たしていること（個人識別の可能性がないこと）の評価は、管理者や第三者が個人を識別するために「合理的に使用する可能性のあるすべての手段」を考慮して行われるべきである。（41項）
- この評価を行うために、監督機関は、AIモデルの匿名性を実証するために管理者から提供された文書を確認する必要がある。匿名性の実証方法には、学習に用いられる個人データの収集の防止・制限、個人データの識別可能性の低減、個人データの抽出の防止、最先端の攻撃に対する耐性（(i) 属性推論・メンバーシップ推論、(ii) 窃盗（exfiltration）、(iii) 学習データの逆流（regurgitation）、(iv) モデル反転、(v) 再構築攻撃）などの、モデルの開発フェーズ中に管理者が取るアプローチが含まれる。（3.2.2節）

# （3）AIモデルの開発時に個人データが違法に処理された場合、その後のAIモデルの処理や運用にどのような影響が及ぶか（1/5）

IISE

- この質問は、開発フェーズでの違法なデータ処理が、AIモデルのその後の（例えばAIモデルの導入フェーズでの）データ処理や運用に及ぼしうる影響について明確化を求めるもの。（109項）
- 以下のケースについて検討。（109項）
  - 開発時に違法に個人データ処理されたAIモデルが、その後の利用で、当該モデル内に保持されている個人データを処理する場合
    - 開発時と同じ管理者が処理する場合（シナリオ１）
    - 開発時とは別の管理者が処理する場合（シナリオ２）
  - 開発時に違法に個人データ処理されたAIモデルが、その後の利用で、個人データ処理を伴わなくなる場合（すなわちAIモデルが匿名であることを管理者が保証する場合）（シナリオ３）
- 開発時のデータ処理において違反が判明した場合、監督機関は、各ケースの状況を考慮し、管理者にデータ処理の違法性を改めるための処置を講ずるよう命じるなど、是正措置を課すことができる。例えば、罰金を科す、処理に一時的な制限を課す、違法に処理されたデータセットの一部を消去する、またはこれが不可能な場合は、手元の事実に応じて、措置の比例性を考慮して、AIモデルの開発に使用されたデータセット全体および／またはAIモデル自体の消去を命じることが含まれる。是正措置の比例性を評価する際、監督機関は、管理者が当該処理の違法性を是正するために適用できる措置 （再学習など）を考慮できる。（114項）
- 個人データが違法に処理された場合、データ主体はGDPR第17条に定められた条件に従って個人データの消去を要求でき、監督機関は職権で個人データの消去を命じることができる。（115項）

# （3）AIモデルの開発時に個人データが違法に処理された場合、その後のAIモデルの処理や運用にどのような影響が及ぶか（2/5）

IISE

〇シナリオ１：管理者がAIモデル開発時に違法に個人データを処理し、同じ管理者がその後の利用で、当該モデル内に保持されている個人データを処理する場合

- 監督機関が開発時のデータ処理に対して是正措置を課す権限は、原則としてその後のデータ処理に影響を及ぼしうる。例えば、監督機関が管理者に違法に処理された個人データを消去するよう命じた場合、そのような是正措置により管理者はその後、措置の対象となった個人データを処理できなくなる。（120項）
- 開発フェーズと導入フェーズが別々の処理目的を伴うかどうか（したがって別々のデータ処理活動を構成するかどうか）、および最初のデータ処理活動の適法性根拠の欠如がその後の処理の適法性にどの程度影響を与えるかは、ケースの状況に応じてケースバイケースで評価するべきである。（122項）
- 例えば、その後のデータ処理がGDPR第6条1項(f)の正当な利益に基づく場合、最初のデータ処理が違法であったという事実は、その後のデータ処理の正当な利益の評価において考慮されるべきである（例えば、データ主体がその後のデータ処理を予期していない可能性があるというデータ主体にとってのリスクまたは事実に関して）。これらの場合、開発フェーズでのデータ処理の違法性が、その後のデータ処理の適法性に影響を及ぼす可能性がある。（123項）

# （3）AIモデルの開発時に個人データが違法に処理された場合、その後のAIモデルの処理や運用にどのような影響が及ぶか（3/5）

IISE

〇シナリオ２：管理者がAIモデル開発時に違法に個人データを処理し、別の管理者がその後の利用で、当該モデル内に保持されている個人データを処理する場合

- 監督機関は、(i) AI モデルを最初に開発した管理者、および (ii) 当該モデルを取得して個人データを独自に処理する管理者（※ディプロイヤーなど）によって実行される両方のデータ処理の適法性を評価するべきである。（126項）
- GDPR第17条1項(d)（違法に処理されたデータの消去）およびGDPR第19条（個人データの訂正もしくは消去、または処理の制限に関する通知義務）は、ケースの状況に応じて、この文脈でも関連する可能性がある。例えば、AIモデルを開発した管理者が当該モデルを導入する管理者に対して行うべき通知など。（127項）
- 監督機関は、AIモデルを導入する管理者が、GDPR第5条1項(a)および第6条の遵守を実証するアカウンタビリティの一環として、当該モデルが個人データを違法に処理して開発されたものではないことを確認するための適切な評価を実施したかどうかを考慮するべきである。監督機関によるこのような評価では、データのソースや、当該AIモデルがGDPRに違反して開発されたものであるか（特に監督機関または裁判所によってGDPR違反と判断された場合）など、当該モデルを導入する管理者が最初のデータ処理が違法であったことを無視できないように、いくつかの非網羅的な基準を管理者が評価したかどうかを考慮するべきである。（129項）

