WHITEPAPER

欧州（EU）AI規制法FAQガイド：規制内容、コンプライアンス、先進事例について

protiviti®
Global Business Consulting

はじめに

人工知能（AI）が世界中で急激な成長を続け、あらゆる企業が生産性、効率性、収益拡大の機会を探る中、多くの国で規制や基準、フレームワークが設けられ始めています。これらの規制の中でも最も注目すべきは、2024年8月に施行された欧州（EU）AI規制法です。

本稿では、同法に関連して今日最も頻繁に目にする質問への回答を提供します。AIに関する詳細およびプロティビティの最新の見解については、当社のAIインテリジェンスハブ（https://www.protiviti.com/us-en/artificial-intelligence-services）をご覧ください。

欧州（EU）AI規制法の概要

欧州（EU）AI規制法は、包括的な規制の枠組みであり、EU全域におけるAIの開発、導入、利用に適用されます。同法はAIを広く定義しており、機械学習のみならず、論理および知識ベースのアプローチを用いて、自律的な要素で動作し、所定の目的を達成できるあらゆるシステムを包含しています。この広範な定義により、さまざまな自動システムが規制の対象となっています。欧州（EU）AI規制法は、説明責任（アカウンタビリティ）、リスク管理、データガバナンス、堅牢性、セキュリティおよび透明性など、AIのさまざまな側面を規制することを目的としています。

欧州(EU)AI規制法における説明責任(アカウンタビリティ)と透明性についてどのような要件がありますか?

欧州(EU)AI規制法は、条文を通じて透明性と説明責任の重要性を強調しており、「この規制は、AIの透明性確保のため技術文書、記録管理などに関する具体的な要件と果たすべき義務を定めることにより、既存の権利保護とその救済手法を明示することを目的とする」と述べています。さらに、同法はその透明性について、適切なトレーサビリティと説明責任を明確化することで、AIの開発および使用の安全性を保証することと定義しています。これには、AIと相互に影響する関係であることを人間に認識させること、そしてAIの能力と限界について開発者や導入者が周知すること、ならびに影響を受ける人々の権利について明示することなどが含まれます。この法律の背景には、AIの透明性と説明責任を担保する狙いがあり、AIの使用者およびその他の利害関係者に情報を提供すべきという責任を設計者および導入者に課しています。

欧州(EU)AI規制法の対象となるAIはどのように識別されますか?

同法は、AIに関連するリスクの重要度を測定するために、リスク分類アプローチを採用しています。その分類は、以下の通り、次の4つの異なるグループから構成されています。

- 最初のグループは同法で明確に禁止されている許容されないリスクで、市民の個人情報やその他重要情報など、基本的人権を明らかに侵害する可能性が高いもの。
- 2つ目は、個人の健康、安全、基本的権利を脅かすものであるため、特定のコンプライアンス対策を実施するなど対応策が求められるハイリスクなもの。
- 3つ目は、嗜好の操作や行動バイアスを防ぐために透明性の確保が義務付けられるミドルリスクなもの。
- 4つ目は、僅かな制限のみを受けるローリスクなもの。

同法に違反した場合、ほとんどの場合は1500万ユーロまたは年間世界売上高の3%を罰金として支払うことになりますが、同法が禁止しているAIのシステム規制に関連する違反の場合は、3500万ユーロまたは年間世界売上高の7%にも達する可能性もあります。

AI導入の際にどのリスクグループが適用されるかを、企業はどのように認識すれば良いですか?

AIの使用事例にどのリスクカテゴリーが適用されるかを判断するには、AIが人権、安全、基本的価値観に与える潜在的影響を考慮する必要があります。以下は、適切なカテゴリーを見極めるためのポイントです。

- **許容できないリスク**:この場合、基本的人権を侵害する可能性が高いため、EUでの開発や使用は禁止されています。欧州(EU)AI規制法では、人間の行動を操作する、脆弱性を悪用する、ソーシャルスコアリングに関与する、サブリミナル効果を使用する、児童に悪影響を及ぼす、監視や社会的分類のためにバイオメトリックデータを使用するなどのAIを許容できないリスク例として挙げています。

- **ハイリスク**:人間の健康、安全および基本的人権に重大な脅威をもたらすAIはこのカテゴリーに分類されます。データの質、技術的な堅牢性、人間による監視、透明性など、厳しい要件を満たさなければ欧州での開発や使用は許可されません。例えば、生体認証、採用、信用スコアリング、法律/規制、教育、健康、交通、公共サービスなど民間の必要不可欠なサービスに使用されるAIなどが含まれます。

- **ミドルリスク**:操作やバイアスを防ぐための透明性対策が必要となります。これらのシステムでは、ハイリスクのシステムに比べて軽い規制要件が適用されます。

- **ローリスク**:リスクが低く、規制要件が最小限の分類となります。例えば、AI対応のビデオゲームやスパムフィルターなどが含まれます。

グローバル企業は、欧州(EU)のAI規制法のすべての要件と基準をどのようにクリアすれば良いですか?