# （3）AIモデルの開発時に個人データが違法に処理された場合、その後のAIモデルの処理や運用にどのような影響が及ぶか（4/5）

IISE

〇シナリオ２（続き）

- AI法ではハイリスクAIシステムのプロバイダーに適合性宣言書の作成を義務付けており、宣言書には、当該AIシステムがEUデータ保護法令を遵守しているという宣言が含まれる。（131項）
- 管理者が（その後の）データ処理の適法性根拠として正当な利益の適切性を評価したかどうか、またどのように評価したかを、監督機関が検証する場合、最初のデータ処理の違法性は、その後のデータ処理の正当な利益の評価の一部として、例えばAIモデルを開発するために個人データが違法に処理されたデータ主体に生じる可能性のある潜在的なリスクを評価することによって考慮されるべきである。（132項）
- 正当な利益のバランシングテストでは、技術的な性質（例えば、AIモデルの開発中に設定されたフィルターまたはアクセス制限の存在。後続の管理者はこれを回避または影響を与えることができず、個人データへのアクセスまたは開示を妨げるかもしれない）や、法的な性質（例えば、最初のデータ処理の違法性の性質と重大性）の様々な側面を、十分に考慮しなければならない。（132項）

# （3）AIモデルの開発時に個人データが違法に処理された場合、その後のAIモデルの処理や運用にどのような影響が及ぶか（5/5）

IISE

〇シナリオ３：開発時に違法に個人データ処理されたAIモデルが、その後の利用で、個人データ処理を伴わなくなる場合（すなわちAIモデルが匿名であることを管理者が保証する場合）

- 管理者がAIモデルの開発時に個人データを違法に処理するが、同じ管理者または別の管理者が（導入フェーズで個人データの別の処理を開始する前に）、個人データが匿名化されたことを保証する場合である。（133項）
- 監督機関は、AIモデルの匿名化に関連する処理だけでなく、開発時に実施されるデータ処理に関しても介入する権限がある。したがって監督機関は、ケースの具体的な状況に応じて、この最初のデータ処理に対して是正措置を課すことができる。（133項）
- AIモデルのその後の運用が個人データの処理を伴わないことが実証された場合、GDPR は適用されない。したがってこの場合、最初のデータ処理の違法性は、AIモデルのその後の運用に影響を与えるべきではない。ただし、管理者がAIモデルの匿名性を主張するだけでは、GDPR の適用を免除するには不十分である。監督機関は、EDPBが質問(1)に対して提示した事項をケースバイケースで考慮してAIモデルの匿名性を評価するべきである。（134項）
- AIモデルが匿名化された後であっても、管理者が導入フェーズで収集した個人データをその後処理する場合、これらのデータ処理活動に関してはGDPRが適用される。この場合、導入フェーズで実行されるデータ処理の適法性は、最初のデータ処理の違法性によって影響を受けるべきではない。（135項）

# 【ご参考】イタリアのデータ保護監督機関によるOpenAIへの制裁金（1/2）

IISE

- イタリアのデータ保護監督機関（イタリアDPA）は2024年12月20日、OpenAIのChatGPTに対する予備調査を終了し、OpenAIに対して1500万ユーロの制裁金を含む是正措置を講じた旨を公表。
（https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10085432）
- これらの是正措置は、（2023年当時はカリフォルニア企業だった）OpenAIと争われていた侵害を確認するものであり、調査は2023年3月に開始されたが、EDPBの「AIモデルにおける個人データ処理に関する意見書」の公表（2024年12月18日）を受けて、調査の結論に達したもの。
- イタリアDPAによると、生成AIチャットボット（Chat GPT）を開発・管理する米国企業OpenAIは、2023年3月に起きたデータ侵害をイタリアDPAに通知しておらず、またChatGPTを学習させるためにユーザーの個人データを適切な適法性の根拠を最初に特定することなく処理し、透明性の原則とユーザーへの情報提供の義務に違反していた。さらに、OpenAI は年齢確認のメカニズムを提供していなかったため、13歳未満の子どもが発達や自己認識の程度に関して不適切な対応にさらされるリスクにつながる恐れがあった。
- イタリアDPAは、まず個人データ処理における有効な透明性を保証することを目的として、OpenAI に対して6ケ月間、ラジオ、テレビ、新聞、インターネットでのコミュニケーションキャンペーンを実施するよう命令した。その内容は、ChatGPT の機能、特に生成AIの学習のためにユーザーおよび非ユーザーデータを収集することや、データ主体が行使できる権利（自分のデータについて異議を述べたり、訂正したり、消去する権利など）に関する一般の理解と認識を促進することである。
- イタリアDPAは OpenAI に1500万ユーロの制裁金を科したが、この制裁金は同社の協力的な姿勢も考慮して計算された。

# 【ご参考】イタリアのデータ保護監督機関によるOpenAIへの制裁金（2/2）

IISE

- なお、OpenAIが予備調査の途中で2024年2月に欧州本社をアイルランドに設立したため、イタリアDPAはワンストップショップメカニズムに従って、手続き書類をアイルランド監督機関（DPC）に送付した。DPCは、OpenAI欧州本社の開設前に調査が完了しなかった進行中の侵害の調査を継続するために、GDPRに基づく主たる監督機関となった。
- OpenAIの「ChatGPTの学習データとしてイタリア市民の個人データを処理することの適法性の根拠は正当な利益である」「正当な利益の評価（legitimate interest assessment: LIA）も実施している」との主張に対し、イタリアDPAは「LIAの文書に日付がなく、ChatGPTの一般公開日（2022年11月30日）より前に実施されたことを証明できない」（後にOpenAIは、LIAの最初の草案は2023年2月24日に完成したと表明）として、GDPR遵守が不十分であったとしている。（https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085455）

# 【ご参考】イタリアのデータ保護監督機関によるDeepSeekへの情報提供要求

- イタリアDPAは2025年1月28日に、Webベースとアプリベースの両方の DeepSeek チャットボットサービスを提供するHangzhou DeepSeek Artificial IntelligenceとBeijing DeepSeek Artificial Intelligenceに情報提供を要求した。（https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10096856）
- イタリアでは数百万人の個人のデータが潜在的に高いリスクに晒されていることから、イタリアDPAは両社とその子会社に対し、収集される個人データ、使用されるソース、データ処理目的、データ処理の適法性の根拠、そして中国に位置するサーバ上に保存されているかどうかについて確認するよう求めた。
- イタリアDPAはまた、これらの企業に対し、当該AIシステムの学習にどのような情報が使用されているのかを尋ね、Webスクレイピング活動を通じて個人データを収集する場合、サービスの登録ユーザーおよび未登録ユーザーに対して個人データの処理についてどのように情報提供したか、または情報提供しているかを明らかにするよう求めた。
- DeepSeekは、要求された情報を20日以内にイタリアDPAに提出する必要がある。

# 付録１：

# EDPBの「ChatGPTタスクフォースによる業務報告書」について

# ChatGPTタスクフォース立ち上げの経緯

IISE

- イタリアのデータ保護監督機関は2023年3月30日、OpenAIに対してChatGPTでイタリア人利用者のデータを処理することの一時禁止を命令。理由は以下の4つ。（https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847）
  - データ主体（本人）への情報提供の欠如
  - アルゴリズムを学習させるために個人データを大量に収集・処理することの適法性の根拠がない
  - 個人データ出力が不正確
  - 13歳以上向けと謳いながら未成年者の年齢確認がされていない
- 同年4月28日、OpenAIによる改善策（適法性の根拠については「管理者の正当な利益」を主張）が取られたとして、イタリアDPAは一時禁止を解除。
- 同月、フランスDPA等も調査を開始。2023年当時OpenAIはEU域内に拠点を持たず、GDPRのワンストップショップメカニズムによる協力手続きを適用できないため、EDPBは2023年4月13日に、ChatGPTにおける個人データ処理に関する執行措置について各国DPA間の協力を促進し、情報交換するためのTFを設立。
- イタリアDPAは2024年1月29日にOpenAIに対してデータ保護法違反を通知。2023年3月の命令後の調査結果に基づき、入手可能な証拠がGDPRの複数の規定への違反の存在を示していると結論付けた。また、将来的な最終決定においてはEDPBのChatGPTタスクフォースで進行中の作業を考慮するとした。
（https://gpdp.it/home/docweb/-/docweb-display/docweb/9978020）
- しかし、2024年2月15日にEU域内（アイルランド・ダブリン）にOpenAIの拠点が設立されたため、2024年2月以降も継続する違反や2月以降に発生した違反については、ワンストップショップメカニズムが適用され、アイルランドDPAが主たる監督機関としてOpenAIに対する是正権限を有することとなった。

# ChatGPTタスクフォース報告書の概要

- EDPBのChatGPTタスクフォースは2024年5月23日に、中間報告書である「ChatGPTタスクフォースによる業務報告書」を公表。各DPAが実施しているOpenAIに対する調査は進行中であり、調査結果の完全な説明を提供することはできないため、「本報告書の検討事項は、調査の特定の側面に関する予備的見解とみなされる」と但し書き。（https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-chatgpt-taskforce_en）
- 同報告書で指摘された、ChatGPTにデータ保護上で求められる要件は「①データ処理の適法性」「②公平性」「③透明性」「④データの正確性」「⑤データ主体の権利」の5つ。
  - 学習データの収集（Webスクレイピング）、およびChatGPTの入力・出力・学習のためのデータ処理の「適法性」。
  - 「公平性」：個人が個人データを入力する場合でも、GDPRの遵守を保証するのはOpenAIの責任であり、データ主体ではない。
  - 「透明性」と「データの正確性」：管理者であるOpenAIは、ChatGPTの出力の確率的な性質に関する適切な情報を提供し、生成されたテキストが偏っていたり、捏造されている可能性があるという事実に明示的に言及する必要がある。
  - データ主体が自らの「権利」を効果的に行使できることが不可欠。
- そしてこれらの要件は、「GDPR第25条(1)で規定されたデータ保護バイデザインの原則がデータ処理手段の決定時および処理自体の時点で考慮されなければならないことに鑑みると、技術的に不可能だという理由は、これらの要件を遵守できないことの正当化にはならない」として、サービスの設計時から組み込むべきことを強調。

# ChatGPTタスクフォース報告書の内容：　①適法性の根拠（1/3）

IISE

- 個人データ処理は、GDPR第6条(1)に規定された適法性の根拠の少なくとも１つ、また特別なカテゴリーの個人データの場合はGDPR第9条(2)に規定された追加要件を満たさなければならない。
- 適法性を評価する際には、個人データ処理の様々な段階を区別することが有用であり、ChatGPTについてはデータ処理の段階は以下に分類できる。
  - i) 学習データの収集（Webスクレイピングデータの使用を含む）
  - ii) データの前処理（フィルタリングを含む）
  - iii) 学習
  - iv) プロンプト（入力等）と出力
  - v) プロンプトを使用した学習
- i)～iii)の3段階は、個人の基本的権利と自由に対する特有のリスクを伴う。Webスクレイピングにより、ネット上の様々な公開ソースから情報が自動的に収集・抽出され、ChatGPT の学習目的に利用されるため。これらの情報にはデータ主体の個人的な生活の様々な側面を網羅する個人データが含まれうる。
- Webスクレイピングに関しては、OpenAI は GDPR 第 6 条(1)(f)（管理者の正当な利益）を適法性の根拠として提示。正当な利益の適法性の評価は、以下の基準に基づく必要がある（ドイツ連邦カルテル庁に対する欧州司法裁判所2023年7月4日判決）。また適法性の評価では、データ主体の合理的な期待を考慮する必要がある。
  - i) 正当な利益の存在
  - ii) 処理の必要性 ：個人データは、処理目的に関連して十分で、関連性があり、必要なものに限定されている必要がある
  - iii) 利益間のバランス：データ主体の基本的権利および自由と、管理者の正当な利益を慎重に評価し、バランスをとる必要がある