グローバル企業に求められる要件と基準をクリアすることは容易ではありません。しかし、多くの大企業は、情報管理などAI以外の規制対応を既に熟知しており、既存のフレームワークを活用することで当該要件や基準をクリアすることは十分可能です。そのためには、まず世界各地の新たな法律や既存の規制への理解を深めることが重要です。これには、欧州(EU)AI規制法の具体的な要件を知るだけでなく、企業全体で使用されているAIのシステムと、それらのシステムに供給されるデータの内容を理解することも含まれます。AIがバイアスを増幅させないようにするためには、特定のグループによる不均衡な取扱いを理解することが極めて重要です。さらに、企業のリーダーや、AIおよびコンプライアンスに精通した第三者の専門家を巻き込むことも不可欠です。これらのアプローチにより、AIのあらゆる側面と当該法律への準拠が可能となります。また、各ステークホルダーの専門知識を活用することで、企業は法律の基準や要件に沿った包括的な戦略を策定することも可能です。

AI、ひいては欧州(EU)AI規制法に関連するGDPRの原則とは何ですか?

2018年5月25日に施行されたEUの一般データ保護規則(GDPR)は、EU居住者の個人データの処理および移転を規制しています。GDPRには、欧州(EU)AI規制法に関連する数多くの原則が含まれており、AIシステムを使用する際の個人データ保護を保証するいくつかの重要な概念が含まれています。これらの原則は、特にAIが個人データを処理する場合、GDPRと欧州(EU)AI規制法の両方を遵守するために不可欠です。以下に関連する主要なGDPRの原則を示します。

- **合法性**:AIは、GDPRに概説されている処理の法的根拠を遵守し、合法的な方法で個人データを処理しなければなりません。
- **公正性**:AIによる個人データの処理は、個人が不当または差別的な結果にさらされないよう、公正でなければなりません。
- **透明性**:AIは透明性をもって運用され、自動意思決定の背後にある論理を含め、個人データがどのように処理されているかについて明確かつアクセス可能な情報を提供しなければなりません。
- **目的の制限**:個人情報は、明示的かつ正当な目的のために収集されなければならず、それらの目的以外での処理を行ってはなりません。
- **データの最小化**:AIは、意図された目的を達成するために必要な最小限の個人データのみを処理しなければなりません。
- **正確性**:AIによって処理される個人データは、正確であり、最新の状態に保たれ、不正確な情報を修正するための措置が講じられていなければなりません。
- **保存の制限**:個人データは、必要な期間を超えて保存してはなりません。
- **完全性および機密性**:AIは、個人データの安全性を確保し、不正または違法な処理や偶発的な損失、破壊または損傷から保護しなければなりません。

GDPR施行後の最初の数年間、回答者の81%が、組織によって収集された顧客データに対してほとんど、あるいはまったく管理できていないと感じていました。(Pew Research)

GDPRは欧州(EU)AI規制法とどのような点で重複していますか?

GDPRが個人データ保護に焦点を当てているのに対し、欧州(EU) AI規制法はAIシステムに関連する広範なリスクに対処することを目的としています。しかし、重複している部分も見られます。例えば、どちらの規制も、自動化された意思決定における透明性と人間の監視の重要性を強調しています。しかし、GDPRへの準拠が自動的に欧州(EU) AI規制法への準拠を保証するわけではなく、その逆も同様であることを認識する必要があります。

欧州(EU)AI規制法とGDPRの両方を考慮すると、企業にはどのような影響がありますか?

EUでAIを開発または使用する組織は、GDPRと欧州(EU) AI規制法の両方を遵守する必要があります。これは、以下の行動を含みます。

- 個人データを処理するAIにGDPRの原則を遵守させる
- AIおよび/または特定のプロセスが法で定義されたリスク分類カテゴリーに該当することを認識する
- 両規制の要件を満たすために必要な技術的および組織的措置を実施する
- AIの使用および両規定に基づく権利について、個人に明確な情報を提供する

上記が未実施であれば、AIの開発・使用の前にGDPRおよび欧州(EU)AI規制法の両方の遵守状況を把握することから始める必要があります。

欧州(EU)AI規制法の遵守に関して、データ収集と処理に関する注目すべき課題は何ですか?

同法には次のような記載があります。「プライバシーおよびデータガバナンスとは、AIがプライバシーとデータ保護の規則に従って開発および使用され、品質と完全性の面で高い基準を満たすデータ処理を行うことを意味します。透明性とは、AIが適切なトレーサビリティと説明責任を明確化しながら開発および使用されることを意味します。同時に、人間にAIと相互に影響することを認識させ、使用者にAIの能力と限界について、また影響を受ける人々にその権利について適切に知らせることを意味します。」

このことを踏まえ、データの処理プロセスとそれへのアクセスはあらゆるAIプロジェクトの重要な要素であり、AI自体の品質に直接影響することを理解する必要があります。また、以下が重要な課題として挙げられます。

- **データの可用性と関連性**:データが正確であるだけでなく、テキスト生成や画像作成などの特定のAIタスクに適切であることの保証をする必要があります。
- **バイアスと多様性**:人間のバイアスがデータに染み込み、AIモデルから偏った出力が出る可能性があります。バイアスのない完全なコンテンツを生成するためには、多様なデータセットが不可欠です。
- **データの不均衡と完全性**:特定のグループやトピックが過小評価されないようにデータセットのバランスをとり、AIタスクに必要な重要な情報が欠けていないことを確認する必要があります。

グローバル企業が欧州(EU)AI規制法の要件と基準を遵守するために重要な要素はありますか?