# ChatGPTタスクフォース報告書の内容：　①適法性の根拠（2/3）

IISE

- 十分な保護措置の存在は、データ主体への不当な影響を軽減する上で特別な役割を果たすため、上記のバランシングテストを管理者に有利なものに変更できる。ChatGPTに対する適法性の評価は調査中だが、そのような保護措置としては、正確な収集基準を設定し、一定のデータカテゴリーが収集されないことや特定のソース（公開ソーシャルメディアプロファイルなど）がデータ収集から除外されることを保証する技術的な措置が考えられる。
- また、学習段階の前に、Webスクレイピングによって収集された個人データを削除または匿名化する措置が講じられるべきである。
- 特別なカテゴリーの個人データの処理に関しては、処理が適法であるためには、さらにGDPR第9条(2)の例外の１つが適用される必要がある。この例外として有力なのは、第9条(2)(e)（データ主体によって明白に公開のものとされた個人データ）である。しかし、個人データが公にアクセス可能であるという事実だけでは、「データ主体がそのようなデータを明白に公開した」ことにはならない。第9条(2)(e)を適用するためには、データ主体が、明示的に、かつ明確な積極的行動によって、当該データを公衆がアクセスできるようにする意図を持っていたかどうかを確認することが重要である。
- 大量の個人データがWebスクレイピングによって収集される現在の状況では、各データセットを個別に調査することはほとんど不可能である。しかし、前述の保護措置は、GDPRの要件を満たすことに貢献することができる。例えば、これらの措置には、GDPR第9条(1)に該当する特別なカテゴリーの個人データのフィルタリングが含まれるべきである。フィルタリングは、データ収集（例えば、データ収集基準の設定）とデータ収集直後（データの削除）の両方に適用されるべきである。

# ChatGPTタスクフォース報告書の内容：　①適法性の根拠（3/3）

IISE

- iv) プロンプト（入力等）と出力、v) プロンプトを使用した学習の段階についても適法性の根拠が必要である。プロンプトとは、ChatGPTなどのLLMとやり取りする際のデータ主体の入力、ファイルのアップロード、ChatGPT のデータ出力の品質に関するユーザーフィードバックを指す。OpenAI はこれらを「コンテンツ」と見なし、これらの情報を使用してモデルを学習させ、改善することを公言している。同社はこの文脈でも、GDPR 第 6 条(1)(f)（管理者の正当な利益）を適法性の根拠として提示している。また OpenAI は、学習目的での「コンテンツ」の使用をオプトアウトするオプションも提供している。
- データ主体には、そのような「コンテンツ」が学習目的で利用されうることを明確かつ確実に情報提供（通知）する必要がある。このような状況は、GDPR 第 6 条(1)(f)に基づく利益間のバランシングテストの文脈において考慮される要素となる。

# ChatGPTタスクフォース報告書の内容：　②公平性

IISE

- GDPR 第 5 条(1)(a)に基づく公平性の原則は、個人データがデータ主体にとって不当に不利益、違法な差別、予期せぬ、または誤解を招くような方法で処理されてはならないことを要求する包括的な原則である。公平性の重要な側面は、リスクの移転があってはならないことである。すなわち、管理者は自社のリスクをデータ主体に移転するべきではない。
- ChatGPT に関しては、例えばデータ主体がチャット入力に責任を負うという条項を利用規約に置くことによって、GDPRの遵守を保証する責任をデータ主体に移転してはならないことを意味する。
- むしろChatGPT が一般に公開された場合、個人が遅かれ早かれ個人データを入力することを想定する必要がある。個人データの入力がデータモデルの一部となり、たとえば特定の質問をする他人と共有される場合、OpenAI は引き続き GDPR を遵守する責任を負い、特定の個人データの入力がそもそも禁止されていたと主張するべきではない。

# ChatGPTタスクフォース報告書の内容：　③透明性と情報提供

IISE

- ウェブサイトなどの公開されているソースから個人データをWebスクレイピングする場合、GDPR 第 14 条（間接収集時のデータ主体への情報提供）の要件が適用される。Webスクレイピングによって大量のデータが収集されることを考えると、通常、各データ主体に状況を情報提供（通知）することは不可能である。この場合、GDPR第14条(5)(b)の例外（※）を適用できる可能性がある。

  ※そのような情報提供が不可能であるか、または過大な負担を要することが明らかな場合であって、管理者がそれらの情報を公衆が利用可能とすることを含め、データ主体の権利および自由ならびに正当な利益を保護するための適切な措置を講じている場合。

- 他方、ChatGPTと直接やり取りしながら個人データが収集される場合、GDPR第13条（直接収集時のデータ主体への情報提供）の要件が適用される。この文脈では、前述の「コンテンツ」（ユーザー入力）が学習目的で利用されうることをデータ主体に情報提供（通知）することが特に重要である。

# ChatGPTタスクフォース報告書の内容：　④データの正確性

IISE

- GDPR第5条(1)(d)に基づくデータの正確性の原則に関連して、入力データと出力データには違いがある。入力データには、Web スクレイピングを通じて収集されたデータや、ChatGPTの使用時にデータ主体が提供する「コンテンツ」（プロンプトなど）が含まれる。出力データには、ChatGPT に入力後の出力が含まれる。
- 学習時のデータ処理の目的はChatGPTをトレーニングすることであり、必ずしも事実上正確な情報を提供することではない。実際に、システムの確率的性質により、現在の学習アプローチでは、偏った出力や虚偽の出力を生成する可能性のあるモデルが作成される。また、ChatGPTによって生成される出力は、実際の正確性に関係なく、個人に関する情報を含め、エンドユーザーによって事実上正確であると受け取られる可能性がある。
- GDPR第5条(1)(a)に基づく透明性の原則に従い、生成されたテキストは構文的には正しくても偏りがあったり虚偽のものである可能性があるという事実を明示的に言及するなど、確率的出力作成メカニズムとその信頼性の限界に関する適切な情報が管理者によって提供されることが重要である。ただし、透明性の原則を遵守するために講じられるこのような措置はChatGPTの出力の誤解を避けるのに有益だが、上記の通りデータ正確性の原則を遵守するには十分ではない。

# ChatGPTタスクフォース報告書の内容：　⑤データ主体の権利

IISE

- GDPRはデータ主体の一連の権利を定義している。個人データにアクセスし、その処理方法について情報提供を受ける権利、削除権、訂正権、または特定の条件下で個人データを第三者に移行する権利（データポータビリティ）、データ主体のデータの処理を制限する権利、 DPAに苦情を申し立てる権利などがある。
- 管理者であるOpenAIは、プライバシーポリシー欧州版でこれらの権利を行使する方法に関する情報を提供している。複雑な処理状況とデータ主体が介入できる事実上の制限を考慮すると、データ主体が簡単にアクセスできる方法で権利を行使できることが不可欠である。
- この文脈において、OpenAIは電子メールによる連絡の可能性を提示しているが、データ主体の一部の権利はアカウント設定を通じてのみ行使できる。GDPRに従い、管理者はデータ主体の権利の行使を容易にするために提供する方式を継続的に改善しなければならない。OpenAIは、少なくとも当面、ChatGPTの技術的な複雑さのために個人データの訂正を実行できない場合、ユーザーに訂正から消去への移行を提案しているが、これについても改善の余地がある。

# 【ご参考】アイルランドのデータ保護監督機関によるGoogleの基盤モデルへの調査

IISE

- アイルランドのデータ保護監督機関（DPC、Data Protection Commission）は2024年9月12日に、GoogleのAIモデルに対する調査を開始。Googleの大規模言語モデルPaLM2の開発時、学習データとしてEU/EEAデータ主体の個人データを処理する際に、GDPR第35条のDPIA（データ保護影響評価）を実施する義務に違反していないかどうかの調査。
  - （https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-launches-inquiry-google-ai-model）
  - GDPR第35条（データ保護影響評価）では、特に新たな技術を用いるような種類の取扱い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おそれがある場合、管理者に事前にDPIAを行う義務が課されている。

# 付録２：

# EDPBの「GDPR第6条(1)(f)（正当な利益）に基づく個人データ処理に関するガイドラインver1.0」について

# 正当な利益ガイドラインの概要（1/2）

IISE

- EDPB（欧州データ保護会議）は2024年10月8日、「GDPR第6条(1)(f)（正当な利益）に基づく個人データ処理に関するガイドラインver1.0」を採択。11月20日までパブコメ募集。GDPR 第6条(1)(f)に規定されている、「管理者または第三者によって追求される正当な利益の目的のために必要な」個人データ処理を管理者が適法的に実行するために満たすべき基準を分析。
  - 「Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR Version 1.0」
  - https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

- GDPR第6条(1)(f)（正当な利益）は、第6条(1)で規定された、個人データ処理の適法性の根拠の1つ。
  - (a) データ主体の同意
  - (b) データ主体が契約当事者となっている契約の履行
  - (c) 管理者が服する法的義務を遵守
  - (d) 自然人の生命に関する利益の保護
  - (e) 公共の利益または公的な権限の行使
  - (f) 管理者または第三者によって追求される正当な利益（legitimate interests）の目的のために処理が必要となる場合。ただし、その利益よりも、個人データの保護を求めるデータ主体（特にそのデータ主体が子どもである場合）の利益ならびに基本的権利および自由の方が優先する場合を除く。
- 第6条(1)(f)は、他の適法性の根拠が適用できないレアな状況や予期しない状況に対する「最後の手段」として扱われるべきではない。また、第6条(1)(f)が他の適法性の根拠よりも制約が少ないという認識に基づいて自動的に選択されたり、その使用が不当に拡大されたりすべきではない。

# 正当な利益ガイドラインの概要（2/2）

IISE

- 個人データ処理がGDPR第6条(1)(f)に基づくためには、 以下の3条件をいずれも満たさなければならない。
  - 第一ステップ：管理者または第三者による正当な利益の追求が存在すること
  - 第二ステップ：その正当な利益のために個人データを処理する必要があること
  - 第三ステップ：データ主体の守るべき利益または基本的権利と自由が、管理者または第三者の正当な利益を上回らないこと（バランシングテスト）

- 特定の個人データ処理がGDPR第6条(1)(f)に基づくかどうかを判断するために、管理者は、これら３つの条件が満たされているか否かを慎重に評価し、文書化する必要がある。この評価は、データ処理の実行前に行う必要がある。

- GDPR第6条(1)(f)の適切な評価は単純な作業ではない。この評価を実行するには（特に管理者とデータ主体の相反する利益と権利のバランスをとるには）、正当な利益の性質や起源、データ主体に対する処理の影響、処理に関するデータ主体の合理的な期待、データ主体への過度の影響を限定しうる追加的な保護措置の存在など、多くの要素を十分に考慮する必要がある。
- 本ガイドラインは、第6条(1)(f)が適用される可能性のある特定の状況（詐欺防止、ダイレクトマーケティング、情報セキュリティなど）を含め、実際に評価をどのように実行すべきかについてのガイダンスを提供。

# 第一ステップの評価：正当な利益が存在するか（1/3）

IISE

〇利益の「正当」性

- 「利益」は、以下のすべての基準が満たされる場合、「正当」とみなされる可能性がある。
  - その利益が適法である。すなわち、EUや加盟国の法律に違反していない：（→例1）
  - その利益が明確かつ正確に表現されている：（→例2）

    正当な利益の範囲は、データ主体の利益または基本的権利と自由と適切にバランスが取れるように、明確に特定されなければならない。
  - その利益はリアルなもので現実に存在し、想定上のものではない：（→例3）

    正当な利益はデータ処理を実行する日に現実に存在し、有効でなければならず、その日に仮定的なものであってはならない（CJEU, judgment of 11 December 2019）。

例１：

- 電子タバコを販売する欧州企業は、EU 内の特定地域に住む顧客に販促メールを送信して自社の製品を販促したいと考えている。そのためには、そのような顧客の個人データ（メールアドレスや氏名など）を収集し、処理する必要がある。ダイレクトマーケティングの目的で個人データを処理することは、正当な利益のために行われるとみなされることが多いが、上記の状況では、その利益は「正当」であるとは見なされない可能性がある。なぜなら、電子タバコの販促を目的としたり直接的・間接的な販促効果を持つような情報社会サービスでの商業通信は、EUたばこ製品指令およびそれに基づく国内ルールの下で一般的に禁止されているからである。

# 第一ステップの評価：正当な利益が存在するか（2/3）

IISE

## ○利益の「正当」性（続き）

例２：

- 「地域住民による犯罪監視」を行う組織は、「地域社会の利益のために」、特定地域にビデオ監視システムを設置し、その地域で起こりうる犯罪行為をモニターすることを決定した。財産、健康、生命の保護は、状況によっては正当な利益とみなされる可能性があるが、本件で行われている処理に関して管理者が表明した利益は、一般的な表現で表現されており、具体的な安全上の問題には言及していないため、非常に曖昧である。したがって、その正当性を評価し、バランシングテスト等を行うには、十分に明確に表現されていない。