この法律では、多くのデータ保護法と同様に、個人は自分のデータへのアクセス、修正、処理の停止を行うことができます(一定の例外を除く)。データの削除が求められた場合、生成AIには重大な課題が生じます。それらの課題には以下のものが含まれます。

- 企業が、生成AIソリューションで使用される学習データを直接管理できない場合がある
- たとえAIが個人のデータを使ってトレーニングされたとしても、AIはトレーニングデータからパターンを識別して使用するため、個人データの痕跡を保持している可能性があり、本当に「忘れる」ことはできない可能性が高い
- システムが、トレーニングデータから得た残骸、パターン、または完全なコンポーネントを再現する可能性がある
- センシティブなデータがトレーニングデータに含まれる場合、モデル全体の再トレーニングが必要になる可能性があるが、これは複雑でリソースを大量に消費するプロセスになりかねない

これは法律の発展途上の分野であり、米国の連邦取引委員会のような規制機関は、いくつかのケースでアルゴリズムによる廃棄を救済措置として用いています。汎用AI(GPAI)モデルのプロバイダーは次のことを遵守しなければなりません。

- トレーニングやテストのプロセス、評価結果を含む技術文書の作成

- GPAIモデルを自社のAIシステムに統合しようとする下流プロバイダーに提供するための情報および文書を作成し、後者がその機能と制限を理解し、準拠できるようにする
- 著作権指令を尊重する方針を確立する
- GPAIモデルのトレーニングに使用したコンテンツについて、十分に詳細な概要を公表する

システムリスクをもたらすGPAIモデルへの影響はどのようなものですか?

GPAIがシステムリスクを引き起こす可能性がある場合、プロバイダーは以下を追加で行う必要があります。

- システムリスクを特定し、軽減するための対抗テストの実施と文書化を含むモデル評価
- 起こりうるシステムリスク(その発生源を含む)の評価とその軽減
- 重大インシデントと可能な是正措置を文書化し、欧州AI事務局および関連する各国の所轄官庁に過度な遅滞なく報告すること
- 適切なレベルのサイバーセキュリティ保護の確保

当該法律では、誰がAIの精度に責任を持ちますか?

他の国や地域では、AIの正確性に対する責任が管轄区域や特定のAI規制によって異なる場合がありますが、欧州(EU) AI規制法では、AIシステムのプロバイダーに最も広範な義務を課しています。

欧州(EU)AI規制法に関して、AI導入に伴うリスクを軽減するための好事例はありますか?

欧州での好事例には次のものが含まれます。

- AIの使用事例とシステム(サードパーティを含む)の一覧を維持し、先に定義したリスクレベル(許容できない、高い、限定的、最小)に基づいて分類
- データ保護法に基づくすべての義務の認識と理解
- 徹底した影響評価の実施
- 透明性の評価とモニタリング
- プライバシーと倫理を設計に統合
- 明確な契約条件の確立
- AIシステムの精度とバイアスの定期的な評価

Call to Action(重要ポイント)

欧州(EU) AI規制法を確実に遵守し、組織内でAIを効果的に管理するためには、以下の対応をとることが極めて重要です:

1 **欧州(EU) AI規制法を理解する**:EU全域におけるAIの開発、導入および利用を管理するために設計された包括的な規制の枠組みを理解する必要があります。同法はAIを広範に定義しており、機械学習、論理ベース、知識ベースのアプローチを用いて、自律的な要素で動作し、所定の目的を達成できるあらゆるシステムを包含しています。

2 **AIシステムを分類する**:人権、安全、基本的な価値観への潜在的な影響を考慮し、AI導入がどのリスクグループに属するかを判断する必要があります。この法律では、「許容できないリスク」、「ハイリスク」、「ミドルリスク」、「ローリスク」という4つのグループによるリスク分類アプローチを採用しています。

3 **GDPR遵守を確保する**:合法性、公正性、透明性、目的の制限、データの最小化、正確性、保存の制限、完全性および機密性など、AIシステムに関連するGDPRの原則に沿ったAIの運用が必要です。

4 **先進事例を導入する**:徹底的な影響評価の実施、透明性と説明可能性の維持、プライバシーと倫理の設計による統合、AIシステムの精度とバイアスの定期的な評価など、AI導入に伴うリスクを軽減するための先進事例を採用します。

5 **最新情報を把握する**:プロティビティのAIインテリジェンスハブなどのリソースを利用して、AIや欧州(EU) AI規制法に関する最新の見解を入手してください。

これらのステップを踏むことで、組織は欧州(EU) AI規制法の複雑さを効果的に回避し、AIの責任ある利用が可能となります。

Face the Future with Confidence®

protiviti®
Global Business Consulting