例３：

- ある新聞社は、顧客管理の一環として、新しい雑誌が創刊された場合に連絡先を取得できるように、購読を更新しなかった過去の購読者で構成されるデータベースの作成を計画している。データベースの作成時点では、新聞社には新しい雑誌を開発して創刊する具体的な計画はない。
- このケースでは、新しい雑誌の創刊は現時点では仮定にすぎないため、管理者がデータベースへの入力（GDPR の適用範囲に含まれるデータ処理）を通じて追求する利益は、リアルで現実に存在するとは見なさない。したがって、管理者が追求する利益は「正当」とは見なされない可能性がある。

# 第一ステップの評価：正当な利益が存在するか（3/3）

IISE

○「管理者または第三者」が追求する利益

- GDPR第6条(1)(f)では「第三者」の正当な利益にも言及しており、特定の第三者の利益もまた正当な利益となりうる（→例4）。第三者の利益の正当性は、管理者自身の利益に関して適用されるのと同じ基準（前述）に従って評価される。

例４：

- タクシー運転手が道路脇に停車し、スクーターがタクシーの横を通り過ぎた際、タクシー後部座席の乗客がドアを開け、スクーターに傷がついた。スクーター所有者は、タクシー運転手の保険会社に保険金を請求した。しかし、保険会社は、事故は運転手ではなくタクシー乗客の行動が原因で発生したという理由で、保険金を支払わないとスクーター所有者に通知し、タクシー乗客の方に損賠賠償を求めるよう通知した。
- これ従い、被害者であるスクーター所有者はタクシー会社に連絡し、加害者であるタクシー乗客に損害賠償請求するために、乗客の身元情報を提供するよう依頼した。
- 本件では、タクシー会社が管理者であり、タクシー乗客がデータ主体である。スクーター所有者は第三者であり、損害賠償請求できるように、損害を引き起こした乗客の身元情報を取得する正当な利益を有する。したがって、この文脈では、データ処理（乗客の個人データの共有）は、第三者の正当な利益を追求するために行われているとみなされうる。

# 第二ステップの評価：個人データ処理が正当な利益のために必要か

IISE

○データ処理の「必要」性

- 「必要」かどうかの評価には、管理者等によって追求される正当な利益が、データ主体の基本的権利と自由をより制限しない他の手段によって、実際に同様な効果をもって合理的に達成できないか否かを確認することが含まれる。合理的で、同様な効果をもつが、より侵害的でない代替手段がある場合、当該データ処理は「必要」とは見なされない可能性がある。
- この文脈で、CJEU（欧州司法裁判所）は、処理の必要性に関する条件は、GDPR第5条(1)(c)に規定された「データ最小化」の原則と併せて検討する必要があることを指摘（CJEU, judgment of 4 July 2023）。データ最小化原則によれば、個人データは「処理の目的に関連して十分で、関連性があり、必要なものに限定されて」いなければならない。CJEUはまた、データ処理は、特定された正当な利益の目的のために「厳密に必要な範囲でのみ」実行されるべきであることを強調（CJEU, judgment of 7 December 2023）。
- この厳密な必要性の要件は、例えばGDPR 前文47では、「詐欺を防止する目的で厳密に必要な個人データ処理は、関係するデータ管理者の正当な利益を構成する」と述べられている。

# 第三ステップの評価：バランシングテスト（1/7）

- 第三ステップの評価では、データ主体の守るべき利益または基本的権利と自由が、管理者や第三者の正当な利益を上回っていないことを評価し、両者のバランスをとる必要がある。（バランシングテスト）
- バランシングテストでは管理者は以下のことを特定し、説明しなければならない。

  - i) データ主体の利益、基本的権利および自由
  - ii) 処理がデータ主体に与える影響
    - a. 処理されるデータの性質
    - b. 処理のコンテキスト
    - c. 処理のさらなる結果
  - iii) データ主体の合理的な期待
  - iv) 相反する権利と利益の最終的なバランス。これには、さらなる軽減措置の可能性も含まれる

- バランシングテストでは、管理者がGDPRで規定された原則や義務を遵守していることが前提となる。したがって、本ガイドラインで示される追加的な保護措置（データ主体への影響を制限・緩和する措置）はGDPRで規定された法的義務を超えるものである。

# 第三ステップの評価：バランシングテスト（2/7）

IISE

○ i) データ主体の利益、基本的権利および自由

- データ主体の基本的権利と自由には、データ保護とプライバシーの権利が含まれる。また、身体の自由と安全の権利、表現と情報の自由、思想・良心・信教の自由、集会と結社の自由、差別の禁止、財産権、身体的・精神的完全性の権利など、データ処理によって直接的または間接的に（例えば萎縮効果を通じて）影響を受けうる基本的権利と自由も含まれる。
- データ主体の利益には、データ処理によって影響を受けうるあらゆる利益が含まれる。これには、金銭的利益、社会的利益、個人的利益が含まれる。

○ ii) 処理がデータ主体に与える影響： a. 処理されるデータの性質

- 処理されるデータの性質を精査する際に、管理者はとりわけ次の点に注意を払う必要がある。
  - 特別な種類の個人データ（センシティブデータ）はGDPR第9条に基づき追加の保護を受けるという事実、および特別な種類の個人データの処理は第9条(2)に規定された特定の追加条件の下でのみ許可されるという事実。
  - 有罪判決および犯罪に関連する個人データは、GDPR第10条に基づき追加の保護を受けるという事実。
  - データ主体が一般的によりプライベートであると考えるデータの種類（例：財務データ、位置データ）、または、より公的な性質を持つと考えるデータの種類（例：職業上の役務に関するデータ）。
- 原則として、処理されるデータの性質がよりセンシティブでプライベートであるほど、そのようなデータの処理がデータ主体に悪影響を及ぼす可能性が高くなり、バランシングテストでそのデータにより多くの重みが与えられる必要がある。

# 第三ステップの評価：バランシングテスト（3/7）

IISE

○　ii) 処理がデータ主体に与える影響：　b. 処理のコンテキスト

- 処理のコンテキストおよび特定のデータ処理方法も、データ主体の権利利益に影響を及ぼす可能性がある。管理者はとりわけ次の点に十分配慮する必要がある。
  - 処理の規模および処理される個人データの量（データ総量、データ主体あたりのデータ量、影響を受けるデータ主体の数）
  - データ主体に対する管理者の地位（例えば雇用主と従業員の関係では、サービス提供者と顧客の関係とは異なる評価が必要になる可能性がある）
  - 処理される個人データが他のデータセットと結合されるかどうか
  - 処理されるデータのアクセス可能性や公開性の程度
  - データ主体の地位（例えば脆弱な個人）
- さらに、GDPR第6条(1)(f)の文言自体から、データ主体が子どもである場合は特別な注意を払う必要がある。CJEUがGDPR前文38を参照して判断したように、子どもは個人データの処理に関するリスク、結果、保護措置、および個人データ処理に関連する権利についてあまり認識していない可能性があるため、個人データ処理に関して特別な保護を受けるに値する。CJEUは、そのような特別な保護は、マーケティング目的、パーソナリティやユーザープロファイルの作成目的、または子どもを直接対象としたサービスの提供の目的で、子どもの個人データを処理する場合に特に適用されるべきであると判断（CJEU, judgment of 4 July 2023）。

# 第三ステップの評価：バランシングテスト（4/7）

IISE

○　ii) 処理がデータ主体に与える影響：　c. 処理のさらなる結果

- 処理の結果は、データ主体の権利利益にさらなる影響を及ぼす可能性がある。処理されるデータの状況と性質に応じて、管理者は次の要因を考慮する必要がある。
  - 管理者が処理する個人データに基づく可能性のある第三者による将来の意思決定や行動
  - データ主体に関する法的効果の発生の可能性
  - 個人の排除や差別
  - 名誉毀損、より広義にはデータ主体の評判・交渉力・自律を損なうリスクがある状況
  - データ主体が被る可能性のある金銭的損失
  - 実際に代替手段がないサービスからの排除
  - 自然人の自由・安全・身体的精神的完全性・生命に対するリスク
- 管理者は、具体的に予見できる悪影響に加えて、データ主体が個人情報のコントロールを失ったり、個人情報の悪用や漏洩に気付いたりすることで生じる可能性のある、より広範な感情的影響も考慮する必要がある。継続的なモニタリング・追跡や個人識別されるリスクから生じうる、研究の自由や表現の自由などの保護されるべき行動に対する萎縮効果も、十分に考慮する必要がある。例えば、プラットフォーマーによるオンライン活動の継続的なオンラインモニタリングは、データ主体の私生活が継続的に監視されているという感覚を引き起こす可能性がある。

# 第三ステップの評価：バランシングテスト（5/7）

IISE

○　iii) データ主体の合理的な期待

- 管理者は、正当な利益とデータ主体の権利利益を比較検討する際に、データ主体の合理的な期待を考慮に入れる必要がある。データ主体の合理的な期待は、特にデータ主体がデータ処理やその結果に過度に驚かされるリスクを制限するために、バランシングテストにおいて重要な役割を果たす。この点で、合理的な期待の概念と、特定の分野で一般的な慣行と見なされるものを区別することが重要である。
- 合理的な期待は、データ主体に提供される情報に必ずしも依存しない。GDPR第12条～14条の情報提供義務を単に履行するだけでは、データ主体が特定の処理を合理的に期待できると見なすのに十分ではない。
- 網羅的ではないが、データ主体の合理的な期待を評価する際の考慮要素は以下。（→例5、例6）
  - データ主体との関係やサービスの性質：
    - データ主体との関係の存在（例：顧客／非顧客）。関係があった場合は、その関係の終了日も含む。
    - 関係の近さ（例：管理者が単一ブランドを持つ企業グループの一部である場合と、平均的な顧客には知られていない経済的つながりを持つ企業グループの場合。後者ではデータ主体がグループ間でのデータ共有を期待する可能性は低い）
    - データ収集の場所と文脈（例：データ主体は銀行ではCCTVを予期するが、衛生施設やサウナ施設では予期しない）
    - サービスの性質と特徴（例：常連顧客と、ニュースレターを購読しただけの見込み顧客では合理的な期待が異なる）
    - 関連する文脈で適用される法的要件（例：関連する関係に適用される機密保持要件）
  - 個人データが処理される「平均的な」データ主体の性質：
    - データ主体の年齢（未成年者の合理的な期待は成人のものと異なる場合がある）
    - データ主体が公人である程度
    - データ主体の（職業上の）地位、および特定の文脈で想定される処理に関する理解と知識のレベル（例：就職面接プロセスに関与する担当者は、自分の個人データの一部が求職者と共有されることをしばしば想定する）。

# 第三ステップの評価：バランシングテスト（6/7）

IISE

○ iii) データ主体の合理的な期待（続き）

例 5:

- SNSは、オンライン広告を通じて資金を調達する。オンライン広告は、SNSの個々の利用者に合わせて、とりわけ消費者行動・関心・購買力・個人の状況に応じて調整される。このような広告は、技術的には利用者に関する詳細なプロファイルの自動作成によって可能になる。そのために、利用者がSNSに登録する際に直接提供するデータに加えて、そのSNS内外で利用者やデバイス関連のその他のデータも収集され、利用者アカウントにリンクされる。データのアグリゲーションにより、利用者の嗜好や関心について詳細な結論を導き出すことができる。
- SNSは無料で利用できるが、利用者は、SNS運営者がパーソナライズ広告の目的で利用者の同意なしに自分の個人データを処理することを合理的に期待することはできない。さらに、SNS利用者はサービス改善などの他の目的であっても、それらのデータが処理されることを合理的に期待することはできない。

例 6:

- ある企業が、インターネットやソーシャルメディアで公開されている人々の顔画像を使用して広告用チラシを印刷している。写真に写っているのは、写真を公開した人々である。この場合、写真がデータ主体自身によって公開されたとしても、データ主体は、自分の写真が第三者企業によって処理され公開されることを合理的に期待することはできない。

# 第三ステップの評価：バランシングテスト（7/7）

IISE

○　iv) 相反する権利と利益の最終的なバランス

- 上記の評価の結果、データ主体の権利利益が管理者や第三者の正当な利益を上回らなければ、GDPR第6条(1)(f)に基づき当該データ処理が行うことが可能である。
- ただし、データ主体の権利利益の方が管理者等の正当な利益を上回る（バランシングテストに不合格）と思われる場合でも、管理者はデータ主体に対する処理の影響を制限するための軽減措置の導入を検討することができる。
- しかしこの軽減措置は、GDPR遵守のために管理者が法的に導入しなければならない措置と混同されてはならない。すなわち緩和措置は、例えば管理者の情報提供義務・セキュリティ義務・データ最小化原則に従う義務・データ主体の権利履行の遵守を保証する措置で構成することはできず、GDPRに基づくこれらの法的義務を遵守するために必要な範囲を超えるものでなければならない。
- 例えば、GDPR下での保護措置に加えて更なる追加の保護措置を導入することは、軽減措置と見なされる場合がある。（例：GDPR第17条(1)に列挙されている特定の根拠が適用されない場合でも消去権を行使できるようにする、GDPR第21条の制限なしに異議を述べる権利を行使できるようにする、処理が第6条(1)(f)に基づく場合でもデータポータビリティの権利を行使できるようにする等。）
- 管理者が軽減措置を実施することを決定した場合、バランシングテストを再度、実行する必要がある。
- バランシングテストはケースバイケースで評価する必要がある。管理者には、バランシングテストが適切に実施され、データ主体の権利利益が管理者等の正当な利益を客観的に上回っていないことを証明する義務がある。

# 企業グループ内での内部管理目的でのデータ処理

IISE

- GDPR前文48によれば、企業グループの一部である管理者は、顧客や従業員の個人データの処理を含め、内部管理目的で企業グループ内で個人データを移転することについて正当な利益をもちうる。（→例7）
- そのような処理が行われる場合、特に従業員の個人データに関する場合、管理者は、加盟国がGDPR第88条に従って規定した雇用文脈における個人データの処理に関するルールに十分配慮する必要があることに留意すべきである。

例 7:

- 企業グループ内のサービスを改善するために、当該グループの本社は、子会社の顧客が実際にどのくらいの期間に顧客であったか、この期間中に子会社について苦情を申し立てたか等について統計を取ることに決定した。これは、当該グループが顧客をより維持するために将来的に組織変更を行う必要があるかどうかを評価するためである。このために、顧客に関する一定の情報が子会社からグループ本社に共有される。本社によるこのデータ処理は顧客との契約関係に直接関連していないため、このような個人データ処理は、具体的な状況に応じて、GDPRの他の規定を遵守することを条件として、GDPR第6条(1)(f)に基づきうる。

# 法執行機関等への個人データの送信

- GDPR前文50では「犯罪行為または公共の安全に対する脅威の可能性を指摘し、個々のケースや同じ犯罪行為または公共の安全に対する脅威に関係する複数のケースで関連する個人データを所轄官庁に送信することは、管理者が追求する正当な利益とみなされるべき」としている。
- 前文50で「個別のケース」や「同じ犯罪行為または脅威」にわざわざ言及していることから、民間事業者が犯罪行為または脅威の可能性を法執行機関に体系的に報告するために個人データを全般的かつ予防的に収集することは、正当な利益としては想定されていないことが分かる。
- 管理者が個人データを予防的かつ体系的に収集・保存して法執行機関に提供できるようにするのではなく、その都度気づいた犯罪行為や公共の安全に対する脅威を法執行機関に報告したい場合には、GDPR第6条(1)(f)に基づき法執行機関と個人データを共有することを検討しうる。

例 8:

- 管理者がサイバー攻撃の被害者となり、個人データの漏洩が発生し、データ漏洩したデータ主体の権利と自由がリスクに晒された。GDPR第33条に従い、管理者は個人データの漏洩を監督機関に遅滞なく通知する。これには個人データの漏洩のレベルと起こり得る結果を判断するために必要な個人データが含まれうるが、これは管理者がGDPR第6条(1)(c)に基づき法的義務を遵守するためのデータ処理である。
- 攻撃を受けた管理者は、IP アドレスやオンライン識別子など、攻撃者に関連する個人データも保有している。管理者は、通知が国内法やEU法で義務付けられていない場合であっても、将来のサイバー攻撃の可能性を防ぎ、データ主体を保護するために、サイバー犯罪を所轄する法執行機関やサイバーセキュリティの所轄官庁にこれらのデータを通知することを望む場合がある。このような処理は、GDPR第6条(1)(f)に基づきうる。

# 報告者の略歴

IISE

- 小泉 雄介　（株）国際社会経済研究所 調査研究部 主幹研究員　yusuke-koizumi@nec.com
- 専門領域：
  - プライバシー/個人情報保護、国民ID/マイナンバー制度、海外政策動向調査、途上国市場調査
- 略歴：
  - 1998年　（株）NEC総研入社 ・ 2008年7月　日本電気（株）に出向
  - 2010年7月　（株）国際社会経済研究所（旧NEC総研）に復帰
  - 2012年～　電子情報技術産業協会（JEITA）個人データ保護専門委員会客員
- 主な著書
  - 『国民ID　導入に向けた取り組み』（共著、NTT出版、2009年）
  - 『現代人のプライバシー』（共著、NEC総研、2005年）
  - 『経営戦略としての個人情報保護と対策』（共著、工業調査会、2002年）　等
- 主な論文
  - 「『国民IDの原則』の素描：選択の自由を手放さないために」（日本セキュリティ・マネジメント学会誌2023年度第2号）
  - 「感情認識の倫理的側面：データ化される個人の終着点」（同学会誌2022年度第2号）
  - 「中央銀行デジタル通貨における個人情報保護と日本での発行モデル」（同学会誌2021年度第2号）
  - 「AI社会における「自由」と「安全」のトレードオフ：顔認識技術のケーススタディ」（同学会誌2020年度第2号）
  - 「『快適で安全』な監視社会 ―個人の自由が保障されなくていいのか」（岩波『世界』2019年6月号）等